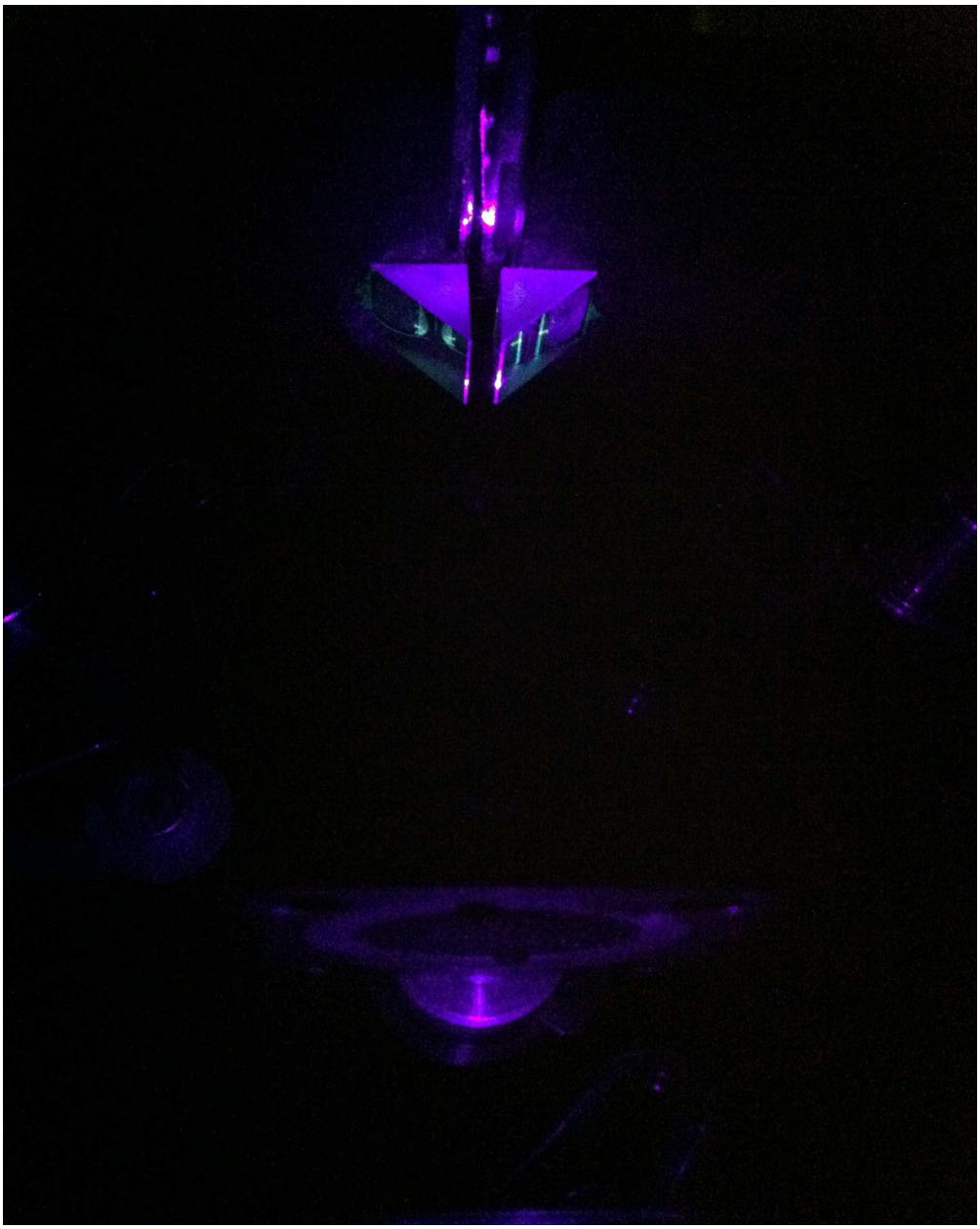
ชุดหนังสือสารสนเทศเชิงควอนตัม ๑

พัฒนาการสารสนเทศเชิงควอนตัม

Development of Quantum Information

พบพร ด่านวิรุทัย
เกียรติศักดิ์ ศรีพิมานวัฒน์
และคณะ

Q-Ti Forum



การทำเนิดความพัวพัน (Entanglement): แสงเลเซอร์ย่านอุลตราไวโอเลตแยกเป็นสองแนวเมื่อผ่านผลึก BBO จากด้านล่างไปยังปริซึมซ้ายขวาด้านบนและทะลุตรงเพื่อการตรวจวัด แล้วจึงได้ฟูโฟตอนพัวพัน (Entangled Photon) ช่วงแสงอินฟาเรดในแนวปริซึมเดียวกันนำไปใช้สำหรับการสื่อสารรหัสลับ

(ภาพจาก *ห้องปฏิบัติการวิจัยการสื่อสารเชิงแสงและควอนตัม - OQC-JCCRU-เนคเทค-สวทช.*)

พัฒนาการสารสนเทศเชิงควอนตัม

(Development of Quantum Information)

พบพร ด่านวิรุทัย
เกียรติศักดิ์ ศรีพิมานวัฒน์
และคณะ

Thai Quantum Information Forum
(Q-Ti Forum)
2012

พัฒนาการสารสนเทศเชิงควอนตัม

(Development of Quantum Information)

โดย : พบพร ด่านวิรุทัย
เกียรติศักดิ์ ศรีพิมานวัฒน์

สนับสนุนเทคนิค : ภูมิ จันทรโมลี
พิทักษ์ พานทอง
ปัทมา คำมล

สนับสนุนการจัดทำ : จุฑาเพชร เวชรังษี
ปรมินทร์ แสงวงษ์งาม
นักศึกษาฝึกงาน ห้องปฏิบัติการวิจัยการสื่อสารเชิงแสงและควอนตัม
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สวทช.

พิมพ์ครั้งที่ 1 เมษายน 2555

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data
พบพร ด่านวิรุทัย.
พัฒนาการสารสนเทศเชิงควอนตัม = Development of Quantum Information.--
ปทุมธานี: กลุ่มวิจัยเทคโนโลยีสารสนเทศควอนตัมไทย, 2555.

170 หน้า.
1. ทฤษฎีควอนตัม. 2. กลศาสตร์. I. เกียรติศักดิ์ ศรีพิมานวัฒน์, ผู้แต่งร่วม. II. ชื่อเรื่อง.

530.12

ISBN 978-616-12-0212-5

Blog : (QIBook2012) *ข้อมูลหนังสือเบื้องต้น การอ้างอิงภาพประกอบ การอภิปรายคำถามท้ายบท และข้อแนะนำกับการแก้ไขข้อผิดพลาด ณ*
URL: http://www.stks.or.th/blog/?p=14123

ปกหลัง: *รูปปั้น เออร์วิน ชโรดิงเงอร์ นักวิทยาศาสตร์รางวัลโนเบลและหนึ่งในบิดาด้านกลศาสตร์ควอนตัมของโลก ณ มหาวิทยาลัยเวียนนา ประเทศออสเตรีย*

คำนำ

ความพยายามของนักวิทยาศาสตร์จากทั่วโลกที่จะนำหลักการของ “กลศาสตร์ควอนตัม” มาประยุกต์ใช้งานกับ “เทคโนโลยีสารสนเทศ” กำลังแพร่ขยายและมีความก้าวหน้าอยู่ทุกมุมโลกในการเข้ามามีบทบาทกับระบบสื่อสารและการคำนวณ ทั้งนี้หลักการของ “กลศาสตร์ควอนตัม” นั้นว่าด้วยเรื่องการเล็กลง เร็วขึ้น หรือการล้ำขอบเขต (Bound) ที่มีอยู่ในโลกวิทยาศาสตร์และเทคโนโลยีปัจจุบัน ไปสู่การหาหลักการใหม่ ๆ เพื่อนำมาประยุกต์ใช้ตอบสนองความต้องการของมนุษย์ได้มากขึ้น ดังนั้นเมื่อ “กลศาสตร์ควอนตัม” และ “เทคโนโลยีสารสนเทศ” สามารถนำมาพัฒนาร่วมกันได้ ย่อมแสดงเป็นนัยได้ว่า การสื่อสารข้อมูล (Communications) การประมวลผลข้อมูล (Computing) หรือเทคโนโลยีอื่น ๆ ที่เกี่ยวข้อง จะสามารถพัฒนาให้ทำงานได้เร็วขึ้น เล็กลง และอาจมีรูปแบบการประยุกต์ใช้งานแบบแปลก ๆ อย่างที่มนุษย์ไม่เคยได้เห็นมาก่อน

วิทยาการสารสนเทศเชิงควอนตัม (Quantum Information Science) การคำนวณเชิงควอนตัม (Quantum Computing) รหัสย่อและการส่งถ่ายข่าวสารเชิงควอนตัม (Quantum Dense Codes/Quantum Teleportation) และรหัสลับเชิงควอนตัม (Quantum Cryptography) จึงได้ถือกำเนิด เหล่าแขนงเทคโนโลยีสารสนเทศเชิงควอนตัม (Quantum Information Technology) นี้ มีพัฒนาการเริ่มทยอยก้าวออกสู่ท้องตลาดเพื่อใช้งานจริงได้บ้างแล้ว รวมทั้งได้มีการคาดการณ์เทคโนโลยี (Technology Forecast/ Foresight) และผลกระทบ (Impact) ทางสังคม การศึกษาและเศรษฐกิจจากหลายสำนักและปรากฏอยู่ในวารสาร รายงาน หรือแผนแม่บทของหน่วยงานวิจัยของหลายประเทศ ตลอดจนองค์กรระหว่างประเทศเช่นกัน ดังเช่น รหัสลับเชิงควอนตัมได้รับการจัดอันดับว่าเป็นหนึ่งในผลิตภัณฑ์ที่ต้องจับตามองของโลกหลังสหัสวรรษใหม่เป็นต้นมา การประชุมวิชาการและการจัดการเรียนการสอนด้านเทคโนโลยีสารสนเทศเชิงควอนตัมเริ่มเกิดขึ้นมากมายทั่วโลก การจัดสรรงบประมาณวิจัยของหน่วยงานวิจัย มหาวิทยาลัย และหน่วยงานทางด้านความมั่นคงและการทหารที่มีแนวโน้มมากขึ้นทุกปีในต่างประเทศ รวมทั้งตัวอย่างของสหภาพยุโรป ที่ได้ดำเนินโครงการรหัสลับเชิงควอนตัมระยะสี่ปี (SECOQC - EU FP6 ปี คศ.2004-2008) มูลค่าสิบเอ็ดล้านยูโร (11 M Euro) เป็นต้น เทคโนโลยีสารสนเทศเชิงควอนตัมได้ “เริ่ม” ก้าวเข้ามามีความสำคัญทางสังคม การศึกษาและเศรษฐกิจชัดเจนมากขึ้นโดยลำดับแล้ว

หนังสือฉบับนี้ จัดอยู่ในขั้นแรกของชุดหนังสือสารสนเทศเชิงควอนตัมสี่ระดับขั้นที่จัดทำเพื่อเผยแพร่และกระตุ้นหรือตอบรับต่อความก้าวหน้าของศาสตร์ฟิสิกส์แขนงใหม่นี้ อันประกอบด้วยบทสรุปงานวิจัยและรายงานการสำรวจสำหรับผู้สนใจงานวิจัยเชิงลึกในขั้นแรก ระดับที่สองคือหนังสือแบบเรียนเชิงเทคนิคสำหรับการศึกษาภาคทฤษฎีและปฏิบัติ ขั้นที่สามคือหนังสือบทความทางวิทยาศาสตร์ อภิธานศัพท์สำหรับบุคคลทั่วไปเพื่อติดตามความรู้ความก้าวหน้าให้สามารถก้าวทันการเปลี่ยนแปลงของเทคโนโลยีแขนงใหม่นี้ และระดับสุดท้ายคือบทวิจารณ์ แผนที่นำทางและยุทธศาสตร์งานวิจัยด้านสารสนเทศเชิงควอนตัมสำหรับผู้บริหาร ผู้กำหนดนโยบายหรือสำหรับบุคคลทั่วไป เพื่อใช้ในการประกอบการวางระบบการศึกษา หลักสูตรและงานวิจัย การพัฒนาบุคลากรกับการเตรียมความพร้อม รวมถึงการเชื่อมโยงสู่ภาคการประยุกต์ที่จะได้ออกแบบให้เหมาะสมสำหรับสังคมวิทยาศาสตร์เทคโนโลยีไทยต่อไป

Thai Quantum Information Forum

(Q-Ti Forum)

สารบัญ

หน้า

หน้า

หน้า

หน้า

บทที่ 1
ภาพรวมสารสนเทศเชิงควอนตัม
(Quantum information aspect)

อภิธานศัพท์ (Glossary)

- **การคัดลอกไม่ได้ (No cloning)**
  ผลจากทฤษฎีควอนตัมที่ไม่สามารถคัดลอกข้อมูลของสถานะเชิงควอนตัมที่ไม่ทราบค่าได้อย่างสมบูรณ์
- **การคำนวณที่มีประสิทธิภาพ (Efficient computation)**
  การแก้ปัญหาที่สามารถหาขั้นตอนวิธีในการคำนวณแบบฟังก์ชันพหุนามได้ ทำให้ใช้เวลาในการคำนวณเป็นฟังก์ชันพหุนามของขนาดปัญหา ปัญหาส่วนใหญ่ถูกนำมาใช้อย่างมากในการคำนวณต่างๆ เช่น ปัญหาการหาเส้นทางเดินที่สั้นที่สุด (โดยใช้คอมพิวเตอร์คำนวณ) เป็นต้น
- **การคำนวณที่ไม่มีประสิทธิภาพ (Inefficient computation)**
  การแก้ปัญหาที่ไม่สามารถหาขั้นตอนวิธีในการคำนวณแบบฟังก์ชันพหุนามได้ ทำให้ใช้เวลาอย่างน้อยเป็นฟังก์ชันเอกซ์โพเนนเชียลของขนาดของปัญหา เช่น ปัญหาหอคอยแห่งฮานอย (Tower of Hanoi) ที่จำนวนครั้งในการย้ายจานจะเพิ่มเป็นฟังก์ชันเอกซ์โพเนนเชียลของจำนวนจาน
- **ความทับซ้อนเชิงตำแหน่งเชิงควอนตัม (Quantum superposition)**
  คุณสมบัติของระบบควอนตัมที่สามารถมีค่าประกอบด้วยสองสถานะขึ้นไปในเวลาเดียวกัน โดยคุณสมบัติดังกล่าวจะยุบตัวลงเหลือเพียงสถานะเดียวเมื่อมีการวัดค่าเกิดขึ้นกับระบบนั้น
- **ทฤษฎีข่าวสาร (Information theory)**
  การผสมผสานความรู้ร่วมกันระหว่างสาขาคณิตศาสตร์ประยุกต์และวิศวกรรมไฟฟ้าที่เกี่ยวข้องกับการแปลงข้อมูลสารสนเทศให้เป็นปริมาณทางคณิตศาสตร์ ซึ่งได้รับการนำเสนอโดยบิดาวิศวกรรมสื่อสารโคลด แชนนอน (Claude E. Shannon)
- **เทคโนโลยีสารสนเทศเชิงควอนตัม (Quantum information technology)**
  เทคโนโลยีที่ประยุกต์จากเทคโนโลยีสารสนเทศแบบดั้งเดิมโดยอาศัยคุณสมบัติเชิงควอนตัมของอนุภาคเพื่อพัฒนาการใช้งานเทคโนโลยีสารสนเทศในรูปแบบใหม่ๆ ที่เร็วขึ้นและปลอดภัยมากขึ้น
- **เทคโนโลยีสารสนเทศแบบดั้งเดิม (Classical information technology)**
  การศึกษา ออกแบบ พัฒนา ประยุกต์ใช้งาน หรือจัดการระบบสารสนเทศด้วยเทคโนโลยีของคอมพิวเตอร์ปัจจุบัน
- **วิทยาการคอมพิวเตอร์ (Computer science)**
  ศาสตร์การศึกษาทฤษฎีพื้นฐานของการคำนวณและสารสนเทศ และวิธีการประยุกต์ใช้งานในระบบคอมพิวเตอร์
- **สปิน (Spin)**
  คุณสมบัติเฉพาะของอนุภาคมูลฐานที่อธิบายถึงลักษณะโมเมนตัมของอนุภาคนั้น

- **โครงการการกระจายสถานะพัวพันระหว่างพื้นดินกับดาวเทียม Space-QUEST (QUantum Entanglement for Space ExperimenTs)**
  โครงการวิจัยการสื่อสารด้วยสถานะพัวพันผ่านอวกาศระหว่างพื้นดินกับดาวเทียม นำโดย อันตัน ไซลิงเงอร์ (Prof. Anton Zeilinger) มหาวิทยาลัยเวียนนา ภายใต้การสนับสนุนของสำนักวิจัยอวกาศแห่งสหภาพยุโรป (European Space Agency: ESA)

- **พหุนาม หรือ โพลิโนเมียล (polynomial)**
  โพลิโนเมียลอันดับที่ "0" หมายถึง ค่าคงที่ ($P_0(x) = c$, constant) โพลิโนเมียลอันดับ "1" หมายถึง เส้นตรง ($P_1(x) = ax + c$) โพลิโนเมียลอันดับ "2" หมายถึง พาราโบลา ($P_2(x) = ax^2 + bx + c$) และโพลิโนเมียลอันดับ n หมายถึง($P_n(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$)

ข้อสรุปประจำบท (Summary)

Classical information technology is the current digital/analog technology era for computing and communications. The reduction in size of the computing devices has to be limited to individual particle scale where quantum behavior dominates and classical model of information becomes invalid. Quantum mechanical description of information is therefore needed to describe the information processing in small scales. Quantum information science is the merging of quantum physics, information theory and computer science to build up a fruitful multi-disciplinary era. Quantum Information Technology is the applications of quantum information into computing, communications, metrology and others. Using the properties like quantum superposition, the quantum states can be used to process several inputs at the same time; this is the ingredient behind the (polynomial-time) quantum factorization algorithm proposed by Peter Shor in 1994. The discovery of this quantum algorithm for factorization has threatened the current security based on computation – public-key cryptography. Meanwhile, the unique quantum property: 'entanglement' (or nonlocality) enables entirely new modes of communications: quantum teleportation, quantum dense coding, and entanglement-assisted quantum cryptography. Quantum teleportation is a scheme to send an exact quantum state through a classical channel employing previously distributed entanglement. Quantum dense coding is about to transmit 2-bit classical message while actually sending only single quantum bit (qubit) through communication channel, also, provided entangled states which are distributed among two parties. Quantum teleportation and dense coding might appear to be far from daily use while quantum cryptography have been well established and also entering the commercialization stage. Quantum cryptography, to be more specific, “quantum key distribution” provides an establishment of secret key among two (and more) parties using quantum states and classical processing. The fragility of quantum states, which will be irreversibly disturbed and turned into another states whenever measurement is done, guarantees the transmission of states with auto-detection of adversary – one attacking on the communication channel. The applications of quantum information in the level of few qubits, i.e., quantum key distribution, quantum communications, and few-quantum-bit computation have been well demonstrated (2010). However, for quantum computing to show significant improvement against classical computing, it requires large number of qubits to be processed in a controlled way. The interaction with the environment which causes the loss of quantum information and quantum properties is the main obstacle. Quantum error correction is then proposed to “protect quantum bit using entanglement”, and fault-tolerant quantum computation is also proposed to reliably process on quantum states even if the quantum evolution (series of quantum logic gates for computation) is not perfect (but bounded by a threshold value). Large-scale quantum computation is then possible, at least, in theory. The studies of quantum control, measurements and creation of multi-particle entanglement have been continuously developing in tempting to bring quantum information technology to real-life applications.

สารสนเทศเชิงควอนตัม (Quantum information) คือศาสตร์ที่ศึกษาและประยุกต์ใช้พฤติกรรมของกลศาสตร์ควอนตัม เพื่องานสารสนเทศหรือข่าวสารเพื่อใช้ในการสื่อสาร การคำนวณ และอื่นๆ เพื่อให้ได้มาซึ่งรูปแบบใหม่ในการสื่อสาร การคำนวณ และอื่นๆ ที่สอดคล้อง ซึ่งไม่มีในการสื่อสารและการคำนวณแบบดั้งเดิม โดยวิทยาการสารสนเทศควอนตัม (Quantum information science) เป็นการรวมความรู้สามสาขาเข้าด้วยกัน ได้แก่ ทฤษฎีสารสนเทศหรือข่าวสาร (Information theory) ซึ่งอธิบายขีดจำกัดของการสื่อสารดั้งเดิม วิทยาการคอมพิวเตอร์ที่ใช้อธิบายกระบวนการคำนวณหรือประมวลผล และสุดท้ายฟิสิกส์ควอนตัมโดยใช้เพื่ออธิบายพฤติกรรมของอนุภาค "*ที่นำมาใช้เป็นตัวสื่อ*" รูปแบบภาพรวมของสารสนเทศเชิงควอนตัมนี้อธิบายได้ด้วยภาพประกอบดังรูปที่ 1.1 [*Steane 1998*]

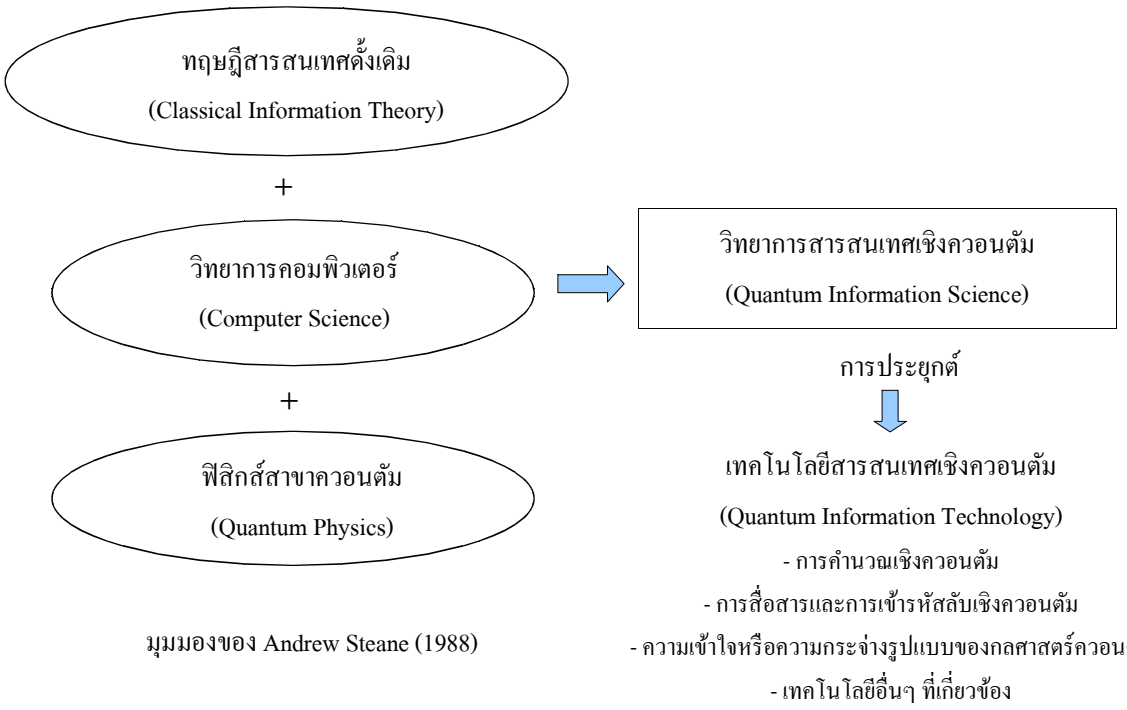
ศาสตร์แขนงนี้เริ่มมาจากการศึกษากระบวนการคำนวณในเชิงฟิสิกส์โดย รอล์ฟ ลานเดาเออร์ (Rolf Landauer) ซึ่งพิสูจน์ว่าทุกครั้งที่มีการลบข้อมูล จะต้องมีความร้อนขนาดหนึ่งเกิดขึ้นเสมอ เป็นการทดสอบความเชื่อมโยงระหว่างวิชาฟิสิกส์กับกระบวนการคำนวณ [*Landauer และ Bennett 1985*] และต่อมาริชาร์ด ไฟน์แมน (Richard Feynman) นักวิทยาศาสตร์รางวัลโนเบลสาขาฟิสิกส์ (ค.ศ. 1965) อภิปรายว่า การพยายามจำลองระบบควอนตัมด้วยความละเอียดสูงถ้าไม่จำกัดหรือมีขอบเขตนั้นจะไม่สามารถทำงานได้อย่างมีประสิทธิภาพในดิจิทัลคอมพิวเตอร์ เนื่องจากจำนวนตัวแปรที่ต้องใช้ในการอธิบายจะเพิ่มเป็นเอกซ์โพเนนเชียล[1.1] แต่ถ้าระบบที่ใช้จำลองระบบควอนตัมที่สนใจนั้น เป็นระบบควอนตัม (quantum mechanical computers) จะสามารถทำการจำลองอย่างมีประสิทธิภาพได้ [*Feynman 1982*] ต่อมาปีเตอร์ ชอร์ (Peter Shor) ได้ค้นพบวิธีคำนวณเชิงควอนตัมที่ช่วยในการแยกตัวประกอบได้ในเวลาลดลงที่จากเอ็กซ์โปเนนเชียลเหลือเพียงโพลิโนเมียล[1.2] [*Shor 1994*] ซึ่งหากทำได้จริงในสเกลใหญ่ๆ หรือมีปริมาณสูงจะส่งผลให้ความปลอดภัยของข้อมูลที่ใช้การเข้ารหัสแบบกุญแจสาธารณะ (Public-key cryptography) จะสูญเสียความปลอดภัยในทันที จึงมีแรงผลักดันในงานวิจัยและทดลองการใช้สถานะควอนตัม เพื่อสร้างกุญแจรหัสลับระหว่างสองฝ่าย (Quantum key distribution) (ซึ่งมีผู้เสนอไว้แล้วตั้งแต่ปี ค.ศ. 1984 – *ดูเรื่องรหัสลับเชิงควอนตัม บทที่ 2*)

คุณสมบัติเบื้องหลังการเกิดเป็นวิทยาการรหัสลับเชิงควอนตัมดังกล่าว คือ การคัดลอกไม่ได้ (No-cloning) ของสถานะควอนตัมที่ไม่ทราบค่า และการเกิดการเปลี่ยนแปลงต่อระบบเมื่อถูกทำการวัด ทำให้คู่สื่อสารทราบถึงการดักจับซึ่งมีผลต่อสถานะโดยคู่สื่อสารสามารถตรวจวัดและยกเลิกการใช้ข้อมูลที่ถูกดักจับนั้น อันเกิดเป็นวิทยาการรหัสลับสมบูรณ์แบบ

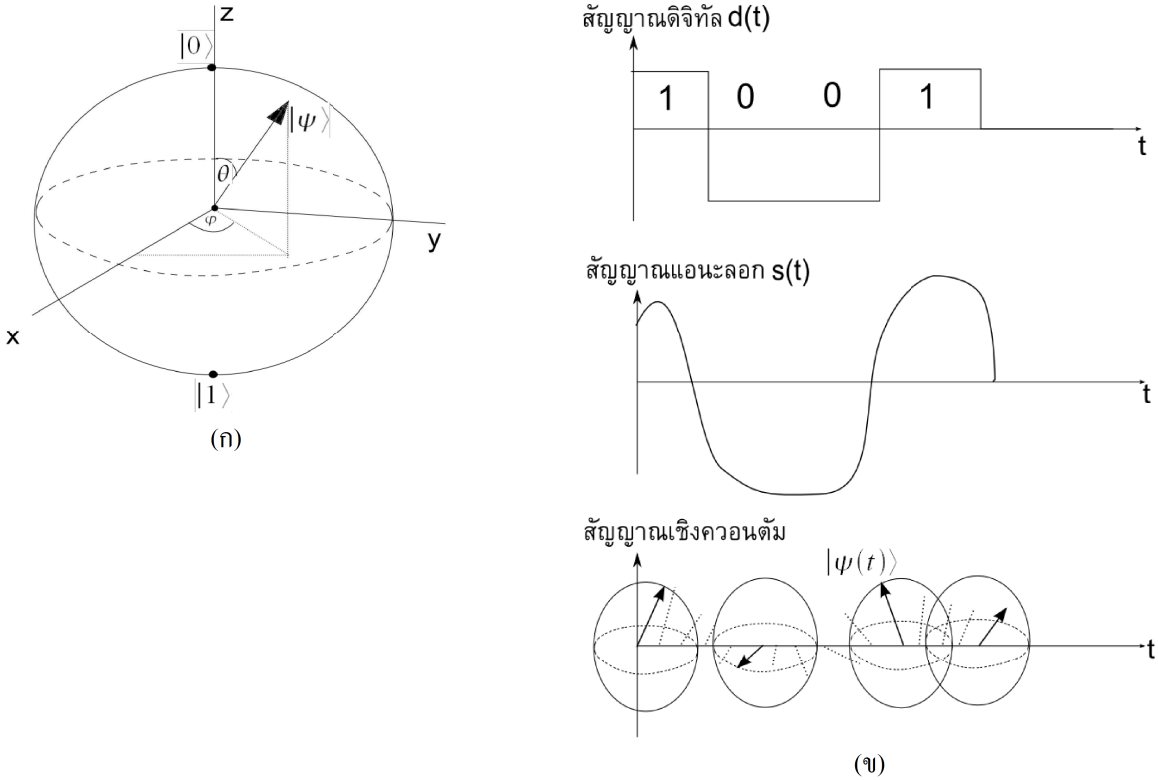
คุณสมบัติเชิงควอนตัมที่อยู่เบื้องหลังการคำนวณเชิงควอนตัมคือ การทับซ้อนเชิงตำแหน่ง (Quantum superposition) ซึ่งทำให้สถานะย่อยๆ ถูกประมวลผลในเวลาเดียวกัน บนรีจิสเตอร์ตัวเดียว และคุณสมบัติพัวพัน (Entanglement) เป็นหัวใจสำคัญในการสื่อสารเชิงควอนตัม และการป้องกันความผิดพลาดของข้อมูลควอนตัมในการคำนวณ โดยที่เมื่อคู่สื่อสารมีสถานะพัวพันร่วมกันแล้ว การสื่อสารในมิติใหม่สามารถทำได้ เช่น การกระจายกุญแจรหัสลับด้วยสถานะพัวพันนั้น การส่งผ่านสถานะควอนตัมโดยการส่งถ่ายเชิงควอนตัม (Quantum teleportation) และการส่งข้อความดิจิทัล (สองบิต) ด้วยสถานะควอนตัมซึ่งใช้บิตน้อยกว่า (หนึ่งคิวบิต) หรือการเข้ารหัสความเข้มสูงเชิงควอนตัม (Quantum dense coding) และการกระจายความลับไปสู่หลายบุคคลในเวลาเดียวกัน ซึ่งการทดลองสร้างสถานะพัวพันดังกล่าวนี้ได้มีความก้าวหน้าไปไกลถึงขั้นเสนอให้ทดลองกระจายสถานะพัวพันระหว่างพื้นดินกับดาวเทียมแล้ว (SPACE-Quest [*Ursin และคณะ 2008*])

1.1 ระบบ n คิวบิต ต้องใช้จำนวนเชิงซ้อน 2^{2n} จำนวนในการอธิบาย

1.2 โพลิโนเมียลอันดับที่ "0" หมายถึง ค่าคงที่ ($P_0(x) = c$, constant) โพลิโนเมียลอันดับ "1" หมายถึง เส้นตรง ($P_1(x) = ax + c$) โพลิโนเมียลอันดับ "2" หมายถึง พาราโบลา ($P_2(x) = ax^2 + bx + c$) และโพลิโนเมียลอันดับ n หมายถึง ($P_n(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$)



รูปที่ 1.1 ภาพรวมของวิทยาการและเทคโนโลยีสารสนเทศควอนตัม
(Quantum Information Science and Technology) [*Steane 1998*]



รูปที่ 1.2 (ก) ทุกจุดบนผิวทรงกลมที่เป็นผลรวมของสถานะทับซ้อนเชิงตำแหน่ง
สามารถแทนสถานะของหนึ่งบิตเชิงควอนตัม (Quantum bit หรือ Qubit)
(ข) เปรียบเทียบระหว่างสัญญาณดั้งเดิม ที่เป็นแบบดิจิทัล แอนะลอก และควอนตัม

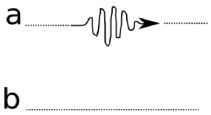
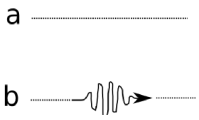
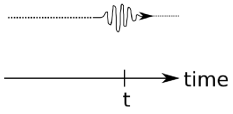
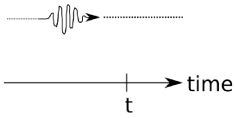
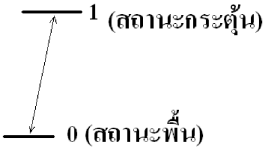
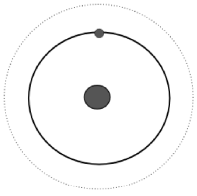
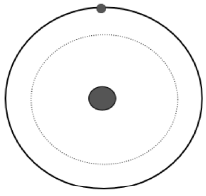
ตารางที่ 1.1 สรุปข้อเปรียบเทียบระหว่างบิต และ คิวบิต

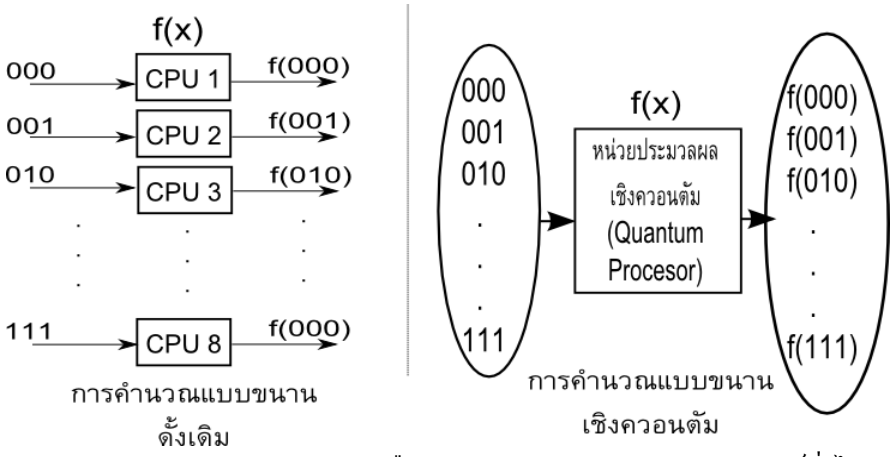
บิต (Bits)	**คิวบิต (Qubits)**
มีค่าได้เป็น “0” หรือ “1”	มีค่าเป็นผลรวมเชิงเส้นของ “0” และ “1” ($a\|0\rangle + b\|1\rangle$)
สามารถวัดค่าบิตได้อย่างแม่นยำ	ไม่สามารถวัดสถานะที่แน่นอนของคิวบิตได้
สามารถวัดค่าบิตได้โดยไม่ทำให้ค่าเดิมเปลี่ยน	การวัดคิวบิตสามารถทำให้ค่าเปลี่ยน
สามารถแยกแยะ “0” และ “1” ออกจากกันได้อย่างชัดเจน	2 คิวบิตใด ๆ ที่ไม่ตั้งฉากกัน ไม่สามารถแยกแยะอย่างชัดเจนได้
สามารถทำการคัดลอกบิตได้โดยไร้ข้อจำกัด	คัดลอกคิวบิต (ที่ไม่ทราบค่า) ไม่ได้
การรู้สถานะของบิตหนึ่ง ไม่มีผลต่อค่าสถานะของอีกบิตหนึ่งที่อยู่ไกลกัน	การรู้สถานะของคิวบิตหนึ่ง จะมีผลต่อค่าสถานะของอีกคิวบิตหนึ่งที่พัวพันกัน ถึงแม้จะอยู่ห่างไกลกันก็ตาม

สำหรับความแตกต่างระหว่างการคำนวณและการสื่อสารแบบดั้งเดิม (ดิจิทัลและแอนะลอก) กับแบบควอนตัมคือ ในการสื่อสารและการคำนวณแบบดั้งเดิม ค่าสถานะของข้อมูลจะเป็นค่าสเกลาร์ (จำนวนเต็ม หรือ จำนวนจริง) แต่การสื่อสารและการคำนวณเชิงควอนตัม ค่าสถานะจะแทนด้วยเวกเตอร์บนเซตซึ่งนิยามระบบควอนตัมนั้นๆ ซึ่งมีค่าเปลี่ยนไปตามเวลา ดังรูปที่ 1.2 โดยสามารถเปรียบเทียบความแตกต่างระหว่างบิตและคิวบิตได้ดังตารางที่ 1.1

ในการคำนวณเชิงควอนตัมนั้นอุปกรณ์สำหรับการคำนวณไม่ได้มีลักษณะเดียวกับคอมพิวเตอร์ปัจจุบันแต่เป็นอุปกรณ์ที่ควบคุมระบบควอนตัมใดๆ ก็ตามที่สามารถกำหนดสถานะเริ่มต้น ควบคุมการเปลี่ยนแปลง และอ่านค่าสถานะออกมาได้ ตามเงื่อนไขการทับซ้อนเชิงตำแหน่ง และคุณสมบัติความพัวพันดังที่ได้กล่าวในช่วงต้น มีการนำเสนอระบบทางกายภาพที่แทนคิวบิตหลายรูปแบบ ซึ่งรูปแบบที่นำเสนอนั้นเป็นอนุภาคใดๆ ก็ตามซึ่งสามารถแทนสองสถานะควอนตัมได้ (เป็นสถานะที่มีการนิยามอย่างชัดเจน และมีคุณสมบัติตั้งฉาก) เช่น โพลาไรเซชันของแสง จำนวนโฟตอน และสปินของอนุภาค (อิเล็กตรอน นิวตรอน) เป็นต้น ดังตารางที่ 1.2

ตารางที่ 1.2 ตัวอย่างระบบทางกายภาพที่นำมาแทนคิวบิต

ระบบกายภาพที่ใช้แทนคิวบิต	คุณสมบัติ	สารสนเทศ (ลอจิก)	
		“0”	**“1”**
โฟตอน	การจัดเรียงตัวเชิงเส้น (Linear polarization)	แนวตั้ง 	แนวนอน
	การจัดเรียงตัวเชิงวงกลม (Circular polarization)	ทวนเข็มนาฬิกา (left-circular polarization)	ตามเข็มนาฬิกา (right-circular polarization)
	จำนวนโฟตอน (Photon number)	ไม่มีโฟตอน	มี 1 โฟตอน
	เส้นทางที่แสงเคลื่อนที่ (Photon path)	ผ่านเส้นทาง a 	ผ่านเส้นทาง b 
	ตะกร้าเวลา ก่อน-หลัง (Time-bin)	โฟตอนมาถึงก่อน 	โฟตอนมาถึงหลัง 
อิเล็กตรอน	สปิน (Spin)	สปินมีทิศ +Z 	สปินมีทิศ -Z 
	ประจุ (Charge)	ไม่มีประจุ (ไม่มีอิเล็กตรอน)	มีประจุ (มี 1 อิเล็กตรอน)
นิวตรอน	สปิน (Spin)	สปินมีทิศ+Z 	สปินมีทิศ -Z 
อะตอม	ระดับพลังงาน (Energy level) 	สถานะพื้น  (ground state)	สถานะกระตุ้น  (excited state)



[CPU: Central Processing Unit หรือหน่วยประมวลผลกลางของคอมพิวเตอร์ทั่วไป]

รูปที่ 1.3 การเปรียบเทียบระหว่างการประมวลผลแบบขนานแบบดั้งเดิม (ดิจิทัล) และแบบควอนตัมที่พิจารณาแบบง่ายบนพื้นฐานของ “จำนวนครั้ง” ของการคำนวณจะลดลงอย่างมีนัยเมื่อใช้การคำนวณแบบควอนตัม – หมายถึงความเร็วในการคำนวณที่สูงขึ้น

อุปกรณ์สำหรับการคำนวณเชิงควอนตัม ที่ใช้ในการควบคุมและอ่านสถานะนั้นมีการจัดทำขึ้นเพื่อให้เหมาะสมกับระบบควอนตัมที่ถูกเลือกใช้ในงานคำนวณเชิงควอนตัม โดยและแต่ละระบบมีข้อดีข้อเสียแตกต่างกัน ซึ่งระบบต่างๆ ประกอบด้วย

1) การคำนวณเชิงควอนตัมด้วยสถานะของแสง อุปกรณ์มีขนาดเล็กและเคลื่อนย้ายได้สะดวก
2) การคำนวณเชิงควอนตัมด้วยไอออนที่ถูกกัก อุปกรณ์มีขนาดใหญ่ ราคาแพง แต่สามารถสร้างคิวบิตได้เป็นจำนวนมาก
3) การคำนวณเชิงควอนตัมด้วยอะตอมที่เป็นกลาง อุปกรณ์มีขนาดใหญ่ ราคาแพง แต่สามารถสร้างคิวบิตได้เป็นจำนวนมาก
4) การคำนวณเชิงควอนตัมด้วยนิวเคลียร์แมกเนติกเรโซแนนซ์ อุปกรณ์มีขนาดใหญ่ ราคาแพง และไม่สามารถเพิ่มจำนวนคิวบิตได้มากนัก แต่ถูกรบกวนจากสิ่งแวดล้อมภายนอกน้อย
5) การคำนวณเชิงควอนตัมด้วยควอนตัมดอท มีราคาแพง และเมื่อต้องการอ่านค่าของคิวบิตจะถูกรบกวนจากสิ่งแวดล้อมภายนอกได้ง่าย แต่อุปกรณ์มีขนาดเล็ก

ดังนั้นเมื่อพิจารณาการประมวลผลแบบขนาน (Parallel computing) ด้วยวิธีการเชิงควอนตัมแล้ว การคำนวณค่าฟังก์ชัน $f(x)$ ซึ่ง x มีค่าตั้งแต่ “000” ถึง “111” พร้อมกัน ต้องใช้หน่วยประมวลผลถึง 8 ตัว ในการคำนวณด้วยวิธีแบบดั้งเดิม (Classical) แต่ควอนตัมคอมพิวเตอร์ใช้หลักการทับซ้อนเชิงตำแหน่ง (Superposition) ของสถานะตั้งแต่ “000” ถึง “111” โดยมีหน่วยประมวลผลคือ การเปลี่ยนแปลงทางกายภาพ (Quantum dynamics หรือ Quantum processor) เพียงหน่วยเดียวในการคำนวณ ซึ่งทำให้ได้ $f(x)$ ออกมาพร้อมๆ กัน ดังรูปที่ 1.3 อันมีนัยถึงศักยภาพด้านการคำนวณที่สูงขึ้นอย่างมากด้วยกระบวนการทางควอนตัมนี้ และเป็นหัวใจของการพิจารณานำศักยภาพดังกล่าวนี้มาใช้งานกับระบบการคำนวณและระบบการสื่อสารรวมทั้งกับวิทยาการรหัสลับในยุค “สารสนเทศเชิงควอนตัม” ในรายละเอียดของบทต่อๆ ไป

เอกสารอ้างอิง

[Bennett และ Landauer 1985] C.H. Bennett, and R. Landauer, "Fundamental Physical Limits of Computation," *Scientific American* 253:1, pp. 48-56, July 1985.

[Feynman 1982] R. P. Feynman, "Simulating Physics with Computers," *Int. J. Th. Phys.,* vol. 21, No. 8, 1982.

[Shor 1994] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pp. 124-134, 1994.

[Steane 1998] A. Steane, "Quantum Computing," Rept. Prog. Phys. Vol. 61, pp 117-173, e-print: arXiv: quant-ph/9708022v2, 1998.

[Ursin และคณะ 2008] R. Ursin, et al. "Space-QUEST: Experiments with quantum entanglement in space," in *IAC Proceedings* A2.1.3, 2008.

คำถามท้ายบทที่ 1 (Questions and Answers)
และอภิปราย (Discussions) ปรับปรุง ณ
Blog: http://www.stks.or.th/blog/?p=14123

บทที่ 2

การสื่อสารเชิงควอนตัมกับการประยุกต์ด้านรหัสลับ

(Quantum communications and cryptography)

อภิธานศัพท์ (Glossary)

- **การเข้ารหัสลับแบบกุญแจสมมาตร (Symmetric-key cryptography)**
  ระบบการสื่อสารความลับโดยที่ต้นทางและปลายทางใช้กุญแจรหัสลับดอกเดียวกัน
- **การเข้ารหัสลับแบบกุญแจอสมมาตร (Asymmetric-key cryptography) หรือ การเข้ารหัสลับแบบกุญแจสาธารณะ (Public-key cryptography)**
  วิธีการเข้ารหัสลับที่ภาคส่งและภาครับใช้กุญแจคนละดอกในการเข้าและถอดรหัส โดยกุญแจทั้งคู่มีลักษณะเป็นฟังก์ชันผกผัน (Inverse function) ต่อกัน
- **การคำนวณเชิงควอนตัม (Quantum computation)**
  การคำนวณภายใต้กฎของกลศาสตร์ควอนตัม โดยการคำนวณเชิงควอนตัมจะเป็นตามคุณสมบัติการทับซ้อนเชิงตำแหน่ง และความพัวพัน ซึ่งทำให้การแก้ปัญหาบางอย่างทำได้เร็วขึ้น โดยความขนานเชิงควอนตัมซึ่งเป็นผลจากคุณสมบัติทับซ้อนเชิงตำแหน่งนั้น
- **กุญแจชิฟต์ (Sifted key)**
  บิตของกุญแจที่ได้จากการลบบิตหรือยกค่าออกจาก “กุญแจดิบ” ที่ต้นทางและปลายทางเลือกใช้เวกเตอร์ฐานไม่ตรงกัน
- **กุญแจดิบ (Raw key)**
  ในวิทยาการรหัสลับเชิงควอนตัม กุญแจดิบ หมายถึงกุญแจรหัสลับที่ได้จากการวัดสถานะเชิงควอนตัมจากผู้ส่ง ในแต่ละครั้งซึ่งมีการสุ่มเลือกรูปแบบฐานสำหรับการวัดสถานะ
- **ควอนตัม (Quantum)**
  ทฤษฎีที่ใช้อธิบายลักษณะของความเป็นก้อน ความไม่ต่อเนื่อง เช่นการที่ค่าของพลังงานมีค่าไม่ต่อเนื่องเป็นต้น โดยสิ่งที่พิจารณาสามารถประพฤติตัวเสมือนเป็นคลื่นหรือเป็นอนุภาคได้
- **ความตั้งฉาก (Orthogonality)**
  ก) เวกเตอร์สองเวกเตอร์ ตั้งฉากกันก็ต่อเมื่อผลคูณจุด (Dot product) หรือ ผลคูณภายใน (Inner product) ระหว่างเวกเตอร์ทั้งสอง มีค่าเป็นศูนย์
  ข) สำหรับเวกเตอร์ที่แทนสถานะควอนตัม เวกเตอร์ที่ตั้งฉากกันจะสามารถแบ่งแยกจากกันได้อย่างชัดเจน (Unambiguously distinguishable) ส่วนเวกเตอร์ที่ไม่ตั้งฉากกัน จะไม่สามารถแบ่งแยกกันได้อย่างชัดเจน (Unambiguously indistinguishable)
- **ความทับซ้อนเชิงตำแหน่งเชิงควอนตัม (Quantum superposition)**
  คุณสมบัติของระบบควอนตัมที่สามารถมีค่าประกอบด้วยสองสถานะขึ้นไปในเวลาเดียวกัน โดยคุณสมบัติดังกล่าวจะยุบตัวลงเหลือเพียงสถานะเดียวเมื่อมีการวัดค่าเกิดขึ้นกับระบบนั้น
- **ความปลอดภัยแบบไม่มีเงื่อนไข (Unconditional security)**
  ความปลอดภัยของข้อมูลที่ไม่ขึ้นกับวิธีการและความสามารถในการคำนวณของผู้ดักจับ
- **ความปลอดภัยสมบูรณ์แบบ (Perfect security)**
  รหัสลับมีความปลอดภัยสมบูรณ์แบบ ก็ต่อเมื่อรหัสลับและข้อความก่อนเข้ารหัสเป็นอิสระต่อกัน
- **ความพัวพัน (Entanglement)**
  คุณสมบัติทางกลศาสตร์ควอนตัม ซึ่งอนุญาตให้วัตถุ

(อนุภาค) ซึ่งอยู่ห่างไกลกัน สามารถมีสถานะร่วมกันได้ เรียกว่า สถานะพัวพัน โดยในสถานะดังกล่าว ไม่มีอนุภาคใดมีค่าสถานะที่แน่นอน ทันทีที่มีการวัดเกิดขึ้น ณ ที่ใดที่หนึ่งในอนุภาคที่พัวพันกัน คุณสมบัติของอนุภาคที่ฝั่งหนึ่งจะมีค่าขึ้นกับผลการวัดที่เกิดขึ้นกับอนุภาคอีกฝั่ง แม้ว่าจะอยู่ห่างไกลกันเพียงใดก็ตาม (สถิติการวัดของสถานะทั้งสองไม่เป็นอิสระต่อกัน)

- **ความสูญเสียความอาพันธ์ (Decoherence)**
  ก) กระบวนการเปลี่ยนแปลงคุณสมบัติของอนุภาค จากคุณสมบัติเชิงควอนตัม กลายเป็นคุณสมบัติแบบดั้งเดิม
  ข) กระบวนการที่ทำให้คลื่นเปลี่ยนคุณสมบัติจาก ความอาพันธ์ (Coherent) ไปเป็นอนาพันธ์ (Incoherent)
  ค) กระบวนการที่สถานะควอนตัมถูกรบกวนโดยสิ่งแวดล้อมจนสูญเสียคุณลักษณะเดิมไป (เหมือนกับ ก))
- **ความอาพันธ์ (Coherence)**
  ก) คุณสมบัติของคลื่นที่มีค่าความถี่และเฟสที่แน่นอน โดยคลื่นอาพันธ์สองลูกสามารถรวมกันโดยตรงและเกิดปรากฏการณ์แทรกสอดที่สังเกตได้
  ข) คุณสมบัติของคิวบิตมีค่าเฟสสัมพัทธ์ที่นิยามอย่างชัดเจน
- **คิวบิต (Qubit)**
  หน่วยพื้นฐานสำหรับการคำนวณและการสื่อสารเชิงควอนตัมหนึ่งคิวบิต มีค่าเป็นผลรวมเชิงเส้นของสถานะ “0” และ “1” ซึ่งเชิงเรขาคณิตพิจารณาว่าเป็นเวกเตอร์ 1 หน่วยบนผิวทรงกลม
- **ผู้ดักจับ (Eve)**
  ในวิทยาการรหัสลับเชิงควอนตัม ผู้ดักจับ หมายถึงผู้บุกรุกซึ่งพยายามดักจับข้อมูลกุญแจรหัสลับ
- **โพลาไรเซชัน (Polarization)**
  แนวการแกว่งตัวของสนามไฟฟ้าในคลื่นแม่เหล็กไฟฟ้า
- **เฟส (Phase)**
  ระยะที่เหลื่อมกันระหว่างหน้าคลื่นที่มีความถี่เดียวกัน โดยมีหน่วยเป็นเรเดียน
- **เฟสสัมพัทธ์ (Relative phase)**
  สำหรับสถานะคิวบิต $a|0\rangle+e^{i\beta}b|1\rangle$ ค่า $e^{i\beta}$ เรียกว่า เฟสสัมพัทธ์ระหว่างสองสถานะ $|0\rangle$ และ $|1\rangle$ โดยเฟสสัมพัทธ์ดังกล่าวมีผลในทางกายภาพ คือทำให้เกิดความแตกต่างของสถิติที่ได้จากการวัดค่า (ต่างจาก Global phase)
- **รหัสอาร์เอสเอ (RSA)**
  การเข้ารหัสลับแบบกุญแจสาธารณะรูปแบบหนึ่ง ซึ่งอยู่บนพื้นฐานของความซับซ้อนเชิงคณิตศาสตร์ในการแยกตัวประกอบจำนวนเต็ม เสนอเป็นครั้งแรกโดย โรนาลด์ ริเวสท์ (Ronald Rivest) อดิ ชาเมียร์ (Adi Shamir) และ ลีโอนาร์ด อเดลแมน (Leonard Adleman) (“RSA”) ในปี ค.ศ. 1978
- **เวกเตอร์ฐาน (Basis)**
  เวกเตอร์ที่นำมารวมกันเชิงเส้นได้เป็นเวกเตอร์ใดๆ ในปริภูมิเวกเตอร์นั้น เช่น เวกเตอร์หน่วยในแกน x และแกน y รวมกัน เป็นเวกเตอร์ฐานสำหรับเวกเตอร์ใดๆ บนระนาบ xy หรือ โพลาไรเซชันแนวตั้ง และแนวนอนรวมกันเป็นเวกเตอร์ฐานสำหรับโพลาไรเซชันในแนวใดๆ บนระนาบตั้งฉากกับทิศที่แสงแผ่ออกไป
- **สถานะควอนตัม (Quantum states)**
  ปริมาณทางคณิตศาสตร์ (เวกเตอร์) ที่แทนระบบทางควอนตัม สถานะควอนตัมของระบบเชิงควอนตัมสองระดับ (Two-level quantum system) มีความหมายเดียวกับ 'คิวบิต'
- **สหสัมพันธ์ (Correlation)**
  สหสัมพันธ์ระหว่างสถานะของสองสิ่งหมายถึง ความรู้ (มาก/น้อย) ถึงสถานะของสิ่งที่สอง เมื่อรู้สถานะของสิ่งแรกแล้ว ถ้าทั้งสองระบบมีสหสัมพันธ์กันอย่างสมบูรณ์แล้ว ทันทีที่ทราบสถานะของสิ่งแรกจะทราบข้อมูลทั้งหมดของสิ่งที่สอง

ข้อสรุปประจำบท (Summary)

For over 30 years since the intuition about applying quantum behavior to information security (Wiesner, 1983 and Bennett&Brassard, 1984), there have been gradual and also rapid progress in both theoretical and experimental sides. In secret key distribution application, quantum states guarantee that adversary cannot obtain the information sent while unperturbing the

states. That is, measuring out the information from quantum states will cause the states to change irreversibly. The change therefore can be detected by both communicating parties and they can ignore that bit of information. *Alice* and *Bob* can safely use the bits where no perturbation occurs. In later proposal, entangled-pair of particles can also be used to distribute the secret key. The test for the presence of adversary can be done by traditionally measuring the error rates or by testing the validity of nonlocal properties using Bell's theorem. Measuring the states cause entanglement (nonlocal) properties to disappear and this can be conceived by *Alice* and *Bob* who can again ignore the bits of communications. However, the fragile nature of quantum states makes that it is not easy to handle reliably in real experiments. All practical steps: preparing states, protecting information from the environment and detection of the states are non-trivial subjects which still need further study and improvement. The attenuated laser pulse with mean photon number much less than one was traditional source for quantum key distribution. Choosing proper degree of freedom or proper qubit representation to match with communication channel setting is also important. Phase-encoding is especially preferred in fiber-based quantum communication where the phase relation between input and output of fiber with the same length are quite fixed. While using polarization-coding in optical fibers meet some difficulties with polarization dispersion along the fibers, causing unwanted change in polarization. On the other hand, polarization-coding of photons is preferred in free-space quantum communication because the air mostly preserve the polarization while there may be fluctuations in phase due to turbulence and the uncertain atmosphere. This makes implementation of phase-coding in free space not quite feasible. There have been experimental demonstrations over a few hundred kilometers of distribution of quantum entanglement showing the ability to tolerate longer distance than using faint laser pulses. There are already projects proposed to demonstrate quantum entanglement and communication from ground to satellites (2010). In theoretical side, the security of each specific quantum key distribution protocols need to be proved. Theorists are trying to minimize the assumptions on the physical devices and on eavesdropping strategies. Security proofs are quite well-established in several quantum key distribution protocols under the tools from classical and quantum information theory. In order to promote and to test quantum key distribution in real world, the quantum key networking has been demonstrated in many places around the world, including the United States, Europe, China, Japan, and others. Stability test of the kind of network over several-months time period has been done in Switzerland. Quantum cryptography has now covered larger area than key distribution, to name a few, quantum authentication, quantum Vernam cipher, and quantum secret sharing have been proposed. The practicalities and merits of quantum information technologies, or, in specific, quantum cryptography have been showing more into the scene. It is interesting to keep the eyes on the progress of this fascinating field.

2.1 วิทยาการรหัสลับทั่วไป

ตั้งแต่มนุษย์เริ่มมีการสื่อสารระหว่างกันจากปกติในชีวิตประจำวันไปจนถึงการสื่อสารที่ต้องการรักษาความลับที่ทรัพยากรทั้งด้านเงิน เวลา หรือแม้กระทั่งชีวิตมนุษย์ได้ถูกนำมาใช้เพื่อทำให้แน่ใจว่าข้อความที่ส่งไปนั้นจะถูกอ่านได้โดยผู้รับที่ต้องการส่งให้เท่านั้น ข่าวสารที่ต้องการให้เป็นความลับเพื่อการติดต่อสื่อสารเหล่านั้นมีดังเช่น ข้อมูลในการศึกสงคราม ข้อมูลด้านธุรกรรมทางการเงิน เป็นต้น

2.1.1 ประวัติการสื่อสารเชิงความลับ

เทคนิคในการสื่อสารความลับเริ่มได้รับการกล่าวถึงโดยพลูทาร์ค (Plutarch) เมื่อ 100 ปี ก่อนคริสตกาลอธิบายไว้ว่า เมื่อบุคคลสองคนต้องการที่จะส่งข้อความลับระหว่างกัน จะมีการสร้างแท่งไม้ซึ่งมีลักษณะเหมือนกัน ทั้งความยาว และพื้นที่หน้าตัด

รูปที่ 2.1 "scytale" หรือแท่งไม้ที่ใช้พันข้อความสำหรับการสื่อสารแบบกุญแจสมมาตรวิธีหนึ่ง

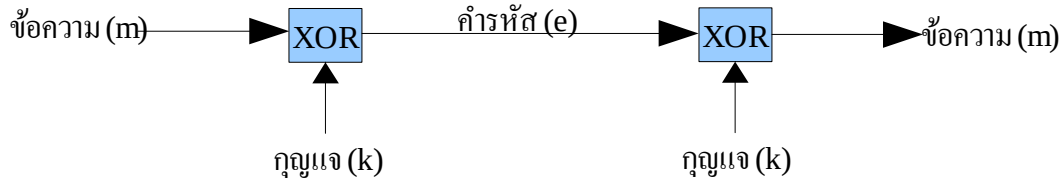
เรียกว่า *'scytale'* (รูปที่ 2.1) และเก็บไว้ที่ผู้ส่งและผู้รับสารฝ่ายละหนึ่งอัน เมื่อต้องการส่งข่าวสารลับ ผู้ส่งจะทำการพันผ้ารอบแท่งไม้ (ลักษณะเดียวกับการพันด้ามไม้เทนนิสหรือแบตมินตัน) จากนั้นเขียนข้อความที่ต้องการลงไปตามแนวยาวของไม้แล้วคลี่ผ้าออก ทำให้ตัวอักษรปะปนกันไม่เป็นคำ แล้วส่งแถบผ้าที่มีตัวอักษรดังกล่าวไปโดยไม่ส่งแท่งไม้ไปด้วย ผู้รับแถบผ้าจะเห็นตัวอักษรปะปนกันไม่เป็นลำดับ เว้นแต่ผู้มีแท่งไม้ที่มีลักษณะเหมือนกันกับผู้ส่ง ซึ่งเมื่อนำแถบผ้ามาพันรอบแท่งไม้นั้น จะปรากฏข้อความที่ต้องการสื่อสารกลับคืนมา ดังรูปที่ 2.1

แนวคิดของการใช้ 'แท่งไม้' ดังกล่าวในการสื่อสารข้อความลับ เรียกว่า วิธีการสื่อสารความลับด้วยกุญแจสมมาตร (Symmetric code หรือ Symmetric key) ซึ่งผู้ส่งและผู้รับสารจะมีสิ่งหนึ่งที่เหมือนกัน เรียกว่า "กุญแจ" (ในกรณีนี้คือแท่งไม้) เพื่อใช้ในการเข้ารหัสและถอดรหัสข้อความลับตามวิธีที่ตกลงกันไว้ ผู้รับสารจะสามารถอ่านข้อความได้ก็ต่อเมื่อมีกุญแจซึ่งมีลักษณะเหมือนกับกุญแจของผู้ส่งสารทุกประการ หากมีผู้ไม่ประสงค์ดีต้องการแกะรหัสข้อความสามารถทำได้โดยใช้กุญแจคุณลักษณะต่างๆ (ในกรณีนี้คือแท่งไม้เส้นผ่านศูนย์กลางต่างๆ) มาทดลองถอดรหัสข้อความทีละครั้ง จนกระทั่งกุญแจที่ปรับใช้ บังเอิญตรงกับของผู้ส่ง จะได้ข้อความลับออกมา ซึ่งกรณีเช่นนี้เหมือนกับการที่โจรได้บัตรเอทีเอ็ม (ATM) แล้วเดาตัวเลขรหัสการกดเงินถูกต้องก็สามารถกดเงินออกมาได้

การเข้ารหัสความลับอีกชนิดหนึ่ง คือ การใช้กุญแจอสมมาตร (Asymmetric-key cryptography) ผู้ส่งสารและผู้รับสารไม่ได้ใช้กุญแจเดียวกันในการเข้าและถอดรหัส หากเป็นฟังก์ชันผกผัน (Inverse function) ต่อกัน นั่นคือ เข้ารหัสด้วยฟังก์ชันหนึ่ง แต่ถอดด้วยอีกฟังก์ชันหนึ่ง แล้วได้ข้อความเดิมกลับมา โดยฟังก์ชันที่ใช้เข้ารหัสจะประกาศให้รู้ได้ (Public) แต่การคำนวณหาฟังก์ชันผกผันที่ใช้ถอดรหัสต้องใช้เวลานาน โดยความลับของข้อมูลจะมีความปลอดภัยจนกว่ากุญแจรหัสลับ (ฟังก์ชันผกผัน) จะถูกค้นพบ โดยปกติอายุของกุญแจจะน้อยกว่าระยะเวลาที่ใช้ในการคำนวณหาฟังก์ชันที่ใช้ในการถอดรหัส เช่น ข้อความลับ มีคุณค่าอยู่ถึง 2 เดือน ต้องใช้รหัสที่ใช้เวลาในการถอดรหัสนานกว่า 2 เดือน ด้วยวิธีการดังกล่าวการสื่อสารความลับจึงสามารถทำได้ อันเป็น การเข้ารหัสโดยใช้กุญแจอสมมาตร เรียกอีกอย่างหนึ่งว่า การเข้ารหัสด้วยกุญแจสาธารณะ (Public-key cryptography)

การสื่อสารเชิงความลับแบบสมมาตรที่รู้จักกันดีวิธีหนึ่งคือ รหัสของซีซาร์[2.1] (Caesar cipher) โดยข้อความที่ต้องการส่งแต่ละตัวอักษรจะถูกแทนที่ด้วยตัวอักษรใหม่ซึ่งเลื่อนไปจากเดิมเป็นค่าคงที่ค่าหนึ่ง (กุญแจ) เช่น ให้เลื่อนไปข้างหน้า 3 ตัวอักษร สมมติข้อความที่ต้องการส่งคือ "ATTACK" จะถูกเปลี่ยนเป็นข้อความลับ "DWWDFN" ด้วยการเลื่อนไปข้างหน้าสามอักษร $(A \rightarrow D\,;T \rightarrow W\,;C \rightarrow F\,;K \rightarrow N)$ ซึ่งเมื่อข้อความลับนี้ถูกส่งไปถึงผู้รับ ซึ่งทราบว่ากุญแจคือการเลื่อนอักษรไปข้างหน้าสามตัวอักษร ผู้รับจะถอดรหัสโดยการย้อนตัวอักษรไป 3 ลำดับ $(D \rightarrow A\,;W \rightarrow T\,;F \rightarrow C\,;N \rightarrow K)$ และได้ข้อความกลับมาเป็น "ATTACK" ซึ่งตรงกับข้อความที่ผู้ส่งต้องการสื่อสาร แต่วิธีการดังกล่าวมี*ข้อเสีย*คือรหัส*ถูกเดาได้ง่าย* เนื่องจากตัวอักษรบางตัว เช่น "A" ซึ่งเป็นสระในภาษาอังกฤษจะปรากฏบ่อยกว่าอักษรอื่นที่ไม่ใช่สระและเมื่อเข้ารหัสแล้วในกรณีข้างต้นถูกเปลี่ยนเป็น "D" ซึ่ง "D" จะปรากฏมากในข้อความที่เข้ารหัสแล้ว นอกจากนี้กลุ่มอักษร เช่น "-ed" สำหรับกริยาอดีต (Past tense) และ "-ing" สำหรับคำอาการนาม (Gerund) ซึ่งปรากฏอยู่แทบทุกประโยคในภาษาอังกฤษ ผู้ดักจับจึงสามารถคาดเดาจากอักษร

[2.1] มาจากชื่อของ จูเลียส ซีซาร์ (Julius Caesar) กษัตริย์ของอาณาจักรโรมัน ในช่วง 100 ถึง 44 ปีก่อนคริสต์ศักราช



รูปที่ 2.2 พื้นฐานการเข้ารหัสแบบการใช้งานครั้งเดียว (One-time pad)

หรือกลุ่มอักษรที่ปรากฏบ่อยได้ว่ารหัสที่ใช้คืออะไร ด้วยเหตุผลดังกล่าว จึงมีการปรับปรุงวิธีเข้ารหัสใหม่ เพื่อให้ตัวอักษรตัวเดียวกันถูกเปลี่ยนเป็นตัวอักษรคนละตัวได้ โดยใช้เลขสุ่มเป็นรหัสในการเปลี่ยน เช่น “ATTACK” เปลี่ยนเป็นคำรหัส “DSVBFJ” ซึ่งรหัส (เลขสุ่ม) สำหรับการเลื่อนอักษรแต่ละตัวคือ 3,-1,2,1,3 และ 1 วิธีการนี้ ทำให้มีการกระจายตัวของอักษรที่ถูกเข้ารหัสแล้วดังนั้นการคาดเดารหัสลับจากอักษรที่ปรากฏบ่อยจึงไม่สามารถทำได้ นอกจากนี้ หากคำรหัสที่ใช้เป็น *จำนวนสุ่มแท้จริง*[2.2] และถูกใช้เพียงครั้งเดียว จะเป็นวิธีการที่ให้ความลับของการสื่อสารอย่างสมบูรณ์แบบ (Perfect security) ซึ่งมีการพิสูจน์ในปี ค.ศ. 1946 [*Shannon 1949*] เรียกวิธีการดังกล่าวว่า การแปะหรือการใช้งานครั้งเดียว (One-time pad) หรือ รหัสเวอร์แนม (Vernam cipher)[2.3]

2.1.2 ความปลอดภัยของข้อมูลโดยสมบูรณ์

สำหรับการคำนวณและการสื่อสารเชิงดิจิทัลได้มีการตกลงเป็นสากลในการแทนตัวอักษรแต่ละตัวด้วยเลขจำนวนเต็มบวก โดยค่าที่กำหนดเป็นมาตรฐานเรียกว่า รหัส ASCII (American Standard Code for Information Interchange) ซึ่งแทนอักษรภาษาอังกฤษแต่ละตัว รวมถึงอักขระพิเศษอื่นๆ ไปเป็นตัวเลขขนาด 7 บิต (0 ถึง 127) เช่น “HELLO” จะถูกเปลี่ยนเป็น “72, 69, 76, 76, 79” ในการแทนค่าการสื่อสารดิจิทัลจะแทนเลขดังกล่าวด้วยเลขฐานสอง เช่น H เท่ากับ 72 เขียนแทนด้วย “100 1000” (หรือเท่ากับ $2^6 + 2^3$) และรหัสที่ใช้ต้องเป็นเลขสุ่มความยาวเท่ากัน (7 บิต) เช่น “010 1100” โดยการเข้ารหัสจะทำด้วยการ “exclusive-OR” (XOR) ระหว่างตัวเลขของแต่ละอักษรในข้อความกับรหัสซึ่งเป็นเลขสุ่ม ในกรณีนี้ อักษรข้อความ “H = 100 1000” “XOR” กับรหัสคือ “010 1100” คำรหัส (ciphertext) เป็น “110 0100” ซึ่งจะถูกตีความเป็นตัวอักษร “d” แทนที่จะเป็น “H” และเมื่อถอดรหัส ก็ใช้รหัสเดียวกันในการ XOR กับคำรหัสที่ปลายทางได้รับ ดังนี้ คำรหัส “110 0100” XOR รหัส “010 1100” ได้ผลลัพธ์เป็นข้อความ “100 1000” = “H” ซึ่งจะได้อักษรเดียวกับต้นทางกลับคืนมา (ตามคุณสมบัติของ exclusive-OR ซึ่งกระทำสองครั้งแล้วจะได้บิตข้อมูลเดิม) โดยการเข้าและถอดรหัสลักษณะนี้เป็นไปในรูปแบบเดียวกันนี้กับทุกตัวอักษรของข้อความ

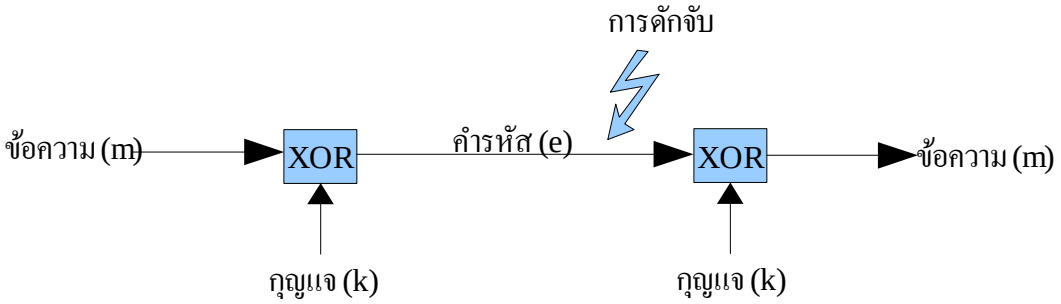
การใช้กุญแจซ้ำเดิมอาจมีความไม่ความปลอดภัย ดังนั้นการเข้ารหัสด้วยวิธีการใช้งานครั้งเดียวจะปลอดภัยก็ต่อเมื่อใช้กุญแจเพียงครั้งเดียว หากมีการใช้ซ้ำผู้ดักจับจะทราบถึงข้อมูลส่วนหนึ่งของข้อความได้ โดยนำคำรหัสของสองครั้งมา exclusive-OR กัน

$$(e_1 \oplus e_2) = (m_1 \oplus k) \oplus (m_2 \oplus k) = (m_1 \oplus m_2) \oplus (k \oplus k) = (m_1 \oplus m_2) \oplus 0 = (m_1 \oplus m_2)$$

ซึ่งผลลัพธ์เป็นค่า exclusive-OR ของข้อความทั้งสองส่วน $(m_1 \oplus m_2)$ ถึงแม้จะยังไม่ใช่ข้อความที่อ่านได้ แต่การใช้กุญแจซ้ำหลายๆ ครั้ง ยิ่งเป็นการเพิ่มข้อมูลเกี่ยวกับกุญแจที่รั่วไหลออกไป และเมื่อผู้ดักจับได้ข้อมูลเพียงพอจากการสังเกตความสัมพันธ์ระหว่างคำรหัสต่างๆ ผู้ดักจับจะทราบถึงรหัสที่ใช้ได้ในที่สุด

2.2 มีการกระจายตัวแบบสม่ำเสมอ (uniform distribution) แต่ละเลขสุ่มเป็นอิสระต่อกัน และลำดับของเลขสุ่มมีลักษณะไม่เป็นคาบ (non-periodic)

2.3 ตั้งชื่อเป็นเกียรติแก่ Gilbert Vernam ซึ่งเสนอวิธีการดังกล่าวในปี ค.ศ. 1926 และในปี ค.ศ. 1949 พิสูจน์ทางคณิตศาสตร์แล้วว่าเป็นวิธีที่ปลอดภัย ไม่สามารถถอดรหัสได้แม้โดยหลักการ



รูปที่ 2.3 ขั้นตอนทั่วไปของวิทยาการรหัสลับพื้นฐาน

2.1.3 ความหมายของวิทยาการรหัสลับ

วิทยาการรหัสลับหมายถึงศาสตร์แห่งการรักษาความปลอดภัยของข้อมูล (Security) รวมถึงเงื่อนไขอื่นๆ เช่น การยืนยันตัวตน (Authentication) และความน่าเชื่อถือของข้อมูล (integrity) [*Bruss และคณะ 2006*] วิทยาการรหัสลับเชิงควอนตัม (Quantum cryptography) หมายถึงศาสตร์ของการประยุกต์กลศาสตร์ควอนตัมเพื่อการใช้งานในด้านความปลอดภัยของการสื่อสารซึ่งครอบคลุมเรื่องการกระจายกุญแจเชิงควอนตัม (Quantum key distribution) การแบ่งปันความลับร่วมกันเชิงควอนตัม (Quantum secret sharing) และอื่นๆ แต่ในที่นี้จะเน้นเรื่องการกระจายกุญแจเชิงควอนตัม เพราะเป็นส่วนเติมเต็มให้รหัสลับที่สมบูรณ์แบบมีความเป็นไปได้ โดยเป็นวิธีการให้ได้มาซึ่งกุญแจสำหรับการเข้ารหัสดังรูปที่ 2.3

2.1.4 ขั้นตอนการสื่อสารความลับ

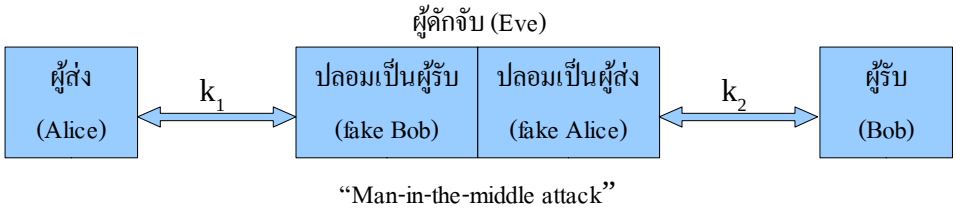
ขั้นตอนของการสื่อสารความลับแบ่งได้เป็นสามขั้นตอนหลักๆ คือ [*Stebila และคณะ 2009*]

2.1.4.1 การตกลงกุญแจรหัสลับร่วมกัน (Key agreement)

ผู้ส่งและผู้รับสารทำการตกลงกันเพื่อให้ได้มาซึ่งกุญแจรหัสลับสำหรับใช้ในการเข้าและถอดรหัส โดยวิธีดั้งเดิมคือใช้ผู้ส่งสารที่ไว้ใจได้ (Trusted courier) นำกุญแจไปสู่ผู้รับ และอีกวิธีหนึ่ง คือใช้การเข้ารหัสแบบกุญแจสาธารณะมาช่วยให้ได้กุญแจรหัสลับร่วมกันผ่านช่องสื่อสารสาธารณะ [*Diffie & Hellman 1976*] หรืออีกวิธีหนึ่ง คือใช้คุณสมบัติทางควอนตัมมาช่วยให้ได้มาซึ่งกุญแจร่วมกัน หรือ “การกระจายกุญแจเชิงควอนตัม” [*Brassard 2006*] ซึ่งเป็นหัวข้อหลักของวิทยาการรหัสลับเชิงควอนตัม

2.1.4.2 การยืนยันตัวตน (Authentication)

แม้ว่าการตกลงกุญแจรหัสลับจะเสร็จสิ้นแล้ว ผู้ส่ง (*Alice*) ต้องมีการยืนยันว่าผู้ที่ได้รับกุญแจไปเป็นผู้รับ (*Bob*) ตัวจริง และในทางกลับกันผู้รับก็ต้องการยืนยันว่าผู้ส่งกุญแจเป็นผู้ส่งตัวจริง เพื่อป้องกันการปลอมแปลงตัวตน (Man-in-the middle attack) ดังรูปที่ 2.4 ผู้ดักจับ (*Eve*) ปลอมเป็นผู้รับเพื่อสื่อสารกับผู้ส่งและขณะเดียวกันปลอมเป็นผู้ส่งเพื่อสื่อสารกับผู้รับหากข้อความที่สื่อสารดังกล่าวเป็นการส่งกุญแจรหัสลับ (k_1 และ k_2) ผลจะปรากฏว่าผู้ดักจับได้กุญแจรหัสลับของทั้งสองฝ่ายไป และสามารถทราบข้อความทั้งหมดที่จะเกิดขึ้นจากการใช้กุญแจดังกล่าว กระบวนการกระจายกุญแจเชิงควอนตัม (ที่ไม่รวมการยืนยันตัวตน) ไม่สามารถป้องกันการบุกรุกด้วยวิธีปลอมตัวตรงกลางได้



รูปที่ 2.4 การบุกรุกด้วยวิธีปลอมแปลงตัวตน

ตารางที่ 2.1 ประเภทของการเข้ารหัสข้อความโดยแบ่งตามชนิดของกุญแจ

ลักษณะกุญแจ	คำอธิบาย	ข้อดี-ข้อด้อย / การนำไปใช้	ตัวอย่าง
สมมาตร (Symmetric key)	ผู้ส่งและผู้รับใช้กุญแจดอกเดียวกัน	**ข้อดี** สามารถสอดคล้องเงื่อนไขความปลอดภัยสมบูรณ์ได้ **ข้อด้อย** ต้องหาวิธีตกลงกุญแจรหัสลับร่วมกัน	แท่งไม้ (Scytale) รหัสซีซาร์ รหัสเวอร์แนม DES AES
อสมมาตร (Asymmetric key)	ผู้ส่งและผู้รับใช้กุญแจคนละดอก (Public key และ Private key)	**ข้อดี** 1) ช่วยให้สามารถสื่อสารด้วยความปลอดภัยผ่านช่องสื่อสารสาธารณะได้ 2) ใช้ช่วยในการตกลงกุญแจรหัสลับร่วมกัน เพื่อนำไปใช้ในการเข้ารหัสแบบกุญแจสมมาตรต่อไปได้ **ข้อด้อย** ความปลอดภัยตั้งอยู่บนสมมติฐานของความซับซ้อนทางคณิตศาสตร์และทรัพยากรการคำนวณของผู้ไม่ประสงค์ดี	Diffie-Hellman, RSA [*Rivest, Shamir & Adleman 1976*], Elliptic-Curve cryptography [*Miller 1986*], ElGamal encryption [*ElGamal 1985*], Rabin cryptosystem

2.1.4.3 การใช้กุญแจในการเข้าและถอดรหัส (Key usage)

ขั้นตอนนี้คือการที่ผู้ส่งและผู้รับ ใช้กุญแจที่ได้ตกลงร่วมกันในการเข้าและถอดรหัสในรูปแบบที่เหมาะสมกับการสื่อสารหนึ่งๆ และการเก็บกุญแจส่วนหนึ่งไว้ใช้ในการยืนยันตัวตนสำหรับขั้นตอนการตกลงกุญแจรหัสลับร่วมกันในช่วงเวลาถัดไปด้วย

2.1.5 ประเภทของการสื่อสารความลับ

การสื่อสารความลับ (Cryptography) แบ่งประเภทตามลักษณะกุญแจที่นำมาใช้ได้สามประเภทหลักๆ ได้แก่ แบบกุญแจสมมาตร กุญแจอสมมาตร และไม่ใช้กุญแจ[2.4] ดังตารางที่ 2.1

[2.4] ใช้ฟังก์ชันแฮช (Hash function) ในวิทยาการรหัสลับจะต่างจากการเข้ารหัสลับ (Encryption/Decryption) ฟังก์ชันแฮชมีโอกาสที่จะทำการส่งข้อความไปยังค่าเดียวกัน ซึ่งแปลว่าฟังก์ชันแฮชมีคุณสมบัติย้อนกลับไม่ได้ ข้อความที่ผ่านฟังก์ชันแฮชโดยทั่วไปเรียกว่า message digest (ข้อความที่ถูกย่อย) ประยุกต์ใช้ในการยืนยันตัวตน (Authentication) และการยืนยันความถูกต้องของข้อมูล (Integrity)

2.2 ทฤษฎีสารสนเทศเชิงควอนตัมและความปลอดภัยของข้อมูล

การรักษาความปลอดภัยของข้อมูลสำหรับการสื่อสารโดยทั่วไปจะใช้เทคโนโลยีทางด้านสารสนเทศทั่วไปเพื่อรับรองความปลอดภัย แต่วิธีการดังกล่าวยังไม่สามารถยืนยันถึงความปลอดภัยได้อย่างสมบูรณ์ วิธีการหนึ่งที่สามารถยืนยันความปลอดภัยที่ได้ผลอย่างสมบูรณ์คือการนำทฤษฎีสารสนเทศเชิงควอนตัมมาใช้งานร่วมกับวิทยาการรหัสลับ ซึ่งกระบวนการพิจารณาถึงความปลอดภัยของข้อมูลมีดังนี้

2.2.1 ความปลอดภัยโดยสมบูรณ์ ความปลอดภัยอย่างไม่มีเงื่อนไข และความปลอดภัยเชิงการคำนวณ

2.2.1.1 ความปลอดภัยโดยสมบูรณ์ (Perfect security)

ถ้าการเข้ารหัส (Encryption) ทำให้คำรหัส (Cyphertext: *C*) มีความเป็นอิสระจากข้อความที่ยังไม่เข้ารหัส (Message: *M*) จะถือว่ารหัสลับนั้น มี*ความปลอดภัยสมบูรณ์* (*Perfect secrecy*) [*Shannon 1949*] ซึ่งสร้างเป็นสมการได้ดังนี้

$$p(M|C) = p(M) \qquad \text{.....(2.1)}$$

โดย M และ C เป็นตัวแปรสุ่ม และความน่าจะเป็นแทนด้วย p ดังนั้น $p(M|C)$ หมายถึง ความน่าจะเป็นของข้อความจะมีค่า M เมื่อคำรหัสมีค่าเท่ากับ C กล่าวคือการล่วงรู้ถึงคำรหัส (C) ก็ไม่ทำได้ให้รู้ถึงข้อความ (M) แต่อย่างใด นั่นคือไม่ทำให้รู้การแจกแจงความน่าจะเป็น (Probability distribution) ของข้อความเพิ่มขึ้น เงื่อนไขความปลอดภัยสมบูรณ์ดังกล่าวในเทอมของทฤษฎีข่าวสารคือ *สารสนเทศร่วมกัน (Mutual information)* ระหว่างข้อความ (M) และคำรหัส (C) เป็นศูนย์ [*Maurer, 1993*]

$$I(M;C) = 0 \qquad \text{.....(2.2)}$$

โดย $I(X;Y) = H(X) - H(X|Y)$ คือสารสนเทศร่วมกันระหว่าง X และ Y ซึ่งหมายถึง ความสามารถที่จะรู้ค่า X จากการรู้ค่าของ Y การที่ $I(X;Y)$ มีค่าเท่ากับศูนย์หมายความว่าการรู้ค่า Y ไม่มีผลต่อการรู้ค่าของ X แต่อย่างใด (รูปที่ 2.5 แสดงการตีความสารสนเทศร่วมกัน) และ เอนโทรปี $H(X)$ คือ ปริมาณความไม่แน่นอนของตัวแปรสุ่ม X นิยามโดย

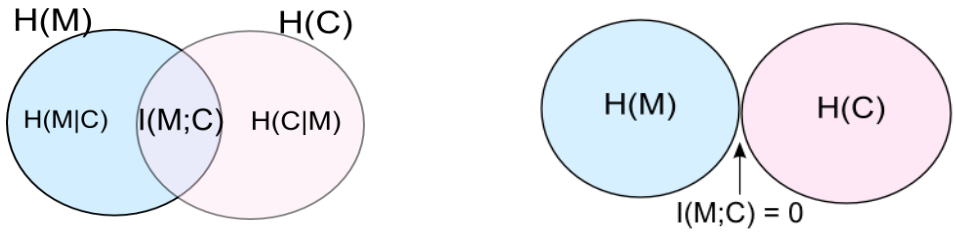
$$H(X) = -\sum_{x} p(x)\log p(x) \qquad \text{.....(2.3)}$$

$H(X)$ มีค่าเท่ากับจำนวนบิตที่น้อยที่สุดที่ใช้ในการอธิบายตัวแปรสุ่ม X (ทฤษฎีการเข้ารหัสแหล่งกำเนิด *"Shannon's source coding theorem"* [*Cover & Thomas 1991*]) และ $H(X|Y)$ หรือเอนโทรปีมีเงื่อนไข (Conditional entropy) คือ ความไม่แน่นอนของตัวแปรสุ่ม X เมื่อกำหนด Y มีค่าแน่นอนค่าหนึ่ง นิยามโดย

$$H(X|Y) = \boldsymbol{E}_{Y} H(X|y) = -\sum_{x,y} p(x,y)\log p(x|y) \qquad \text{.....(2.4)}$$

นอกจากนี้ ค.ศ. 1949 (พ.ศ. 2492) โคลด แชนนอน (Claude Shannon) ยังได้พิสูจน์เงื่อนไขที่จำเป็นสำหรับการมีความปลอดภัยโดยสมบูรณ์ กล่าวคือกุญแจรหัสลับต้องมีความยาวอย่างน้อยเท่ากับความยาวของข้อความที่ต้องการส่ง

$$H(k) \geq H(m) \qquad \text{.....(2.5)}$$



(ก) (ข)

รูปที่ 2.5 (ก) ความสัมพันธ์ระหว่างเอนโทรปี (*H*) เอนโทรปีมีเงื่อนไข *H(X|Y)* และสารสนเทศร่วมกัน (*I*) (ข) แทนคำอธิบายความปลอดภัยสมบูรณ์ $I(M;C) = 0$ การรู้ข้อมูลของ C ไม่มีผลต่อการรู้ข้อมูล M กล่าวอีกแง่หนึ่งคือ M และ C เป็นอิสระต่อกัน

หมายถึงอัตราการสร้างกุญแจรหัสลับร่วมกันต้องมากกว่าหรือเท่ากับอัตราการกำเนิดข้อความ โดยรหัสลับเวอร์แนมใช้กุญแจสุ่มซึ่งมีความยาวเท่ากับข้อความ ซึ่งเป็นคุณสมบัติสอดคล้องกับเงื่อนไขดังกล่าว ทำให้รหัสลับเวอร์แนมมีความปลอดภัยโดยสมบูรณ์ [*Dusek และคณะ 2006*]

2.2.1.2 ความปลอดภัยอย่างไม่มีเงื่อนไข และความปลอดภัยเชิงการคำนวณ (Unconditional security and computational security)

ความปลอดภัยโดยสมบูรณ์ของข้อมูล ซึ่งไม่ขึ้นกับทรัพยากรในการคำนวณ (เช่นเวลาและหน่วยความจำ) และกลวิธีในการเปลี่ยนแปลงข้อความโดยผู้ดักจับแต่อย่างใด (Security without any assumptions on Eve's computing resource and modification strategies) ส่วนความปลอดภัยเชิงการคำนวณ (Computational security) คือความปลอดภัยของข้อมูลที่ตั้งอยู่บนพื้นฐานของความซับซ้อนทางคณิตศาสตร์ โดยระยะเวลาที่ผู้ดักจับต้องใช้ในการคำนวณเพื่อถอดรหัสข้อความจะต้องมากกว่าหรือเท่ากับระยะเวลาที่ต้องการปกป้องข้อมูลนั้นๆ โดยทั่วไปให้นิยามว่า เป็นวิธีเข้ารหัสที่ต้องใช้เวลาในการถอดรหัสเป็นฟังก์ชันเอกซ์โพเนนเชียลของความยาวรหัส เช่น การแยกตัวประกอบใน RSA ซึ่งขั้นตอนวิธีที่ดีที่สุดในการคำนวณเชิงดิจิทัลสำหรับการแยกตัวประกอบ ต้องใช้เวลาเป็นอันดับเอกซ์โพเนนเชียล[2.5]

> จากอสมการที่ 2.5 ความปลอดภัยโดยสมบูรณ์ซึ่งต้องอาศัยการกระจายกุญแจที่เป็นจำนวนสุ่มไปยังผู้สื่อสารทั้งคู่ในอัตราที่มากกว่าหรือเท่ากับอัตราการสร้างข้อความนั้น เป็นเสมือนเรื่องที่ห่างไกลจากการใช้งานได้ในความเป็นจริง (สิ้นเปลืองทรัพยากร/ไม่คุ้มค่า) แต่หากเปลี่ยนการตั้งสมมติฐานเดิมจากแบบจำลองของแชนนอนที่ว่า "*ผู้ดักจับมีสิทธิ์รู้ข้อมูลเท่ากันกับผู้รับทุกประการ*" เป็น "*ผู้ดักจับไม่สามารถได้รับปริมาณข้อมูลเท่ากันกับผู้รับ*" ส่วนประเด็นที่วิธีการตกลงกุญแจรหัสลับที่มีความยาวเพียงพอนั้นสามารถกระทำทดแทนได้ด้วยความช่วยเหลือของกลศาสตร์ควอนตัม ซึ่งระบุว่าผลจากการวัดสถานะไม่สามารถบอกล่วงหน้าได้ ดังนั้นสถานะที่ผู้ดักจับรับรู้และส่งต่อให้ผู้รับ จะมีค่าแตกต่างจากผลลัพธ์ที่ผู้รับตรวจจับได้ ซึ่งจากความแตกต่างนี้เปรียบเสมือนเป็นเซ็นเซอร์ (Sensor) ตรวจหาผู้ดักจับ ทำให้ผู้ส่งและผู้รับสามารถสังเคราะห์บิตข้อความลับออกจากผลการตรวจวัดสถานะทั้งหมดและทราบสภาวะได้ กระบวนการดังกล่าวเรียกว่า *การกระจายกุญแจเชิงควอนตัม*

เมื่อนำมาเปรียบเทียบรายละเอียดของเงื่อนไขย่อยๆ ดังตารางที่ 2.2 แล้ว จึงเป็นที่มาของการนำกลศาสตร์ควอนตัมมาประยุกต์ใช้กับสารสนเทศในส่วนของรหัสลับได้ต่อไป

[2.5] หากมีการค้นพบขั้นตอนวิธีใหม่ในการคำนวณ เช่น ขั้นตอนวิธีเชิงควอนตัมแบบชอร์ [Shor 1994] จะทำให้รหัสดังกล่าวไม่สอดคล้องกับเงื่อนไขนี้ หรือแม้แต่มีการค้นพบขั้นตอนวิธีเชิงดิจิทัล ที่ใช้เวลาเป็นโพลิโนเมียล ความปลอดภัยของ RSA จะเสียไปในทันที ทั้งนี้ ยังไม่มีการพิสูจน์ว่า ไม่มีขั้นตอนวิธีเชิงดิจิทัลใดๆ ที่แก้ปัญหาแยกตัวประกอบได้เร็วกว่าอันดับเอกซ์โพเนนเชียล [Gisin และคณะ 2002]

ตารางที่ 2.2 การเปรียบเทียบ สมมติฐาน เงื่อนไขจำเป็นสำหรับความปลอดภัยสมบูรณ์ภายใต้สมมติฐานนั้น รวมทั้งปัญหาและการแก้ไข (ประเด็นสำคัญจาก [*Maurer 1993*])

สมมติฐานของขั้นตอนการตกลงกุญแจรหัสลับร่วมกัน	**เงื่อนไขจำเป็นสำหรับความปลอดภัยสมบูรณ์แบบ**	**ปัญหาที่อาจเกิดขึ้น**	**แนวทางการแก้ไข**
ผู้ดักจับได้รับข้อมูลเท่ากันกับผู้รับทุกประการ (ยกเว้นกุญแจรหัสลับที่แจกให้ผู้ส่งและ ผู้รับก่อนหน้าการสื่อสารนั้น)	ความยาวกุญแจมากกว่าหรือเท่ากับความยาวของข้อความ	เมื่อมีการส่งข้อความลับไปสักระยะหนึ่ง ข้อความ m จะต้องมีความยาวมากกว่ากุญแจรหัสลับ k แน่นอน (เพราะกุญแจรหัสลับซึ่งแจกก่อนหน้านั้น มีความยาวคงที่) ทำให้เงื่อนไขดังกล่าวไม่สามารถสอดคล้องได้	(1) ผู้ส่งและผู้รับใช้กุญแจรหัสลับที่มีอยู่ไปผ่านฟังก์ชันสร้างจำนวนสุ่มเทียม (Pseudo-random number generator) ที่มีคาบยาวมาก เพื่อให้ได้มาซึ่งกุญแจใหม่ที่ยาวกว่าเดิม แต่ยังคงมีสหสัมพันธ์ระหว่างกุญแจใหม่ที่ยาวขึ้นและกุญแจรหัสลับเดิม รวมถึงยังมีเงื่อนไขด้านทรัพยากรที่ต้องใช้ในการสร้างจำนวนสุ่มเทียมที่มีคาบยาวพอ (2) อาศัยรหัสลับแบบกุญแจสาธารณะมาช่วยในการส่งข้อความซึ่งจะถูกใช้เป็นกุญแจรหัสลับใหม่ ผ่านทางช่องสื่อสารสาธารณะ แต่ความปลอดภัยของกุญแจใหม่ ก็มีค่าเท่ากับความปลอดภัยของการเข้ารหัสแบบกุญแจสาธารณะ
ผู้ดักจับได้รับข้อมูลไม่เท่ากันกับผู้รับ	ความยาวกุญแจ *ไม่จำเป็น* ต้องมากกว่าหรือเท่ากับความยาวของข้อความ	(1) ต้องหาวิธีสื่อสารในทางปฏิบัติที่ทำให้ผู้รับและผู้ดักจับได้ข้อมูลไม่เท่ากัน (2) ผู้ดักจับ อาจได้รับข้อมูลกุญแจมากกว่า	(1) การใช้สถานะควอนตัมแทนข้อความสามารถทำให้ข้อมูลที่ผู้ดักจับและผู้รับได้รับแตกต่างกันได้ เนื่องจากการวัดข้อมูลมีผลทำให้สถานะเปลี่ยนไป และผลการวัดคือข้อความที่ทั้งผู้ดักจับ และผู้รับสารได้รับนั้นเป็นไปตามหลักความน่าจะเป็น กล่าวคือ *ถึงแม้ผู้ดักจับจะทราบว่าสถานะที่ถูกส่งเข้าสู่ภาครับเป็นสถานะใด ผู้ดักจับก็ไม่ทราบได้ว่า สถานะที่ผู้รับวัดได้ (ได้รับ) เป็นอะไร* เพราะเป็นไปตามความน่าจะเป็นขึ้นกับสถานะและรูปแบบการวัด ซึ่งเป็นสิ่งที่ช่วยให้ผู้รับและผู้ส่งสามารถมีข้อมูลร่วมกันมากกว่าที่ผู้ดักจับรับรู้ได้ ทั้งหมดนี้เป็นส่วนหนึ่งของ *การกระจายกุญแจเชิงควอนตัม* (2) มีการสื่อสารเพิ่มเติมเพื่อปรับข้อมูลของผู้ส่งและผู้รับให้ตรงกันยิ่งขึ้น โดยอาศัย

สมมติฐานของขั้นตอนการตกลงกุญแจรหัสลับร่วมกัน	เงื่อนไขจำเป็นสำหรับความปลอดภัยสมบูรณ์แบบ	ปัญหาที่อาจเกิดขึ้น	แนวทางการแก้ไข
			ความลับคือรูปแบบการวัดสถานะของภาครับ และวิธีการเตรียมสถานะของภาคส่ง ที่ผู้ดักจับไม่อาจทราบได้ (เป็นการตกลงกันของผู้ส่ง/ผู้รับก่อน)

2.2.2 ข้อมูลดักจับจากกุญแจรหัสลับ และอัตราการสร้างกุญแจรหัสลับ (Eve's information and secret key rate)

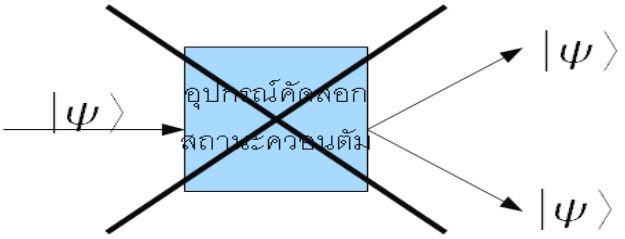
ความปลอดภัยของข้อมูลในหัวข้อข้างต้น สามารถอธิบายได้ในเทอมของทฤษฎีสารสนเทศดั้งเดิม (Classical information theory) ซึ่งหน่วยข้อมูลพื้นฐานเป็นค่าไม่ต่อเนื่องหรือค่าดิจิทัล [0,1] ส่วนการวิเคราะห์ปริมาณข่าวสารและพฤติกรรมในการคำนวณและการสื่อสารเชิงควอนตัมจะอธิบายด้วย *ทฤษฎีสารสนเทศเชิงควอนตัม* (Quantum information theory) ซึ่งมาตรวัดความไม่เป็นระเบียบหรือความไม่แน่นอนของข้อมูลเชิงควอนตัมจะอธิบายด้วย *ฟอน นอยมานน์เอนโทรปี* (Von Neumann entropy) [*Nielsen & Chuang 2000*] ซึ่งเป็นเสมือนรูปแบบควอนตัมของ*แชนนอนเอนโทรปี* (Shannon entropy) ในทฤษฎีสารสนเทศดั้งเดิม

2.2.3 การกระจายกุญแจรหัสลับด้วยคุณสมบัติควอนตัม (quantum key distribution)

การนำกลศาสตร์ควอนตัมมาประยุกต์ในเทคโนโลยีสารสนเทศ โดยเฉพาะด้านวิทยาการรหัสลับ เริ่มต้นโดยแนวคิดของสตีเฟน วีส์เนอร์ (Stephen Wiesner) ประมาณปี ค.ศ. 1970 (และตีพิมพ์ในปี ค.ศ. 1983) เสนอการใช้สถานะควอนตัมที่ไม่ตั้งฉาก (Non-orthogonal) ซึ่งมีคุณสมบัติแยกแยะจากกันไม่ได้ 100% (Unambiguously indistinguishable) มาแทนข้อมูล เช่นรหัสธนบัตร [*Wiesner 1983*] และผู้ไม่รู้สถานะควอนตัมดังกล่าว ไม่สามารถแยกแยะสถานะที่ไม่ตั้งฉาก รวมถึงไม่สามารถอ่านค่าสถานะโดยไม่ทำให้สถานะนั้นเปลี่ยนไปได้ ทำให้รหัสธนบัตรซึ่งแทนด้วยสถานะควอนตัมดังกล่าวไม่สามารถทำการปลอมได้ (No-cloning [*Wootters & Zurek 1982*]) หลังจากนั้นชาร์ลส์ เบนเนตต์ (Charles Bennett) และจิลส์ บราสซาร์ด (Gilles Brassard) ได้ร่วมกันเสนอแนวคิดการใช้สถานะควอนตัมที่ตั้งฉากและไม่ตั้งฉาก (4 สถานะ) แทนข้อมูลที่ทำให้ได้มาซึ่งกุญแจรหัสลับร่วมกันระหว่างคู่สื่อสาร โดยความพยายามในการดึงข้อมูลจากสถานะควอนตัมจะต้องแลกเปลี่ยนกับการทำให้เกิดการเปลี่ยนแปลงต่อสถานะ ซึ่งผู้สื่อสารทั้งคู่จะตรวจพบความเปลี่ยนแปลง โดยความผิดพลาดของผลลัพธ์จะสูงขึ้นผิดปกติ และสามารถยกเลิกข้อมูลชุดนั้นได้ [*Bennett & Brassard 1984*] หลังจากได้มีการทดลองในห้องปฏิบัติการเพื่อพิสูจน์หลักการดังกล่าวเป็นครั้งแรก [*Bennett และคณะ 1992*] และมีการเสนอเกณฑ์วิธีที่ใช้สถานะรูปแบบอื่นตามมา เช่น สถานะพัวพัน (Entangled states) [*Ekert 1991*, *Bennett-Brassard-Mermin 1992*] หรือใช้สองสถานะไม่ตั้งฉาก และใช้ 6 สถานะไม่ตั้งฉาก [*Bruss 1998*] เป็นต้น นอกจากนี้การค้นพบวิธีคำนวณทางควอนตัมสำหรับการแยกตัวประกอบซึ่งส่งผลให้รหัสลับแบบอสมมาตร ได้แก่ RSA และ Elliptic-Curve เป็นต้นนั้น จะถูกถอดรหัสได้ภายในเวลาเป็นโพลิโนเมียลด้วยการประมวลผลทางควอนตัม ซึ่งถึงแม้ยังไม่มีการสร้างอุปกรณ์คำนวณเชิงควอนตัมในสเกลใหญ่ (เช่นในระดับพันคิวบิต) ได้จริงถึงขั้นแยกตัวประกอบจำนวนมากเช่นรหัส RSA128 บิตได้ ความสนใจในวิทยาการรหัสลับซึ่งไม่ขึ้นกับความซับซ้อนทางการคำนวณ (หากแต่ขึ้นกับคุณสมบัติทางฟิสิกส์) กลับมีมากขึ้น และช่วงปี ค.ศ. 1995 – 2000 จึงได้มีความก้าวหน้าในวิทยาการรหัสลับเชิงควอนตัมเกิดเพิ่มขึ้น ทั้งด้านการทดลองที่ออกสู่ภาคสนามในระยะหลายกิโลเมตร [*Muller และคณะ 1997*] และด้านทฤษฎีในการกลั่นกุญแจรหัสลับ การเสนอวิธีป้องกันการดักจับ และการพิสูจน์ทางคณิตศาสตร์ถึงความปลอดภัยของการกระจายกุญแจด้วยวิธีทางควอนตัม [*Shor & Preskill 2000*], [*Renner, Gisin & Kraus 2005*] นอกจากนี้ยังมีการพัฒนาไปสู่ระดับพาณิชย์ด้วย [*IdQ.NET, MagiQ.NET*]

ตารางที่ 2.3 สรุปแนวคิดเชิงตรรกะของวิทยาการรหัสลับเชิงควอนตัม ช่องขวามือเป็นประโยคย้อนกลับซึ่งมีค่าเท่ากับฝั่งซ้ายมือ [*Gisin และคณะ 2002*]

ไม่มีการรบกวนต่อระบบ *→ ไม่มีการวัดข้อมูล* *→ ไม่มีการดักจับเกิดขึ้น* *No perturbation → No Information gain* *(no measurement)* *→ No eavesdropping*	*มีการวัดข้อมูล / มีการดักจับ* *→ มีการวัดข้อมูล* *→ ดักได้โดย Alice และ Bob* *Information gain /* *Eavesdropping → Perturbation* *→ detectable by Alice & Bob*
ต้องการความแน่นอนในแกน ตั้ง-นอน *→ เกิดความไม่แน่นอนในแนวทแยง* *(uncertainty relation)* *Infinite precision in one basis* *→ infinite uncertainty in the non-compatible basis*	*ต้องการความแน่นอนในแนวทแยง* *→เ กิดความไม่แน่นอนในแกนตั้ง-นอน* *(uncertainty relation)* *Infinite precision in one basis* *→ infinite uncertainty in the non-compatible basis*



รูปที่ 2.6 ข้อมูลเชิงควอนตัม (ที่ไม่ทราบค่า) ไม่สามารถถูกคัดลอกได้ [*Wootters & Zurek 1982*]
ซึ่งหมายถึงการดักจับเพื่อลอกข้อมูลควอนตัมโดยผู้ดักจับไม่สามารถกระทำได้

แนวคิดพื้นฐานของพฤติกรรมทางควอนตัมที่ช่วยสนับสนุนความเข้าใจการทำงานของวิทยาการรหัสลับและการสื่อสารเชิงควอนตัม ได้แก่ สิ่งที่ทำไม่ได้ในระบบควอนตัม ดังต่อไปนี้ [*Gisin และคณะ 2002*]

1) การวัดสถานะที่ไม่ทำให้เกิดการรบกวนต่อระบบเลยนั้น ทำไม่ได้

2) การวัดค่าตำแหน่งและโมเมนตัมของอนุภาคด้วยความละเอียดไม่จำกัดนั้น ทำไม่ได้

3) การวัดโพลาไรเซชันของโฟตอนในแนวตั้ง-นอน และแนวทแยงมุม ไม่สามารถทำพร้อมกันได้

4) การวาดภาพที่แน่นอนของระบบควอนตัมหนึ่งๆ และการเปลี่ยนแปลงทั้งหมดของระบบนั้น ไม่สามารถทำได้

ซึ่งเกิดเป็นประโยคสำคัญของช่วงต้นปีของคริสต์สหัสวรรษใหม่ว่า *"ผลลัพธ์ของกลศาสตร์ควอนตัมที่ปรากฏเหมือนเป็นแง่ลบดังกล่าวนั้น กลับกลายเป็นผลเชิงบวกเมื่อไม่นานมานี้ โดยวิทยาการรหัสลับเชิงควอนตัม เป็นหนึ่งในตัวอย่างที่ช่วยให้เห็นภาพของการปฏิวัติครั้งนี้"* [*Gisin และคณะ 2002*]

การห้ามไม่ให้มีความพยายามในการดักจับข้อมูลใดๆ นั้นไม่สามารถกระทำได้ หากแต่การใช้สถานะควอนตัมมาแทนข้อมูลนั้น ช่วยให้ผู้ส่งและผู้รับ ล่วงรู้พฤติกรรมของผู้ดักจับ เนื่องจากการดักจับข้อมูลควอนตัมโดยไม่ทำให้เกิดการเปลี่ยนแปลงเลย

นั้นไม่สามารถกระทำได้[2.6] และหากตรวจพบผลลัพธ์ของสถานะที่เปลี่ยนไปอันเนื่องจากการดักข้อมูล ผู้ส่งและผู้รับสามารถยกเลิกการใช้ข้อมูลดังกล่าวได้ทันที และหากทดสอบแล้วพบว่าข้อมูลไม่ถูกเปลี่ยนแปลงในลักษณะที่มีการดักจับ ผู้ส่งและผู้รับก็สามารถใช้ข้อมูลนั้นได้ด้วยความปลอดภัย [*Preskill 1998*]

หมายเหตุ สัดส่วนความปลอดภัย (Secret fraction: r) เป็นค่าที่บ่งบอกถึงปริมาณกุญแจรหัสลับที่สร้างได้เทียบกับปริมาณกุญแจดิบที่วัดได้ นิยามโดย [*Scarani และคณะ 2009*]

$$r = \lim_{N \to \infty} l/n \qquad \text{.....(2.6)}$$

โดย l หมายถึงความยาวของกุญแจรหัสลับที่สร้างได้ เมื่อมีการสื่อสารสัญญาณควอนตัมเป็นจำนวน N และผู้รับวัดสัญญาณควอนตัมออกมาได้กุญแจดิบความยาว n

2.3 เกณฑ์วิธีการสื่อสาร

วิทยาการรหัสลับเชิงควอนตัมมีเกณฑ์วิธีที่แตกต่างจากการสื่อสารแบบดั้งเดิมโดยมีการเพิ่มช่องทางสื่อสารสำหรับการกระจายกุญแจผ่านช่องสื่อสารเชิงควอนตัมที่เป็นความลับ โดยรูปแบบของการส่งกุญแจด้วยวิธีดังกล่าวสามารถอธิบายได้ดังนี้

2.3.1 ขั้นตอนโดยทั่วไปของการกระจายกุญแจเชิงควอนตัม

เกณฑ์วิธี (Protocol) ในการกระจายกุญแจเชิงควอนตัมโดยทั่วไปแบ่งได้เป็นสองส่วนหลักๆ ได้แก่ ส่วนการสื่อสารเชิงควอนตัม (Quantum part) และ การสื่อสารแบบดั้งเดิม (Classical part)[2.7] [*Renner, Gisin & Kraus 2005*]

2.3.1.1 การส่งสถานะควอนตัม (Quantum key transmission/ raw key exchange)

การส่งสถานะควอนตัมได้แก่การส่งข้อมูลควอนตัม (สถานะควอนตัม) ระหว่างสองตำแหน่งขึ้นไป ตัวอย่างเช่นกรณีการส่งสถานะระหว่างสองตำแหน่งเริ่มจาก ผู้ส่งทำการเตรียมสถานะควอนตัมโดยขึ้นกับเลขสุ่มเพื่อให้บุคคลใดๆ ไม่สามารถคาดเดาข้อมูลที่ส่งได้ ผู้รับทำการวัดสถานะควอนตัมดังกล่าว ซึ่งผลลัพธ์จากการวัดสถานะควอนตัมจะออกมาเป็นข้อมูลดิจิทัล เรียกว่า *กุญแจดิบ* (Raw key) จากนั้นคู่สื่อสารทำการสื่อสารเพื่อบอกลำดับเวกเตอร์ฐาน (Basis) ที่ใช้กับแต่ละคิวบิตในขั้นตอนการเลือกกุญแจ และทั้งคู่ทำการลบข้อมูลบิตในการวัดที่ใช้ลำดับเวกเตอร์ฐานไม่ตรงกัน (Incompatible)[2.8] ผลลัพธ์ที่ได้จากการตัดบิตที่เกิดจากลำดับเวกเตอร์ฐานไม่ตรงกัน เรียกว่า *กุญแจซิฟต์* (Sifted key)[2.9] ซึ่งจะนำมาประมวลผลต่อในขั้นถัดไป

2.3.1.2 การประเมินคุณสมบัติช่องสัญญาณ และ การประมวลผลภายหลัง (Channel parameter estimation and classical post-processing)

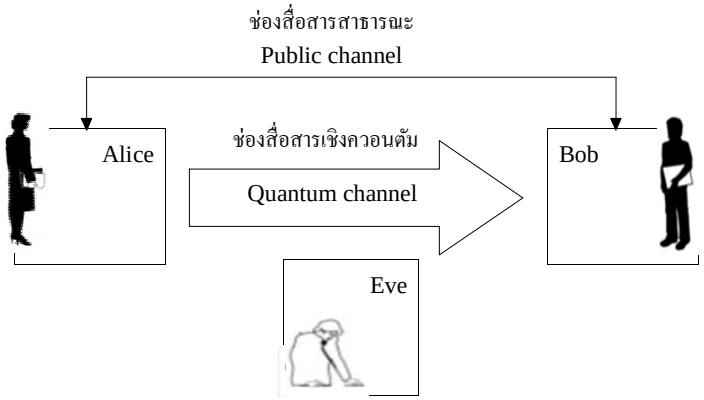
การประมวลผลภายหลัง เป็นการสื่อสารเชิงดิจิทัลผ่านช่องสัญญาณสาธารณะ (Public channel) และการประมวลผลข้อมูลดิจิทัล จนกระทั่งได้กุญแจรหัสลับ (Secret key) ร่วมกัน ระหว่างคู่สื่อสาร (ทั้งหมดในขั้นนี้เป็นกระบวนการแบบดั้งเดิม) การประมวลผลภายหลังประกอบด้วยขั้นตอนย่อย ดังต่อไปนี้

2.6 ยกเว้นกรณีที่ตัวดำเนินการสำหรับดักวัดข้อมูล เป็นตัวดำเนินการเจาะจง (eigenoperator) ของสถานะควอนตัมที่แทนข้อมูลนั้น เช่นกรณีที่ผู้ดักจับเลือกเวกเตอร์ฐานถูกต้องในการดักจับบนโพรโตคอล BB84

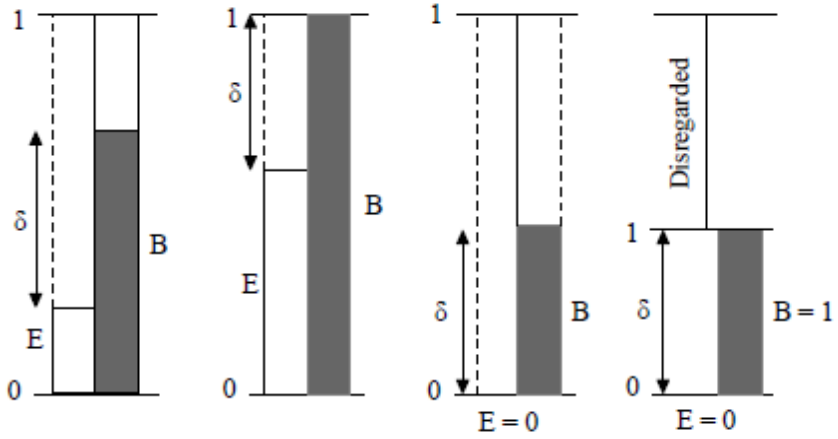
2.7 แบ่งขั้นตอนตาม [*Renner, Gisin & Kraus 2005*] โดยเพิ่มขั้นตอนการยืนยันตัวตนต่อท้าย

2.8 เช่น {โพลาไรซ์แนวตั้ง-นอน} และ {+45°, -45°} ถือว่าเวกเตอร์ฐานไม่ตรงกัน

2.9 การซิฟท์คือกระบวนการที่ผู้ส่งและผู้รับสื่อสารกันเพื่อตัดบิตที่ผู้รับเลือกวิธีถอดรหัสไม่ถูกต้องทิ้งไป [*Scarani และคณะ 2009*]



(ก)



(ข)

รูปที่ 2.7 (ก) ขั้นตอนการทำงานของการกระจายกุญแจรหัสลับเชิงควอนตัมโดยทั่วไป จะแยกช่องทางสื่อสารเป็นสองช่องทางคือช่องสื่อสารสาธารณะ และช่องสื่อสารเชิงควอนตัมสำหรับส่งกุญแจเชิงควอนตัม (ข) ความยาวของกุญแจในแต่ละขั้นตอน สีอ่อนแสดงข้อมูลที่ผู้ดักจับ (ตัวอักษร *E*) มีต่อกุญแจและสีเข้มแสดงปริมาณข้อมูลกุญแจที่ผู้ส่งและผู้รับมีร่วมกัน (ตัวอักษร *B*) ส่วนสัญลักษณ์ δ คือความแตกต่างของข้อมูลกุญแจที่ผู้ส่งและผู้รับมีร่วมกันเทียบกับที่ผู้ดักจับมี เมื่อจบขั้นตอน 'ขยายสภาวะส่วนตัว' ข้อมูลที่ผู้ดักจับรับรู้ต่อกุญแจรหัสลับ (ในอุดมคติ) มีค่าเป็นศูนย์ [*Gisin และคณะ 2002*]

- การประเมินคุณสมบัติช่องสัญญาณ (Channel parameter estimation)

โดยการเปิดเผยข้อมูลบางส่วนของกุญแจซิฟต์เพื่อหาความผิดพลาดด้วยวิธีทางสถิติ จะทำให้ทราบถึงอัตราความผิดพลาดโดยประมาณ (Estimated error rate) และคำนวณปริมาณสารสนเทศที่ผู้ดักจับมีสิทธิ์รับรู้ซึ่งเพิ่มขึ้นตามอัตราความผิดพลาด จากนั้นอาศัยข้อมูลส่วนที่เหลือ (ยังไม่เปิดเผย) ซึ่งมีความยาวเท่ากับความยาวกุญแจซิฟต์เดิมลบด้วยจำนวนบิตในกุญแจซิฟต์ที่ถูกเปิดเผย (กุญแจที่เปิดเผยแล้ว จะนำมาใช้ไม่ได้)

- การไกล่เกลี่ยความผิดพลาดของข้อมูล (Information reconciliation)

ผู้ส่งและผู้รับประมวลผลเพื่อแก้ไขข้อผิดพลาด (บิตที่ไม่ตรงกันของกุญแจซิฟต์) เพื่อให้ได้มาซึ่ง*ข้อมูลกุญแจที่ตรงกัน* (Reconciled key) และ*อัตราความผิดพลาดที่แท้จริง* (Exact Bit Error Rate: BER) ซึ่งจะใช้ประมาณข่าวสารสูงสุดเกี่ยวกับกุญแจซึ่งผู้ดักจับได้รับ

- การขยายสภาวะส่วนตัว (Privacy Amplification)

จากคุณสมบัติช่องสัญญาณ (BER และอื่น ๆ) คู่สื่อสารคำนวณหา*ตัวแปรสำหรับลดขนาดกุญแจ* (Shrinking parameter) เพื่อนำไปลดความยาวของกุญแจที่ตรงกัน (ลดข้อมูลข่าวสารที่ผู้ดักจับจะมีต่อกุญแจรหัสลับ) เพื่อให้ได้มาซึ่ง*กุญแจที่กลั่นกรองแล้ว* (Distilled key) ที่มีความยาวลดลงอีก เมื่อถึงขั้นตอนนี้ยังเป็นที่สงสัยว่ากุญแจที่กลั่นกรองแล้วนี้ เป็นกุญแจร่วมกันระหว่างผู้ส่งและผู้รับตัวจริงหรือไม่ จึงต้องมีการยืนยันตัวตนระหว่างคู่สื่อสารว่าเป็นคู่สื่อสารที่ต้องการสื่อสารกันจริง

- การยืนยันตัวตน (Authentication)

เพื่อยืนยันว่ากุญแจที่ได้มาเป็นกุญแจร่วมกันระหว่างผู้ส่งและผู้รับจริง ขั้นตอนทั้งหมดที่การสื่อสารข้างต้นต้องถูกนำมาผ่านกระบวนการยืนยันตัวตนเพื่อป้องกันการโจมตีแบบปลอมตัวมาอยู่ตรงกลาง (Man-in-the-middle attack) ซึ่งเป็นการปลอมตัวเข้าไปหลอกผู้ส่งและผู้รับว่ากำลังติดต่อกันอยู่ โดยมีผู้ดักจับอยู่ตรงกลาง การยืนยันตัวตนทำได้โดยอาศัยกุญแจรหัสลับที่มีอยู่ก่อนหน้าขั้นตอน QKD[2.10] โดยวิธีมาตรฐานในการยืนยันตัวตนเสนอโดย มาร์ค เวกแมน (Mark Wegman) และลาร์รี่ คาร์เตอร์ (Larry Carter) [*Stinton 1994*]

2.3.2 เกณฑ์วิธีสถานะควอนตัมไม่ต่อเนื่อง (Discrete-Variable Protocols)

สถานะควอนตัมไม่ต่อเนื่อง หมายถึงสถานะที่มีจำนวนสถานะฐาน (Basis state) จำกัด และแทนอนุภาคแต่ละอนุภาคด้วยข้อมูลดิจิทัลหนึ่งบิต ซึ่งมีหลายเกณฑ์วิธี เช่น

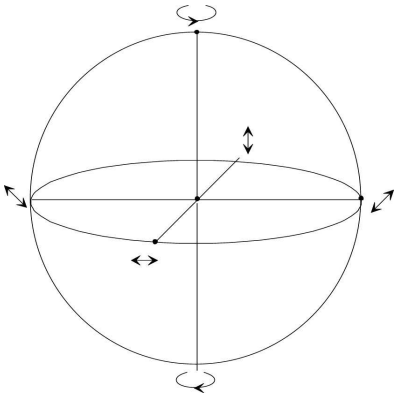
2.3.2.1 เกณฑ์วิธีที่ไม่ใช้สถานะพัวพัน (Prepare & Measure protocols)

- เบนเนตต์-บราสซาร์ด 1984 (BB84)

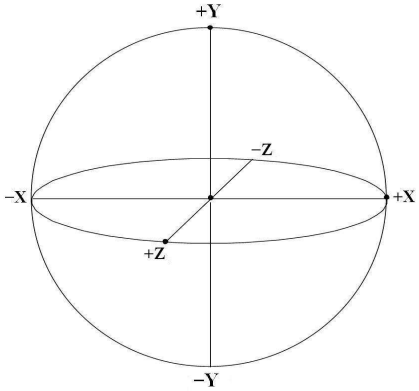
วิธีกระจายกุญแจรหัสลับเชิงควอนตัมวิธีแรกมีการเสนอ โดย ชาร์ลส์ เบนเนตต์ (Charles H. Bennett) และ จิลส์ บราสซาร์ด (Gilles Brassard) ซึ่งถูกตีพิมพ์ในงานประชุมวิชาการของสมาคมสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (The Institute of Electronics and Electrical Engineers; IEEE) ที่ประเทศอินเดียในปี ค.ศ. 1984 [*Bennett & Brassard 1984*] ซึ่งเป็นจุดสำคัญในการกระตุ้นการผสมผสานความรู้ในสาขาต่างๆ คือ วิทยาการคอมพิวเตอร์ วิศวกรรมการสื่อสาร ฟิสิกส์ควอนตัม เป็นต้น มารวมกัน ซึ่งเริ่มปรากฏชัดเจนขึ้นในทศวรรษต่อมา (ช่วงปี ค.ศ. 1990 เป็นต้นไป)

โดยทั่วไป การทำงานของการกระจายกุญแจเชิงควอนตัมด้วยสถานะไม่ต่อเนื่อง จะอธิบายในแบบจำลองสปิน ½ (Bloch sphere) หรือแบบจำลองสถานะโพลาไรซ์ของโฟตอนเดี่ยว (Poincaré sphere) ซึ่งมีความเหมือนกันทางคณิตศาสตร์คือแทนด้วยเวกเตอร์หน่วย (unit vector) บนผิวทรงกลม โดยสถานะที่อยู่ฝั่งตรงข้ามกันบนผิวทรงกลม เป็นสถานะที่ตั้งฉาก (orthogonal) และแบ่งแยกจากกันได้อย่างชัดเจนด้วยการวัดสถานะ ได้แก่ สถานะสปินในทิศตรงข้ามวัดได้ด้วยการวางแนวสนามแม่เหล็กเหนือ-ใต้ ตามการทดลองของชแตน-แกร์ลาด (Stern-Gerlach experiment) หรือสถานะโพลาไรเซชันของแสงที่ตั้งฉาก (วัดได้โดยใช้ตัวแยกแสงเชิงโพลาไรซ์ และตัวตรวจหาโฟตอน) สถานะควอนตัมดังกล่าว พิจารณาได้ว่าเป็นเวกเตอร์ที่ชี้บนผิวทรงกลมดังรูปที่ 2.8

[2.10] การกระจายกุญแจเชิงควอนตัม (QKD) ไม่สามารถแก้ปัญหาเรื่องการยืนยันตัวตนได้ จำเป็นต้องมีกุญแจรหัสลับร่วมกันระหว่างผู้ส่งและผู้รับอยู่ก่อนแล้ว จากนั้น QKD ใช้ในการเพิ่มจำนวนกุญแจให้ยาวมากขึ้นตามต้องการ เหตุนี้ทำให้บางครั้ง quantum key distribution ถูกเรียกว่า quantum key growing แทน (เนื่องจากอาศัยกุญแจที่มีอยู่ก่อน มาใช้เป็นเสมือนเมล็ดพันธุ์สำหรับเพิ่มจำนวนกุญแจ)



(ก) ทรงกลมปวงกาเร (Poincaré sphere)



(ข) ทรงกลมบล็อช (Bloch sphere)

รูปที่ 2.8 (ก) ทรงกลมปวงกาเรแทนสถานะโพลาไรเซชันของแสง (ข) ทรงกลมบล็อชแทนสถานะสปินของอนุภาคที่มีสปิน 1/2 โดยสถานะควอนตัมสองระดับ (two-level quantum system) หรือบิตควอนตัมใดๆ สามารถแทนได้ด้วยเวกเตอร์หน่วยบนผิวทรงกลม

ตารางที่ 2.4 เปรียบเทียบสถานะโพลาไรเซชันซึ่งเขียนแทนด้วยสถานะเชิงควอนตัมตามเกณฑ์วิธี BB84 ต้นฉบับ

สถานะโพลาไรเซชัน	สถานะควอนตัม
แนวตั้ง $(\updownarrow)$	$\|0\rangle$
แนวนอน $(\leftrightarrow)$	$\|1\rangle$
แนว +45 องศา $(\nearrow)$	$(\|0\rangle+\|1\rangle)/\sqrt{2}$
แนว -45 องศา $(\nwarrow)$	$(\|0\rangle-\|1\rangle)/\sqrt{2}$

เกณฑ์วิธี BB84 ต้นฉบับนั้นใช้สถานะโพลาไรเซชันของแสง 4 สถานะคือ แนวตั้ง $(\updownarrow)$ แนวนอน $(\leftrightarrow)$ แนว +45 องศา $(\nearrow)$ และแนว -45 องศา $(\nwarrow)$ ซึ่งเขียนเป็นสถานะเชิงควอนตัมได้ตามลำดับ ดังนี้ $|0\rangle$, $|1\rangle$, $(|0\rangle+|1\rangle)/\sqrt{2}$ และ $(|0\rangle-|1\rangle)/\sqrt{2}$

- เบนเนตต์ 1992 (B92) เป็นการใช้สถานะควอนตัมสองสถานะที่ไม่ตั้งฉากกันมาแทนข้อมูล และอาศัยคุณสมบัติที่สถานะควอนตัมซึ่งไม่ตั้งฉากจะไม่สามารถแยกแยะได้ ดังนั้นผู้ดักจับจึงไม่อาจดักข้อมูลที่ถูกเตรียมมาตอนแรกได้
- หกสถานะ (Six-state protocol) เป็นการใช้สถานะควอนตัมหกสถานะที่เป็นสถานะไอเกน (Eigenstates) ของตัวดำเนินการเพาลี (Pauli operators) โดยเป็นวิธีที่เพิ่มความสับสนให้ผู้ดักจับในการตีความหมายข้อมูล [*Bruss 1998*] สถานะทั้งหกสถานะที่ถูกนำมาใช้แสดงตำแหน่งดังรูปที่ 2.8 (ก) ทั้งหกตำแหน่ง
- ซาร์ก 2004 (SARG04) เพื่อป้องกันการโจมตีแบบแบ่งจำนวนโฟตอน (Photon-number splitting attack) ได้มีการเสนอการปรับปรุงเกณฑ์วิธี BB84 ในขั้นประมวลผลข้อมูลดิจิทัล โดยแทนบิตของกุญแจด้วยเวกเตอร์ฐาน แทนที่จะแทนด้วยเวกเตอร์สถานะเหมือนใน BB84 ปกติ [*Scarani และคณะ 2004*]

2.3.2.2 เกณฑ์วิธีที่ใช้สถานะพัวพัน (Entanglement-based protocols)

- เอเคอร์ท 1991 (Ekert91) เสนอให้ใช้อสมการของเบลล์เป็นตัวทดสอบความมีอยู่ของคุณสมบัติพัวพัน และความปรากฏตัวของผู้ดักจับบนช่องสัญญาณควอนตัม ซึ่งการดักจับสถานะควอนตัมโดยผู้ดักจับทำให้คุณสมบัติพัวพันสูญเสียไป โดยทดสอบได้ตามทฤษฎีของเบลล์

• เบนเนตต์-บราสซาร์ด-เมอร์มิน 1992 (BBM92) เป็นเกณฑ์วิธีที่ใช้สถานะพัวพันแต่ไม่จำเป็นต้องตรวจหาการดักจับด้วยทฤษฎีของเบลล์ หากแต่ใช้วิธีเดียวกับใน BB84 ซึ่งมีการพิสูจน์ว่า BBM92 และ BB84 ให้ผลเหมือนกัน [*Bennett, Brassard & Mermin 1992*] โดย BBM92 เสมือนว่าโฟตอนเคลื่อนที่ย้อนทิศของเวลาจากผู้ส่งไปยังแหล่งกำเนิดความพัวพัน (Entanglement source) และเคลื่อนตามเวลาไปยังผู้รับ

ความปลอดภัยของเกณฑ์วิธีที่ใช้สถานะพัวพันขึ้นกับปริมาณความพัวพันที่มีร่วมกันระหว่างคู่สื่อสาร [*Shor & Preskill 2000*] ซึ่งมีการสาธิตว่าเกณฑ์วิธีดังกล่าวสามารถทนทานต่อการลดทอนตามระยะทางได้ดีกว่าการใช้สัญญาณพัลส์ความเข้มต่ำด้วยเกณฑ์วิธีที่ไม่ใช้สถานะพัวพัน

2.3.3 เกณฑ์วิธีสถานะควอนตัมแบบต่อเนื่อง (Continuous-Variable Protocols)

สถานะควอนตัมแบบต่อเนื่อง หมายถึงสถานะที่มีจำนวนสถานะฐานเป็นอนันต์และมีค่าเป็นจำนวนจริงหรือจำนวนเชิงซ้อนได้ เช่น สถานะของตำแหน่งและโมเมนตัมของอนุภาค ในแสงได้แก่สถานะอาพันธ์ (coherent states) เช่น แสงเลเซอร์ และแสงที่ถูกบีบอัด (Squeezed light) ซึ่งมีการกระจายตัวแบบเกาส์

2.3.3.1 เกณฑ์วิธีที่ใช้สถานะแบบเกาส์ (Gaussian Protocols)

• การกระจายกุญแจเชิงควอนตัมของสถานะที่ถูกบีบอัด (Squeezed-state QKD) อาศัยหลักความไม่แน่นอนระหว่างคู่ตัวแปรที่ไม่ตั้งฉากกัน (quadrature) เช่น แอมปลิจูด (Amplitude: n) และเฟส (Phase: ϕ) ซึ่งสัมพันธ์กันโดย $\Delta n \Delta \phi \geq \hbar/2$ โดยผู้ส่งทำการสุ่มเวกเตอร์ฐานว่าจะทำการบีบความไม่แน่นอนให้เล็กลงตามแนวแอมปลิจูดหรือมุมเฟส เมื่อถึงปลายทาง ผู้รับทำการสุ่มเวกเตอร์ฐานว่าจะเลือกวัดมุมเฟสหรือแอมปลิจูด จากนั้นสื่อสารเพื่อเก็บไว้เฉพาะบิตที่ใช้เวกเตอร์ฐานในการวัดตรงกัน [*Ralph 2001*] อย่างไรก็ตามวิธีการดังกล่าวไม่ได้ใช้โฟตอนเดี่ยว แต่เป็นแสงที่กระจายตัวแบบเกาส์และมีจำนวนโฟตอนเฉลี่ยค่าหนึ่ง จึงทำให้ผู้ดักจับสามารถแบ่งสัญญาณแสงไปส่วนหนึ่งเพื่อทำการวัดได้ [*Ralph 2000*] นอกจากนี้ได้มีการพิสูจน์ว่า การเทเลพอร์ตสถานะควอนตัมแบบต่อเนื่อง (continuous-variable quantum teleportation) เป็นวิธีที่ดีที่สุดสำหรับผู้ดักจับในการดึงข้อมูลเชิงควอนตัมออกมา ต่อมา ปีเตอร์ ชอร์ (Peter Shor) และ จอห์น พรีสกิล (John Preskill) พิสูจน์ว่า ถ้าใช้สัดส่วนการบีบสถานะ (squeezing ratio) มากกว่า 2.51 dB โพรโตคอลแบบสถานะบีบอัดนี้พิสูจน์ได้ว่ามีความปลอดภัย [*Shor & Preskill 2000*]

• การกระจายกุญแจเชิงควอนตัมของสถานะโคฮีเรนท์ (Coherent-state QKD) วัดสถานะด้วยวิธีการตรวจหาแบบโฮโมดายน์ (Homodyne detection) และอาศัยการไกล่เกลี่ยความผิดพลาดแบบย้อนศร (reverse reconciliation) คือ ผู้ส่งสถานะควอนตัม และผู้ประกาศผลลัพธ์บางส่วนผ่านช่องสัญญาณสาธารณะเป็นคนละคนกัน กล่าวคือ Bob เป็นผู้ประกาศข้อมูลเกี่ยวกับการวัดสถานะเพื่อการแก้ไขข้อผิดพลาด

• การกระจายกุญแจเชิงควอนตัมของการวัดจตุรัสหลายชั้น (simultaneous quadrature measurement QKD) เป็นวิธีที่ไม่ต้องใช้การสุ่มเลือกรูปแบบในการวัดสถานะเชิงควอนตัม (random switch) สำหรับการวัดสถานะ [*Weedbrook และคณะ 2004*] และให้ผลการสร้างกุญแจรหัสลับสูงกว่าสองวิธีแรก

• การใช้สถานะที่ถูกบีบอัดร่วมกับร่วมกับการตรวจหาแบบเฮเทโรไดน์ [*Garcia-Patron & Cerf 2009*] เป็นวิธีที่ทนทานต่อสัญญาณรบกวนได้มากที่สุดในบรรดาโพรโตคอลแบบเกาส์ทั้งหมด นอกจากนั้น ผลลัพธ์ที่น่าประหลาดคือการเพิ่มสัญญาณรบกวน (noise) ในขั้นตอน post-processing ทำให้ได้อัตราการสร้างรหัสลับ (secret key rate) เพิ่มขึ้น

2.3.3.2 เกณฑ์วิธีที่ใช้การมอดูเลตแบบไม่ต่อเนื่อง (Discrete modulation protocols)

เกณฑ์วิธีที่ใช้สถานะควอนตัมแบบต่อเนื่องโดยการมอดูเลตแบบไม่ต่อเนื่อง ซึ่งใช้ในกรณีที่มีสัญญาณรบกวนในช่องสื่อสารเชิงควอนตัมไม่มาก โดยจะทำให้กุญแจที่ได้มีความเหมาะสมสำหรับรหัสแก้ไขความผิดพลาดต่างๆ มากขึ้น นำเสนอโดย [*Scarani และคณะ 2009*]

2.3.4 เกณฑ์วิธีที่ใช้การอ้างอิงการกระจายเฟส (Distributed-phase-reference protocols)

จากเกณฑ์วิธีที่ได้กล่าวมาข้างต้นจะเริ่มต้นจากการนำเสนอของนักวิจัยทางด้านทฤษฎี แต่เกณฑ์วิธีที่ใช้การอ้างอิงการกระจายเฟสนี้ได้รับการนำเสนอจากนักวิจัยเพื่อแก้ปัญหาในการทดลอง โดยอาศัยคุณสมบัติของเฟสของสัญญาณพัลส์ในลำดับต่างๆ

2.3.5 การพิสูจน์ความปลอดภัยของการกระจายกุญแจรหัสลับเชิงควอนตัม (Security Proofs)

ชอร์และพรีสกิล พิสูจน์ว่าตราบเท่าที่อัตราผิดพลาดบิตเชิงควอนตัม (Quantum Bit Error Rate: QBER) น้อยกว่าหรือเท่ากับ 11% โพรโตคอล BB84 จะมีความปลอดภัยอย่างสมบูรณ์ [*Shor & Preskill 2000*] มีการพิสูจน์ความปลอดภัยแบบไม่มีเงื่อนไขของโพรโตคอลแบบที่ใช้โฟตอนเดี่ยว โดยไม่จำเป็นต้องตั้งสมมติฐานว่าแหล่งกำเนิดจำนวนสุ่มสร้างจำนวนสุ่มซึ่งกระจายตัวแบบเป็นระเบียบแต่อย่างใด

มีการเสนอวิธีพิสูจน์ความปลอดภัยของการกระจายกุญแจรหัสลับเชิงควอนตัมที่ไม่ขึ้นกับอุปกรณ์ (device-independent QKD) ซึ่งช่วยให้ไม่ต้องอิงกับรายละเอียดของการทดลอง รวมถึงการรบกวนภายในอุปกรณ์ทั้งฝั่งผู้ส่งและผู้รับ รวมถึงสิ่งที่นอกเหนือการควบคุมภายในช่องสัญญาณควอนตัม แต่การตั้งสมมติฐานทั่วไปที่ทำให้ขีดจำกัดของปริมาณกุญแจรหัสลับที่สร้างได้ (theoretical limit) ลดลง เมื่อเทียบกับสมมติฐานแบบเดิม รวมทั้งอัตราบิตผิดพลาดเชิงควอนตัม (QBER) สูงสุดที่ยังคงอนุญาตให้สร้างกุญแจรหัสลับได้ อยู่ที่ 7.1% (จากเดิม 11%) [*Acin และคณะ 2007*] แต่ผลการพิสูจน์เชิงทฤษฎีดังกล่าวใช้ได้กับการกระจายกุญแจรหัสลับด้วยสถานะพัวพัน (Entangled-based QKD) เท่านั้น [Scarani และคณะ 2009] ซึ่งใช้ไม่ได้กับวิธีไม่พัวพันเช่นใน BB84 การพิสูจน์ความปลอดภัยเชิงทฤษฎีที่ครอบคลุมที่สุด ยังคงต้องค้นหาต่อไป

2.4 พัฒนาการการทดลองในห้องปฏิบัติการ กับการใช้งานภาคสนาม (Laboratory & field experiments)

การทดลองระบบวิทยาการรหัสลับเชิงควอนตัมจริงจะมีความแตกต่างจากการประมาณด้วยทฤษฎี เนื่องจากขีดจำกัดของอุปกรณ์และผลกระทบจากสิ่งแวดล้อมต่างๆ ซึ่งจะพิจารณาดังนี้

2.4.1 อัตราผิดพลาดบิตเชิงควอนตัม (Quantum Bit Error Rates: QBER)

อัตราผิดพลาดบิตเชิงควอนตัม [*Gisin และคณะ 2002*] หมายถึง สัดส่วนระหว่างบิตที่ผิดพลาดต่อจำนวนบิตทั้งหมด ในกุญแจซิฟต์ (Sifted key) หรือ กุญแจที่ตัดบิตที่ใช้เวกเตอร์ฐานไม่ตรงกันออกแล้ว

$$QBER = \frac{N_{\text{wrong}}}{N_{\text{right}} + N_{\text{wrong}}} = \frac{R_{\text{error}}}{R_{\text{sift}} + R_{\text{error}}} \approx \frac{R_{\text{error}}}{R_{\text{sift}}} \qquad \text{.....(2.7)}$$

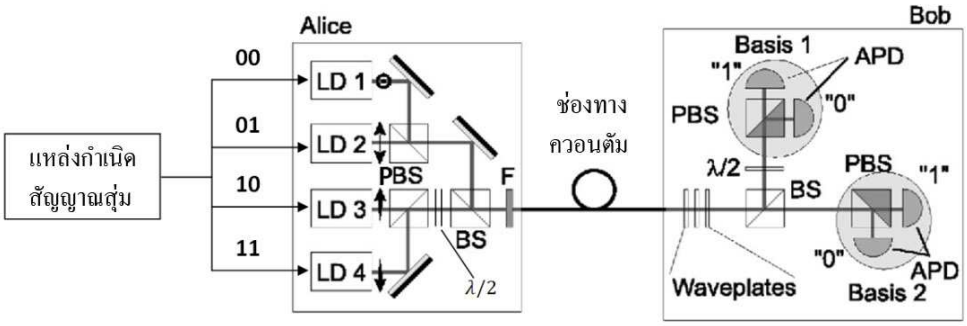
โดย N_{wrong} คือ จำนวนบิตของกุญแจซิฟต์ที่ผู้ส่งและผู้รับมีไม่ตรงกัน

N_{right} คือ จำนวนบิตในกุญแจซิฟต์ที่ผู้ส่งและผู้รับมีตรงกัน

ดังนั้นเมื่อ N_{right} รวมกับ N_{wrong} จะเท่ากับความยาวกุญแจซิฟต์ทั้งหมด (N_{sift}) ส่วน R_{error} หมายถึงอัตราการเกิดบิตที่ผิดพลาดต่อหน่วยเวลา และ R_{sift} หมายถึงอัตราการสร้างกุญแจซิฟต์ต่อหน่วยเวลา โดยในโพรโตคอลมาตรฐาน (BB84) R_{sift} จะมีค่าเป็นครึ่งหนึ่งของอัตราการสร้างกุญแจดิบ (R_{raw}) เนื่องจากมีความน่าจะเป็นเท่ากับ ½ ที่ผู้ส่งและผู้รับ เลือกเวกเตอร์ฐานตรงกัน [*Gisin และคณะ 2002*]

$$R_{sift} = \frac{1}{2} R_{raw} = \frac{1}{2} q\, f_{rep}\, \mu\, t_{link}\, \eta \qquad \text{.....(2.8)}$$

เมื่อ q คือ อัตราการส่งกุญแจซิฟต์



รูปที่ 2.9 การทำงานของระบบ BB84 ซึ่งแทนข้อมูลด้วยโพลาไรเซชัน เมื่อ LD คือไดโอดเลเซอร์จำนวน 4 ตัว BS คือกระจกแยกลำแสงทำหน้าที่แยกและรวมแนวแสง F คือฟิลเตอร์ลดทอนความเข้ม Waveplate คือแผ่นหน่วงคลื่น λ/2 คือแผ่นหน่วงครึ่งคลื่น PBS คือกระจกแยกลำแสงโพลาไรซ์ APD คือไดโอดรับแสงชนิดแอวัลแลนซ์ [*Gisin และคณะ 2002*]

f_{rep} คือ ความถี่ของสัญญาณพัลส์จากผู้ส่ง

μ คือ จำนวนโฟตอนเฉลี่ยต่อพัลส์

t_{link} คือ ความเป็นไปได้ที่โฟตอนจะถูกส่งไปถึงผู้รับ

η คือ ความเป็นไปได้ในการตรวจหาโฟตอนที่ภาครับ

2.4.2 การทดลองกระจายกุญแจเชิงควอนตัมด้วยแสงลดทอนความเข้ม (Attenuated laser pulse)

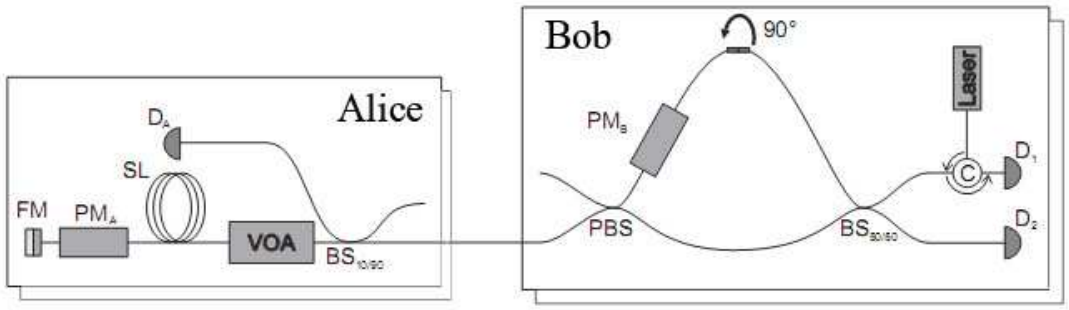
การกระจายกุญแจเชิงควอนตัมด้วยการลดทอนความเข้มแสงนิยมใช้สถานะเชิงควอนตัมในสองรูปแบบเพื่อสร้างระบบกุญแจ คือการแทนด้วยโพลาไรเซชัน และการแทนด้วยเฟส ดังนี้

2.4.2.1 โพลาไรเซชัน (Polarization)

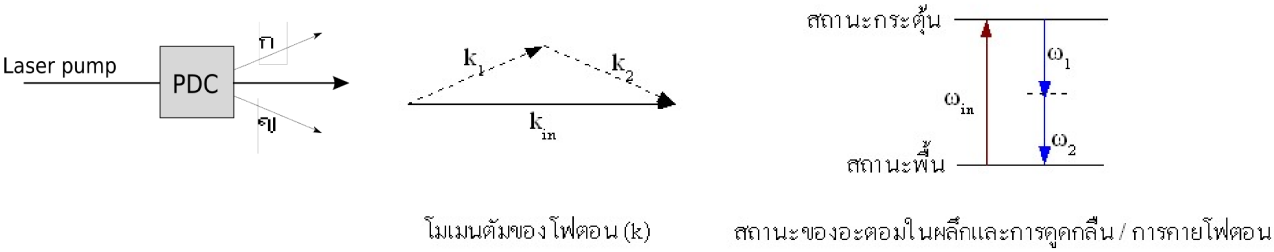
การกระจายกุญแจเชิงควอนตัมด้วยโพลาไรเซชันที่นิยมคือเกณฑ์วิธี BB84 ซึ่งแทนข้อมูลด้วยโพลาไรเซชันสี่สถานะ โดยมีอุปกรณ์หลักคือชุดกำหนดโพลาไรเซชัน (สำหรับเตรียมสถานะภาคส่ง) และแยกโพลาไรเซชัน (สำหรับสถานะภาครับ) เพื่อใช้แทนบิตข้อมูลโดยผู้ส่งและผู้รับกำหนดบิตที่แทนด้วยสถานะโพลาไรเซชันร่วมกัน แล้วทำการสื่อสารสถานะควอนตัม หากรูปแบบของเวกเตอร์ฐานในการรับตรงกันจะได้บิตข้อมูลที่ตรงกันเป็นพื้นฐานเบื้องต้นของการเข้ารหัสด้วยการใช้โพลาไรเซชัน ดังรูปที่ 2.9 การแทนด้วยสถานะโพลาไรซ์นิยมในการสื่อสารผ่านอากาศ เพราะการเปลี่ยนแปลงของโพลาไรซ์เกิดขึ้นได้ค่อนข้างยาก การทดลองต้นแบบเกิดขึ้นเมื่อปี ค.ศ.1989 ที่สถาบันไอบีเอ็ม [Bennett และคณะ 1992]

2.4.2.2 การเข้ารหัสด้วยเฟส (Phase-encoding)

การแทนสถานะด้วยโพลาไรเซชัน หากทำการส่งสถานะผ่านเส้นใยนำแสงในระยะไกล จะเกิดการบิดของโพลาไรซ์ซึ่งทำให้สถานะเปลี่ยนไป (หากไม่มีการชดเชยกลับคืน) จึงมีการเสนอ ให้ใช้สถานะแทนด้วยเฟส ซึ่งเฟสนี้เป็นคุณสมบัติที่คงที่ตามระยะทางการส่งในเส้นใยนำแสง โดยหลักการทำงานพิจารณาได้ตามระบบ “Plug&Play Autocompensating QKD” ซึ่งจะแทนข้อมูลด้วยมุมเฟส โดยมีอุปกรณ์หลักคือ กระจกฟาราเดย์ (Faraday Mirror) ซึ่งทำหน้าที่สะท้อนแสงกลับพร้อมทั้งหมุนโพลาไรเซชันไป 90 องศา ทำให้โฟตอนที่เคลื่อนที่จากฝั่ง *Bob* ผ่านเส้นทางสั้น ซึ่งสมมติว่ามีโพลาไรซ์แนวนอน แต่เมื่อขากลับโพลาไรซ์จะถูกเปลี่ยนเป็นแนวตั้งและถูกสะท้อนที่กระจกแยกลำแสงโพลาไรซ์ (Polarizing beam splitter: PBS) เข้าสู่เส้นทางยาว ส่วนโฟตอนที่ขาไปผ่านเส้นทางยาว ขากลับจะผ่านเส้นทางสั้น ด้วยหลักการเดียวกัน ทำให้ระยะทางที่โฟตอนสองสถานะวิ่งผ่านมีระยะเท่ากันทุกประการ และจากการเพิ่มการเลื่อนเฟส (Phase modulation) จะทำให้วิธีดังกล่าวทำเสมือนมาตรแทรกสอดแบบแมส- แซนเดอร์ (Mach-Zehnder interferometer) ที่สมบูรณ์ได้ นอกจากนี้ผลการเปลี่ยนแปลงทิศโพลาไรซ์เนื่องจากสายไฟเบอร์ยังถูกชดเชยอัตโนมัติเมื่อแสงเคลื่อนที่ย้อนกลับ ดังรูปที่ 2.10



รูปที่ 2.10 การทำงานของระบบ “Plug&Play Autocompensating QKD” ซึ่งแทนข้อมูลด้วยมุมเฟส เมื่อ FM คือกระจกฟาราเดย์ PM คืออุปกรณ์มอดูเลตทางเฟส SL คือขดเส้นใยแสงระยะสั้น D คือตัวตรวจหา VOA คืออุปกรณ์ปรับความเข้มแสง BS คืออุปกรณ์แยกแสง C คืออุปกรณ์เปลี่ยนแนวแสงไปยังเส้นทางทวนเข็มนาฬิกา [*IdQ.NET*]



รูปที่ 2.11 อธิบายการทำงานของหน่วยแปลงผันลงเชิงพารามิเตอร์ (Parametric Down Converter) เมื่อแสงผ่านสู่ผลึกที่มีคุณสมบัติไม่เป็นเชิงเส้น (Nonlinear crystal) บางชนิด เช่น Barium Borate (BBO) จะมีความเป็นไปได้ที่แสง (โฟตอนเดี่ยว) จะถูกดูดกลืนโดยผลึกแล้วคายพลังงานแสงออกมาในรูปของโฟตอนจำนวนสองโฟตอน ซึ่งมีพลังงานรวมและโมเมนตัมเท่ากับโฟตอนหนึ่งหน่วยที่เข้ามานั้น ตามหลักอนุรักษ์พลังงานและโมเมนตัม ดังนั้น หากโฟตอนหนึ่งหน่วยถูกปล่อยออกมาในเส้นทางเฉียงขึ้น จะต้องมีโฟตอนอีกหนึ่งหน่วยถูกปล่อยในเส้นทางเฉียงลง เพื่อให้โมเมนตัมลัพธ์ในแนวตั้งมีค่าเป็นศูนย์เช่นเดิม

2.4.3 การทดลองกระจายกุญแจด้วยคู่สถานะพัวพัน (Entangled-photon pairs)

คู่โฟตอนที่ออกมาจากการแปลงผันลงเชิงพารามิเตอร์ (Parametric Down Conversion: PDC) ด้วยวิธีการผ่านผลึกที่มีคุณสมบัติไม่เป็นเชิงเส้น จะมีคุณสมบัติของความพัวพันเชิงควอนตัมอยู่ภายใน ซึ่งกระบวนการเกิดคู่โฟตอนดังกล่าวสามารถแสดงได้ดังรูปที่ 2.11

มีการพิสูจน์ว่าการใช้สถานะพัวพันสามารถทนทานต่อการลดทอนตามระยะทาง (Attenuation/ dissipation) ได้ดีกว่าการใช้แสงลดทอนความเข้ม (Faint pulse) [*Ma และคณะ 2007*] โดยได้มีการพิสูจน์การกระจายกุญแจเชิงควอนตัมด้วยสถานะพัวพันที่ระยะทาง 100 กม. [*Honjo และคณะ 2008*] และ 200 กม. (วางแหล่งกำเนิดไว้ตรงกลาง [*Dynes และคณะ 2009*]) ที่ประเทศญี่ปุ่นด้วยสถานะพัวพันเชิงเวลา และเกณฑ์วิธีกระจายกุญแจ BBM92 [*Honjo และคณะ 2008*] และจนถึง 144 กม. (ระหว่างเกาะ LaPalma และเกาะ Tenerife ประเทศสเปน) ด้วยสถานะพัวพันเชิงโพลาไรซ์ [*Scheidl และคณะ 2009*] โดยในการทดลอง แหล่งกำเนิดความพัวพันตั้งไว้ที่ฝั่งผู้ส่ง (หากจัดวางแหล่งกำเนิดความพัวพันไว้ระหว่างกลางของคู่สื่อสาร จะทำให้สามารถกระจายสถานะพัวพันที่ระยะทางสองเท่า คือ 288 กม. ได้) โดยการทดลองที่ระยะทางดังกล่าวเป็นการยืนยันในเบื้องต้นถึงความเป็นไปได้ของการสื่อสารเชิงควอนตัมจากพื้นโลกสู่ดาวเทียม (Space-QUEST [*Ursin และคณะ 2008*]) เพื่อพิสูจน์ว่าไม่มีข้อจำกัดด้านระยะทางต่อไป การยืนยันความมีอยู่ของคุณสมบัติพัวพันระหว่างอนุภาคทำได้โดยทดสอบผลการวัดสถานะในแต่ละช่วงเวลา ว่ายังคงขัดต่ออสมการ

ของเบลล์อยู่หรือไม่ [*Ekert 1991*] ส่วนในแง่มุมของการเพิ่มอัตราการสร้างกุญแจรหัสลับ ได้มีการทดลองจนถึงระดับเมกะบิตต่อวินาที โดยใช้โพรโตคอลเพิ่มการเปลี่ยนเฟส (Differential-phase shift) ด้วยอัตราเร็ว 1.3 Mbps [*Zhang และคณะ 2009*] และแบบสถานะลวง (Decoy-state) [*Dixon และคณะ 2008*]

2.5 ข้อจำกัดและความท้าทายด้านเทคโนโลยี

หลังจากการนำเสนอต้นแบบระบบวิทยาการรหัสลับเชิงควอนตัมต้นแบบแรกด้วยระยะทางในการสื่อสาร 30 ซม. กลุ่มนักวิจัยทั่วโลกได้แข่งขันกันพัฒนางานวิจัยเพื่อเพิ่มประสิทธิภาพของระบบดังกล่าวให้สูงขึ้น ทั้งวิธีการกำเนิดโฟตอน การส่งโฟตอน การตรวจหาโฟตอน ซึ่งการพัฒนาดังกล่าวมีรายละเอียดดังนี้

2.5.1 แหล่งกำเนิดแสง (photon sources)

2.5.1.1 แหล่งกำเนิดโฟตอนเดี่ยว

แหล่งกำเนิดโฟตอนเดี่ยวจะต้องมีคุณสมบัติที่สำคัญคือ กำเนิดเพียงโฟตอนเดียวอย่างแท้จริง โดยแต่ละโฟตอนที่เกิดขึ้นมีความยาวคลื่นค่าเดียว ซึ่งงานวิจัยที่สามารถสร้างอุปกรณ์กำเนิดโฟตอนเดี่ยวได้อย่างแท้จริงแล้ว ของบริษัทฮิตาชิ [*Xu และคณะ 2008*] และบริษัทโตชิบา [*Shield 2007*]

2.5.1.2 แหล่งกำเนิดแบบพัลส์แสงความเข้มน้อย

วิธีการกำเนิดโฟตอนเดี่ยวที่นิยมใช้คือการใช้สัญญาณพัลส์จากไดโอดชนิดเลเซอร์ความเข้มต่ำ แล้วลดทอนความเข้มจนเหลือโฟตอนเฉลี่ยต่อพัลส์น้อยกว่า 1 มาก ($\mu \ll 1$) ทำให้มีความน่าจะเป็นสูงที่จะไม่มีโฟตอน หรือมีเพียงโฟตอนเดี่ยวออกมา ส่วนความน่าจะเป็นที่จะมี 2 โฟตอนขึ้นไปนั้นมีค่าน้อยมากๆ ซึ่งความเป็นไปได้ในการเกิดโฟตอนจะเป็นไปตามสถิติของปัวซง (Poisson) โดยวิธีการลดความเข้มของแสงจากไดโอดชนิดเลเซอร์นี้มีความสะดวก และมีราคาไม่สูงมาก ทำให้สามารถสร้างอุปกรณ์ต่างๆ ให้มีขนาดเล็กได้

2.5.1.3 แหล่งกำเนิดคู่โฟตอนพัวพัน (entangled photon sources)

แหล่งกำเนิดคู่โฟตอนพัวพันนิยมใช้กระบวนการแปลงผันลงเชิงพารามิเตอร์แบบเกิดขึ้นเอง (Spontaneous Parametric Down Conversion: SPDC) คือ กระบวนการการทำลายโฟตอน แล้วให้กำเนิดโฟตอนสองโฟตอนที่มีพลังงานรวมเท่ากับโฟตอนที่ถูกทำลาย แต่การจะเกิดเหตุการณ์นี้ได้ต้องจัดให้โฟตอนมีอันตรกิริยากับตัวกลางผลึกที่มีคุณสมบัติทัศนศาสตร์ไม่เชิงเส้น เมื่อโฟตอนเดี่ยวผ่านเข้าไปในผลึกที่มีคุณสมบัติไม่เชิงเส้นเช่น BBO (Beta-Barium Borate) ในแนวที่เหมาะสมจะทำให้เกิดโฟตอนออกมาโดยมีความน่าจะเป็นที่จะพบโฟตอนมีลักษณะเป็นกรวยสองกรวย กรวยหนึ่งเป็นแสงโพลาไรซ์แนวนอน อีกกรวยหนึ่งเป็นแสงโพลาไรซ์แนวตั้ง จุดที่กรวยทั้งสองตัดกันจะเป็นผลรวมของโพลาไรเซชันทั้งสองชนิด ซึ่งเป็นจุดที่เกิดคู่โฟตอนพัวพันซึ่งหากไม่ทำการวัดจะไม่สามารถทราบได้ว่าเป็นแสงโพลาไรซ์แนวตั้ง หรือแนวนอน

2.5.2 ช่องสัญญาณ (quantum channels)

แหล่งกำเนิดโฟตอน (ภาคส่ง) และตัวตรวจหาโฟตอน (ภาครับ) เชื่อมโยงกันด้วยช่องสัญญาณควอนตัม (Quantum channel) อนึ่ง ตัวช่องสัญญาณเองไม่ได้เป็นระบบควอนตัม หากแต่หมายถึงสื่อกลางใด ๆ ที่นำพาข้อมูลซึ่งบรรจุอยู่ในระบบควอนตัมหนึ่ง ๆ ไปได้ สิ่งที่แตกต่างจากช่องสัญญาณดั้งเดิมคือ ในกรณีควอนตัม ข้อมูลถูกแทนลงในสถานะควอนตัมเพียงครั้งเดียวในระบบเดียว (การสื่อสารดั้งเดิม โฟตอนจำนวนนับไม่ได้ มีข้อมูลเดียวกันบรรจุอยู่) สถานะควอนตัมที่ใช้สื่อสารส่วนมากจะเป็นสถานะควอนตัมสองระดับ (Two-level quantum systems) เรียกว่าบิตเชิงควอนตัม (Quantum bits) ในระหว่างการเคลื่อนที่ของสัญญาณควอนตัม จะต้องมีวิธีการปกป้องข้อมูลควอนตัมจากการรบกวนโดยสิ่งแวดล้อม[2.11] สถานะควอนตัมมีความอ่อนไหวต่อ

[2.11] สิ่งแวดล้อมในที่นี้หมายถึง อะไรก็ตามที่นอกเหนือปริมาณอิสระ (Degree of freedom) ที่ใช้แทนข้อมูลที่สนใจ ไม่จำเป็นต้องอยู่นอกระบบทางกายภาพที่ใช้แทนข้อมูลนั้น เช่น กรณีที่ใช้สถานะโพลาไรซ์แทนข้อมูล ความถี่ของโฟตอนเดียวกันนั้นก็ถือว่าเป็นสิ่งแวดล้อม และความเหนี่ยวนำระหว่างความถี่ และโพลาไรเซชัน ต้องถูกพิจารณา

การถูกรบกวนโดยสิ่งแวดล้อม (Decoherence) รวมถึงการสูญเสีย (Dissipation/ loss) ดังนั้นปัจจัยด้านช่องสัญญาณจึงต้องได้รับการพิจารณาโดยละเอียดเช่นกัน โดยหากสัญญาณรบกวนจากช่องสัญญาณสูงมากจนทำให้อัตราผิดพลาดบิตเชิงควอนตัม (Quantum bit error rate: QBER) สูงกว่าหรือเท่ากับ QBER กรณีมีผู้ดักจับ จะทำให้ไม่สามารถสร้างกุญแจรหัสลับได้เลย

นอกจากนี้ อุปสรรคของการสื่อสารเชิงควอนตัมคือ เวกเตอร์ฐานในการวัดสถานะของฝั่งผู้รับ และเวกเตอร์ฐานที่ใช้เตรียมสถานะโดยผู้ส่ง ต้องมีความสัมพันธ์ระหว่างกันในลักษณะที่แน่นอนอย่างหนึ่ง เช่นโพลาไรเซชันจะถูกบิดไปด้วยมุมคงที่ค่าหนึ่งเสมอ เมื่อผ่านช่องสื่อสารนั้น ซึ่งทำให้ผู้รับสามารถทำการชดเชยความเปลี่ยนแปลงของเวกเตอร์ฐานระหว่างช่องสื่อสารได้ เช่น ชดเชยโพลาไรเซชันให้บิดกลับมาแนวเดิม ถ้าหากความสัมพันธ์ระหว่างเวกเตอร์ฐานดังกล่าวมีการเปลี่ยนแปลงตามเวลา ที่ภาครับต้องมีระบบป้อนกลับเพื่อปรับการชดเชยตามเวลาเช่นเดียวกัน แต่หากการเปลี่ยนแปลงตามเวลาเป็นไปรวดเร็วเกินไป การสื่อสารจะล้มเหลวได้ [*Gisin และคณะ 2002*]

ช่องสื่อสารเชิงควอนตัมสามารถแบ่งได้เป็นสองชนิด ดังนี้

2.5.2.1 ช่องสัญญาณเส้นใยแสงหรือไฟเบอร์ (Fiber link)

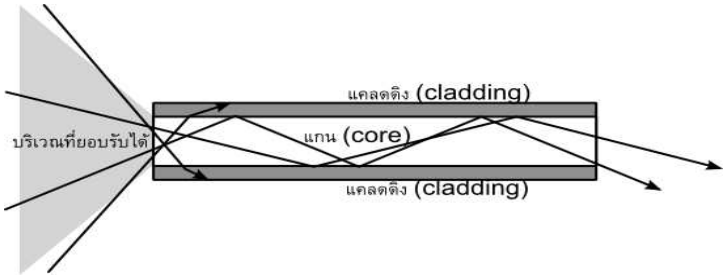
แสงถูกนำพาไปได้โดยผ่านเส้นใยแสง (Optical fibers) ซึ่งมีลักษณะของดัชนีการหักเห $n(x,y)$ ตามพื้นที่หน้าตัดของเส้นใย การเปลี่ยนระดับของดัชนีการหักเหในบริเวณขอบ ทำให้แสงถูกหักเหจนกระทั่งเบนกลับมายังแนวแกนของเส้นใย ตลอดเวลา 25 ปี นับจนถึง ค.ศ. 2002 ได้มีความพยายามในการพัฒนาคุณภาพของเส้นใยแสง โดยแต่เดิมมีความลดทอนอยู่ที่หลายเดซิเบล (dB) ต่อกิโลเมตร ลงเหลือ 2 เดซิเบลต่อกิโลเมตร สำหรับความยาวคลื่น 800 นาโนเมตร เหลือ 0.35 เดซิเบลต่อกิโลเมตร สำหรับความยาวคลื่น 1310 นาโนเมตร และเหลือ 0.2 เดซิเบลต่อกิโลเมตร สำหรับความยาวคลื่น 1510 นาโนเมตร [*Gisin และคณะ 2002*] ดังนั้นแสงความยาวคลื่น 1510 นาโนเมตร ที่มีความลดทอนต่ำที่สุด จึงพบว่าถูกนำมาใช้ทำการทดลองการสื่อสารเชิงควอนตัมได้

กรณีเส้นใยแสงที่มีแกนหนา สามารถนำพาแสงที่เข้ามาในทิศทางต่างๆ ได้ดังรูปที่ 2.12 เส้นใยแสงดังกล่าวเรียกว่าไฟเบอร์หลายโหมด[2.12] (multi-mode fiber) ซึ่งโดยทั่วไปมีเส้นผ่านศูนย์กลางของบริเวณแกนประมาณ 50 ไมโครเมตร ซึ่งแสงในโหมดต่างๆ จะเหนี่ยวนำกันอย่างง่ายดาย ทำให้สถานะควอนตัมถ้าถูกส่งผ่านไฟเบอร์หลายโหมดนี้ จะถูกรบกวนด้วยแสงในโหมดต่างๆ ที่เคลื่อนที่ไปในเส้นใยแสงเดียวกัน ดังนั้นเส้นใยแสงแบบหลายโหมดจึงไม่เหมาะสมในการนำมาใช้สำหรับการสื่อสารเชิงควอนตัม ส่วนเส้นใยแสงที่มีเส้นผ่านศูนย์กลางของบริเวณแกนเล็กลงถึงประมาณ 2-3 เท่าของความยาวคลื่น จะทำให้แสงในโหมดเส้นทางเดียวเท่านั้นที่ถูกนำพาไปได้ เส้นใยแสงลักษณะดังกล่าว เรียกว่า ไฟเบอร์โหมดเดี่ยว (Single-mode fiber) สำหรับแสงในความถี่ทั่วไปของการสื่อสาร (ความยาวคลื่น 1.3 และ 1.5 ไมโครเมตร) เส้นผ่านศูนย์กลางของไฟเบอร์โหมดเดี่ยวอยู่ที่ประมาณ 8 ไมโครเมตร เส้นใยแสงโหมดเดี่ยวมีความเหมาะสมในการใช้เป็นช่องสื่อสารควอนตัม โดยเฉพาะ เมื่อเฟสของแสงที่ปลายทางมีความสัมพันธ์ที่แน่นอนกับเฟสที่ต้นทาง คือสายไฟเบอร์ไม่ถูกดึงให้ยาวขึ้น หรือหดสั้นลง ดังนั้น เส้นใยแสงจึงเหมาะสมในการสื่อสารที่อาศัยการแทรกสอด และแทนข้อมูลด้วยความต่างเฟส [*Gobby และคณะ 2004*]

ดังนั้น เส้นใยแสงโหมดเดี่ยว ที่มีดัชนีหักเหลักษณะสมมาตรในเชิงทรงกระบอก ซึ่งทำให้ไม่มีการบิดสถานะของแสง เช่นของโพลาไรเซชันในลักษณะที่ไม่พึงประสงค์ จึงเป็นช่องสัญญาณควอนตัมในอุดมคติ (Ideal quantum channel) ได้ แต่ในความเป็นโดยปกติจริงเส้นใยแสงทั้งหมดมีความอสมมาตรอยู่ ซึ่งทำให้โพลาไรเซชันของแสงเกิดการเปลี่ยนแปลงในลักษณะที่ไม่ต้องการ เช่นเดียวกับปรากฏการณ์ที่คลื่นความถี่ต่างกันเคลื่อนที่ด้วยความเร็วต่างกันในช่องสัญญาณ (Chromatic dispersion) ซึ่งล้วนต้องได้รับการพิจารณา

เช่นในกรณีช่องสัญญาณที่มีการเปลี่ยนโพลาไรซ์แบบขึ้นตรงกับความถี่ และความสัมพันธ์โดยตรงระหว่างโพลาไรเซชันและความถี่ก็ต้องได้รับการพิจารณาเช่นเดียวกัน

[2.12] โหมดในกรณีนี้ หมายถึงโหมดของทิศทางและตำแหน่ง (Spatial mode) โดยแสงความถี่ต่างๆ ที่แผ่ไปในทิศทางเดียวกันถือว่าอยู่ในโหมดเดียวกัน (ในที่นี้) ในที่อื่นๆ อาจกล่าวถึงโหมดความถี่โดยแสงความถี่ต่างกันถือว่าอยู่ต่างโหมด



รูปที่ 2.12 เส้นใยแสงแบบหลายโหมด (multi-mode fiber) แสดงทิศการแผ่ออกไปของคลื่นแสงไปตามเส้นใยแสง ซึ่งประกอบขึ้นด้วยสองส่วนคือส่วนแกน และส่วนแคลดดิงซึ่งมีค่าดัชนีหักเหต่ำกว่าบริเวณแกนและทำให้แสงเกิดการหักเหจนกระทั่งเลี้ยวกลับสู่แนวแกนดังเดิม โดยจะเป็นเช่นนี้ไปตลอดแนวเส้นใยแสง อนึ่งหากแสงมีทิศเข้ามาเกินจากช่วงยอมรับได้ แสงนั้นจะไม่สามารถเกิดการหักเหเลี้ยวกลับหมดภายในเส้นใยได้

2.5.2.2 ช่องสัญญาณผ่านอากาศ (Free-space link)

แม้ว่าการสื่อสารผ่านเส้นใยแสงจะได้รับการพัฒนาไปมาก แต่ก็มีข้อจำกัดถึงบริเวณที่เส้นใยจะสามารถถูกลากไปได้และความพร้อมใช้ของช่องสื่อสาร ความพยายามในการพัฒนาการสื่อสารผ่านอากาศ โดยเริ่มจากเป็นเส้นทางตรง (Line of sight) ซึ่งได้มีการพัฒนาแล้วสำหรับการสื่อสารดั้งเดิมจึงเป็นอีกแนวทางคู่ขนานหนึ่ง ถูกนำมาทดลองเช่นกันในการกระจายกุญแจรหัสลับเชิงควอนตัม [*Hughes และคณะ 2000*] รวมทั้งการกระจายคู่สถานะพัวพัน [*Ursin และคณะ 2007*]

การสื่อสารเชิงควอนตัมผ่านอากาศ มีข้อดีคือสภาพแวดล้อมบนผิวโลกมีช่วงความถี่สำหรับการสื่อสาร (Transmission window) คือ ช่วงความถี่ที่คลื่นแสงถูกดูดกลืนผ่านอากาศน้อยมาก ที่ช่วงประมาณ 770 นาโนเมตร และตัวกลางซึ่งเป็นอากาศมีลักษณะไม่ทำให้เกิดการเบี่ยงเบนโพลาไรเซชันหรือเบี่ยงเบนน้อยมาก ดังนั้นสถานะโพลาไรซ์ของโฟตอนจึงถูกนำมาแทนข้อมูลในการสื่อสารเชิงควอนตัมผ่านอากาศ

อย่างไรก็ตาม ข้อเสียของการใช้อากาศเป็นสื่อกลางเมื่อเทียบกับการใช้เส้นใยแสง คือ ในเส้นใยแสง พลังงานของคลื่นแสงจะถูกอนุรักษ์อยู่ในบริเวณช่องสัญญาณนั้น แต่ในการแผ่ของแสงผ่านอากาศจะต้องมีการสูญเสียพลังงานบางส่วนไปยังสิ่งแวดล้อม นอกจากเรื่องการสูญเสียพลังงานแล้ว แสงจากดวงอาทิตย์รวมถึงแสงจากดวงจันทร์นั้นส่งผลต่อตัวตรวจหาแสงที่ภาครับได้ แต่อุปสรรคนี้แก้ไขได้โดยใช้ตัวกรองความถี่ (Spectral filter) ตัวกรอง (Spatial filter) และการแยกแยะเวลา (Timing discrimination) ซึ่งอาศัยช่วงสอดคล้องทางเวลา (Coincidence) ที่หลักนาโนวินาที

ส่วนคุณภาพของการสื่อสารเชิงควอนตัมผ่านอากาศ ขึ้นตรงกับสถาพแวดล้อมและเป็นไปได้ก็ต่อเมื่อเส้นทางสะดวกและท้องฟ้าปลอดโปร่ง นอกจากนี้หากอากาศมีสภาพแปรปรวน (Turbulence) แสงที่ส่งไปจะมีความเหลื่อมล้ำในแกนเวลาในช่วงเวลารวดเร็ว (Time jitter) และระยะเวลาช้า (wander) เกิดขึ้น โดยปัญหาความคลาดเคลื่อนในแกนเวลานี้ สามารถแก้ไขได้โดยการส่งพัลส์แสงอ้างอิงที่มีความถี่ต่างกัน (ซึ่งคาดว่าได้รับผลกระทบจาก Time jitter น้อยกว่า) ไปทุกครั้งก่อนส่งสัญญาณควอนตัมจริงไป นอกจากนี้ยังสามารถใช้พัลส์แสงอ้างอิงในการสะท้อนกลับจากภาครับ เพื่อให้ภาคส่งปรับทิศทางการส่งให้เหมาะสมได้อีกด้วย

นอกจากนี้ปัญหาที่สำคัญคือการบานออกของลำแสง ซึ่งเกิดจากการเลี้ยวเบนผ่านรูปล่อยแสงที่ฝั่งผู้ส่ง ทำให้บริเวณตกกระทบถึงฝั่งผู้รับมีช่วงกว้างออก แต่แก้ปัญหาได้ด้วยการใช้อุปกรณ์เชิงแสงที่มีขนาดใหญ่ขึ้น นับจากต้นแบบของเบนเนตต์และบราสซาร์ด (BB84) นำเสนอในเมืองบังกาลอร์ ประเทศอินเดีย การสาธิตกระจายกุญแจรหัสลับเชิงควอนตัมผ่านอากาศอย่างเป็นระบบครั้งแรกจึงมีขึ้นใน ค.ศ. 1996 โดย ไบรอัน จาคอบ (Bryan C. Jacobs) และเจมส์ ฟรานสัน (James D. Franson) [*Jacobs & Franson 1996*] และ ค.ศ. 2000 โดยกลุ่มของ ริชาร์ด ฮิวส์ (Richard J. Hughes) ในปี ค.ศ. 2000 [*Hughes และคณะ 2000*] (บทวิเคราะห์อย่างละเอียดเรื่องการกระจายกุญแจรหัสลับเชิงควอนตัมผ่านอากาศ [*Gilbert & Hamrick 2000*])

2.5.3 ตัวตรวจหาโฟตอนเดี่ยว (single-photon detectors)

เมื่อมีแหล่งกำเนิดโฟตอนเดี่ยวเทียมและแหล่งกำเนิดคู่โฟตอนพัวพัน รวมถึงช่องสื่อสารเชิงควอนตัมที่เหมาะสมแล้ว ความสำเร็จของวิทยาการรหัสลับเชิงควอนตัมก็ขึ้นอยู่กับความสามารถในการตรวจหาโฟตอนเดี่ยว (single-photon detection) ซึ่งโดยหลักการแล้ว ทำได้หลายวิธี เช่น ใช้ตัวคูณเชิงแสง (Photo multiplier) ตัวตรวจหาแสงชนิดไดโอดแบบถล่มทลาย (Avalanche Photodiodes : APD) [*Mikhailova & Andreev 2006*] การใช้ Josephson junction ในสารตัวนำยิ่งยวด (Superconductors) [*Hao และคณะ 2009*] และการใช้ควอนตัมดอท [*Blakesley และคณะ 2005*] โดยตัวตรวจหาโฟตอนเดี่ยวในอุดมคติต้องสอดคล้องกับเงื่อนไขต่อไปนี้ [*Gisin และคณะ 2002*]

1) ประสิทธิภาพการตรวจหาโฟตอนเดี่ยว (quantum detection efficiency) สูง และทำงานได้ในช่วงความถี่กว้าง
2) ความน่าจะเป็นในการเกิดสัญญาณรบกวน (dark count probability) คือการมีสัญญาณขึ้นในขณะที่ไม่มีโฟตอนตกกระทบมีค่าน้อย
3) ระยะเวลานับตั้งแต่โฟตอนตกกระทบ จนกระทั่งเกิดกระแสไฟฟ้าตรวจวัดขึ้นนั้น ต้องเป็นระยะเวลาคงที่ เพื่อให้ได้ผลลัพธ์ในแกนเวลาที่มีความละเอียด
4) เวลาในการคืนสภาพ (recovery time หรือ dead time) มีค่าน้อย เพื่อให้ได้อัตราการส่ง-รับข้อมูล (data rate) และอัตราการสร้างกุญแจ (key rate) สูง

นอกจากนี้ยังต้องระวังในการรักษาตัวตรวจหาแสงให้อยู่ในสภาพที่ทำงานได้ ซึ่งในการลดสัญญาณรบกวนอันเกิดจากความร้อน (Thermal noise) ตัวตรวจหาโฟตอนต้องถูกรักษาไว้ในอุณหภูมิที่ต่ำมากด้วยฮีเลียมเหลว หรือวิธีทำความเย็นด้วยไนโตรเจน ซึ่งเป็นอุปสรรคในการทำให้การสื่อสารเชิงควอนตัมไปสู่เชิงพาณิชย์ เงื่อนไขความเป็นอุดมคติของตัวตรวจหาโฟตอนเดี่ยวไม่สามารถสอดคล้องได้ทั้งหมดในเวลาเดียวกัน ตัวตรวจหาโฟตอนเดี่ยวที่นิยมคือ ตัวตรวจหาแสงชนิดไดโอดแบบถล่มทลาย (Avalanche photodiode: APD) โดยมีสารกึ่งตัวนำสามชนิดที่นิยมนำมาสร้าง APD ได้แก่ ซิลิกอน (Si) แกเลียมอาเซไนด์ (GaAs) และ อินเดียมแกเลียมอาเซไนด์ (InGaAs) งานวิจัยเพื่อพัฒนาตัวตรวจหาโฟตอน เช่น การลดเวลาที่ใช้ในการคืนสภาพ และเพิ่มประสิทธิภาพการตรวจหา เป็นต้น จึงเป็นงานที่ส่งผลโดยตรงต่อเทคโนโลยีรหัสลับและการสื่อสารเชิงควอนตัม ดิซอน (Dixon) และคณะวิจัยที่ศูนย์วิจัยโตชิบาแห่งสหภาพยุโรป (Toshiba Research Europe Ltd.) รายงานผลการวิจัยตัวตรวจหาโฟตอนเดี่ยวแบบถล่มทลายที่สร้างจากอินเดียมแกเลียมอาเซไนน์ (InGaAs) ซึ่งให้ค่า dead time เพียง 1.93 ns และอัตราการตรวจหาโฟตอนเดี่ยวถึง 497 MHz [*Dixon และคณะ 2009*] โดยตัวตรวจหาโฟตอนเดี่ยวจากกลุ่มวิจัยดังกล่าวได้ถูกนำมาใช้ในการสาธิตทดลองกระจายกุญแจเชิงควอนตัมซึ่งได้อัตราการสร้างกุญแจรหัสลับเชิงควอนตัมสูงถึง 1.02 Mb/s ที่ระยะทาง 20 กม. [*Yuan และคณะ 2009*]

2.5.4 แหล่งกำเนิดจำนวนสุ่มเชิงควอนตัม (quantum random number generators)

กุญแจที่ใช้ในการเข้ารหัสลับแบบใช้งานครั้งเดียวต้องเป็นความลับและมีความยาวเท่ากับข้อความ รวมถึงต้องเป็นจำนวนสุ่มแท้จริง ในขณะที่ดิจิทัลคอมพิวเตอร์ซึ่งมีขนาดหน่วยความจำจำกัดนั้นไม่สามารถใช้สร้างจำนวนสุ่มแท้จริงได้ (เพราะไม่ว่าจะใช้ฟังก์ชันที่ซับซ้อนเพียงใด ก็ต้องวนกลับไปถึงจุดที่สถานะซ้ำเดิม หรือเป็นคาบในที่สุด[2.13]) จำนวนสุ่มแท้จริงจึงต้องสร้างจากปรากฏการณ์สุ่มในธรรมชาติ โดยมีการเสนอให้ใช้สัญญาณรบกวนในวงจรอิเล็กทรอนิกส์ [*Petries และคณะ 2000*] การใช้ระบบไม่เป็นระเบียบ (Chaotic) ซึ่งเมื่อเปลี่ยนแปลงไปเป็นเวลามากกว่าค่าหนึ่ง สถานะที่ได้จะลู่เข้าสู่จำนวนสุ่มแท้จริง [*Bernstein & Lieberman 1989*]

ในทางควอนตัม ตัวเลือกที่เป็นธรรมชาติตัวอย่างหนึ่งคือ เส้นทางที่โฟตอนเดี่ยวเคลื่อนที่ผ่านตัวแยกลำแสง (beam

[2.13] อธิบายในเชิงคณิตศาสตร์ด้วย “ทฤษฎีรังของนกพิราบ” (Pigeon's hole theorem) ที่กล่าวว่า เมื่อมีรังนกอยู่ n รัง และมีนกทั้งหมด n+1 ตัว จะต้องมีอย่างน้อยหนึ่งรัง ที่มีนกอยู่มากกว่าหนึ่งตัว โดยในที่นี้ “รังนก” เทียบได้กับสถานะในหน่วยความจำของคอมพิวเตอร์ และ “ตัวนก” หมายถึงสถานะที่คำนวณได้ในแต่ละช่วงเวลา นั่นคือ สมมติว่าหน่วยความจำบรรจุสถานะได้ N สถานะ เมื่อทำการวนรอบการสร้างจำนวนสุ่มเทียม ถึงรอบที่ N+1 จะต้องได้ค่าซ้ำกับค่าใดค่าหนึ่งที่เคยสร้างได้แล้ว (กลับมาเป็นคาบ)

splitter) แบบ 50:50 [*Stefanov และคณะ 1999*] หรือใช้สถานะสปินในแนว z วิ่งผ่านการวัดสปินในแนว x ในการทดลองของสเติร์นและเกอร์แลค [*Gerlach & Stern 1922*] (ซึ่งจะถูกสุ่ม 50:50 ว่าสถานะผลลัพธ์จะเป็น $+x$ หรือ $-x$) ซึ่งโดยหลักการแล้วสามารถทำให้เกิดจำนวนสุ่มแท้จริงได้ ส่วนในทางปฏิบัติต้องพิจารณาสหสัมพันธ์ระหว่างสถานะของอนุภาคในช่วงเวลาใกล้เคียงกัน แต่สิ่งที่เป็นอุปสรรคในการสร้างจำนวนสุ่มเชิงควอนตัมด้วยสถานะของแสง คือระยะเวลาคืนสภาพของตัวตรวจหาโฟตอน โดยในช่วงเวลาที่ตัวตรวจหาโฟตอนคืนสภาพไม่สมบูรณ์ ความไม่พร้อมของตัวนำไฟฟ้าที่ตัวตรวจหาจะทำให้เกิดสัญญาณที่มีสหสัมพันธ์ระหว่างช่วงเวลาติดๆ กัน ซึ่งปรากฏการณ์นี้จะยิ่งส่งผลมากขึ้นหากส่งพัลส์แสงเข้าสู่ภาครับในอัตราที่เร็วขึ้น ซึ่งจากขีดจำกัดด้านเทคโนโลยีดังกล่าวทำให้อัตราการสร้างจำนวนสุ่มเชิงควอนตัมยังถูกจำกัดอยู่ที่ระดับเมกะเฮิรตซ์ ของช่วงเวลาอ้างอิง ค.ศ. 2002 [*Gisin และคณะ 2002*]

ในเกณฑ์วิธีกระจายกุญแจแบบ BB84 ผู้ส่งต้องสร้างจำนวนสุ่มสองบิตต่อหนึ่งสถานะของแสงที่ถูกส่งไป ส่วนผู้รับต้องสุ่มเวกเตอร์ฐานหนึ่งบิตต่อหนึ่งสถานะของแสงที่เข้ามา ดังนั้นภาคส่งจึงต้องสามารถสร้างจำนวนสุ่มด้วยอัตราที่สูงกว่าภาครับถึงสองเท่า (หรือมากกว่าสองเท่า เนื่องจากสถานะที่สูญเสียไปในช่องสัญญาณ ผู้รับไม่จำเป็นต้องสุ่มเวกเตอร์ฐานเพื่อทำการวัด) วิธีการหนึ่งที่จะแก้ปัญหาเบื้องต้น คือผู้ส่งสร้างจำนวนสุ่มเก็บไว้รอก่อนเริ่มการส่งสถานะควอนตัม แต่ก็มีข้อเสียคือการเก็บจำนวนสุ่มที่จะนำมาสร้างเป็นกุญแจไว้ในหน่วยความจำ เป็นการเพิ่มโอกาส (ช่วงเวลา) ที่ผู้ดักจับสามารถเข้ามาล้วงข้อมูลจำนวนสุ่มดังกล่าวได้ [*Gisin และคณะ 2002*] (การสร้างจำนวนสุ่มแบบเวลาจริง จะไม่พบปัญหานี้) มีวิธีแก้ปัญหาการเลือกเวกเตอร์ฐานในการกระจายกุญแจรหัสลับเชิงควอนตัมวิธีหนึ่งคือ ใช้ตัวแยกลำแสงเป็นตัวเลือกเวกเตอร์ฐานอย่างอัตโนมัติ โดยโฟตอนที่วิ่งทะลุและสะท้อน จะถูกบิดโพลาไรเซชันไม่เท่ากัน (ในกรณีที่แทนข้อมูลด้วยโพลาไรเซชัน) ขึ้นกับเวกเตอร์ฐานที่ต้องการวัด

2.5.5 หน่วยย้ำสัญญาณเชิงควอนตัม (Quantum repeaters)

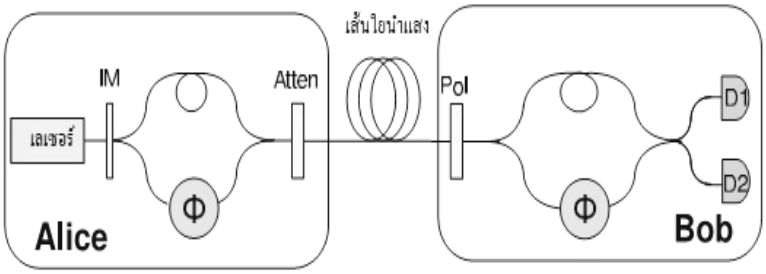
ความลดทอนตามเส้นทางทำให้การสื่อสารเชิงควอนตัมในระยะไกล (หลัก 100 กม. ขึ้นไป) ทำได้ยาก จึงมีการเสนอวิธีแก้โดยการสร้างกลไกเพื่อให้เกิดการย้ำหรือการทวนสัญญาณเชิงควอนตัมที่ซับซ้อนและห่างไกลในการสร้างเพื่อใช้งานจริง วิธีหนึ่งคือการใช้สถานะพัวพันที่กระจายในคู่จุดเชื่อมต่อ (A--S_1, S_2--B) จากนั้นทำการวัดสถานะแบบร่วมกัน (Joint measurement หรือ Bell-state measurement) ระหว่างรอยต่อที่ไม่มีความพัวพัน (คู่ S1--S2) เพื่อทำหน้าที่สลับคู่พัวพัน (Entanglement swap) ให้ท้ายสุดได้คู่สถานะพัวพันระหว่างผู้ส่งและผู้รับ ซึ่งสามารถนำมาใช้สร้างกุญแจรหัสลับหรือการสื่อสารเชิงควอนตัมแบบอื่นๆ ได้ [*Zhao และคณะ 2003*] ซึ่งยังคงอยู่ในระหว่างการพิจารณาทั้งแนวคิดเพื่อความปลอดภัยของข้อมูลกับการสร้างจริง

2.6 พัฒนาการของผลิตภัณฑ์

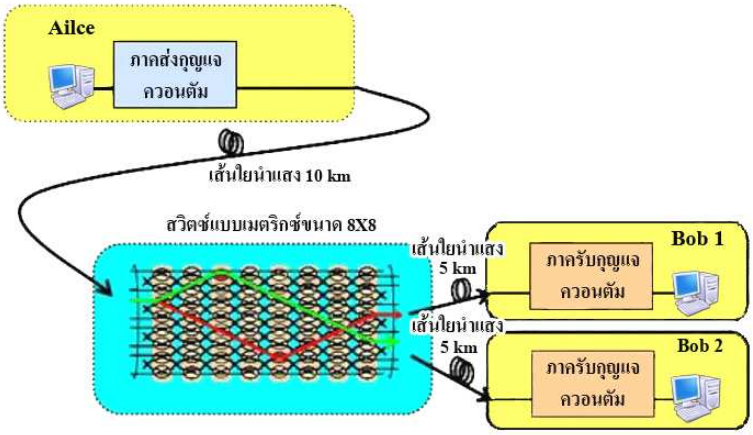
ผลิตภัณฑ์ทางด้านวิทยาการรหัสลับเชิงควอนตัมมีการผลิตและจำหน่ายมาตั้งแต่ช่วงต้นทศวรรษที่ 2000 โดยสามารถแบ่งประเภทได้ดังนี้

2.6.1 อุปกรณ์เชิงพาณิชย์

อุปกรณ์กระจายกุญแจรหัสลับเชิงควอนตัมเริ่มมีการผลิตออกจำหน่ายในปี ค.ศ. 2003 โดยบริษัท ID Quantique ประเทศสวิตเซอร์แลนด์ [*IdQ.NET*] และยังคงมีการพัฒนาและจำหน่ายอย่างต่อเนื่อง โดยอุปกรณ์ดังกล่าวเป็นแบบ “Plug & Play” ซึ่งมีการชดเชยสถานะเชิงควอนตัมอย่างอัตโนมัติตามเส้นทางไป-กลับ ของภาคส่งและภาครับ [*Muller และคณะ 1997*] ประเทศสหรัฐอเมริกามีบริษัท MagiQ Technologies จำหน่ายและวิจัยผลิตภัณฑ์กระจายกุญแจรหัสลับเชิงควอนตัม โดยอ้างว่าได้รับการติดต่อจากหน่วยราชการด้านการทหาร (DARPA) และสถาบันวิจัยอวกาศ (NASA) ของสหรัฐฯ [*MagiQ.NET*] แต่เนื่องจากตลาดของผู้ใช้ระบบวิทยาการรหัสลับเชิงควอนตัมยังจำกัด และต้นทุนที่สูง อีกทั้งเทคโนโลยีที่ยังไม่อิ่มตัว ทำให้บริษัทต่างๆ ที่จัดจำหน่ายผลิตภัณฑ์กระจายกุญแจรหัสลับดังกล่าวจึงมีการผลิตเมื่อมีผู้ร้องขอเป็นส่วนใหญ่และร่วมกับอุตสาหกรรมด้านรหัสลับแบบเดิมพัฒนาระบบลูกผสมเพื่อให้สามารถใช้ฐานกลุ่มลูกค้าฐานเดิมได้เป็นหลัก



รูปที่ 2.13 แบบจำลองการทำงานของการใช้มาตรแทรกสอดแบบแมส- แซนเดอร์ และการเข้ารหัสด้วยการเลื่อนเฟส ที่ทีมวิจัยของโตชิบาใช้ รูปดัดแปลงจาก[*Peev และคณะ 2009*]



รูปที่ 2.14 การกระจายกุญแจรหัสลับเชิงควอนตัมผ่านสวิตช์เชิงแสง ทำจาก Planar Lightwave circuit (PLC) ขนาด 8 x 8 ช่วยเลือกเส้นทางไปยังผู้รับสองจุดได้ ซึ่งเป็นความร่วมมือระหว่างบริษัท NTT และมหาวิทยาลัยสแตนฟอร์ด รูปดัดแปลงจาก [*NTT.NET*]

2.6.2 ต้นแบบอนาคต

บริษัทโตชิบา (Toshiba) ซึ่งมีศูนย์วิจัยอยู่ที่สหราชอาณาจักร ภายใต้การนำของ แอนดรูว์ ชิลด์ส (A. J. Shields) ได้ทำการพัฒนาระบบวิทยาการรหัสลับเชิงควอนตัมในรูปแบบพัลส์ความเข้มต่ำทิศทางเดียว (One-way weak pulse) และการแทนสถานะด้วยเฟส (Phase coding) ที่แตกต่างระหว่างแสงในสองเส้นทางตามแบบจำลองของมาตรแทรกสอดแบบแมส- แซนเดอร์ ศูนย์วิจัยของบริษัทเอ็นทีที (Nippon Telegraph and Telephone: NTT) ประเทศญี่ปุ่นประกาศผลสำเร็จของการทดลองกระจายกุญแจรหัสลับเชิงควอนตัมผ่านหลายผู้รับโดยใช้สวิตช์เชิงแสง (optical switch) ดังรูปจำลองรูปที่ 2.14 ซึ่งทำหน้าที่เปลี่ยนเส้นทางสถานะควอนตัมของแสงที่ส่งไปได้ โดยการทดลองและพัฒนาเป็นความร่วมมือกับมหาวิทยาลัยสแตนฟอร์ด ในปี ค.ศ. 2005 [*NTT.NET*] นอกจากนั้นประเทศออสเตรเลียมีบริษัทจำหน่ายผลิตภัณฑ์วิทยาการรหัสลับเชิงควอนตัม Quintessence Labs จำหน่ายชุดกระจายกุญแจรหัสลับเชิงควอนตัมด้วยแสงความเข้มสูง หรือการกระจายกุญแจด้วยสถานะต่อเนื่องรูปแบบหนึ่ง และเริ่มทยอยมีบริษัทที่ผันตัวออกมาจากหน่วยปฏิบัติการในมหาวิทยาลัยเพิ่มมากขึ้นตามลำดับ

2.7 ประเด็นหลักกับการพัฒนา

นอกเหนือจากผลิตภัณฑ์ที่มีจำหน่ายจริงในเชิงพาณิชย์แล้ว ยังมีการนำเสนอถึงความก้าวหน้าของงานวิจัยทางด้านวิทยาการรหัสลับจากหลายๆ หน่วยงานทั่วโลก ซึ่งประกอบด้วย

2.7.1 เครือข่ายการกระจายกุญแจรหัสลับเชิงควอนตัม (QKD Network)

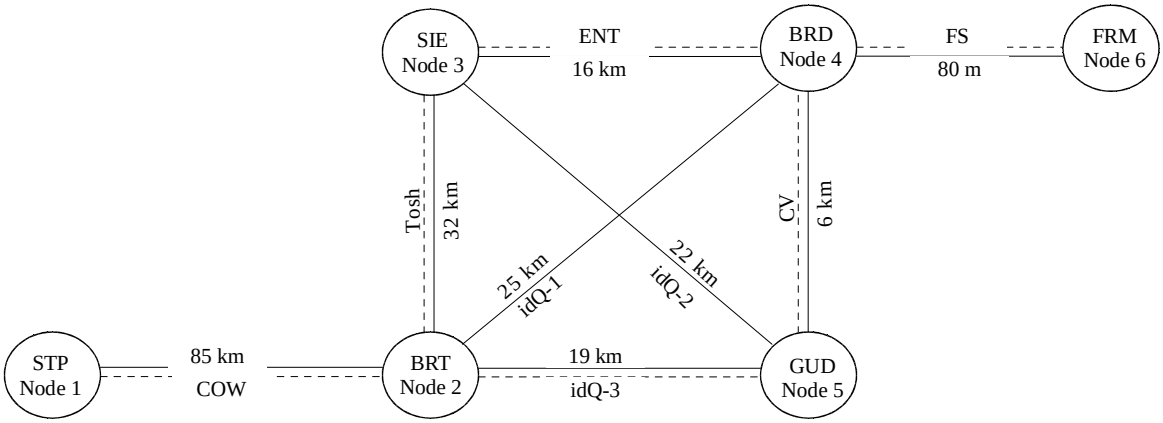
ในปี ค.ศ. 2004 บริษัท BBN Technologies ซึ่งเป็นบริษัททางด้านเทคโนโลยีขั้นสูง ประเทศสหรัฐอเมริกา ร่วมกับมหาวิทยาลัยบอสตัน ประเทศสหรัฐอเมริกา สาธิตเครือข่ายการกระจายกุญแจรหัสเชิงควอนตัมโดยใช้สวิตช์เชิงแสง (Optical switches) [*Pearson และคณะ 2004*] ข้อดีของการใช้สวิตช์เชิงแสงและอุปกรณ์กำหนดเส้นทางเชิงแสง คือคู่สื่อสารไม่จำเป็นต้องกระจายกุญแจผ่านโหนดเชื่อถือได้ (Trusted nodes) [*Chapuran และคณะ 2009*]

ค.ศ. 2008 หลายประเทศในสหภาพยุโรป ร่วมกันสาธิตระบบวิทยาการรหัสลับเชิงควอนตัมผ่านเครือข่ายในโครงการเครือข่ายกระจายกุญแจเชิงควอนตัมในยุโรป (Secure Communication based on Quantum Cryptography: SECOQC) โดยใช้โครงสร้างที่ให้โหนดระหว่างทางเป็นโหนดเชื่อถือได้ [*Peev และคณะ 2009*] โดยมีการปรับใช้โพรโตคอลและวิธีจัดอุปกรณ์สำหรับการกระจายกุญแจรหัสลับต่างๆ กันไปในแต่ละลิงค์ ได้แก่ (1) วิธีชดเชยอัตโนมัติตามเส้นทางและแทนรหัสด้วยความต่างเฟส (Phase-coding Plug&Play configuration) โดยบริษัท ID Quantique (2) วิธีใช้แสงลดทอนความเข้มและแทนรหัสด้วยความมีพัลส์และไม่มีพัลส์ (Coherent one-way protocol: COW) โดยมหาวิทยาลัยเจนีวา (University of Geneva) ร่วมกับสถาบันเทคโนโลยีแห่งออสเตรีย (Austrian institute of technology: AIT) (3) วิธีมาตรแทรกสอดแบบแมส-แซนเดอร์ (Mach-Zehnder Interferometer) โดยใช้พัลส์แสงลดทอนความเข้ม (One-way weak pulse) โดยศูนย์วิจัยบริษัทโตชิบา แห่งสหราชอาณาจักร (4) วิธีใช้คู่สถานะพัวพันของโฟตอนร่วมกับโพรโตคอลของ เบนเนตต์ (Bennett) บราสซาร์ด (Brassard) และ เมอร์มิน (Mermin) (BBM92) โดยความร่วมมือของมหาวิทยาลัยแห่งเวียนนา (University of Vienna) สถาบันเทคโนโลยีแห่งออสเตรีย และสถาบันเทคโนโลยีสวิสซูริค (ETH Zurich, Swiss Federal Institute of Technology) และ (5) วิธีใช้สถานะต่อเนื่อง (Continuous-variable QKD) โดยกลุ่มวิจัยที่ฝรั่งเศส (CNRS) ร่วมกับเบลเยียม นำโดยแกรนจิเออร์ (P. Grangier) โดยจัดการสาธิตเครือข่ายดังรูปที่ 2.15

เนื่องจากโครงการเครือข่ายกระจายกุญแจเชิงควอนตัม SECOQC ได้ทำการสาธิตการกระจายกุญแจเชิงควอนตัมในเครือข่ายพร้อมกันเพียงระยะเวลาระดับชั่วโมง จึงอาจยังไม่เพียงพอต่อการทดสอบเสถียรภาพของระบบการกระจายกุญแจบนเครือข่ายดังกล่าว มหาวิทยาลัยเจนีวา นำโดยนิโคลัส จีไซน์ (Nicolas Gisin) ร่วมกับบริษัท ID Quantique รวมทั้งองค์กรวิจัยทางนิวเคลียร์แห่งสหภาพยุโรป (European Organization for Nuclear Research: CERN) และองค์กรต่างๆ ในปี ค.ศ. 2009 ได้ทำการสาธิตระบบเครือข่ายกระจายกุญแจเชิงควอนตัม SwissQuantum ซึ่งทดลองเป็นระยะเวลาต่อเนื่อง 6 เดือน (ถึงเดือนธันวาคม 2552) โดยแสดงผลการกระจายกุญแจบนเว็บไซต์แบบออนไลน์ [*Swissquantum.NET*]

และในปี ค.ศ. 2010 สำนักงานเทคโนโลยีสารสนเทศและการสื่อสารแห่งประเทศญี่ปุ่น (National Institute of Information and Communications Technology: NICT) สำนักงานส่งเสริมเทคโนโลยีสารสนเทศ ประเทศญี่ปุ่น (Information-technology Promotion Agency: IPA) และ สถาบันพัฒนาวิทยาศาสตร์และเทคโนโลยีอุตสาหกรรมแห่งประเทศญี่ปุ่น (National Institute of Advanced Industrial Science and Technology: AIST) ร่วมกับบริษัท และสถาบันวิจัยจากหลายประเทศ สาธิตระบบวิทยาการรหัสลับเชิงควอนตัมและการสื่อสารเชิงควอนตัม ณ กรุงโตเกียว โดยจัดการสาธิตเครือข่ายดังรูปที่ 2.16

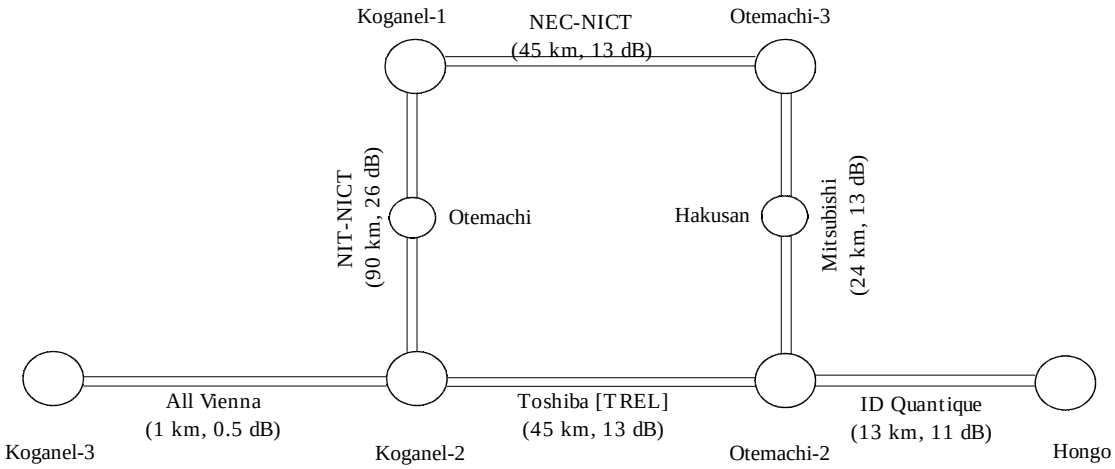
(ก)



(ข)

(ค)

รูปที่ 2.15 (ก) การจำลองบนภาพถ่ายดาวเทียมแสดงตำแหน่งของโหนดต่างๆ ในการสาธิตเครือข่ายกระจายกุญแจเชิงควอนตัมในยุโรป (SECOQC) ในปี ค.ศ. 2008 (ข) การเชื่อมต่อการกระจายกุญแจเชิงควอนตัมต่าง ๆ ที่ใช้ในเครือข่าย (COW: Coherent One-way; Tosh: One-way weak pulse (Toshiba); idQ: Plug&Play configuration; ENT: Entanglement-based QKD; FS: Free-space QKD) [*Peev และคณะ 2009*] (ค) ทีมงานผู้ร่วมจัดการสาธิต และหน่วยงานที่ให้การสนับสนุน



(ก)

(ข)

รูปที่ 2.16 (ก) แผนที่เครือข่ายการกระจายกุญแจเชิงควอนตัม ณ กรุงโตเกียว ค.ศ. 2010
(ข) ทีมงานผู้ร่วมจัดการสาธิต และหน่วยงานที่ให้การสนับสนุน

2.7.2 การสร้างมาตรฐานการกระจายกุญแจรหัสลับเชิงควอนตัม (Standardization of Quantum Key Distribution)

เนื่องจากเป็นเทคโนโลยีใหม่ มีหน่วยงานที่พยายามรวมกลุ่มกันเพื่อกำหนดมาตรฐานของการสื่อสารเชิงควอนตัมให้เป็นสากล ตัวอย่างหนึ่งคือองค์กรที่ทำหน้าที่กำหนดมาตรฐานอุตสหกรรมทางด้านโทรคมนาคมแห่งสหภาพยุโรป (European Telecommunications Standards Institute: ETSI) มีการกำหนดมาตรฐานสำหรับการสื่อสารเชิงควอนตัมโดยกำหนดกลุ่มทำงานเป็น ISG-QKD (Industry Specification Group on Quantum Key Distribution) ซึ่งเป็นมาตรฐานของการกระจายกุญแจรหัสลับเชิงควอนตัมสำหรับภาคอุตสาหกรรม เริ่มมีการลงนามในสัญญาในเดือนกรกฎาคม ค.ศ. 2009 โดยในเดือนธันวาคม ค.ศ. 2009 มีจำนวนองค์กรจากประเทศต่างๆ ทั่วโลก 21 องค์กรเข้าร่วมกำหนดมาตรฐาน

2.7.3 วิทยาการรหัสลับควอนตัมที่นอกเหนือจากการกระจายกุญแจรหัสลับ

2.7.3.1 การยืนยันตัวตนเชิงควอนตัม (Quantum Authentication)

การกระจายกุญแจรหัสลับเชิงควอนตัมช่วงเริ่มต้นยังคงขึ้นอยู่กับวิธีการยืนยันตัวตนแบบดั้งเดิม (Classical authentication) ทำให้ไม่อาจเรียกกระบวนทั้งหมดว่าเป็นวิทยาการรหัสลับเชิงควอนตัมล้วนๆ ได้ จึงมีการเสนอวิธีใช้คุณสมบัติพัวพันทางควอนตัมมาช่วยในการยืนยันตัวตน โดยให้ผู้ส่งและผู้รับได้มีสถานะพัวพันร่วมกันฝั่งจะหนึ่งคิวบิต จากนั้น การยืนยันตัวตนทำโดยนำคิวบิตที่สาม (คิวบิตตัวช่วย) มาเกี่ยวข้อง (Interact) กับคิวบิตที่เป็นกุญแจยืนยันตัวตน แล้วส่งคิวบิตตัวช่วยไปยังอีกฝั่งเพื่อผ่านตัวดำเนินการและวัดสถานะบนเวกเตอร์ฐานเจาะจงชุดหนึ่ง ซึ่งได้มีการพิสูจน์ว่า นอกจากคู่ผู้ส่ง-ผู้รับที่มีคู่คิวบิตพัวพันนั้นแล้ว ก็ไม่มีผู้อื่น

ผู้ใดผ่านการทดสอบการยืนยันตัวตนดังกล่าวได้ นอกจากนั้นหากไม่มีข้อผิดพลาดกับคิวบิต คู่คิวบิตสำหรับยืนยันตัวตนดังกล่าวยังสามารถใช้ซ้ำได้ [Zeng & Guo 2000][Li & Zhang 2006] อย่างไรก็ตามวิธีการดังกล่าวตั้งอยู่บนสมมติฐานที่ผู้ส่งและผู้รับมีกุญแจร่วมกันอยู่ก่อนคือคู่สถานะพัวพัน และจำเป็นต้องมีหน่วยเก็บข้อมูลเชิงควอนตัม (Quantum memory) ในการสร้างวิธีการดังกล่าวด้วย

2.7.3.2 รหัสเวอร์แนมเชิงควอนตัม (Quantum Vernam Cipher)

จากแนวคิดการใช้งานครั้งเดียวของกิลเบิร์ต เวอร์แนม (Gilbert Vernam) นำไปสู่แนวคิดที่คู่เคียงกันคือ รหัสเวอร์แนมด้วยสถานะควอนตัม แต่แตกต่างตรงที่ในการใช้งานครั้งเดียวกุญแจต้องเป็นเลขสุ่มและใช้ได้เพียงครั้งเดียว แต่การใช้สถานะควอนตัมเป็นกุญแจสำหรับรหัสเวอร์แนมเชิงควอนตัมสามารถใช้ซ้ำได้อีก และยังช่วยตรวจสอบข้อผิดพลาดได้อีกด้วย [*Leung 2002*]

2.7.3.3 การสื่อสารความลับร่วมกันเชิงควอนตัม (Quantum Secret Sharing)[2.14]

จากความไม่ไว้ใจกันระหว่างสองบุคคล (บุคคลที่สอง และ บุคคลที่สาม) โดย บุคคลแรกจะแจกข้อความลับให้กับบุคคลที่สองและสาม โดยที่ไม่ให้คนใดคนหนึ่งในบุคคลที่สองและสามนั้นรู้ข้อความลับทั้งหมด (ต้องรู้ข้อความลับนั้นร่วมกัน) เพื่อป้องกันการไม่ซื่อสัตย์หรือหักหลัง โดยได้มีการทดลองใช้สถานะพัวพันสามคิวบิต (GHZ states) สาธิตการทำงานดังกล่าว [*Tittel และคณะ 2001*] และมีการเสนอการใช้สถานะไม่พัวพันในการสื่อสารลับร่วมกัน [*Guo & Guo 2003*] ซึ่งมีข้อดีตรงที่สามารถขยายจำนวนผู้สื่อสารได้ง่ายกว่าวิธีการใช้สถานะพัวพัน (เนื่องจากสถานะพัวพันหลายอนุภาคยังสร้างได้ยากหรือน้อย)

นอกจากข้างต้น ยังมีการออกแบบสมาร์ตการ์ดเชิงควอนตัม (Quantum smart card) และ ตู้กดเงิน (เอทีเอ็ม) เชิงควอนตัม (Quantum telling machine) [*Hruby 1998*] โดยอาศัยการเข้ารหัสด้วยเฟส และแนวคิดจากวีส์เนอร์ เบนเนตต์ และ บราสซาร์ด [*Wiesner 1983; Bennett & Brassard 1984*] เป็นต้น

2.8 การคาดการณ์เทคโนโลยีวิทยาการรหัสลับเชิงควอนตัม

มีการคาดการณ์เทคโนโลยีทางด้านการสื่อสารและการคำนวณเชิงควอนตัมว่าจะเป็นเทคโนโลยีใหม่ที่มีใช้ในเชิงธุรกิจและมีผลกระทบสำคัญในอนาคต จากหลายสำนักวิชาการและสถาบันที่สำคัญต่างๆ อาทิ

- ในปี พ.ศ. 2546 นิตยสารทางด้านเทคโนโลยีคอมพิวเตอร์ (PCMagazine) ฉบับเดือนกรกฎาคมได้คาดการณ์ว่าวิทยาการรหัสลับเชิงควอนตัมจะเป็นหนึ่งในยี่สิบเทคโนโลยีที่ควรจับตามองว่าในอนาคตจะมีการนำมาใช้งานอย่างแพร่หลาย
- ในปี พ.ศ. 2546 นิตยสาร Technology Review โดยสถาบันเทคโนโลยีแมสซาชูเซตส์ (Massachusetts Institute of Technology) ประเทศสหรัฐอเมริกา ฉบับเดือนกุมภาพันธ์ได้คาดการณ์ว่าวิทยาการรหัสลับเชิงควอนตัมจะเป็นหนึ่งในสิบเทคโนโลยีที่จะเปลี่ยนแปลงโลกที่เกี่ยวข้องกับการดำเนินชีวิตประจำวัน
- ในปี พ.ศ. 2548 นิตยสาร IEEE Spectrum จัดพิมพ์โดยสถาบันวิชาชีพวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (Institute of Electrical and Electronics Engineers: IEEE) ฉบับเดือนพฤศจิกายนได้คาดการณ์เกี่ยวกับสิบบริษัทชั้นนำที่ผลิตและจำหน่ายเทคโนโลยีแห่งอนาคตในอีกสิบปีข้างหน้า โดยหนึ่งในสิบบริษัทนั้นได้แก่ บริษัท MagiQ Technology ประเทศสหรัฐอเมริกา ที่จำหน่ายผลิตภัณฑ์เกี่ยวกับวิทยาการรหัสลับเชิงควอนตัม
- ในปี พ.ศ. 2549 RAND Corporation ซึ่งเป็นองค์กรไม่หวังผลกำไรที่นำเสนอข้อมูลที่มีความท้าทายแก่สาธารณชนทั่วโลก ได้คาดการณ์ว่าภายในปี พ.ศ. 2549 ถึงปี พ.ศ. 2563 เทคโนโลยีวิทยาการรหัสลับเชิงควอนตัมจะเป็นหนึ่งในสิบหกเทคโนโลยีที่จะมีการใช้งานในเชิงธุรกิจอย่างแพร่หลาย

[2.14] จุดมุ่งหมายของการสื่อสารความลับร่วมกัน (Secret sharing) นั้นแตกต่างจากการกระจายกุญแจเชิงควอนตัม (Quantum key distribution: QKD) ไปยังหลายบุคคที่ QKD เป็นการแจกข้อความลับเหมือนกันทุกประการไปยังบุคลคลที่สองและสาม (ต่างคนต่างรู้ข้อความลับ)

- ในปี พ.ศ. 2549 ในงาน Intelligent Nation 2015 มีการนำเสนอแผนการหลักภายใน 10 ปี ของประเทศสิงคโปร์ โดยคาดการณ์ว่าในอีก 5-10 ปีต่อจากนั้น นับจากปีที่นำเสนอ จะมีการนำผลิตภัณฑ์ของวิทยาการรหัสลับเชิงควอนตัมมาใช้ในการรักษาความปลอดภัยข้อมูลของหน่วยงานรัฐบาล และสถาบันการเงินทั่วประเทศ
- ในปี พ.ศ. 2552 Global Industry Analysts, Inc. ประเทศสหรัฐอเมริกา ได้ตีพิมพ์ผลการวิจัยตลาด โดยได้คาดการณ์ว่าในปี พ.ศ. 2558 มูลค่าการตลาดของวิทยาการรหัสลับเชิงควอนตัมทั่วโลกจะมีค่าประมาณ 842 ล้านเหรียญสหรัฐ

จากการคาดการณ์เกี่ยวกับเทคโนโลยีวิทยาการรหัสลับเชิงควอนตัมของสถาบันต่างๆ ข้างต้นแสดงให้เห็นถึงความสำคัญของเทคโนโลยีดังกล่าว โดยที่หลายประเทศกำลังพยายามผลักดันให้เป็นโครงการในระดับชาติ เนื่องจากเล็งเห็นถึงผลกระทบของการนำเทคโนโลยีนี้มาใช้งานจริง และยังเป็นการเตรียมความพร้อมสำหรับเทคโนโลยีที่จะก่อตัวขึ้นในอนาคต โดยการกำหนดอยู่ในแผนพัฒนาหรือแผนที่นำทางด้านสารสนเทศของตนเอง

บทสรุป

ในช่วงเวลาที่ผ่านมามากกว่า 30 ปี (ตั้งแต่ ค.ศ. 1984 จนถึงปี ค.ศ. 2010) ได้มีการนำเสนอถึงการนำพฤติกรรมเชิงควอนตัมมาประยุกต์สำหรับการรักษาความปลอดภัยของข้อมูลข่าวสาร ซึ่งวิธีการหนึ่งที่ได้รับความสนใจและเริ่มมีการใช้งานจริงคือ วิทยาการรหัสลับเชิงควอนตัม ซึ่งมีความปลอดภัยกว่าระบบวิทยาการรหัสลับแบบดั้งเดิมเนื่องจากสามารถล่วงรู้ถึงการถูกดักจับรหัสลับได้อย่างแท้จริง โดยมีเกณฑ์วิธีที่นิยมใช้คือ (1) เกณฑ์วิธีที่ใช้สถานะควอนตัมไม่ต่อเนื่อง ประกอบด้วย เกณฑ์วิธี BB84 ที่อาศัยสถานะควอนตัมสี่สถานะในการสื่อสาร เกณฑ์วิธี B92 ที่อาศัยสถานะควอนตัมสองสถานะในการสื่อสาร เกณฑ์วิธีหกสถานะที่อาศัยสถานะควอนตัมหกสถานะ เกณฑ์วิธี SARG04 ที่ปรับปรุงเกณฑ์วิธี BB84 ให้เหมาะสมกับการใช้งานมากขึ้น เกณฑ์วิธี Ekert91 ที่อาศัยคุณสมบัติความพัวพันเชิงควอนตัมโดยตรวจหาการดักจับด้วยอสมการของเบลล์ เกณฑ์วิธี BBM92 ที่อาศัยคุณสมบัติความพัวพันเชิงควอนตัมแต่ไม่ใช้การตรวจหาการดักจับด้วยอสมการของเบลล์ (2) เกณฑ์วิธีที่ใช้สถานะควอนตัมแบบต่อเนื่อง นอกจากงานวิจัยพื้นฐานแล้วผลิตภัณฑ์ทางด้านการกระจายกุญแจรหัสลับเชิงควอนตัมได้เริ่มมีจำหน่ายเชิงพาณิชย์แล้วโดยบริษัท ID Quantique ประเทศสวิตเซอร์แลนด์ และบริษัท MagiQ Technologies ประเทศสหรัฐอเมริกา อีกทั้งมีบริษัทที่กำลังพัฒนาต้นแบบที่ใกล้เคียงกับการใช้งานจริงประกอบด้วยบริษัทโตชิบา ซึ่งมีศูนย์วิจัยที่สหราชอาณาจักร บริษัท Nippon Telegraph and Telephone ประเทศญี่ปุ่น บริษัท QuintessenceLabs ประเทศออสเตรเลีย และเริ่มมีบริษัทอื่นๆ ที่ผันตัวออกมาจากหน่วยปฏิบัติการภายในมหาวิทยาลัยเพิ่มมากขึ้นทั้งด้านฮาร์ดแวร์และซอฟท์แวร์ที่เกี่ยวข้อง

เอกสารอ้างอิง

[Acin และคณะ 2007] A. Acin, et al. "Device-Independent Security of Quantum Cryptography against Collective Attacks," *Phys. Rev. Lett.,* vol. 98, p. 230501, 2007.

[Brassard 2006] G. Brassard, "Brief History of Quantum Cryptography: A Personal Perspective," in *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security, Awaji Island, Japan,* October 2005. [Online]. Available: http://arxiv.org/abs/quant-ph/0604072. [Accessed: Dec. 2009].

[Bennett & Brassard 1984] C. H. Bennett, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India*, pp. 175-179, 1998.

[Bennett และคณะ 92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol.5, pp. 3-28, 1992.

[Bennett 1992] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.,* vol.68, pp. 3121 - 3124, 1992.

[Bennett, Brassard & Mermin 1992] C. H. Bennett, G, Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.,* vol. 68, pp. 557-559, 1992.

[Bernstein & Lieberman 1989] G. M. Bernstein, and M. A. Lieberman, "Secure random number generation using chaotic circuits," in *Military Communications Conference, 1989.* MILCOM'89. Conference Record. vol.3 pp. 640-644, 1989.

[Blakesley และคณะ 2005] J. C. Blakesley, et al. "Efficient Single Photon Detection by Quantum Dot Resonant Tunneling Diodes," *Phys. Rev. Lett.,* vol 94, p. 067401, 2005.

[Bruss และคณะ 2006] D. Bruss, et al. "Quantum Cryptography: A Survey," *Electronic Colloquium on Computational Complexity*, Revision 2 of Report No.146, 2005.

[Bruss 1998] D. Bruss, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.,*vol. 81, pp. 3018–3021, 1998.

[Chapuran และคณะ 2009] T. E. Chapuran, et al. "Optical networking for quantum key distribution and quantum communications," *New J. Phys.,* vol. 11, p. 105001, 2009.

[Cover & Thomas 1991] T. M. Cover, and J. A. Thomas, *Elements of information theory,* 1st Edition, New York: Wiley-Interscience, 1991.

[Diffie & Hellman 1976] W. Diffie, and M. Hellman, "New directions in cryptography," *IEEE Transactions on information Theory*, 1976.

[Dixon และคณะ 2008] A. R. Dixon, et al. "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Opt. Express,* vol. 16, p. 18790, 2008.

[Dixon และคณะ 2009] A. R. Dixon, et al. "Ultrashort dead time of photon-counting InGaAs avalanche photodiodes," *Appl. Phys. Lett.,* vol.94, p. 231113, 2009.

[Dusek และคณะ 2006] M. Dusek, N. Lutkenhaus, and M. Hendrych, "Quantum Cryptography," *Progress in Optics,* vol. 49,

Wolf, E. (Ed.), 2006.

[Dynes และคณะ 2009] J. F. Dynes, et al. “Efficient entanglement distribution over 200 kilometers,” *Opt. Express,* vol. 17, pp. 11440-11449, 2009.

[ElGamal 1985] T. ElGamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” *IEEE Transactions on Information Theory,* vol. IT-31, n. 4, pp. 469–472, 1985. หรือ *CRYPTO 84*, pp. 10-18, Springer-Verlag.

[Garcia-Patron & Cerf 2009] R. Garcia-Patron, and N. J. Cerf, “Unconditional optimality of Gaussian attacks against continuous-variable QKD,” *Phys. Rev. Lett.,* vol. 97, p. 190503, 2006.

[Gerlach & Stern 1922] W. Gerlach, and O. Stern, “Der experimentelle nachweis der richtungsquantelung in magnetfeld,” *Zeitschrift fur Physik, vol.9, p. 349-352*

[Gilbert & Hamrick 2000] G. Gilbert, and M. Hamrick, “Practical Quantum Cryptography: A Comprehensive Analysis (Part One),” *arXiv.org e-Print archive*, 2000. [Online]. Available: http://arxiv.org/abs/quant-ph/0009027. [Accessed: Dec. 2009].

[Gisin และคณะ 2002] N. Gisin, G. Ribordy, W. Tittel, H. and Zbinden, “Quantum Cryptography,” *Rev. Mod. Phys.,* vol. 74, p. 145, 2002.

[Gobby และคณะ 2004] C. Gobby, Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber,” *Appl. Phys. Lett.,* vol. 84, p. 3762, 2004.

[Guo & Guo 2003] G. P. Guo, and G. C. Guo, “Quantum secret sharing without entanglement,” *Physics Letters A,* vol. 310, pp. 247-251, 2003.

[Hao และคณะ 2009] L. Hao, et al. “Characteristics of focused ion beam nanoscale Josephson devices,” *Supercond. Sci. Technol.,* vol. 22, p. 064011, 2009.

[Hruby 1998] J. Hruby, “Trends in Quantum Cryptography in Czech Republic,” *Lecture Notes in Computer Science*, vol. 1438, pp. 261-272, 1998.

[Honjo และคณะ 2008] T. Honjo, et al. “Long-distance entanglement-based quantum key distribution over optical fiber,” *Opt. Express,* vol.16, pp. 19118-19126, 2008.

[Hughes และคณะ 2000] R. J. Hughes, et al. “Free-space quantum key distribution in daylight,” *J. Mod. Opt.,* vol.47, No. 2/3, pp. 549-562, 2000.

[IdQ.NET] *ID Quantique SA.* [Online]. Available: http://www.idquantique.com. [Accessed: Dec. 2009].

[Jacobs & Franson 1996] B. C. Jacobs, J. D. and Franson, “Quantum cryptography in free space,” *Optics Letters,* vol.21, No.22, 1996.

[Leung 2002] D. Leung, “Quantum Vernam Cipher,” *Quantum Information and Computation,* vol. 2, No.1 pp. 14-34, 2002.

[Li & Zhang 2006] X. Li, and D. Zhang, “A quantum authentication protocol using entangled states as authentication key,” *WSEAS Transactions on Computers,* vol. 5, no. 5, pp. 830-835. May 2006.

[Mikhailova & Andreev 2006] M. P. Mikhailova, and I. A. Andreev, “High-speed Avalanche Photodiodes for the 2–5 μm Spectral Range,” in *Mid-infrared Semiconductor Optoelectronics, Springer series in optical sciences,* pp. 547-592, 2006.

[Ma และคณะ 2007] X. Ma, C-H. F. Fung, and H. K. Lo, "Quantum key distribution with entangled photon sources," *Phys. Rev. A,* vol.76, No. 012307, 2007.

[MagiQ.NET] *MagiQ Technologies, Inc.* [Online]. Available: http://www.magiqtech.com. [Accessed: Dec. 2009].

[Maurer 1993] U. Maurer, "Secret Key Agreement by Public Discussion from Common Information," *IEEE Transactions on Information Theory*, vol. 39, pp. 733-742, 1993.

[Miller 1986] V. S. Miller, "Uses of Elliptic Curve in Cryptography," in *Williams, H. C. (Ed.) Advances in Cryptology – CRYPTO '85*, LNCS 218, pp. 417-426, Springer-Verlag Berlin Heidelberg, 1986.

[Muller และคณะ 1997] A. Muller, et al. "''Plug and play'' systems for quantum cryptography," *Appl. Phys. Lett.,* vol. 70 , pp. 793-795, 1997.

[Nielsen & Chuang 2000] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information,* Cambridge University Press, 2000

[NTT.NET] *NTT Basic Research Laboratories.* [Online]. Available: http://www.brl.ntt.co.jp/E. [Accessed: Dec. 2009].

[Peev และคณะ 2009] M. Peev, et al. "The SECOQC quantum key distribution network in Vienna," *N. J. Phys.,* vol. 11, No.075001, 2009.

[Petries และคณะ 2000] C. S. Petries, and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Cir. Sys.,* vol.47, No.5, pp. 615-621, 2000.

[Quintessence.NET] *QuintessenceLabs Pty. Ltd.* [Online]. Available: http://www.quintessencelabs.com. [Accessed: Dec. 2009].

[Ralph 2000] T. C. Ralph, "Security of continuous-variable quantum cryptography," *Phys. Rev. A,* vol. 62, p. 062306, 2000.

[Renner, Gisin & Kraus 2005] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A,* vol. 72, p. 012332, 2005.

[Rivest, Shamir & Adleman 1976] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems," *Communication of the ACM*, pp. 120-126, 1978.

[Sasaki และคณะ 2009] M. Sasaki, et al "Updating Quantum Cryptography version 1.0," *arXiv.org e-Print archive*, 2009. [Online]. Available: http://arxiv.org/abs/0905.4325/. [Accessed: Dec. 2009].

[Scheidl และคณะ 2009] T. Scheidl, et al. "Feasibility of 300km quantum key distribution with entangled states," *New Journal of Physics,* vol. 11, p. 085002, 2009.

[Scarani และคณะ 2004] V. Scarani, et al. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Phys. Rev. Lett*., vol. 92, p. 057901, 2004.

[Scarani และคณะ 2009] V. Scarani, et. al. "The Security of Practical Quantum Key Distribution," *Rev. Mod. Phys*., vol.81, pp. 1301-1350, 2009.

[Shannon 1949] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28(4), pp. 657–715, 1949.

[Shor 1994] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pp. 124-134, 1994.

[Shor & Preskill 2000] P. W. Shor, and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.,* vol.85, pp. 441-444, 2000.

[Shield 2007] A. Shields, "Semiconductor quantum light sources," *Nature Photonics,* vol. 1, pp. 215 – 223, 2007.

[Stebila และคณะ 2009] D. Stebila, M. Mosca, and N Lutkenhaus, "The Case for Quantum Key Distribution," *arXiv.org e-Print archive*, 2009. [Online]. Available: http://arxiv.org/abs/0902.2839. [Accessed: Dec. 2009].

[Stefanov และคณะ 1999] A. Stefanov, et al. "Optical Quantum Random Number Generator," *arXiv.org e-Print archive*, 1999. [Online]. Available: http://arxiv.org/abs/quant-ph/9907006. [Accessed: Dec. 2009].

[Stinton 1994] D. R. Stinton, "Universal Hashing and Authentication Codes," *Designs, Codes and Cryptography,* vol. 4, pp. 369-380, 1994.

[Tittel และคณะ 2001] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing," *Phys. Rev. A,* vol. 63, p. 042301, 2001.

[Swissquantum.NET] *Swissquantum.* [Online]. Available: http://www.swissquantum.com. [Accessed: Dec. 2009].

[Ursin และคณะ 2007] R. Ursin, et al. "Free-Space distribution of entanglement and single photons over 144 km," *Nature Physics,* vol. 3, pp. 481 – 486, 2007.

[Ursin และคณะ 2008] R. Ursin, et al. "Space-QUEST: Experiments with quantum entanglement in space," in *IAC Proceedings* A2.1.3, 2008.

[Weedbrook และคณะ 2004] C. Weedbrook, et al. "Quantum Cryptography without Switching," *Phys. Rev. Lett.,* vol 93, p. 170504, 2004.

[Wiesner 1983] S. Wiesner, "Conjugate Coding," *ACM SIGACT News.,* vol. 15, no. 1, pp. 78-88. Winter-Spring, 1983.

[Wootters & Zurek 1982] W. K. Wootters, and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802-803, 1982.

[Xu และคณะ 2008] X. Xu, et al. "Plug and Play single photons at 1.3 μm approaching gigahertz operation," *Appl. Phys. Lett.,* vol. 93, p. 021124, 2008.

[Yuan และคณะ 2009] Z. L. Yuan, t. al. "Practical gigahertz quantum key distribution based on avalanche photodiodes," *N. J. Phys.*, vol. 11, p. 045019, 2009.

[Zeng & Guo 2000] G. Zeng, and G. Guo, "Quantum authentication protocol," *arXiv.org e-Print archive*, 2000. [Online]. Available: http://arxiv.org/abs/quant-ph/0001046. [Accessed: Dec. 2009].

[Zhang และคณะ 2009] Q. Zhang, et al. "Megabits secure key rate quantum key distribution," *New J. Phys.,* vol. 11, 045010, 2009.

[Zhao และคณะ 2003] Z. Zhao, T. Yang, Y. A. Chen, A. N. Zhang, and J. W. Pan, "Experimental realization of entanglement concentration and a quantum repeater," *Phys. Rev. Lett.*, vol. 90, no. 20, p. 207901, 2003.

ฉ้าถามท้ายบทที่ 2 (Questions and Answers)

และอภิปราย (Discussions) ปรับปรุง ณ

Blog: http://www.stks.or.th/blog/?p=14123

บทที่ 3
การสื่อสารเชิงควอนตัมพื้นฐาน
(Principle of quantum communications)

อภิธานศัพท์ (Glossary)

- **การคอมมิทบิต (Bit commitment)**
  กระบวนการสื่อสาร ที่ผู้ส่งเลือกข้อความหนึ่งบิต แล้วส่งผลจากการเลือกนั้นไปยังผู้รับโดยผู้รับไม่สามารถเปิดดูข้อความที่ผู้ส่งเลือก (Commit) จนกว่าจะได้รับอนุญาตจากผู้ส่ง และผู้ส่งไม่สามารถเปลี่ยนแปลงข้อความที่ 'เลือกแล้ว' ได้
- **การคอมมิทบิตเชิงควอนตัม (quantum bit commitment)**
  การคอมมิทบิตโดยใช้สถานะควอนตัม ซึ่งเชื่อว่าสามารถกระทำได้ แต่ปี ค.ศ. 1997-1998 โดมินิก ไมเยอร์ (D. Mayers) โล (Lo) และ เชาว์ (Chao) พิสูจน์ว่า การคอมมิทบิตเชิงควอนตัมอย่างสมบูรณ์ไม่สามารถกระทำได้
- **การวัดสถานะแบบเบลล์ (Bell-state measurement)**
  กระบวนการวัดสถานะควอนตัมเพื่อแยกแยะว่าสถานะที่เข้ามาเป็นสถานะเบลล์แบบใดในสี่รูปแบบ
- **การสูญเสียความอาพันธ์เชิงควอนตัม (Quantum decoherence)**
  การสูญเสียข้อมูลและคุณสมบัติเชิงควอนตัมจากผลกระทบของสิ่งแวดล้อม (เกิดความพัวพันกับสิ่งแวดล้อมยิ่งๆ ขึ้น เมื่อเวลาผ่านไป) ทำให้ข้อมูลเชิงควอนตัมเปลี่ยนคุณลักษณะไปเป็นข้อมูลดั้งเดิม หรือการสูญเสียข้อมูล*เฟสสัมพัทธ์*ระหว่างสองสถานะย่อยที่ทับซ้อนเชิงตำแหน่ง
- **ความตั้งฉาก (Orthogonality)**
  (1) สองเวกเตอร์ ตั้งฉากกันก็ต่อเมื่อผลคูณจุดหรือผลคูณภายในระหว่างเวกเตอร์ทั้งสอง มีค่าเป็นศูนย์
  (2) สถานะควอนตัมที่อธิบายด้วยเวกเตอร์ตั้งฉาก เป็นสถานะซึ่งแบ่งแยกได้อย่างชัดเจนด้วยการวัดสถานะ
- **การทับซ้อนเชิงตำแหน่ง (Superposition)**
  คุณสมบัติของระบบควอนตัมที่สามารถมีค่าประกอบด้วยสองสถานะขึ้นไปในเวลาเดียวกัน โดยคุณสมบัติดังกล่าวจะยุบตัวลงเหลือเพียงสถานะเดียวเมื่อมีการวัดค่าเกิดขึ้นกับระบบนั้น
- **ความเป็นท้องถิ่น (Locality)**
  ความเป็นอิสระของสองสิ่งที่อยู่ห่างไกลกัน การกระทำใดๆ ต่อสิ่งหนึ่งไม่สามารถมีผลต่ออีกสิ่งหนึ่งอย่างทันทีทันใดได้ เช่น การทอดลูกเต๋าในกรุงเทพมหานคร ไม่มีผลต่อผลลัพธ์การทอดลูกเต๋าในเวลาเดียวกันที่นครเวียงจันทน์ กล่าวโดยหลักสถิติคือตัวแปรสุ่มที่เกิดจากการวัดระบบทางกายภาพสองระบบที่อยู่ห่างไกลกัน ณ เวลาเดียวกัน ต้องมีความเป็นอิสระต่อกัน
- **ความพัวพัน (Entanglement)**
  คุณสมบัติทางกลศาสตร์ควอนตัม ซึ่งอนุญาตให้วัตถุ (อนุภาค) ซึ่งอยู่ห่างไกลกัน สามารถมีสถานะร่วมกันได้ เรียกว่า *สถานะพัวพัน* โดยแต่ละอนุภาคที่มีความพัวพันกัน สถิติการวัด *ไม่เป็นอิสระต่อกัน*ถึงแม้อนุภาคจะอยู่ห่างไกลและถูกวัดในขณะเวลาเดียวกัน
- **ความมีอยู่จริงของสถานะ (Realism)**
  ความเชื่อว่าสถานะของสิ่งในธรรมชาติ มีอยู่จริงโดยเป็นอิสระจากการสังเกต (การวัดสถานะไม่มีผลต่อระบบ) เป็นความเชื่อของอัลเบิร์ต ไอน์สไตน์ (Albert Einstein) และนักฟิสิกส์ส่วนใหญ่ช่วงก่อนศริสต์ศตวรรษที่ 20
- **ความไม่เป็นท้องถิ่น (Nonlocality)**
  ความไม่เป็นอิสระเชิงสถิติ เมื่อวัดสถานะของสองสิ่งที่อยู่ห่างไกล ณ เวลาเดียวกัน เป็นคำอธิบายอย่างหนึ่งของคุณสมบัติพัวพัน

- **ความอาพันธ์ (Coherence)**
  (1) คุณสมบัติของคลื่นที่มีความถี่และเฟสที่แน่นอน คลื่นอาพันธ์จากสองแหล่งกำเนิดจะแทรกสอดกันแล้วเกิดริ้วแทรกสอดชัดเจนและคงที่ เช่น แสงเลเซอร์จัดเป็นคลื่นที่มีความอาพันธ์
  (2) ในกลศาสตร์ควอนตัมหมายถึง คุณสมบัติที่สถานะควอนตัมยังคงค่า*เฟส-สัมพัทธ์*ที่แน่นอนไว้ได้
- **ค่าต่อเนื่อง (Continuous)**
  ค่าที่เป็นจำนวนจริง มีค่าแบ่งย่อยไปเท่าไรก็ได้และไม่สามารถนับได้ หรือหมายถึงโครงสร้างเชิงคณิตศาสตร์แบบอื่นที่แทนได้ด้วยจำนวนจริง
- **ค่าไม่ต่อเนื่อง (Discrete)**
  ค่าที่เป็นจำนวนเต็ม โดยทั่วไปหมายถึง จำนวนเต็มบวกหรือศูนย์ 0, 1, 2, 3, … ซึ่งเป็นค่าที่นับได้
- **คิวบิต (Qubit)**
  หน่วยพื้นฐานสำหรับการคำนวณและการสื่อสารเชิงควอนตัม 1 คิวบิต มีค่าเป็นผลรวมเชิงเส้นของสถานะ “0” และ “1” ในเชิงเรขาคณิตสังเกตเป็นเวกเตอร์หนึ่งหน่วยบนผิวทรงกลม
- **บิต (Bit)**
  หน่วยพื้นฐานสำหรับการคำนวณและการสื่อสารแบบดิจิทัล หนึ่งบิตมีได้สองค่าคือ “0” หรือ “1” เท่านั้น
- **เกตลอจิกเชิงควอนตัม (Quantum logic gate)**
  รูปแบบควอนตัมของลอจิกเกตเชิงดิจิทัล เกตลอจิกเชิงควอนตัมจะมีคุณสมบัติย้อนกลับได้ และสามารถประมวลผลสถานะควอนตัมที่มีคุณสมบัติการทับซ้อนเชิงตำแหน่งได้
- **เฟสสัมพัทธ์ (Relative phase)**
  สำหรับสถานะคิวบิต $a|0\rangle + e^{i\beta}b|1\rangle$ ค่า $e^{i\beta}$ เรียกว่า เฟสสัมพัทธ์ระหว่างสองสถานะ $|0\rangle$ และ $|1\rangle$ ซึ่งมีผลเชิงกายภาพหรือผลเชิงสถิติในการวัดสถานะ
- **เฟสองค์รวม (Global phase)**
  สำหรับคิวบิต $e^{i\alpha}|\psi\rangle$ เทอม $e^{i\alpha}$ เรียกว่า เฟสองค์รวม ซึ่งไม่มีผลเชิงกายภาพ เนื่องจากสถานะควอนตัมแทนด้วย 'รังสี' (“ray”) ซึ่งหมายถึงเวกเตอร์ที่มีแอมพลิจูดเป็นเท่าใดก็ได้
- **โฟตอน (Photon)**
  หน่วยที่เล็กที่สุดของแสงมีค่าพลังงานเท่ากับค่าคงที่ของพลังค์ (Planck's constant) คูณความถี่ของคลื่นแสงนั้น
- **เวกเตอร์จำนวนเชิงซ้อน (Complex vector)**
  เวกเตอร์ที่มีค่าสมาชิกในแต่ละมิติเป็นจำนวนเชิงซ้อน เขียนแทนด้วย ($C1$, $C2$, $C3$, ..., Cn) สำหรับเวกเตอร์เชิงซ้อน n มิติ โดยที่ C หมายถึงจำนวนเชิงซ้อน
- **สถานะเชิงการคำนวณ (Computational basis states)**
  สถานะควอนตัมที่แทนชื่อสถานะด้วยเลขดิจิทัล (“0”, “1”, “2”, ... หรือ “00”, “01”, “10”, “11”, ...)
- **สถานะทางกายภาพ (Physical states)**
  รูปแบบเชิงกายภาพที่แทนสถานะเชิงการคำนวณ เช่น ให้โฟตอนที่มีโพลาไรเซชัน “แนวตั้ง” แทนสถานะ “0” และ “แนวนอน” แทนสถานะ “1”
- **สถานะเบลล์ (Bell States)**
  สถานะควอนตัมของสองคิวบิต ที่มีความพัวพันสูงสุดและมีความตั้งฉากระหว่างกัน สถานะเบลล์มีสี่รูปแบบได้แก่ $(|00\rangle \pm |11\rangle)/\sqrt{2}$ และ $(|10\rangle \pm |01\rangle)/\sqrt{2}$
- **หน่วยย้ำสัญญาณเชิงควอนตัม (Quantum repeater)**
  การกระทำต่อสถานะควอนตัมอย่างใดก็ตามที่ช่วยให้ส่งสถานะควอนตัมที่ต้องการไปได้ในระยะทางไกลขึ้น โดยอาจส่งข้อมูลควอนตัมผ่านต่อไปยังอนุภาคอื่นเสมือนเป็นหน่วยทวนสัญญาณ

ข้อสรุปประจำบท (Summary)

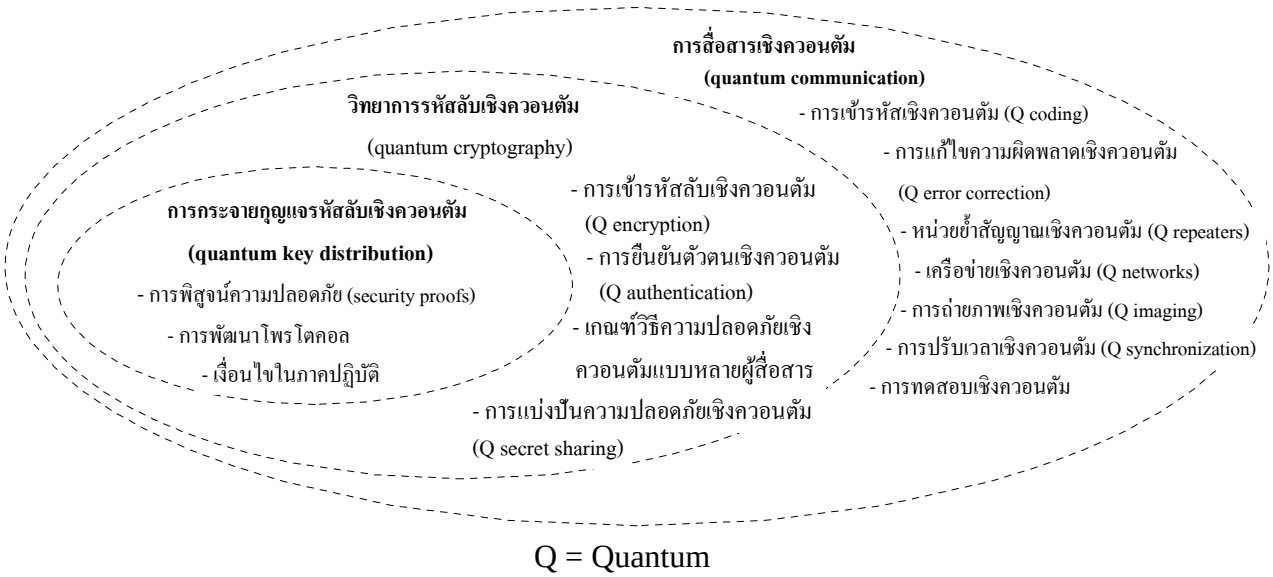
Quantum communications enabled many communication schemes those are not available in any classical (digital & analog) communication techniques. The nonlocal correlation between two distant quantum systems or “entanglement” can be used as a fruitful resource for quantum communications. First, already mentioned in quantum cryptography, entangled photons

can be used to generate secret random information to be used as secret key for encryption. Second, entanglement can be employed to reliably send exact quantum information through classical channel or without sending the particle carrying the information. The quantum information appears at the destination by reconstruction of states (one of the entangled pair) according to the received classical message and, at the same time, being destroyed at the sender. The communication scheme is called “quantum teleportation” and has been experimentally demonstrated since 1997. Third, provided entangled pair are distributed, one of two parties can digitally 'modulate' the received entangled particle and send it to the receiver holding another part of entangled-pair who can recover the two-bit message tried to send. This gives availability of sending two bits of information in single quantum bit -- “superdense coding” which has been demonstrated since 1996 in Innsbruck, Austria. Moreover, teleporting one of entangled pair result in “entanglement swapping” or creation of entanglement between two particles that never interacts. This gives a beautiful solution to implementation of long-distance quantum communications. To give one example, quantum key distribution can be done in multiple larger distance using this technique. The trade-offs between practical value and perfection of quantum communication scheme have been worldwide under investigation. It is believed that the next generation of 'quantum' communication could be resulted from viewing “entanglement” as an “information resource”.

3.1 ภาพรวม

จากการสื่อสารแบบดั้งเดิมที่อาจเป็นค่าต่อเนื่อง หรือค่าดิจิทัล (ไม่ต่อเนื่อง) จากต้นทางไปยังปลายทางด้วยวิธีการต่างๆ มาจนถึงการสื่อสารเชิงควอนตัม ที่ครอบคลุมการส่งสถานะควอนตัมจากต้นทางไปยังปลายทางโดยสถานะควอนตัมนั้นอาจแทนด้วยสารสนเทศควอนตัม หรือสารสนเทศดั้งเดิมแบบดิจิทัลดังกล่าวก็ได้ (ใช้สถานะตั้งฉากสองสถานะแทน “0” และ “1”) การสื่อสารเชิงควอนตัมนี้ มีคุณลักษณะบางอย่างที่ไม่มีในการสื่อสารแบบดั้งเดิมเพราะอาศัยสมบัติทางกลศาสตร์ควอนตัม เช่นความพัวพันและการวัดซึ่งทำให้สถานะยุบตัว (Collapse) สู่ค่าผลลัพธ์ที่วัดได้ คุณสมบัติเหล่านี้ทำให้เกิดการสื่อสารรูปแบบใหม่ เช่น การเทเลพอร์ทเชิงควอนตัม (Quantum teleportation) ซึ่งเป็นการส่งสถานะควอนตัมด้วยการส่งข้อความเพียงสองบิตและอาศัยความพัวพันที่มีอยู่ก่อน ส่วนการวัดค่าที่ทำให้สถานะยุบตัวหรือการที่สถานะไม่ตั้งฉากสองสถานะอันไม่สามารถแยกแยะจากกันได้ถูกนำมาประยุกต์ในการสื่อสารด้วยความปลอดภัยที่อาศัยสถานะควอนตัมนั้นมาช่วยในการกระจายกุญแจรหัสลับระหว่างคู่สื่อสารโดยการดักจับใดๆ ต่อสถานะไม่ตั้งฉากดังกล่าวจะทำให้ผู้ส่งและผู้รับทั้งคู่รู้ได้ถึงการดักนั้น นอกจากนี้คุณสมบัติพัวพันสามารถนำมาใช้ส่งข้อความดิจิทัล ด้วยการส่งสถานะควอนตัมเป็นปริมาณครึ่งหนึ่งของข้อมูลดิจิทัลได้ (ส่งหนึ่งคิวบิต แทนการส่งข้อความดิจิทัลสองบิต) เกิดเป็นการเข้ารหัสความหนาแน่นสูงเชิงควอนตัม (Superdense coding) ดังรูปที่ 3.1

การสื่อสารเชิงควอนตัมแขนงที่ใกล้เคียงกับการประยุกต์ในชีวิตประจำวัน คือ วิทยาการรหัสลับเชิงควอนตัมของบทก่อนหน้าซึ่งหากผสมผสานกับการสื่อสารเชิงควอนตัมรูปแบบอื่นด้วย จะช่วยเพิ่มระยะทางได้ (เช่น ใช้คุณสมบัติพัวพันหลายคู่ช่วยในการสร้างหน่วยทวนสัญญาณเชิงควอนตัม และการกระจายกุญแจรหัสลับเชิงควอนตัมผ่านดาวเทียม หรือระหว่างหลายคู่สื่อสาร) และเพิ่มมิติใหม่สำหรับการสื่อสารที่วิทยาศาสตร์บริสุทธิ์และประยุกต์มีการผสมผสานกัน การสื่อสารเชิงควอนตัมนี้เป็นสาขาวิชาที่กว้างครอบคลุมกระบวนการและการประยุกต์ด้านความซับซ้อนของการสื่อสารเชิงควอนตัม (Quantum communication complexity) [*Brassard 2003*] การคอมมิทบิตเชิงควอนตัม (Quantum bit commitment) และการกระจายกุญแจรหัสลับเชิงควอนตัมดังกล่าว ในส่วนนี้จะขยายมาครอบคลุมการเทเลพอร์ทเชิงควอนตัม การเข้ารหัสความหนาแน่นสูงเชิงควอนตัม และการควบคุมความผิดพลาดเชิงควอนตัมเป็นเบื้องต้นเพื่อความเข้าใจการสื่อสารควอนตัมในรูปแบบอื่นๆ ที่นอกเหนือจากวิทยาการรหัสลับ



รูปที่ 3.1 ภาพรวมของการสื่อสารเชิงควอนตัม ดัดแปลงจากการนำเสนอของริชาร์ด ฮิวช์ (Richard Hughes) ในงาน "Workshop on Quantum Information Science" กรุงเวียนนา ประเทศออสเตรีย 23-25 เมษายน ค.ศ. 2009 [*Hughes 2009*]

การสื่อสารเชิงควอนตัม โดยหลักการสามารถใช้สถานะของอนุภาคใดๆ ซึ่งประพฤติตัวตามหลักกลศาสตร์ควอนตัม เช่น สถานะของอิเล็กตรอน โปรตอน นิวตรอน หรือ โฟตอน (แสง) แต่ตัวเลือกที่เป็นธรรมชาติและใช้อยู่เป็นปกติสำหรับการสื่อสารเชิงควอนตัมคือ สถานะของแสง เนื่องจากโฟตอนถูกรบกวนจากสิ่งแวดล้อมตามเส้นทางน้อยกว่าอนุภาคอื่น ๆ และเป็นอนุภาคที่เคลื่อนที่เร็วสูง การแบ่งชนิดการสื่อสารเชิงควอนตัมแบ่งตามการประยุกต์ใช้โฟตอนในจำนวนต่างกัน ได้แก่ [*Gisin & Thew 2007*]

1) โฟตอนเดี่ยว: ผู้ส่งแทนสถานะของแสงตามข้อความที่ต้องการจากนั้นส่งไปยังผู้รับ เช่น การกระจายกุญแจรหัสลับเชิงควอนตัม
2) โฟตอน 2 โฟตอน: ใช้คุณสมบัติพัวพัน เพื่อเตรียมสถานะที่ต้องการร่วมกัน ณ ระยะไกล หรือใช้คุณสมบัติพัวพันเพื่อส่งข้อความดิจิทัล ด้วยการสื่อสารจำนวนน้อยครั้ง
3) โฟตอน 3 โฟตอน: การเทเลพอร์ทสถานะควอนตัมโดยไม่ต้องส่งอนุภาคเจ้าของสถานะนั้นไป หรือการประยุกต์อื่นๆ เช่น การสื่อสารความลับร่วมกันเชิงควอนตัม หรือ การกระจายกุญแจรหัสลับร่วมกันหลายผู้สื่อสาร (Multi party quantum key distribution)
4) โฟตอน 4 โฟตอน: สร้างความพัวพันให้เกิดขึ้นระหว่างคู่อนุภาคที่ไม่เคยมีอันตรกิริยากันมาก่อน (Entanglement swapping) และการประยุกต์เพื่อสร้างหน่วยย้ำสัญญาณเชิงควอนตัมในลักษณะดังกล่าว

3.2 มุมมองความพัวพันในฐานะของทรัพยากรข่าวสาร

คุณสมบัติพัวพัน (quantum entanglement) หรือ ความไม่เป็นอิสระเชิงสถิติระหว่างสถานะของสองอนุภาคที่มีระยะห่างไกลเพียงใดก็ตาม นำมาประยุกต์ให้เกิดสิ่งแปลกใหม่ในการสื่อสารซึ่งไม่มีในการสื่อสารแบบดั้งเดิม (ทั้งแอนะลอก และดิจิทัล) นั่นคือ การส่งสถานะหนึ่งคิวบิตด้วยการส่งข้อมูลดิจิทัลสองบิต (การเทเลพอร์ตเชิงควอนตัม) และการส่งข้อมูลดิจิทัลสองบิตด้วยการส่งสถานะควอนตัมคิวบิตเดียว (การเข้ารหัสความหนาแน่นสูงเชิงควอนตัม) การศึกษาเรื่องนี้จะทำให้เห็นภาพว่าเหตุใดนักวิจัยด้านสารสนเทศควอนตัมจึงกล่าวว่า "ความพัวพันเป็นทรัพยากรข่าวสาร" (Entanglement as information resource) [*Nielsen & Chuang 2000*]

รูปที่ 3.2 ผู้ร่วมค้นพบหลักการเทเลพอร์ทเชิงควอนตัม *แถวบน* (ซ้ายไปขวา) ริชาร์ด จอสซา (Richard Jozsa) วิลเลียม วูทเทอร์ส (William K. Wootters) ชาร์ลส์ เบนเนตต์ (Charles H. Bennett) *แถวล่าง* (ซ้ายไปขวา) จิลส์ บราสซาร์ด (Gilles Brassard) โคลด เครโป (Claude Crépeau) และอาเชอร์ เปเรส (Asher Peres)

(ภาพจาก www.cs.mcgill.ca)

3.3 การเทเลพอร์ทหรือการส่งถ่ายเชิงควอนตัม

ปี ค.ศ. 1993 นักวิทยาศาสตร์หกคนดังรูปที่ 3.2 ร่วมกันค้นพบกระบวนวิธีการสื่อสารแบบใหม่ คือการส่งสถานะควอนตัมโดยไม่ต้องส่งอนุภาค (สิ่งที่แทนสถานะควอนตัมนั้น) หากแต่ส่งข้อความดิจิทัลแทน และเมื่อเสร็จสิ้นกระบวนการสถานะควอนตัมจะปรากฏที่ปลายทางอย่างสมบูรณ์ และสถานะของอนุภาคเดิมที่ต้นทางก็เสียสภาพไป เรียกกระบวนการดังกล่าวว่า “การเทเลพอร์ตเชิงควอนตัม” (Quantum teleportation) [*Bennett และคณะ 1993*]

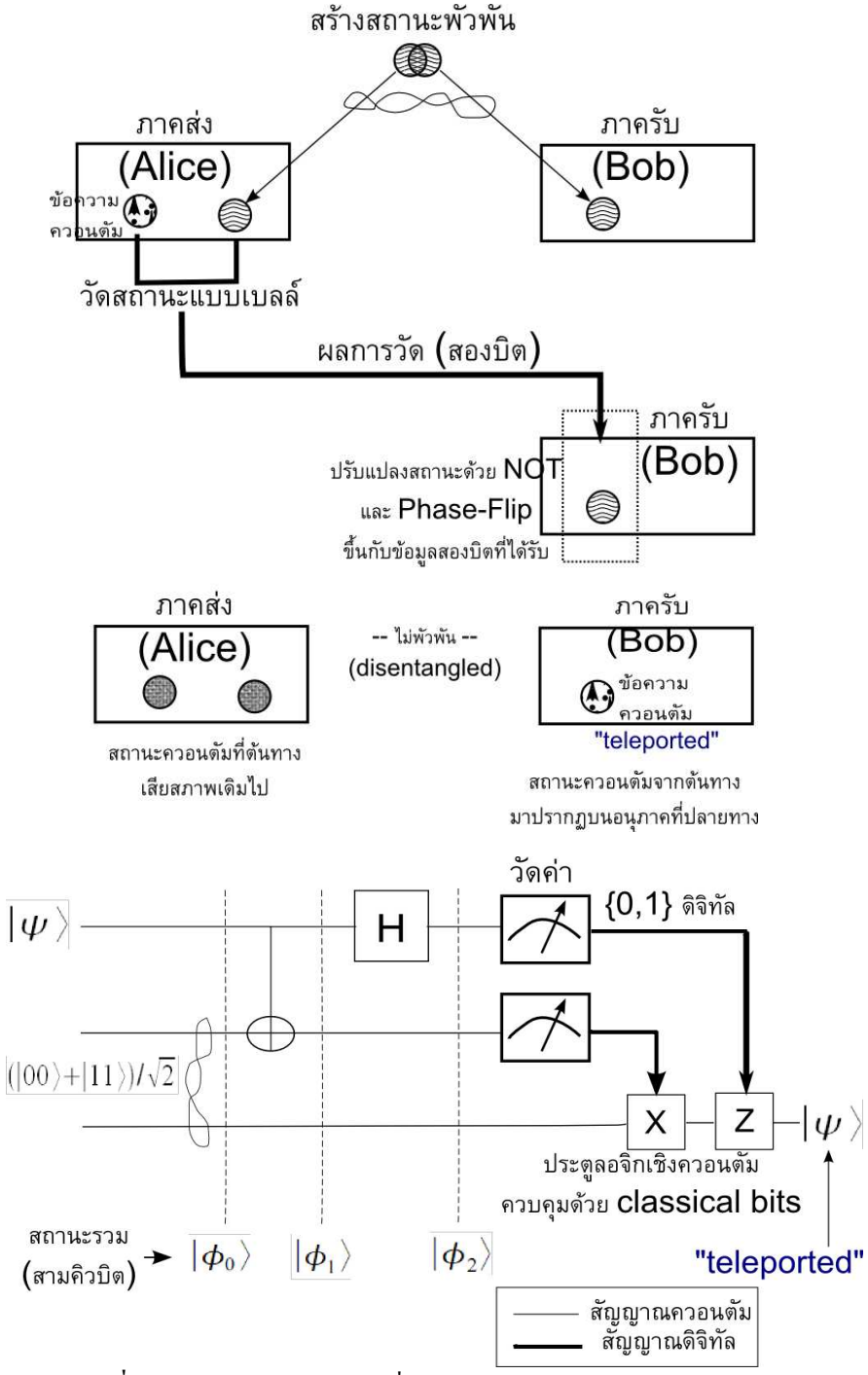
พื้นฐานการเทเลพอร์ตเชิงควอนตัมเริ่มต้นโดยการสร้างสถานะพัวพันระหว่างสองอนุภาค (สองคิวบิต) แล้วส่งแต่ละคิวบิตไปยังผู้ส่งและผู้รับฝั่งละหนึ่งอนุภาค จากนั้นทำการวัดค่าร่วมกัน (Joint measurement) ระหว่างอนุภาคที่แทนข้อมูลควอนตัมที่ต้องการเทเลพอร์ท กับอนุภาคที่มีสถานะพัวพันกับอีกอนุภาคหนึ่งที่ปลายทาง จากนั้นต้นทางต้องบอกผลการวัดค่า (สองบิต) ไปยังปลายทาง เช่น ผู้ส่งเขียนจดหมาย หรือ โทรศัพท์หาผู้รับเพื่อบอกผล จากนั้นผู้รับปรับสถานะของคิวบิตที่อยู่กับตัว ด้วยเกต NOT เชิงควอนตัม (Quantum NOT gate) และเกตกลับเฟส (Phase shift gate) ที่ควบคุมด้วยข้อมูลสองบิตจากผู้ส่งเมื่อเสร็จสิ้นแล้วสถานะคิวบิตที่อยู่ฝั่งผู้ส่งจะไปปรากฏที่ฝั่งผู้รับแทน ดังรูปที่ 3.3

พิจารณาสถานะในแต่ละขั้นตอนของกระบวนการเทเลพอร์ต สถานะเริ่มต้น (สถานะของสามคิวบิต) ตามรูปที่ 3.3 (ละสัมประสิทธิ์ $1/\sqrt{2}$ ออกเพื่อลดความซับซ้อนในการพิจารณา)

$$|\phi_0\rangle = |\psi\rangle(|00\rangle+|11\rangle)/\sqrt{2} = (a|0\rangle+b|1\rangle)(|00\rangle+|11\rangle)/\sqrt{2}$$
$$= a(|000\rangle+|011\rangle)+b(|100\rangle+|111\rangle) \qquad \text{.....(3.1)}$$

ผ่าน CNOT

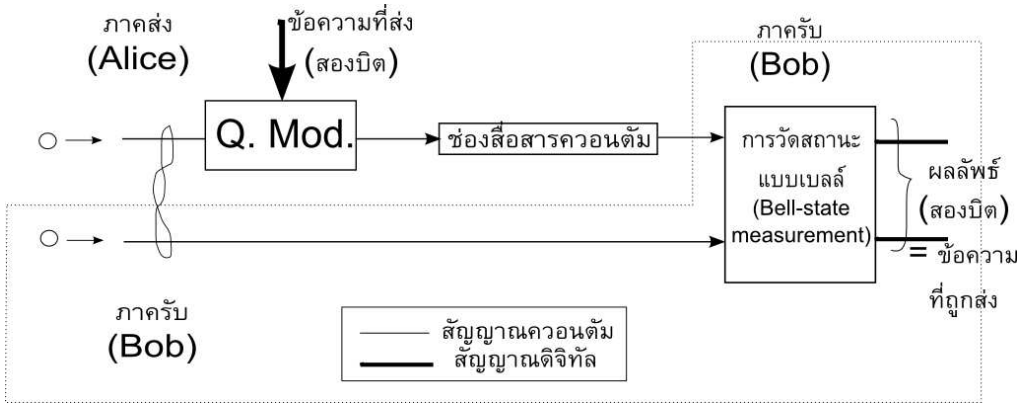
$$|\phi_1\rangle = a(|000\rangle+|011\rangle)+b(|110\rangle+|101\rangle) \qquad \text{.....(3.2)}$$



รูปที่ 3.3 วงจรแทนกระบวนการสื่อสารแบบเทเลพอร์ตเชิงควอนตัม

ผ่านเกตฮาร์ดามาร์ด (Hadamard gate)

$$
\begin{aligned}
|\phi_2\rangle &= a(|0\rangle+|1\rangle)|00\rangle+a(|0\rangle+|1\rangle)|11\rangle \\
&\quad +b(|0\rangle-|1\rangle)|10\rangle+b(|0\rangle-|1\rangle)|01\rangle \\
&= a|000\rangle+a|100\rangle+a|011\rangle+a|111\rangle+b|001\rangle-b|101\rangle+b|010\rangle-b|110\rangle
\end{aligned}
\qquad \text{.....(3.3)}
$$



รูปที่ 3.4 สรุปการทำงานของการเข้ารหัสความหนาแน่นสูงเชิงควอนตัม

จัดรูปแล้วได้เป็น

$$|\phi_2\rangle = |00\rangle(a|0\rangle + b|1\rangle) + |10\rangle(a|0\rangle - b|1\rangle) \\ + |01\rangle(a|1\rangle + b|0\rangle) + |11\rangle(a|1\rangle - b|0\rangle) \qquad \text{.....(3.4)}$$

จะสังเกตได้ว่าข้อมูลสัมประสิทธิ์ a และ b ไปปรากฏที่คิวบิตที่สาม ในขณะที่สถานะของสองคิวบิตแรกกลายเป็นสถานะตั้งฉากกันสี่สถานะ $|00\rangle$, $|01\rangle$, $|10\rangle$ และ $|11\rangle$ เมื่อวัดสองคิวบิตแรก จะทราบว่าสามารถแบ่งแยกสถานะทั้งสี่ได้อย่างชัดเจน และจากผลการวัดสถานะที่ได้ นำมาปรับค่าคิวบิตที่สามด้วยเกต NOT และเกตกลับเฟส จะได้สถานะควอนตัม $|\psi\rangle = a|0\rangle + b|1\rangle$ ไปปรากฏที่คิวบิตที่สาม (ซึ่งเดิมอยู่ที่คิวบิตแรก) อย่างสมบูรณ์ [*Bennett และคณะ 1993*]

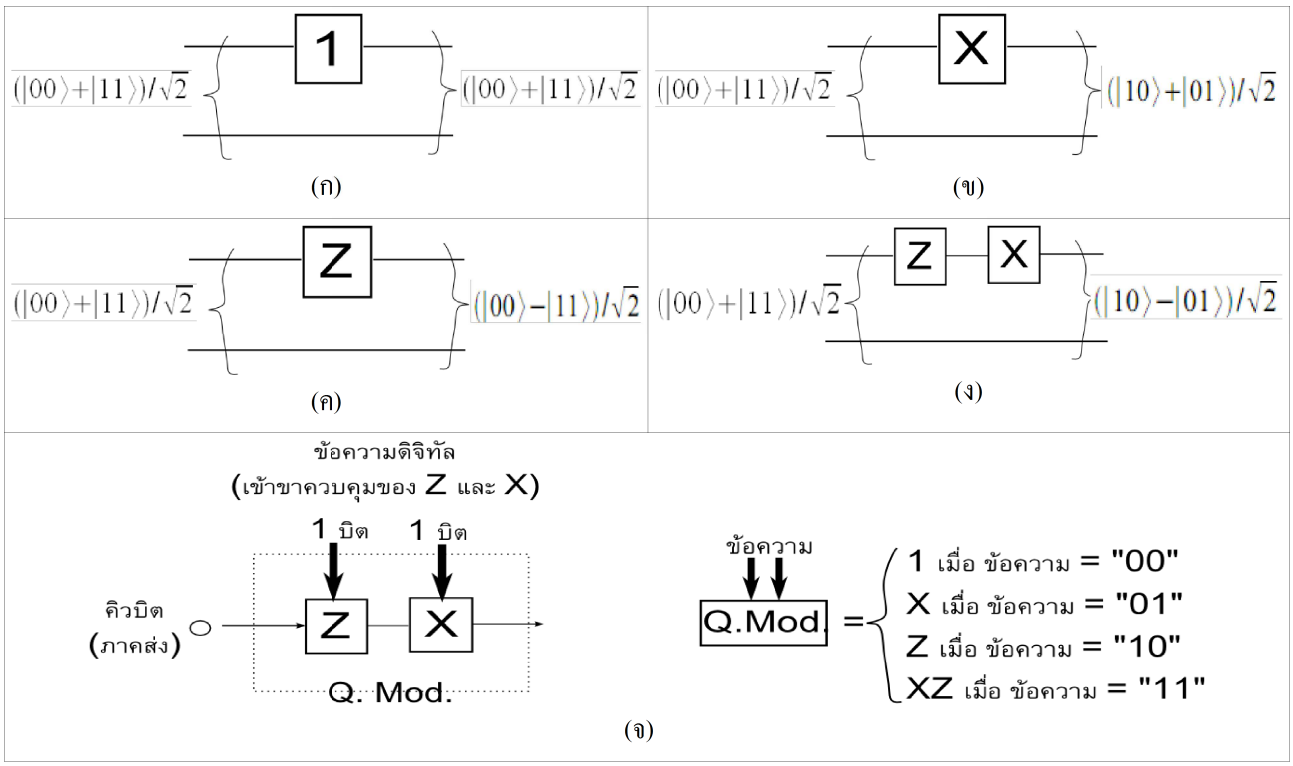
3.4 การเข้ารหัสความหนาแน่นสูงเชิงควอนตัม (Quantum superdense coding)

ปี ค.ศ. 1992 ชาร์ลส์ เบนเนตต์[3.1] และ สตีเฟน วีส์เนอร์[3.2] เสนอการประยุกต์ใช้สถานะพัวพันในรูปแบบสถานะเบลล์ (Bell States) ในการแทนข้อมูลดิจิทัลสองบิต และสามารถสื่อสารข้อมูลสองบิต ด้วยการส่งสถานะควอนตัมเพียงคิวบิต (อนุภาค) เดียว [*Bennett & Wiesner 1992*]

ขั้นตอนสรุปของการเข้ารหัสความหนาแน่นสูงเชิงควอนตัมอธิบายได้ตามรูปที่ 3.4 โดยแหล่งกำเนิดสถานะพัวพัน สร้างสถานะพัวพันสองคิวบิตและส่งให้ผู้ส่งและผู้รับฝั่งละหนึ่งคิวบิต (รูปที่ 3.4) จากนั้นผู้ส่งจะกล้ำสัญญาณ (Modulate) ข้อมูลสองบิตด้วยการเปลี่ยนสถานะของคิวบิตที่อยู่กับตัว ด้วยตัวดำเนินการเชิงควอนตัมสี่แบบ คือ ตัวดำเนินการเอกลักษณ์ (Identity) ตัวดำเนินการเกต NOT ตัวดำเนินการเกตกลับเฟส และ ทั้งตัวดำเนินการ NOT และตัวดำเนินการกลับเฟส จากนั้นส่งคิวบิตที่ปรับสถานะแล้วไปให้ผู้รับซึ่ง ผู้รับจะวัดสถานะแบบเบลล์ ซึ่งทำให้รู้ว่าผู้ส่งปรับสถานะคิวบิตด้วยวิธีใดในสี่รูปแบบ (“สองบิต” ที่ต้องการส่ง) โดยที่วงจรการแทนข้อมูลดิจิทัลด้วยสถานะควอนตัม ที่มีการทำงานดังแสดงในรูปที่ 3.4 การเข้าใจกระบวนการเข้ารหัสเชิงควอนตัมดังกล่าว ต้องรู้จักกับสถานะพัวพันที่นำมาใช้ในกรณีนี้ นั่นคือ “สถานะแบบเบลล์”

3.1 ชาร์ลส์ เบนเนตต์ เป็นบุคคลเดียวกับที่เสนอแนวคิดวิทยาการรหัสลับเชิงควอนตัมร่วมกับจิลส์ บราซซาร์ดในปี ค.ศ. 1984 ต่อมาเสนอแนวคิดเกี่ยวกับการเทเลพอร์ตเชิงควอนตัมร่วมกับนักวิทยาศาสตร์อีกห้าคนในปี ค.ศ. 1993

3.2 สตีเฟน วีส์เนอร์ เสนอแนวคิดการใช้สถานะควอนตัมไม่ตั้งฉากในการแทนข้อมูล เช่นเลขธนบัตรเพื่อป้องกันการปลอมแปลง ซึ่งแนวคิดของวีส์เนอร์นี้นำไปสู่วิทยาการรหัสลับเชิงควอนตัมในเวลาต่อมา

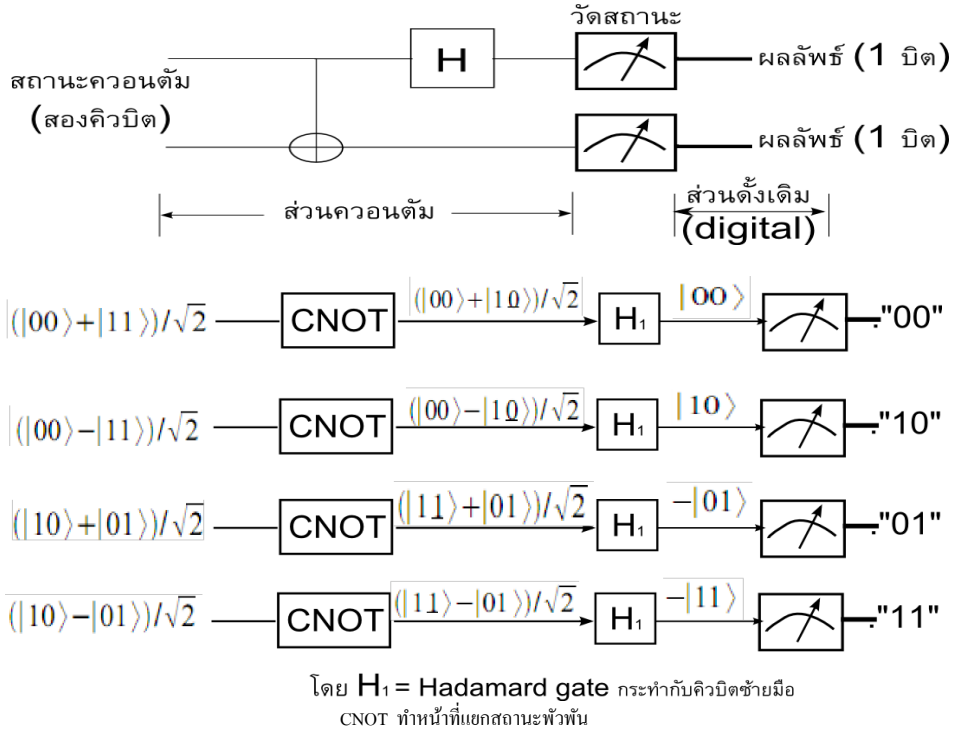


รูปที่ 3.5 การแทนข้อมูลดิจิทัลด้วยสถานะควอนตัม ในกระบวน*การเข้ารหัสความหนาแน่นสูงเชิงควอนตัม*

(ก) ดำเนินการเอกลักษณ์ (ข) การดำเนินการ NOT (ค) การดำเนินการกลับเฟส

(ง) การดำเนินการ NOT และกลับเฟสกับคิวบิตที่ฝั่งผู้ส่ง ตามข้อความสองบิตที่ต้องการส่ง

(จ) สรุปวิธีการปรับเปลี่ยนสถานะควอนตัมตามข้อความสองบิต (Quantum modulation ในรูปที่ 3.4)



รูปที่ 3.6 การวัดสถานะแบบเบลล์ เมื่อสถานะที่เข้ามาเป็นสถานะเบลล์ทั้งสี่แบบให้ผลเป็นข้อมูลสถานะสองบิตที่แยกแยะได้

3.4.1 สถานะเบลล์ (Bell states)

สถานะแบบเบลล์[3.3] คือสถานะพัวพันระหว่างอนุภาค ในกรณีนี้จะพิจารณาสองอนุภาค (สองคิวบิต) ซึ่งมีความพัวพันสูงสุด (Perfect correlation) มีสี่รูปแบบ ได้แก่

$$(|00\rangle+|11\rangle)/\sqrt{2} \quad , \quad (|10\rangle+|01\rangle)/\sqrt{2}$$
$$(|00\rangle-|11\rangle)/\sqrt{2} \quad \text{และ} \quad (|10\rangle-|01\rangle)/\sqrt{2} \qquad \text{.....(3.5)}$$

ซึ่งทั้งสี่สถานะเป็นสถานะที่ตั้งฉากกันจึงสามารถแยกแยะจากกันได้อย่างชัดเจน โดยวิธีการแยกแยะสถานะแบบเบลล์ทั้งสี่รูปแบบเรียกว่าการวัดสถานะแบบเบลล์ (Bell-state measurement)

3.4.2 การวัดสถานะแบบเบลล์ (Bell-state Measurement/ Bell-state analyzer)

ในกระบวนการเข้ารหัสความหนาแน่นสูงเชิงควอนตัม เมื่อผ่านกระบวนการกำหนดสถานะแบบเบลล์ทั้งสี่รูปแบบ เข้าสู่วงจรการวัดสถานะแบบเบลล์ จะให้ผลดังรูปที่ 3.6 จากรูป เกต CNOT ทำหน้าที่แยกสถานะพัวพัน ให้เป็นสถานะแบ่งแยกได้ (ไม่พัวพัน “disentangled”) และเกตฮาร์ดามาร์ดทำหน้าที่ ยุบสถานะจากสถานะทับซ้อนเชิงตำแหน่งให้กลายเป็นสถานะเดี่ยว จากนั้นกระบวนการวัดค่า คือ การแยกแยะสถานะระหว่าง “0” และ “1” ดังรูปที่ 3.6

3.4.3 หลักการเข้ารหัสความหนาแน่นสูงเชิงควอนตัม (การประยุกต์สถานะเบลล์)

จากการที่สถานะของเบลล์ทั้งสี่รูปแบบ เป็นสถานะตั้งฉากและแยกแยะจากกันได้อย่างชัดเจน จึงมีการเสนอว่าสถานะทั้งสี่นี้สามารถนำมาใช้ในการสื่อสารข้อมูลดิจิทัลสองบิต (สี่สถานะ) ด้วยการส่งสถานะควอนตัมได้ โดยเริ่มต้นมีการสร้างสถานะพัวพันสองอนุภาค (สองคิวบิต) และส่งให้ผู้ส่งและผู้รับฝั่งละอนุภาค จากนั้นผู้ส่งทำการปรับสถานะคิวบิตที่ฝั่งของตนด้วยตัวดำเนินการเชิงควอนตัม (Quantum operator/ Quantum logic gate) สี่รูปแบบ ซึ่งให้ผลเป็นสถานะร่วมของสองคิวบิตสี่รูปแบบ (คือสถานะแบบเบลล์ทั้งสี่) จากนั้นผู้ส่งส่งคิวบิตจากฝั่งของตนไปยังผู้รับ ซึ่งจะทำการวัดสถานะแบบเบลล์ของอนุภาคทั้งคู่ และจะรู้ว่าผู้ส่งดำเนินการอะไรกับอนุภาคด้วยวิธีการทั้งสี่แบบก่อนจะส่งมา ซึ่งหมายถึงข้อความดิจิทัลสองบิต ที่ผู้ส่งแทนด้วยตัวดำเนินการสี่แบบนั้น สามารถขยายความขั้นตอนการเข้ารหัสความหนาแน่นสูงเชิงควอนตัมได้ดังต่อไปนี้

ขั้นแรก การแลกเปลี่ยนความพัวพันร่วมกัน (Entanglement sharing) เริ่มจากแหล่งกำเนิดความพัวพัน สร้างสถานะพัวพันสองคิวบิต ส่งให้กับผู้ส่งและผู้รับฝั่งละหนึ่งคิวบิต แทนสถานะดังกล่าวด้วย (คิวบิตซ้ายมือถูกส่งให้ผู้ส่งและคิวบิตขวามือถูกส่งให้ผู้รับ)

$$(|00\rangle+|11\rangle)/\sqrt{2} \qquad \text{.....(3.6)}$$

ขั้นที่สอง ผู้ส่งทำการกล้ำข้อความสองบิต ด้วยตัวดำเนินการเชิงควอนตัมสี่รูปแบบ ได้แก่

“00” ใช้ตัวดำเนินการเอกลักษณ์ ให้ผลลัพธ์คือสถานะ

$$(|00\rangle+|11\rangle)/\sqrt{2} \quad \text{(เหมือนเดิม)} \qquad \text{.....(3.7)}$$

“01” ใช้ตัวดำเนินการ NOT ให้ผลลัพธ์คือสถานะ

$$(|10\rangle+|01\rangle)/\sqrt{2} \quad \text{(ทำการ NOT กับคิวบิตซ้ายมือ)} \qquad \text{.....(3.8)}$$

[3.3] ตั้งชื่อเพื่อให้เกียรติแก่ จอห์น เบลล์ (John Bell) ผู้เสนอทฤษฎีที่ช่วยการทดลองเพื่อพิสูจน์ว่า ปรากฏการณ์ความพัวพันมีจริง ในปี ค.ศ. 1964

"10" ใช้ตัวดำเนินการกลับเฟส ให้ผลลัพธ์คือสถานะ

$$(|00\rangle - |11\rangle)/\sqrt{2}$$ (ทำการกลับเฟสจากบวกเป็นลบ) .....(3.9)

"11" ใช้ตัวดำเนินการ NOT และตัวดำเนินการกลับเฟส ให้ผลลัพธ์คือสถานะ

$$(|10\rangle - |01\rangle)/\sqrt{2}$$ (ทำการ NOT กับคิวบิตซ้ายมือ และกลับเฟส) .....(3.10)

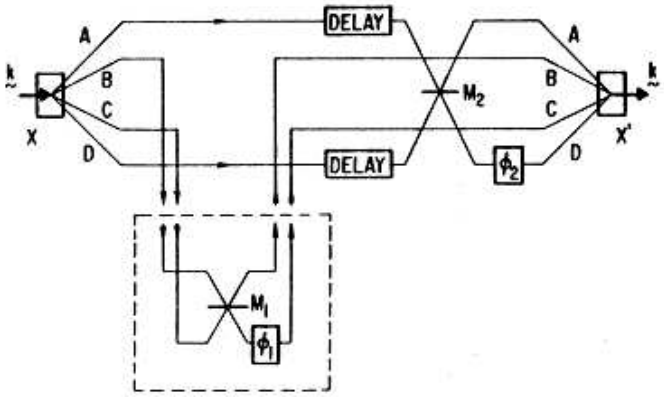
(ในขั้นตอนที่สองนี้คิวบิตอยู่ที่ผู้ส่งและผู้รับฝั่งละหนึ่งคิวบิต)

<u>*ขั้นที่สาม*</u> ผู้ส่งส่งคิวบิตที่ถูกกล้ำแล้ว ไปยังผู้รับและผู้รับทำการวัดสถานะแบบเบลล์ ทำให้ได้ผลลัพธ์ออกมาเป็น "00" "01" "10" หรือ "11" นั่นคือข้อมูลดิจิทัลสองบิตที่ผู้ส่งต้องการสื่อสาร

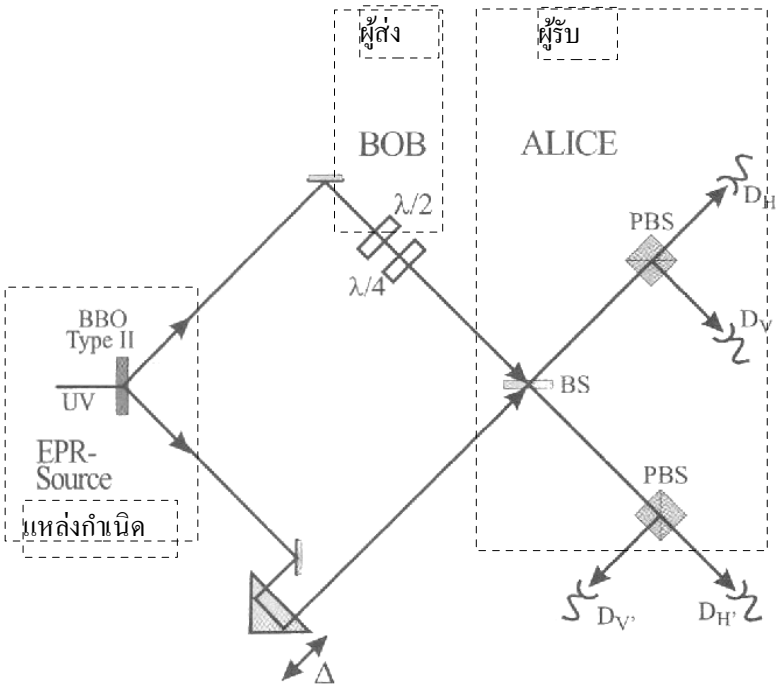
สำหรับการสื่อสารที่ใช้แสงนั้นการเข้ารหัสความหนาแน่นสูงเหมือนกับการส่งข้อความสองบิต ด้วยการส่งเพียง "โฟตอนเดี่ยว" ซึ่งหลักการนี้ไม่มีทางเป็นไปได้หากไม่มีคุณสมบัติความพัวพัน เพราะโฟตอนเดี่ยวแทนสถานะตั้งฉาก (แบ่งแยกได้) ได้เพียงสองสถานะหรือ 1 บิต เท่านั้นแต่เมื่อมีความพัวพันแล้วจะเป็นไปได้จึงเป็นเหตุผลหนึ่งที่กล่าวว่า "ความพัวพันเป็นเหมือนทรัพยากรข่าวสาร" ดังกล่าว

3.4.4 การทดลองเข้ารหัสความหนาแน่นสูงเชิงควอนตัม

ในบทความแรกที่เสนอการเข้ารหัสความหนาแน่นสูงเชิงควอนตัม เบนเนตต์ และวีส์เนอร์ ได้ออกแบบการทดลองไว้ดังรูปที่ 3.7 โดยการใช้สถานะคิวบิตที่แทนด้วยเส้นทาง (คิวบิตที่หนึ่งแทนด้วยการมีโฟตอนในเส้นทาง A = "0" และ D = "1" เช่นเดียวกันคิวบิตที่สอง แทนด้วย C = "0" และ B = "1") โดยสถานะพัวพันสร้างจากกระบวนการแปลงผันลง (down conversion) ซึ่งให้ผลลัพธ์เป็นโฟตอนคู่ที่มีความพัวพันเชิงโมเมนตัม (คู่โฟตอนผ่าน "A-C" พร้อมกัน หรือ "D-B" พร้อมกันเท่านั้น หรือแทนด้วยสถานะพัวพัน $|AC\rangle + |DB\rangle \equiv |00\rangle + |11\rangle$) ใช้ตัวเลื่อนเฟส (phase shifters) และตัวแยกลำแสง (กระจกเคลือบเงา 50:50 แทนสัญลักษณ์ M) ซึ่งเลื่อนเข้า-ออก ได้ ในการ 'modulation' ข้อความสองบิตลงบนคิวบิตที่สอง (โฟตอนในแนว C และ D) ดังต่อไปนี้ (1) ไม่เปลี่ยนสถานะคิวบิต ให้ผลลัพธ์เป็น $|AC\rangle + |DB\rangle = |00\rangle + |11\rangle$ เช่นเดิม (2) ตั้งค่าตัวเลื่อนเฟส $\phi_1 = \pi$ ให้ผลลัพธ์เป็น $|AC\rangle - |DB\rangle = |00\rangle - |11\rangle$ (3) สลับแนวลำแสง B และ C โดยนำตัวแยกลำแสง M_1 ออก ให้ผลลัพธ์เป็น $|AB\rangle + |DC\rangle = |01\rangle + |10\rangle$ (4) กระทำตามข้อ 2. และ 3. โดยใส่ทั้ง M_1 และ $\phi_1 = \pi$ ให้ผลลัพธ์เป็น $|AB\rangle - |DC\rangle = |01\rangle - |10\rangle$ ทำให้ได้สถานะแบบเบลล์ทั้งสี่รูปแบบด้วยวิธีดังกล่าว ส่วนที่ภาครับมีการติดตั้งตัวแยกลำแสง M_2 และตัวเลื่อนเฟส ϕ_2 ให้เหมาะสมกับการติดตั้งที่ภาคส่ง จะมี 'ความน่าจะเป็น' ที่แสงจะรวมกันภายในผลึกเป็นโฟตอนเดี่ยวที่พลังงานสูงขึ้น ในกระบวนการแปลงผันขึ้น (up-conversion) แม้ความน่าจะเป็นของเหตุการณ์จะน้อย แต่ทันทีที่ตรวจพบโฟตอนที่ปลายทาง ภาครับจะสรุปได้ว่าภาคส่งใช้วิธีการใดในสี่รูปแบบในการ modulate แสง (นั่นคือข้อความสองบิต ดังรูปที่ 3.7)



รูปที่ 3.7 รูปแบบการทดลองที่เสนอไว้ในบทความแรกของการเข้ารหัสความหนาแน่นสูงเชิงควอนตัม
โดย M_1 และ M_2 แทนตัวแยกลำแสง (beam splitter) ϕ_1 แทนตัวเลื่อนเฟสสำหรับปรับสถานะ
ของโฟตอน B และ C ϕ_2 แทนตัวเลื่อนเฟสสำหรับปรับสถานะของโฟตอน A และ D
รูปสี่เหลี่ยมฝั่งซ้าย (และฝั่งขวา) แทนกระบวนการแปลงผันลงและแปลงผันขึ้น ตามลำดับ
รูปดัดแปลงจาก [*Bennett & Wiesner 1992*]



รูปที่ 3.8 การจัดอุปกรณ์เพื่อสาธิตการเข้ารหัสความหนาแน่นสูงเชิงควอนตัม ด้วยสถานะพัวพันเชิงโพลาไรซ์ของแสง
ในรูป "*BOB*"[3.4] ทำหน้าที่กล้ำข้อความดิจิทัลสองบิต ด้วย แผ่นหน่วงคลื่นสองแผ่น ($\lambda/2$ และ $\lambda/4$
แทนตัวดำเนินการ NOT และ Phase-flip) BS แทน กระจกแยกลำแสง (Beam splitter)แบบ 50 เปอร์เซ็นต์
PBS แทนกระจกแยกลำแสงเชิงโพลาไรซ์ (Polarizing beam splitter)
Δ แทนอุปกรณ์สำหรับปรับระยะทางเพื่อให้โฟตอนทั้งสองเส้นทางมาถึง BS พร้อมกัน
D_H D_H' และ D_V D_V' แทนตัวตรวจหาโฟตอนที่มีโพลาไรซ์ 'แนวนอน' และ 'แนวตั้ง' ตามลำดับ
รูปดัดแปลงจาก [*Mattle และคณะ 1996*]

[3.4] หมายเหตุ: แผนภาพแสดงการทดลองดังกล่าว ตั้งชื่อผู้ส่ง ว่า "*Bob*" และผู้รับชื่อ "*Alice*" [*Mattle และคณะ 1996*] สลับกับแผนภาพในหัวข้ออื่นๆ อนึ่งควรพิจารณาตามการทำงานว่าผู้ใดทำการกล้ำสัญญาณ (ผู้ส่ง) และผู้ใดตรวจวัดสัญญาณ (ผู้รับ)

ส่วนการทดลองจริงเกิดขึ้นเป็นครั้งแรกเมื่อ ค.ศ. 1996 โดยกลุ่มวิจัยที่อินสบรุค ประเทศออสเตรีย ดังรูปที่ 3.8 อาศัยสถานะพัวพันเชิงโพลาไรซ์ของแสงที่สร้างจากกระบวนการ parametric down conversion ประเภทที่ให้สถานะโพลาไรซ์เดียวกันออกมา คือ $(|\updownarrow\updownarrow\rangle + |\leftrightarrow\leftrightarrow\rangle)/\sqrt{2}$ ซึ่งแทนสถานะเชิงการคำนวณ (“0” และ “1”) $(|00\rangle + |11\rangle)/\sqrt{2}$ จากนั้นส่งคิวบิต (โฟตอน) ให้ *Alice* และ *Bob* ฝั่งละหนึ่งคิวบิต โดยผู้ส่งในกรณีการทดลองนี้กำหนดเป็น *Bob* ทำการกล้ำคิวบิตด้วยข้อความสองบิต ผ่านทาง “*waveplate*” สองตัว และส่งคิวบิตที่ได้ไปยังผู้รับ (*Alice*) ซึ่งทำการวัดสถานะแบบเบลล์ โดยกระจกแยกลำแสง (BS) ทำหน้าที่เป็นเกตฮาร์ดามาร์ด (H) กระจกแยกลำแสงโพลาไรซ์ (PBS) ทำหน้าที่แยกสถานะระหว่างโพลาไรซ์แนวตั้งและแนวนอน (ทำหน้าที่แทน  ในรูปวงจรเชิงควอนตัม) จากนั้นวิเคราะห์ความสอดคล้องของการตรวจพบโฟตอน และสรุปว่าวิธีการกล้ำสัญญาณโดยผู้ส่งเป็นอะไร ได้ผลลัพธ์เป็นข้อความสองบิต

สรุปการเข้ารหัสความเข้มสูงเชิงควอนตัม นอกจากสามารถใช้ส่งข้อความดิจิทัลสองเท่าตัว (สองบิต) ด้วยการส่งข้อมูลควอนตัมเพียงหนึ่งเท่า (หนึ่งคิวบิต) ยังสามารถทำหน้าที่แทนการสื่อสารความลับไปในตัว เนื่องจาก ผู้ดักจับใดๆ ที่ได้คิวบิตระหว่างสื่อสารไป ไม่สามารถทำการวัดเพื่อถอดรหัสข้อมูลได้ถ้าไม่มีอีกคิวบิตที่พัวพันกัน (ซึ่งเก็บไว้ที่ฝั่งผู้รับ) [*Bennett & Wiesner 1992*] แต่ความปลอดภัยนี้ตั้งอยู่บนสมมติฐานที่คู่สื่อสารได้สถานะพัวพันร่วมกันเก็บไว้ก่อนแล้ว หากผู้ดักจับสามารถดักคิวบิตทุกขั้นตอนนับตั้งแต่การกระจายคู่โฟตอนพัวพัน ย่อมสามารถดักรู้ข้อมูลสองบิตของการสื่อสาร ด้วยคิวบิตพัวพันที่ดักไว้ก่อนและคิวบิตที่ถูกส่งระหว่างการสื่อสารแบบเข้ารหัสด้วยความหนาแน่นสูง

3.5 การควบคุมความผิดพลาดเชิงควอนตัม

สำหรับทั้งการสื่อสารและการคำนวณเชิงควอนตัม (ที่นำเสนอในบทถัดไป) สิ่งที่เป็นอุปสรรคต่อความสำเร็จในการสื่อสารหรือประมวลผลข้อมูลเชิงควอนตัมแต่ละครั้ง คือการมีอันตรกิริยากับสิ่งแวดล้อม อันทำให้เกิดความผิดพลาดของข้อมูลควอนตัม โดยคุณสมบัติควอนตัม คือการทับซ้อนเชิงตำแหน่งและคุณสมบัติพัวพันบางส่วนหรือทั้งหมดได้สูญเสียไป เรียกกระบวนการดังกล่าวว่า 'Decoherence' โดยในปี ค.ศ. 1993 เดวิด ดอยช์ (David Deutsch) เสนอวิธีการทำให้ข้อมูลคืนสภาพ (Recoherence)[3.5] [*Brooks 1999*] โดยการใช้สถานะควอนตัมลักษณะเหมือนกันซ้อนๆ กันหลายคิวบิต เพื่อแทนข้อมูลเดียวกันในลักษณะสมมาตร (Symmetry) โดยเมื่อความผิดพลาดเกิดขึ้น จะทำให้ความสมมาตรดังกล่าวสูญเสียไป และสามารถตรวจพบได้โดยการตรวจสอบสถานะควอนตัมส่วนที่ไม่เกิดข้อผิดพลาด

วิธีแก้ไขความผิดพลาดเชิงควอนตัม (Quantum Error Correction) ได้ถูกนำเสนอในเชิงคณิตศาสตร์โดยปีเตอร์ ชอร์ (Peter Shor) จากห้องปฏิบัติการเบลล์ และแอนดรู สตีน (Andrew Steane) จากมหาวิทยาลัยออกซ์ฟอร์ด โดยวิธีของทั้งคู่มีความเหมือนกันในเชิงคณิตศาสตร์ โดยการแทนข้อมูลหนึ่งคิวบิต ด้วยหลายคิวบิต (เช่น 3 คิวบิต 7 คิวบิต และ 9 คิวบิต) ความผิดพลาดที่เกิดขึ้นกับหนึ่งคิวบิตใดๆ ไม่มีผลต่อการกู้คืนข้อมูลควอนตัมในคิวบิตตั้งต้น โดยสามารถแยกคิวบิตที่เสีย ทิ้งไปและเก็บข้อมูลควอนตัมที่ถูกส่งในตอนแรกไว้กับคิวบิตที่เหลือได้ นอกจากนี้สิ่งที่น่าสนใจในเชิงคณิตศาสตร์ คือ ความปลอดภัยของการกระจายกุญแจเชิงควอนตัม (Quantum key distribution) สามารถพิสูจน์และอธิบายได้ด้วยการทำงานของรหัสแก้ไขความผิดพลาดเชิงควอนตัม [*Shor & Preskill 2000*]

ในทางปฏิบัติ การสื่อสารเชิงควอนตัมต้องมีการเลือกวิธีแทนสถานะที่เหมาะสมกับลักษณะช่องสัญญาณ เช่นการแทนสถานะด้วยโพลาไรเซชัน เหมาะสมกับการสื่อสารผ่านอากาศ เนื่องจากอากาศทำให้เกิดการเปลี่ยนโพลาไรซ์น้อยกว่าเส้นใยแสง และในการแทนสถานะด้วยความต่างเฟส เหมาะสมกับการสื่อสารผ่านเส้นใยแสง เนื่องจากเฟสแปรผันตามดัชนีการหักเหและระยะ

[3.5] ในงานสัมมนา “Rank Prize Funds Mini-Symposium on Quantum Communication and Cryptography” ที่ Broadway ประเทศอังกฤษ [*Brooks 1999*]

หากความผิดพลาดของสถานะในช่องสัญญาณของการสื่อสารเชิงควอนตัม เป็นลักษณะยูนิแทรี (Unitary) คือมีคุณสมบัติย้อนกลับได้ เช่น การบิดทิศโพลาไรซ์ของแสงในเส้นใยแสง การกู้คืนสถานะจะทำได้โดยกระทำการชดเชยสถานะด้วยตัวดำเนินการผกผัน (Inverse operator) ของตัวดำเนินการ เช่นการบิดโพลาไรซ์กลับในมุมเท่าเดิม แต่ถ้าความผิดพลาดเกิดในลักษณะไม่ยูนิแทรี (Non-unitary) คือ ย้อนกลับไม่ได้ การป้องกันข้อผิดพลาดของสถานะควอนตัมทำได้โดยแทนสถานะควอนตัมด้วยจำนวนคิวบิตที่มากขึ้น (มิติใหญ่ขึ้น) โดยอาศัยคิวบิตช่วยเหลือ (Auxiliary qubits) และเมื่อถึงปลายทางผู้รับทำการกู้คืนโดยกระทำให้ความผิดพลาดไปปรากฏที่คิวบิตช่วยเหลือ และข้อมูลที่ต้องการส่งมาปรากฏที่คิวบิตหลักแทน ซึ่งวิธีการนี้เรียกว่าวิธีแก้ไขความผิดพลาดเชิงควอนตัม

ทางของช่องสัญญาณ ซึ่งมีความคงที่อยู่มากในเส้นใยแสง (หากไม่มีการเปลี่ยนอุณหภูมิอย่างรุนแรงทำให้มีการยืดหรือหดของเส้นใยแสง) ส่วน "อากาศ" ซึ่งมีการเปลี่ยนแปลงของแกสในบริเวณเดียวกันอยู่ตลอดเวลาทำให้ดัชนีการหักแหเปลี่ยนแปลงตามเวลา และความต่างเฟสจึงมีค่าไม่แน่นอน ทำให้ไม่เหมาะสมต่อการสื่อสารโดยใช้เฟสแทนสถานะเป็นต้น

บทสรุป

บทนี้นำเสนอเทคนิคการสื่อสารที่อาศัยคุณสมบัติความพัวพันเชิงควอนตัม มาใช้ในการส่งข้อมูลในรูปแบบที่ไม่มีในการสื่อสารดั้งเดิม (ทั้งแอนะลอก และดิจิทัล) นั่นคือ การส่งสถานะควอนตัมอย่างแน่นอนด้วยการส่งข้อความดิจิทัลสองบิต (Quantum teleportation) และในทางกลับกันคือ การส่งข้อความสองบิตด้วยการส่งสถานะควอนตัมหนึ่งคิวบิตหรือการเข้ารหัสความหนาแน่นสูงเชิงควอนตัม (Quantum superdense coding) ซึ่งเป็นเหตุที่คุณสมบัติพัวพัน ถูกมองว่าเป็น 'ทรัพยากรข่าวสาร' (“Information resource”) ซึ่งการเทเลพอร์ทเชิงควอนตัมได้ทำการทดลองจริงแล้วทั้งในการส่งสถานะควอนตัมของแสง [*Bouwmeester และคณะ 1997*] และสถานะของอะตอม [*Barrett และคณะ 2004*] โดยในการทดลองสถานะควอนตัมที่ถูกส่งไป มีความผิดเพี้ยนจากสถานะที่ต้นทางไปบ้าง จึงมีการวัดค่า “ความเหมือน” ระหว่างสถานะต้นทาง และสถานะที่ปรากฏ ณ ปลายทาง เรียกว่า “Fidelity” ซึ่งคุณภาพประการหนึ่งของการเทเลพอร์ทบอกได้ด้วยค่านี้ การเทเลพอร์ทมีความสำคัญในการสื่อสารเชิงควอนตัมระยะไกล เนื่องจากการที่สถานะควอนตัมมีความอ่อนไหว (จะถูกกลืนหาย หรือเปลี่ยนสถานะโดยสิ่งแวดล้อมได้ง่าย) การส่งสถานะควอนตัมจึงมีอุปสรรคมาก การเทเลพอร์ทจะทำให้สามารถส่งสถานะควอนตัมด้วยการส่งสัญญาณดิจิทัล (ซึ่งสามารถส่งได้ไกล) ไปแทนโดยต่อเนื่องก็จะเป็นส่วนสำคัญในการวิจัยการสร้างหน่วยซ้ำสัญญาณเชิงควอนตัม (Quantum repeaters) ตามมาด้วย ส่วนการเข้ารหัสความหนาแน่นสูงเชิงควอนตัมทำงานในทางกลับกัน คือการส่งข้อความถึง “สองบิต” ด้วยการส่งสถานะควอนตัมเพียงหนึ่งคิวบิต ทำให้ปริมาณข่าวสารที่ส่งได้ต่อหนึ่งครั้งเพิ่มขึ้นเป็นปริมาณสองเท่า อย่างไรก็ดี ในการทดลองแรกที่สาธิตการเข้ารหัสความหนาแน่นสูงเชิงควอนตัม ได้ปริมาณข่าวสารที่ส่งต่อหนึ่งคิวบิตเท่ากับ 1.58 บิต (ซึ่งน้อยกว่า 2.00 บิต ในอุดมคติ) [*Mattle และคณะ 1996*] ในการทดลองจริง ความไม่สมบูรณ์ของการเตรียมสถานะที่ต้องการจะวัดด้วยค่าความถูกต้อง (Fidelity)[3.6] และความไม่สมบูรณ์ของช่องสื่อสาร (ทำให้เกิดกระบวนการสูญเสียพฤติกรรมเชิงควอนตัม) เป็นสิ่งที่ต้องได้รับการพิจารณา โดยได้มีการเสนอวิธีควบคุมความผิดพลาดเชิงควอนตัม และแบบจำลองการสื่อสารเชิงควอนตัมภายใต้การรบกวนของสิ่งแวดล้อมขึ้นเพื่อแก้ไขอุปสรรคดังกล่าวตามมา การศึกษาเรื่องเทเลพอร์เทชัน และการเข้ารหัสความหนาแน่นสูงดังกล่าวนี้ช่วยให้เข้าใจหลักความพัวพันและความสำคัญในชีวิตประจำวันมากขึ้น และยังเป็นพื้นฐานอีกมุมหนึ่งเพื่อการศึกษาค้นคว้าเกี่ยวกับการสื่อสารในยุคใหม่ “ยุคสารสนเทศเชิงควอนตัม”

[3.6] หากสถานะที่ได้ มีคุณสมบัติเหมือนสถานะที่ต้องการจะถือว่าค่าความถูกต้องเท่ากับ 100%

เอกสารอ้างอิง

[Barrett และคณะ 2004] M. D. Barett, et al., "Deterministic quantum teleportation of atomic qubits," *Nature*, vol. 429, pp. 737, 2004.

[Bennett และคณะ 1992] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, pp. 3-28, 1992.

[Bennett และคณะ 1993] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, No.13, p. 1895, 1993.

[Bouwmeester และคณะ 1997] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental Quantum Teleportation," *Nature*, vol. 390, p. 575, 1997.

[Bennett & Wiesner 1992] C. H. Bennett, and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, p. 2881, 1992.

[Brassard 2003] G. Brassard, "Quantum communication complexity," *Foundations of Physics*, vol. 33, no. 11, pp. 1593 – 1616, 2003.

[Braunstein & Kimble 2000] S. L. Braunstein, and H. J. Kimble, "Dense Coding for Continuous Variables," *Phys. Rev. A,* vol. 61, p. 042302, 2000.

[Brooks 1999] M. Brooks, *Quantum Computing and Communications*. London: Springer-Verlag, 1999.

[Gisin & Thew 2007] N. Gisin, and R. Thew, "Quantum Communication," *Nature Photonics,* vol. 1, no. 3**,** pp. 165-171, 2007.

[Hughes 2009] R. Hughes, "Remarks on Quantum Communications," Presentation at *Workshop on Quantum Information Science*, Vienna, 23rd-25th April 2009.

[Mattle และคณะ 1996] K. Mattle, et al., "Dense Coding in Experimental Quantum Communication," *Phys. Rev. Lett.,* vol. 76, pp. 4656–4659, 1996.

[Nielsen & Chuang 2000] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000 .

[Shor & Preskill 2000] P. W. Shor, and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.,* vol. 85*,* pp. 441-444, 2000.

คำถามท้ายบทที่ 3 (Questions and Answers)
และอภิปราย (Discussions) ปรับปรุง ณ
Blog: http://www.stks.or.th/blog/?p=14123

บทที่ 4
พื้นฐานการคำนวณเชิงควอนตัม
(Fundamental of quantum computing)

อภิธานศัพท์ (Glossary)

- **กระบวนวิธีของดอยช์-จอสซา (Deutsch-Jozsa algorithm)**
  กระบวนวิธีเชิงควอนตัมสำหรับแก้โจทย์ปัญหาเชิงควอนตัมชนิดแรกที่ได้รับการพิสูจน์ว่าทำงานเร็วกว่าวิธีดั้งเดิมเป็นเอกซ์โพเนนเชียลโดย เดวิด ดอยช์ และ ริชาร์ด จอสซา ปี ค.ศ. 1992
- **การคำนวณเชิงควอนตัม (Quantum computation/ Quantum computing)**
  การคำนวณภายใต้กฎของกลศาสตร์ควอนตัม การคำนวณเชิงควอนตัมขึ้นกับคุณสมบัติการทับซ้อนเชิงตำแหน่ง และความพัวพัน ซึ่งทำให้การแก้ปัญหาบางกรณีทำได้เร็วขึ้นด้วยความขนานเชิงควอนตัมซึ่งเป็นผลจากคุณสมบัติทับซ้อนเชิงตำแหน่ง
- **การคำนวณเชิงควอนตัมแบบทางเดียว (One-way quantum computing)**
  การคำนวณเชิงควอนตัมที่ใช้สถานะพัวพันจำนวนมากมาทำการวัดสถานะบางส่วนและให้เกิดผลเป็นวงจรควอนตัมที่ต้องการกระทำต่อคิวบิตที่เหลืออยู่
- **การคำนวณเชิงควอนตัมแบบอิงการวัดสถานะ (Measurement-based quantum computing)**
  ความหมายเหมือน one-way quantum computing
- **การคำนวณแบบดั้งเดิม (Classical computing)**
  การคำนวณที่สถานะมีได้เฉพาะเจาะจงค่าหนึ่ง ได้แก่ กรณีค่าไม่ต่อเนื่อง (0 หรือ 1) เรียกว่า การคำนวณเชิงดิจิทัล และ ค่าต่อเนื่อง (จำนวนจริง) เรียกว่า การคำนวณเชิงแอนะลอก
- **การแยกตัวประกอบ (Factorization)**
  การแยกตัวประกอบของจำนวนเต็ม N หมายถึงการแทน N ในรูปผลคูณของจำนวนเฉพาะ $N = q_0 \times q_1 \times q_3 \times \ldots \times q_N$ โดยที่ $q_0, ..., q_N$ เป็นจำนวนเฉพาะ
- **การสูญเสียความอาพันธ์เชิงควอนตัม (Decoherence)**
  การสูญเสียข้อมูลและคุณสมบัติเชิงควอนตัมจากผลกระทบของสิ่งแวดล้อม ทำให้ข้อมูลเชิงควอนตัมเปลี่ยนคุณลักษณะไปเป็นข้อมูลดั้งเดิม (classical) หรืออีกมุมหนึ่งคือ การสูญเสียข้อมูล*เฟสสัมพัทธ์*ระหว่างสองสถานะย่อยที่ทับซ้อนกันเชิงตำแหน่ง
- **ความสามารถในการเจาะจงตำแหน่ง (Addressability)**
  ความสามารถในการเจาะจงคิวบิตหนึ่งๆ เพื่ออ่านค่าหรือปรับเปลี่ยนสถานะคิวบิตที่ต้องการนั้น เพื่อการทำงานของเกตลอจิกเชิงควอนตัมและการวัดสถานะของคิวบิตใด ๆ
- **ความสามารถในการปรับขนาด (Scalability)**
  คุณสมบัติที่ระบบควอนตัมหนึ่งๆ ที่สามารถเพิ่มจำนวนคิวบิตสำหรับการคำนวณเชิงควอนตัม โดยที่คุณสมบัติเชิงควอนตัมยังคงอยู่ภายใต้การควบคุม
- **เครื่องกลทูริง (Turing Machine)**
  แบบจำลองทางคณิตศาสตร์ ซึ่งอธิบายการคำนวณเชิงดิจิทัลทุกรูปแบบ และเป็นต้นกำเนิดของดิจิทัลคอมพิวเตอร์ (เชิงทฤษฎี)
- **จำนวนเฉพาะ (Prime number)**
  จำนวนเต็มบวกที่มีตัวประกอบเป็น 1 และตัวมันเองเท่านั้น
- **โจทย์ปัญหาของดอยช์ (Deutsch's problem)**
  โจทย์ปัญหาที่มีผู้เล่นสองคน ผู้เล่น ก. มีฟังก์ชัน f ซึ่งเป็นได้เพียงสองชนิดคือ ฟังก์ชันสมดุล และฟังก์ชันคงที่ และผู้เล่น ข. ทำหน้าที่เลือกตัวเลขเลขหนึ่งระหว่าง 0 ถึง 2^N-1 แล้วส่งเลขดังกล่าว (x) ให้ ก. เพื่อคำนวณ $f(x)$ และตอบกลับไป คำถามคือ วิธีใดที่ ก. และ ข. จะ

สื่อสารกันน้อยที่สุดเพื่อให้ ข. ตัดสินใจได้ว่า f เป็นฟังก์ชันชนิดใด

- **เกตลอจิก (Logic gate)**
  หน่วยพื้นฐานที่ประกอบขึ้นเป็นคอมพิวเตอร์ ทำการประมวลผลฟังก์ชัน เช่น AND OR และ NOT
- **เกตลอจิกเชิงควอนตัม (Quantum logic gate)**
  รูปแบบควอนตัมของลอจิกเกตเชิงดิจิทัล เกตลอจิกเชิงควอนตัมจะมีคุณสมบัติย้อนกลับได้ และสามารถประมวลผลสถานะควอนตัมที่มีคุณสมบัติทับซ้อนเชิงตำแหน่งได้
- **ฟังก์ชันคงที่ (Constant function)**
  ฟังก์ชันที่ให้ค่าออกเป็นค่าเดิมเสมอ ไม่ว่าอินพุตจะเป็นอะไร เช่น $f(x)$ เท่ากับ 1 สำหรับค่า x ใด ๆ
- **ฟังก์ชันสมดุล (Balanced function)**
  ฟังก์ชันที่มีการกระจายของผลลัพธ์ 0 และ 1 เป็นจำนวนเท่ากัน คือฟังก์ชันที่ทำให้จำนวนข้อมูลเข้า (x) ที่ทำให้ $f(x)=0$ เท่ากับจำนวนข้อมูลเข้าที่ทำให้ $f(x) = 1$ กรณีเซตของ x เป็น $\{0,1\}$ f มีลักษณะ $f(0)=0, f(1)=1$ หรือ $f(0)=1, f(1)=0$
- **เฟสองค์รวม (Global phase)**
  สำหรับคิวบิต $e^{i\alpha}|\psi\rangle$ เทอม $e^{i\alpha}$ เรียกว่าเฟสองค์รวมซึ่งไม่มีผลเชิงกายภาพ เนื่องจากสถานะควอนตัมแทนด้วย 'รังสี' (“ray”) ซึ่งหมายถึงเวกเตอร์ที่มีแอมปลิจูดเป็นเท่าใดก็ได้
- **วงจรเชิงควอนตัม (Quantum circuit)**
  การเรียงต่อกันของเกตลอจิกเชิงควอนตัม และสถานะควอนตัมขาเข้าและขาออก เพื่อทำหน้าที่คำนวณเชิงควอนตัมหรือแทนการเปลี่ยนแปลงเชิงควอนตัมที่ต้องการ
- **ออราเคิล (Oracle)**
  “กล่องดำ” ที่ทำหน้าที่คำนวณเชิงควอนตัมให้ได้ผลลัพธ์ตามต้องการ โดยสร้างขึ้นจากการนำเกตลอจิกเชิงควอนตัมมาประกอบกันอย่างไรก็ได้ เพื่อให้ได้ผลตามประสงค์
- **แฮมิลโทเนียน (Hamiltonian)**
  ตัวดำเนินการที่ใช้วัดพลังงานของระบบ หรือตัวดำเนินการที่กระทำกับเวกเตอร์สถานะแล้วให้ค่าไอเกนเป็นพลังงาน ตั้งชื่อเป็นเกียรติแก่ วิลเลียม โรวาน แฮมิลตัน (William Rowan Hamilton) นักคณิตศาสตร์ชาวไอร์แลนด์

ข้อสรุปประจำบท (Summary)

Classical computers has been technologically developed by miniaturizing the size of logical operations devices, from large-size relays, vacuum tubes, and transistors to smaller and smaller transistors. However, there is a fundamental limit on physically miniaturizing the transistor size on single atom or electron where the quantum mechanical properties dominate and the fundamental units of information also need to be changed. Classical information -- bits, where information can be either “0” or “1” and can always be copied are invalid to be modeled in quantum systems, where information is in superposition of many states and cannot be copied. The art of processing quantum information in meaningful ways is the topic of quantum computation science. Superposition property of quantum states can be applied to give more information in single processing and result in exponential speed-up in some problems such as determining global characteristic of a function (Deutsch-Jozsa algorithm), factorization of integers (Shor's algorithm) and quadratic speed-up in searching (Grover's algorithm). In quantum computing, information is encoded in quantum states, computation is represented by reversible evolution of the states and readout is done by measuring on the quantum states. Like classical computation, every complex quantum computation is composed of only simple set of operations. Single-qubit reversible transformation and a two-qubit controlled-NOT (CNOT) gate are proved to be fundamental operations for universal quantum computation. Therefore, being able to physically realize single-qubit and CNOT gate in a scalable means result in arbitrary quantum computation. However, one important obstacles of large-scale quantum

computing is the sensitivity of the states to the environments; every quantum system has its own “age” to be able to express full quantum information or quantum coherence. The process destroying meaningful quantum information by interaction with the environments is called “decoherence”. It is proved that there exist the way to reliably protect quantum information from decoherence, by encoding qubit message into larger number of qubits and let them sent into a noisy quantum channel, in the decoding or error-recovering the qubits can be measured to get the error syndrome and the errors can be made to occur at the auxiliary qubits and then be discarded; thus leaving the main qubit containing the information sent. Moreover, even if the quantum gates used to implement quantum error correcting codes themselves are in errors, quantum computation can still be done reliably given that the error in each gates does not exceed a threshold. These tolerance against error in quantum logic operations and the existence of codes protecting quantum information bring about the hope in realization of quantum computers in a large, meaningful scale. The experimental realization in quantum logic gates and quantum algorithms at few number of qubits has been demonstrated in various systems, such as nuclear magnetic resonance (NMR), linear optics, quantum dots, trapped ions and others. The “winning” quantum system to be used as quantum computers is still the question to be explored.

4.1 หน่วยพื้นฐานของการคำนวณเชิงควอนตัม

ในการคำนวณข้อมูลต่างๆ ด้วยวงจรอิเล็กทรอนิกส์หรือคอมพิวเตอร์นั้นต้องอาศัยอุปกรณ์สำหรับการคำนวณ ซึ่งอุปกรณ์ดังกล่าวได้รับการพัฒนาให้มีขนาดเล็กลงเรื่อยๆ จนกระทั่งถึงขีดจำกัดหนึ่งที่อุปกรณ์ต้องคงคุณสมบัติการทำงานรูปแบบเดิมไว้ ทำให้ไม่สามารถมีขนาดเล็กลงมากกว่านั้นได้ หากต้องการให้อุปกรณ์มีขนาดเล็กลงมากกว่านั้น จะต้องใช้การคำนวณในรูปแบบที่แตกต่างจากเดิมเป็นคำนวณในระดับควอนตัม โดยการคำนวณเชิงควอนตัมจะมีข้อมูลแบบบิต “0” และ “1” เกิดได้พร้อมกันเรียกว่าสถานะซ้อนทับทางตำแหน่ง ซึ่งจากคุณสมบัติการซ้อนทับทางตำแหน่งนี้สามารถเพิ่มประสิทธิภาพในการประมวลผลในการแก้ไขปัญหาบางอย่างได้ดีกว่าการประมวลผลด้วยคอมพิวเตอร์ในปัจจุบัน

4.1.1 ประวัติคอมพิวเตอร์... กว่าจะเป็นควอนตัม

ก่อนที่จะมีการประดิษฐ์คอมพิวเตอร์ขึ้นมาใช้งาน ได้มีการนำเสนอถึงรูปแบบการคำนวณ ที่นำไปสู่เครื่องคำนวณ ซึ่งรูปแบบการคำนวณดังกล่าวได้รับการพัฒนาและออกแบบเพื่อให้ใช้งานได้จริง จนกระทั่งเกิดเป็นเครื่องคอมพิวเตอร์ในเวลาต่อมาและเป็นพื้นฐานสำหรับการพัฒนาไปสู่คอมพิวเตอร์เชิงควอนตัม โดยรายละเอียดของรูปแบบการคำนวณและการพัฒนามีดังนี้

4.1.1.1 เครื่องกลทูริง (Turing Machine)

เครื่องจักรกล เครื่องคำนวณเชิงดิจิทัล หรืออุปกรณ์สื่อสารต่างๆ ก่อนจะถึงยุคการผลิตเชิงอุตสาหกรรม ย่อมเริ่มจากการออกแบบ โดยเริ่มจากการออกแบบเชิงหลักการ การออกแบบโดยละเอียด และการสร้างขึ้นจริง แบบจำลองที่ถือว่าเป็นต้นแบบของอุปกรณ์คำนวณเชิงดิจิทัลทุกชนิด เรียกว่า 'เครื่องกลทูริง' หรือแบบจำลองการคำนวณทูริง ซึ่งจัดเป็นแบบจำลองเชิงความคิดของเครื่องคำนวณแบบง่ายเสนอโดย อลัน ทูริง[4.1] (Alan Turing) ในปี ค.ศ. 1937 ดังรูปที่ 4.1

4.1.1.2 นิยามของเครื่องกลทูริง

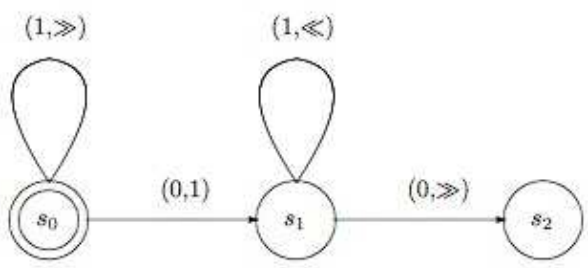
เครื่องกลของทูริง หรือแบบจำลองการคำนวณของทูริง (Turing Machine) เป็นแบบจำลองทางคณิตศาสตร์ ซึ่งอธิบายการทำงานของการคำนวณเชิงดิจิทัลทั้งหมดได้ นับว่าเป็นการออกแบบการทำงานของคอมพิวเตอร์อย่างรัดกุมเป็นครั้งแรก โดยแบบจำลองประกอบด้วย (1) 'เทป' (2) หัวอ่าน (3) กฎเกณฑ์สำหรับการเปลี่ยนแปลง สำหรับแต่ละสถานะเข้า (4) หัวเขียน สำหรับเขียนผลลัพธ์ (Output) โดยเทปมีความยาวไม่จำกัดและภายในแบ่งออกเป็นเซลล์หรือช่องเล็ก ซึ่งโดยแต่ละเซลล์ภายในสามารถบรรจุ

[4.1] นักคณิตศาสตร์ชาวอังกฤษ ซึ่งในสงครามโลกครั้งที่ 2 ได้คิดค้นเครื่องจักรที่ใช้ในการถอดรหัสลับของการส่งข่าวสารระหว่างสงคราม

รูปที่ 4.1 อลัน ทูริง นักคณิตศาสตร์ ชาวอังกฤษ

$<s_0, 1, s_0, » >$
$< s_0, 0, s_1, 1 >$
$< s_1, 1, s_1, « >$
$< s_1, 0, s_2, » >$

(ก)



(ข)

รูปที่ 4.2 แผนภาพลำดับสถานะ การทำงานของเครื่องกลทูริง แบบ 2 สถานะ (ก) ตารางนิยามกฎการเปลี่ยนแปลง (ข) แผนภาพการเปลี่ยนของสถานะ โดยลูกศรแทนทิศการเปลี่ยนสถานะและค่าในวงเล็บ *(input symbol, output symbol)* แทนสัญลักษณ์เข้าที่ทำให้เกิดการเปลี่ยนสถานะ และสัญลักษณ์ใหม่ที่จะถูกเขียนลงบนเทปในเซลล์นั้นๆ รูปดัดแปลงจาก [*StateDiagram.NET*]

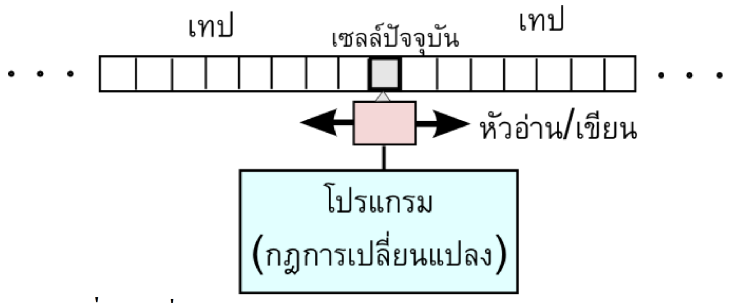
สัญลักษณ์ (Symbol) “0” หรือ “1” ได้ (กรณีใช้สองตัวอักษรต่อหนึ่งสัญลักษณ์) หัวอ่านและเขียนจะทำหน้าที่สแกนสัญลักษณ์นั้นภายใต้ช่วงเวลาใดๆ บนเทปหัวอ่านจะเคลื่อนย้ายไปมาทั้งซ้ายและขวา ขึ้นกับกฎเกณฑ์ที่ระบุไว้ เช่น สถานะเข้า “0” สถานะปัจจุบัน “S_1” ให้เทปเลื่อนไปทางขวา (หรือซ้าย) โดยจะมีการทำงานซ้ำ (อ่าน – เขียนสถานะผลลัพธ์ และเลื่อนเทปเพื่ออ่านสถานะเข้าถัดไป) จนกว่าหัวอ่านจะสแกนเสร็จ หรือไปถึงสถานะสิ้นสุดการทำงาน ในยุคดิจิทัลคอมพิวเตอร์ 'เทป' แทนด้วยหน่วยความจำ (Random Access Memory: RAM) ซึ่งหัวอ่านและเขียนเทป แทนด้วย 'หน่วยประมวลผล' (CPU) และกฎเกณฑ์การเปลี่ยนแปลง แทนด้วย 'โปรแกรม'[4.2] ดังรูปที่ 4.2 และ 4.3

4.1.1.3 กฎการเปลี่ยนแปลง (Transition rules/ Program)

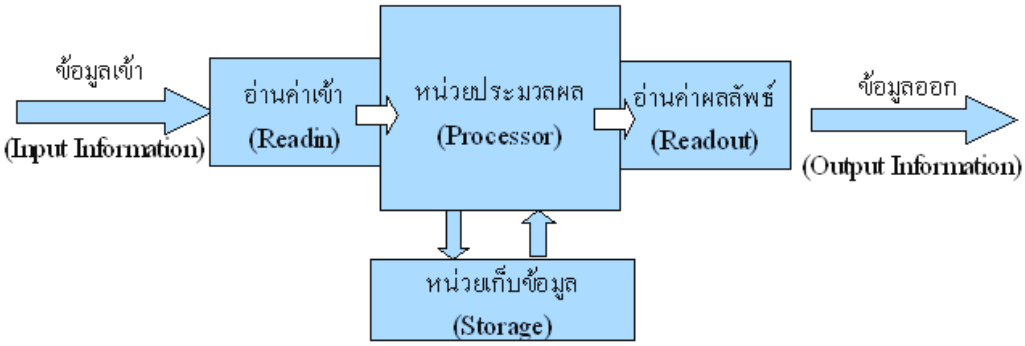
แบบจำลองการคำนวณของทูริงตามรูปที่ 4.2 (ก) แบ่งเป็นสี่ส่วน โดยแทนด้วยจตุอันดับ (4 tuples) <สถานะปัจจุบัน ($State_0$), สัญลักษณ์ (Symbol), สถานะถัดไป ($State_{Next}$), การกระทำ (Action)> ซึ่งหมายถึง “ถ้าสถานะปัจจุบัน = $State_0$ และสถานะเข้า = Symbol ให้เลื่อนสถานะไปสู่ $State_{Next}$ และมี 'การกระทำ' เกิดขึ้น” โดยกฎการเปลี่ยนแปลงนี้จะเก็บไว้เป็นตารางซึ่งโยงระหว่างสถานะปัจจุบัน สถานะเข้า (Symbol) ไปยังสถานะถัดไป และการกระทำ หมายถึงการเขียนสัญลักษณ์ใหม่ {0, 1, <<, >>}[4.3] ลงบนเทปในเซลล์ภายใต้ช่วงเวลานั้นๆ

[4.2] ในแบบจำลองการคำนวณของฟอน นอยมานน์ โปรแกรมและสัญลักษณ์ถูกเก็บไว้ที่เดียวกัน (ในสิ่งที่เรียกว่า 'เทป') ซึ่งเป็นแบบจำลองของดิจิทัลคอมพิวเตอร์ในปัจจุบัน

[4.3] สัญลักษณ์ '<<' หมายถึง ให้เลื่อนเทปไปทางซ้าย และ '>>' หมายถึง ให้เลื่อนเทปไปทางขวา



รูปที่ 4.3 เครื่องกลของทูริง หรือแบบจำลองการคำนวณของทูริง



รูปที่ 4.4 กระบวนการพื้นฐานของคอมพิวเตอร์

4.1.1.4 หลักการทำงานแบบง่ายของแบบจำลองทูริง

สิ่งที่ทำให้แบบจำลองการคำนวณของทูริงทำการคำนวณได้ คือ 'กฎการเปลี่ยนแปลง' ซึ่งทำงานเหมือนโปรแกรมของเครื่อง นอกจากนี้ต้องกำหนด 'สถานะเริ่มต้น' ของหัวอ่านก่อนเริ่มรับสัญลักษณ์เข้า (Input) จากรูปที่ 4.2 สถานะถูกแทนด้วยรูปวงกลม และวงกลมที่ซ้อนทับกันกำหนดให้เป็นสถานะเริ่มต้น การเปลี่ยนแปลงจากสถานะหนึ่งไปสู่อีกสถานะหนึ่งนั้นจะแทนด้วยลูกศร โดยตรงหัวลูกศรจะเป็นสถานะที่เกิดการเปลี่ยนแปลงแล้ว ส่วนสัญลักษณ์ตามรูป สัญลักษณ์แรกในวงเล็บของทุกวงเล็บบอกถึงการอ่านของหัวอ่าน ณ ขณะนั้น ส่วนสัญลักษณ์ที่สองในวงเล็บบอกถึงการเกิดการปฏิบัติการหรือเกิดการเขียนของหัวอ่าน ณ ขณะนั้น ซึ่งการทำงานของแบบจำลองทูริงนี้จะทำงานไล่ไปเป็นลำดับจากสถานะเริ่มต้นจนสิ้นสุดการทำงานที่สถานะสุดท้าย

ดังนั้นแบบจำลองการคำนวณของทูริงจึงเป็นแบบจำลองพื้นฐานที่มีคำจำกัดความอย่างชัดเจน และเมื่อรวมกับแบบจำลองของฟอน นอยมานน์ (Von Neumann) คือ ยุบส่วนโปรแกรมไปไว้กับข้อมูลในเทป ทำให้สามารถสร้างคอมพิวเตอร์ขึ้นจริงจากแบบจำลองดังกล่าวได้ และเป็นแบบจำลองที่ใช้อยู่จนในดิจิทัลคอมพิวเตอร์ปัจจุบันดังรูปที่ 4.4

4.1.1.5 ประเภทของคอมพิวเตอร์

คอมพิวเตอร์ (Computer) หมายถึง เครื่องจักรที่สามารถตั้งโปรแกรมได้ ประมวลผล เรียก และเก็บข้อมูลได้ [*Britannica 2008*] คอมพิวเตอร์เรียกอีกอย่างหนึ่งว่า เครื่องคำนวณ (Computing machine) ซึ่งหมายถึงระบบทางกายภาพในธรรมชาติ ซึ่งการเปลี่ยนแปลงของระบบสามารถมองได้ว่าเป็นกระบวนการคำนวณ [*Deutsch 1989*] ชนิดของคอมพิวเตอร์สามารถแบ่งตามปริมาณสารสนเทศที่นำมาเป็นข้อมูลเข้า และข้อมูลออก ดังตารางที่ 4.1

ตารางที่ 4.1 เปรียบเทียบชนิดของคอมพิวเตอร์

ประเภทของคอมพิวเตอร์	หน่วยสารสนเทศที่เล็กที่สุด	ชนิดข้อมูลที่ถูกประมวลผล	ฟิสิกส์ที่นำมาอธิบาย	ตัวอย่าง
แอนะลอกคอมพิวเตอร์	จำนวนจริง	ค่าต่อเนื่อง	ฟิสิกส์ดั้งเดิม	แรงดันอากาศ ศักย์ไฟฟ้าที่ต่อเนื่อง
ดิจิทัลคอมพิวเตอร์	“0” หรือ “1”	ค่าไม่ต่อเนื่อง	ฟิสิกส์ดั้งเดิม และฟิสิกส์กึ่งดั้งเดิม (Semi-classical physics)	คอมพิวเตอร์ตั้งโต๊ะ เครื่องคิดเลข โทรศัพท์เคลื่อนที่
คอมพิวเตอร์เชิงควอนตัม	$\alpha\|0\rangle+\beta\|1\rangle$ โดยที่ α และ β เป็นจำนวนเชิงซ้อน $\|\alpha\|^2+\|\beta\|^2=1$	เวกเตอร์จำนวนเชิงซ้อน	ฟิสิกส์ควอนตัม	โฟตอน อะตอม อิเล็กตรอน

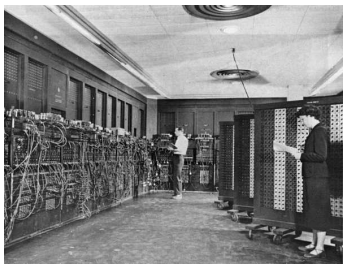
- คอมพิวเตอร์ดั้งเดิม

คอมพิวเตอร์ดั้งเดิม[4.4] อธิบายได้ด้วยฟิสิกส์ดั้งเดิม โดยเป็นการใช้สิ่งที่มีอยู่ทางกายภาพ มาเป็นตัวแทนในการประมวลผลข้อมูล ซึ่งปริมาณข้อมูลพื้นฐานสำหรับคอมพิวเตอร์ดั้งเดิมมีสองแบบ คือ ค่าเป็นจำนวนจริง (ค่าต่อเนื่อง) เรียกเครื่องประมวลผลสำหรับปริมาณดังกล่าวว่า *แอนะลอกคอมพิวเตอร์* (Analog computers) และปริมาณพื้นฐานอีกแบบหนึ่งเป็นค่าจำนวนเต็ม (ค่าไม่ต่อเนื่อง) เรียกอุปกรณ์สำหรับประมวลผลค่าไม่ต่อเนื่องดังกล่าวว่า *ดิจิทัลคอมพิวเตอร์* (Digital computers)

- แอนะลอกคอมพิวเตอร์ หมายถึง สิ่งที่ใช้ปริมาณที่มีค่าต่อเนื่องในธรรมชาติมาแทนสารสนเทศที่ต้องการคำนวณ เช่นศักย์ไฟฟ้า แรงดันของเหลว การเคลื่อนไหวเชิงกล และการเปลี่ยนแปลงทางกายภาพที่กำหนดเองแทนการคำนวณ แอนะลอกคอมพิวเตอร์เหมาะกับการใช้จำลองระบบพลวัต ซึ่งสามารถประมวลผลได้แบบเวลาจริง(Real time) มักนำมาใช้จำลองการทำงานของเครื่องบิน โรงไฟฟ้าพลังงานนิวเคลียร์ กระบวนการทางเคมีอุตสาหกรรม เป็นต้น [*Britannica 2008*] แอนะลอกคอมพิวเตอร์สามารถแทนตัวเลขได้ละเอียดอย่างไม่มีข้อจำกัด เพราะเป็นค่าต่อเนื่อง แต่ไม่สามารถตรวจสอบและแก้ไขความผิดพลาดอันเนื่องมาจากสัญญาณรบกวนได้ (ในขณะที่ดิจิทัลคอมพิวเตอร์ทำได้)
- ดิจิทัลคอมพิวเตอร์ หมายถึง อุปกรณ์ที่ใช้สถานะของระบบในธรรมชาติสองสถานะพื้นฐานมาแทนสารสนเทศ “0” และ “1” และการเปลี่ยนแปลงของระบบภายใต้เวลาแทนการประมวลผล อาศัยเกตลอจิก (Logic gate) จำนวนหนึ่งมาประกอบกันเพื่อทำหน้าที่คำนวณตามความประสงค์ เครื่องคอมพิวเตอร์ที่ใช้กันในสำนักงานนั้นจัดเป็นดิจิทัลคอมพิวเตอร์ เกตลอจิกจะทำงานโดยอาศัยคุณสมบัติของทรานซิสเตอร์ที่ควบคุมการเปิด-ปิดของวงจรด้วยการกำหนดค่าของกระแสไฟฟ้าหรือแรงดันไฟฟ้า

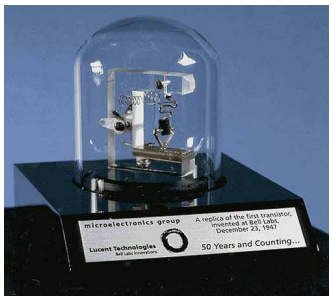
[4.4] ณ ที่นี้ หมายถึง ดิจิทัลคอมพิวเตอร์ เนื่องจากหน่วยพื้นฐานของการคำนวณ (บิต) มีลักษณะใกล้เคียงกับ 'คิวบิต' ของการคำนวณเชิงควอนตัม

(ก.1)

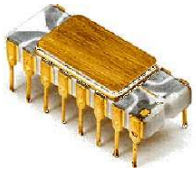


(ข.1)

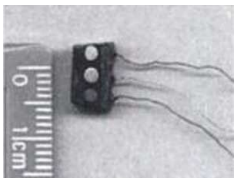
(ค)



(ก.2)



(ข.2)



(ก.3)

(ข.3)

รูปที่ 4.5 หน่วยย่อยของคอมพิวเตอร์ดั้งเดิม (ก) หน่วยย่อยของอุปกรณ์คำนวณ (ก.1) หลอดสูญญากาศที่ประดิษฐ์โดยลี เดอ ฟอเรสต์ (Lee de Forest) ในปี ค.ศ. 1907 [*Gurevich 2006*] (ก.2) ทรานซิสเตอร์เลียนแบบทรานซิสเตอร์ตัวแรกในปี ค.ศ. 1947 โดยบริษัท Lucent Technologies และ (ก.3) ทรานซิสเตอร์ระดับอุตสาหกรรมตัวแรกโดยห้องทดลองของเบลล์ (Bell Laboritories) ในปี ค.ศ. 1951 [*Gurevich 2006*] (ข.1) ENIAC เครื่องคอมพิวเตอร์เครื่องแรกของโลก (ข.2) ไมโครโปรเซสเซอร์ 4 บิต รุ่น Intel 4004 [*Stassen 1997*] (ข.3) คอมพิวเตอร์ส่วนบุคคลประเทศรัสเซียรุ่น DVK-3 (ค) ตัวอย่างอุปกรณ์คำนวณช่วง ค.ศ. 1995 - 2009

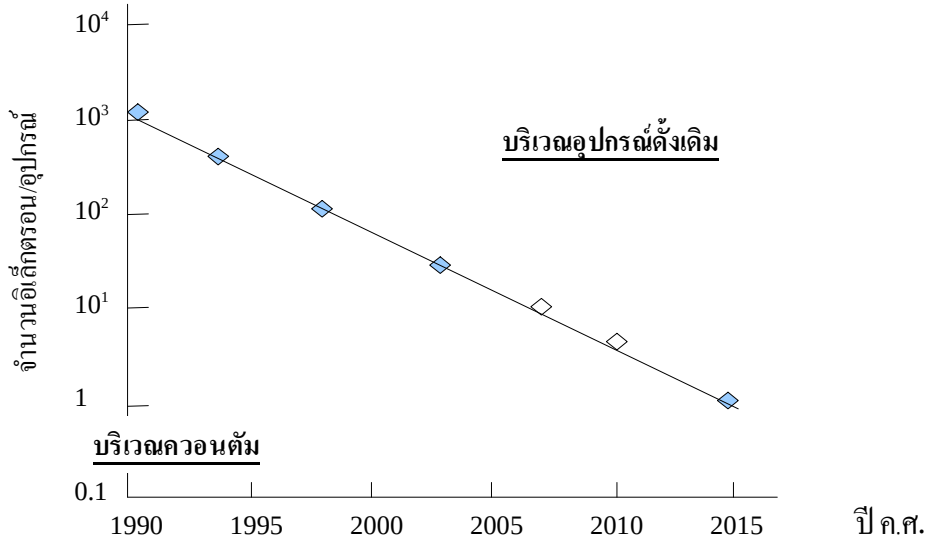
- **คอมพิวเตอร์เชิงควอนตัม**

คอมพิวเตอร์เชิงควอนตัม[4.5] หมายถึง สิ่งในธรรมชาติที่อธิบายด้วยกลศาสตร์ควอนตัม และทำหน้าที่ประมวลผลข้อมูลที่มีหน่วยย่อยเรียกว่า คิวบิต คือ ผลรวมของสถานะ “0” และ “1” ด้วยสัมประสิทธิ์เป็นจำนวนเชิงซ้อน อาศัยคุณสมบัติของฟิสิกส์ควอนตัมเช่นความทับซ้อนเชิงตำแหน่งและคุณสมบัติพัวพันระหว่างสถานะ ทำให้มีคุณลักษณะใหม่ๆ และโดดเด่นในการคำนวณความเร็วที่สูงขึ้นมาก ซึ่งต่างจากการคำนวณแบบดั้งเดิม

4.1.2 วิวัฒนาการของคอมพิวเตอร์

นับตั้งแต่คริสต์ศตวรรษที่ 20 เป็นต้นมามุมมองการพัฒนาของคอมพิวเตอร์ดั้งเดิมมีสองด้าน คือด้านสถาปัตยกรรม ซึ่งมีรากฐานมาจากแบบจำลองเครื่องคำนวณอเนกประสงค์ (Universal Computing Machine) ของทูริง แนวคิดการรวมรหัสโปรแกรม

[4.5] ในที่นี้หมายถึง การคำนวณเชิงควอนตัมด้วยสถานะควอนตัมไม่ต่อเนื่อง (Discrete quantum states) เท่านั้น ส่วนการคำนวณเชิงควอนตัมด้วยสถานะต่อเนื่อง (Continuous-variable quantum computing) [*Braunstein และ van Loock 2005*] อยู่นอกขอบเขตของเนื้อหา



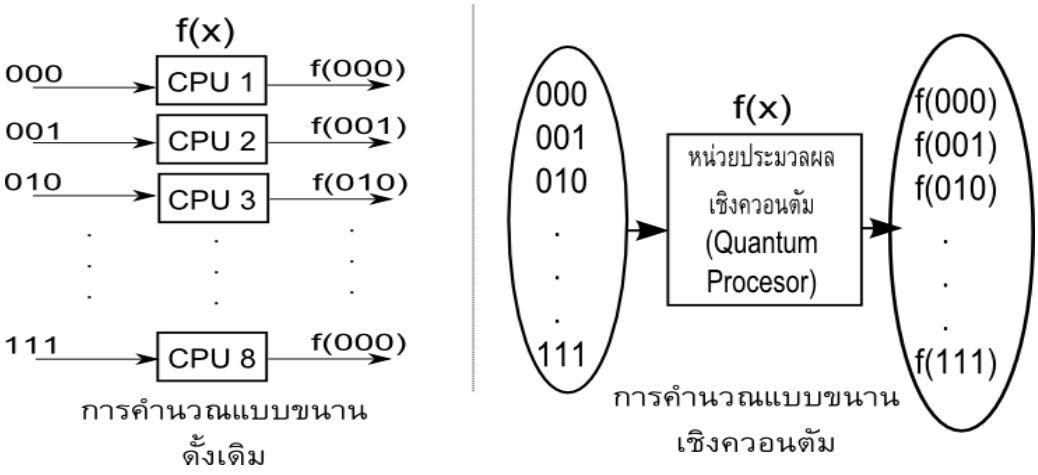
รูปที่ 4.6 กราฟกฎของมัวร์ หากกฎของมัวร์ยังเป็นจริงต่อไปอุปกรณ์ลอจิกในปี ค.ศ.2015 จะมีอิเล็กตรอนเพียง 1 ตัว และต้องอธิบายด้วยกลศาสตร์ควอนตัม

เข้ากับส่วนของข้อมูลโดย ฟอน นอยมานน์ (von Neumann) และวิธีการเชิงทฤษฎีวิธีการสร้างเกตลอจิกด้วยรีเลย์โดย เชสตาคอฟ (Shestakov) แชนนอน (Shannon) และ นากาชิมา (Nakashima) [*Reilly 2003*] และจากหลักการเดียวกันมีการวิวัฒนาการไปสู่การใช้หลอดสูญญากาศและทรานซิสเตอร์ในที่สุด โดยมีการพัฒนาบนพื้นฐานเดิม แต่เป็นการลดขนาดหน่วยเก็บข้อมูลและปรับปรุงการประมวลผลให้ดีขึ้น (optimization) ในลำดับการทำงาน รวมทั้งเพิ่มหน่วยประมวลผลย่อยๆ มาร่วมทำงานขนานกันไป โดยมีชื่อเรียกต่างๆ ตามโครงสร้าง ขนาด และวัตถุประสงค์ของการทำงาน เช่น ซูเปอร์คอมพิวเตอร์ (Supercomputers) [*Adiga และคณะ 2002*] คอมพิวเตอร์แบบคลาวด์หรือก้อนเมฆ (Cloud computers) [*Buyya และคณะ 2008*] และคอมพิวเตอร์แบบกริด (Grid computers) [*Foster และคณะ 2008*] เป็นต้น

อีกด้านหนึ่งคือด้านเทคโนโลยี ซึ่งช่วยในการเพิ่มความจุข้อมูลสำหรับอุปกรณ์ที่มีขนาดเท่าเดิม โดยการลดขนาดของทรานซิสเตอร์ลงเรื่อยๆ ด้วยวิธีการต่างๆ ทำให้เกิดการเพิ่มทั้งประสิทธิภาพ ความเร็วในการคำนวณและข้อดีอื่นๆ ตามมา อย่างไรก็ตามการลดขนาดของทรานซิสเตอร์ลงจนถึงจุดหนึ่งจะมีข้อจำกัดเนื่องจากขนาดจะเล็กลงจนเข้าสู่ขนาดของอะตอมในที่สุด (ดังรูปที่ 4.6) ฟิสิกส์ดั้งเดิมและกึ่งดั้งเดิมที่ใช้อธิบายคุณสมบัติของสารกึ่งตัวนำและทรานซิสเตอร์จะไม่สามารถอธิบายได้ต่อไป ดังนั้นกลศาสตร์ควอนตัมจึงต้องเข้ามาอธิบายแทน อีกทั้งปริมาณสารสนเทศพื้นฐานยังต้องเปลี่ยนแปลงเนื่องจากคุณสมบัติทางควอนตัมฟิสิกส์นั่นเอง จากหน่วยของบิตคือ “0” หรือ “1” กลับกลายเป็นผลรวมของสองสถานะ “0” และ “1” ในรูปสัมประสิทธิ์ที่บ่งบอกความน่าจะเป็นที่จะตรวจวัดได้สถานะนั้นๆ แทน

นอกจากคอมพิวเตอร์ที่ผลิตจากอุปกรณ์อิเล็กทรอนิกส์ (ใช้กระแสไฟฟ้า ทรานซิสเตอร์ และวงจรรวม) แล้ว ยังมีการเสนอธรรมชาติอย่างอื่นมาทำหน้าที่คำนวณได้เช่นกัน เช่น คอมพิวเตอร์จากดีเอ็นเอ (DNA computers) [*Liu และคณะ 2008*] คอมพิวเตอร์เชิงแสง (Optical computers) [*Lohmann 1986*] ซึ่งล้วนเหมือนกันในเชิงข้อมูล (ดิจิทัล/แอนะลอก) เช่นคุณสมบัติการคัดลอกได้ (เช่นการคัดลอกดีเอ็นเอ) การวัดค่าได้โดยไม่กระทบต่อข้อมูลนั้นๆ ทว่ามีอุปกรณ์คำนวณที่ต่างกันอย่างสิ้นเชิงกับคอมพิวเตอร์ต่างๆ ดังกล่าวตั้งแต่โครงสร้างพื้นฐานของข้อมูลกระบวนการคำนวณ วิธีการสร้างและอื่นๆ ที่เป็นไปภายใต้กลศาสตร์ควอนตัม เรียกว่าคอมพิวเตอร์เชิงควอนตัม[4.6]

[4.6] ในคอมพิวเตอร์เชิงควอนตัม ข้อมูล หรือสถานะควอนตัมที่ไม่ทราบค่า ไม่สามารถถูกคัดลอกโดยสมบูรณ์ได้ แต่ในคอมพิวเตอร์ดั้งเดิม เช่น ดิจิทัลคอมพิวเตอร์หรือดีเอ็นเอคอมพิวเตอร์ ข้อมูลถูกคัดลอกได้อย่างสมบูรณ์



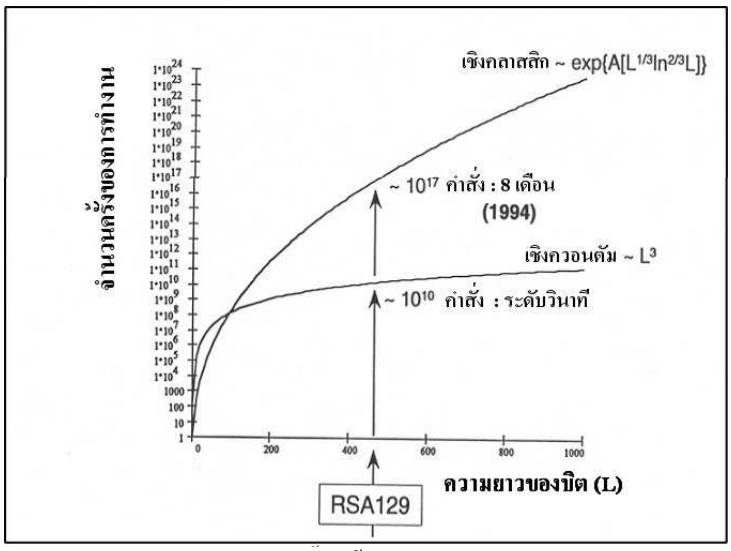
รูปที่ 4.7 เปรียบเทียบการทำงานของคอมพิวเตอร์ดั้งเดิมและ ควอนตัมคอมพิวเตอร์ – คอมพิวเตอร์ดั้งเดิม หน่วยประมวลผลหนึ่งตัวประมวลข้อมูลได้หนึ่งชุด ส่วนหน่วยประมวลผลเชิงควอนตัมหนึ่งหน่วย มีการประมวลผลต่อข้อมูลเข้าทุกตัวในเวลาเดียวกัน

รูปที่ 4.8 ริชาร์ด ฟายน์แมน

4.1.3 พื้นฐานควอนตัมคอมพิวเตอร์

คอมพิวเตอร์ดั้งเดิมทั้งหลายใช้การประมวลผลเดียวหรือแบบขนานโดยใช้หน่วยประมวลผลหลายตัวมาร่วมกันด้วยสถาปัตยกรรมแบบต่างๆ ในการเพิ่มประสิทธิภาพของการคำนวณ คอมพิวเตอร์เชิงควอนตัมอาศัยคุณสมบัติทางฟิสิกส์ควอนตัมมาเพิ่มประสิทธิภาพหรือเพิ่มคุณสมบัติใหม่ในการคำนวณ โดยไม่ได้เพิ่มหน่วยประมวลผล เช่นกระบวนการประมวลผลแบบขนานที่ใช้การเปลี่ยนแปลงทางฟิสิกส์ซึ่งแทนหน่วยประมวลผลควอนตัมเพียงหนึ่งกระบวนการ (Quantum processor หนึ่งหน่วย ดังรูปที่ 4.7 ขวามือ) แทนที่จะใช้หลายหน่วยเหมือนอย่างการคำนวณแบบดั้งเดิม (รูปที่ 4.7 ซ้ายมือ)

การประมวลผลแบบขนานด้วยคอมพิวเตอร์ดั้งเดิม ในการคำนวณค่า $f(x)$ ของ x ซึ่งมีค่าตั้งแต่ “000” ถึง “111” ต้องใช้หน่วยประมวลผลย่อย 8 ตัว ในการคำนวณขนานกันถึงจะให้คำตอบออกมาพร้อมกัน ส่วนควอนตัมคอมพิวเตอร์ ใช้หลักการทับซ้อนเชิงตำแหน่งของสถานะตั้งแต่ “000” ถึง “111” โดยมีหน่วยประมวลผล คือ การเปลี่ยนแปลงทางกายภาพ (Dynamics) เพียงหน่วยเดียวในการคำนวณ ซึ่งจะได้ $f(x)$ ออกมาพร้อมกัน



รูปที่ 4.9 กราฟของเวลาที่ใช้แยกตัวประกอบ ตามวิธีดั้งเดิมและวิธีเชิงควอนตัม โดยพิจารณาที่รหัส RSA129 วิธีดั้งเดิมใช้เวลา 8 เดือน ส่วนวิธีเชิงควอนตัมใช้เวลาเพียงหลักวินาที ด้วยคอมพิวเตอร์ในยุคปี ค.ศ. 1994 [รูปดัดแปลงจาก *presentation ของ Tony Hey "Quantum Computing: Progress and Prospects" 2001*]

ในปี ค.ศ. 1981 ริชาร์ด ฟายน์แมน (Richard Feynman) นักวิทยาศาสตร์รางวัลโนเบลสาขาฟิสิกส์ (ปี ค.ศ. 1965) ทางด้านพลศาสตร์ไฟฟ้าควอนตัม (Quantum electrodynamics) เสนอว่าคอมพิวเตอร์เชิงควอนตัมเท่านั้นที่จะจำลองการทำงานของระบบควอนตัมได้อย่างมีประสิทธิภาพ[4.7] [*Feynman 1982*] และในช่วงเวลาเดียวกัน พอล เบนิออฟฟ์ (Paul Benioff) [*Benioff 1982*] พิสูจน์ว่ากลศาสตร์ควอนตัม สามารถจำลองหรืออธิบายการทำงานของเครื่องกลทูริงได้ ซึ่งแปลว่าควอนตัมคอมพิวเตอร์มีความสามารถในการคำนวณไม่น้อยไปกว่าเครื่องกลทูริง [*Cirasella 2008*] แต่ยังไม่มีการพิสูจน์ว่าปัญหาใดบ้างที่คอมพิวเตอร์เชิงควอนตัมจะแก้ปัญหาได้ดีกว่าคอมพิวเตอร์ดั้งเดิม ในปี ค.ศ. 1985 เดวิด ดอยช์ (David Deutsch) เสนอแบบจำลองเครื่องคำนวณอเนกประสงค์ในรูปแบบควอนตัม หรือเรียกอีกอย่างว่าเครื่องคำนวณอเนกประสงค์เชิงควอนตัม (Universal quantum computer) [*Deutsch 1985*] ซึ่งเป็นแนวคิดที่ค่อนข้างเป็นนามธรรม และในปี ค.ศ. 1989 ดอยช์ เสนอแบบจำลอง "วงจรเชิงควอนตัม" (Quantum circuits) ซึ่งทำงานได้เช่นเดียวกับเครื่องคำนวณอเนกประสงค์เชิงควอนตัมทุกประการ [*Deutsch 1989*] และ ค.ศ. 1992 เดวิด ดอยช์ และริชาร์ด จอสซา (Richard Josza) แสดงให้เห็นตัวอย่างปัญหาอย่างง่ายที่คอมพิวเตอร์เชิงควอนตัมแก้ได้เร็วกว่าในอันดับเอกซ์โพเนนเชียล [*Deutsch & Jozsa 1992*] โดยอาศัยคุณสมบัติการทับซ้อนเชิงตำแหน่ง แต่โจทย์ปัญหาดังกล่าวเป็นปัญหาคณิตศาสตร์พื้นฐานด้านการวิเคราะห์คุณลักษณะของฟังก์ชันว่าเป็นฟังก์ชันคู่หรือฟังก์ชันคี่ซึ่งไม่ได้มีความสำคัญกับชีวิตจริง จึงเป็นไม่เป็นที่สนใจนัก

จนกระทั่งปี ค.ศ.1994 แดเนียล ไซมอน (Daniel Simon) เสนอขั้นตอนวิธีวิเคราะห์คุณลักษณะความเป็นคาบของฟังก์ชัน [*Simon 1994*] อันทำให้ปีเตอร์ ชอร์ (Peter Shor) นำมาต่อยอดไปสู่การค้นพบวิธีแยกตัวประกอบด้วยการคำนวณเชิงควอนตัมในปีเดียวกัน [*Shor 1994*] ซึ่งโดยหลักการแล้วสามารถนำไปถอดรหัสที่เข้ารหัสด้วยกุญแจสาธารณะ[4.8] (Public key cryptography) ด้วยความเร็วที่เพิ่มตามจำนวนบิตของตัวเลขยกกำลังสาม แทนที่จะเป็นเอกซ์โพเนนเชียล นอกเหนือจากนี้ในปี ค.ศ. 2007 ได้มีการค้นพบวิธีแยกตัวประกอบแบบดั้งเดิมที่สามารถแยกตัวประกอบของจำนวนมหาศาลเช่น 2^{1039}-1 อย่างมีประสิทธิภาพ โดยทดลองแล้วหาผลลัพธ์ได้ในเวลา 1.8 ชั่วโมง ด้วยเครื่องคอมพิวเตอร์รุ่น Opteron 2.2 GHz แม้ว่าวิธีแยกตัวประกอบของจำนวน 2^{1039}-1 จะยังคงอิงคุณสมบัติเฉพาะของตัวเลขนี้ ซึ่งการแยกตัวประกอบของ RSA 1024 บิต ยังคงทำได้ยากกว่าด้วยวิธีเดียวกัน แต่ก็เป็นก้าวหนึ่งที่แสดงให้เห็นว่าความปลอดภัยของรหัส RSA ไม่มีความมั่นคงหากมีการค้นพบขั้นตอนวิธีใหม่ๆ ขึ้นมา [*Aoki และคณะ 2007*]

4.7 แท้จริงแล้วยู มานิน (Yu Manin) ได้เสนอแนวคิดนี้ไว้ก่อนแล้วในปี ค.ศ.1980 เป็นภาษารัสเซีย แต่ทั่วโลกไม่มีใครทราบในเวลานั้น [*Manin 1980*]

4.8 ทั้งวิธี RSA ซึ่งอิงอาศัยการแยกตัวประกอบ และวิธีเส้นโค้งเชิงวงรีที่อิงอาศัยขั้นตอนวิธีไม่ต่อเนื่อง

การวิจัยด้านการคำนวณเชิงควอนตัมได้รับความสนใจเพิ่มขึ้นเป็นอย่างมากนับจากมีการค้นพบขั้นตอนวิธีแบบชอร์ และการเข้ารหัสโดยอาศัยความซับซ้อนทางคณิตศาสตร์จึงไม่น่าไว้ใจอีกต่อไป และงานวิจัยทางด้านการเข้ารหัสที่อาศัยคุณสมบัติทางกลศาสตร์ควอนตัมมาช่วยในการกระจายกุญแจแทนที่จะใช้ความซับซ้อนทางคณิตศาสตร์เพียงอย่างเดียวจึงได้รับความสนใจมากขึ้นในเวลาเดียวกัน โดยมีการเสนอไว้อย่างเป็นทางการตั้งแต่ช่วงปี ค.ศ. 1970-1984 โดยสตีเฟน วีส์เนอร์ (Stephen Wiesner) ชาร์ลส์ เบนเนต (Charles Bennett) และ จิลส์ บราสซาร์ด (Gilles Brassard) ค.ศ. 1996 ลอฟ กรอฟเวอร์ (Lov Grover) ค้นพบกระบวนวิธีเชิงควอนตัมสำหรับค้นหาข้อมูลที่ไม่จัดลำดับด้วยเวลาที่เร็วขึ้นจากวิธีเชิงดิจิทัลใช้เวลา N เป็น $\sqrt{N}$ เมื่อ N แทนจำนวนข้อมูล นับเป็นอีกตัวอย่างหนึ่งที่การคำนวณทางควอนตัมสามารถแก้ปัญหาได้เร็วกว่าคอมพิวเตอร์ดั้งเดิม

คอมพิวเตอร์เชิงควอนตัมมีการทำงานตามหลักความน่าจะเป็น กล่าวคือการแก้โจทย์ปัญหาอาจไม่ประสบความสำเร็จทุกครั้ง หากแต่มีความน่าจะเป็นสูงที่จะประสบความสำเร็จ และอาศัยการตรวจความถูกต้องของคำตอบที่ใช้เวลาน้อย (โพลิโนเมียล) จึงสามารถทำงานซ้ำๆ จนได้คำตอบที่ถูกต้องได้ [*Preskill 1998*] เช่น การแยกตัวประกอบตามวิธีของชอร์ก็อาจไม่สำเร็จทุกครั้ง เช่น ทราบจำนวนที่เป็นผลคูณของ a และ b การหาค่าของ a และ b คือการแยกตัวประกอบ แต่การตรวจสอบ คือ การคูณสองจำนวนว่ามีค่าตรงกับจำนวนที่ต้องการแยกตัวประกอบ เช่น ทราบค่าจำนวน a และ b สามารถหาค่า $a \times b$ ได้หรือไม่นั้น ทำได้รวดเร็ว

4.1.4 ภาพรวมของการประมวลผลสารสนเทศเชิงควอนตัม

การประมวลผลสารสนเทศเชิงควอนตัมเป็นการใช้เทคโนโลยีทางควอนตัมมาประยุกต์สำหรับการประมวลผลด้านต่างๆ เพื่อให้มีประสิทธิภาพสูงกว่าการประมวลผลในปัจจุบัน

4.1.4.1 ความน่าสนใจของคอมพิวเตอร์เชิงควอนตัมและสารสนเทศเชิงควอนตัม

เมื่ออาศัยคุณสมบัติของกลศาสตร์ควอนตัมเพื่อการประมวลผลและการใช้งานด้านต่างๆ จะช่วยให้ได้คุณลักษณะใหม่ๆ ที่เป็นประโยชน์ เช่น ด้านความปลอดภัยข้อมูล การจำลองพฤติกรรมของอนุภาค และการเพิ่มความละเอียดในเทคโนโลยีการวัด

- **ด้านความปลอดภัยของข้อมูล**
  - การแยกตัวประกอบ – ถอดรหัสกุญแจสาธารณะ

    วิทยาการเข้ารหัสเพื่อความปลอดภัยของข้อมูลแบ่งเป็นสองวิธีหลักๆ คือ วิธีใช้กุญแจเดียว (Secret key) และแบบสองกุญแจ (Public key และ Private key) การเข้ารหัสแบบสองกุญแจอาศัยความซับซ้อนในคำนวณ ซึ่งทิศทางหนึ่งคำนวณยาก เช่น การแยกตัวประกอบ แต่อีกทิศทางคำนวณได้ง่าย เช่น การคูณจำนวนเต็ม โดยมีหลักการคือเวลาที่ใช้ในการคำนวณที่ผู้ดักจับต้องใช้ถอดรหัสจะต้องมากกว่าเวลาที่สารสนเทศนั้นมีมูลค่า เช่น ข่าวสารหนึ่งมีคุณค่าเป็นระยะเวลา 6 เดือน เวลาที่ผู้ดักจับต้องใช้ในการคำนวณเพื่อถอดรหัสจะต้องมากกว่า 6 เดือน จึงถือได้ว่ารหัสนั้นปลอดภัย โดยสร้างปัญหาที่ต้องแก้ด้วยระยะเวลาเพิ่มเป็นเอกซ์โพเนนเชียลตามขนาดข้อมูล เช่น การแยกตัวประกอบจำนวนเฉพาะ ซึ่งวิธีการสร้างความปลอดภัยในลักษณะดังกล่าวสามารถทำได้ไม่ยาก แต่จากการค้นพบวิธี “แยกตัวประกอบเชิงควอนตัม” ของชอร์ ทำให้เวลาที่ใช้ในการถอดรหัสแยกตัวประกอบดังกล่าวลดลงจากอันดับเอกซ์โพเนนเชียลเป็นโพลิโนเมียล และเวลาที่ใช้ในการถอดรหัสจะต่างกันโดยสิ้นเชิง เช่น จาก 8 เดือน อาจลดเหลือระดับวินาที เป็นต้น ซึ่งส่งผลถึงความปลอดภัยของข้อมูลได้
  - โปรแกรมควอนตัม (ไม่สามารถละเมิดลิขสิทธิ์ เพราะใช้แล้วต้องทิ้ง)

    สถานะเชิงควอนตัมเมื่อถูกอ่านค่า สถานะจะถูกปรับให้อยู่ในเซตของผลลัพธ์ที่เป็นไปได้ตามแนวที่ถูกอ่านค่านั้น ด้วยเหตุนี้ หากแทนรหัสต้นฉบับ (Source code) โปรแกรมด้วยสถานะเชิงควอนตัม หลังจากเรียกโปรแกรมทำงานครั้งหนึ่ง ต้องมีการอ่านค่าและประมวลผลอันทำให้สถานะซึ่งแทนรหัสต้นฉบับของโปรแกรมเปลี่ยนแปลงไป จึงนำไปใช้ซ้ำไม่ได้ และเลียนแบบไม่ได้เช่นกัน [*Preskill 1999*]

➢ เงินควอนตัม (ทำธนบัตรปลอมไม่ได้)

วีส์เนอร์ (Wiesner) เสนอการใช้สถานะควอนตัมที่ไม่ตั้งฉากกันมาแทนตัวเลข เช่นเลขรหัสธนบัตร ซึ่งจะไม่สามารถทำปลอมได้ เนื่องจากการอ่านค่าสถานะควอนตัมทำให้สถานะยุบตัวลงสู่ค่าในแนวที่ถูกวัดนั้น สถานะควอนตัมที่ไม่ทราบค่าไม่สามารถคัดลอกได้ [*Wiesner 1983*] ซึ่งเป็นแนวคิดที่พัฒนาสู่วิทยาการรหัสลับเชิงควอนตัม

➢ การกระจายกุญแจรหัสลับด้วยหลักกลศาสตร์ควอนตัม

เบนเนต และบราสซาร์ด นำแนวคิดของ วีส์เนอร์ มาใช้ในการตกลงกุญแจรหัสลับร่วมกัน (Secret key agreement) ระหว่างคู่สื่อสาร โดยอาศัยการแทนค่าตัวเลขด้วยสถานะควอนตัมที่ตั้งฉากและไม่ตั้งฉากกัน โดยการดักจับใดๆ จะทำให้สถานะเปลี่ยนไปจนตรวจสอบได้ที่ปลายทางซึ่งมีการกระจายตัวของความน่าจะเป็นของผลลัพธ์เปลี่ยนไป [*Bennett & Brassard 1984*]

- **การจำลองการเปลี่ยนแปลงของอนุภาค**

ฟายน์แมนเสนอว่า การจำลองระบบเชิงควอนตัมด้วยคอมพิวเตอร์ปกติจะใช้จำนวนขั้นตอน (หรือเวลา) ในการทำงานเพิ่มเป็นเอกซ์โพเนนเชียลตามขนาดของระบบนั้น สำหรับระบบควอนตัมหนึ่งซึ่งต้องอาศัยคอมพิวเตอร์เดิมขนาด 1 ล้านล้านบิต ประมวลผลเป็นเวลาหลายปีเพื่อทำการจำลองการทำงาน แต่ด้วยคอมพิวเตอร์เชิงควอนตัมขนาด 40 คิวบิต ประมวลผลประมาณ 100 ขั้นตอน สามารถทำงานได้เท่าเทียมกัน [Lloyd 1995] นอกจากนี้ยังมีคุณสมบัติทางควอนตัมบางอย่าง เช่น คุณสมบัติความพัวพัน ที่ไม่มีคอมพิวเตอร์ดั้งเดิมใดๆ สามารถทำการจำลองได้เพราะเป็นปรากฏการณ์ที่เกิดขึ้นกับระบบควอนตัมเท่านั้น แต่หากใช้ระบบควอนตัมหรือคอมพิวเตอร์เชิงควอนตัม ทำการจำลองตัวมันเองย่อมทำได้เพราะคุณสมบัติเหมือนกันทุกประการ "A quantum system has no problem simulating itself." [Preskill.NET]

- **ด้านเทคโนโลยีการวัด (Metrology)**

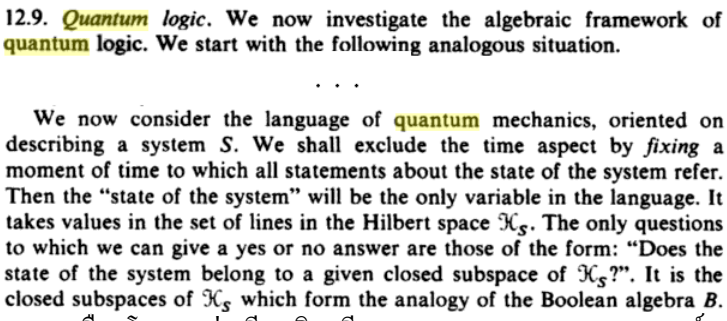
คุณสมบัติเชิงควอนตัม เช่น ความพัวพัน สามารถนำมาเพิ่มความละเอียดในการวัดได้ จากขอบเขตเดิม คือความละเอียดดีที่สุด $1/\sqrt{N}$ เป็นขอบเขตใหม่คือ $1/N$ เรียกว่าขีดจำกัดไฮเซนเบิร์ก (Heisenberg limit) โดยใช้สถานะพัวพันอันดับ N นอกจากนี้ยังมีการประยุกต์ในการวัดอื่นๆ เช่น การประสานเวลา (Clock synchronization) [*Jozsa 2000*] การทดลองเพื่อค้นหาคลื่นความโน้มถ่วง (Gravitational waves) [*Caves 1980*] และการกัดลายวงจรด้วยแสงที่มีสถานะพัวพัน (Quantum lithography) [*Boto และคณะ 2000*] เป็นต้น

4.1.4.2 สารสนเทศเชิงควอนตัม

สารสนเทศเชิงควอนตัม (Quantum information) คือ ข้อมูลที่ถูกแทนไว้ในระบบเชิงควอนตัม มีลักษณะเป็นผลรวมเชิงเส้นของเวกเตอร์ฐาน สำหรับระบบที่มีสองสถานะเรียกสารสนเทศที่แทนระบบเชิงควอนตัมดังกล่าวว่า คิวบิต หรือ ควอนตัมบิต สารสนเทศเชิงควอนตัมแตกต่างจากสารสนเทศดั้งเดิมตรงที่

- ไม่สามารถดึงค่า (วัดค่า) สารสนเทศเชิงควอนตัมออกมาจากระบบเชิงควอนตัมหรืออนุภาคโดยที่ไม่ทำให้สถานะของอนุภาคหรือระบบควอนตัมเปลี่ยนไปสู่สถานะที่แทนค่าที่วัดได้ (การวัดค่าสารสนเทศควอนตัมทำให้สถานะของระบบเปลี่ยนไปสู่ค่าที่เป็นผลของการวัดนั้น)
- ไม่สามารถคัดลอกสารสนเทศควอนตัมที่ไม่ทราบค่าได้
- สารสนเทศควอนตัมสามารถอยู่ในรูปผลรวมเชิงเส้น หรือ การทับซ้อนเชิงตำแหน่งของสถานะพื้นฐานที่ตั้งฉากกัน หลายสถานะ (ถ้าใช้สองสถานะพื้นฐานตั้งฉาก จะเรียกสารสนเทศควอนตัมนั้นว่า คิวบิต)

ความแตกต่างระหว่างสารสนเทศดั้งเดิม (classical information) และสารสนเทศเชิงควอนตัมอธิบายเพิ่มเติมในหัวข้อ 4.1.5 "หน่วยพื้นฐานของการคำนวณเชิงดิจิทัลและการคำนวณเชิงควอนตัม (บิต และ คิวบิต)"



12.9. *Quantum logic*. We now investigate the algebraic framework of quantum logic. We start with the following analogous situation.

. . .

We now consider the language of quantum mechanics, oriented on describing a system S. We shall exclude the time aspect by *fixing* a moment of time to which all statements about the state of the system refer. Then the "state of the system" will be the only variable in the language. It takes values in the set of lines in the Hilbert space $\mathcal{H}_S$. The only questions to which we can give a yes or no answer are those of the form: "Does the state of the system belong to a given closed subspace of $\mathcal{H}_S$?". It is the closed subspaces of $\mathcal{H}_S$ which form the analogy of the Boolean algebra B.

รูปที่ 4.10 การอธิบายความเชื่อมโยงระหว่างพีชคณิตบูลีน (Boolean algebra) และกลศาสตร์ควอนตัมโดย ยู มานิน ในหนังสือ "A course in mathematical logic" หน้า 87-88 ค.ศ. 1977 ปรากฏคำว่า 'Quantum logic' เป็นครั้งแรก [*Manin 77*]

4.1.4.3 ความเข้าใจที่คลาดเคลื่อนเกี่ยวกับคอมพิวเตอร์เชิงควอนตัม

มีการอธิบายคอมพิวเตอร์เชิงควอนตัมว่าหมายถึงการประมวลผลใดๆ ก็ตามด้วยระบบทางกายภาพที่เป็นไปตามหลักกลศาสตร์ควอนตัม แต่เนื่องจากกลศาสตร์ควอนตัมสามารถอธิบายปรากฏการณ์ตั้งแต่อนุภาคเล็กๆ ไปจนถึงมวลสารใหญ่ๆ ได้ "คอมพิวเตอร์ตั้งโต๊ะและคอมพิวเตอร์พกพาล้วนเป็นไปภายใต้หลักกลศาสตร์ควอนตัม แต่ไม่ใช่คอมพิวเตอร์เชิงควอนตัม" [*Mermin 2006*]

ถึงแม้ว่าควอนตัมคอมพิวเตอร์จะสามารถคำนวณแก้ปัญหาอย่างเช่นการแยกตัวประกอบได้รวดเร็วขึ้นเป็นอันดับเอกซ์โพเนนเชียลก็ตาม ควอนตัมคอมพิวเตอร์ไม่สามารถแก้โจทย์ปัญหาใดๆ ก็ตามที่คอมพิวเตอร์ทั่วไปไม่สามารถคำนวณได้ [*Preskill 1998*] ทั้งนี้ เหตุผลหนึ่งคือข้อจำกัดในการอ่านสถานะ ทันทีที่คิวบิตถูกอ่าน (หรือวัด)ค่า ผลลัพธ์ที่ได้จะมีเพียงสองค่า คือ สถานะ "0" และสถานะ "1" เท่านั้น ซึ่งก็เท่ากับข้อมูลดิจิทัล 1 บิตนั่นเอง [*Nielsen & Chuang 2000*]

> *ควอนตัมคอมพิวเตอร์ไม่ได้หมายถึงคอมพิวเตอร์ที่คำนวณได้เร็วกว่าคอมพิวเตอร์ปกติในทุก ๆ กรณี หากแต่ทำได้เร็วขึ้นในเฉพาะบางโจทย์ปัญหาที่อาศัยคุณสมบัติของควอนตัมฟิสิกส์ (เช่น ความทับซ้อนเชิงตำแหน่ง หรือ superposition) มาช่วยได้เท่านั้น ส่วนปัญหาอื่น ๆ ควอนตัมคอมพิวเตอร์ไม่ได้เพิ่มความรวดเร็วในการแก้ปัญหาแต่อย่างใด กระบวนวิธีแก้โจทย์ปัญหาที่อาศัยคุณสมบัติทางควอนตัมมาช่วยให้แก้โจทย์ได้ดีกว่าคอมพิวเตอร์รูปแบบเดิม รวมเรียกว่าขั้นตอนวิธีเชิงควอนตัม (Quantum algorithms) เช่น วิธีแยกตัวประกอบของจำนวนเฉพาะที่เสนอโดยปีเตอร์ ชอร์ ในปี ค.ศ. 1994 [Shor 1994] วิธีค้นฐานข้อมูลที่ไม่ได้เรียงลำดับเสนอโดยลอฟ กรอฟเวอร์ (Lov Grover) ในปี ค.ศ. 1996 [Grover 1996] หรือแนวคิดการจำลองระบบควอนตัมด้วยระบบควอนตัมด้วยกันเสนอโดยริชาร์ด ฟายน์แมน ในปี ค.ศ. 1982 [Feynman 1982] โดยยังเป็นเรื่องที่ค้นคว้าวิจัยอยู่ว่ามีโจทย์ปัญหาใดอีกที่มีความสำคัญและควอนตัมคอมพิวเตอร์สามารถแก้โจทย์ได้รวดเร็วกว่าคอมพิวเตอร์เดิม [Shor 2003]*

ซึ่งความเร็วของการแก้ปัญหานิยามโดยอัตราส่วนของทรัพยากร คือเวลาและหน่วยความจำต่อขนาดของปัญหา เช่น วิธีแก้สมการของเพลล์ (Pell's Equation) ที่ใช้เวลาเป็นโพลิโนเมียล ค้นพบโดย ชอน ฮอลล์เกรน (Sean Hallgren) ในปี ค.ศ. 2007 [*Hallgren 2007*]

บิตควอนตัมจำนวน n คิวบิต สามารถเข้ารหัสข้อมูลดิจิทัลได้เพียง n บิต ไม่ใช่ 2^n บิตอย่างที่เข้าใจกันโดยทั่วไป (เช่น สามคิวบิต เข้าใจว่าแทนข้อมูลแปดบิต (2^3) ได้) แต่ทฤษฎีบท โฮเลโว-ชูมัคเกอร์-เวสต์มอร์แลนด์ (Holevo-Schumacher-Westmoreland) กล่าวว่าปริมาณสารสนเทศของ n คิวบิต จะมีค่าไม่เกิน n (ไม่ใช่ 2^n) และไม่สามารถเข้ารหัสข้อมูล (แบบไม่มีการสูญเสีย) ให้มีความยาวสั้นกว่าปริมาณสารสนเทศได้ [*Nielsen & Chuang 2000*] หรือในอีกแง่มุมหนึ่ง n คิวบิต ประกอบด้วยสถานะที่แบ่งแยกจากกันได้อย่างชัดเจน 2^n สถานะ ซึ่งหากใช้ n คิวบิตแทนสถานะ (ตัวเลข) มากกว่า 2^n ค่า จะทำให้มีสถานะที่ไม่ตั้งฉากกัน ซึ่งสถานะที่ไม่ตั้งฉากกันนี้ไม่สามารถแบ่งแยกจากกันได้อย่างชัดเจน เช่น หากกำหนดให้ 1 คิวบิต แทนตัวเลข 3 ตัว คือ "0" แทนด้วย

PHYSICAL REVIEW A VOLUME 51, NUMBER 4 APRIL 1995

Quantum coding

Benjamin Schumacher*
Department of Physics, Kenyon College, Gambier, Ohio 43022
(Received 9 April 1993)

ACKNOWLEDGMENTS

The term "qubit" was coined in jest during one of the author's many intriguing and valuable conversations with W. K. Wootters, and became the initial impetus for this work. The author is also grateful to C. H. Bennett and R. Jozsa for their helpful suggestions and for numerous words of encouragement.

รูปที่ 4.11 ที่มาของคำว่า "qubit" กล่าวไว้ในกิตติกรรมประกาศของบทความ *Physical Review A*, vol. 51, หน้า 2738 ค.ศ. 1995 โดย เบนจามิน ชูมัคเกอร์ (Benjamin Schumacher) [*Schumacher 1995*]

$|0\rangle$ "1" แทนด้วย $|1\rangle$ และ "2" แทนด้วย $|2\rangle$ โดยกำหนดให้ $|2\rangle=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$ หากทำการวัดค่า จะได้ $|2\rangle$ ผลลัพธ์เป็น $|0\rangle$ หรือ $|1\rangle$ ก็ได้ดังนั้นหากมี 1 คิวบิต (ไม่ทราบค่า) ส่งเข้ามา และทำการวัดค่าในแนว $\{|0\rangle,|1\rangle\}$ ถ้าได้ออกมาเป็น $|0\rangle$ ก็สรุปไม่ได้ว่าข้อความที่ส่งมาเป็น "0" หรือ "2" หากได้ออกมาเป็น $|1\rangle$ ก็สรุปไม่ได้ว่าข้อความที่ส่งมาเป็น "1" หรือ "2" กันแน่ แต่หากใช้ 1 คิวบิต แทนข้อมูล 1 บิต คือ "0" แทนด้วย $|0\rangle$ และ "1" แทนด้วย $|1\rangle$ ซึ่งเป็นสถานะตั้งฉากกัน ในกรณีนี้ "0" และ "1" สามารถแบ่งแยกจากกันได้อย่างชัดเจน (หากวัดในแนว $\{|0\rangle,|1\rangle\}$) จึงเป็นการอธิบายจำนวนบิตควอนตัมข้างต้น

4.1.5 หน่วยพื้นฐานของการคำนวณเชิงดิจิทัลและการคำนวณเชิงควอนตัม (บิต และ คิวบิต)

การอธิบายความแตกต่างของหน่วยพื้นฐานของการคำนวณและการสื่อสารเชิงดิจิทัล (บิต) และเชิงควอนตัม (คิวบิต) สามารถอธิบายได้ในเชิงเปรียบเทียบระหว่างหน่วยข้อมูลทั้งสอง

4.1.5.1 ความแตกต่างในเชิงนิยาม

บิต[4.9] คือ ปริมาณที่มีค่าได้เพียงค่าเดียวในสองค่าคือ "0" หรือ "1" เท่านั้น เป็นปริมาณพื้นฐานทางการคำนวณและการสื่อสารแบบดิจิทัล

คิวบิต คือ สถานะทางควอนตัมซึ่งประกอบด้วยเวกเตอร์ฐานตั้งฉากกัน 2 เวกเตอร์ เป็นปริมาณพื้นฐานทางการคำนวณและการสื่อสารเชิงควอนตัม หนึ่งคิวบิตสามารถแทนค่าศูนย์และหนึ่งได้ในเวลาเดียวกัน และด้วยค่าสัมประสิทธิ์ที่บ่งบอกถึงความน่าจะเป็นที่จะวัดค่าได้สถานะนั้น ๆ ซึ่งแสดงการแทนสถานะดังรูปที่ 4.12

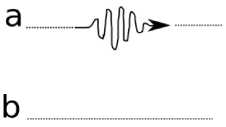
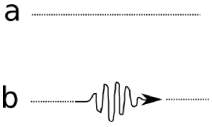
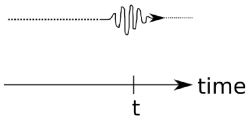
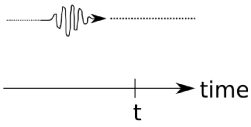
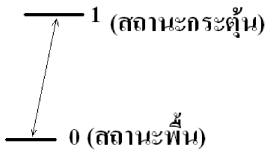
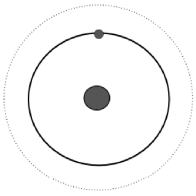
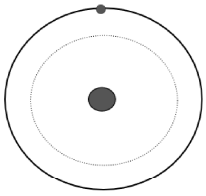
ทั้งบิต และ คิวบิต สามารถพิจารณาได้ในสองแง่มุม คือ เป็นปริมาณหรือแบบจำลองทางคณิตศาสตร์ หรือเป็นระบบทางกายภาพที่ใช้แทนปริมาณนั้นๆ นำเสนอในตารางที่ 4.2 และ 4.3

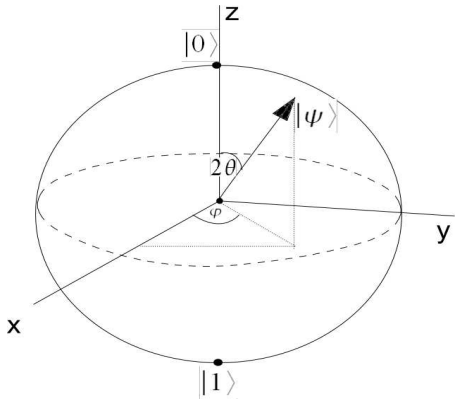
[4.9] ในที่นี้มิได้อ้างถึง 'บิต' ในแง่หน่วยวัดปริมาณสารสนเทศ ซึ่งนิยามด้วยความน่าจะเป็นของการเกิดข้อความบิตนั้น

ตารางที่ 4.2 เปรียบเทียบระหว่างบิตและคิวบิต

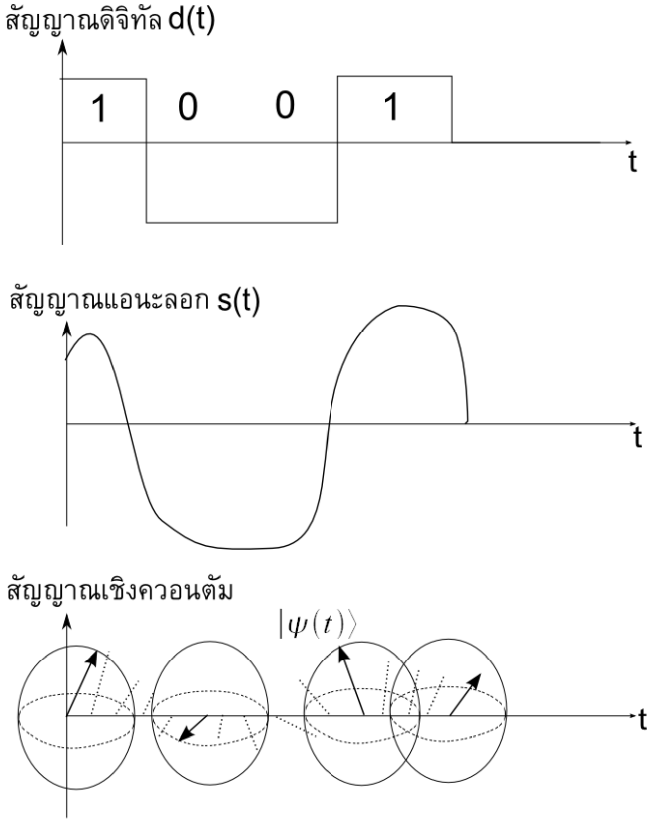
บิต	คิวบิต
ที่มาของคำ: binary digit → 'bit' ผู้นำมาใช้คนแรก: จอห์น เทอร์กีย์ (John Tukey) (ปี ค.ศ. 1947) ซึ่งอ้างถึงโดย โคลด แชนนอน (ปี ค.ศ. 1948) : 'bit' มาตรวัดปริมาณสารสนเทศ	*ที่มาของคำ*: quantum binary digit → 'qubit' ผู้นำมาใช้คนแรก: เบนจามิน ชูมัคเกอร์ (ปี ค.ศ. 1995)ในบทความ “Quantum coding” Phys. Rev. A, vol. 51, 2738
แง่ความหมาย/คุณสมบัติ ในเชิงคณิตศาสตร์ 1 bit แทนสองสถานะ และมีได้เพียงสถานะเดียว ณ เวลาหนึ่ง ๆ เช่น “0” หรือ “1” เท่านั้น แทนด้วยเมทริกซ์ “0” แทนด้วย $\begin{bmatrix}1\\0\end{bmatrix}$ “1” แทนด้วย $\begin{bmatrix}0\\1\end{bmatrix}$ 1 bit ในเชิงเรขาคณิตแทนได้ด้วยจุดสองจุด จุดหนึ่งแทนเลข “0” อีกจุด แทนเลข “1” 0 1	*ความหมาย/คุณสมบัติ* ในเชิงคณิตศาสตร์ 1 qubit เป็นผลรวมเชิงเส้นของสองสถานะ โดยมีสัมประสิทธิ์เป็นจำนวนเชิงซ้อน บ่งบอกถึงความน่าจะเป็นที่จะวัดได้สถานะนั้น แทนด้วยสัญลักษณ์ Dirac Bra-Ket $\lvert\psi\rangle=\alpha\lvert 0\rangle+\beta\lvert 1\rangle \quad , \quad \alpha,\beta\in C;\lvert\alpha\rvert^2+\lvert\beta\rvert^2=1$ หรือแทนด้วยเมทริกซ์ (นำสัมประสิทธิ์มาแทน) $\lvert\psi\rangle$ แทนด้วย $\begin{bmatrix}\alpha\\\beta\end{bmatrix}$ 1 qubit ในเชิงเรขาคณิตแทนด้วยเวกเตอร์ขนาดหนึ่งหน่วยบนผิวทรงกลม ซึ่งทิศทางของเวกเตอร์และโปรเจ็กชันบนแกนที่ทำการวัด จะบ่งบอกถึงความน่าจะเป็นที่จะวัดค่าได้สถานะนั้น (สังเกตรูปที่ 4.12 เมื่อให้ $\alpha=\cos\theta$)
ระบบทางกายภาพที่แทน 'bit' เช่น ไม่มีกระแสผ่าน หรือมีน้อยมากเท่ากับ “0” มีกระแสไฟผ่านเท่ากับ “1”	ระบบทางกายภาพที่แทน 'qubit' 1 qubit หมายถึง ระบบควอนตัมที่ประกอบด้วยสถานะสองสถานะ (Two-level quantum systems)
Bit sequence (ข้อความดิจิทัล) ….0100011010111010..... (ดูรูปที่ 4.13)	Qubit sequence (ข้อความควอนตัม) ($\ldots..\lvert\psi_1\rangle\lvert\psi_2\rangle\lvert\psi_3\rangle\lvert\psi_4\rangle\lvert\psi_5\rangle\ldots..$ ดูรูปที่ 4.13)
ผลลัพธ์เมื่อมีการวัดสถานะ $0\rightarrow$ วัดค่า $\rightarrow$ 0 (100%) $1\rightarrow$ วัดค่า $\rightarrow$ 1 (100%)	*ผลลัพธ์เมื่อมีการวัดสถานะ* $\alpha\lvert 0\rangle+\beta\lvert 1\rangle \rightarrow$ วัดค่า $\rightarrow\lvert 0\rangle$ ด้วยความน่าจะเป็น = $\lvert\alpha\rvert^2$ $\alpha\lvert 0\rangle+\beta\lvert 1\rangle \rightarrow$ วัดค่า $\rightarrow\lvert 1\rangle$ ด้วยความน่าจะเป็น = $\lvert\beta\rvert^2$ โดยที่ $\lvert\alpha\rvert^2+\lvert\beta\rvert^2=1$

ตารางที่ 4.3 ตัวอย่างระบบทางกายภาพที่นำมาแทนคิวบิต

ระบบกายภาพที่ใช้แทนคิวบิต	คุณสมบัติ	สารสนเทศ (ลอจิก)	
		“0”	**“1”**
โฟตอน	การจัดเรียงตัวเชิงเส้น (Linear polarization)	แนวตั้ง 	แนวนอน
	การจัดเรียงตัวเชิงวงกลม (Circular polarization)	ทวนเข็มนาฬิกา (left-circular polarization)	ตามเข็มนาฬิกา (right-circular polarization)
	จำนวนโฟตอน (Photon number)	ไม่มีโฟตอน	มี 1 โฟตอน
	เส้นทางที่แสงเคลื่อนที่ (Photon path)	ผ่านเส้นทาง a 	ผ่านเส้นทาง b 
	ตะกร้าเวลา ก่อน-หลัง (time-bin)	โฟตอนมาถึงก่อน 	โฟตอนมาถึงทีหลัง 
อิเล็กตรอน	สปิน (spin)	สปินมีทิศ +Z 	สปินมีทิศ -Z 
	ประจุ (charge)	ไม่มีประจุ (ไม่มีอิเล็กตรอน)	มีประจุ (มี 1 อิเล็กตรอน)
นิวตรอน	สปิน (spin)	สปินมีทิศ+Z 	สปินมีทิศ -Z 
อะตอม	ระดับพลังงาน (energy level) 	สถานะพื้น  (ground state)	สถานะกระตุ้น  (excited state)



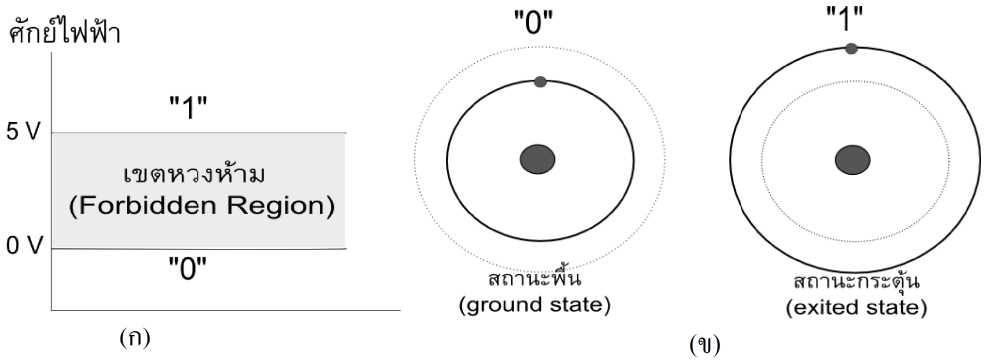
รูปที่ 4.12 การแทนสถานะคิวบิตด้วยเวกเตอร์ที่ชี้ไปบนผิวของทรงกลมที่เรียกว่าทรงกลมบล็อช (Bloch sphere) หรือ ทรงกลมปวงกาเร (Poincare sphere) สถานะของคิวบิตกำหนดโดยค่ามุมสองค่า θ และ ϕ คือ $|\psi\rangle=\cos\theta|0\rangle+e^{i\varphi}\sin\theta|1\rangle$



รูปที่ 4.13 เปรียบเทียบสัญญาณดิจิทัล สัญญาณแอนะลอก และสัญญาณควอนตัม

ข้อความดิจิทัล (digital message หรือ bit sequence) คือ สัญลักษณ์บิตจำนวนหนึ่งที่นำมาเรียงต่อกัน (เช่น 0100111010011...) โดยในการสื่อสารเชิงดิจิทัล ข้อความที่ต้องการส่งแต่ละตัวอักษรจะถูกแปลงไปเป็นตัวเลขฐานสองและส่งออกไปได้ ส่วนข้อความเชิงควอนตัม (Quantum message หรือ Qubit sequence) คือ สถานะรวมของคิวบิตหลายๆ ตัวเรียงกันเป็นลำดับ เช่น $|\psi\rangle=(a_0|0\rangle+b_0|1\rangle)(a_1|0\rangle+b_1|1\rangle)(a_2\rangle 0\rangle+b_2|1\rangle)...(a_{n-1}|0\rangle+b_{n-1}|1\rangle)$ คือข้อความควอนตัมความยาว n คิวบิต[4.10] โดยแสดงการเปรียบเทียบสัญญาณบิต คิวบิต และดิจิทัลดังรูปที่ 4.13

[4.10] ในกรณีที่ข้อความควอนตัมดังกล่าวเป็นสถานะที่อยู่ใน 'ระบบปิด' ส่วนของกรณีระบบเปิด หรือมีการรบกวนจากสิ่งแวดล้อม ข้อความควอนตัมจะต้องแสดงในรูปสถานะผสม (mixed states) ซึ่งอยู่ในรูปของออองซองเบิล (ensemble) ของสถานะย่อย ๆ



รูปที่ 4.14 ตัวอย่างการใช้ระบบทางกายภาพแทน “0” และ “1”
(ก) การใช้ศักย์ไฟฟ้าแทนเลข (ข) ระดับพลังงานของอะตอมแทนเลข

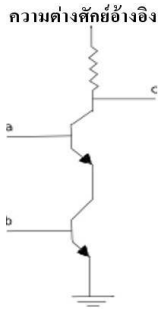
ตารางที่ 4.4 สรุปข้อเปรียบเทียบระหว่างบิต และ คิวบิต

Bits	**Qubits**
มีค่าได้เป็น “0” หรือ “1”	มีค่าเป็นผลรวมเชิงเส้นของ “0” และ “1” ($a\,\vert 0\rangle + b\,\vert 1\rangle$)
สามารถวัดค่าบิตได้โดยแม่นยำ	ไม่สามารถวัดสถานะที่แน่นอนของคิวบิตได้
สามารถวัดค่าบิตได้โดยไม่ทำให้ค่าเดิมเปลี่ยน	การวัดคิวบิตสามารถทำให้ค่าเปลี่ยน
สามารถแยกแยะ “0” และ “1” ออกจากกันได้อย่างชัดเจน	2 คิวบิตใด ๆ ที่ไม่ตั้งฉากกัน ไม่สามารถแยกแยะอย่างชัดเจนได้
สามารถทำการคัดลอกบิตได้โดยไร้ข้อจำกัด	คัดลอกคิวบิต (ที่ไม่ทราบค่า) ไม่ได้[4.11]
การรู้สถานะของบิตหนึ่ง ไม่มีผลต่อค่าสถานะของอีกบิตหนึ่งที่อยู่ไกลกัน	การรู้สถานะของคิวบิตหนึ่ง จะมีผลต่อค่าสถานะของอีกคิวบิตหนึ่งที่พัวพันกัน ถึงแม้จะอยู่ห่างไกลกันก็ตาม

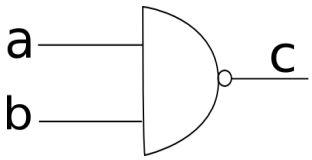
4.1.5.2 ระบบทางกายภาพที่แทนบิตและคิวบิต

ในทางคณิตศาสตร์ 1 บิตคือตัวเลขที่มีได้เพียงสองค่า คือ “0” หรือ “1” เท่านั้น ส่วนการเลือกใช้สิ่งใดในธรรมชาติที่นำมาแทนสถานะ “0” และ “1” นี้ แล้วแต่จะกำหนด แต่ก็พยายามกำหนดให้เป็นที่เข้าใจตรงกัน เช่น ในคอมพิวเตอร์ที่ใช้กันอยู่ ใช้สภาพการนำไฟฟ้าของทรานซิสเตอร์ควบคุมค่าศักย์ไฟฟ้า ณ จุดที่กำหนดให้เป็น ถ้าความต่างศักย์เป็นศูนย์ที่หรือใกล้เคียงศูนย์กำหนดให้แทนเลข “0” ความต่างศักย์ที่มีค่าสูงกว่าค่าหนึ่ง กำหนดให้แทนเลข “1” หรืออาจแทนในรูปแบบอื่นๆ แล้วแต่การกำหนด ส่วนระบบทางกายภาพที่แทนคิวบิตมีการนำเสนอหลายรูปแบบ ซึ่งเป็นอนุภาคใดๆ ที่สามารถแทนสองสถานะเชิงควอนตัม (ที่มีการนิยามอย่างชัดเจน และมีคุณสมบัติตั้งฉาก) ได้ เช่น โพลาไรเซชันของแสง จำนวนของโฟตอน สปินของอนุภาค (อิเล็กตรอน นิวตรอน) เป็นต้น ดังรูปที่ 4.14 และตารางที่ 4.3

[4.11] ถ้ารู้ว่าสถานะของคิวบิต มีเพียงค่าใดค่าหนึ่งระหว่างสองสถานะที่ตั้งฉากกัน คิวบิตนั้นจะแทนข้อมูลได้เหมือนบิตธรรมดา คือ “0” และ “1” โดยแยกแยะจากกันได้อย่างชัดเจน และสามารถคัดลอกได้



(ก)

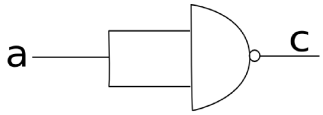


(ข)

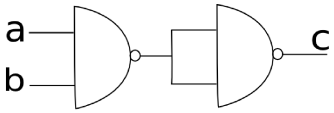
a	b	c
0	0	1
0	1	1
1	0	1
1	1	0

(ค)

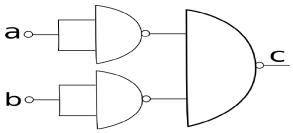
รูปที่ 4.15 เกต NAND: (ก) วงจรทรานซิสเตอร์ (ข) สัญลักษณ์ (ค) ตารางค่าตรรก



(ก) เกต NOT ที่สร้างจากเกต NAND

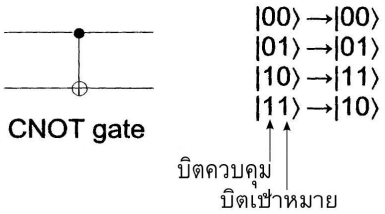


(ข) เกต AND ที่สร้างจากเกต NAND



(ค) เกต OR ที่สร้างจากเกต NAND

รูปที่ 4.16 การใช้เกต NAND สร้างเกต NOT เกต AND และเกต OR



รูปที่ 4.17 เกต Control-NOT สำหรับคิวบิต [*ภาพปรับปรุงจาก Morsch 2008*]

4.2 วงจรเชิงควอนตัม (Quantum Circuits)

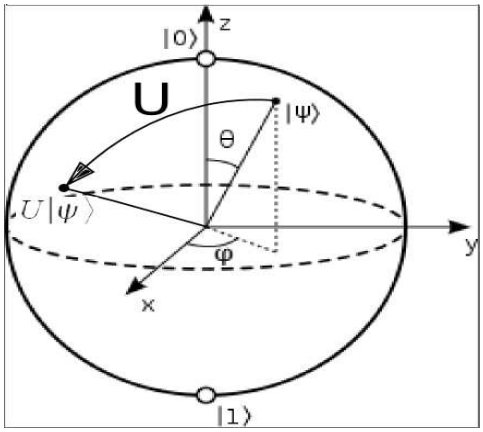
ในการคำนวณข้อมูลต่างๆ ต้องมีอุปกรณ์เฉพาะสำหรับการคำนวณ โดยในการคำนวณด้วยคอมพิวเตอร์ทั่วไปจะใช้เกตลอจิกเป็นวงจรสำหรับการคำนวณ แต่การคำนวณเชิงควอนตัมต้องอาศัยคุณสมบัติของการเปลี่ยนแปลงสถานะควอนตัม จึงต้องใช้วงจรที่มีคุณสมบัติเฉพาะทางควอนตัมช่วยในการคำนวณ

4.2.1 วงจรลอจิก (ตรรกะ) ดั้งเดิม

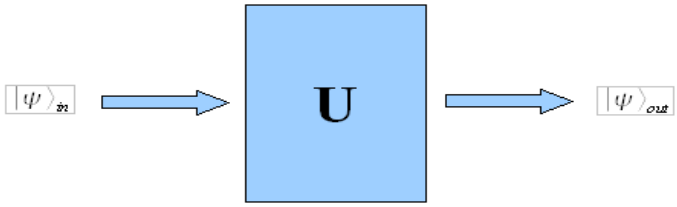
การที่จะใช้คอมพิวเตอร์ช่วยคิดคำนวณอย่างเช่นการบวก ลบ คูณ หาร เลขจำนวนมาก ๆ อาศัยเกตลอจิกประกอบกันเป็นวงจรดิจิทัล ในการคำนวณ เช่น การบวกโดยเกต exclusive-OR และทดเลขด้วยเกต AND ร่วมกับเกต exclusive-OR โดยการคำนวณทุกอย่างในคอมพิวเตอร์สามารถทำได้โดยอาศัยเพียงเกตลอจิกชนิดเดียวคือเกต NAND มาประกอบกัน (เรียกว่าเกตนี้เป็นเกตอเนกประสงค์) [*Nielsen & Chuang 2000*] หรืออาจใช้เกตลอจิกสามชนิดได้แก่เกต AND OR และ NOT โดยเกตแต่ละเกตสามารถสร้างขึ้นได้จากเกต NAND ทั้งสิ้น

4.2.2 วงจรเชิงควอนตัม

วงจรเชิงควอนตัม เสนอโดย เดวิด ดอยช์ (David Deutsch) ในปี ค.ศ. 1989 เป็นแบบจำลองที่ใช้อธิบายการเปลี่ยนแปลงของสถานะควอนตัมซึ่งทำหน้าที่แทนการประมวลผลข้อมูล โดยสามารถเขียนเป็นเส้นวงจรได้คล้ายกับเส้นวงจรทางไฟฟ้า และการเปลี่ยนแปลงแต่ละช่วงเวลาจะแทนด้วย 'เกตลอจิกเชิงควอนตัม' (Quantum logic gate) ต่อมาในปี ค.ศ. 1995 ได้มีการพิสูจน์ว่า การคำนวณเชิงควอนตัมทุกรูปแบบสามารถประกอบขึ้นจากหน่วยย่อยเพียงสองชนิดคือ (1) การเปลี่ยนแปลงแบบย้อนกลับได้ของหนึ่งคิวบิต และ (2) ตัวดำเนินการ Controlled-NOT ของสองคิวบิต [*Barenco และคณะ 1995*]



รูปที่ 4.18 การแปลงคิวบิต เมื่อพิจารณาเชิงเรขาคณิตเทียบได้กับการหมุนเวกเตอร์บนผิวทรงกลมบล็อช



รูปที่ 4.19 การแปลงคิวบิต (ลูกศร แทนการเปลี่ยนแปลงของเวลา)

ก่อนหน้านั้นในปี ค.ศ. 1985 ริชาร์ด ฟายน์แมนเคยเสนอการนำกลศาสตร์ควอนตัมมาออกแบบเกตลอจิกโดยการหาแฮมิลโตเนียน (Hamiltonian)[4.12] ซึ่งระบุการแปลงคิวบิตที่ให้ผลลัพธ์เป็นการ “บวก” เป็นต้น [*Stolze และ Suter 2004*] การแปลงของ 1 คิวบิต เทียบได้กับการหมุนเวกเตอร์ที่แทนสถานะคิวบิตบนผิวของทรงกลมบล็อชหรือทรงกลมปวงกาเร ซึ่งแสดงได้ดังรูปที่ 4.18 และรูปที่ 4.19

การแปลงของ 1 คิวบิต กล่าวโดยทั่วไปก็เหมือนกับการแปลงสถานะควอนตัม ซึ่งมีสองรูปแบบหลักๆ คือ

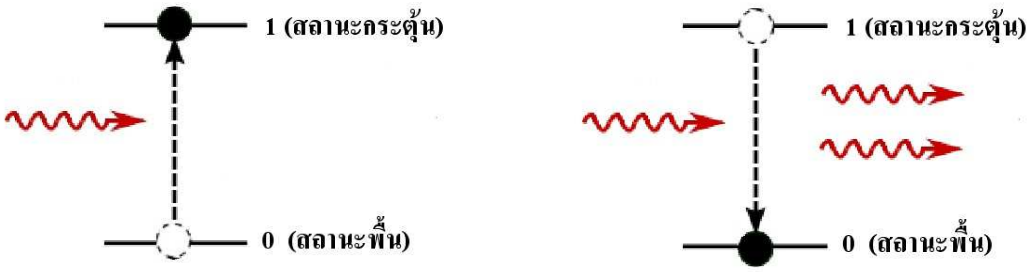
1) การแปลงแบบย้อนกลับได้ (reversible transformation) ซึ่งเป็นการเปลี่ยนแปลงของระบบปิด (ไม่สูญเสียพลังงาน ไม่สูญเสียข้อมูลไปยังสิ่งแวดล้อม) จะแทนด้วยตัวดำเนินการที่อนุรักษ์ขนาดของเวกเตอร์สถานะ หรือการแปลงยูนิแทรี (Unitary transformation: U) ซึ่งมีคุณสมบัติย้อนกลับได้ โดย $U^{-1} = U^{\dagger}$ (เมื่อ '†' หมายถึง การสลับเปลี่ยน (Transpose) และสังยุค (Conjugate) ต่อเมทริกซ์)

2) การแปลงแบบย้อนกลับไม่ได้ (Irreversible transformation) ซึ่งเป็นการเปลี่ยนสถานะของระบบเปิด (คือมีปฏิสัมพันธ์กับสิ่งแวดล้อม มีการสูญเสียข่าวสารไปยังสิ่งแวดล้อม) เช่นกระบวนการเกิดสัญญาณรบกวน (อันเนื่องจากสภาพแวดล้อม) หรือการสอดเครื่องมือเข้าไปทำการวัดสถานะของระบบควอนตัม อันเป็นการดึงข่าวสารออกมาจากสถานะที่ต้องการรู้ แต่การดึงข่าวสารออกมา ต้องแลกด้วยการนำเครื่องมืออะไรบางอย่างเข้าไปกระทำต่อระบบ อันทำให้สถานะถูกเปลี่ยนแปลงแบบย้อนกลับไม่ได้

ในที่นี้พิจารณาเฉพาะการแปลงแบบย้อนกลับได้ โดยการแปลงแบบนี้ทางคณิตศาสตร์พิจารณาได้ในรูป $|\psi\rangle \rightarrow U|\psi\rangle$ หรือ $|\psi\rangle_{out} = U|\psi\rangle_{in}$

การแปลงคิวบิต $|\psi\rangle_{out} = U|\psi\rangle_{in}$ สามารถแทนด้วยเมทริกซ์ขนาด 2×2 กระทำกับเวกเตอร์หรือเมทริกซ์ 2×1 ได้ดังต่อไปนี้

[4.12] ตัวดำเนินการที่ใช้วัดพลังงานของระบบ



(ก) (ข)

รูปที่ 4.20 การทำงานพื้นฐานของเกตลอจิก 'NOT' เชิงควอนตัม กระทำต่อสถานะของอะตอมที่สถานะพื้น (“0”) และสถานะกระตุ้น (“1”) โดยการกระตุ้นด้วยพัลส์แสงความถี่ที่เหมาะสมที่มีค่าเท่ากับช่วงความต่างของระดับพลังงาน (ก) กรณีแรกการดูดกลืนโฟตอน (Photon absorption) สถานะเดิมอยู่ที่ “0” จะถูกกระตุ้นให้ดูดกลืนความถี่นั้น และสถานะจะเปลี่ยนจาก “0” เป็น “1” (NOT) (ข) กรณีที่สองการเปล่งแสงแบบเร่งเร้า (Stimulated emission) สถานะเดิมอยู่ที่ “1” จะถูกกระตุ้นและปล่อยโฟตอนออกมาสองโฟตอนที่มีความถี่ เฟส โพลาไรเซชัน และมีทิศทางเดียวกัน อะตอมจะลดระดับพลังงานลงมาที่สถานะพื้น (“0”)

$$\begin{bmatrix}\alpha_{out}\\ \beta_{out}\end{bmatrix}=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}\alpha_{in}\\ \beta_{in}\end{bmatrix} \qquad \text{.....(4.1)}$$

$$|\psi\rangle_{out}\equiv U|\psi\rangle_{in} \qquad \text{.....(4.2)}$$

โดยที่ $|\psi\rangle_{out}\equiv\begin{bmatrix}\alpha_{out}\\ \beta_{out}\end{bmatrix}$, $U=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$, $|\psi\rangle_{in}\equiv\begin{bmatrix}\alpha_{in}\\ \beta_{in}\end{bmatrix}$ และทุกจำนวนในเมทริกซ์เป็นจำนวนเชิงซ้อน หากเมทริกซ์ U เป็นยูนิแทรีคือ $U^{-1}=\begin{bmatrix}a* & c*\\ b* & d*\end{bmatrix}$ ($a*$ แทนสังยุคเชิงซ้อนของ a) U จะแทนกระบวนการทางกายภาพแบบย้อนกลับได้ ซึ่งเป็นการเปลี่ยนแปลงของระบบปิด อย่างไรก็ตามการเปลี่ยนแปลงของระบบเปิดก็สามารถอธิบายด้วยการแปลงแบบยูนิแทรีเช่นเดียวกัน แต่เป็นการแปลงแบบยูนิแทรีซึ่งกระทำกับสถานะรวมของระบบและสถานะของสิ่งแวดล้อม ซึ่งเป็นการอธิบายการเปลี่ยนแปลงของระบบเปิดด้วยการแปลงของระบบรวม (Universe) คือระบบที่สนใจและสิ่งแวดล้อมรวมกัน สรุปว่าเป็นระบบปิดระบบหนึ่ง ซึ่งแสดงได้ดังสมการ

$$|\psi\rangle_{in}|\textit{สิ่งแวดล้อม}\rangle_{in}\rightarrow^{U}\rightarrow|\psi\rangle_1|\textit{สิ่งแวดล้อม}\rangle_1+|\psi\rangle_2|\textit{สิ่งแวดล้อม}\rangle_2$$

การแปลงคิวบิตในห้องทดลอง เช่นคิวบิตที่แทนด้วยระดับพลังงานของอะตอม (สถานะพื้นเป็น “0” สถานะกระตุ้นเป็น “1”) การแปลงคิวบิต (ซึ่งแทนด้วยเมทริกซ์ unitary) ทำได้โดยการกระตุ้นอะตอมด้วยคลื่นแม่เหล็กไฟฟ้าที่มีความยาวคลื่นพอดีกับความต่างของระดับพลังงานระหว่างสถานะพื้นและสถานะกระตุ้นนั้น เพื่อให้อะตอมดูดกลืนพลังงานและเปลี่ยนจากสถานะพื้นเป็นสถานะกระตุ้น ดังรูปที่ 4.20 และการเปลี่ยนจากสถานะกระตุ้นเป็นสถานะพื้นทำได้โดยป้อนแสงความยาวคลื่นเดียวกันเข้าไปกระตุ้นให้อะตอมปล่อยรังสีออกมา เป็นความยาวคลื่นและเฟสที่ตรงกับแสงที่มากระตุ้นนั้น และอะตอมจะเปลี่ยนสถานะจากสถานะกระตุ้นเป็นสถานะพื้นหลังปล่อยรังสี เรียกว่า การเปล่งแสงแบบเร่งเร้าและวิธีการดังกล่าวสามารถแทนตัวดำเนินการ 'NOT'

ได้ เมื่อให้สถานะพื้น แทน “0” และสถานะกระตุ้นแทน “1” (“0” เปลี่ยนเป็น “1” และ “1” เปลี่ยนเป็น “0” ด้วยการทำงานดังกล่าว) ควอนตัมคอมพิวเตอร์มีแบบจำลองอยู่หลายแบบได้แก่

1) แบบจำลองวงจรเชิงควอนตัม (Quantum Circuit Model)

2) แบบจำลองการคำนวณเชิงควอนตัมแบบอะเดียบาติก (Adiabatic-control quantum computing)

3) แบบจำลองการคำนวณเชิงควอนตัมแบบควบคุมองค์รวม (Global-control quantum computing)

4) แบบจำลองการคำนวณเชิงควอนตัมแบบทางเดียว (One-way quantum computing) [*Perez-Delgado & Kok 2009*]

ในที่นี้พิจารณาเฉพาะแบบจำลองวงจรเชิงควอนตัม เพราะมีลักษณะคล้ายคลึงกับวงจรดิจิทัลลอจิกดั้งเดิมและสามารถอธิบายครอบคลุมการคำนวณเชิงควอนตัมทุกรูปแบบ ตามที่ แอนดรู เหยา (Andrew Yao) พิสูจน์ว่าแบบจำลองควอนตัมเทียบเท่ากับแบบจำลองเครื่องกลทูริงเชิงควอนตัมทุกประการ [*Yao 1993*]

การเปลี่ยนแปลงของสองคิวบิต (2-qubit unitary gates) แบ่งเป็นสองรูปแบบคือ

1) การเปลี่ยนแปลงแบบมีอันตรกิริยา คือสถานะเข้าของคิวบิตหนึ่ง (Control qubit) มีผลต่อรูปแบบการดำเนินการที่จะกระทำต่ออีกคิวบิตหนึ่ง (Target qubit)

2) ไม่มีอันตรกิริยา (เป็นการกระทำต่อแต่ละคิวบิต แยกกัน) ในการคำนวณเชิงควอนตัมทั่วไปจำเป็นต้องมีการเปลี่ยนแปลงแบบมีอันตรกิริยาเช่น controlled-NOT gate ซึ่งสามารถจำลองกระบวนการเกิดความพัวพันหรือการทำให้หายพัวพัน (Dis-entangling) ได้

4.2.3 ความแตกต่างระหว่างลอจิกดั้งเดิมและควอนตัมลอจิก

การประมวลผลเชิงตรรกสำหรับข้อมูลดั้งเดิม (Classical logic) และการประมวลผลเชิงตรรกสำหรับข้อมูลเชิงควอนตัม (Quantum logic) แตกต่างตรงที่สถานะควอนตัมอยู่ในรูปการทับซ้อนเชิงตำแหน่งของสถานะลอจิกย่อย ๆ และทุกสถานะจะถูกประมวลผลพร้อมกัน ดังรูปที่ 4.7 ในขณะที่การประมวลผลตรรกแบบดั้งเดิม แต่ละหน่วยประมวลผลจะประมวลผลข้อมูลเข้าได้เพียงหนึ่งสถานะเท่านั้นต่อหนึ่งหน่วยประมวลผล ซึ่งสิ่งนี้เองอยู่เบื้องหลังความสามารถที่ควอนตัมคอมพิวเตอร์สามารถแก้ปัญหาได้รวดเร็วกว่าดิจิทัลคอมพิวเตอร์ในระดับเอกซ์โพเนนเชียล

หน่วยพื้นฐานของการคำนวณเชิงดิจิทัลและการคำนวณเชิงควอนตัม ได้แก่เกตลอจิกซึ่งอาศัยตัวดำเนินการของตรรกศาสตร์ เช่น AND OR NOT มาประกอบกันเข้าเพื่อทำหน้าที่คำนวณตามความต้องการ เช่นการบวกเลข ได้เกตลอจิกเฉพาะเจาะจงบางชนิดที่นำมาประกอบกันเข้าแล้วทำหน้าที่คำนวณทุกรูปแบบในการคำนวณ เรียกว่าเกตอเนกประสงค์ (Universal gates) สำหรับการคำนวณ

ในปี ค.ศ. 1995 อาดรีอาโน บาเรนโก (Adriano Barenco) และคณะ [*Barenco และคณะ 1995*] ได้พิสูจน์ว่า เกตการแปลงหนึ่งคิวบิต และเกต CNOT สำหรับสองคิวบิต ทำหน้าที่เป็นเกตอเนกประสงค์สำหรับการคำนวณเชิงควอนตัมได้ ดังนั้นการทำงานของเกต CNOT จึงเป็นสิ่งที่สมควรศึกษาเพื่อความเข้าใจกระบวนการคำนวณเชิงควอนตัม อนึ่งนอกจากเกต CNOT จะทำหน้าที่ในการคำนวณแล้วยังมีบทบาทสำคัญในการสื่อสารเชิงควอนตัมด้วย โดยจะเป็นแบบจำลองการสร้างสถานะพัวพันและการวัดสถานะแบบเบลล์ ซึ่งเป็นส่วนสำคัญของการสื่อสารแบบเทเลพอร์ทเชิงควอนตัมและการเข้ารหัสด้วยความเข้มสูง

เกตลอจิกที่มีทั้งในการคำนวณเชิงดิจิทัลและเชิงควอนตัม คือ เกตลอจิกแบบย้อนกลับได้ (Reversible logic gate) เพราะในกลศาสตร์ควอนตัม การสูญเสียข้อมูล (กระบวนการย้อนกลับไม่ได้) จะไม่เกิดขึ้นตราบเท่าที่ยังไม่มีการวัดค่า หรือไม่มีกระบวนการสูญเสียพฤติกรรมเชิงควอนตัมเกิดขึ้น โดยเกต CNOT หรือเกต XOR ที่ยังคงข้อมูลของบิตแรกไว้ เป็นหนึ่งในเกตลอจิกแบบย้อนกลับได้และมีใช้อยู่ทั้งในการคำนวณเชิงดิจิทัลและแบบดั้งเดิม

4.2.4 แบบจำลองนอกเหนือจากวงจรเชิงควอนตัม

การคำนวณเชิงควอนตัมนอกจากอาศัยการทำงานของวงจรเกตลอจิกเชิงควอนตัมเลียนแบบเกตลอจิกทางดิจิทัลทั่วไปแล้ว

ยังสามารถใช้การคำนวณในรูปแบบอื่นๆ ได้เช่น

4.2.4.1 การคำนวณเชิงควอนตัมแบบทางเดียว (One-way quantum computation)

การคำนวณเชิงควอนตัมแบบทางเดียวได้รับการเสนอโดย เราเซนดอร์ฟ (Raussendorf) และบรีเกล (Briegel) ในปี ค.ศ. 2000 เป็นการใช้สถานะพัวพันจำนวนมากเรียกว่าสถานะกลุ่มอนุภาค (Cluster states) มาเป็นสิ่งตั้งต้นสำหรับการคำนวณ จากนั้นการวัด (Measurement) บนคิวบิตจำนวนหนึ่งในสถานะกลุ่มอนุภาคจะทำให้เกิดเกตลอจิกเชิงควอนตัมที่ต้องการ ลงบนคิวบิตที่เหลืออยู่ และเนื่องจากการวัดสถานะเป็นกระบวนการย้อนกลับไม่ได้ การคำนวณโดยใช้การวัดสถานะดังกล่าวนี้จึงเรียกว่าการประมวลผลเชิงควอนตัมแบบทางเดียว (One-way quantum computation) หรือ การคำนวณเชิงควอนตัมแบบอิงอาศัยการวัด (Measurement-based quantum computation) ซึ่งมีข้อดีกว่าแบบจำลองวงจรเชิงควอนตัม (Quantum circuit) เนื่องจากทรัพยากรตั้งต้นคือสถานะกลุ่มอนุภาคไม่ได้มีความเฉพาะเจาะจงถึงรูปแบบการคำนวณที่จะเกิดขึ้นจึงสามารถทำการคำนวณเชิงควอนตัมลักษณะที่ต้องการโดยไม่จำเป็นต้องมีเกต CNOT ที่ประสิทธิภาพสูงเหมือนเช่นกรณีวงจรเชิงควอนตัม[4.13][*Perez-Delgado&Kok 2009*]

4.2.4.2 การคำนวณเชิงควอนตัมแบบควบคุมองค์รวม (Globally-controlled quantum computing)

การคำนวณเชิงควอนตัมแบบควบคุมองค์รวม เสนอโดย เซธ ลอยด์ (Seth Lloyd) ในปี ค.ศ. 1993 ซึ่งวิธีการคำนวณเชิงควอนตัมลักษณะนี้มีความแตกต่างจากแบบจำลองวงจรเชิงควอนตัมอย่างสิ้นเชิง เนื่องจากหน่วยย่อยของการคำนวณไม่ใช่เกตลอจิกเชิงควอนตัม แต่อาศัยการมีอันตรกิริยาระหว่างสองเซลล์เชิงควอนตัมที่อยู่ติดกัน ซึ่งสามารถเปิด-ปิด อันตรกิริยาดังกล่าวได้ ตัวอย่างเช่นการใช้อนุภาคที่มีสปิน 1/2 ในคริสตัลหรือในแลตทิซเชิงแสง (Optical lattice) เรียกเซลล์เชิงควอนตัมในโครงสร้างหนึ่งมิติของอนุภาคดังกล่าวว่า 'โซ่สปิน' (Spin chain) การอ่านสถานะของเซลล์เชิงควอนตัมต้องทำการวัดสถานะแบบองค์รวม (Global) ไม่สามารถเจาะจงสถานะของสปินที่ต้องการได้อย่างตรงไปตรงมา [*Perez-Delgado & Kok 2009*] แบบจำลองนี้มีลักษณะเหมือนกับออโตมาตาเซลลูลาร์เชิงควอนตัม (Quantum cellular automata) [*Lent และคณะ 1993*] ซึ่งมีเงื่อนไขเพิ่มเติมเล็กน้อยและเป็นแบบจำลองที่ได้รับการพิสูจน์ว่าสามารถทำการคำนวณเชิงควอนตัมทุกรูปแบบได้ (universal) [*Volbrecht & Cirac 2006*]

4.2.4.3 การคำนวณเชิงควอนตัมแบบแอเดียแบติก (Adiabatic quantum computing)

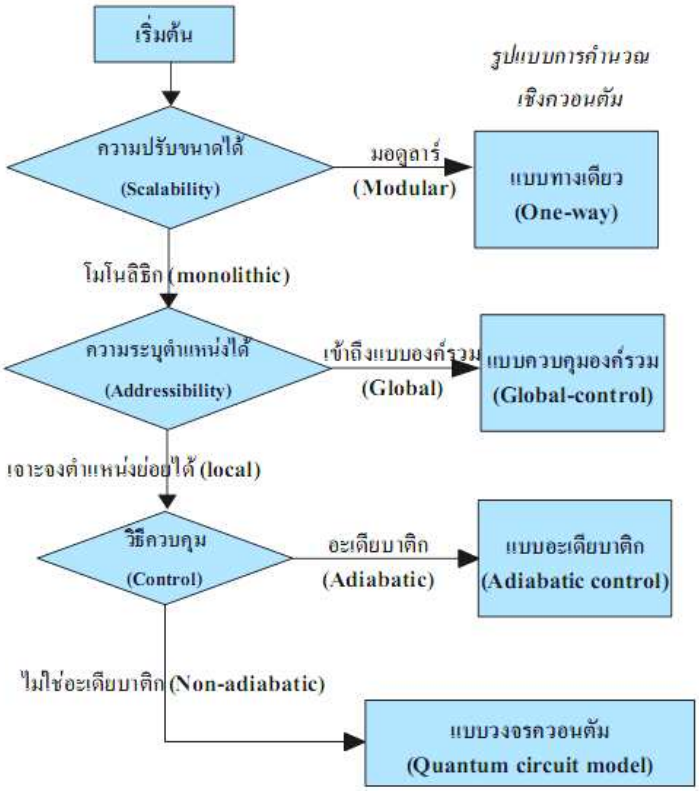
การคำนวณเชิงควอนตัมแบบแอเดียแบติกไม่ได้แบ่งช่วงเวลาแบบไม่ต่อเนื่องเหมือนเช่นในแบบจำลองวงจรเชิงควอนตัม [*Perez-Delgado และ Kok 2009*] แต่ใช้เวลาและการเปลี่ยนแปลงแบบต่อเนื่อง เป็นรูปแบบการคำนวณเชิงควอนตัมที่ตั้งอยู่บนทฤษฎีแอเดียแบติก (Adiabatic theorem) ซึ่งเสนอโดยแมกซ์ บอร์น (Max Born) และ ฟอกซ์ (V. Fox) ตั้งแต่ปี ค.ศ. 1928 โดยหลักการของการคำนวณเชิงควอนตัมแบบแอเดียแบติก จะแทนการคำนวณด้วยฮามิลโทเนียน ซึ่งเปลี่ยนแปลงจากเริ่มต้น H_0 (ฮามิลโทเนียนของสถานะพื้น) ไปยัง H_f (ฮามิลโทเนียนของสถานะผลลัพธ์) โดยขั้นตอนวิธีที่เหมาะสมสำหรับการสาธิตการทำงานของการคำนวณแบบแอเดียแบติกคือ การค้นฐานข้อมูลเชิงควอนตัม [*Grover 1996*]

จากการที่มีแบบจำลองหลายชนิดในการคำนวณเชิงควอนตัม จึงจำเป็นต้องมีวิธีตัดสินใจว่าสำหรับระบบควอนตัมหนึ่งๆ ควรใช้แบบจำลองการคำนวณใดจึงเหมาะสม โดยได้มีการเสนอวิธีเลือกใช้แบบจำลองการคำนวณ สรุปได้เป็นแผนผัง ดังรูปที่ 4.21

4.3 ขั้นตอนวิธีเชิงควอนตัม (Quantum Algorithms)

ในปี ค.ศ. 1992 เดวิด ดอยช์ (David Deutsch) และริชาร์ด จอสซา (Richard Jozsa) ร่วมกันเสนอกระบวนวิธีแก้ปัญหาเชิงควอนตัมวิธีแรก ซึ่งอาศัยคุณสมบัติทับซ้อนเชิงตำแหน่งมาช่วยในการแก้ปัญหาการวิเคราะห์คุณลักษณะของฟังก์ชันว่าเป็นฟังก์ชันคงที่ (Constant function) หรือฟังก์ชันสมดุล (Balanced function) เรียกกระบวนวิธีดังกล่าวว่า *'วิธีของดอยช์-จอสซา'* (Deutsch-Jozsa algorithm) [*Deutsch & Jozsa 1992*] ซึ่งจากคุณสมบัติทับซ้อนเชิงตำแหน่งทำให้ได้คำตอบเร็วขึ้นเป็นเอกซ์โพเนนเชียล ถึงแม้โจทย์ปัญหาดังกล่าวจะห่างไกลจากการใช้ประโยชน์จริงในชีวิตประจำวัน แต่ก็เป็นสิ่งที่ควรศึกษาเพื่อให้เห็นภาพการทำงานของการแก้ปัญหาด้วยวิธีเชิงควอนตัม การทดลองสาธิตการทำงานตามกระบวนวิธีของดอยช์-จอสซา มีขึ้นด้วย NMR โดยใช้สถานะ

[4.13] เนื่องจากในการคำนวณเชิงควอนตัมแบบทางเดียวเกต CNOT ที่ต้องการอาจถูกทำให้เกิดในบริเวณใด ๆ ของสถานะกลุ่มอนุภาคก็ได้



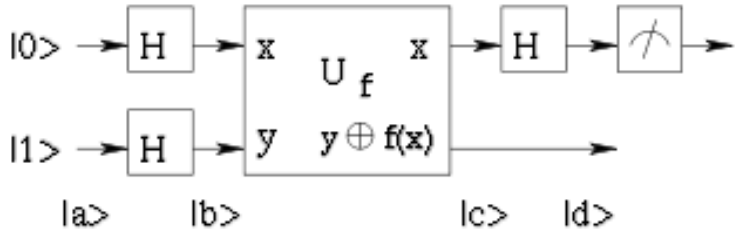
รูปที่ 4.21 แผนผังวิธีการเลือกรูปแบบหรือแบบจำลองการคำนวณเชิงควอนตัม ซึ่งเหมาะสมกับระบบควอนตัมในทางกายภาพหนึ่งๆ [*Perez-Delgado และ Kok 2009*]

สปินของนิวเคลียสแทนคิวบิต มีนักวิจัยหลายกลุ่มทั่วโลกทำการทดลองเพื่อยืนยันการทำงานของขั้นตอนวิธีเชิงควอนตัมนี้ เช่นกลุ่มของไอแซก ชวง (Isaac Chuang) [*Chuang และคณะ 1998*] และกลุ่มของโจนาธาน โจนส์ (Jonathan Jones) ในปี ค.ศ. 1998 [*Jones & Mosca 1998*] และการทดลองการดักจับไอออนในปี ค.ศ.2003 โดยสเตฟาน กุลเด (Stephan Gulde) และกลุ่มวิจัยที่ออสเตรีย [*Gulde และคณะ 2003*]

ในปี ค.ศ. 1994 แดน ไซมอน (Dan Simon) ได้เสนอวิธีทางควอนตัมในการหาคาบของฟังก์ชัน [*Simon 1994*] และจากสิ่งที่ไซมอนเสนอ ทำให้ปีเตอร์ ชอร์ (Peter Shor) ค้นพบวิธีเชิงควอนตัมสำหรับการแยกตัวประกอบและการหาลอการิธึมไม่ต่อเนื่องในเวลาเป็นโพลิโนเมียล [*Shor 1994*] แทนที่จะเป็นเอกซ์โพเนนเชียลดังเช่นวิธีที่ดีที่สุดในคอมพิวเตอร์เชิงดิจิทัล การค้นพบของชอร์ ทำให้ความปลอดภัยของข้อมูลที่ขึ้นกับความซับซ้อนทางคณิตศาสตร์ในการแยกตัวประกอบ เช่น RSA หรือในการหาผลเฉลยของสมการ เช่น วิทยาการรหัสลับด้วยเส้นโค้งเชิงวงรี (Elliptic-curve cryptography) ซึ่งแก้ได้ด้วยขั้นตอนวิธีลอการิทึมไม่ต่อเนื่องแบบชอร์ (Shor's discrete-log algorithm) ขาดความปลอดภัยในทันที (ในเชิงทฤษฎี) หากอุปกรณ์คำนวณเชิงควอนตัมในสเกลใหญ่และมีเสถียรภาพสามารถสร้างขึ้นได้จริง และหลังจากนั้นอีกสองปี ลอฟ กรอฟเวอร์ (Lov Grover) จากห้องทดลองของเบลล์ ได้เสนอวิธีค้นฐานข้อมูลเชิงควอนตัมซึ่งช่วยหาข้อมูลไม่เรียงลำดับได้รวดเร็วกว่าแบบดั้งเดิมในลำดับยกกำลังสองเท่า [*Grover 1996*]

4.3.1 กระบวนวิธีของดอยช์-จอสซา (Deutsch-Jozsa algorithm)

วิธีของดอยช์-จอสซา เป็นวิธีการคำนวณเชิงควอนตัมวิธีแรกเพื่อสาธิตให้เห็นว่าการแก้ปัญหาด้วยการคำนวณเชิงควอนตัมสามารถทำได้จริง และมีประสิทธิภาพในการคำนวณสูงกว่าวิธีการของคอมพิวเตอร์ในปัจจุบัน ซึ่งมีวิธีการดังนี้



รูปที่ 4.22การทำงานของขั้นตอนวิธีแบบดอยช์-จอสซาบนสองคิวบิต

4.3.1.1 โจทย์ปัญหาของดอยช์ (Deutsch's problem)

กระบวนวิธีเชิงควอนตัมแรกนี้มีการเสนอเพื่อสาธิตการเพิ่มความเร็วในการแก้ปัญหาด้วยการคำนวณเชิงควอนตัม ซึ่งแก้ปัญหาบางอย่างได้เร็วกว่าวิธีคำนวณดั้งเดิมในระดับเอกซ์โพเนนเชียล ปัญหาเพื่อการสาธิตดังกล่าวเรียกว่า *'โจทย์ปัญหาของดอยช์'* โดยนิยามว่า มีผู้เล่นสองคน ผู้เล่น ก. มีฟังก์ชัน $f:\{0,1\}^N$ --> {0,1} ซึ่งเป็นได้เพียงสองชนิดคือฟังก์ชันสมดุล หรือฟังก์ชันคงที่ และผู้เล่น ข. ทำหน้าที่เลือกตัวเลขเพียงค่าเดียวระหว่าง 0 ถึง 2^N-1 แล้วส่งตัวเลขดังกล่าว (x) ให้ ก. เพื่อคำนวณ $f(x)$ และตอบกลับไป คำถามคือ วิธีใดที่ ก. และ ข. จะสื่อสารกันน้อยที่สุดเพื่อให้ ข. ตัดสินใจได้ว่า f เป็นฟังก์ชันชนิดใด [*Nielsen & Chuang 2000*]

วิธีดั้งเดิม ผู้เล่น ข. สามารถส่งตัวเลข x ไปยัง ก. ได้เพียงครั้งละหนึ่งตัวเลข ในกรณีแย่ที่สุด ผู้เล่น ข. ต้องส่งตัวเลข x เป็นจำนวน $2^N/2 + 1$ ตัวเลขจึงทราบได้ว่า f เป็นฟังก์ชันคงที่หรือสมดุล[4.14] ในขณะที่วิธีเชิงควอนตัมของดอยช์-จอสซา ใช้การส่งตัวเลขเพียง*ครั้งเดียว* ซึ่งมีความหมายว่าใช้เวลาเร็วขึ้นเป็นเอกซ์โพเนนเชียล [*Deutsch & Jozsa 1992*]

4.3.1.2 วิธีของดอยช์-จอสซา

การทำงานด้วยวิธีของดอยช์-จอสซา แสดงเป็นกระบวนการทำงานเชิงควอนตัมได้ดังรูปที่ 4.22
การทำงานจะเริ่มจากจากสถานะเริ่มต้น

$$|a\rangle = |0\rangle|1\rangle \qquad \text{.....(4.3)}$$

ถูกเปลี่ยนเป็นสถานะทับซ้อนเชิงตำแหน่งด้วยเกตฮาดามาร์ด (H)

$$|b\rangle = (H \otimes H)|0\rangle|1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \qquad \text{.....(4.4)}$$

จากนั้นผ่านเกต 2 คิวบิต U_f ที่แทนการทำงานของฟังก์ชัน f(x) นิยามโดย

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle \qquad \text{.....(4.5)}$$

[4.14] หากส่ง x เป็นจำนวน $2^N/2$ ตัวเลข แล้วพบว่า $f(x) = 0$ ทั้งหมด ยังไม่สามารถสรุปได้ว่า f เป็นฟังก์ชันคงที่ หรือ ฟังก์ชันสมดุล

ดังนั้นสถานะผลลัพธ์

$$
\begin{aligned}
|c\rangle &= |0\rangle|0\oplus f(0)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|0\oplus f(1)\rangle - |1\rangle|1\oplus f(1)\rangle \\
&= |0, f(0)\rangle - |0, \overline{f(0)}\rangle + |1, f(1)\rangle - |1, \overline{f(1)}\rangle \\
&= \ldots \\
&= \left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)\left(|0\rangle - |1\rangle\right) \\
&= \pm\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right) \quad \text{ถ้า } f(0) = f(1) \\
&= \pm\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right) \quad \text{ถ้า } f(0) \neq f(1)
\end{aligned}
\qquad \ldots\ldots(4.6)
$$

และเมื่อผ่านเกตฮาดามาร์ดสุดท้าย สถานะทับซ้อนเชิงตำแหน่งของคิวบิตที่หนึ่ง จะถูกเปลี่ยนเป็นสถานะ $|0\rangle$ และ $|1\rangle$

$$
\begin{aligned}
|d\rangle &= \pm|0\rangle(|0\rangle - |1\rangle) \quad \text{ถ้า } f(0) = f(1) \text{ (}\textit{ฟังก์ชันคงที่}\text{)} \\
&= \pm|1\rangle(|0\rangle - |1\rangle) \quad \text{ถ้า } f(0) \neq f(1) \text{ (}\textit{ฟังก์ชันสมดุล}\text{)}
\end{aligned}
\qquad \ldots\ldots(4.7)
$$

ดังนั้น จากการวัดคิวบิตแรกที่อยู่บนสุด หรือซ้ายมือในสมการของสถานะผลลัพธ์ $|d\rangle$ จะทราบทันทีว่าฟังก์ชัน f มีลักษณะฟังก์ชันคงที่หรือฟังก์ชันสมดุล เนื่องจากสถานะ $|0\rangle$ และ $|1\rangle$ เป็นสถานะตั้งฉากและสามารถแยกแยะจากกันได้ด้วยการวัดสถานะเพียงครั้งเดียว อนึ่งเครื่องหมายบวกและลบด้านหน้าสุดนั้น เป็นเฟสองค์รวม (Global phase) ซึ่งไม่มีผลทางกายภาพ[4.15]

การคำนวณเชิงควอนตัมอาศัยคุณสมบัติทับซ้อนเชิงตำแหน่งซึ่งแต่ละสถานะย่อยจะถูกดำเนินการพร้อมกันด้วยเกตลอจิกเชิงควอนตัม และที่ฝั่งผลลัพธ์ถึงแม้ว่าผลการวัดสถานะจะถูกแปลงไปสู่ค่าใดค่าหนึ่ง แต่ก็สามารถรู้พฤติกรรมของเกตลอจิก U_f ได้ในการทำงานเพียงครั้งเดียวถึงจะเป็นความรู้ที่ไม่สมบูรณ์ก็ตามที เช่นในกรณีของขั้นตอนวิธีแบบดอยช์-จอสซา จะรู้คุณลักษณะของ f ว่า เป็นฟังก์ชันสมดุลหรือฟังก์ชันคงที่ในการทำงานเพียงครั้งเดียว แต่ไม่รู้พฤติกรรมทั้งหมดของ f

4.3.1.3 การเปรียบเทียบวิธีของดอยช์-จอสซา กับปัญหาที่ใกล้เคียงชีวิตประจำวัน

จากการที่โจทย์ปัญหาของดอยช์ และวิธีแก้ปัญหาของดอยช์-จอสซา อธิบายด้วยคณิตศาสตร์ซึ่งปรากฏเหมือนขาดความสำคัญในชีวิตประจำวัน จึงมีการเปรียบเทียบปัญหาดังกล่าว ว่าเหมือนกับการพิจารณาตัดสินเหรียญหนึ่ง ว่าเป็นเหรียญปกติ (มีหัว-ก้อย) หรือเหรียญที่โกง (สองหน้าเหมือนกัน) เหรียญที่ปกติ เทียบได้กับฟังก์ชันสมดุล และเหรียญที่โกง เทียบได้กับฟังก์ชันคงที่ ดังรูปที่ 4.23 โดยในวิธีแบบดั้งเดิม ต้องเปิดดูเหรียญ*สองครั้ง*จึงทราบว่าเหรียญนั้นเป็นแบบสมดุล หรือแบบคงที่ ส่วนในวิธีเชิงควอนตัมจะทำการดูเพียง*ครั้งเดียว* [*Stolze & Suter 2004*]

4.3.2 วิธีค้นหาข้อมูลเชิงควอนตัมโดยกรอฟเวอร์ (Grover's search algorithm)

ขั้นตอนวิธีแบบกรอฟเวอร์ (Grover's Algorithm) เป็นวิธีการค้นหาฐานข้อมูลซึ่งมีการนำเสนอดังรูปที่ 2.24 โดยเป็นวิธีค้นฐานข้อมูลที่ไม่เรียงลำดับด้วยเวลา $\sqrt{N}$ เมื่อ N คือจำนวนข้อมูล ซึ่งวิธีดั้งเดิมคือการไล่หาทีละข้อมูลแบบเชิงเส้นจะใช้เวลาต่ำที่สุดคือ 1 (ค้นแล้วเจอทันที) และใช้เวลามากที่สุด N (ค้นเจอเมื่อถึงข้อมูลสุดท้าย) และใช้เวลาเฉลี่ย N/2 ดังนั้นการที่วิธีเชิงควอนตัมช่วยลดเวลาเหลือ $\sqrt{N}$ เรียกว่าเป็น 'เร็วขึ้นยกกำลังสอง' (Quadratic improvement) เนื่องจาก $N = (\sqrt{N})^2$ ซึ่งความแตกต่างจะปรากฏชัดเมื่อ N มีค่ามาก

วิธีค้นหาของกรอฟเวอร์สามารถสรุปเป็นแผนภาพได้ดังรูปที่ 4.25

[4.15] ไม่มีผลต่อสถิติการวัด เนื่องจากความน่าจะเป็นที่จะออกสถานะแต่ละอย่างเท่ากับขนาดของสัมประสิทธิ์ของสถานะนั้น ยกกำลังสอง ซึ่งจะทำให้เครื่องหมาย +/- ด้านหน้าสุดหายไป

(ก) (ข)

รูปที่ 4.23 เปรียบเทียบการทำงานของการแก้โจทย์ปัญหาของดอยช์-จอสซา (ก) เหรียญแบบสมดุล ด้านหน้า-หลัง ไม่เหมือนกัน (ข) เหรียญแบบคงที่ (constant) ด้านหน้า-หลัง เหมือนกัน เมื่อตีความเป็นฟังก์ชันของการมองดูเหรียญทีละด้าน (input x = ด้านหน้า/หลัง) (output f = หัว/ก้อย) ฟังก์ชันสมดุล "balanced function" f(ด้านหน้า) = หัว f(ด้านหลัง) = ก้อย ฟังก์ชันคงที่ "constant function" f(ด้านหน้า) = หัว f(ด้านหลัง) = หัว

A fast quantum mechanical algorithm for database search

Lov K. Grover

3C-404A. Bell Labs

(ก)

Summary

Imagine a phone directory containing N names arranged in completely random order. In order to find someone's phone number with a probability of $\frac{1}{2}$, any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of $\frac{N}{2}$ names. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names. By properly adjusting the phases of various operations, successful computations reinforce each other while others interfere randomly. As a result, the desired phone number can be obtained in only $O(\sqrt{N})$ steps. The algorithm is within a small constant factor of the fastest possible quantum mechanical algorithm.

(ข)

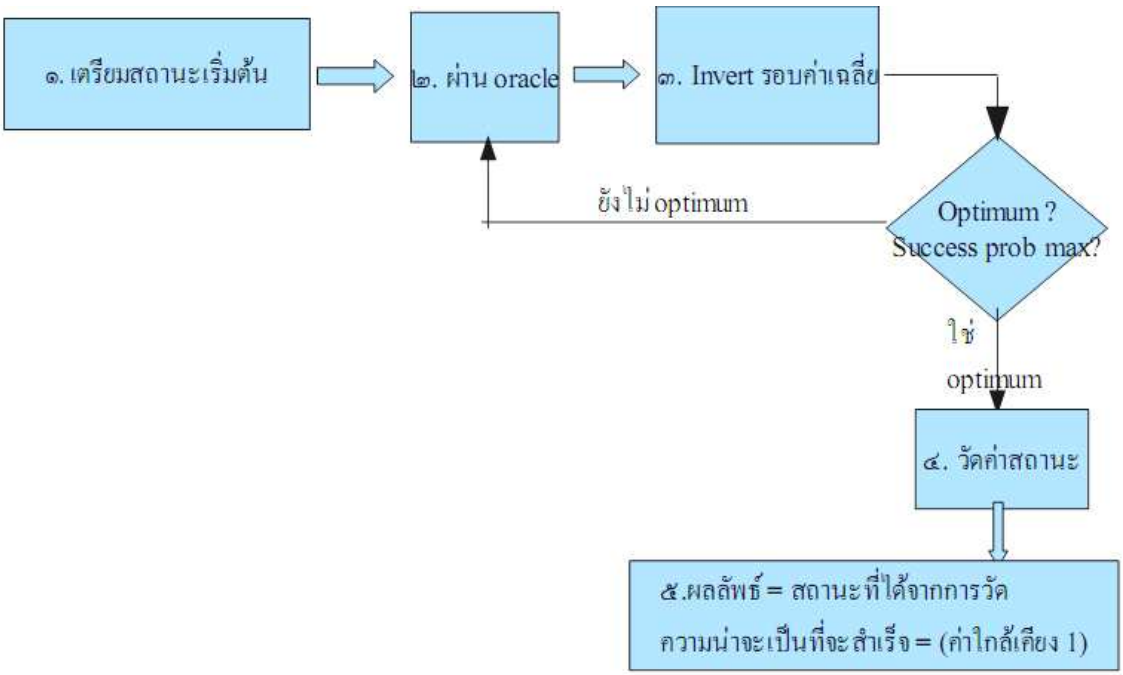
(ค)

รูปที่ 4.24 (ก) หัวบทความค้นฐานข้อมูลด้วยวิธีทางควอนตัม (ข) สรุปความ [*Grover 1996*] (ค) ลอฟ กรอฟเวอร์ (Lov Grover) ผู้ค้นพบวิธีเชิงควอนตัมสำหรับการค้นหาข้อมูล [*Bell-Labs.com*]

ขั้นตอนวิธีแบบกรอฟเวอร์มีขั้นตอนการทำงานเริ่มจากมีข้อมูลที่ไม่เรียงลำดับทั้งหมด N ข้อมูล (ใช้เลขดัชนี 0, 1, …, N-1) โดยข้อมูลที่ต้องการค้นหาอยู่ในลำดับที่ a

ขั้นต้น นิยามฟังก์ชัน f โดยที่ $f(x)=0$ เมื่อ $x\neq a$ และ $f(x)=1$ เมื่อ $x=a$ ทำหน้าที่เป็นฟังก์ชันระบุเป้าหมาย (Tagging function) แล้วจึงดำเนินการดังนี้

1) เตรียมสถานะเริ่มต้นโดยการผ่านสถานะ |000...0> ไปยังเกตฮาดามาร์ดทั้ง n คิวบิต



รูปที่ 4.25 สรุปขั้นตอนการทำงานของการค้นฐานข้อมูลเชิงควอนตัม

$$\frac{1}{\sqrt{N}}(|0\rangle+|1\rangle+...|N-1\rangle) \qquad .....(4.8)$$

2) การผ่านออราเคิลโดยทำการกลับเครื่องหมายหรือการกลับเฟสของคิวบิต x ซึ่ง $f(x) = 1$ ผลที่ได้ คือ

$$\frac{1}{\sqrt{N}}(|0\rangle+|1\rangle+...-|x\rangle+|x+1\rangle|N-1\rangle) \qquad .....(4.9)$$

3) ทำการผกผัน (Invert) รอบค่าเฉลี่ยเมื่อสถานะแทนด้วย

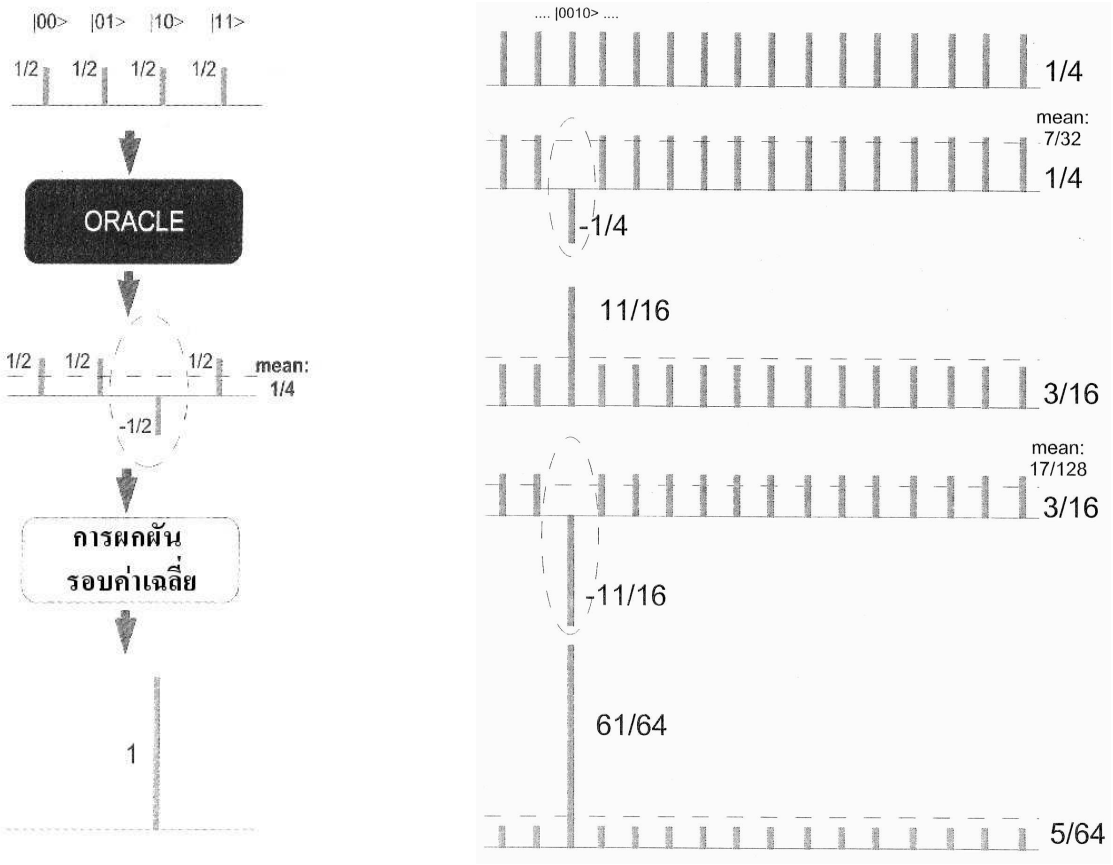
$$\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} l_i|i\rangle \qquad .....(4.10)$$

ค่าเฉลี่ยของแอมปลิจูด (m) นิยามโดย

$$m=\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} l_i \qquad .....(4.11)$$

และการผกผันรอบค่าเฉลี่ยทำให้ได้ค่าแอมพลิจูดใหม่ l_i* ซึ่งนิยามโดย $l_i(\text{ใหม่})=m-(l_i-m)=2\mathrm{m}-l_i$

4) ตรวจสอบว่าขั้นตอนวิธีทำงานมาถึงค่าเหมาะที่สุด (Optimum) หรือยัง โดยพิจารณาจากค่าที่ให้ความน่าจะเป็น (Probability) ที่จะได้สถานะที่ต้องการสูงสุด ถ้ายังไม่ถึงค่าเหมาะสมที่สุดให้กลับไปขั้นตอนที่ 3 ใหม่



รูปที่ 4.26 การทำงานของการค้นหาข้อมูลแบบกรอฟเวอร์บนฐานข้อมูล
(ก) สองคิวบิต และ (ข) สี่คิวบิต รูปดัดแปลงจาก [*Morsch 2008*]

5) ถ้าถึงค่าเหมาะสมที่สุดแล้วทำการวัดสถานะ ด้วยความน่าจะเป็นที่เข้าใกล้ค่าหนึ่งจะได้สถานะที่ต้องการค้นหาออกมา และสิ้นสุดกระบวนการค้นหาข้อมูล

จากที่กล่าวมาสามารถแสดงตัวอย่างการค้นหาข้อมูลเชิงควอนตัมได้เช่นสองกรณีดังต่อไปนี้

ตัวอย่างที่ 1 ฐานข้อมูลสองบิต

การค้นหาข้อมูลสองคิวบิต โดยสมมติว่าข้อมูลที่ต้องการค้นหาอยู่ที่คิวบิต “10” เริ่มจากเตรียมสถานะตั้งต้นเป็น สถานะทับซ้อนเชิงตำแหน่งของทุกสถานะในสองคิวบิต คือ $\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)$ (ดูรูปที่ 4.26 (ก) ประกอบ) จากนั้นทำการผ่านเข้าสู่กล่องดำเพื่อกลับเครื่องหมายของคิวบิตที่ต้องการค้นหา[4.16] เป็น $\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle+|11\rangle)$ คำนวณหาค่าเฉลี่ยของสัมประสิทธิ์ได้ $m = (½ + ½ - ½ + ½)/4 = ¼$ จากนั้นทำการหมุนรอบค่าเฉลี่ย สัมประสิทธิ์ของ $|00\rangle$ คือ ½ จะเปลี่ยนเป็น $m - (½ - m) = ¼ - (½ - ¼) = 0$ เช่นเดียวกับสัมประสิทธิ์ของ $|01\rangle$ และ $|11\rangle$ (ซึ่งสัมประสิทธิ์จะถูกเปลี่ยนจาก ½ เป็นศูนย์ ด้วยการหมุนรอบค่าเฉลี่ย) ส่วนสถานะ $|10\rangle$ ซึ่งมีสัมประสิทธิ์เป็น -1/4 เมื่อหมุนรอบค่าเฉลี่ย สัมประสิทธิ์จะถูกเปลี่ยนเป็น $m - (-1/4 - m) = ¼ - (-¼ - ¼) = 1$ นั้นคือ มีความน่าจะเป็น 100% ที่ทำการวัดสถานะแล้วจะให้ผลลัพธ์เป็น $|10\rangle$

[4.16] การกลับเครื่องหมายลักษณะนี้ ไม่มีผลต่อความน่าจะเป็นของการวัดแต่อย่างใด เนื่องจากความน่าจะเป็นที่จะได้สถานะ |10> ยังคงเท่ากับ ¼ หรือ $(-½)^2$ เช่นเดิม

ตัวอย่างที่ 2 ฐานข้อมูลสี่บิต

มีการทำงานลักษณะเดียวกับกรณีสองคิวบิต หากแต่ต้องเพิ่มจำนวนรอบ เนื่องจากการทำงานของขั้นตอนวิธีหนึ่งครั้ง ยังไม่ให้ค่าความน่าจะเป็นสูงสุดสำหรับสถานะที่ต้องการ (ครั้งแรกได้ 11/16 หรือประมาณ 47%) แต่เมื่อทำการ 'ผ่านกล่องดำ' และ 'หมุนรอบค่าเฉลี่ย' ครั้งที่สองแล้ว จึงได้ความน่าจะเป็นที่สูงขึ้นอีก (กลายเป็น 61/64 หรือประมาณ 91%) อย่างไรก็ตามการทำงานของขั้นตอนวิธีไม่ได้ลู่เข้าสู่ความน่าจะเป็นที่มีค่า 1 เมื่อจำนวนรอบมากขึ้นแต่อย่างใด หากแต่มีจุดหนึ่งที่ให้ความน่าจะเป็นสูงสุด จากนั้นค่าจะกลับลดลงอีก

จำนวนรอบที่ดีที่สุดในกระบวนการหมุนรอบค่าเฉลี่ยด้วยขั้นตอนวิธีแบบกรอฟเวอร์ คือจำนวนรอบที่ทำให้กระบวนการค้นหาเชิงควอนตัมได้ค่าความน่าจะเป็นสูงสุดที่จะได้สถานะที่ต้องการ เมื่อผ่านลูปการผ่านออราเคิลและผกผันรอบค่าเฉลี่ยทั้งหมด $\frac{\pi}{4}\sqrt{N}$ ครั้ง โดยเมื่อถึงจุดที่แอมพลิจูดของสถานะเป้าหมายมีค่าสูงสุดแล้ว หากทำการวนซ้ำจะทำให้ผลลัพธ์แย่ลง "กระบวนวิธีค้นหาเชิงควอนตัมเปรียบเหมือนการต้มน้ำซุป โอกาสแห่งความสำเร็จ (Success probability) จะมีค่าสูงสุดเมื่อจำนวนการวนรอบพอดี หากมากกว่านั้นความน่าจะเป็นที่จะสำเร็จจะกลับลดลงอีก" [*Brassard 1997*]

สรุปแล้วการค้นหาข้อมูลแบบกรอฟเวอร์อาศัยคุณสมบัติความทับซ้อนเชิงตำแหน่ง ร่วมกับเทคนิคการปรับเปลี่ยนสัมประสิทธิ์ของสถานะรอบแกนสมมาตรให้เท่ากับค่าเฉลี่ยของสัมประสิทธิ์ทั้งหมด โดยจัดเป็นหนึ่งในวิธีทางควอนตัมที่ช่วยให้การทำงานเร็วกว่าวิธีการแบบดั้งเดิม (กรณีนี้ เร็วขึ้น จาก N เป็น $\sqrt{N}$) อย่างไรก็ตาม ในการทดลองจริงนอกจากต้องหาระบบควอนตัมที่นำมาแทนคิวบิตแล้ว ยังต้องหาวิธีปรับเปลี่ยนสถานะให้ได้ผลลัพธ์ตามที่ต้องการใน 'กล่องดำ' และ 'การหมุนรอบค่าเฉลี่ย' [*Ivanov และคณะ 2008*]

4.3.3 วิธีแยกตัวประกอบเชิงควอนตัมของชอร์ (Shor's factorization algorithm)

ขั้นตอนวิธีแบบชอร์ (Shor's algorithm) พัฒนามาจากวิธีการหาคาบเชิงควอนตัมของ แดน ไซมอน (Dan Simon) [*Simon 1994*] ซึ่งแสดงดังรูปที่ 4.27 นับเป็นขั้นตอนวิธีที่ดึงดูดความสนใจในวิชาการคำนวณเชิงควอนตัมและความปลอดภัยของข้อมูลเป็นอย่างมากเนื่องจากผลลัพธ์ที่ได้คือ

> การแยกตัวประกอบเฉพาะของจำนวนเต็มด้วยเวลาเพียง N^3 เมื่อ N *คือจำนวนบิตของตัวเลขในการคำนวณ ซึ่งจากเดิมต้องใช้เวลาถึงอันดับ* 2N *(เอกซ์โพเนนเชียล) โดยสิ่งที่อยู่เบื้องหลังการทำงานของวิธีแยกตัวประกอบของชอร์ คือ คุณสมบัติทับซ้อนเชิงตำแหน่ง [Shor 1994]* ขั้นตอนวิธีเชิงควอนตัมสำหรับการแยกตัวประกอบดังกล่าว ไม่ได้ประกอบด้วยขั้นตอนที่เป็น 'ควอนตัม' ทุกขั้นตอนแต่อย่างใด หากแต่ประกอบด้วยส่วนที่มีการคำนวณแบบดั้งเดิมผสมผสานกัน ดังนั้น ในที่นี้จึงจะเริ่มการพิจารณาการแยกตัวประกอบด้วยวิธีดั้งเดิมก่อนที่จะผสมส่วนควอนตัมลงไปจนกลายเป็น 'วิธีแยกตัวประกอบแบบชอร์'

- **วิธีแยกตัวประกอบดั้งเดิมโดยการหาคาบของลำดับ (Sequence) ซึ่งอาศัยการหาคาบของฟังก์ชันร่วมกับการหาตัวหารร่วมมาก (ห.ร.ม.)[4.17] ของจำนวนเต็ม สรุปได้เป็นขั้นตอนดังต่อไปนี้**

  1) จำนวนเต็มที่ต้องการแยกตัวประกอบ คือ N

  2) เลือกจำนวนเต็ม a ซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กับ N กล่าวคือไม่มีตัวประกอบร่วมกับ N (ยกเว้น 1)

  3) หาลำดับ $a^X \bmod N$ เมื่อ $x = 0, 1, 2, 3,...$ และ $\bmod N$ หมายถึงการหารด้วย N แล้วคงไว้แต่เศษ

  4) หาคาบของลำดับ $\{a^x \bmod N\}$ ให้คาบแทนด้วย q กล่าวคือ $a^{(x+q)} \bmod N = a^x \bmod N$

  ถ้า q เป็นเลขคู่ ให้ไปต่อขั้นตอนที่ 5

  ถ้า q เป็นเลขคี่ ให้ไปเริ่มขั้นตอนที่ 1 ใหม่

[4.17] หารร่วมมาก (ห.ร.ม.) ของ a และ b หมายถึงจำนวนเต็ม c ที่มากที่สุดที่ทำให้ทั้ง a และ b หารด้วย c ลงตัว

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs

(ก)

Abstract

"...This paper gives Las Vegas algorithms for finding discrete logarithms and factoring ... that take a number of steps which is polynomial in the input size... (We thus give the first examples of quantum cryptanalysis.)"

(ข)

(ค)

รูปที่ 4.27 (ก) ชื่อผลงานของบทความแรกที่นำเสนอวิธีเชิงควอนตัมสำหรับแยกตัวประกอบ (ข) บทคัดย่อ [*Shor 1994*] (ค) ปีเตอร์ ชอร์ (Peter W. Shor)

5) คำนวณหา $a^{q/2} + 1$ และ $a^{q/2} - 1$

6) ห.ร.ม. $(a^{q/2} + 1, N)$ และ ห.ร.ม. $(a^{q/2} - 1, N)$ เป็นตัวประกอบเฉพาะ (prime factor) ของ N

หรือ N = ห.ร.ม.$(a^{q/2} + 1, N) \times$ ห.ร.ม.$(a^{q/2} - 1, N)$

ตัวอย่าง จงแยกตัวประกอบของ 21 ซึ่งทำได้โดยกระบวนการดังที่กล่าวมา เริ่มจาก

1) กำหนด $N = 21$

2) เลือก $a = 8$ ซึ่ง ห.ร.ม. ของ 8 และ 21 เท่ากับ 1 แสดงว่า 8 และ 21 เป็นจำนวนเฉพาะสัมพัทธ์กัน

3) ลำดับ $a^x \bmod N$ $\{8^0 \bmod 21 = 1, 8^1 \bmod 21 = 8, 8^2 \bmod 21 = 1, 8^3 \bmod 21 = 8, \ldots.\}$

4) (หาคาบ) ลำดับในขั้นตอนที่ 3 มีลักษณะซ้ำ {1,8,1,8,...} ดังนั้น คาบ = 2 *(q = 2)*

5) $a^{q/2} + 1 = 8^1 + 1 = 9$ และ $a^{q/2} - 1 = 7$

6) หาตัวหารร่วมมาก ห.ร.ม. (9, 21) = 3 และ ห.ร.ม. (7, 21) = 7

คำตอบ ได้ตัวประกอบของ 21 คือ 3 และ 7 นั่นคือ $21 = 3 \times 7$

สรุปว่าคุณสมบัติทัซ้อนเชิงตำแหน่ง ช่วยให้คำนวณลำดับ $a^x \bmod N$ โดยผ่านรีจิสเตอร์ (Register) เพียงครั้งเดียว และการแปลงฟูเรียร์เชิงควอนตัม[4.18] (Quantum Fourier Transform) ใช้ในการหาคาบของลำดับไปสู่การหาตัวประกอบต่อไป ซึ่งเมื่อประมวลเวลาที่ใช้ทั้งหมดแล้ว จะอยู่ที่อันดับ n^3 เมื่อ n เป็นความยาวของตัวเลขที่ต้องการแยกตัวประกอบ

- **กระบวนวิธีเชิงควอนตัมในการแยกตัวประกอบ (Shor's algorithm) สามารถแบ่งได้ดังนี้**

1) ส่วนการคำนวณแบบดั้งเดิม

- จำนวนเต็มที่ต้องการแยกตัวประกอบ คือ N
- เลือกจำนวนเต็ม a ซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กับ N กล่าวคือไม่มีตัวประกอบร่วมกับ N (ยกเว้น 1)

[4.18] ผลลัพธ์จากการแปลงฟูเรียร์ ก็คือความถี่หรือคาบของฟังก์ชันนั้น ๆ

2) ส่วนการคำนวณเชิงควอนตัม

- เตรียมสถานะเริ่มต้น $(|0\rangle+|1\rangle+|2\rangle+...+|k\rangle)|0\rangle$ โดยที่ k เป็นค่าที่มากพอที่จะปรากฏคาบของลำดับ $a^x \bmod N$

- ผ่านสถานะเริ่มต้น สู่ '$a^x \bmod N$' ออราเคิล ซึ่งทำหน้าที่แปลงสถานะ $|x\rangle|0\rangle$ ไปเป็น $|x\rangle|a^x mod\ N\rangle$ ดังนั้นสถานะเริ่มต้น $(|0\rangle+|1\rangle+|2\rangle+...+|k\rangle)|0\rangle$ จึงถูกเปลี่ยนเป็น $|0\rangle|a^0 mod\ N\rangle+|1\rangle|a^1 mod\ N\rangle+|2\rangle|a^2 mod\ N\rangle+...+|k\rangle|a^k mod\ N\rangle$

- ทำการวัดค่าสถานะของรีจิสเตอร์เชิงควอนตัมที่สอง (สถานะควอนตัมขวามือ) ได้ผลลัพธ์เป็นสถานะ $(|j\rangle+|j+q\rangle+|j+2q\rangle+...)|a^j mod\ N\rangle$ ด้วยความน่าจะเป็น $1/(k+1)^2$

- ผ่านสถานะที่ได้จากการวัดค่าเข้าสู่วงจรการแปลงฟูเรียร์เชิงควอนตัม เพื่อหาคาบของสถานะควอนตัมซ้ายมือ (คาบของ $|j\rangle+|j+q\rangle+|j+2q\rangle+...$ ได้คาบ = q)

3) กลับมาในส่วนการคำนวณแบบดั้งเดิม

- จาก q ที่ได้ คำนวณหา $a^{q/2}+1$ และ $a^{q/2}-1$

- ได้ ห.ร.ม. $(a^{q/2}+1, N)$ และ ห.ร.ม. $(a^{q/2}-1, N)$ เป็นตัวประกอบเฉพาะของ N

<u>ตัวอย่าง</u> การแยกตัวประกอบด้วยวิธีควอนตัมได้เช่นการแยกตัวประกอบของ 15 ซึ่งมีกระบวนการดังต่อไปนี้

1) กำหนด $N = 15$

2) (ส่วนการคำนวณแบบดั้งเดิม) เลือก $a = 7$ ซึ่งไม่มีตัวประกอบร่วมกับ 15

3) (ส่วนการคำนวณเชิงควอนตัม) เตรียมสถานะเริ่มต้น $|0\rangle|0\rangle+|1\rangle|0\rangle+|2\rangle|0\rangle+|3\rangle|0\rangle+...+|k\rangle|0\rangle$

4) (ส่วนการคำนวณเชิงควอนตัม) ผ่านสถานะเริ่มต้น สู่ '$7^x \bmod 15$' Oracle $|x\rangle|a^x mod\ N\rangle$ ได้ (รีจิสเตอร์ที่สอง -- ขวามือ เก็บ sequence) $|0\rangle|1\rangle+|1\rangle|7\rangle+|2\rangle|4\rangle+|3\rangle|13\rangle+|4\rangle|1\rangle+|5\rangle|7\rangle+...$

5) (ส่วนการคำนวณเชิงควอนตัม) ทำการวัดค่าสถานะของควอนตัมรีจิสเตอร์ที่สอง (สมมติว่าได้ผลลัพธ์เป็น “7” สถานะรวมที่ได้จะเป็น $(|1\rangle+|5\rangle+|9\rangle+|13\rangle+|17\rangle+|21\rangle)|7\rangle$

6) (ส่วนการคำนวณเชิงควอนตัม) นำสถานะที่ได้จากการวัด ผ่านเข้าสู่ Quantum Fourier Transform เพื่อหาคาบของสถานะควอนตัมในวงเล็บซ้ายมือ $|1\rangle+|5\rangle+|9\rangle+|13\rangle+|17\rangle+|21\rangle$ (ได้คาบ $q = 4$)

7) (ส่วนการคำนวณแบบดั้งเดิม) จาก q ที่ได้ หา $a^{q/2}+1 = 7^2+1 = 50$ และ $a^{q/2}-1 = 7^2-1 = 48$

8) (ส่วนการคำนวณแบบดั้งเดิม) ห.ร.ม.(50, 15) = 5 และ ห.ร.ม.(48, 15) = 3 ก็คือตัวประกอบของ 15

นั่นคือ $15 = 5 \times 3$

สรุปแล้ววิธีเชิงควอนตัมสำหรับการแยกตัวประกอบแบบชอร์ อาศัยการผสมผสานระหว่างวิธีดั้งเดิมและวิธีเชิงควอนตัม โดยอาศัยคุณสมบัติทับซ้อนเชิงตำแหน่งช่วยให้การหาคาบของฟังก์ชันเร็วขึ้นเป็นเอกซ์โพเนนเชียล และจากคาบดังกล่าวนำไปหาตัวประกอบต่อไปได้โดยตรง การแยกตัวประกอบเชิงควอนตัม ได้มีการทดลองจริงแล้วในการสั่นพ้องแม่เหล็กนิวเคลียร์ (Nuclear Magnetic Resonance: NMR) [*Vandersypen และคณะ 2001*] และในแสงที่ทำงานบนชิป [*Politi และคณะ 2009*]

4.3.4 สรุปกระบวนวิธีเชิงควอนตัม

กระบวนวิธีเชิงควอนตัมอาศัยคุณสมบัติทับซ้อนเชิงตำแหน่งช่วยให้สถานะเข้าหลายค่าถูกประมวลผลพร้อมกัน และอาศัยการวัดสถานะที่สามารถดึงข้อมูลที่ซ่อนอยู่ระหว่างการประมวลผลได้ กรณีกระบวนวิธีของดอยช์และจอสซา คุณสมบัติของฟังก์ชันสามารถวิเคราะได้ด้วยการวัดสถานะเพียงครั้งเดียว แต่คุณสมบัตินั้นไม่ใช่ข้อมูลทั้งหมดของฟังก์ชันนั้น หากแต่เป็นข้อมูลที่โจทย์สนใจ

4.4 การสูญเสียความอาพันธ์เชิงควอนตัม

สิ่งที่เป็นอุปสรรคของการสื่อสารและการคำนวณเชิงควอนตัม คือการรับผลกระทบจากสิ่งแวดล้อม ทำให้สูญเสียข้อมูลและคุณสมบัติเชิงควอนตัมบางอย่าง เรียกกระบวนการดังกล่าวว่า การสูญเสียความอาพันธ์เชิงควอนตัม หรือ 'Decoherence' โดยแต่ละระบบทางกายภาพมีความสามารถในการแยกตัวและคงคุณสมบัติเชิงควอนตัมไม่เท่ากัน ระยะเวลาที่ระบบจะคงคุณสมบัติเชิงควอนตัมที่ประสงค์ไว้ได้เรียกว่าระยะเวลาคงสถาพความอาพันธ์ (Decoherence time: T_d) การคำนวณเชิงควอนตัมจะต้องเสร็จภายในระยะเวลานี้ แต่ปัจจัยที่มีผลต่อการคำนวณเชิงควอนตัมไม่ใช่ระยะเวลาคงสภาพความอาพันธ์โดยตรง แต่เป็นจำนวนตัวดำเนินการลอจิกเชิงควอนตัม (Quantum logic operations) สูงสุดที่สามารถกระทำได้ต่อคิวบิตนั้นๆ (Number of operations: n_{op}) นิยามโดยระยะเวลาคงสภาพความอาพันธ์หารด้วยเวลาที่ใช้ในการทำงานต่อหนึ่งเกตลอจิกเชิงควอนตัม[4.19] (Gate operation time: T_{op})

$$n_{op} = \frac{T_d}{T_{op}} \qquad \text{.....(4.12)}$$

ซึ่งเป็นปริมาณที่บ่งบอกถึงความสามารถในการคำนวณเชิงควอนตัมบนระบบทางกายภาพหนึ่งๆ หาก n_{op} มีค่ามาก ระบบนั้นก็สามารถทำการคำนวณเชิงควอนตัมที่ซับซ้อน เช่นการแยกตัวประกอบเลขขนาดใหญ่ได้ การเปรียบเทียบค่านี้จากระบบกายภาพต่างๆที่ใช้สร้างลอจิกเกตแสดงดังภาพที่ 4.5

4.5 การควบคุมความผิดพลาดเชิงควอนตัมและการคำนวณเชิงควอนตัมแบบทนทานต่อความผิดพลาด

ความผิดพลาดของข้อมูลเชิงควอนตัมอันเนื่องจากอิทธิพลของสิ่งแวดล้อมเป็นอุปสรรคต่อการประมวลผลข้อมูลเชิงควอนตัม โดยเฉพาะในจำนวนคิวบิตและจำนวนกระบวนการหรือตัวดำเนินการจำนวนมากๆ ซึ่งนับแต่ปี ค.ศ. 1995 ได้มีการเสนอวิธีแก้ไขความผิดพลาดเชิงควอนตัม โดยการแทนข้อมูลควอนตัมหรือคิวบิตด้วยสถานะเชิงควอนตัมจำนวนมากขึ้นนั่นคือมีจำนวนคิวบิตมากขึ้น หรือเวกเตอร์ในมิติใหญ่ขึ้น

คาลเดอร์แบงค์ (A. R. Calderbank) ชอร์ (P.W. Shor) และ สตีน (A. Steane) เสนอวิธีเข้ารหัสเพื่อป้องกันความผิดพลาดรูปแบบใดๆ ก็ตามที่จะเกิดกับหนึ่งคิวบิต (CSS codes) ซึ่งตั้งอยู่บนสมมติฐานที่กระบวนการเข้ารหัสและถอดรหัสเชิงควอนตัมด้วยเกตลอจิกเชิงควอนตัมไม่มีข้อผิดพลาด แต่หากความผิดพลาดเกิดขึ้นกับเกตลอจิกเชิงควอนตัมเสียเอง การคำนวณเชิงควอนตัมก็ยังคงดำเนินไปอย่างเชื่อถือได้ตราบเท่าที่ความผิดพลาดมีค่าไม่เกินขีดจำกัดค่าหนึ่ง (Threshold) เรียกว่าการทนต่อความผิดพลาดจากการคำนวณเชิงควอนตัม (Fault-tolerant quantum computing) ซึ่งพิสูจน์โดย ปีเตอร์ ชอร์ ในปี ค.ศ. 1996 [Shor 1996] สรุปความว่า การคำนวณเชิงควอนตัมด้วยเกตลอจิกจำนวน t สามารถดำเนินได้ ตราบเท่าที่ความผิดพลาดของแต่ละเกตลอจิกมีค่าไม่เกินอันดับ $1/(\log c\ t)$ เมื่อ c คือค่าคงที่ ทำให้การทดลองการคำนวณเชิงควอนตัมสามารถกระทำได้ ถึงแม้การเปลี่ยนแปลงของสถานะควอนตัมหรือเกตลอจิกเชิงควอนตัมจะไม่สามารถดำเนินการได้โดยสมบูรณ์ อย่างไรก็ตามสำหรับการคำนวณเชิงควอนตัมที่ซับซ้อน เช่น การแยกตัวประกอบตัวเลขขนาดใหญ่ด้วยวิธีควอนตัม (t มาก) ความผิดพลาดของการทำงานเกตลอจิกเชิงควอนตัมต้องลดลง (ตาม t ที่มากขึ้น) ซึ่งเป็นขีดจำกัดของการคำนวณเชิงควอนตัมในภาคการทดลองจริง

[4.19] สิ่งที่ทำหน้าที่แทนตัวดำเนินการเชิงควอนตัมพื้นฐานเกตยูนิแทรี 1 คิวบิตและเกต CNOT

ตารางที่ 4.5 เปรียบเทียบระยะเวลาคงสภาพความอาพันธ์ เวลาการทำงานต่อหนึ่งเกตลอจิกเชิงควอนตัม และจำนวนตัวดำเนินการลอจิกเชิงควอนตัมที่ทำงานได้ ในระบบทางกายภาพต่างๆ (ข้อมูลภายใต้เทคโนโลยีในปี ค.ศ. 2000 [*Nielsen และ Chuang 2000*])

ระบบทางกายภาพ	เวลาก่อนสูญเสียความอาพันธ์ (วินาที) (Decoherence time: T_d)	เวลาทำงานต่อหนึ่งเกตลอจิกเชิงควอนตัม (วินาที) (Gate operation time: T_{op})	จำนวนตัวดำเนินการลอจิกเชิงควอนตัมที่ทำงานได้ (Number of operations: $n_{op} = T_d/T_{op}$)
สปินเชิงนิวเคลียร์ (Nuclear spin)	10^{-2} -- 10^{8}	10^{-3} -- 10^{-6}	10^{5} -- 10^{14}
สปินของอิเล็กตรอน (Electron spins)	10^{-3}	10^{-7}	10^{4}
ไอออนที่ถูกกัก (Trapped ions)	10^{-1}	10^{-14}	10^{13}
อิเล็กตรอนใน Au	10^{-8}	10^{-14}	10^{6}
อิเล็กตรอนใน GaAs	10^{-10}	10^{-13}	10^{3}
ควอนตัมดอท	10^{-6}	10^{-9}	10^{3}
Optical cavity	10^{-5}	10^{-14}	10^{9}
Microwave cavity	$10^{0} = 1$	10^{-4}	10^{4}

บทสรุป

เทคโนโลยีคอมพิวเตอร์เชิงคลาสสิกหรือแบบดั้งเดิมได้รับการพัฒนามาอย่างต่อเนื่องเริ่มจากการทำงานตามรูปแบบของเครื่องกลทูริง ด้วยอุปกรณ์คำนวณจากการใช้ไฟฟ้า เช่นหลอดสูญญากาศ ไปสู่ทรานซิสเตอร์และวงจรรวมที่มีขนาดเล็กลง จนในที่สุดจะไม่สามารถทำให้อุปกรณ์ที่ใช้ในการคำนวณเล็กลงไปได้อีก เนื่องจากขนาดของอุปกรณ์จะเข้าไปสู่ระดับเล็กที่ต้องใช้การอธิบายด้วยหลักควอนตัม แนวทางที่จะสามารถพัฒนาความเร็วของคอมพิวเตอร์ต่อไปได้คือการใช้ควอนตัมเข้ามาช่วยในการคำนวณเรียกว่าควอนตัมคอมพิวเตอร์ ศักยภาพในการคำนวณที่อาศัยคุณสมบัติทางควอนตัมทำให้สามารถคำนวณคำตอบของปัญหาบางรูปแบบทำได้เร็วกว่าคอมพิวเตอร์ปกติ เช่น การค้นฐานข้อมูลเชิงควอนตัมโดยวิธีของกรอฟเวอร์ ซึ่งจะใช้เวลาค้นฐานข้อมูลได้เร็วกว่าคอมพิวเตอร์มาก หรือการแยกตัวประกอบของชอร์ ซึ่งสามารถหาตัวประกอบของตัวเลขที่มีจำนวนหลักมากๆ ได้รวดเร็วกว่าคอมพิวเตอร์ปกติเช่นกัน ควอนตัมคอมพิวเตอร์เป็นวิวัฒนาการของกลศาสตร์ควอนตัมกับการคำนวณที่มีศักยภาพสูงยิ่งที่ได้เริ่มต้นการสร้างจริงแล้ว แต่ก็ยังคงต้องได้รับการพัฒนาอีกมากถึงจะไปสู่การใช้งานจริงได้ต่อไป

เอกสารอ้างอิง

[Adiga และคณะ 2002] N. R. Adiga, et al., "An overview of the BlueGene/L Supercomputer," in *Proceedings of the 2002 ACM/IEEE conference on Supercomputing, Baltimore, Maryland,* pp. 1 - 22, 2002.

[Aoki และคณะ 2007] K. Aoki, et al., "A kilobit special number field sieve factorization," in *International Association for Cryptologic Research (IACR)*, 2007.

[Barenco และคณะ 1995] A. Barenco, et al., "Elementary gates for quantum computation," *Physical Review A*, vol. 52, p. 3457, 1995.

[Bell-Labs.com] "Lov K. Grover," *bell-labs.com*. [Online] Available: http://www.bell-labs.com/user/lkgrover/ [Accessed: Dec 15, 2009].

[Benioff 1982] P. Benioff, "Quantum Mechanical Hamiltonian Models of Turing Machines," *J. of Statistical Physics*, vol. 29, no. 3, 1982.

[Bennett & Brassard 1984] C. H. Bennett, and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179, 1984.

[Boto และคณะ 2000] A. N. Boto, et al., "Quantum Interferometric Optical Lithography: Exploiting Entanglement to Beat the Diffraction Limit," *Phys. Rev. Lett.*, vol. 85, pp. 2733–2736, 2000.

[Brassard 1997] G. Brassard, "Searching a Quantum Phone Book," *Science,* vol. 275, no. 5300, pp. 627-628, 1997.

[Braunstein & van Loock 2005] S. L. Braunstein, and P. van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol 77, pp. 513–577, 2005.

[Britannica 2008] *Britannica Concise Encyclopedia (2008) ภาคภาษาไทย เล่ม 1*. กรุงเทพ: มีเดีย เม็กเน็ท และ มีเดีย เอกซเพอร์ทีส อินเตอร์เนชั่นแนล (ประเทศไทย), 2551.

[Buyya และคณะ 2008] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," in *Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08)*, Dalian, China, Sep. 25-27, 2008.

[Chuang และคณะ 1998] I. L. Chuang, I. M. K. Vandersypen, X. Zhou, D. W. Leung, and S. Lloyd, "Experimental realization of a quantum algorithm," *Nature*, vol. 393, pp. 143-146, 1998.

[Cirasella 2008] J. Cirasella, "Historical Bibliography of Quantum Computing in Appendix A," in *Quantum Computing for Computer Scientists*, N. S. Yanofsky and M. A. Mannucci, Ed. Cambridge: Cambridge University Press, 2008, pp. 319-324.

[Deutsch 1985] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," in *Proceedings of the Royal Society of London A,* vol. 400, pp. 97-117, 1985.

[Deutsch 1989] D. Deutsch, "Quantum Computational Networks," in *Proceedings of the Royal Society of London A*, vol. 425, no. 1868, pp. 73-90, 1989.

[Deutsch & Jozsa 1992] D. Deutsch, and R. Jozsa, "Rapid Solution of Problems by Quantum Computation," in *Proceeding of*

Royal Society London A, vol. 439, no. 1907, pp. 553-558, 1992.

[Feynman 1982] R. P. Feynman, "Simulating Physics with Computers," *Int. J. Th. Phys.,* vol. 21, no. 8, 1982.

[Foster และคณะ 2008] I. Foster, et al., "Cloud Computing and Grid Computing 360-Degree Compared," *Grid Computing Environments Workshop, GCE '08, Nov. 12-16, 2008.* pp. 1-10, 2008.

[Grover 1996] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings, STOC 1996, Philadelphia PA, USA*, pp. 212-219, 1996.

[Gulde และคณะ 2003] S. Gulde, et.al., "Implementation of the Deutsch–Jozsa algorithm on an ion-trap quantum computer," *Nature,* vol.421, pp. 48-50, 2003.

[Gurevich 2006] V. Gurevich, *Electric Relays: Principles and Applications*. New York: CRC Press, Taylor & Francis Group, 2006.

[Hallgren 2007] S. Hallgren, "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem," *Journal of the ACM*, vol. 54, no. 1, article no. 4, 2007.

[Ivanov และคณะ 2008] S. S. Ivanov, P. A. Ivanov, and N. V. Vitanov, "Simple implementation of a quantum search with trapped ions," *Phys. Rev. A*, vol. 78, p. 030301, 2008.

[Jones & Mosca 1998] J. A. Jones, and M. Mosca, "Implementation of a quantum algorithm to solve Deutsch's problem on a nuclear magnetic resonance quantum computer," *J. Chem. Phys.*, vol.109, pp. 1648–1653, 1998.

[Jozsa 2000] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, "Quantum Clock Synchronization Based on Shared Prior Entanglement," *Phys. Rev. Lett*., vol. 85, pp. 2010-2013, 2000.

[Lent และคณะ 1993] C. S. Lent, et al., "Quantum cellular automata," *Nanotechnology*, vol. 4, pp. 49-57, 1993.

[Liu และคณะ 2008] Q. Liu, et al., "DNA computing on surfaces," *Nature*, vol. 403, pp. 175-179, 2000.

[Lloyd 1995] S. Lloyd, "Quantum-mechanical computers," *Sci. Amer*., vol. 273, pp. 44, 1995.

[Lohmann 1986] A. W. Lohmann, "What classical optics can do for the digital optical computer," *Applied Optics*, vol. 25, issue 10, pp. 1543-1549, 1986.

[Manin 1977] Y. Manin, *A course in mathematical logic*. Graduate Texts in Math. vol. 53, New York: Springer-Verlag, 1977

[Manin 1980] Y. Manin, "Computable and uncomputable (in Russian)," *Moscow, Sovet-skoye Radio*, 1980.

[Mermin 2006] N. D. Mermin, *Quantum Computer Science*. Cambridge: Cambridge University Press, 2006

[Morsch 2008] O. Morsch, *Quantum Bits and Quantum Secrets*. Berlin: Wiley-VCH, 2008.

[Nielsen & Chuang 2000] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[Perez-Delgado & Kok 2009] C. A. Perez-Delgado, and P. Kok, "What is a quantum computer, and how do we build one?," *arXiv.org e-Print archive*, June 2009. [Online]. Available: http://arxiv.org/abs/0906.4344v1. [Accessed: Dec. 31, 2009].

[Politi และคณะ 2009] A. Politi, et al., "Shor's Quantum Factoring Algorithm on a Photonic Chip," *Science*, vol. 325, no. 5945, p. 1221, 2009.

[Preskill 1999] J. Preskill, "Plug-in quantum software," *Nature*, vol. 402, p. 357, 1999.

[Preskill.NET] J. Preskill, "Physics 219: Quantum Computation," *Physics 219 Course Information*. [Online]. Available:

http://www.theory.caltech.edu/~preskill/ph229/. [Accessed: Mar. 26, 2009].

[Reilly 2003] E. D. Reilly, *Milestones in Computer Science and Information Technology*. Westport, Conn. USA: Greenwood Press, 2003, pp. 249.

[Schumacher 1995] B. Schumacher, "Quantum Coding," *Phys. Rev. A*, vol. 51, p. 2738, 1995.

[Shor 1994] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pp. 124-134, 1994.

[Shor 1996] P. W. Shor, "Fault-Tolerant Quantum Computation," *37th Symposium on Foundations of Computing*, IEEE Computer Society Press, pp. 56-65, 1996.

[Shor 2003] P. W. Shor, "Why haven't more quantum algorithms been found?," *Journal of the ACM (JACM),* vol. 50, issue 1, pp. 87-90, 2003.

[Simon 1994] D. R. Simon, "On the Power of Quantum Computation," *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pp. 116-123, 1994.

[Spiller & Munro 2006] T. P. Spiller, and W. J. Munro, "Towards a quantum information technology industry," *J. Phys. Condensed Matter*, vol. 18, pp. V1-V10, 2006.

[Stassen 1997] F. Stassen, "On the 50th Anniversary of the Transistor," *Electroconference 1997,* Copenhagen, 1997.

[StateDiagram.NET] "Turing Machines," *Stanford Encyclopedia of Philosophy.* [Online]. Available: http://plato.stanford.edu/entries/turing-machine. [Accessed : Dec 16, 2009].

[Stolze & Suter 2004] J. Stolze, and D. Suter, *Quantum Computing*. Berlin: Wiley-VCH, 2004.

[Vandersypen และคณะ 2001] L. M. K. Vandersypen, et al., "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, pp. 883–887, 2001.

[Volbrecht & Cirac 2006] K. G. H. Vollbrecht, J. I. Cirac, "Reversible universal quantum computation within translation invariant systems," *Phys. Rev. A*, vol. 73, no. 1, p. 012324, 2006.

[Wiesner 1983] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78-88, 1983.

[Yao 1993] A. S. Yao, "Quantum Circuit and Complexity," in *Proceedings of the 34th Ann. IEEE Symp. on Foundations of Computer Science*, pp. 352-361, 1993.

คำถามท้ายบทที่ 4 (Questions and Answers)
และอภิปราย (Discussions) ปรับปรุง ณ
Blog: http://www.stks.or.th/blog/?p=14123

บทที่ 5
เทคโนโลยีการคำนวณเชิงควอนตัม
(Quantum computing technology)

อภิธานศัพท์ (Glossary)

- **ขั้นตอนวิธีแบบดอยช์-จอสซา (Deutsch-Jozsa algorithm)**
  ขั้นตอนวิธีเชิงควอนตัมสำหรับแก้โจทย์ปัญหาของดอยช์ เป็นวิธีเชิงควอนตัมชนิดแรกได้รับการพิสูจน์ว่าทำงานเร็วกว่าวิธีดั้งเดิมเป็นเอกซ์โพเนนเชียล พิสูจน์โดยเดวิด ดอยช์ และริชาร์ด จอสซา ในปี ค.ศ. 1992
- **การคำนวณเชิงควอนตัม (Quantum computation/ quantum computing)**
  การคำนวณภายใต้กฎของกลศาสตร์ควอนตัม การคำนวณเชิงควอนตัมขึ้นกับคุณสมบัติการทับซ้อนเชิงตำแหน่ง และความพัวพัน ซึ่งทำให้การแก้ปัญหาบางอย่างทำได้เร็วขึ้นโดยความขนานเชิงควอนตัมซึ่งเป็นผลจากคุณสมบัติทับซ้อนเชิงตำแหน่ง
- **การคำนวณเชิงควอนตัมแบบทางเดียว (One-way quantum computing)**
  การคำนวณเชิงควอนตัมที่ใช้สถานะพัวพันจำนวนมากมาทำการวัดสถานะบางส่วนและให้เกิดผลเป็นวงจรเชิงควอนตัมที่ต้องการกระทำต่อคิวบิตที่เหลืออยู่
- **การคำนวณเชิงควอนตัมแบบอิงการวัดสถานะ (Measurement-based quantum computing)**
  ความหมายเหมือน one-way quantum computing
- **การคำนวณแบบดั้งเดิม (Classical computing)**
  การคำนวณที่สถานะมีได้เฉพาะเจาะจงค่าหนึ่ง ได้แก่ กรณีค่าไม่ต่อเนื่อง (0 หรือ 1) เรียกว่า การคำนวณเชิงดิจิทัล และ ค่าต่อเนื่อง (จำนวนจริง) เรียกว่า การคำนวณเชิงแอนะลอก
- **การทำความเย็นแบบดอปเปลอร์ (Doppler cooling)** หรือ **การทำความเย็นด้วยเลเซอร์ (Laser cooling)**
  การทำให้อนุภาคมีพลังงานจลน์ (อุณหภูมิ) ลดลงโดยอาศัยการชนด้วยแสงความถี่ที่เหมาะสม เมื่ออนุภาคที่เคลื่อนที่เข้าหาลำแสงมีการดูดกลืนแสงจะได้รับการถ่ายเทโมเมนตัมทำให้ความเร็วลดลง
- **การลดเฟสร่วมกัน (Collective dephasing)**
  กระบวนการที่เกิดขึ้นระหว่างอันตรกิริยาของระบบควอนตัมกับสิ่งแวดล้อมภายนอก มีผลทำลายเฟสที่สัมพันธ์กันระหว่างคิวบิต
- **การสั่นพ้องแม่เหล็กนิวเคลียร์ (Nuclear magnetic resonance: NMR)**
  เทคนิคการปรับแปลงและการวัดสถานะของนิวเคลียสภายในอะตอมหรือโมเลกุลชนิดต่างๆ โดยอาศัยคุณสมบัติของสปินเมื่ออยู่ในสนามแม่เหล็กและการตอบสนองต่อคลื่นแม่เหล็กไฟฟ้าที่มากระตุ้นด้วยความถี่แตกต่างกันสำหรับแต่ละชนิดของนิวเคลียส
- **การสูญเสียความอาพันธ์เชิงควอนตัม (Decoherence)**
  การสูญเสียข้อมูลและคุณสมบัติเชิงควอนตัมจากผลกระทบของสิ่งแวดล้อม ทำให้ข้อมูลเชิงควอนตัมเปลี่ยนคุณลักษณะไปเป็นข้อมูลดั้งเดิม อีกนัยหนึ่งคือ การสูญเสียข้อมูลเฟสสัมพัทธ์ระหว่างสองสถานะย่อยที่ทับซ้อนกันเชิงตำแหน่ง
- **เกตลอจิกรากที่สองของการสลับคิวบิต ("square-root SWAP" gate)**
  การทำงานครึ่งหนึ่งของรอบการทำงาน (Half cycle) ของเกต SWAP โดยเกตลอจิก $\sqrt{SWAP}$ และการหมุนหนึ่งคิวบิต สามารถประกอบกันเป็น CNOT gate ได้ ดังนั้น $\sqrt{SWAP}$ และการหมุนหนึ่งคิวบิตจึงทำหน้าที่เป็นเกตอเนกประสงค์ได้
- **เกตลอจิกสลับคิวบิต (SWAP gate)**
  เกตลอจิกที่ทำหน้าที่สลับสถานะของคิวบิตที่หนึ่งและ

คิวบิตที่สอง สามารถสร้างขึ้นจากการทำงานของเกต CNOT สลับกันสามครั้ง

- **เกตลอจิก CNOT (Controlled-NOT gate)**
  เกตลอจิกเชิงควอนตัมซึ่งจะทำการพลิกสถานะของคิวบิตเป้าหมายให้เป็นสถานะตรงกันข้าม (“0” --> “1”; “1” --> “0”) เมื่อสถานะของคิวบิตควบคุมเป็น “1” และไม่มีการเปลี่ยนแปลงเกิดขึ้นเมื่อคิวบิตควบคุมมีค่า “0” เกตลอจิก CNOT ร่วมกับการหมุนหนึ่งคิวบิต (Single-qubit rotation) ประกอบกันเป็นเกตอเนกประสงค์
- **ควอนตัมดอท (Quantum dots)**
  โครงสร้างของสารกึ่งตัวนำซึ่งสามารถกักอนุภาค เช่น อิเล็กตรอนไว้ในบริเวณจำกัดในปริภูมิสามมิติ โดยสถานะของอนุภาคที่ถูกกักไว้ในควอนตัมดอทจะใช้แทนคิวบิตในการคำนวณเชิงควอนตัมได้
- **ความตั้งฉาก (Orthogonality)**
  (1) สองเวกเตอร์ ตั้งฉากกันก็ต่อเมื่อผลคูณจุด หรือผลคูณภายในระหว่างเวกเตอร์ทั้งสอง มีค่าเป็นศูนย์
  (2) สถานะควอนตัมที่อธิบาย ด้วยเวกเตอร์ตั้งฉาก เป็นสถานะซึ่งแบ่งแยกได้อย่างชัดเจนด้วยการวัดสถานะ
- **ความถี่โหมด (Mode frequency)**
  ความถี่ของแหล่งกำเนิดสัญญาณในย่านความถี่เรโซแนนซ์ ซึ่งจะให้พลังงานของสัญญาณออกมามากที่สุด
- **ความปรับขนาดได้ (Scalability)**
  คุณสมบัติที่ระบบควอนตัมหนึ่งๆ สามารถเพิ่มจำนวนคิวบิตสำหรับการคำนวณเชิงควอนตัม โดยที่คุณสมบัติเชิงควอนตัมยังคงอยู่ภายใต้การควบคุม
- **ความพัวพัน (Entanglement)**
  คุณสมบัติทางกลศาสตร์ควอนตัม ซึ่งอนุญาตให้วัตถุ (อนุภาค) ซึ่งอยู่ห่างไกลกัน สามารถมีสถานะร่วมกันได้ เรียกว่า *สถานะพัวพัน* โดยแต่ละอนุภาคที่มีความพัวพันกัน สถิติการวัด *ไม่เป็นอิสระต่อกัน*ถึงแม้อนุภาคจะอยู่ห่างไกลและถูกวัดในขณะเวลาเดียวกัน
- **ความสามารถในการเจาะจงตำแหน่ง (Addressability)**
  ความสามารถในการเจาะจงคิวบิตหนึ่งๆ เพื่ออ่านค่าหรือปรับเปลี่ยนสถานะคิวบิตที่ต้องการนั้น
- **ความอาพันธ์ (Coherence)**
  (1) คุณสมบัติของคลื่นที่มีความถี่และเฟสที่แน่นอน คลื่นอาพันธ์จากสองแหล่งกำเนิดจะแทรกสอดกันแล้วเกิดริ้วแทรกสอดชัดเจนและคงที่ เช่น แสงเลเซอร์จัดเป็นคลื่นที่มีความอาพันธ์
  (2) ในกลศาสตร์ควอนตัม หมายถึง คุณสมบัติที่สถานะควอนตัมยังคงค่าเฟสสัมพัทธ์ที่แน่นอนไว้ได้
- **คิวบิต (Qubit)**
  หน่วยพื้นฐานสำหรับการคำนวณและการสื่อสารเชิงควอนตัม 1 คิวบิต มีค่าเป็นผลรวมเชิงเส้นของสถานะ “0” และ “1” ในเชิงเรขาคณิตสังเกตเป็นเวกเตอร์ 1 หน่วยบนผิวทรงกลม
- **ค่าต่อเนื่อง (Continuous)**
  ค่าที่เป็นจำนวนจริง มีค่าแบ่งย่อยไปเท่าไรก็ได้และไม่สามารถนับได้ หรือหมายถึงโครงสร้างเชิงคณิตศาสตร์แบบอื่นที่แทนได้ด้วยจำนวนจริง
- **ค่าไม่ต่อเนื่อง (Discrete)**
  ค่าที่เป็นจำนวนเต็ม โดยทั่วไปหมายถึง จำนวนเต็มบวกหรือศูนย์ 0, 1, 2, 3, … ซึ่งเป็นค่าที่นับได้
- **เงื่อนไขของดิวินเชนโซ (DiVincenzo criteria)**
  เงื่อนไขจำเป็นสำหรับการที่ระบบควอนตัมหนึ่งๆ จะทำหน้าที่เป็นควอนตัมคอมพิวเตอร์ได้ มีทั้งหมด 5 ข้อสำหรับการคำนวณเชิงควอนตัม และเพิ่มเติมอีกสองข้อสำหรับการสื่อสารเชิงควอนตัม เสนอโดย เดวิด ดิวินเชนโซ ในปี ค.ศ. 1995 และ 2000
- **ตัวนำประจุ (Charge carriers)**
  ในสารกึ่งตัวนำ ตัวนำประจุหมายถึงอิเล็กตรอนซึ่งนำประจุลบ และโฮล (Hole) ซึ่งเสมือนนำประจุบวก
- **บิต (Bit)**
  หน่วยพื้นฐานสำหรับการคำนวณและการสื่อสารแบบดิจิทัล หนึ่งบิต มีค่าได้สองค่าคือ “0” หรือ “1” เท่านั้น
- **โพลาไรเซชัน (Polarization)**
  แนวการแกว่งตัวกลับไป-กลับมา ของสนามไฟฟ้าคลื่นแม่เหล็กไฟฟ้า หรือการจัดเรียงมุมของคลื่นแม่เหล็กไฟฟ้า

- **เฟสสัมพัทธ์ (Relative phase)**
  สำหรับสถานะคิวบิต $a|0\rangle+e^{i\beta}b|1\rangle$ ค่า $e^{i\beta}$ เรียกว่า เฟสสัมพัทธ์ระหว่างสองสถานะ (หรือสองฟังก์ชันคลื่น) $|0\rangle$ และ $|1\rangle$ ซึ่งมีผลเชิงกายภาพหรือผลเชิงสถิติในการวัดสถานะ
- **เฟสองค์รวม (Global phase)**
  สำหรับคิวบิต $e^{i\alpha}|\psi\rangle$ เทอม $e^{i\alpha}$ เรียกว่า เฟสองค์รวม ซึ่งไม่มีผลเชิงกายภาพ เนื่องจากสถานะควอนตัมแทนด้วย “รังสี” (ray) ซึ่งหมายถึงเวกเตอร์ที่มีแอมปลิจูดเป็นเท่าใดก็ได้
- **ระยะเวลาก่อนสูญเสียความอาพันธ์ (Decoherence time)** หรือ **ระยะเวลาคงสภาพความอาพันธ์ (Coherence time)**
  ระยะเวลาที่สถานะควอนตัมยังคงคุณสมบัติความอาพันธ์ เช่นการทับซ้อนเชิงตำแหน่ง และการแทรกสอดเชิงควอนตัม (Quantum interference) ที่แน่นอนได้
- **แลตทิซเชิงแสง (Optical lattices)**
  วิธีที่ใช้กักอะตอมซึ่งเป็นกลางทางไฟฟ้าให้อยู่ในบริเวณจำกัด โดยอาศัยโครงสร้างซึ่งเกิดจากคลื่นนิ่ง (Standing wave) ซึ่งเกิดจากแสงเลเซอร์สองแนวขึ้นไปตัดกันเป็นบริเวณคลื่นเสริม และหักล้าง ทำให้เกิดพลังงานศักย์ที่มีลักษณะเหมือนอาร์เรย์ (Array)
- **เวกเตอร์จำนวนเชิงซ้อน (Complex vector)**
  เวกเตอร์ที่มีค่าสมาชิกในแต่ละมิติ เป็นจำนวนเชิงซ้อน แทนด้วย ($C1$, $C2$, $C3$, ..., Cn) สำหรับเวกเตอร์เชิงซ้อน n มิติ โดยที่ C หมายถึงจำนวนเชิงซ้อน
- **สถานะควบแน่นแบบโบส-ไอน์สไตน์ (Bose-Einstein condensate: BEC)**
  สถานะของก๊าซที่ถูกทำให้มีพลังงานต่ำลงจนเข้าใกล้ศูนย์เคลวิน ฟังก์ชันคลื่นของอนุภาคจำนวนมากจะซ้อนทับกัน ณ จุดๆ เดียวทำให้มีสถานะเหมือนกัน
- **สปิน (Spin)**
  คุณสมบัติการตอบสนองต่อสนามแม่เหล็กของอนุภาค โดยสเปกตรัมของพลังงานของอนุภาคเมื่ออยู่ในสนามแม่เหล็กจะแยกชั้นพลังงานขึ้นอยู่กับสปินของอนุภาคนั้นๆ อนุภาคที่มีคุณสมบัติสปิน 1/2 มีค่าสปินได้สองค่าคือ +1/2 และ -1/2 (คือทิศขึ้นและทิศลงตามลำดับ) ส่วนอนุภาคที่มีสปิน 3/2 มีค่าสปินได้ทั้งหมดสี่ค่า {+3/2, +1/2, -1/2, -3/2} และอนุภาคที่มีสปิน 5/2 มีค่าสปินได้ทั้งสิ้นหกค่า
- **สปินของนิวเคลียส (Nuclear spin)**
  คุณสมบัติสปินของนิวเคลียสของอะตอมใดๆ ที่สนใจเท่ากับผลรวมสปินของอะตอมและสปินของนิวตรอนที่รวมกันเป็นนิวเคลียสนั้น ใน NMR การวัดสปินของนิวเคลียสจะวัดจากอะตอมลักษณะเหมือนกันจำนวนมากๆ
- **อะตอมที่เป็นกลาง (Neutral atoms)**
  อะตอมที่ไม่มีการสูญเสียหรือรับอิเล็กตรอน มีค่าประจุรวมเป็นศูนย์
- **อันตรกิริยา (Interaction)**
  การกระทำใดๆ ระหว่างอนุภาคตั้งแต่สองอนุภาคขึ้นไป
- **อิเล็กโทรด (Electrode)**
  ตัวนำไฟฟ้าที่ใช้ประสานระหว่างส่วนที่เป็นอโลหะเข้ากับตัววงจรไฟฟ้า
- **เอ็กซิตอน (Exciton)**
  คู่อิเล็กตรอนและโฮล ซึ่งเกิดจากการที่อิเล็กตรอนดูดกลืนแสงแล้วเปลี่ยนระดับพลังงาน โดยพลังงานของเอ็กซิตอนมีค่าเท่ากับ พลังงานช่วงต่างระหว่างอิเล็กตรอนและโฮล (Band-gap energy) ลบด้วยพลังงานที่ดึงดูดอิเล็กตรอนและโฮลเข้าด้วยกัน (Binding energy)
- **ไอออน (Ions)**
  อะตอมที่มีการสูญเสีย (หรือรับ) อิเล็กตรอน ทำให้มีประจุรวมเป็นบวก (หรือลบ) จึงถูกกระทำด้วยแรงแม่เหล็กไฟฟ้า
- **ไอออนที่ถูกกัก (Trapped ions)**
  ไอออนซึ่งถูกกักให้อยู่ในบริเวณจำกัด โดยอาศัยการทำให้มีพลังงานต่ำและกักบริเวณด้วยแรงแม่เหล็กไฟฟ้า การเปลี่ยนสถานะและการวัดสถานะทำได้โดยการกระตุ้นด้วยพัลส์แม่เหล็กไฟฟ้า เป็นตัวเลือกหนึ่งในการทำหน้าที่เพื่อการคำนวณเชิงควอนตัม

- **แฮมิลโทเนียน (Hamiltonian)**
  ตัวดำเนินการที่ใช้วัดพลังงานของระบบ หรือตัวดำเนินการที่กระทำกับเวกเตอร์สถานะแล้วให้ค่าเจาะจง (Eeigenvalue) เป็นพลังงาน ตั้งชื่อเป็นเกียรติแก่ วิลเลียม โรวาน แฮมิลตัน (William Rowan Hamilton) นักคณิตศาสตร์ชาวไอร์แลนด์

- **โฮล (Hole)**
  บริเวณในสารกึ่งตัวนำที่ว่างจากการมีอิเล็กตรอน (ซึ่งเดิมเคยอยู่บริเวณนั้น) ทำหน้าที่เสมือนเป็นประจุบวก

ข้อสรุปประจำบท (Summary)

Any two-level quantum systems can represent qubits, ability to initialize and manipulate the states is the ability to perform quantum computation process. Quantum measurement represents readout mechanism where information is transferred back to classical world. In 1995, David DiVincenzo suggested five requirements for a physical system to be able to perform quantum computing. Up to the beginning of 2010, there is no real winners for quantum computing devices; each physical systems has merits and caveats. Experimental investigation still need to prove the robustness and scalability of quantum computing realized in each systems. Nuclear magnetic resonance (NMR) has been successfully demonstrated as the first quantum computing machine. It has been shown of working up to seven-qubit Shor's algorithm implementation and higher. Unfortunately, it lacks of scalability. Solid-state NMR has been proposed to solve the scalability problem in NMR since 1998; experiments and theoretical improvement have been on progress. Trapped-ion quantum computers, based on electromagnetic force to trap the ions in a limited region (traditionally in linear) provides a good addressability. Ionic spins have small coupling to the environments and therefore give long coherence time. However, since the ions have charge which is affected by electrical forces, decoherence may also occur from the interaction with external force. Moreover, coulomb repulsive forces prohibit ions to be put arbitrarily close to each other. Trapped neutral atoms has been proposed to solve decoherence due to external electric field and the limit of spacing due to Coulomb repulsion as in ions. In neutral atom traps, standing wave of crossed laser beams provides electromagnetic potential which is patterned periodically and results in trapping structure for atoms. Both neutral atoms and ions need to be cooled before being trapped, doppler cooling where photons with appropriate wavelengths are used to strike atoms or ions to gradually decrease their velocity until approaching lowest limit. Neutral atoms trapped in optical lattices have been shown to represent a large amount of qubits, which, when entangling them together, can be a good resource for measurement-based quantum computing or one-way quantum computing -- another paradigm apart from quantum circuit model. Quantum dots refer to three-dimentional structures of semiconductor which can confine an electron in each dot region. Electrons confined in quantum dots has quantized energy level being able to represent quantum logic. Charge or spin degree of freedoms are traditional representative for qubit states. Where new approaches suggest to use exciting states -- states of electron and hole pairs which act like negative and positive (virtual) particle bounding to each others. Light or photons seem to be a good candidate for qubits in quantum computation because of its long coherence time and almost no interaction to the environments in a certain period. Photonic qubits are traditionally represented by polarizations and spatial mode states. Single qubit rotations in photons can be directly implemented by three waveplates corresponding to a unitary rotation of a vector in Poincare sphere. Two-qubit gate was firstly proposed to be implemented by light passing through a nonlinear crytal called *Kerr media* where light in the second mode is conditionally phase shifted when light is presented in the other mode. However, experimental realization of Kerr nonlinear is

non-trivial. Second approach to two-qubit gates uses entangled pair as a mediator to create a herald (conditioned on specific detection of photons to success) two-qubit gates. An innovative approache to implementing two-qubit gates has been proposed in 2001 to use only linear optical elements to realize quantum computing machine. It has been shown that beam splitters, phase shifters, single-photon sources and detectors are sufficient to reliably implement quantum computers. Later, optical quantum computing in a photonic chip -- doped by "silica-on-silicon" has been implemented . Silicon and silica have been used to act as 'core' and 'cladding' respectively, in order to guide photons similar to optical fibers. This brings an attention to miniaturizing optical quantum computers.

5.1 การคำนวณเชิงควอนตัม

ในปี ค.ศ. 1965 กอร์ดอน มัวร์ (Gordon E. Moore) ผู้ร่วมก่อตั้งบริษัทอินเทล ตั้งคำทำนายไว้ว่าทุกๆ หนึ่งปีครึ่ง ว่าปริมาณหน่วยความจำและจำนวนเกตลอจิกในชิพหนึ่งตัวจะเพิ่มขึ้นเป็นเท่าตัว [*Schaller 1997*] (กล่าวคือความสามารถในการคำนวณจะเพิ่มขึ้นหนึ่งเท่าตัวในเวลาหนึ่งปีครึ่ง ด้วยอุปกรณ์คำนวณที่มีขนาดเท่าเดิม) สิ่งที่มัวร์ทำนายไว้ได้เป็นจริงมาตลอด 30 ปี [*Morsch 2008*] คำทำนายนี้จึงถูกเรียกว่า “กฎของมัวร์” อีกนัยหนึ่งคือขนาดของทรานซิสเตอร์จะลดลงเท่าตัวทุกๆ ช่วงเวลาดังกล่าว อย่างไรก็ตาม

> *หากกฎของมัวร์ยังเป็นจริง ขนาดของทรานซิสเตอร์จะเล็กลงจนเข้าสู่ขนาดของโมเลกุล อะตอม และอิเล็กตรอนตามลำดับ ซึ่งเมื่อถึงสเกลนั้น ปรากฏการณ์ทางควอนตัมจะแสดงออกมาอย่างชัดเจน และลอจิกแบบเดิมซึ่งมีค่าที่แน่นอน “0” หรือ “1” ก็จะใช้ไม่ได้ กลายเป็นสถานะทับซ้อนเชิงตำแหน่ง (“0” และ “1” ในเวลาเดียวกัน) แทน และมีพฤติกรรมอื่นๆ เช่นความพัวพัน (entanglement) เพิ่มเข้ามาด้วย จึงเป็นอีกสาเหตุหนึ่งที่การคำนวณยุคต่อไปจำต้องอธิบายด้วยกลศาสตร์ควอนตัม*

และตรรกศาสตร์สำหรับการคำนวณจึงกลายเป็นตรรกศาสตร์เชิงควอนตัม ซึ่งมีคุณสมบัติดังเช่น การทับซ้อนเชิงตำแหน่ง ซึ่งระบบควอนตัมที่มีอยู่ทางกายภาพว่าเป็นระบบที่สามารถทำหน้าที่คำนวณเชิงควอนตัมได้มีดังนี้

ปี ค.ศ. 1995 เดวิด ดิวินเชนโซ (David DiVincenzo) ซึ่งทำงานวิจัยให้บริษัท IBM เสนอเงื่อนไขจำเป็นที่อุปกรณ์ “คำนวณเชิงควอนตัม” ทุกชนิดจำเป็นต้องมี ทั้งสิ้น 5 ข้อดังต่อไปนี้ [*DiVincenzo 1996*]

1) สถานะของคิวบิตนิยามได้อย่างชัดเจน (Well-defined) และทำงานได้ปกติในจำนวนคิวบิตที่มากขึ้น (Scalable)
2) สามารถเตรียมสถานะเริ่มต้น $|0...0000\rangle$ ได้
3) สถานะควอนตัมมีระยะเวลาคงสภาพความอาพันธ์มากกว่าระยะเวลาที่เกตลอจิกเชิงควอนตัมต้องใช้ในการทำงานในกระบวนการคำนวณทั้งหมด
4) มีเกตอเนกประสงค์เชิงควอนตัมที่ทำงานได้กับระบบควอนตัมนั้น
5) สามารถทำการวัด (อ่านค่า) ออกมาได้

เงื่อนไขจำเป็นข้อแรก หมายถึงต้องมีระบบทางกายภาพที่มีสถานะซึ่งแทนคิวบิตได้ และสามารถขยายขนาด (เพิ่มปริมาณคิวบิต) ของระบบกายภาพนั้นได้ตามต้องการ โดยที่คุณสมบัติเชิงควอนตัมทุกอย่างยังคงทำงานได้

ข้อที่สอง เตรียมสถานะเริ่มต้นได้ มิฉะนั้นการคำนวณจะไม่สามารถเริ่มได้ เหมือนกับเตรียมสถานะว่าง (Blank state) สำหรับใส่ค่าที่ต้องการเข้าไป เช่นตัวเลขที่ต้องการแยกตัวประกอบ เป็นต้น

ข้อที่สาม เนื่องจากการคำนวณเชิงควอนตัม ขึ้นกับการที่อนุภาคซึ่งประพฤติตัวตามกลศาสตร์ควอนตัม (เช่น การทับซ้อนทางตำแหน่ง และความพัวพัน) สูญเสียไป เนื่องจากการมีอันตรกิริยากับสิ่งแวดล้อม กลายเป็นสถานะที่ประพฤติตัวแบบดั้งเดิม

(classical) เช่น ยุบตัวเป็นสถานะ “0” หรือ “1” กรณีใดกรณีหนึ่ง กระบวนการที่ทำให้คุณสมบัติเชิงควอนตัมสูญเสียไปเรียกว่า การสูญเสียความอาพันธ์และเวลาที่อนุภาคจะคงคุณสมบัติควอนตัมอยู่ ซึ่งยังไม่ถูกทำให้สูญเสียความอาพันธ์เรียกว่าระยะเวลาคงสภาพความอาพันธ์ ถ้าเวลาดังกล่าวซึ่งเปรียบเสมือนเวลาที่ของอนุภาคที่เหมาะสมใช้ทำงานคำนวณเชิงควอนตัม มีค่าน้อยกว่าเวลาที่ใช้ในการคำนวณทั้งหมดหรือเวลาที่ควอนตัมลอจิกเกตใช้ในการทำงาน การคำนวณจะไม่สามารถเสร็จสิ้นได้เพราะพฤติกรรมเชิงควอนตัมสูญเสียไปก่อนที่จะคำนวณเสร็จ จากทั้งหมดข้างต้นสรุปได้ว่า

ระยะเวลาที่อนุภาคยังคงคุณสมบัติ (T_d) > เวลาที่ใช้ในการคำนวณทั้งหมด

(เวลาที่เกตลอจิกเชิงควอนตัมใช้ในการทำงาน: T_{op})

ข้อที่สี่ หมายถึงความสามารถที่จะปรับแปลงสถานะควอนตัมให้เป็นไปตามเกตลอจิกที่ต้องการ เช่นเกต NOT เกตฮาดามาร์ดและเกตยูนิแทรีสำหรับหนึ่งคิวบิต และตัวดำเนินการ CNOT สำหรับสองคิวบิต ซึ่งต้องอาศัยการมีอันตรกิริยาระหว่างสองอนุภาคเป็นอย่างน้อย และเวลาที่ใช้ในการเปลี่ยนสถานะของอนุภาคให้เป็นไปตามตัวดำเนินการลอจิกที่ต้องการขึ้นกับระบบทางกายภาพที่ใช้แทนสถานะคิวบิต เช่นสำหรับเกต NOT ที่กระทำกับคิวบิตของระดับพลังงานอะตอม เวลาที่ใช้มีค่าเท่ากับเวลาที่ใช้ในการกระตุ้นอะตอมด้วยคลื่นแม่เหล็กไฟฟ้าให้เปลี่ยนระดับพลังงาน ส่วนเวลาในการทำงานของเกต CNOT ขึ้นกับความเข้มของอันตรกิริยาระหว่างสองอนุภาคที่แทนคิวบิต เวลาที่ใช้ในการปรับเปลี่ยนสถานะควอนตัมเพื่อให้เกิดผลลัพธ์เป็นการคำนวณ หรือลอจิกที่ต้องการ นั่นคือเวลาในอสมการของข้อที่สาม (ด้านขวามือ)

ข้อที่ห้า หากควบคุมการเปลี่ยนแปลงของสถานะควอนตัมตามต้องการได้แล้ว แต่ไม่สามารถอ่านค่าสถานะออกมาได้ กระบวนการทั้งสิ้นก็เปล่าประโยชน์ เหมือนการคำนวณในวงจรคอมพิวเตอร์แต่ไม่มีผลลัพธ์เป็นภาพบนหน้าจอ หรือมีเสียงออกทางลำโพง การคำนวณดังกล่าวก็ไม่มีประโยชน์ต่อผู้ใช้ในการคำนวณเชิงควอนตัมเช่นเดียวกัน ต้องสามารถวัดค่าสถานะออกมาได้ เช่นในการคำนวณเชิงควอนตัมที่ใช้สถานะของโฟตอนเดี่ยว ตัวตรวจหาโฟตอนต้องมีประสิทธิภาพสูงพอที่จะตรวจหาโฟตอนเดี่ยวได้ด้วยความน่าจะเป็นที่สูง และในการใช้หลายอนุภาค เช่น ใช้การกักไอออน ต้องสามารถระบุ (Address) สถานะของอนุภาค (คิวบิต) ที่ต้องการและอ่านค่าสถานะดังกล่าวออกมาได้ เช่นอาศัยการกระตุ้นด้วยพัลส์ของคลื่นแม่เหล็กไฟฟ้าในความถี่ที่เหมาะสม

ในปี ค.ศ. 2000 ดิวินเชนโซ เสนอเงื่อนไขเพิ่มเติมอีกสองข้อ สำหรับ “การสื่อสารเชิงควอนตัม”

6) ความสามารถในการส่งผ่านสถานะจากคิวบิตที่อยู่นิ่ง ไปสู่คิวบิตที่เคลื่อนที่ได้ เช่น แสง และทำงานในทางกลับกันได้

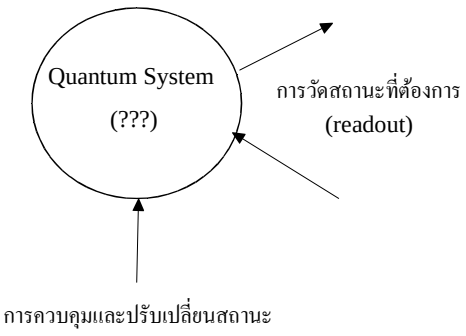
7) สามารถส่งสถานะคิวบิตที่เคลื่อนที่ได้ จากตำแหน่งหนึ่งไปยังอีกตำแหน่งที่แน่นอนได้

ข้อที่หก การส่งผ่านสถานะควอนตัมจากคิวบิตที่อยู่นิ่ง เช่นไอออนที่ถูกกักในสนามไฟฟ้า ซึ่งทำหน้าที่เป็นหน่วยความจำเชิงควอนตัม ถ่ายทอดสถานะ (ข้อมูลควอนตัม)ไปสู่คิวบิตที่ทำหน้าที่สื่อสาร เช่น โฟตอน และในภาครับสามารถถ่ายทอดสถานะจากคิวบิตพาหะของการสื่อสาร เช่น โฟตอน ไปสู่อนุภาคที่แทนคิวบิตอยู่นิ่งที่ภาครับได้

ข้อที่เจ็ด ความสามารถที่จะคงอนุรักษ์สถานะของอนุภาคในระหว่างการส่งจากตำแหน่งหนึ่งไปยังอีกตำแหน่งหนึ่งด้วยวิธีการใดก็ตาม หมายถึงสถานะควอนตัมสามารถส่งผ่านไปยังเป้าหมายได้ด้วยความน่าจะเป็นที่สูงพอในทางปฏิบัติ

> *ควอนตัมคอมพิวเตอร์หรืออุปกรณ์คำนวณเชิงควอนตัม ไม่ได้มีลักษณะปรากฏเช่นเดียวกับคอมพิวเตอร์ตั้งโต๊ะหรือคอมพิวเตอร์พกพา หากแต่หมายถึงระบบควอนตัมใดๆ ก็ตามที่สามารถกำหนดสถานะเริ่มต้น ควบคุมการเปลี่ยนแปลง และอ่านค่าสถานะออกมาได้ตามเงื่อนไขจำเป็นของดิวินเชนโซ*

ลักษณะของควอนตัมคอมพิวเตอร์ภาพรวมจึงมีดังรูปที่ 5.1 โดยอุปกรณ์สำหรับการคำนวณเชิงควอนตัม (ปัจจุบัน พ.ศ. 2554 หมายถึงอุปกรณ์ในห้องปฏิบัติการ) ที่ใช้ควบคุมและอ่านสถานะมีการจัดขึ้นให้เหมาะสมกับระบบควอนตัม (อนุภาคใดๆ) ที่ถูกเลือกใช้ในงานคำนวณเชิงควอนตัม ดังแสดงต่อไปว่าระบบทางกายภาพใดบ้างที่มีคุณสมบัติพอที่จะใช้ในงานคำนวณเชิงควอนตัม และแต่ละระบบมีข้อดีข้อเสียอย่างไร



รูปที่ 5.1 ลักษณะโดยสังเขปของอุปกรณ์คำนวณเชิงควอนตัม

5.2 อุปกรณ์สำหรับคำนวณเชิงควอนตัม

นับตั้งแต่ปลายคริสต์ศตวรรษที่ 20 นักวิทยาศาสตร์มีการวิจัยและค้นพบระบบทางกายภาพมากมายที่ทำหน้าที่คำนวณเชิงควอนตัมได้ แต่ละระบบล้วนแต่มีข้อดีและข้อเสียแตกต่างกันไป [*Nielsen & Chuang 2000*] บางส่วนของระบบทางกายภาพที่สามารถใช้ในงานคำนวณเชิงควอนตัมแบ่งได้เป็นสองหมวดหมู่หลัก ได้แก่ [*Morsch 2008*]

1) คิวบิตที่แทนด้วยสถานะของอนุภาค เช่น สถานะของอะตอม อิเล็กตรอน โฟตอน

2) คิวบิตที่แทนด้วยสถานะของระบบขนาดใหญ่ (Macroscopic) ที่ประพฤติตัวแบบควอนตัม เช่น สถานะสปินใน NMR

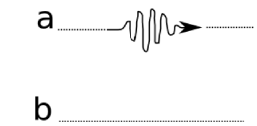
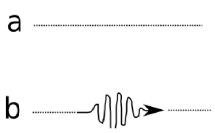
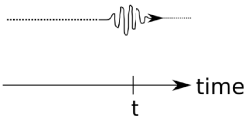
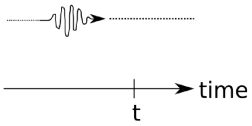
หมวดหมู่แรก อาศัยความจริงที่อนุภาค เช่นอะตอม หรือ โฟตอน นั้น ประพฤติตัวแบบควอนตัมอย่างชัดเจนอยู่แล้ว สถานะของอนุภาคนั้นจึงนำมาแทนข้อมูลเชิงควอนตัมสำหรับการคำนวณได้ เช่น ระดับพลังงานของอะตอม หรือ โพลาไรเซชันของแสง แต่ความลำบากของการใช้สถานะของอะตอม คือจะต้องใช้อะตอมที่แตกตัวเป็นอิสระจากอะตอมอื่นๆ ซึ่งในของแข็งและของเหลวนั้นอะตอมก็ล้วนจับตัวกันอย่างใกล้ชิด ส่วนในสถานะก๊าซ อะตอมมีพลังงานสูงและมีการเคลื่อนที่แบบสุ่ม ควบคุมยาก จึงต้องมีวิธีการกักอะตอมให้อยู่กับที่และแยกตัวเป็นอิสระจากอะตอมอื่น ส่วนการใช้สถานะของแสง หรือ โฟตอน แทนข้อมูลควอนตัมนั้นมีปัญหากรณีแรกคือ โฟตอนเคลื่อนที่ด้วยความเร็วสูง (ความเร็วแสง) และอีกปัญหาหนึ่งคือความยุ่งยากในการทำให้สองโฟตอนมีอันตรกิริยาระหว่างกันเพื่อทำหน้าที่เกตลอจิกสำหรับสองคิวบิต (เช่นการส่องแสงจากไฟฉายสองกระบอกตัดกัน ไม่เกิดปฏิกิริยาต่อกันแต่อย่างใด) อย่างไรก็ตาม การทำให้โฟตอนมีอันตรกิริยาต่อกันเพื่อให้ได้เกตลอจิกสองคิวบิตนั้นมีเทคนิคที่สามารถกระทำได้ [*Knill, Laflamme & Milburn 2001*]

หมวดหมู่ที่สอง อาศัยโครงสร้างทางกายภาพที่เฉพาะเจาะจง โดยทั่วไปหมายถึงโครงสร้างขนาดใหญ่ ซึ่งสามารถปรับแต่งให้ประพฤติตัวแบบควอนตัมและแทนข้อมูลควอนตัมได้ อย่างไรก็ตาม ถึงแม้พฤติกรรมเชิงควอนตัมจะแสดงออกมาได้ ส่วนอื่นๆ ในโครงสร้างนั้นๆ ก็เหนี่ยวนำให้คุณสมบัติควอนตัมเลือนหายไปในเวลารวดเร็ว ถึงแม้จะมีปัญหาดังกล่าวข้างต้น นักวิทยาศาสตร์ก็ได้ร่วมกันค้นพบเทคนิคและสาธิตการทำงานคำนวณเชิงควอนตัมในระบบทางกายภาพต่าง ๆแล้วดังแสดงบางส่วนดังต่อไปนี้

5.2.1 การคำนวณเชิงควอนตัมด้วยสถานะของแสง

สถานะของแสง เช่น โพลาไรเซชัน หรือแนวการแกว่งตัวของสนามไฟฟ้าในสองแนวที่ตั้งฉากกันสามารถนำมาแทนข้อมูลควอนตัมสำหรับการคำนวณเชิงควอนตัมได้ดังตารางที่ 5.1 และการเปลี่ยนสถานะด้วยอุปกรณ์ทัศนศาสตร์ เช่น ตัวแยกลำแสง เป็นต้นนั้น ทำหน้าที่เปลี่ยนสถานะสำหรับหนึ่งคิวบิต ข้อดีของการใช้แสงแทนสถานะควอนตัมคือ โฟตอนมีระยะเวลาคงสภาพความอาพันธ์นานเมื่อเทียบกับสถานะของอนุภาคอื่นๆ แต่ข้อเสียคือ การทำให้โฟตอนสองตัวมีอันตรกิริยาระหว่างกันเพื่อให้เกิดการดำเนินการเชิงลอจิกสำหรับสองคิวบิตทำได้ลำบาก อย่างไรก็ตาม มีการเสนอเทคนิคที่ช่วยให้สองโฟตอนมีอันตรกิริยาต่อกันได้โดยผ่านผลึกที่มีคุณสมบัติไม่เป็นเชิงเส้นเพื่อให้เกิดการดำเนินการลอจิกสำหรับสองคิวบิตได้แต่การใช้ผลึกคุณสมบัติเชิงเส้น

ตารางที่ 5.1 องศาอิสระ (Degree of freedom) ต่างๆ ที่ใช้แทนคิวบิตในโฟตอน

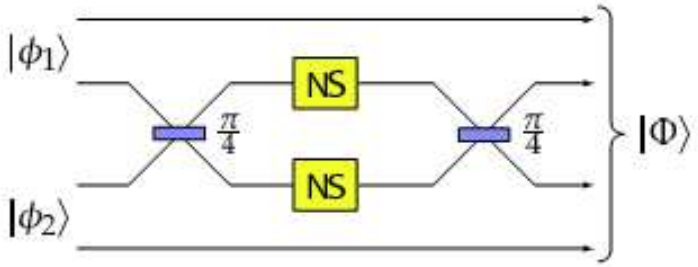
คุณสมบัติของโฟตอน ที่ใช้แทนคิวบิต	**สารสนเทศ (ลอจิก)**	
	$\|0\rangle$	$\|1\rangle$
โพลาไรเซชันเชิงเส้น (Linear polarization)	แนวตั้ง ↕	แนวนอน ↔
โพลาไรเซชันเชิงวงกลม (Circular polarization)	ทวนเข็มนาฬิกา (left-circular polarization)	ตามเข็มนาฬิกา (right-circular polarization)
จำนวนโฟตอน (Photon number)	ไม่มีโฟตอน	มี 1 โฟตอน
เส้นทางที่แสงเคลื่อนที่ (Photon path หรือ spatial mode)	ผ่านเส้นทาง a 	ผ่านเส้นทาง b 
ตะกร้าเวลา ก่อน-หลัง (time-bin)	โฟตอนมาถึงก่อน 	โฟตอนมาถึงหลัง 

ประสบปัญหาหลายประการในทางปฏิบัติ จึงมีการเสนอวิธีคำนวณเชิงควอนตัมด้วยสถานะของแสง (ซึ่งรวมถึงการทำงานของเกตลอจิกสองคิวบิต) โดยใช้เพียง ตัวแยกลำแสง ตัวเลื่อนเฟส แหล่งกำเนิดโฟตอนเดี่ยว และตัวตรวจหาโฟตอน โดย เอมมานูเอล นิลล์ (Emmanuel Knill) เรมอนด์ ลาฟลามม์ (Raymond Laflamme) และ เจอราร์ด มิลเบิร์น (Gerard Milburn) (KLM) ในปี ค.ศ. 2001 [*Knill, Laflamme & Milburn 2001*]

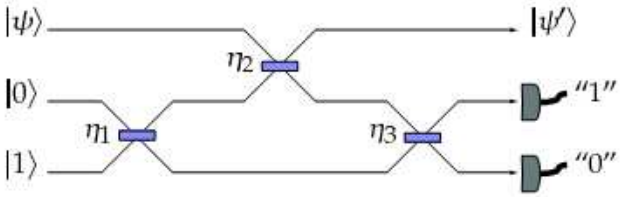
วงจรอย่างย่อซึ่งแทนการทำงานของเกตลอจิกควบคุมเฟส (Controlled Phase)[5.1] อธิบายได้ดังรูปที่ 5.2 ซึ่งประกอบด้วยตัวแยกลำแสง 50:50 (แทนด้วย $\frac{\pi}{4}$) และตัวดำเนินการเครื่องหมายไม่เชิงเส้น (Nonlinear Sign: NS) ซึ่งทำหน้าที่เปลี่ยนสถานะ $a|0\rangle+b|1\rangle+c|2\rangle$ เป็น $a|0\rangle+b|1\rangle-c|2\rangle$ โดยตัวดำเนินการ NS ดังกล่าวสามารถสร้างขึ้นจากตัวแยกลำแสง (ในอัตราส่วนใดๆ ที่ไม่เป็นต้อง 50:50 แทนตัวแปรอัตราส่วนของการทะลุผ่านต่อสะท้อนด้วย η_k) และตัวตรวจหาโฟตอนเดี่ยว

เกตลอจิกหนึ่งคิวบิตสำหรับสถานะของแสงสามารถสร้างจากแผ่นคลื่น (Waveplate) จำนวนสามชุด ซึ่งทำหน้าที่หมุนโพลาไรเซชันแบบย้อนกลับได้บนทรงกลมสามมิติ (การเปลี่ยนแปลงของหนึ่งคิวบิต) การสร้างเกตลอจิกสองคิวบิตวิธีแรกสร้างจากการผ่านแสงสู่ผลึกไม่เชิงเส้นแบบเคอร์ (Kerr nonlinear crystal) ซึ่งจะทำหน้าที่เลื่อนเฟสของโฟตอนหนึ่งก็ต่อเมื่อมีอีกโฟตอนเข้ามาสู่ผลึกพร้อมกัน เมื่อแทนสถานะคิวบิตด้วยเส้นทางของแสง วิธีการดังกล่าวทำให้เกิดเกตลอจิกเลื่อนเฟสที่ถูกควบคุม (Controlled-Phase shift: CZ) ได้ดังรูปที่ 5.3 และจากเกตลอจิก CZ ร่วมกับเกตลอจิกฮาดามาร์ด (H) สองชุด ซึ่งอาศัยตัวแยกลำแสงประกอบขึ้นเป็น CNOT ได้ (ดูภาคผนวก) ดังรูปที่ 5.4 การสร้างเกตลอจิกสองคิวบิตวิธีที่สอง อาศัยคู่โฟตอนพัวพันเพิ่มเติมจากโฟตอนที่แทนคิวบิต เป็นตัวกลางในการนำพาให้เกิดอันตรกิริยาระหว่างสองคิวบิต (คิวบิตควบคุม และคิวบิตเป้าหมายใน CNOT)

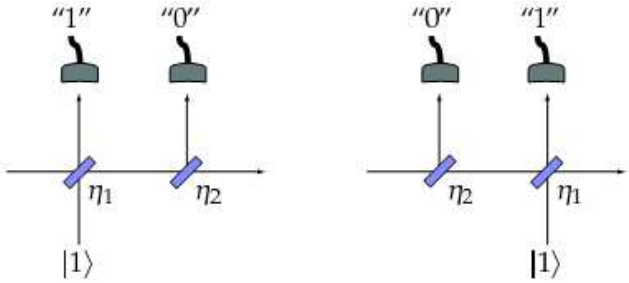
[5.1] เมื่อรวมกับเกตลอจิกหนึ่งคิวบิตจะทำหน้าที่คำนวณเชิงควอนตัมทุกรูปแบบได้ (เช่นเดียวกับเกตลอจิก CNOT)



รูปที่ 5.2 การทำงานของเกตลอจิก controlled phase (CZ) ตามที่เสนอโดย KLM [*Kok และคณะ 2007*]



(ก)

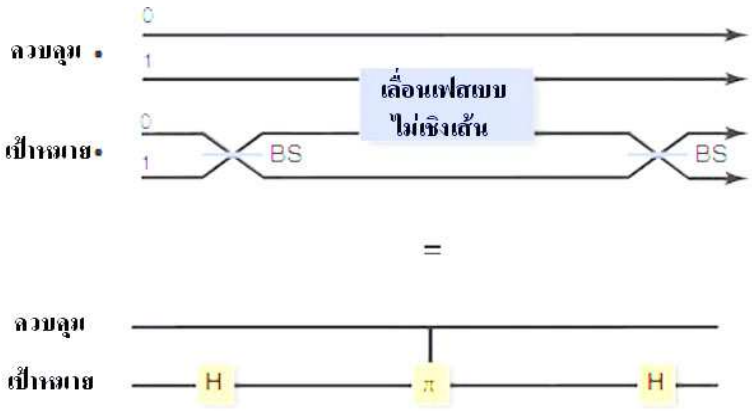


(ข)

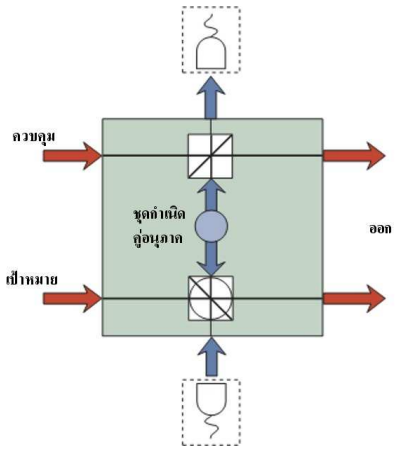
รูปที่ 5.3 การสร้างตัวดำเนินการ NS สำหรับประกอบขึ้นเป็นเกตลอจิก CZ ตามที่เสนอโดย KLM

(ก) วิธีแรกของการสร้าง NS เสนอโดย KLM โดยอัตราการทะลุผ่านของตัวแยกลำแสง $\eta_1=\eta_3=1/(4-2\sqrt{2})$ และ $\eta_2=3-2\sqrt{2}$ ความน่าจะเป็นที่จะสำเร็จเท่ากับ 1/4

(ข) วิธีที่สองสำหรับสร้าง NS เสนอโดย [*Ralph และคณะ 2002*] ซึ่งใช้ตัวแยกลำแสงเพียงสองตัว และความน่าจะเป็นที่จะสำเร็จเท่ากับ $(3-\sqrt{2})/7$ รูปดัดแปลงจาก [*Kok และคณะ 2007*]



รูปที่ 5.4 การสร้าง CNOT gate ซึ่งกระทำต่อคิวบิตที่แทนด้วยเส้นทางเดินของแสง รูปดัดแปลงจาก [*O'Brien 2007*]



รูปที่ 5.5 การทำงานของเกตลอจิก CNOT บนคิวบิตซึ่งแทนด้วยโพลาไรเซชัน
โดยใช้คู่โฟตอนพัวพันช่วยให้เกิดเกตลอจิกดังกล่าว รูปดัดแปลงจาก [*Pittman และคณะ 2004*]

5.2.1.1 ทรัพยากรที่ใช้ในการคำนวณเชิงควอนตัมด้วยสถานะของแสง

การจะสร้างเกตลอจิกสองคิวบิตชนิด CNOT ให้ใกล้เคียงความแน่นอน (ด้วยความน่าจะเป็น 95%) ต้องใช้ทรัพยากรตั้งต้นถึงมากกว่า 10^4 คู่โฟตอนพัวพัน จึงมีรูปแบบวิธีประมวลผลสารสนเทศเชิงควอนตัมที่ไม่ต้องอิงอาศัยเกตลอจิกสองคิวบิตที่แน่นอน (ความน่าจะเป็นที่จะสำเร็จมีค่าน้อยได้) ซึ่งแบบจำลองการคำนวณเชิงควอนตัมแบบทางเดียว (One-way quantum computation) [*Raussendorf & Briegel 2001*] มีความเหมาะสมในแง่มุมนี้ เพราะการเตรียมสถานะพัวพันสำหรับการคำนวณเป็นแบบความน่าจะเป็นได้ (ซึ่งเกตลอจิก CNOT ในสถานะแสงก็มีลักษณะสำเร็จแบบความน่าจะเป็น) [*O'Brien 2007*] และสถานะพัวพันทั้งหมดที่เกิดจากกรณีที่สำเร็จในการสร้างมารวมกัน จะถูกใช้เป็นทรัพยากรในการคำนวณต่อไป

5.2.1.2 ความคืบหน้าด้านเทคโนโลยีและงานวิจัย

- แหล่งกำเนิดโฟตอนเดี่ยว

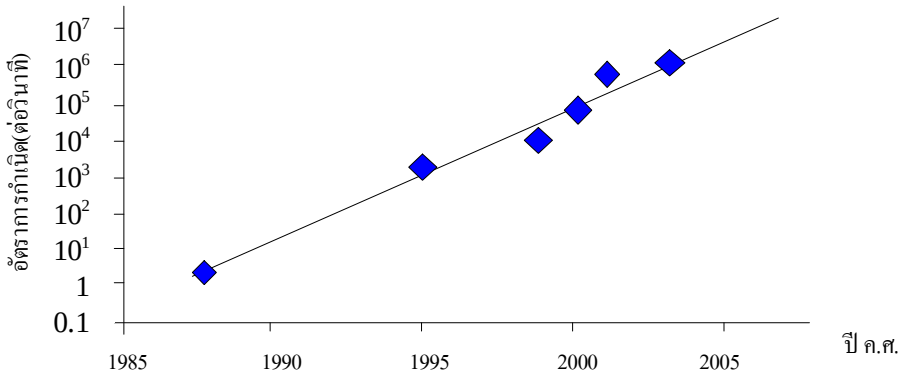
สิ่งที่จำเป็นต่อการคำนวณเชิงควอนตัมด้วยสถานะของแสงคือ แหล่งกำเนิดโฟตอนเดี่ยวที่มีประสิทธิภาพสูง โฟตอนเดี่ยวนั้นเกิดจากอนุภาคใดอนุภาคหนึ่งเปลี่ยนระดับพลังงานหนึ่งครั้งพร้อมทั้งปล่อยแสง (โฟตอน) ออกมาในความถี่มีพลังงานเท่ากันกับระดับพลังงานที่เปลี่ยนนั้น โดยวิธีการที่ถูกเสนอในการสร้างโฟตอนเดี่ยว ได้แก่ (1) การปั๊มเลเซอร์เข้าสู่คริสตัลไม่เป็นเชิงเส้น (เช่น Barium Borate : BBO) และจะมีโอกาสที่โฟตอนหนึ่งจะถูกดูดกลืนและปล่อยคู่โฟตอนออกมา โดยการตรวจพบหนึ่งโฟตอนจะเป็นการยืนยันว่ามีอีกหนึ่งโฟตอนถูกปล่อยออกมาด้วย ในทิศทางที่หักล้างกันเชิงโมเมนตัม (2) การใช้สารกึ่งตัวนำ เช่น ควอนตัมดอท (3) การใช้ผลึกเพชรที่มีตำหนิด้วยอะตอมไนโตรเจน (Nitrogen-vacancy (NV) centered diamond) เป็นต้น

- แหล่งกำเนิดสถานะพัวพัน

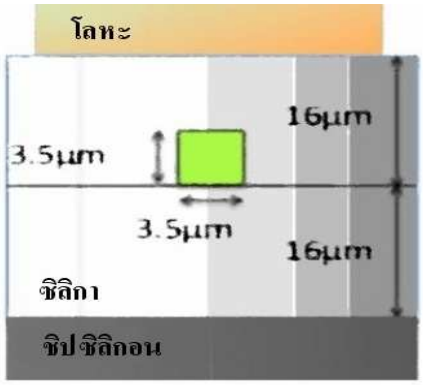
การสร้างสถานะพัวพันเชิงแสงสำหรับการคำนวณเชิงควอนตัม พบว่าประสิทธิภาพการสร้างคู่พัวพันผ่านวิธีแปลงผันลงเชิงพารามิเตอร์ (parametric down conversion) จะสูงขึ้น 100 เท่าทุกๆ 5 ปี ดังรูปที่ 5.6 โดยขีดจำกัดของคำทำนายนี้ในทศวรรษที่ 90 อยู่ที่ข้อจำกัดอัตราการตรวจหาโฟตอนของตัวตรวจหาซึ่งจำกัดอยู่ที่ประมาณ 10 เมกะเฮิรตซ์ [*Everitt 2005*]

- การสาธิตการคำนวณเชิงควอนตัม

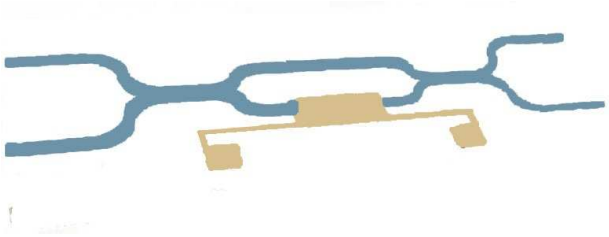
ในปี ค.ศ. 2008 กลุ่มวิจัยโฟโทนิกส์ ณ มหาวิทยาลัยบริสตอล สหราชอาณาจักร นำเสนอผลการวิจัยการคำนวณเชิงควอนตัมด้วยสถานะของแสงซึ่งทำงานได้บนชิปดังรูปที่ 5.7 และรูปที่ 5.8 จากเดิมที่อยู่บนโต๊ะอุปกรณ์ทัศนศาสตร์ขนาดใหญ่ ซึ่งอาศัยซิลิกาโดปบนซิลิกอนเพื่อทำหน้าที่นำแสง เป็นส่วนแกนและส่วนเปลือก (Cladding) เหมือนการทำหน้าที่ในเส้นใยแสง นอกจากนี้ยังได้สาธิตการทำงานของมาตรแทรกสอดแบบแมส-แซนเดอร์ ไปจนถึงการแยกตัวประกอบด้วยขั้นตอนวิธีเชิงควอนตัมแบบชอร์บนชิปดังกล่าว [*Politi และคณะ 2009*]



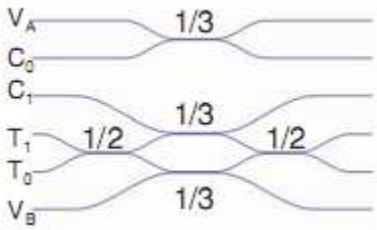
รูปที่ 5.6 กฎของมัวร์สำหรับการสร้างคู่โฟตอนพัวพันจากแหล่งการแปลงลงเชิงพารามิเตอร์ (parametric down conversion) จากการเก็บสถิติพบว่าทุกๆ 5 ปี สะสามารถสร้างคู่โฟตอนพัวพัน (ต่อหนึ่งวินาที) ได้เป็นจำนวนมากขึ้นถึง 100 เท่า รูปดัดแปลงจาก [*Everitt 2005*]



รูปที่ 5.7 ลักษณะซิลิกาที่ถูกโดปลงบนซิลิกอนเพื่อทำหน้าที่เป็นตัวนำแสง โดยซิลิกอนทำหน้าที่เป็นแกน (Core) และซิลิกาทำหน้าที่เป็นเปลือกหรือแคลดดิ้ง เสมือนการนำโฟตอนในเส้นใยแสง รูปดัดแปลงจาก [*O'Brien และคณะ 2009*]



(ก)



(ข)

รูปที่ 5.8 (ก) วงจรการแทรกสอดแบบมัค-เซนเดอร์ ซึ่งโลหะที่ปรับอุณหภูมิได้ (รูปสี่เหลี่ยมและเส้นเหลี่ยม) ถูกใช้ในการเปลี่ยนค่าดัชนีการหักเหของแสงในบริเวณนำพาแสงที่ต้องการ (ทำให้เกิดการเปลี่ยนเฟส) รูปดัดแปลงจาก [*O'Brien และคณะ 2009*] (ข) วงจรการสร้างเกตลอจิก CNOT บนชิป โดยมีเส้นแสดงแนวซิลิกอนนำแสง และเลขเศษส่วนแทนอัตราการทะลุผ่านของ coupler (ซึ่งทำหน้าที่เหมือนตัวแยกลำแสง) C_0 และ C_1 แทนเส้นทางของโฟตอนกรณีคิวบิตควบคุมมีสถานะ “0” และ “1” T_0 และ T_1 แทนเส้นทางของโฟตอนกรณีคิวบิตเป้าหมายมีสถานะ “0” และ “1” สำหรับ V_A และ V_B นั้นไม่จำเป็นต่อการใช้คำนวณเนื่องจากสถานะของทั้ง V_A และ V_B เป็นอิสระต่อเส้นทางอื่นๆ รูปดัดแปลงจาก [*Politi และคณะ 2009*]

5.2.2 การคำนวณเชิงควอนตัมด้วยไอออนที่ถูกกัก (Trapped ions)

การใช้อะตอมแทนสถานะเชิงควอนตัมเพื่อการคำนวณนั้นมีปัญหาคือ อะตอมจะต้องแยกเป็นอิสระจากอะตอมอื่นๆ เพื่อให้แทนสถานะของคิวบิตเดียวได้ อะตอมในสถานะของแข็งและของเหลวมีการจับตัวกันแน่นทำให้ไม่สามารถแยกอะตอมเดี่ยวได้ ส่วนอะตอมในสถานะก๊าซมีอิสระในการเคลื่อนที่สูงทำให้ระบุตำแหน่งได้ยาก ด้วยเหตุนี้จึงมีการเสนอวิธีประยุกต์การกักไอออนให้นิ่งอยู่ในบริเวณจำกัดโดยอาศัยแรงผลักจากสนามไฟฟ้า หากไอออนพยายามเคลื่อนที่ออกจากบริเวณนั้น ไอออนจะถูกแรงทางไฟฟ้าผลักให้กลับมาสู่จุดเดิมซึ่งเป็นจุดสมดุล (สนามไฟฟ้าเป็นศูนย์) การประยุกต์ใช้ไอออนที่ถูกกักด้วยสนามไฟฟ้ามาทำหน้าที่ในการคำนวณเชิงควอนตัม เสนอโดย ปีเตอร์ โซลเลอร์ (Peter Zoller) และอิกนาซิโอ ซิแรก (Ignazio Cirac) ในปี ค.ศ. 1995 ซึ่งได้อธิบายวิธีการทำให้เกิดตัวดำเนินการ Controlled-NOT บนไอออนที่ถูกกักนั้น [*Cirac & Zoller 1995*] ซึ่งมีวิธีการดังนี้

5.2.2.1 การกักไอออนและการแทนคิวบิต

รูปแบบการกักไอออนที่ใช้ในงานคำนวณเชิงควอนตัมค้นพบโดย โวล์ฟกัง พอล (Wolfgang Paul) ในปี ค.ศ. 1950 (ซึ่งทำให้เขาได้รับรางวัลโนเบลสาขาฟิสิกส์ในปี ค.ศ. 1989 [*Nobel.NET*]) อนุภาคที่มีประจุใดๆ ไม่สามารถถูกกักในปริภูมิสามมิติ ด้วยสนามไฟฟ้าสถิตย์เพียงอย่างเดียว จากสมการลาปลาซ[5.2] (Laplace equations) ของสนามไฟฟ้าสถิตย์ให้ผลเฉลยว่าไม่มีจุดต่ำสุด[5.3] ของพลังงานศักย์ (ซึ่งจะใช้กักอนุภาคที่มีประจุ) มีเพียงจุดอานม้า[5.4] (Saddle points) ซึ่งหากเปลี่ยนจากสนามไฟฟ้าสถิตย์เป็นสนามแม่เหล็กไฟฟ้าที่ความถี่วิทยุที่มีความถี่และความเข้มของสนามเหมาะสม จะสามารถกักอนุภาคที่มีประจุ (ไอออน) ไว้ในบริเวณที่ต้องการได้ ดังรูปที่ 5.9 ปัญหาอีกประการหนึ่งของการกักไอออนคือ การทำให้ไอออนมีพลังงานต่ำลงเนื่องจากพลังงานจลน์ที่สูง (ความเร็วสูง) จะถูกกักบริเวณด้วยแรงแม่เหล็กไฟฟ้าดังกล่าวได้ยาก

5.2.2.2 การทำให้ไอออนมีอุณหภูมิลดลง (Ion/Atomic Cooling)

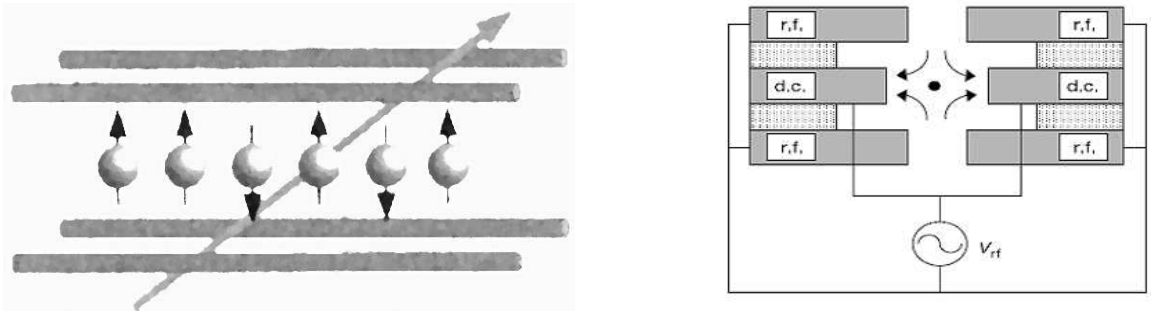
การลดอุณหภูมิของไอออนทำได้โดยอาศัยคุณสมบัติที่แสงมีโมเมนตัมและสามารถชนอนุภาค (เช่น อะตอม หรือไอออน) ให้เปลี่ยนแปลงความเร็วได้ และจากการที่ไอออนซึ่งเคลื่อนที่ด้วยความเร็วต่างกันในแนวสนามไฟฟ้าตอบสนองต่อแสงความถี่ต่างกัน จึงสามารถเลือกใช้แสงเพื่อชนไอออนหรืออะตอมที่มีความเร็วสูงให้มีความเร็วลดลงจนมีพลังงานต่ำ (เย็นลง) และค่อย ๆ ปรับความถี่แสงสำหรับกระตุ้นอนุภาคที่ความเร็วลดลงแล้วให้มีความเร็วลดลงเรื่อย ๆ ตามลำดับจนถึงระดับพลังงานต่ำสุดที่ทำได้ วิธีการนี้เรียกว่า การทำความเย็นแบบดอปเปลอร์ (Doppler cooling)[5.5] หรือการทำความเย็นด้วยเลเซอร์ (Laser cooling) [*Diedrich และคณะ 1989; Nielsen & Chuang 2000]* โดยขีดจำกัดของการทำความเย็นแบบดอปเปลอร์อยู่ที่ระดับพลังงานต่ำสุดเท่ากับ $k_B T \approx \hbar \Gamma / 2$ (เมื่อ Γ แทนความถี่ที่ไอออนดูดกลืนหรือปลดปล่อยแสงเพื่อเปลี่ยนระดับพลังงาน และ k_B แทนค่าคงที่ของโบลต์ซมันน์) ซึ่งการทำความเย็นของไอออนหรืออะตอม ให้พลังงานต่ำกว่าขีดจำกัดการทำความเย็นแบบดอปเปลอร์ (วิธีการทำความเย็นด้วยแสงเลเซอร์โดยทำให้อะตอมเคลื่อนที่ช้าลงด้วยปรากฏการณ์ดอปเปลอร์) ทำได้โดยวิธีที่เรียกว่า การทำความเย็นแบบไซด์แบนด์ (Side-band cooling) โดยการกระตุ้นให้เกิดการเปลี่ยนระดับพลังงานในไอออนหรืออะตอมหนึ่งระดับและคายพลังงานโดยมีความน่าจะเป็นที่จะคายพลังงานมากกว่าพลังงานที่ดูดกลืนเข้าไปและทำให้ระดับพลังงานของระบบลดลงไปอีก ซึ่งทำให้ได้อุณหภูมิต่ำลงอีกถึง $k_B T \ll \hbar \omega_z$ (เมื่อ ω_z แทนความถี่เชิงมุมของการสั่นของอะตอมหรือไอออน) ดังรูปที่ 5.10

5.2 สมการที่อธิบายว่าอนุพันธ์เชิงตำแหน่งอันดับสอง (Laplacian) ของพลังงานศักย์หรือศักย์ไฟฟ้า มีค่าเป็นศูนย์เสมอ

5.3 จุดที่อนุพันธ์อันดับหนึ่ง (ความชัน) เป็นศูนย์ แต่อนุพันธ์อันดับสอง (ความเว้า) มีค่าเป็นบวก

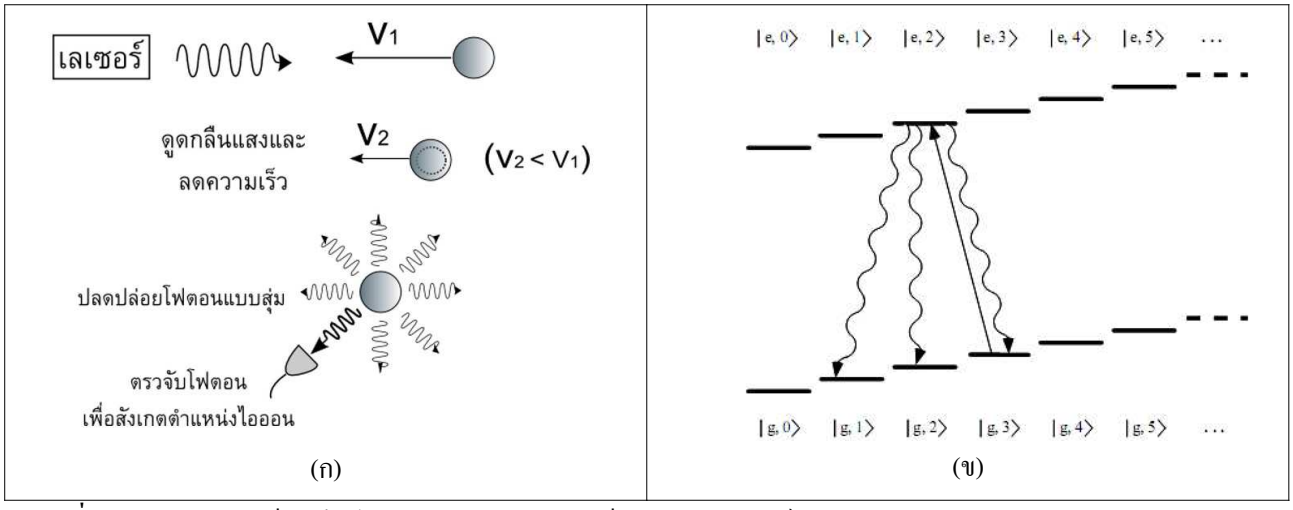
5.4 จุดในพื้นผิวสามมิติที่เป็นจุดต่ำสุดในแกนหนึ่ง แต่เป็นจุดสูงสุดสำหรับอีกแกนหนึ่ง พื้นผิวดังกล่าวมีลักษณะเหมือนอานม้า

5.5 จากการที่ความยาวคลื่นของไอออนเปลี่ยนแปลงตามขนาดและทิศทางของความเร็ว เหมือนในปรากฏการณ์ดอปเปลอร์ซึ่งอธิบายได้ด้วยตัวอย่างที่ว่า เหตุใดเสียงจากรถจักรยานยนต์ที่เคลื่อนที่ใกล้เข้ามาจึงมีความถี่สูง



(ก) (ข)

รูปที่ 5.9 (ก) ไอออนที่ถูกกักด้วยสนามไฟฟ้าลอยอยู่ในบริเวณจำกัด ให้สถานะสปินทิศขึ้น แทน "0" ทิศลงแทน "1" และใช้พัลส์แสงในการปรับสถานะได้ [*Morsch 2008*] (ข) วิธีจัดอุปกรณ์การกักไอออนด้วยวิธีของพอล (Paul trap) อธิบายกระแสไฟที่ปล่อยสู่แท่งอิเล็กโทรดในรูป ก. โดย d.c. หมายถึงไฟฟ้ากระแสตรง และ r.f. หมายถึงไฟฟ้ากระแสสลับความถี่วิทยุ (Radio Frequency) รูปดัดแปลงจาก [*Kielpinski และคณะ 2002*]



(ก) (ข)

รูปที่ 5.10 การทำความเย็นให้กับไอออน (ก) การทำความเย็นแบบดอปเปลอร์ ภาพปรับปรุงจาก [*NationalPhysLabUK.NET*] (ข) การทำความเย็นแบบไซด์แบนด์ โดย "g" และ "e" แทนสถานะพื้นและสถานะกระตุ้นของอิเล็กตรอนในไอออน และจำนวนเต็ม 0,1,2,... แทนระดับพลังงานของการสั่นของไอออน โดยมีโอกาสจากสองในสามที่ไอออนจะลดระดับพลังงานลงจากเดิม (เส้นรูปคลื่น) รูปดัดแปลงจาก [*Steane 1997*]

5.2.2.3 ความสามารถในการคงคุณสมบัติความอาพันธ์เชิงควอนตัม

การสร้างควอนตัมคอมพิวเตอร์ด้วยไอออนที่ถูกกักนั้นประสบความสำเร็จในการสร้างต้นแบบที่มีจำนวนคิวบิตไม่มาก อย่างไรก็ตามหากต้องการสร้างควอนตัมคอมพิวเตอร์ที่สามารถรองรับคิวบิตจำนวนมากด้วยวิธีนี้จะประสบปัญหาทั้งเชิงทฤษฎีและปฏิบัติ หนึ่งในแนวทางการแก้ไขปัญหาดังกล่าวคือสร้างระบบการคำนวณที่มีขนาดเล็กหลายๆระบบ แล้วจึงเชื่อมต่อระบบเหล่านั้นด้วยการสื่อสารเชิงควอนตัมแทนการสร้างระบบใหญ่ระบบเดียว [*Kielpinski และคณะ 2002*]

แม้ว่าวิธีนี้จะสามารถแก้ปัญหาการคงคุณสมบัติความอาพันธ์เชิงควอนตัมของระบบย่อยแต่ละระบบได้ แต่ก็ได้ก่อให้เกิดปัญหาใหม่ที่ตามมาคือ ปัญหาการคงคุณสมบัติเชิงควอนตัมในระหว่างการสื่อสารระหว่างระบบ เนื่องจากในกระบวนการสื่อสารนั้นจะต้องมีขั้นตอนที่มีการส่งไอออนจากระบบย่อยหนึ่งไปสู่อีกระบบย่อยหนึ่ง ขั้นตอนนี้เองที่อาจก่อให้เกิดการสูญเสียความอาพันธ์เชิงควอนตัมได้ เช่นการรบกวนจากสนามแม่เหล็กโดยปรากฏการณ์ซีมานน์ (Zeeman effect) การรบกวนนี้จะทำให้เฟสของ

สถานะเปลี่ยนไป[5.6] เช่น $|\downarrow\rangle+|\uparrow\rangle$ เปลี่ยนเป็น $|\downarrow\rangle+e^{i\alpha}|\uparrow\rangle$ โดยเฟสที่เปลี่ยนไปนั้น ถึงแม้ว่าจะมีความเป็นไปได้ที่จะวัดค่าในเชิงทฤษฎี แต่การวัดค่าในทางปฏิบัตินั้นทำได้ยากมาก

สำหรับวิธีการแก้ปัญหาที่ตามมานี้ เดฟ คีลปินสคี (Dave Kielpinski) และคณะเสนอวิธีแก้ปัญหาโดยวิธีที่เรียกว่าการลดเฟสร่วมกัน (Collective dephasing) วิธีนี้จะแทนสถานะ "0" ของคิวบิตด้วย $|\downarrow\uparrow\rangle$ และแทนสถานะ "1" ด้วย $|\uparrow\downarrow\rangle$ ต่อมาสมมติว่าอนุภาคหนึ่งถูกรบกวนระหว่างการส่ง ผลลัพธ์ที่ได้คือ $|0\rangle+|1\rangle\rightarrow e^{i\alpha_1}|\downarrow\uparrow\rangle+e^{i\alpha_2}|\uparrow\downarrow\rangle=|0\rangle+e^{i\Delta\alpha}|1\rangle$ โดย ดั $\Delta\alpha\equiv\alpha_2-\alpha_1$ งนั้นถ้า $\Delta\alpha=0$ การเปลี่ยนเฟสของอนุภาคจะไม่ส่งผลต่อค่าของคิวบิต (การที่ $\Delta\alpha=0$ เกิดขึ้นได้เพราะโดยประมาณแล้วกลุ่มของอนุภาคเดินทางโดยใช้เส้นทางเดียวกันในเวลาเดียวกัน)

5.2.2.4 การทำงานของเกตลอจิกเชิงควอนตัม

นักวิจัยจำนวนหนึ่งได้แสดงให้เห็นว่าการคำนวณทางควอนตัมแบบใดๆ ก็ตามที่ต้องกระทำกับคิวบิตจำนวนมากสามารถแบ่งออกเป็นการคำนวณที่มีหลายขั้นตอนต่อกันได้ โดยแต่ละขั้นประกอบไปด้วยการคำนวณที่ใช้เพียงคิวบิตเดียวหรือสองคิวบิต [*Wineland และคณะ 1998*] การคำนวณในลักษณะนี้มีความคล้ายคลึงกับการคำนวณแบบดั้งเดิมซึ่งคำนวณโดยใช้เกตลอจิกสำหรับเกตลอจิกเชิงควอนตัมที่เป็นพื้นฐานที่สุดนั้นจะมีอยู่สองแบบด้วยกันคือเกตหมุนบิตเดี่ยว (Single bit rotation gate) และเกต NOT ควบคุมบิตคู่ (Two-bit controlled-NOT gate) สำหรับเกตหมุนบิตเดี่ยวหรือตัวดำเนินการ $R(\theta,\varphi)$ เป็นตัวดำเนินการที่กระทำกับคิวบิตดียว และมีคุณสมบัติดังนี้

$$\begin{aligned}|\downarrow\rangle &\rightarrow \cos(\theta/2)|\downarrow\rangle-ie^{i\varphi}\sin(\theta/2)|\uparrow\rangle \\ |\uparrow\rangle &\rightarrow \cos(\theta/2)|\uparrow\rangle-ie^{i\varphi}\sin(-\theta/2)|\downarrow\rangle\end{aligned} \qquad \text{.....(5.1)}$$

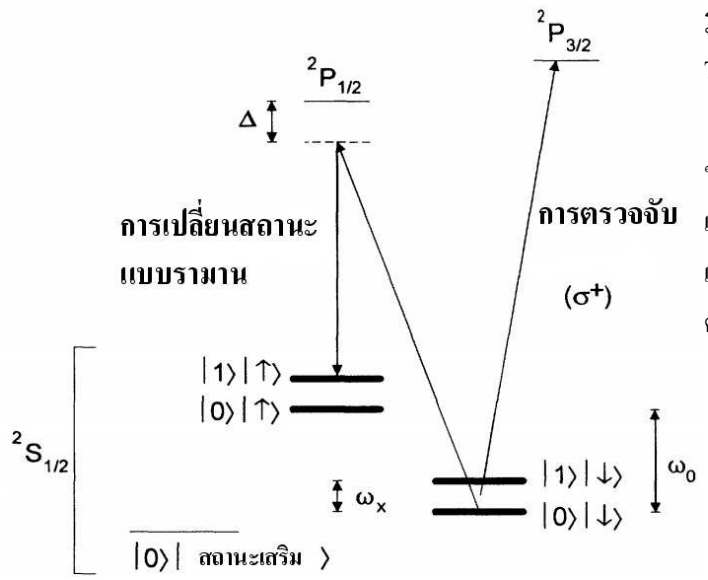
โดย θ และ φ เป็นตัวแปร (Parameter) ของเกตควบคุมการหมุน (Rotation gate)

ส่วนเกต NOT ควบคุมบิตคู่ (CN gate) นั้นคล้ายกับเกต XOR ในคอมพิวเตอร์แบบดั้งเดิม โดยเกตลอจิกประเภทนี้จะมีบิตหนึ่งเป็นบิตที่ควบคุมผลลัพธ์ของบิตอื่น บิตที่ใช้ควบคุมเรียกว่าบิตควบคุม (Control bit) ในขณะบิตที่ถูกควบคุมเรียกว่าบิตเป้าหมาย (Target bit) สำหรับวิธีการทำงานนั้นบิตเป้าหมายในที่นี้ตั้งชื่อว่าไอออน k จะกลับทิศของสปิน $|\uparrow\rangle_k \Leftrightarrow |\downarrow\rangle_k$ ก็ต่อเมื่อบิตควบคุมซึ่งอาจตั้งชื่อว่าไอออน j อยู่ในสถานะ $|\uparrow\rangle$ เท่านั้น ดังนั้นจะได้การแปลงรูปของบิต j และ k ดังนี้

$$\begin{aligned}|\downarrow\rangle_j|\downarrow\rangle_k &\rightarrow |\downarrow\rangle_j|\downarrow\rangle_k \\ |\downarrow\rangle_j|\uparrow\rangle_k &\rightarrow |\downarrow\rangle_j|\uparrow\rangle_k \\ |\uparrow\rangle_j|\downarrow\rangle_k &\rightarrow |\uparrow\rangle_j|\uparrow\rangle_k \\ |\uparrow\rangle_j|\uparrow\rangle_k &\rightarrow |\uparrow\rangle_j|\downarrow\rangle_k\end{aligned} \qquad \text{.....(5.2)}$$

ก่อนที่จะนำเสนอระบบในธรรมชาติที่ให้ผลเช่นเดียวกับเกตลอจิกทั้งสองดังกล่าวนั้น จะต้องทราบถึงวิธีการเปลี่ยนสถานะจากสถานะหนึ่งไปสถานะอื่นๆ ด้วยดังรูปที่ 5.11 การเปลี่ยนสถานะจะใช้แสงจากแหล่งกำเนิดเลเซอร์สองแหล่งยิงไปยังไอออนที่ต้องการจะเปลี่ยนสถานะ โดยความถี่โหมดของเลเซอร์ทั้งสองต้องมีผลต่างเท่ากับระดับพลังงานที่ต้องการจะเปลี่ยนสถานะ (นิยามของความถี่โหมดคือ $\omega=2\pi f$ โดย f เป็นความถี่ของแสงเลเซอร์) รูปที่ 5.11 แสดงตัวอย่างการเปลี่ยนสถานะจาก $|0\rangle|\downarrow\rangle$ ไปยังสถานะ $|1\rangle|\uparrow\rangle$ เนื่องจากผลต่างระดับพลังงานของ $|0\rangle|\downarrow\rangle$ กับ $|1\rangle|\uparrow\rangle$ มีค่าเท่ากับ $\omega_0+\omega_x$ ดังนั้นผลต่างของความถี่โหมดของแสงเลเซอร์ทั้งสองต้องมีค่า $\omega_0+\omega_x$ ด้วย เงื่อนไขอีกประการของการเปลี่ยนสถานะเช่นนี้คือค่าพลังงานสูงสุดที่ไอออนมีก่อนจะเปลี่ยนไปอีกสถานะหนึ่งต้องทำให้ค่า $\Delta\gg\omega_{0,}\omega_x,\gamma$ (Δ แสดงอยู่ในรูปที่ 5.11)โดย γ คือค่าความถี่โหมดของคลื่นแม่เหล็กไฟฟ้าที่สถานะ P ในสถานะกระตุ้น (Excited state) ปลดปล่อยออกมา

[5.6] เฟสที่เปลี่ยนไปนี้ขึ้นกับเส้นทางที่อนุภาคเดินทาง



รูปที่ 5.11 การเปลี่ยนสถานะแบบรามาน (Raman Transition) จากสถานะ $|0\rangle|\downarrow\rangle$ ไปยังสถานะ $|1\rangle|\uparrow\rangle$ โดยการยิงเลเซอร์จากสองแหล่งที่มีผลต่างของ mode frequency เท่ากับ $\omega_0+\omega_x$ ซึ่งเป็นความถี่เชิงมุมที่เท่ากับผลต่างของระดับพลังงานพอดี ภาพนี้ยังแสดงวิธีการตรวจวัดสถานะซึ่งนำเสนอในหัวข้อถัดไป รูปดัดแปลงจาก [*Monroe และคณะ 1995*]

สำหรับการเปลี่ยนสถานะของเกตหมุนบิตเดี่ยวนั้นทำได้โดยการยิงเลเซอร์จากสองแหล่งที่มีความถี่โหมดเท่ากับ ω_0 สำหรับเฟส θ ที่เปลี่ยนไปนั้นจะขึ้นอยู่กับระยะเวลาที่ยิงเลเซอร์ทั้งสองไปยังไอออน (วิธีการเรียกชื่อพัลส์ของแสงเลเซอร์จะเรียกตามเฟสที่เลเซอร์ทำให้เปลี่ยนไป เช่น หาก θ เปลี่ยนไปเท่ากับ π จะเรียกพัลส์นั้นว่าพัลส์ π เป็นต้น) การยิงคู่ของลำแสงไปยังไอออนในลักษณะนี้จะไม่ทำให้ไอออนเปลี่ยนสถานะระหว่างสถานะ $|0\rangle$ และ $|1\rangle$ แต่จะทำให้สปินของไอออน ($|\uparrow\rangle$ และ $|\downarrow\rangle$) เปลี่ยนไป

ทางด้านของเกต CN นั้น ซิแรก(Cirac) และโซลเลอร์(Zoller) พบวิธีการแปลงของเกต CN ดังนี้

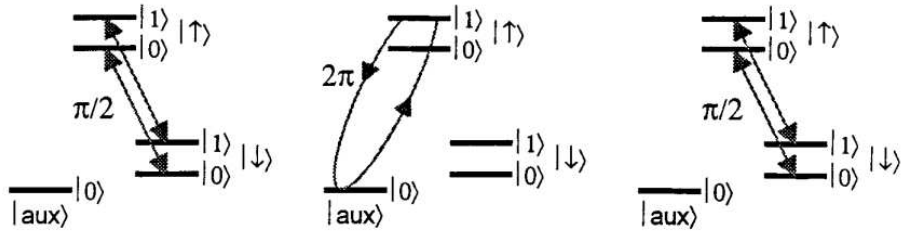
$$\begin{aligned}
|0\rangle|\downarrow\rangle_k &\rightarrow |0\rangle|\downarrow\rangle_k \\
|0\rangle|\uparrow\rangle_k &\rightarrow |0\rangle|\uparrow\rangle_k \\
|1\rangle|\downarrow\rangle_k &\rightarrow |1\rangle|\uparrow\rangle_k \\
|1\rangle|\uparrow\rangle_k &\rightarrow |1\rangle|\downarrow\rangle_k
\end{aligned} \qquad \text{.....(5.3)}$$

ซึ่งสามารถสร้างระบบทางกายภาพที่สามารถรองรับสมการทางคณิตศาสตร์ดังกล่าวได้ดังรูปที่ 5.12

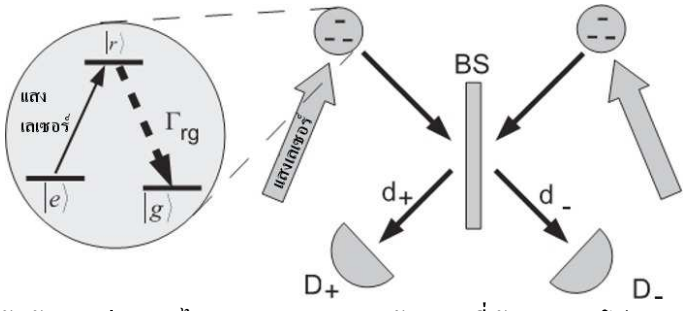
สำหรับขั้นตอนการเปลี่ยนสถานะตามแผนภาพจากซ้ายไปขวาแสดงดังนี้

- ยิงลำแสงที่มีค่าพัลส์ $\pi/2$ ไปยังไอออน จะทำให้ไอออนมีค่าเปลี่ยนไป +1/4 ของวัฏจักรราบี (Rabi cycle[5.7])
- ยิงสำแสงที่มีค่าพัลส์ 2π ไปยังไอออน ซึ่งหากไอออนอยู่ในสถานะ $|0\rangle$ ลำแสงที่ยิงไปจะไม่มีผลทำให้สถานะเปลี่ยนแปลง แต่หากไอออนอยู่ในสถานะ $|1\rangle$ กระบวนการนี้จะทำให้ไอออนเปลี่ยนสถานะโดยมีขั้นตอนคือ $|1\rangle|\uparrow\rangle \rightarrow |0\rangle|aux\rangle \rightarrow -|1\rangle|\uparrow\rangle$ ซึ่งครบขั้นตอนของวัฏจักรราบี
- ยิงสำแสงที่มีค่าพัลส์ $\pi/2$ ไปยังไอออน กระบวนการนี้จะทำให้ไอออนมีสถานะเปลี่ยนไป -1/4 ของวัฏจักรราบี หากไอออนอยู่ในสถานะ $|0\rangle$ จะทำให้สถานะของไอออนกลับมาเหมือนขณะก่อนเริ่มขั้นตอนแรก ในขณะที่หากไอออนอยู่ในสถานะ $|1\rangle$ จะทำให้ไอออนเปลี่ยนเฟสไป 2π

[5.7] Rabi Cycle เป็นวัฏจักรของระบบเชิงควอนตัมที่มีสองสถานะที่อยู่ภายในสนามซึ่งถูกทำให้แกว่ง ระบบสองสถานะนี้มีสถานะที่เป็นได้สองรูปแบบ ถ้าหากระดับพลังงานไม่มีการสูญหายเมื่อระบบได้รับพลังงานจะทำให้ระบบอยู่ในสถานะกระตุ้นเชิงควอนตัม



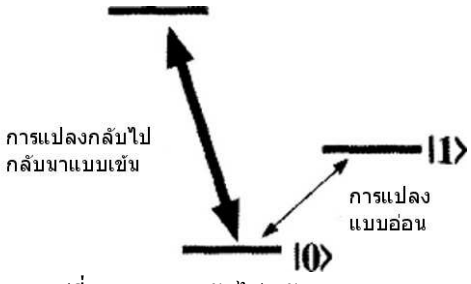
รูปที่ 5.12 การทำงานของเกต NOT ควบคุม (Controlled NOT gate)
เมื่อ |aux> คือสถานะเสริม รูปดัดแปลงจาก [*Wineland และคณะ 1998*]



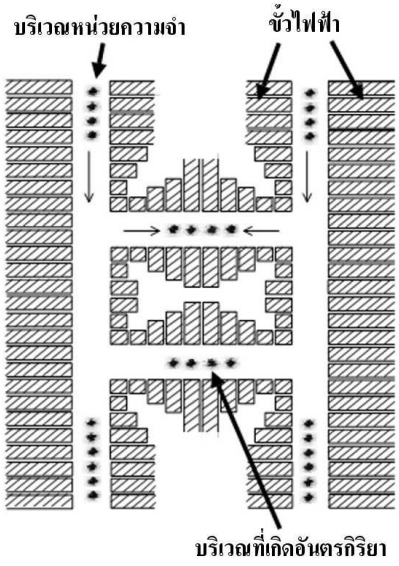
รูปที่ 5.13 การสร้างสถานะพัวพันระหว่างสองไอออน การตรวจพบสัญญาณที่ตัวตรวจหาโฟตอนหนึ่งครั้ง ทำให้สถานะของไอออนทั้งสองถูกโปรเจกต์หรือวางทาบไปยังสถานะพัวพันแบบเบลล์ |*e*,*g*> + |*g*,*e*> ตัวแยกลำแสง (Beam Splitter: BS) ทำให้ไม่สามารถทราบได้ว่าโฟตอนถูกปล่อยมาจากไอออนใด รูปดัดแปลงจาก [*Zippilli และคณะ 2009*]

5.2.2.5 การสร้างสถานะพัวพันระหว่างไอออน

วิธีการอย่างง่ายสำหรับสร้างสถานะพัวพันระหว่างไอออนทำได้โดยผ่านกระบวนการกระเจิงแบบรามาน (Spontaneous Raman scattering) โดยเตรียมสถานะของไอออนทั้งสองให้อยู่ในสถานะกระตุ้น (excited: "*e*") แทนด้วย |*e*,*e*> หลังจากนั้นกระตุ้นไอออนทั้งคู่ด้วยเลเซอร์ซึ่งมีความถี่ตรงกับระดับพลังงานระหว่างสถานะกระตุ้น (|*e*>) ไปยังสถานะชั่วคราว (|*r*>) ซึ่งไม่มีความเสถียรและจะปลดปล่อยโฟตอนความถี่ใหม่ (Γ_{rg} ดังรูปที่ 5.13) ทำให้ลดระดับพลังงานลงมาเป็นสถานะพื้น (|*g*>) กรณีไอออนซ้ายมือปลดปล่อยโฟตอนในขณะที่ไอออนขวามือไม่มีการปลดปล่อยโฟตอน สถานะผลลัพธ์จะได้ |สถานะพื้น, สถานะกระตุ้น> หรือ |*g*,*e*> และกรณีไอออนขวามือปลดปล่อยโฟตอนและไอออนซ้ายมือไม่ปลดปล่อยโฟตอน สถานะผลลัพธ์จะเป็น |สถานะกระตุ้น, สถานะพื้น> หรือ |*e*,*g*> ซึ่งรูปทั่วไปของสถานะสองคิวบิตดังกล่าวแทนด้วย *a*|*e*,*e*> + *b*|*e*,*g*> + *c*|*g*,*e*> + *d*|*g*,*g*> และเหตุการณ์ที่พบหนึ่งโฟตอนปรากฏหลังตัวแยกลำแสง ทำให้สรุปได้ว่าสถานะของไอออนไม่ใช่ |*e*,*e*> (ไม่มีการปลดปล่อยโฟตอน) และไม่ใช่ |*g*,*g*> ซึ่งมีการปลดปล่อยสองโฟตอน (สมมติว่าชุดตรวจหาโฟตอนสามารถแยกแยะโฟตอนระหว่างหนึ่งและสองโฟตอนได้) ดังรูปที่ 5.13



รูปที่ 5.14 การเปลี่ยนสถานะกลับไปกลับมา (Cycling transition)
อธิบายการอ่านค่าออกของคิวบิตไอออน รูปดัดแปลงจาก [*Stolze & Suter 2004*]



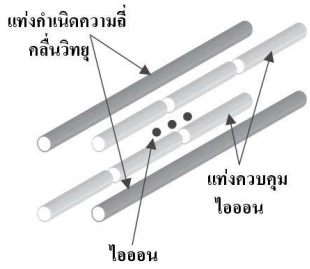
รูปที่ 5.15 สถาปัตยกรรมควอนตัมคอมพิวเตอร์ที่อาศัยการกักไอออน ภาพจาก [*Kielpinski และคณะ 2002*]

5.2.2.6 การอ่านค่าออก

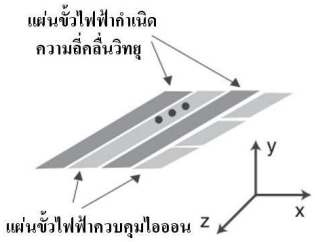
ข้อดีของการคำนวณเชิงควอนตัมด้วยไอออนที่ถูกกักคือ การอ่านสถานะทำได้แม่นยำ (เลือกสถานะไอออนที่ต้องการได้) และมีความน่าจะเป็นที่จะทำสำเร็จสูง ความถี่ของแสงที่ใช้กระตุ้นเพื่ออ่านสถานะออกต้องเป็นความถี่ที่ตรงกับการเปลี่ยนสถานะกลับไปกลับมาระหว่างสองสถานะ ซึ่งสถานะคิวบิตจะถูกกระตุ้นด้วยความถี่เหมาะสมและเปลี่ยนไปยังสถานะที่ไม่เสถียรแล้วปลดปล่อยโฟตอนเพื่อกลับมาสถานะเดิม ดังรูปที่ 5.14

5.2.2.7 ความคืบหน้างานวิจัยการคำนวณเชิงควอนตัมด้วยการกักไอออน

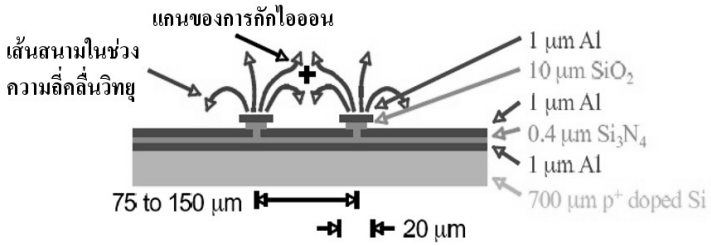
ในปี ค.ศ. 2002 เดฟ คีลปินสคี (Dave Kielpinski) คริสโตเฟอร์ มอนโร (Christopher Monroe) และเดวิด ไวน์แลนด์ (David Wineland) ร่วมกันออกแบบสถาปัตยกรรมสำหรับควอนตัมคอมพิวเตอร์ในสเกลใหญ่โดยอาศัยวิธีการกักไอออนด้วยโครงสร้างเรียกว่าอุปกรณ์คู่ประจุเชิงควอนตัม (Quantum charge-coupled device: QCCD) ดังรูปที่ 5.15 ประกอบด้วยโครงสร้างของขั้วไฟฟ้าที่ถูกแบ่งเป็นส่วนย่อยๆ โดยมีบริเวณหลักสองบริเวณคือ บริเวณหน่วยความจำเชิงควอนตัม (Quantum memory region) สำหรับกักไอออนที่ต้องการให้คงสถานะเดิมไว้ และบริเวณที่เกิดอันตรกิริยา (Interaction region) สำหรับการคำนวณเชิงควอนตัมโดยอาศัยอันตรกิริยาระหว่างไอออนเพื่อให้เกิดการดำเนินการลอจิกเชิงควอนตัม (Quantum logic operation) ที่ต้องการ โดยเมื่อมีคำสั่งเรียกใช้ลอจิกเชิงคอวนตัมจะมีการปรับค่าสนามไฟฟ้าที่ป้อนเข้าสู่ขั้วไฟฟ้าแต่ละแท่งเพื่อค่อยๆ ผลักให้ไอออนที่ต้องการเคลื่อนที่จากบริเวณหน่วยความจำเข้าสู่บริเวณสำหรับการคำนวณ และเคลื่อนที่กลับสู่บริเวณหน่วยความจำเมื่อคำนวณแล้วเสร็จ [*Kielpinski และคณะ 2002*]



(ก)



(ข)



(ค)

รูปที่ 5.16 (ก) โครงสร้างการกักไอออนเชิงเส้นในโครงสร้างสามมิติ (ข) โครงสร้างของการกักไอออนบนระนาบ รูปดัดแปลงจาก [*Seidelin และคณะ 2006*] (ค) วิธีการเจือสารกึ่งตัวนำเพื่อสร้างเป็นชิปสำหรับกักไอออน รูปดัดแปลงจาก [*Leibrandt และคณะ 2009*]

5.2.2.8 การเพิ่มจำนวนคิวบิตในการคำนวณเชิงควอนตัมด้วยสถานะไอออนที่ถูกกัก

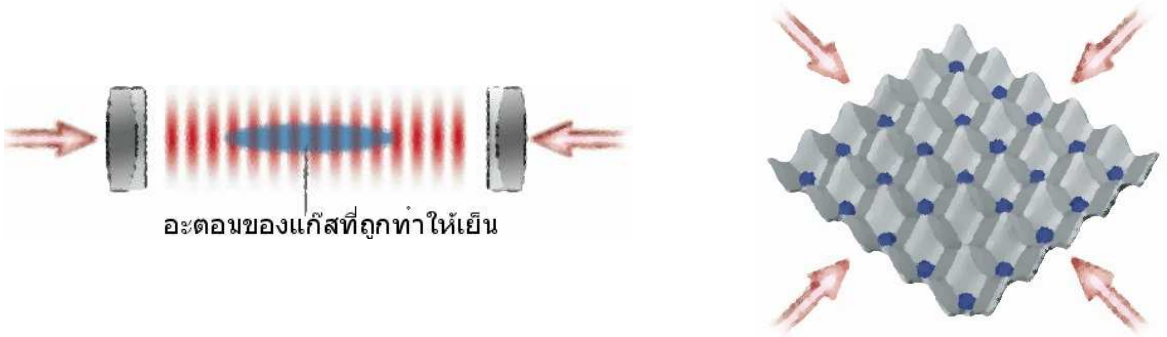
การคำนวณเชิงควอนตัมด้วยการกักไอออนต้องได้รับการพัฒนาส่วนสำคัญคือการปรับจากการกักไอออนในห้องทดลองขนาดใหญ่ ไปสู่การกักไอออนด้วยชิปสารกึ่งตัวนำ (Semiconductor chip) ดังรูปที่ 5.16 การกักไอออนด้วยวิธีดังกล่าวสาธิตโดยกลุ่มวิจัยจากมหาวิทยาลัยมิชิแกน (University of Michigan) ประเทศสหรัฐอเมริกา นำโดยแดน สติก (Dan Stick) และคริสโตเฟอร์ มอนโร (Christopher Monroe) [*Stick และคณะ 2006*] กลุ่มวิจัยจากสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ประเทศสหรัฐอเมริกา นำโดยซิกนี ไซเดลิน (Signe Seidelin) และเดวิด ไวน์แลนด์ (David wineland) [*Seidelin และคณะ 2006*] และกลุ่มวิจัยจากสถาบันเทคโนโลยีแมสซาชูเซตส์ (Massachusetts Institute of Technology: MIT) ประเทศสหรัฐอเมริกา นำโดยเคนเนธ บราวน์ (Kenneth Brown) [*Brown และคณะ 2007*]

5.2.3 การคำนวณเชิงควอนตัมด้วยอะตอมที่เป็นกลาง

จากข้อเสียของการกักไอออนในสนามไฟฟ้าคือปรากฏการสูญเสียความอาพันธ์ ที่เกิดจากสนามไฟฟ้าภายนอกเข้าไปเหนี่ยวนำและมีผลต่อสถานะของคิวบิตในไอออน แต่หากเปลี่ยนจากการใช้ไอออนเป็นการใช้อะตอมที่เป็นกลางจะไม่ถูกเหนี่ยวนำด้วยสนามไฟฟ้า แต่ต้องใช้วิธีอื่นในการกักอนุภาค (เช่นสนามแม่เหล็ก) โดยวิธีการที่มีการเสนอเพื่อให้กักอะตอมที่เป็นกลางได้แก่

- การใช้แลททิซเชิงแสง

เมื่อคลื่นสองชุดรวมกันในขอบเขตจำกัดจะเกิดริ้วของการแทรกสอดแบบเสริมและแบบหักล้าง การเกิดริ้วของคลื่นเมื่อกำหนดเงื่อนไขขอบเขต (เช่นสายกีตาร์ถูกตรึงไว้ที่ปลายทั้งสอง) คลื่นในแนวนั้นจะมีบริเวณเสริมและหักล้างที่เป็นริ้วคงที่เช่นเดียวกับเชือกตรึงที่ถูกสะบัดหรือสายกีตาร์ที่ถูกดีด อาศัยหลักการเดียวกันเมื่อแสงเลเซอร์สองแนวเคลื่อนที่สวนกันจะเกิดริ้วของคลื่นแม่เหล็กไฟฟ้าบริเวณเสริมและหักล้าง ซึ่งผลกระทบของสนามแม่เหล็กไฟฟ้านี้ต่ออะตอมที่เป็นกลางทางไฟฟ้าจะเหมือนว่าเป็นบ่อศักย์ (Potential well) เป็นแถวซึ่งขึ้นกับจำนวนทิศทางของลำแสงที่ตัดกัน เช่น สองแนวตัดกันบนเส้น (หนึ่งมิติ) สามและสี่แนวตัดกันเป็นระนาบ (สองมิติ) อะตอมจะถูกกักไว้ในบริเวณที่ศักย์ไฟฟ้าต่ำสุดในแต่ละแลททิซ ดังรูปที่ 5.17 ในโครงสร้างสองมิติ มีลักษณะคล้าย “รางไข่” [*Morsch 2008*]



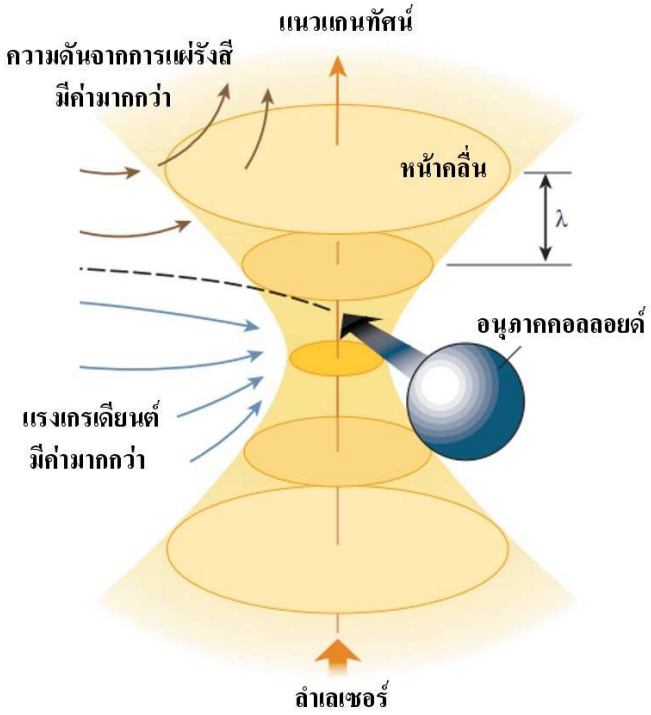
รูปที่ 5.17 การกักอะตอมที่เป็นกลางด้วยแลททิซเชิงแสง ในโครงสร้าง (ก) หนึ่งมิติ และ (ข) สองมิติ
รูปดัดแปลงจาก [*Bloch 2008*]

- การใช้ลำเลเซอร์ซึ่งถูกโฟกัส (Laser-focused beam) หรือแหนบเชิงแสง (Optical tweezers)

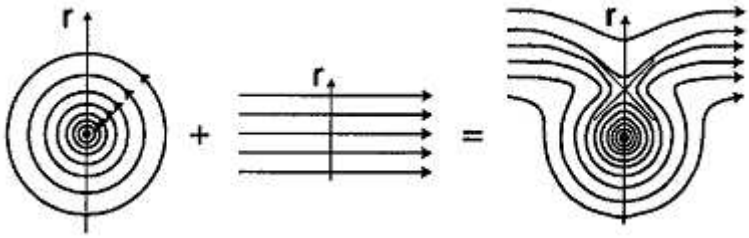
แหนบเชิงแสงใช้แรงจากแสงซึ่งถูกโฟกัสในการกักอนุภาค การกักอะตอมด้วยวิธีนี้ยังอยู่ในขั้นทฤษฎี [*Grier 2003*] โดยปกติแล้วอนุภาคขนาดเล็กมากๆ (เล็กกว่าความยาวคลื่นของแสง) เมื่อถูกยิงด้วยแสงจะเกิดปรากฏการณ์ที่เรียกว่าคู่ขั้วไฟฟ้า (Electric dipole) ซึ่งปรากฏการณ์นี้เกิดขึ้นจากการเหนี่ยวนำสนามไฟฟ้าจากแสง การเกิดคู่ขั้วไฟฟ้าจะทำให้สนามไฟฟ้าในแนวโฟกัสของแสงมีค่าเพิ่มขึ้น ผลก็คือการชนของอนุภาคกับโฟตอนจะทำให้อนุภาควิ่งเข้าหาจุดที่ถูกโฟกัสซึ่งเป็นตำแหน่งที่ต้องการกักอนุภาค การกักอนุภาคด้วยวิธีนี้มีแรงที่สำคัญอยู่สองแรง คือแรงเนื่องจากแสงจากเลเซอร์ อีกแรงหนึ่งเกิดจากความดันเนื่องจากการแผ่รังสีออกจากอนุภาคอันเนื่องมาจากการถ่ายเทโมเมนตัมจากโฟตอนไปยังอนุภาค การที่อนุภาคจะถูกกักได้นั้นแรงเนื่องจากแสงเลเซอร์ต้องมีค่ามากกว่าความดันอันเนื่องมาจากการแผ่รังสี ซึ่งในทางทฤษฎีสามารถทำได้จากการแยกลำแสงออกจากจุดโฟคอล (Focal) ให้ไวพอ ดังรูปที่ 5.18

- การใช้สนามแม่เหล็กสถิตย์ (Static magnetic field)

การใช้สนามแม่เหล็กสถิตย์จะใช้สนามแม่เหล็กสองส่วน คือสนามแม่เหล็กที่วนรอบแนวกระแสไฟฟ้า (เป็นวงกลมรอบทิศกระแสไฟฟ้า) และสนามแม่เหล็กเชิงเส้น ซึ่งเมื่อรวมกันแล้วจะมีจุดๆ หนึ่งซึ่งสนามแม่เหล็กลัพธ์เป็นศูนย์ ทำให้อนุภาคซึ่งมีขั้วทางแม่เหล็กถูกผลักและกักไว้ ณ จุดๆ นั้นได้ [*Reichel และคณะ 1999*] ดังรูปที่ 5.19



รูปที่ 5.18 การทำงานของแหนบเชิงแสง จากภาพหากแรงจากเลเซอร์ (Gradient force) มีค่ามากกว่าความดันจากการแผ่รังสี (Radiation pressure) จะทำให้อนุภาคถูกกักอยู่บริเวณจุดโฟกัสได้ ในทางตรงกันข้าม หากความดันจากการแผ่รังสีมีค่ามากกว่า จะทำให้อนุภาคถูกผลักหลุดจากจุดโฟกัส รูปดัดแปลงจาก [*Grier 2003*]



รูปที่ 5.19 การกักอะตอมที่เป็นกลางทางไฟฟ้าด้วยสนามแม่เหล็กสถิตย์ ภาพขวาสุดแทนสนามแม่เหล็กลัพธ์ซึ่งมีจุดที่สนามรวมเป็นศูนย์ รูปดัดแปลงจาก [*Reichel และคณะ 1999*]

นอกจากนี้ ก่อนที่อะตอมจะถูกกักในสนามแม่เหล็กจะต้องมีการทำให้พลังงานจลน์หรืออุณหภูมิอยู่ในระดับต่ำสุด (Ultracold) หรือในอุดมคติคือสถานะควบแน่นแบบโบซ-ไอน์สไตน์ วิธีการทำให้อะตอมเย็นลงใช้วิธีเดียวกับที่อธิบายในเรื่องการกักไอออนคือการใช้แสงในความถี่ที่เหมาะสมชนให้อะตอมลดความเร็วลงเรื่อยๆ ด้วยการทำความเย็นแบบดอปเปลอร์หรือ การทำความเย็นด้วยเลเซอร์ และวิธีทำความเย็นแบบไซด์แบนคือกระตุ้นให้อะตอมสุ่มปล่อยพลังงานในรูปแสงโดยมีความน่าจะเป็นที่จะปล่อยพลังงานในช่วงกว้างและลดระดับพลังงานลง (ดูเพิ่มเติมในหัวข้อ 5.2.2 การคำนวณเชิงควอนตัมด้วยไอออนที่ถูกกัก)

5.2.3.1 การแทนคิวบิต

การบรรจุอะตอมลงบนโครงสร้างเพื่อแทนคิวบิตโดยใช้แลททิซเชิงแสงมีคุณสมบัติคือ

- แลททิซเชิงแสงสามารถใช้กักอะตอมจำนวนมากซึ่งถูกทำให้เย็นลงด้วยวิธีการทำความเย็นด้วยเลเซอร์หรือวิธีการควบแน่นแบบโบซ–ไอน์สไตน์
- ปัญหาของการระบุสถานะคิวบิตหนึ่งในโครงสร้างแลททิซเชิงแสงซึ่งมีระยะระหว่างคิวบิต (อะตอม) เพียงครึ่งหนึ่งของความยาวคลื่นแสงเลเซอร์ที่ใช้สร้างแลททิซ (ความยาวคลื่นน้อยมาก) ซึ่งทางแก้มีดังต่อไปนี้ [*Heinrich 2004*] การออกแบบโครงสร้างแลททิซให้มีระยะระหว่างอะตอมที่ถูกกักมากกว่าขนาดความยาวคลื่นแสงที่ใช้

[*Peil และคณะ 2003*] การใช้แสงที่มีความยาวคลื่นมากขึ้นทำให้ระยะระหว่างอะตอมในแลททิซซึ่งติดกันห่างไกลยิ่งขึ้นทำให้อ่านค่าได้ง่ายขึ้น การควบคุมการบรรจุอะตอมไว้ในโครงสร้างแลททิซเชิงแสงให้มีเพียงบางส่วนของแลททิซมีอะตอมบรรจุอยู่ ส่วนบางแลททิซถูกเว้นว่างทำให้เกิดระยะห่างระหว่างคิวบิต และการกักอะตอมที่เป็นกลางรูปแบบอื่น นอกเหนือจากวิธีแลททิซเชิงแสง เช่นใช้การกักด้วยแม่เหล็ก

การเลือกสถานะของอะตอมเพื่อแทนคิวบิตสำหรับการควบคุมด้วยแลตทิซเชิงแสงจะมีวิธีการเลือกดังนี้

- คิวบิตจากสถานะภายใน (Internal-state qubit) จะแทนคิวบิตด้วยสถานะที่ละเอียดมาก (Hyperfine states) เมื่อถูกกระทำด้วยสนามแม่เหล็กหรือสนามไฟฟ้า และสามารถแยกแยะด้วยการวิเคราะห์การเกิดสเปกตรัมของอะตอม (Atomic spectroscopy)
- คิวบิตจากสถานะเคลื่อนที่ (Motional qubits) จะแทนคิวบิตด้วยระดับพลังงานที่ไม่ต่อเนื่องภายในศักย์ของโครงสร้างแลททิซเชิงแสง
- คิวบิตจากการเลือกใช้ระดับพลังงานของอะตอมในสเปกตรัมอื่นๆ ต้องพิจารณาถึงการมีอันตรกิริยากับสิ่งแวดล้อม ซึ่งจะขาดความเสถียรในการทำหน้าที่แทนคิวบิต อย่างไรก็ดีสถานะดังกล่าวสามารถนำมาใช้เป็นสถานะชั่วคราว (Intermediate states) ระหว่างการทำงานสำหรับลอจิกเชิงควอนตัมได้

5.2.3.2 การเตรียมสถานะเริ่มต้น

- กรณีเลือกใช้สถานะภายใน สถานะถูกเตรียมโดยวิธีมาตรฐาน คือเทคนิคการปั๊มด้วยแสง (Optical pumping techniques) ซึ่งมีการเสนอตั้งแต่ปี ค.ศ. 1950 วิธีการดังกล่าวทำให้ได้สถานะที่ต้องการด้วยความถูกต้อง (Fidelity) มากกว่า 0.9999 [*Raizen และคณะ 2009*]
- กรณีเลือกใช้สถานะการเคลื่อนที่ คิวบิตจะถูกทำให้เย็นลงจนถึงสถานะพื้นเชิงการเคลื่อนที่ (Motional ground state) ซึ่งทำได้โดยการทำให้เย็นด้วยเลเซอร์ และวิธีทำให้เย็นแบบไซด์แบนด์ (ดูในหัวข้อ 5.2.2 การคำนวณเชิงควอนตัมด้วยไอออนที่ถูกกัก)
- การใช้อนุภาคที่ทำให้เย็นด้วยการควบแน่นแบบโบซ–ไอน์สไตน์ มีความเหมาะสมสำหรับการเตรียมสถานะคิวบิตทั้งแบบที่ใช้สถานะภายใน และสถานะการเคลื่อนที่

5.2.3.3 ระยะเวลาคงสภาพความอาพันธ์

การสูญเสียความอาพันธ์ของสถานะคิวบิตในการเก็บข้อมูลเองซึ่งเป็นการสูญเสียคุณสมบัติเชิงควอนตัมที่ต้องการให้มีสถานะเดิมเพื่อใช้ในการเก็บข้อมูล สามารถแบ่งได้เป็นกรณีต่างๆ ดังนี้

- กรณีการใช้สถานะภายในแทนคิวบิต มีระยะเวลาคงสภาพความอาพันธ์อยู่ที่หลายวินาที แต่ยังไม่มีรายงานการคำนวณเวลาที่แน่นอนและคาดว่ามีความแตกต่างกันตามระบบควอนตัมที่เลือกใช้ [*Heinrich 2004*]
- กรณีการใช้สถานะการเคลื่อนที่ ระยะเวลาคงสภาพความอาพันธ์มีค่าเวลานาน เนื่องจากอันตรกิริยาระหว่างคิวบิตกับสิ่งแวดล้อมมีน้อย แต่ยังไม่มีรายงานการคำนวณระยะเวลาคงสภาพความอาพันธ์ที่แน่นอน [*Heinrich 2004*]
- กลไกการสูญเสียความอาพันธ์ส่วนหลักๆ เกิดจากการกระเจิงด้วยโฟตอน (Photon scattering) และสาเหตุอื่นๆ เช่น ความแปรปรวนของสนามที่ใช้กัก (Trapping field fluctuations) และการชนแบบไม่อนุรักษ์กับอนุภาคของแก๊สที่อยู่ภายนอก ทั้งนี้วิธีการกักอะตอมด้วยแลททิซเชิงแสงสำหรับระยะเวลายาวนานจริงๆ ยังไม่ถูกค้นพบ (ค.ศ. 2010)

การสูญเสียความอาพันธ์จากความไม่สมบูรณ์ของเกตลอจิกเชิงควอนตัม ซึ่งเป็นผลจากการทำงานลอจิกเชิงควอนตัมที่ไม่สมบูรณ์ เช่นการสร้างอันตรกิริยาระหว่างอะตอมสองอะตอมเพื่อให้ได้เกต CNOT แต่กลับมีผลกระทบต่อคิวบิตอื่นๆ ที่ไม่ต้องการให้เกิด

นอกจากนี้มีตัวแปรอื่นๆ ซึ่งล้วนต้องได้รับการพิจารณา [*Heinrich 2004*] ดังนี้

- เสถียรภาพของแสงเลเซอร์ที่นำมาใช้ (มีความเข้มแสงคงที่เพียงใด)
- เสถียรภาพของระยะเวลากระตุ้นด้วยพัลส์ (Pulse timing stability)
- การเปล่งรังสีแบบเกิดขึ้นเองของอะตอมที่อยู่นอกเหนือสถานะคิวบิตสำหรับการคำนวณ
- ความพัวพันระหว่างสองสถานะที่ไม่ต้องการให้เกิด
- การเปลี่ยนแปลงของคิวบิตซึ่งอยู่ภายนอกเซตของสถานะที่ใช้นิยาม เช่น นิยามคิวบิตโดย “0” หมายถึง สถานะพื้น และ “1” หมายถึง สถานะกระตุ้นอันดับที่หนึ่ง แต่อะตอมถูกกระตุ้นให้อยู่ที่สถานะกระตุ้นอันดับที่สาม

ระยะเวลาคงสภาพความอาพันธ์ (T_d) เมื่อคิดองค์ประกอบหลักๆ มีค่าประมาณ 1 มิลลิวินาที ส่วนเวลาในการทำงานของเกตลอจิกเชิงควอนตัม (Quantum gate operation time: T_{op}) มีค่าประมาณ 0.1 ถึง 100 ไมโครวินาที ขึ้นกับความถี่แสงที่ใช้ในการกักอะตอม ทำให้ได้จำนวนตัวดำเนินการที่ทำงานได้ต่อคิวบิต (Number of operations per qubit: n_{op}) คือ $T_d / T_{op} = 10$ ถึง 10^4 เกตลอจิก [*Heinrich 2004*]

5.2.3.4 การทำงานของเกตลอจิกเชิงควอนตัม

การทำงานของเกตลอจิกเชิงควอนตัม เมื่อกระทำกับอะตอมที่ถูกทำให้เย็นจัดต้องรักษาผลกระทบเชิงความร้อนจากสิ่งแวดล้อมให้น้อยที่สุด เนื่องจากความร้อนมีผลให้สถานะคิวบิต เช่น สปิน หรือสถานะเชิงการเคลื่อนที่แปรสภาพไป ในขณะเดียวกัน อะตอมสองอะตอมใดๆ ต้องสามารถถูกทำให้เคลื่อนที่เข้าใกล้กันเพื่อให้เกิดอันตรกิริยาสำหรับเกตลอจิกสองคิวบิตได้ การควบคุมสถานะและการบังคับให้อะตอมเดี่ยวเคลื่อนที่โดยคงคุณสมบัติอาพันธ์ระหว่างทาง (Coherent movement & coherent control) [*Mandel และคณะ 2003*] มีงานวิจัยโดยกลุ่มวิจัยแห่งมหาวิทยาลัยบอนน์ (University of Bonn) ประเทศเยอรมนี แสดงผลการจัดเรียงอะตอมในโครงสร้างแลททิซเชิงแสงให้เป็นระเบียบได้ [*Morsch 2008*] การทำงานของเกตลอจิกเชิงควอนตัม แบ่งได้เป็นสองรูปแบบ คือ

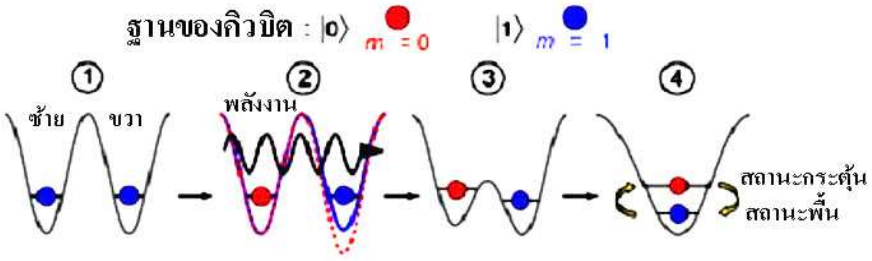
- เกตลอจิกสำหรับหนึ่งคิวบิต (Single-qubit gates)

  การหมุนเวกเตอร์ของหนึ่งคิวบิต (Single-qubit rotation) หรือเกตลอจิกสำหรับหนึ่งคิวบิตทำงานด้วยหลักการเดียวกันกับวิธีที่ใช้การสั่นพ้องแม่เหล็กนิวเคลียร์ และการวิเคราะห์สเปกตรัมด้วยเลเซอร์ (ดูเรื่องการคำนวณเชิงควอนตัมด้วยการสั่นพ้องแม่เหล็กนิวเคลียร์ในหัวข้อต่อไป)

- เกตลอจิกสำหรับสองคิวบิต (Two-qubit gates)

  เนื่องจากอะตอมในโครงสร้างแลททิซเชิงแสงอยู่ติดกันมากจึงสามารถควบคุมให้มีการชนกันแบบยืดหยุ่น (Elastic controlled collisions) เพื่อให้เกิดการทำงานของเกตลอจิกสองคิวบิตระหว่างสองอะตอมที่อยู่ติดกัน อย่างไรก็ตาม การชนนั้นจะอนุรักษ์โมเมนต์แม่เหล็กสำหรับอะตอมทั้งหมดในโครงสร้าง แต่ไม่ได้อนุรักษ์โมเมนต์แม่เหล็กของสองอะตอมที่อยู่ติดกัน จึงอาจมีการถ่ายเทโมเมนตัมไปสู่อะตอม (คิวบิต) อื่นๆ ที่ไม่ต้องการซึ่งเกิดเป็นความผิดพลาดของเกตลอจิก จึงมีเทคนิคการเลือกแทนสถานะของอะตอมที่เหมาะสม เพื่อให้การชนเกิดการอนุรักษ์ของตัวแปรที่เลือก เมื่อมีการชนระหว่างสองอะตอม [*Jaksch และคณะ 1999*]

กรณีที่ใช้สถานะเชิงการเคลื่อนที่ของอะตอม (Motional qubit states) ซึ่งแบ่งเป็นสถานะของการสั่นสองระดับคือ สถานะพื้น (“0”) และสถานะกระตุ้น (“1”) สองอะตอมที่ติดกันจะถูกทำให้มีอันตรกิริยากันได้โดยการลดกำแพงศักย์ (Potential barrier) ที่กั้นระหว่างสองอะตอม และเมื่ออะตอมยุบลงอยู่แลททิซเดียวกันจะเกิดอันตรกิริยาแบบแลกเปลี่ยน (Exchange interaction) ระหว่างกัน ผลลัพธ์ทำให้ได้เกต SWAP คือการสลับค่าระหว่างคิวบิตที่หนึ่งและคิวบิตที่สอง และครึ่งวัฏจักรของเกต SWAP หรือร่วมกับเกตลอจิกหนึ่งคิวบิต สามารถทำหน้าที่คำนวณเชิงควอนตัมทุกรูปแบบได้ ซึ่งการทำงานดังกล่าวแสดงดังรูปที่ 5.20



รูปที่ 5.20 การลดระดับพลังงานที่กั้นระหว่างสองแลททิซโดยการกระตุ้นด้วยคลื่น

5.2.3.5 การอ่านค่าออก

การอ่านค่าของอนุภาคที่อยู่ในแลททิซเชิงแสงทำได้โดยอาศัยหลักการเดียวกับการอ่านค่าออกของไอออนที่ถูกกัก นั่นคือการยิงด้วยชุดของพัลส์รามาน (Raman pulse) เพื่อกระตุ้นให้อนุภาคที่ต้องการอ่านค่ามีการแยกของระดับพลังงานอยู่ในสถานะที่ละเอียดมาก จากนั้นจึงวัดค่าพลังงานที่อนุภาคที่ถูกยิงรังสีปล่อยออกมาก็จะสามารถระบุได้ว่าอนุภาคนั้นอยู่ในสถานะของคิวบิต “0” หรือ “1” [*Brennen และคณะ 2008*]

การอ่านค่าของอนุภาคแต่ละอนุภาคมีปัญหาอีกประการหนึ่งคือเรื่องความแม่นยำ เนื่องจากอนุภาคมักจะอยู่ชิดกันมาก ซึ่งระยะห่างนี้บางครั้งน้อยกว่าความยาวคลื่นของแสงทำให้การอ่านค่าทำได้ยากและไม่แม่นยำ ทางแก้หนึ่งคือการกักอนุภาคโดยใช้สนามแม่เหล็กและการแยกออกของเส้นสเปกตรัมของอะตอมเมื่อใส่สนามไฟฟ้าจากภายนอกแทน อีกวิธีที่มีการนำเสนอคือการออกแบบให้บ่อศักย์ที่ใช้กักอนุภาคมีระยะห่างระหว่างกันมากขึ้น ซึ่งสามารถทำได้โดยการใช้การซ้อนทับกันของคลื่นที่เกิดจากเลเซอร์ที่มีความยาวคลื่นยาวมากๆ จากหลายทิศทาง

5.2.3.6 ความคืบหน้างานวิจัย

ในปี ค.ศ. 2000 รอน โฟลมาน (Ron Folman) และคณะวิจัยที่มหาวิทยาลัยอินส์บรูค (University of Innsbruck) ประเทศออสเตรีย นำเสนอผลการทดลองกักและควบคุมอะตอมที่เป็นกลางด้วยสนามแม่เหล็กบนชิปสารกึ่งตัวนำที่สร้างจากทองคำและแกลเลียมอาร์เซไนด์ (GaAs) [*Folman และคณะ 2000*]

ในปี ค.ศ. 2007 คาร์ล เนลสัน (Karl Nelson) และคณะวิจัยที่มหาวิทยาลัยเพนซิลวาเนีย (University of Pennsylvania) ประเทศสหรัฐอเมริกา สาธิตการถ่ายภาพอะตอมที่ถูกกักในโครงสร้างแลททิซเชิงแสง 3 มิติ ซึ่งสามารถถ่ายภาพอะตอมทั้งหมด 250 อะตอมในแลททิซได้ (ซึ่งก่อนหน้าที่มีรายงานวิจัยการถ่ายภาพสถานะอะตอมเพียงไม่ถึง 10 อะตอม) และภาพถ่ายแสดงถึงระยะเวลาคงความอาพันธ์ที่นานในระดับหลายวินาที ซึ่งการถ่ายภาพอะตอมจำนวนมากได้นี้เป็นการปูทางไปสู่การเปลี่ยนสถานะและวัดสถานะสำหรับการคำนวณเชิงควอนตัมด้วยอะตอมที่เป็นกลางซึ่งมีคิวบิตเป็นจำนวนมากต่อไป [*Nelson และคณะ 2007*]

ในปี ค.ศ. 2009 มาร์ค ไรเซน (Mark Reizen) และคณะวิจัยที่มหาวิทยาลัยเทกซัส ออสติน (The University of Texas at Austin) ประเทศสหรัฐอเมริกา รายงานผลการทดลองเตรียมสถานะคิวบิตของอะตอมลิเทียมด้วยความถูกต้องถึง 0.99998 ซึ่งเป็นการแก้ปัญหาความคลาดเคลื่อนในการกำหนดสถานะเริ่มต้นแก่คิวบิตในการคำนวณเชิงควอนตัมได้ [*Raizen และคณะ 2009*]

ในปี ค.ศ. 2009 ปีเตอร์ เวิร์ทซ์ (Peter Würtz) และคณะวิจัยที่ประเทศเยอรมนี นำเสนอผลการทดลองการเข้าถึงสถานะคิวบิตในแลททิซเชิงแสงซึ่งมีระยะห่างระหว่างแลททิซ 600 นาโนเมตร โดยเข้าถึงสถานะด้วยกล้องจุลทรรศน์อิเล็กตรอนแบบส่องกราด (Scanning Electron Microscope: SEM) พร้อมทั้งแสดงการจัดเรียงอะตอมให้เป็นรูปสมการชเรอดิงเงอร์ (Schrodinger's equation: $H\psi = E\psi$) [*Wurtz และคณะ 2009*] และในปีเดียวกันคณะวิจัยซึ่งร่วมมือระหว่างประเทศเยอรมนี ออสเตรีย และสหราชอาณาจักร สามารถบรรจุอะตอมอุณภูมิปกติซึ่งทำให้เย็นและกักบริเวณในโครงสร้างแลททิซเชิงแสงบนชิปได้ [*Gallego และคณะ 2009*]

5.2.3.7 สรุปการคำนวณเชิงควอนตัมด้วยอะตอมที่เป็นกลาง

ข้อดีของการใช้สถานะของอะตอมซึ่งไม่มีประจุแทนคิวบิต คือ ไม่ถูกแรงทางไฟฟ้ากระทำโดยตรงจึงมีการสูญเสียคุณสมบัติเนื่องจากสิ่งแวดล้อมได้น้อยกว่า (มีระยะเวลาคงสภาพความอาพันธ์นาน) แต่ยังไม่มีการคำนวณแน่ชัดว่าระยะเวลาคงสภาพความอาพันธ์ที่ได้มีค่าเป็นเท่าใด [*Heinrich 2004*] นอกจากนั้นยังมีการนำเสนอว่าการใช้อะตอมที่เป็นกลางในแลททิซเชิงแสงมีความเหมาะสมกับการคำนวณเชิงควอนตัมแบบทางเดียว [*Bloch 2008; Briegel และคณะ 2009*]

5.2.4 การคำนวณเชิงควอนตัมด้วยนิวเคลียร์แมกเนติกเรโซแนนซ์

การเหนี่ยวนำของสนามแม่เหล็กต่อสถานะสปินของนิวเคลียสได้รับการสังเกตตั้งแต่ปี ค.ศ. 1946 โดยกลุ่มวิจัยของเอ็ดเวิร์ด เพอร์เซลล์ (Edward Purcell) และ ฟีลิกซ์ บลอค (Felix Bloch) [*Laflamme และคณะ 2002*] ทำให้ทั้งสองได้รับรางวัลโนเบลสาขาฟิสิกส์ประจำปี ค.ศ. 1952 การค้นพบดังกล่าวนำไปสู่การวิเคราะห์โครงสร้างของโมเลกุล และการศึกษาการเปลี่ยนแปลงของของแข็งและของเหลว รวมถึงการถ่ายภาพทางการแพทย์โดยการสร้างภาพด้วยเรโซแนนซ์แม่เหล็ก (Magnetic Resonance Imaging: MRI) [*Ernst และคณะ 1994*] ภายหลังพบว่าสามารถนำมาประยุกต์งานคำนวณเชิงควอนตัมได้ [*Jones 2001*]

ในกระบวนการสั่นพ้องแม่เหล็กนิวเคลียร์ของเหลวหรือของแข็งซึ่งประกอบด้วยโมเลกุลของสิ่งที่ต้องการศึกษาจะถูกป้อนด้วยสนามแม่เหล็กความเข้มสูง ทำให้มีการแยกของระดับพลังงานอันเนื่องจากสปินของอนุภาค หลังจากนั้นมีการกระตุ้นด้วยคลื่นแม่เหล็กไฟฟ้าความถี่สั่นพ้อง (Resonance frequency หรือ radio frequency: RF[5.8]) ซึ่งทำให้สปินของอนุภาคที่สนใจดูดกลืนพลังงานคลื่นแม่เหล็กไฟฟ้าในความถี่ที่เหมาะสมและเบนออกจากแนวเดิม จากอนุภาคจะปล่อยคลื่นแม่เหล็กไฟฟ้าออกม พร้อมๆ กับการที่สปินคืนสภาพสู่สถานะเดิม จากการวัดสเปกตรัมของคลื่นที่ปล่อยออกมา และระยะเวลาที่ใช้ในการคืนสภาพ (Relaxation time) จะทราบสถานะและปริมาณของโมเลกุลที่อยู่ในวัตถุนั้นว่ามีมากน้อยเพียงใด และในการใช้การสั่นพ้องแม่เหล็กนิวเคลียร์ในการคำนวณเชิงควอนตัม เกตลอจิกเชิงควอนตัมรูปแบบต่างๆ จะทำงานโดยการกระตุ้นอนุภาคด้วยคลื่นแม่เหล็กไฟฟ้าในทิศทางและความถี่ที่เหมาะสมหลายๆ ชุดเพื่อให้ได้ผลลัพธ์เป็นตัวดำเนินการลอจิกเชิงควอนตัมที่ต้องการ ในที่นี้จะพิจารณาตามเงื่อนไขห้าข้อของดิวินเซนโซ ว่าเหตุใดนิวเคลียร์แมกเนติกเรโซแนนซ์จึงเหมาะสมสำหรับงาน คำนวณเชิงควอนตัม เป็นลำดับดังต่อไปนี้ (1) การแทนคิวบิต (2) การเตรียมสถานะเริ่ม (3) การคงสภาพคุณสมบัติควอนตัม (4) การทำงานของเกตลอจิกเชิงควอนตัม และ (5) การอ่านค่าออก รวมทั้งเพิ่มเติมเรื่อง (6) การควบคุม และ (7) การคำนวณเชิงควอนตัมด้วยการสั่นพ้องแม่เหล็กนิวเคลียร์ในของแข็ง[5.9]

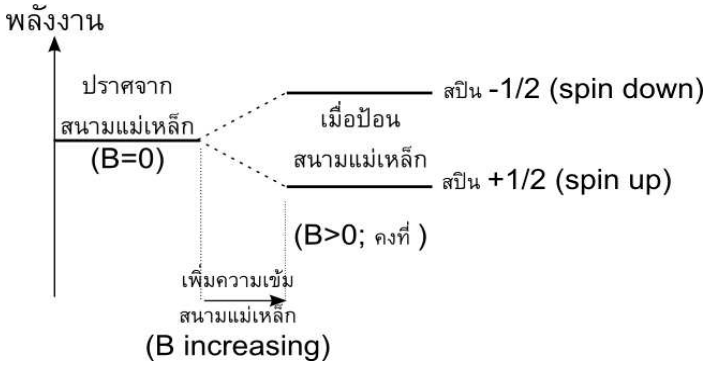
5.2.4.1 การแทนคิวบิต

คิวบิตในการคำนวณเชิงควอนตัมด้วยการสั่นพ้องแม่เหล็กนิวเคลียร์แทนด้วยสถานะสปิน 1/2 ของนิวเคลียสซึ่งเมื่ออยู่ในสนามแม่เหล็ก $\vec{B}$ จะมีพลังงาน $-\vec{\mu}\cdot\vec{B}$ โดยที่โมเมนต์แม่เหล็ก (Magnetic moment) $\vec{\mu}=\mu_N\vec{I}$ เมื่อ $\vec{I}$ เป็นสปินเวกเตอร์ซึ่งมีได้สองค่าคือ $|\uparrow\rangle$ และ $|\downarrow\rangle$ และค่าแมกเนตอนของบอห์ร (Bohr's magnetron) μ_N มีค่าประมาณ 5.1×10^{-27} A/m^2) เนื่องจากสถานะสปิน 1/2 ลักษณะนี้สามารถแทนได้ในทรงกลมบล็อช จึงมีคุณสมบัติเหมือนหนึ่งคิวบิตทุกประการ อนุภาคที่มีสปินทิศเดียวกับสนามแม่เหล็กจะมีพลังงานต่ำกว่าอนุภาคที่มีสปินในทิศตรงข้าม โดยปรากฏการณ์แยกระดับของพลังงานของอนุภาคที่มีสปินเมื่ออยู่ในสนามแม่เหล็กเรียกว่าปรากฏการณ์ของซีมาน (Zeeman effect) ดังรูปที่ 5.21 โดยจำนวนระดับพลังงานที่แยกออกเมื่อถูกป้อนสนามแม่เหล็ก มีจำนวนเท่ากับ $2I+1$ ระดับ โดยที่ I เป็นค่าคุณสมบัติสปินของอนุภาคนั้น เช่น อนุภาคสปิน 1/2 มี $2\times(1/2)+1$ เท่ากับ 2 ระดับพลังงาน และอนุภาคสปิน 1 มีทั้งหมด $2\times1+1$ เท่ากับ สามระดับ และอนุภาคสปินศูนย์ มีหนึ่งระดับพลังงาน

อะตอมบางชนิดที่มีจำนวนโปรตอนและนิวตรอนเท่ากัน จะมีสปินรวมของนิวเคลียส (Nuclear spin) เป็นศูนย์ (เนื่องจากการหักล้างกันระหว่างสปินของนิวตรอนและโปรตอน) เช่น คาร์บอน-12 (^{12}C) ออกซิเจน-16 (^{16}O) และ ซัลเฟอร์-32 (^{32}S) เป็นต้น

5.8 เนื่องจากความถี่ที่ใช้อยู่ในระดับเมกะเฮิรตซ์

5.9 เนื้อหาเพิ่มเติมที่ใกล้เคียงศึกษาได้จาก [Everitt 2005]



รูปที่ 5.21 การแยกชั้นของพลังงานอันเนื่องจากอันตรกิริยาระหว่างสปิน และสนามแม่เหล็ก รูปปรับปรุงจาก [*Chen และคณะ 2007*]

ตารางที่ 5.2 ความถี่เรโซแนนซ์ที่แตกต่างกันในอะตอมชนิดต่างๆ ในกรณีสนามแม่เหล็กมีความเข้มเท่ากับ 11.75 เทสลาร์ [*Everitt 2005*]

ชนิดอะตอม	^{1}H	^{19}F	^{31}P	^{13}C	^{29}Si	^{15}N
ความถี่เรโซแนนซ์ (ความถี่วิทยุ)	500 MHz	470 MHz	202 MHz	125 MHz	99 MHz	50 MHz

คุณลักษณะของนิวเคลียสและสปินของนิวเคลียสสามารถแยกได้เป็น 3 กรณี ดังนี้ [*Chen และคณะ 2007*]

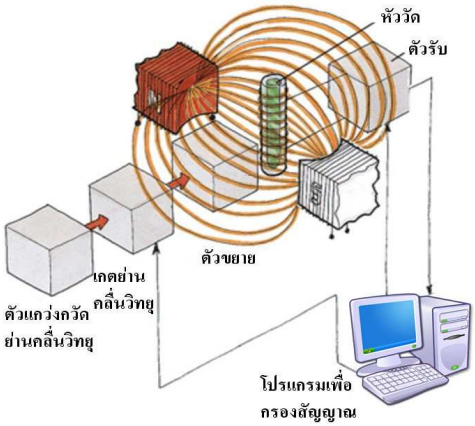
- จำนวนนิวตรอนและโปรตอนมีเท่ากัน และเป็นจำนวนคู่ กรณีนี้นิวเคลียสมีสปินเป็นศูนย์
- จำนวนนิวตรอนและโปรตอนมีจำนวนรวมกันเป็นจำนวนคี่ กรณีนี้สปินของนิวเคลียสมีค่าเป็นเศษส่วนสอง ได้แก่สปิน 1/2 3/2 5/2 เป็นต้น
- จำนวนนิวตรอนและโปรตอนมีเท่ากันและเป็นจำนวนคู่ กรณีนี้สปินของนิวเคลียสมีค่าเป็นจำนวนเต็มบวก 1 2 3 เป็นต้น เช่น ไนโตรเจน-14 มีจำนวนนิวตรอนและโปรตอนเท่ากับเจ็ดทั้งคู่ (^{14}N) มีค่าสปินของนิวเคลียสเท่ากับ 1

สถานะสปินของนิวเคลียสที่ถูกนำมาใช้งานในการคำนวณเชิงควอนตัมด้วยนิวเคลียร์แมกเนติกเรโซแนนซ์ โดยทั่วไปเป็นนิวเคลียสที่มีสปิน *1/2*[5.9] ในไอโซโทปเฉพาะเจาะจง เช่น ไฮโดรเจน-1 (^{1}H) ฟลูออรีน-19 (^{19}F) ฟอสฟอรัส-31 (^{31}P) คาร์บอน-13 (^{13}C) ซิลิกอน-29 (^{29}Si) และไนโตรเจน-15 (^{15}N) ในการสั่นพ้องแม่เหล็กนิวเคลียร์ของสถานะของเหลว อะตอมแต่ละชนิดจะเป็นส่วนหนึ่งของโมเลกุลในสารละลาย ซึ่งสถานะของแต่ละคิวบิตจะถูก “ประมาณ” ด้วยโมเลกุล (ที่เป็นอิสระต่อกัน) ลักษณะซ้ำกันเป็นจำนวนถึงประมาณ 10^{18} โมเลกุล โดยแต่ละโมเลกุลเป็นระบบที่ประกอบด้วย N สปิน (N คิวบิต)

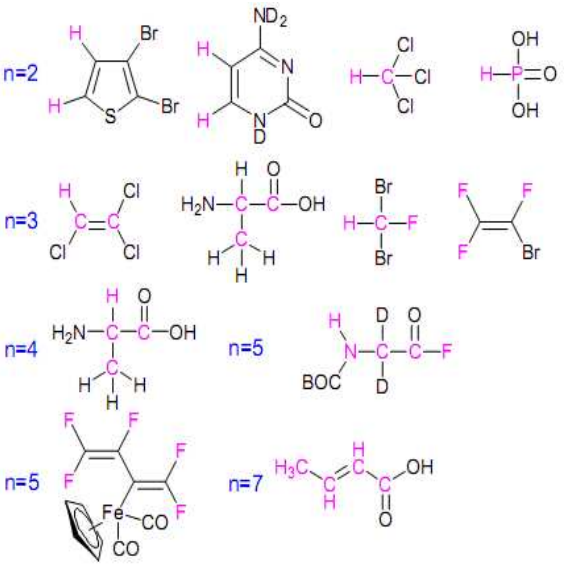
5.2.4.2 การจัดอุปกรณ์การสั่นพ้องแม่เหล็กนิวเคลียร์

การจัดอุปกรณ์ทดลองการสั่นพ้องแม่เหล็กนิวเคลียร์ ประกอบด้วยสองส่วนหลักๆ ได้แก่ ส่วนแรกคือสารละลายหรือตัวอย่าง (Sample หรือ probe) ซึ่งบรรจุอนุภาคที่มีสปินไม่เป็นศูนย์ ซึ่งจะทำหน้าที่แทนคิวบิตสำหรับการคำนวณ และส่วนที่สองคือชุดอุปกรณ์ทั้งหมดที่เหลือ รวมเรียกว่าชุดแยกเสปกตรัมด้วยเอ็นเอ็มอาร์ (NMR spectrometer) โดยมีการสร้างสนามแม่เหล็ก

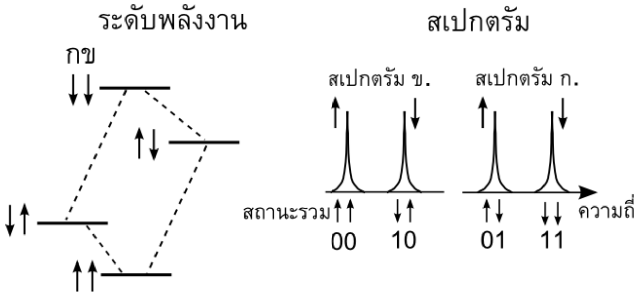
[5.9] กรณีสปิน 3/2 และ 5/2 ซึ่งแต่ละอนุภาคมีสปินได้มากกว่าสองค่า ได้มีการศึกษาและทดลองเช่นกัน (มิได้พิจารณาในที่นี้)



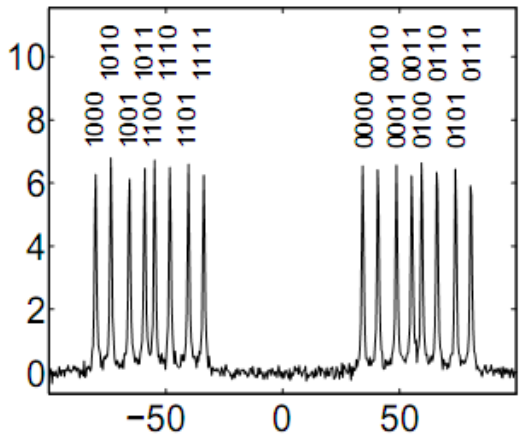
รูปที่ 5.22 การจัดอุปกรณ์การสั่นพ้องแม่เหล็กนิวเคลียร์ โดยบรรจุโมเลกุลที่จะทำการทดสอบหรือการคำนวณเชิงควอนตัมในหัววัดและส่วนที่เหลือทั้งหมดรวมเรียกว่าชุดแยกเสปกตรัมด้วยเอ็นเอ็มอาร์ ประกอบด้วย แหล่งกำเนิดสนามแม่เหล็กความเข้มสูง (N-S) และหน่วยสร้างและรับพัลส์แม่เหล็กความถี่คลื่นวิทยุ ควบคุมด้วยอุปกรณ์อิเล็กทรอนิกส์ รูปดัดแปลงจาก [*HiQ.NET*]



(ก)



(ข)



(ค)

รูปที่ 5.23 (ก) การเลือกชนิดของโมเลกุลสำหรับการคำนวณเชิงควอนตัมในจำนวนคิวบิต (*n*) ต่างๆ โดยใช้นิวเคลียสของอะตอม รูปดัดแปลงจาก [*Jones 2001*] (ข) กรณีสองคิวบิตแทนด้วยสถานะของสองสปิน และการแยกแยะแต่ละสถานะด้วยสเปกตรัม รูปดัดแปลงจาก [*Stolze & Suter 2004*] (ค) สเปกตรัมของสถานะสปินสี่คิวบิต รูปดัดแปลงจาก [*Vandersypen และคณะ 2000*]

ความเข้มสูงและคงที่ ซึ่งทำจากขดลวดแม่เหล็กตัวนำยิ่งยวด (Superconducting magnet) เพื่อให้เกิดการแยกของสเปกตรัมของสถานะสปินที่ต่างกัน และมีขดลวดเพื่อสร้างคลื่นแม่เหล็กไฟฟ้าความถี่สั่นพ้องหรือความถี่วิทยุ และขดลวดเพื่อรับคลื่นแม่เหล็กไฟฟ้าซึ่งตอบสนองกลับมา ขดลวดทั้งคู่ถูกจัดวางในระนาบตั้งฉากกับแนวสนามแม่เหล็กความเข้มสูง ดังรูปที่ 5.22 จากการจัดอุปกรณ์ดังกล่าวสามารถควบคุมการกำหนดและอ่านค่าของสถานะแต่ละคิวบิตด้วยความถี่สั่นพ้องของอะตอมที่ประกอบขึ้นเป็นโมเลกุลต่างๆ โดยค่าความถี่ที่ใช้สำหรับการกำหนดค่าคิวบิตมีรายละเอียดดังตารางที่ 5.2 และชนิดของโมเลกุลสำหรับการคำนวณเชิงควอนตัมจะเลือกใช้โมเลกุลที่เหมาะสมดังรูปที่ 5.23

5.2.4.3 การเตรียมสถานะเริ่มต้น

ความถี่คลื่นวิทยุของนิวเคลียสที่นำมาใช้ในการสั่นพ้องแม่เหล็กนิวเคลียร์ มีขนาดพลังงานน้อยมาก (ความถี่ระดับเมกะเฮิรตซ์) เมื่อเทียบกับพลังงานการสั่นอันเนื่องจากอุณหภูมิห้อง (Thermal fluctuations) ซึ่งมีค่าประมาณ 6 เทระเฮิรตซ์ [*Everitt 2005*] ดังนั้นที่อุณหภูมิห้องสถานะของนิวเคลียสจะเป็นแบบสุ่มสูง ซึ่งอยู่ในรูปสถานะผสม (แทนด้วยเมทริกส์สถานะ ρ) ระหว่างสปินทิศขึ้น และสปินทิศลง ด้วยความน่าจะเป็นเท่ากัน $\rho = \frac{1}{2}|\uparrow\rangle\langle\uparrow| + \frac{1}{2}|\downarrow\rangle\langle\downarrow|$ ซึ่งสถานะผสมนี้เหมือนไม่เหมาะสมสำหรับงานคำนวณเชิงควอนตัมเนื่องจากเป็นสถานะที่ไม่อยู่ในรูปการทับซ้อนเชิงอาพันธ์ (Coherent superposition) ระหว่างสองสถานะ (เพราะไม่มีเทอมเฟสสัมพัทธ์) แต่มีเทคนิคสำหรับการคำนวณเชิงควอนตัมด้วยสถานะดังกล่าว [*Gershenfeld & Chuang 1997*] ซึ่งจะอ่านผลลัพธ์ของสถานะโดยการเฉลี่ยจากสถานะทั้งหมด วิธีการนี้มีข้อเสียคือ สัญญาณผลลัพธ์จะลดลงเป็นเอกซ์โพเนนเชียลตามจำนวนคิวบิตที่เพิ่มขึ้นทำให้ขยายจำนวนคิวบิตในการคำนวณได้ยาก [*Warren 1997*]

5.2.4.4 ระยะเวลาคงสภาพความอาพันธ์

สปินของนิวเคลียสถูกเหนี่ยวนำจากสิ่งแวดล้อมน้อยมาก เนื่องจากแทบจะไม่ถูกกระทำด้วยแรงไฟฟ้าและแม่เหล็ก รวมถึงพลังงานการสั่นจากภายนอก โดยมีระยะเวลาคงความอาพันธ์ (T_d) นานมาก (ตั้งแต่ 10 มิลลิวินาที ถึง 10^8 วินาที) ในขณะที่เวลาในการทำงานของเกตลอจิก $T_{op} = 10^{-3}$ ถึง 10^6 วินาที จำนวนลอจิกเกตที่ทำงานได้ $n_{op} = T_d/T_{op} = 10^5$ ถึง 10^{14} เกต

5.2.4.5 การทำงานของเกตลอจิกเชิงควอนตัม

เกตลอจิกเชิงควอนตัมของการสั่นพ้องแม่เหล็กนิวเคลียร์จะใช้คลื่นวิทยุที่มีความถี่เหมาะสม และมีลักษณะเป็นช่วงๆ (RF pulse) เพื่อเปลี่ยนสถานะของการสปินของอะตอมที่ต้องการ [*Price และคณะ 1999*] สถานะเริ่มต้นจะอยู่ในลักษณะที่อนุภาคทุกอนุภาคที่ถูกควบคุมอยู่จะมีคุณสมบัติของสปินเหมือนกันทุกประการเมื่อมองจากโดเมนเชิงความถี่ (Frequency domain) จากนั้นจะใช้ความถี่ที่เหมาะสมต่อการจัดการเกตลอจิกนั้นจะต้องเป็นความถี่ที่สั่นพ้องกับลักษณะของอนุภาคนั้น [*Chuang และคณะ 1998*]

5.2.4.6 การอ่านค่าออก

การอ่านค่าออกทำได้โดยใช้คลื่นแม่เหล็กไฟฟ้าที่มีความถี่เหมาะสมยิงไปที่อนุภาคที่เป็นเป้าหมาย การยิงคลื่นเหล่านี้จะทำให้อนุภาคเปลี่ยนลักษณะการสปินไป การเปลี่ยนการสปินนี้จะทำให้อนุภาคมีการรับหรือคายพลังงานออกมา ซึ่งหากผู้รับตั้งเครื่องมือตรวจหาอย่างเหมาะสมแล้ว จะสามารถตรวจวัดสเปกตรัมเหล่านี้ได้ เนื่องจากคิวบิต "1" กับคิวบิต "0" มีการรับและคายสเปกตรัมคนละเส้นกัน [*Vandeersypen และคณะ 2002*]

5.2.4.7 การควบคุม

สิ่งหนึ่งที่การสั่นพ้องแม่เหล็กนิวเคลียร์แตกต่างจากควอนตัมคอมพิวเตอร์แบบอื่นๆคือ วิธีนี้ไม่สามารถใช้ควบคุมอนุภาคเดี่ยวๆได้ แต่ทุกๆอนุภาคที่ในระบบจะถูกควบคุมพร้อมๆกัน นอกจากนี้ยังมีข้อควรระวังอีกประการหนึ่งคือ การอ่านค่าสถานะจะรบกวนระบบทิศโดยเฉลี่ยของสนามแม่เหล็กของระบบ [*Schack & Caves 2008*]

5.2.4.8 สรุปการคำนวณเชิงควอนตัมด้วยการสั่นพ้องแม่เหล็กนิวเคลียร์

การคำนวณเชิงควอนตัมด้วยการสั่นพ้องแม่เหล็กนิวเคลียร์เป็นการใช้โครงสร้างในสเกลใหญ่ที่ประพฤติตัวแบบควอนตัม เช่น สถานะสปินของโมเลกุลในของเหลว (จำนวนโมเลกุลโครงสร้างเดียวกันมีปริมาณมาก) ซึ่งสถานะของสปินมีความไม่ต่อเนื่อง

และสามารถนำมาแทนข้อมูลควอนตัม (คิวบิต)ได้ การสั่นพ้องแม่เหล็กนิวเคลียร์ที่มีการเสนอให้ใช้ในงานคำนวณเชิงควอนตัมมีทั้งในสถานะของแข็ง (ใช้ซิลิกอน ^{29}Si และ ^{28}Si) [*Kane 1998; Ladd และคณะ 2002*] และในสถานะของเหลว [*Jones 2001*] *ข้อเสีย*ของการใช้การสั่นพ้องแม่เหล็กนิวเคลียร์ในสถานะของเหลวทำการคำนวณเชิงควอนตัม คือขาดคุณสมบัติการเพิ่มปริมาณ (Scalability) คิวบิต หากต้องการเพิ่มปริมาณคิวบิต ต้องเลือกชนิดของโมเลกุลให้มีโครงสร้างใหญ่ขึ้นและมีคุณสมบัติเฉพาะตรงตามต้องการ จึงทำให้อุปกรณ์คำนวณเชิงควอนตัมที่อาศัยการสั่นพ้องแม่เหล็กนิวเคลียร์ไม่เหมาะสมในการพัฒนาไปถึงระดับอุตสาหกรรม [*Morsch 2008*]

5.2.5 การคำนวณเชิงควอนตัมด้วยควอนตัมดอท (Quantum dot)

ควอนตัมดอท หมายถึง โครงสร้างของสารกึ่งตัวนำที่สามารถกักบริเวณอิเล็กตรอนให้อยู่ในพื้นที่จำกัดบนปรภูมิสามมิติได้ ซึ่งขนาดของบริเวณนั้นอยู่ในระดับไมโครเมตรถึงนาโนเมตร บริเวณดังกล่าว (เรียกว่า “dot” หรือจุด) พลังงานของอิเล็กตรอนจะมีค่าไม่ต่อเนื่อง ควอนตัมดอทสามารถพิจารณาได้เป็น 'อะตอมเสมือน' (Artificial atoms) [*Le Bellac 2006*] ซึ่งคุณสมบัติของอะตอมเสมือนนี้สามารถถูกควบคุมได้โดยผู้ทดลอง และตัวนำประจุในบริเวณแถบการนำ (Conduction band) ของควอนตัมดอทสามารถถูกควบคุมได้อย่างแม่นยำ โครงสร้างสารกึ่งตัวนำที่ประกอบขึ้นเป็นควอนตัมดอทพิจารณาได้ดังรูปที่ 5.24 5.25 และ 5.26 การใช้ควอนตัมดอทในงานคำนวณเชิงควอนตัมถูกเสนอครั้งแรกในปี ค.ศ. 1998 โดยแดเนียล ลอสส์ (Daniel Loss) และเดวิด ดิวินเชนโซ (David DiVincenzo) ซึ่งเสนอให้ใช้สถานะสปินของอิเล็กตรอนในโครงสร้างควอนตัมดอทสำหรับแทนคิวบิตในการคำนวณ [*Loss & DiVincenzo 1998*]

5.2.5.1 การแทนคิวบิตในควอนตัมดอท

ควอนตัมดอทมีลักษณะเหมือนถาดหลุมใส่อาหารทรงกระบอก เส้นผ่านศูนย์กลางประมาณ 100 นาโนเมตร สูงประมาณ 300 นาโนเมตร โดยคุณสมบัติทางกายภาพในควอนตัมดอทที่ทำหน้าที่แทนสถานะคิวบิตได้ แบ่งเป็นสองรูปแบบหลักๆ ดังนี้

- ใช้เอ็กซิตอน (Exciton)

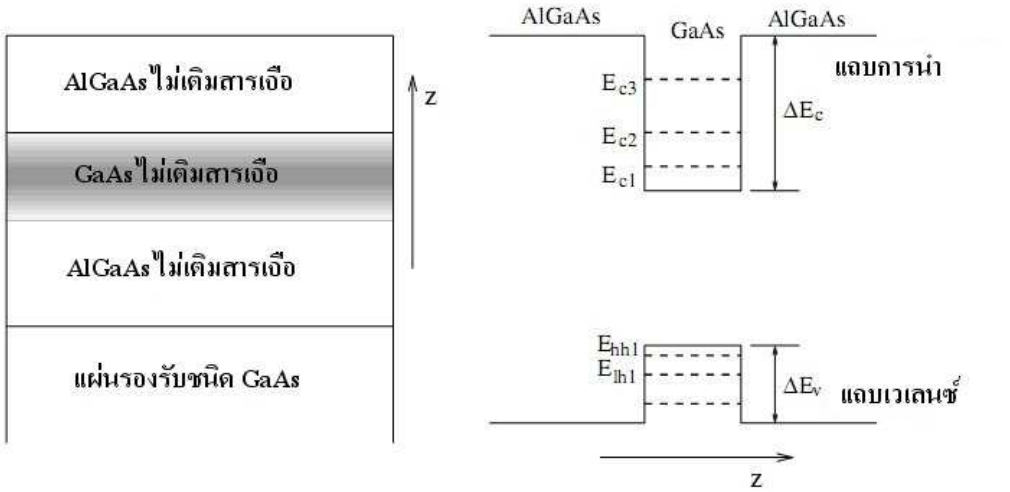
เอ็กซิตอน หรือคู่ของอิเล็กตรอนและโฮล ซึ่งเกิดจากการที่อิเล็กตรอนดูดกลืนแสงแล้วเปลี่ยนระดับพลังงาน โดยพลังงานของเอ็กซิตอนมีค่า $E_{ex} = E_g - E_b$ โดยที่ E_g แทนช่วงพลังงานที่ต่างกัน (Band gap) ระหว่างอิเล็กตรอนและโฮล และ E_b แทนพลังงานที่ดึงดูดกัน (Binding energy) ระหว่างอิเล็กตรอนและโฮล

- ใช้สปินของอิเล็กตรอน (Electron spin)

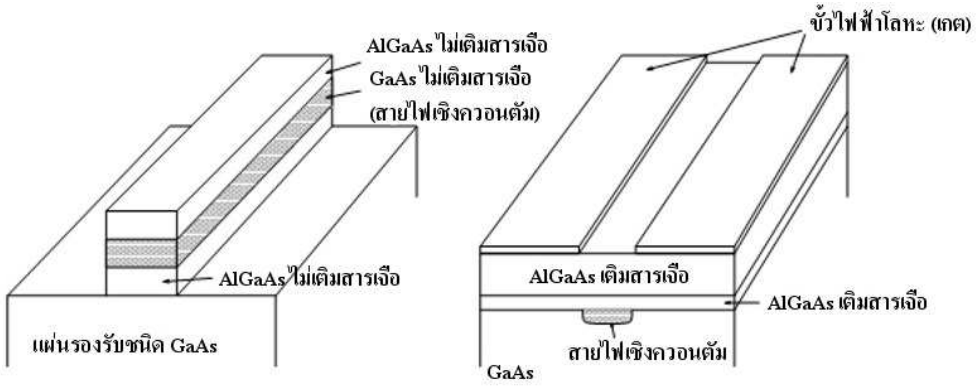
การใช้สปินของอิเล็กตรอนแทนคิวบิตมีข้อดีหลายประการ ได้แก่ (1) เป็นระบบควอนตัมสองสถานะ (2-level quantum system) ซึ่งแทนคิวบิตได้อย่างถูกต้องและไม่มีการขยับไปยังองศาอิสระอื่นที่เหนือไปจากสองสถานะนั้น
(2) สถานะสปินมีอันตรกิริยากับสิ่งแวดล้อมน้อยมาก ทำให้มีระยะเวลาคงความอาพันธ์ได้นานในระดับไมโครวินาที
(3) สถานะสปินของอิเล็กตรอนถูกส่งผ่านไปบนเส้นทางได้ง่าย เนื่องจากสปินของอิเล็กตรอนมีอันตรกิริยากับสนามแม่เหล็ก มากกว่าอันตรกิริยาของสปินนิวเคลียสกับสนามแม่เหล็ก เนื่องจากอันตรกิริยาดังกล่าวแปรผกผันกับมวลของอนุภาค และมวลอิเล็กตรอนเล็กกว่าโปรตอนถึง 10^3 เท่า

5.2.5.2 การทำงานของเกตลอจิกเชิงควอนตัม

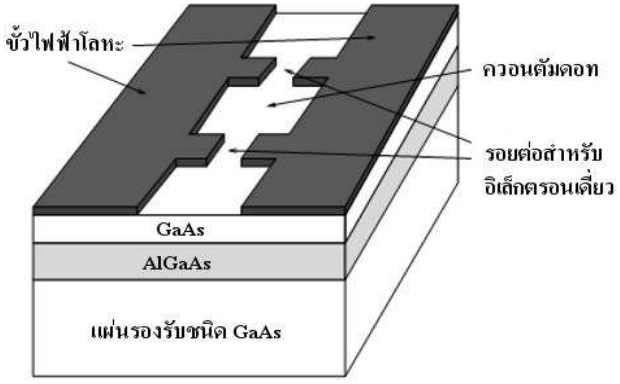
สถานะสปินของอิเล็กตรอนในควอนตัมดอทเตรียมได้โดยการกระตุ้นด้วยแสงที่มีโพลาไรเซชันเชิงวงกลม หรือใช้วิธีฉีดสปิน (Spin injection) จากวัสดุแม่เหล็ก [*Ohno และคณะ 1999; Zhu และคณะ 2001*] กรณีใช้สถานะของเอ็กซิตอนแทนคิวบิต เกตลอจิกสองคิวบิต ทำงานได้โดยใช้ควอนตัมดอทสองดอทซึ่งอยู่ใกล้เคียงกัน ซึ่งถ้าระยะห่างระหว่างสองดอทมีค่าประมาณ 5 นาโนเมตร อิเล็กตรอนและโฮลจะสามารถกระโดดข้ามไปมาระหว่างสองควอนตัมดอทติดกันได้ ซึ่งทำให้เกิดการเปลี่ยนสถานะของสองคิวบิต ดังตารางที่ 5.3 เมื่อ



รูปที่ 5.24 โครงสร้างของควอนตัมดอทในหนึ่งมิติ หรือที่เรียกว่าบ่อศักย์เชิงควอนตัม ซ้ายมือแสดงรูปแบบสารกึ่งตัวนำที่ทำให้เกิดโครงสร้างบ่อศักย์เชิงควอนตัม และขวามือแสดงระดับพลังงานที่ไม่ต่อเนื่องทั้งในแถบเวเลนซ์ (Valance band) และแถบการนำ (Conduction band) รูปดัดแปลงจาก [*Chen และคณะ 2007*]

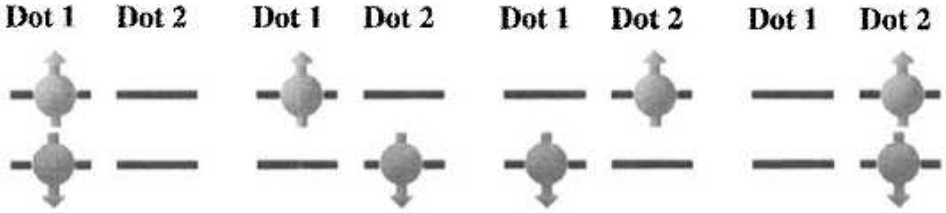


รูปที่ 5.25 โครงสร้างของควอนตัมดอทในสองมิติ หรือเส้นเชิงควอนตัม (Quantum wires) ซึ่งเกิดจากบ่อศักย์ควอนตัมเรียงต่อกันเป็นแนวยาว รูปดัดแปลงจาก [*Chen และคณะ 2007*]



รูปที่ 5.26 โครงสร้างของควอนตัมดอทแบบสามมิติ อิเล็กตรอนถูกกักไว้ในบริเวณจำกัด (บริเวณควอนตัมดอท) โดยศักย์ไฟฟ้าที่ป้อนสู่ขั้วไฟฟ้าทำให้รอยต่อ (Junction) ระหว่างสองดอทแคบลงเพื่อกักอิเล็กตรอนหรือกว้างขึ้นได้ รูปดัดแปลงจาก [*Chen และคณะ 2007*]

ตารางที่ 5.3 การแทนสถานะสองคิวบิตในควอนตัมดอท

สถานะทางกายภาพ				
สถานะเชิงลอจิก	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$

หมายเหตุ: ลูกศรชี้ขึ้นแทนอิเล็กตรอน และลูกศรชี้ลงแทนโฮล ในกรณีสถานะเอ็กซิตอน ส่วนกรณีสถานะสปินของอิเล็กตรอน ลูกศรแทนทิศสปินของอิเล็กตรอนทั้งสอง รูปดัดแปลงจาก [*Stolze & Suter 2004*]

$|00\rangle$ หมายถึง ทั้งอิเล็กตรอนและโฮลอยู่ในดอทที่ 1

$|11\rangle$ หมายถึง ทั้งอิเล็กตรอนและโฮลอยู่ในดอทที่ 2

$|01\rangle$ หมายถึง อิเล็กตรอนอยู่ในดอทที่ 1 และโฮลอยู่ดอทที่ 2

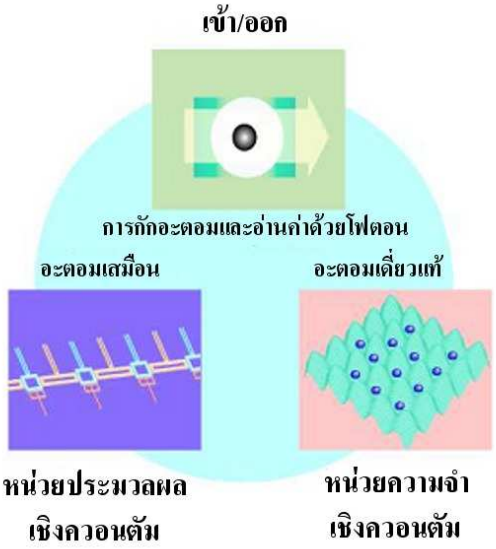
$|10\rangle$ หมายถึง อิเล็กตรอนอยู่ในดอทที่ 2 และโฮลอยู่ดอทที่ 1

ปัญหาสำคัญของการใช้ควอนตัมดอทในงานคำนวณเชิงควอนตัมคือกระบวนการวัดค่า หรืออ่านค่าออก ซึ่งการจะอ่านค่าได้ต้องมีอุปกรณ์สำหรับวัดค่าที่อยู่ใกล้ควอนตัมดอทมากๆ และการที่อุปกรณ์นั้นเข้ามาใกล้มีผลทำให้สถานะควอนตัมของอิเล็กตรอนในนั้นถูกทำลายไป [Morsch 2008]

5.2.5.3 การอ่านค่าออก

การอ่านค่าออก เป็นปัญหาที่สำคัญของการคำนวณเชิงควอนตัมด้วยควอนตัมดอท โดยวิธีการที่ถูกนำเสนอมีดังต่อไปนี้ กรณีการอ่านสถานะสปินของอิเล็กตรอน การอ่านค่าออกทำได้โดยการเปลี่ยนสถานะองศาอิสระเชิงสปิน (Spin degree of freedom) ไปเป็นสถานะองศาอิสระเชิงประจุ (Charge degree of freedom) แล้วตรวจหาสัญญาณไฟฟ้า [*Hanson และคณะ 2005*] หรือวิธีอ่านค่าออกด้วยสัญญาณแสง

ส่วนการอ่านค่าออกในกรณีสถานะคิวบิตของเอ็กซิตอน อิเล็กตรอนและโฮลจะรวมตัวกัน (อิเล็กตรอนปลดปล่อยพลังงานแสงและกลับมาอยู่ตำแหน่งของโฮลเดิม) เมื่อเวลาผ่านไปประมาณ 1 นาโนวินาที ซึ่งความยาวคลื่นของแสงที่ปลดปล่อยออกมาในการรวมตัวของอิเล็กตรอนและโฮลนั้น จะบ่งบอกถึงสถานะของอิเล็กตรอนและโฮลก่อนหน้าจะมีการปลดปล่อยแสง อย่างไรก็ตาม การรวมตัวของอิเล็กตรอนและโฮลทำให้เกิดการสูญเสียข้อมูลแบบย้อนกลับไม่ได้ และถึงแม้จะมีแสงปลดปล่อยออกมา ความน่าจะเป็นที่จะตรวจพบแสงนั้นมีค่าน้อยเนื่องจากทิศทางของโฟตอนที่ถูกปล่อยออกมาเป็นแบบสุ่ม ทำให้การอ่านค่าสถานะด้วยวิธีดังกล่าวขาดประสิทธิภาพ นอกเหนือจากวิธีการตรวจหาโฟตอนที่ปล่อยออกมาขณะอิเล็กตรอนรวมตัวกับโฮล ยังสามารถใช้วิธีการเปลี่ยนสถานะของอิเล็กตรอนที่ถูกกระตุ้นดังกล่าวไปสู่สถานะของตัวนำไฟฟ้าอิสระ (Free carriers) ซึ่งตรวจหาได้ด้วยสัญญาณไฟฟ้า [*Stolze & Suter 2004; Zrenner และคณะ 2002*]



รูปที่ 5.27 ตัวอย่างแบบจำลองการคำนวณเชิงควอนตัมด้วยการผสมผสานระบบควอนตัมหลายระบบ
รูปดัดแปลงจาก [*Bulata และคณะ 2010*]

5.2.6 การคำนวณเชิงควอนตัมแบบผสมผสานหลายระบบ (hybrid quantum computation)

จากการพิจารณาถึงความเหมาะสมของการคำนวณเชิงควอนตัมที่ได้มีการนำเสนอถึงการอาศัยประสิทธิภาพของการคำนวณเชิงควอนตัมในรูปแบบต่างๆ คอมพิวเตอร์เชิงควอนตัมที่เหมาะสมอาจจะอาศัยการคำนวณแบบผสมผสานหลายระบบ [*Bulata และคณะ 2010*] นั่นคือการคำนวณเชิงควอนตัมด้วยอะตอมที่เป็นกลางจะรักษาสภาพความอาพันธ์ได้นานกว่าระบบอื่น จึงเหมาะสมจะทำเป็นหน่วยความจำ การคำนวณเชิงควอนตัมด้วยไอออนที่ถูกกัก หรือด้วยควอนตัมดอทสามารถใช้เป็นหน่วยประมวลผลเชิงควอนตัมได้ และการคำนวณเชิงควอนตัมด้วยไอออนที่ถูกกักสามารถอ่านสถานะได้แม่นยำ สามารถใช้เป็นหน่วยส่งข้อมูลเข้าออกสำหรับคอมพิวเตอร์เชิงควอนตัมได้โดยคอมพิวเตอร์เชิงควอนตัมแบบผสมผสานหลายระบบอาจมีแผนผังดังรูปที่ 5.27

บทสรุป

การคำนวณเชิงควอนตัมเป็นการคำนวณด้วยเครื่องมือที่อาศัยคุณสมบัติทางควอนตัมซึ่งต้องมีการเตรียมอุปกรณ์ที่แตกต่างจากคอมพิวเตอร์ปัจจุบัน โดยเดวิด ดิวินเชนโซ ได้เสนอเงื่อนไขในการคำนวณว่าต้องมี 5 ข้อ เพื่อให้สามารถทำการคำนวณด้วยวิธีทางควอนตัมได้ ต่อมาในภายหลังได้มีการเพิ่มข้อกำหนดเป็น 7 ข้อ ซึ่งเป็นข้อกำหนดที่ท้าทายให้นักวิจัยจากทั่วโลกพัฒนาเครื่องมือที่เหมาะสมสำหรับการคำนวณดังกล่าว โดยระบบการคำนวณที่ได้รับความสนใจคือ การคำนวณเชิงควอนตัมด้วยสถานะของแสง การคำนวณเชิงควอนตัมด้วยไอออนที่ถูกกัก การคำนวณเชิงควอนตัมด้วยอะตอมที่เป็นกลาง การคำนวณเชิงควอนตัมด้วยการสั่นพ้องแม่เหล็กนิวเคลียร์ และการคำนวณเชิงควอนตัมด้วยควอนตัมดอท ซึ่งแต่ละระบบจะมีข้อดีและข้อด้อยแตกต่างกัน สุดท้ายได้มีการเสนอถึงการคำนวณเชิงควอนตัมด้วยวิธีผสมผสานระบบต่างๆ เข้าด้วยกัน โดยอาศัยข้อดีของแต่ละระบบเพื่อให้ได้ประสิทธิภาพสูงสุด ซึ่งยังคงได้รับการพัฒนาต่อไปสู่การเป็นอุปกรณ์เพื่อใช้งานการคำนวณความเร็วสูงได้ในชีวิตจริง

ตารางที่ 5.4 เปรียบเทียบข้อดีและข้อเสียของการใช้ระบบควอนตัมต่าง ๆ ในการคำนวณเชิงควอนตัม

ระบบควอนตัมที่ใช้	ข้อดี	ข้อเสีย
1. โฟตอน	• มีระยะเวลาคงสภาพความอาพันธ์ (coherence time) นาน	• ซับซ้อนในการสร้างเกตลอจิกสองคิวบิต
2. ไอออนที่ถูกกัก	• มีระยะเวลาคงสภาพความอาพันธ์นาน • เปลี่ยนสถานะและอ่านสถานะได้แม่นยำ	• เพิ่มจำนวนคิวบิตได้ยาก เนื่องจากไอออนผลักกันด้วยแรงคูลอมบ์
3. อะตอมที่เป็นกลางซึ่งถูกกัก	• มีระยะเวลาคงสภาพความอาพันธ์นาน • เพิ่มจำนวนคิวบิตได้เป็นจำนวนมาก	• ยากในการเข้าถึงสถานะของอะตอมซึ่งมีโครงสร้างอยู่ติดกันมาก (ระยะห่างประมาณความยาวคลื่นแสง)
4. นิวเคลียร์แมกเนติกเรโซแนนซ์ หรือการสั่นพ้องแม่เหล็กนิวเคลียร์ (liquid-state NMR)	• มีระยะเวลาคงสภาพความอาพันธ์นาน • การปรับเปลี่ยนสถานะและการอ่านสถานะได้รับการพัฒนามาอย่างดีแล้ว	• เพิ่มจำนวนคิวบิตได้ยาก เนื่องจากต้องเลือกโมเลกุลชนิดใหม่ในปริมาณคิวบิตที่มากขึ้น • การขาดคุณสมบัติพัวพันที่สมบูรณ์ระหว่างสถานะผสมของสปินใน NMR
5. ควอนตัมดอท	• มีระยะเวลาคงสภาพความอาพันธ์นาน	• ยากในการอ่านค่าออก (readout)

เอกสารอ้างอิง

[Bloch 2008] I. Bloch, "Quantum coherence and entanglement with ultracold atoms in optical lattices," *Nature*, vol. 453, pp. 1016-1022, 2008.

[Briegel และคณะ 2009] H. Briegel, et al., "Measurement-based quantum computation," *Nature Physics*, vol. 5, no. 1, pp. 19-26, 2009.

[Brennen และคณะ 2008] G.K. Brennen, C. M. Caves, P.S. Jessen, I.H. Deutsch "Quantum Logic Gates in Optical Lattices," *Phys. Rev. Lett*., vol. 82, pp. 1060-1063, 1999.

[Brown และคณะ 2007] K. Brown, et al., "Loading and characterization of a printed-circuit-board atomic ion trap," *Phys. Rev. A*, vol. 75, p. 015401, 2007.

[Bulata และคณะ 2010] I. Buluta, S. Ashhab, and F. Nori, "Natural and artificial atoms for quantum computation," *arXiv.org e-Print archive*, Feb. 2010. [Online]. Available: http://arxiv.org/abs/1002.1871v1. [Accessed: Feb. 2009].

[Chuang และคณะ 1998] I. L. Chuang, M. K. Vandersypen, J. S. Harris, "Bulk Spin Quantum Computation: Toward Large-Scale Quantum Computation," in *ISSCC98,* pp. 96-97, 1998.

[Chen และคณะ 2007] G. Chen, et al., *Quantum Computing Devices: Principles, Designs, and Analysis*. New York: Chapman & Hall/CRC Press, 2007.

[Cirac & Zoller 1995] J. I. Cirac, and P. Zoller, "Quantum Computation with Cold Trapped Ions," *Phys. Rev. Lett.,* vol. 74, no. 20 , pp. 4091-4094, 1995.

[Diedrich และคณะ 1989] F. Diedrich, et al., "Laser cooling to the zero-point energy of motion," *Phys. Rev. Lett.*, vol 64, pp. 403--406, 1989.

[DiVincenzo 1996] D. DiVincenzo, "Topics in Quantum Computers," *arXiv.org e-Print archive*, Dec. 1996. [Online]. Available: http://arxiv.org/abs/cond-mat/9612126v2. [Accessed: Dec. 2009].

[Ernst และคณะ 1994] R. R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*. New York: Oxford University Press, 1994.

[Everitt 2005] H. O. Everitt, *Experimental Aspects of Quantum Computing*. New York: Springer, 2005.

[Folman และคณะ 2000] R. Folman, *et al.,* "Controlling Cold Atoms using Nanofabricated Surfaces: Atom Chips," *Phys. Rev. Lett*., vol. 84, no. 20, pp. 4749--4752, 2000.

[Gallego และคณะ 2009] D. Gallego, *et al,.* "An optical lattice on an atom chip," *Optics Letters,* vol. 34, pp. 3463-3465, 2009.

[Gershenfeld & Chuang 1997] N. A. Gershenfeld, and I. L. Chuang, "Bulk Spin-Resonance Quantum Computation," *Science*, vol. 275, pp. 350-356, 1997.

[Grier 2003] D. G. Grier "A revolution in optical manipulation," *Nature*, vol. 424, pp. 810-816, 2003.

[Hanson และคณะ 2005] R. Hanson, et al., "Single-Shot Readout of Electron Spin States in a Quantum Dot Using Spin-Dependent Tunnel Rates," *Phys. Rev. Lett*., vol. 94, p. 196802, 2005.

[Heinrich 2004] T. Heinrich, "Neutral Atom Approaches to Quantum Information Processing and Quantum Computing," in *A Quantum Information Science and Technology Roadmap Part 1: Quantum Computation* Version 2.0. [Online]. Available: http://qist.lanl.go. [Accessed: Dec. 2009].

[HiQ.NET] "NMR – Analytical methods," *HiQ*. [Online]. Available: http://hiq.aga.cl/international/web/lg/spg/likelgspg.nsf/docbyalias/anal_nmr. [Accessed: Dec. 2009].

[Jaksch และคณะ 1999] D. Jaksch, et al., "Entanglement of Atoms via Cold Controlled Collisions," *Phys. Rev. Lett*., vol. 82, pp. 1975-1978, 1999.

[Jones 2001] J. A. Jones, "Quantum Computing and Nuclear Magnetic Resonance," *Phys. Chem. Comm*., vol. 11, 2001.

[Kane 1998] B.E. Kane, "A silicon-based nuclear spin quantum computer," *Nature*, vol. 393, pp. 133-137, 1998.

[Kok และคณะ 2007] P. Kok, et al., "Review article: Linear optical quantum computing," *Rev. Mod. Phys*., vol. 79, p. 135, 2007.

[Kielpinski และคณะ 2002] D. Kielpinski, C. Monroe, and D. J. Wineland, "Architecture for a large-scale ion-trap quantum computer," *Nature,* vol. 417, pp. 709-711, 2002.

[Knill, Laflamme & Milburn 2001] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature,* vol. 409, pp. 46-52, 2001.

[Ladd และคณะ 2002] T. D. Ladd, et al., "All-silicon quantum computer," *Phys. Rev. Lett.*, vol. 89, p. 017901, 2002.

[Laflamme และคณะ 2002] R. Laflamme, et al., "Introduction to NMR Quantum Information Processing," *arXiv.org e-Print archive*, Jul. 2002. [Online]. Available: http://arxiv.org/abs/quant-ph/0207172v1. [Accessed: Dec. 2009].

[Leibrandt และคณะ 2009] D. R. Leibrandt, et al., "Demonstration of a scalable, multiplexed ion trap for quantum information processing," *arXiv.org e-Print archive*, Jul. 2009. [Online]. Available: http://arxiv.org/abs/0904.2599. [Accessed: Dec. 2009].

[Le Bellac 2006] M. Le Bellac, *A Short Introduction to Quantum Information and Quantum Computation: English translation.* Cambridge: Cambridge University Press, 2006.

[Loss & DiVincenzo 1998] D. Loss, and D. DiVincenzo, "Quantum Computation with Quantum Dots," *Phys. Rev. A*, vol. 57, no. 1, pp. 120-126, 1998.

[Mandel และคณะ 2003] O. Mandel, et al. "Coherent transport of neutral atoms in spin-dependent optical lattice potentials," *Phys. Rev. Lett*., vol. 91, p. 010407, 2003.

[Morsch 2008] O. Morsch, *Quantum Bits and Quantum Secrets: How Quantum Physics is Revolutionizing Codes and Computers*. Berlin: Wiley-VCH, 2008.

[Monroe และคณะ 1995] C. Monroe, et al., "Demonstration of a Fundamental Quantum Logic Gate," *Phys. Rev. Lett.*, vol. 75, no. 25, pp. 4714-4717, 1995.

[NationalPhysLabUK.NET] "Laser Cooling," *UK National Physics Laboratory Website.* [Online]. Available: http://www.npl.co.uk/content-categories/research/laser-cooling. [Accessed: Dec. 15, 2009].

[Nelson และคณะ 2007] K. D. Nelson, X. Li, and D. S. Weiss, "Imaging single atoms in a three-dimensional array," *Nature Physics*, vol 3, pp. 556-560, 2007.

[Nielsen & Chuang 2000] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000.

[NIST.NET] "NIST Tech Beat," *National Institute of Standards and Technology*. [Online]. Available: http://www.nist.gov/public_affairs/techbeat/tb2009_0630.htm#trap. [Accessed: Dec. 15, 2009]

[Nobel.NET] "Wolfgang Paul - Autobiography," Nobelprize.org. [Online]. Available: http://nobelprize.org/nobel_prizes/physics/laureates/1989/paul-autobio.html. [Accessed: Dec. 15, 2009]

[O'Brien 2007] J. L. O'Brien, "Optical Quantum Computing," *Science*, vol. 318, pp. 1567-1570, 2007.

[O'Brien และคณะ 2009] J. L.O'Brien, A. Furusawa, and J. Vuckovic, "Photonic quantum technologies," *Nature Photonics,* vol. 3, pp. 687-695, 2009.

[Ohno และคณะ 1999] Y. Ohno, et al., "Electrical spin injection in a ferromagnetic semiconductor heterostructure," *Nature*, vol. 402, pp. 790-792, 1999.

[Peil และคณะ 2003] S. Peil, "Patterned loading of a Bose-Einstein condensate into an optical lattice," *Phys. Rev. A*, vol. 67, p. 051603, 2003.

[Pittman และคณะ 2004] T. B. Pittman, et al., "Quantum Computing Using Linear Optics," *John Hopkins APL Technical Digest,* vol. 25, no. 2, pp. 84-90, 2004.

[Politi และคณะ 2009] A. Politi, et al., "Shor's Quantum Factoring Algorithm on a Photonic Chip," *Science,* vol. 325, p. 1221, 2009.

[Price และคณะ 1999] M. D. Price, et al., "Construction and Implementation of NMR Quantum Logic Gates for Two Spin Systems," *Journal of Magnetic Resonance,* vol. 140, p. 371-378, 1999.

[Raizen และคณะ 2009] M. G. Raizen, et al., "Ultra-high fidelity qubits for quantum computing," *arXiv.org e-Print archive*, Jun. 2009. [Online]. Available: http://arxiv.org/abs/0906.2114v1. [Accessed: Dec. 2009].

[Reichel และคณะ 1999] J. Reichel, et al., "Atomic Micromanipulation with Magnetic Surface Traps," *Phys. Rev. Lett.,* vol. 83, pp. 3398-3401, 1999.

[Ralph และคณะ 2002] T. C. Ralph, "Simple scheme for efficient linear optics quantum gates," *Phys. Rev. A*, vol. 65, p. 012314, 2001.

[Raussendorf & Briegel 2001] R. Raussendorf, and H. J. Briegel, "A One-Way Quantum Computer," *Phys. Rev. Lett*., vol. 86, pp. 5188–5191, 2001.

[Schack & Caves 2008] R. Schack, C.M. Caves, "Classical model for bulk-ensemble NMR quantum computation," *Phys. Rev. A*, vol 60, pp. 4354-4362, 1999.

[Schaller 1997] R. R. Schaller, "Moor's law Past, Present, and Future," *IEEE Spectrum* , vol. 34, no.6, pp. 52-59, 997.

[Seidelin และคณะ 2006] S. Seidelin, et al., "Microfabricated Surface-Electrode IonTrap for Scalable Quantum Information Processing," *Phys. Rev. Lett.*, vol. 96, p. 253003, 2006.

[Steane 1997] A. Steane, "The ion trap quantum information processor," *Applied Physics B: Lasers and Optics*, vol. 64, no. 623-643, 1977.

[Stick และคณะ 2006] D. Stick, et al., "Ion trap in a semiconductor chip," *Nature*, vol. 2, pp. 36-39, 2006.

[Stolze & Suter 2004] J. Stolze, and D. Suter, *Quantum Computing*. Berlin: Wiley-VCH, 2004.

[Vandersypen และคณะ 2000] L. M.K. Vandersypen, et al., “Experimental Realization of an Order-Finding Algorithm with an NMR Quantum Computer,” *Phys. Rev. Lett.*, vol. 85, pp. 5452–5455, 2000.

[Vandersypen และคณะ 2002] L. M.K. Vandersypen, C. S. Yannoni, and I. L. Chuang “Liquid State NMR Quantum Computing,” in *Encyclopedia of Nuclear Magnetic Resonance, volume 9: Advances in NMR,* D. M. Grant, Ed. West Sussex, UK: John Wiley & Sons, 2002, pp. 1-10.

[Warren 1997] W. S. Warren, “The Usefulness of NMR Quantum Computing,” *Science*, vol. 277, pp. 1688-1690, 1997.

[Wineland และคณะ 1998] D.J. Wineland, et al. “Experimental Primer on the Trapped Ion Quantum Computer,” *Fortschr. Phys.*, vol. 46, pp. 363-390, 1998.

[Wurtz และคณะ 2009] P. Würtz, et al., “Experimental Demonstration of Single-Site Addressability in a Two-Dimensional Optical Lattice,” *Phys. Rev. Lett*., vol. 103, p. 080404, 2009.

[Zhu และคณะ 2001] H. J. Zhu, et al., “Room-Temperature Spin Injection from Fe into GaAs,” *Phys. Rev. Lett.,* vol. 87, p. 016601, 2001.

[Zippilli และคณะ 2009] S. Zippilli, et al., “Entanglement of distant atoms by projective measurement: The role of detection efficiency,” *New Journal of Physics*, vol. 10, pp. 103003, 2009.

[Zrenner และคณะ 2002] A. Zrenner, et al., “Coherent properties of a two-level system based on a quantum-dot photodiode,” *Nature*, vol. 418, pp. 612-614, 2002.

คำถามท้ายบทที่ 5 (Questions and Answers)
และอภิปราย (Discussions) ปรับปรุง ณ
Blog: http://www.stks.or.th/blog/?p=14123

บทที่ 6
พัฒนาการงานวิจัยสารสนเทศเชิงควอนตัม
(Quantum information research summary)

อภิธานศัพท์ (Glossary)

- **กฎของมัวร์ (Moore's law)**
  กฎที่นำเสนอโดยกอร์ดอน มัวร์ (Gordon E. Moore) ซึ่งกล่าวถึงเทคโนโลยีทางด้านไมโครอิเล็กทรอนิกส์ว่าปริมาณของทรานซิสเตอร์บนวงจรรวมจะเพิ่มเป็นเท่าตัวทุกช่วงเวลาระยะเวลาประมาณสองปี
- **การกระจายกุญแจเชิงควอนตัมด้วยสถานะแบบต่อเนื่อง (Continuous-variable QKD)**
  การกระจายกุญแจเชิงควอนตัมด้วยสถานะที่มีจำนวนฐานเป็นอนันต์ เช่น สถานะของตำแหน่งและโมเมนตัมของอนุภาค
- **การกล้ำสัญญาณเฟส (Phase modulation)**
  การแปลงสัญญาณโดยทำให้ค่าเบี่ยงเบนของเฟสของสัญญาณพาห์เป็นสัดส่วนกับแอมพลิจูดของสัญญาณแถบความถี่ฐานของข่าวสาร
- **การสื่อสารในแนวสายตา (Line of sight)**
  การสื่อสารที่อาศัยเส้นทางที่ปราศจากสิ่งกีดขวางระหว่างต้นทางไปยังปลายทาง
- **ควอนตัมดอท (Quantum dot)**
  สารกึ่งตัวนำที่มีโครงสร้างขนาดเล็กในระดับนาโนเมตร อาจเรียกว่าผลึกนาโน มีจุดเด่นคือ มีขนาดเล็กมาก โดยมีเส้นผ่านศูนย์กลาง 2-10 นาโนเมตร หรือ 10-50 อะตอม และถูกควบคุมด้วยการกระตุ้นจากภายนอก
- **ความยาวคลื่นชนิดยาว (Long wavelength)**
  ความยาวคลื่นระหว่าง 1,565 - 1,625 นาโนเมตร ตามการแบ่งความยาวคลื่นในย่านการสื่อสารเชิงแสง
- **มาตรแทรกสอดแบบแซ็กแน็ก (Sagnac interferometer)**
  เครื่องมือในการวัดความเร็วเชิงมุมในการหมุนที่มีความละเอียดสูงโดยอาศัยการแทรกสอดของแสง
- **วงโคจรต่ำ (Low-earth-orbit: LEO)**
  วงโคจรเหนือผิวโลกที่ความสูงระหว่าง 160 ถึง 2,000 กิโลเมตรโดยประมาณ

ข้อสรุปประจำบท (Summary)

Quantum information can be focused basically on just two main research areas; quantum communications and quantum computing. Quantum communication based on cryptography is clearly the rising topic as it is the first successful research area through the commercialization. Since its first prototype implemented in 1992, this high potential topic has been highlighting gradually worldwide on both academic and information security industry. This combined field of quantum mechanics physics and classical cryptography as a new absolute secure encryption technology, has been a fascinating for over a decade. In order to promote and to implement quantum key distribution in practice, its networking has been demonstrated many places around the world. New techniques for achieving longer distance, higher speed, and others, have been proposing continuously such as those on DARPA (2003), SECOQC (2008), SwissQuantum (2009), or Tokyo QKD network (2010) and etc. Consequently, there are lots of active research groups and a number of QKD networks implemented around the world. Therefore, it is interesting to keep the eyes on the progress of this fascinating field and also looking forward to linking those potential networks together. On another

main hand merging quantum mechanics with computing purpose, quantum computing extends the computational potential of those traditional computers. It allows, for instance, searching by large-scale data instead of using only words, and faster integer factorizing. However, the best system suitable to be utilized for implementing the quantum computer has still been being explored. There are many potential candidates which have been realized for a few number of qubits, such systems are nuclear magnetic resonance (NMR), linear optics, quantum dots, and trapped ions. In order to develop these two main branches of quantum information systematically, technology or research policy and forecasting have also been mentioned worldwide. There are a number of countries considering quantum information as one of those important milestones on their national technological roadmap.

6.1 งานวิจัยด้านการสื่อสารและการคำนวณเชิงควอนตัมทั่วโลก

พัฒนาการของเทคโนโลยีสารสนเทศเชิงควอนตัมสามารถแบ่งการพิจารณาแยกกลุ่มออกได้เป็นสองส่วน คือการสื่อสารเชิงควอนตัมหรือการนำไปประยุกต์ใช้สำหรับการสื่อสาร และการคำนวณเชิงควอนตัม โดยการคาดการณ์การเติบโตของเทคโนโลยีด้านนี้สรุปแสดงด้วยผลของสำนักวิจัยหรือวิชาการต่างๆ ดังรูปที่ 6.1 มีรายละเอียดสถานภาพงานวิจัยทั้งสองสาขาของทั่วโลกโดยสังเขปจากช่วงแรกที่มีผลการพัฒนาเด่นชัด คือต้นทศวรรษสากลแรก (ถึง ค.ศ.2004) และผลของช่วงต่อๆมา ดังนี้

6.1.1 ภาพรวมงานวิจัยด้านการสื่อสารเชิงควอนตัมทั่วโลก

การสื่อสารเชิงควอนตัมเป็นศาสตร์ในการแปลงสถานะเชิงควอนตัมจากสถานที่หนึ่งไปยังสถานที่อื่นโดยอาศัยคิวบิตหรือหน่วยพื้นฐานของการสื่อสารเป็นตัวดำเนินการ ซึ่งเป็นการผสานความรู้เทคโนโลยีเชิงควอนตัมหลายด้านที่มีการวิจัยและพัฒนาโดยมหาวิทยาลัยและหน่วยงานวิจัยของรัฐบาลในหลายประเทศ อาทิ สหรัฐอเมริกา สหภาพยุโรป และประเทศญี่ปุ่น การประยุกต์เทคโนโลยีสารสนเทศเชิงควอนตัมในช่วงแรกมุ่งเน้นไปที่การกระจายกุญแจลับเชิงควอนตัม อันเป็นกระบวนการสื่อสารที่อาศัยการส่งสถานะเชิงควอนตัมเพียงครั้งละหนึ่งหรือสองคิวบิตที่เริ่มมีใช้งานจริงสำหรับการสื่อสารแบบจุดต่อจุดในระยะทางใกล้ได้แล้ว สถานภาพงานวิจัยด้านการสื่อสารเชิงควอนตัมสำหรับการใช้งานจริงทั่วโลกระยะแรกจึงมุ่งเน้นไปที่ระบบวิทยาการรหัสลับเชิงควอนตัมที่แบ่งตามรูปแบบของการจัดกระบวนการสื่อสารหรือเทคนิคที่ใช้ดังนี้

6.1.1.1 การสื่อสารด้วยแหล่งกำเนิดแสงเลเซอร์ชนิดพัลส์ผ่านเส้นใยแสง

แสงเลเซอร์ชนิดพัลส์ผ่านเส้นใยแสงเป็นการกำเนิดจากการจัดอุปกรณ์โดยอาศัยการลดทอนความเข้มของแสงจากสัญญาณพัลส์ที่ขับด้วยไดโอดเลเซอร์ผ่านเส้นใยแสงชนิดโหมดเดี่ยวจากผู้ส่งไปยังผู้รับ การจัดการสื่อสารในรูปแบบนี้มีกลุ่มวิจัยที่มุ่งเน้นทำการหลักๆ ดังตารางที่ 6.1 โดยเป้าหมายในช่วงระยะเวลา 10 ปี ข้างหน้า (เริ่มต้นจากปี พ.ศ. 2547) คือ

- มีอัตราการส่งสัญญาณพัลส์ความเร็วอย่างน้อย 1 กิกะเฮิรตซ์
- อัตราการกำเนิดกุญแจลับอย่างต่อเนื่องได้มากกว่า 100,000 บิตต่อวินาที
- สามารถจัดโครงข่ายแบบผู้ใช้หลายกลุ่มซึ่งครอบคลุมพื้นที่ระยะไกล
- สามารถจัดระบบร่วมกับการกระจายกุญแจลับเชิงควอนตัมผ่านตัวกลางอากาศได้
- สามารถจัดชุดทวนสัญญาณเชิงควอนตัมเพื่อเพิ่มระยะในการส่งระหว่างเมืองได้ (ประมาณ 500 กิโลเมตร)

นอกจากกลุ่มวิจัยทางด้านแหล่งกำเนิดแสงเลเซอร์ชนิดพัลส์ผ่านเส้นใยแสงแบบพื้นฐานทั่วไปแล้ว ยังมีกลุ่มวิจัยที่ทำการค้นคว้าพัฒนาชนิด “Plug-and-Play” เพื่อให้เกิดความสะดวกในการใช้งาน และนำไปสู่การใช้งานจริงในเครือข่ายสื่อสารปกติได้ การจัดการสื่อสารในรูปแบบนี้มีผลการสำรวจกลุ่มวิจัยหลักดังตารางที่ 6.2

รูปที่ 6.1 การคาดการณ์เทคโนโลยีวิทยาการรหัสลับเชิงควอนตัม

ตารางที่ 6.1 กลุ่มวิจัยด้านการกระจายกุญแจลับเชิงควอนตัมด้วยแสงเลเซอร์ชนิดพัลส์ผ่านเส้นใยแสง [*Heinrich 2004*]

ผู้นำกลุ่มวิจัย	สถานที่ในการวิจัย	หัวข้อหลักในการวิจัย
-	บริษัทเอลแซก ไบรีย์ (Elsag-Bailey) ประเทศอิตาลี	เกณฑ์วิธีทางด้านซอฟต์แวร์
ซี แอลเลียต (C. Elliott)	บริษัทบีบีเอ็น เทคโนโลยี (BBN Technology) ประเทศสหรัฐอเมริกา	ระบบโครงข่ายการกระจายกุญแจลับเชิงควอนตัมระดับเมือง
เจ เจ ฟรานสัน (J. J. Franson)	ห้องปฏิบัติการฟิสิกส์ประยุกต์มหาวิทยาลัยจอห์นส์ฮอปกินส์ (Johns Hopkins University Applied Physics Laboratory: JHU/APL) ประเทศสหรัฐอเมริกา	ระบบการสื่อสารชนิดตัวกลางอากาศและผ่านเส้นใยแสง
เจ พี คูดเกแบร์ (J.-P. Goedgebuer)	มหาวิทยาลัยฟรองซ์ กงเต (University of Franche-Comte) ประเทศฝรั่งเศส	การกล้ำสัญญาณเฟส
ที ฮาเซกาวา (T. Hasegawa)	บริษัทมิตซูบิชิ (Mitsubishi Electric) ประเทศญี่ปุ่น	ระบบการกระจายกุญแจลับเชิงควอนตัม
ดี เอียนมะ (D. Hjelme)	มหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยีนอร์วีเจียน (Norwegian University of Science and Technology: NTNU) ประเทศนอร์เวย์	ระบบการกระจายกุญแจลับเชิงควอนตัม

ผู้นำกลุ่มวิจัย	สถานที่ในการวิจัย	หัวข้อหลักในการวิจัย
อาร์ เจ ฮิวจ์ส (R.J. Hughes)	ห้องปฏิบัติการแห่งชาติลอส อลามอส (Los Alamos National Laboratory : LANL) ประเทศสหรัฐอเมริกา	ระบบการกระจายกุญแจลับเชิงควอนตัม
เอ ชิลด์ส (A. Shields)	บริษัท โตชิบา (Toshiba) ศูนย์วิจัย ณ ประเทศอังกฤษ	ระบบการกระจายกุญแจลับเชิงควอนตัม และแหล่งกำเนิดโฟตอนเดี่ยว
พี ดี ทาวน์เซนด์ (P.D. Townsend)	มหาวิทยาลัยคอร์ก (University College Cork) ประเทศไอร์แลนด์	ระบบโครงข่ายการกระจายกุญแจลับเชิงควอนตัมระดับเมือง
เฮช เจิง (H. Zeng)	มหาวิทยาลัยครุศาสตร์แห่งภาคตะวันออก (East China Normal University) ประเทศจีน	การเข้ารหัสด้วยเฟสโดยอาศัยมาตรแทรกสอดแบบแซ็กแน็ก (Sagnac interferometer)

ตารางที่ 6.2 กลุ่มวิจัยด้านการกระจายกุญแจลับเชิงควอนตัมด้วยแสงเลเซอร์ชนิดพัลส์ผ่านเส้นใยแสงชนิด “Plug and Play” [*Heinrich 2004*]

ผู้นำกลุ่มวิจัย	สถานที่ในการวิจัย	หัวข้อหลักในการวิจัย
ดี เบอธูน และ ดับเบิลยู ริสก์ (D. Bethune & W. Risk)	ศูนย์วิจัยไอบีเอ็มอัลมาเดน (IBM Almaden Research Center) ประเทศสหรัฐอเมริกา	ระบบการกระจายกุญแจลับเชิงควอนตัม
ดี เอียนมะ (D. Hjelme)	มหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยีนอร์เวย์ (Norwegian University of Science and Technology) ประเทศนอร์เวย์	การทดสอบระบบชนิด “plug and play” ในกรณีถูกดักจับและการป้องกัน
เค นากามูระ (K. Nakamura)	บริษัท NEC ประเทศญี่ปุ่น	ระบบการกระจายกุญแจลับเชิงควอนตัม
เอ็ม นีลเซน (M. Nielsen) และคณะ	มหาวิทยาลัยออร์ฮูส (University of Aarhus) ประเทศเดนมาร์ก	ระบบการกระจายกุญแจลับเชิงควอนตัม
จี ริบอร์ดี (G. Ribordy)	บริษัท ID Quantique ประเทศสวิตเซอร์แลนด์	ระบบ “plug and play” เชิงพาณิชย์
เอ ไทรโฟนอฟ (A. Trifonov)	บริษัท MagiQ ประเทศสหรัฐอเมริกา	ระบบ “plug and play” เชิงพาณิชย์
เอ โยชิซาวา (A. Yoshizawa)	สถาบันพัฒนาวิทยาศาสตร์และเทคโนโลยีอุตสาหกรรมแห่งประเทศญี่ปุ่น	ระบบการกระจายกุญแจลับเชิงควอนตัม
เอ คาร์ลสัน (A. Karlsson)	ราชวิทยาลัยเทคโนโลยี (The Royal Institute of Technology: KTH) ประเทศสวีเดน	การจัดระบบที่ความยาวคลื่นชนิดยาว

โดยเป้าหมายรวมในช่วงระยะเวลา 10 ปี ต่อจาก พ.ศ. 2547 สำหรับการวิจัยทางด้านนี้ (ตารางที่ 6.2) คือ

- มีอัตราการส่งสัญญาณพัลส์มีความเร็วอย่างน้อย 1 กิกะเฮิรตซ์
- มีอัตราการกำเนิดกุญแจลับอย่างต่อเนื่องได้มากกว่า 100,000 บิตต่อวินาที
- สามารถจัดโครงข่ายแบบผู้ใช้หลายกลุ่มซึ่งครอบคลุมพื้นที่ระดับเมือง
- สามารถจัดระบบร่วมกับการกระจายกุญแจลับเชิงควอนตัมผ่านตัวกลางอากาศได้
- สามารถจัดชุดทวนสัญญาณเชิงควอนตัมเพื่อเพิ่มระยะในการส่งระหว่างเมืองได้ (ประมาณ 500 กิโลเมตร)

6.1.1.2 การสื่อสารด้วยแหล่งกำเนิดแสงเลเซอร์ชนิดพัลส์ผ่านตัวกลางอากาศ

การจัดอุปกรณ์สื่อสารโดยอาศัยการลดทอนความเข้มของแสงจากสัญญาณพัลส์ที่ขับด้วยไดโอดเลเซอร์ผ่านตัวกลางอากาศจากผู้ส่งไปยังผู้รับ เป็นอีกหนึ่งแนวทางในการสื่อสารนำเอาสถานะคอวนตัมเฉพาะที่เหมาะสมกับสภาพอากาศ (แต่ไม่เหมาะสมกับเส้นใยนำแสง) ส่งผ่านอากาศจากภาคส่งไปยังผู้รับในระยะสายตาและพิกัดความสามารถของอุปกรณ์ การจัดการสื่อสารในรูปแบบนี้มีกลุ่มวิจัยที่ตั้งเป็นป้าหมายหลักแสดงดังตารางที่ 6.3

ตารางที่ 6.3 กลุ่มวิจัยด้านการกระจายกุญแจลับเชิงควอนตัมด้วยแสงเลเซอร์ชนิดพัลส์ผ่านตัวกลางอากาศ [*Heinrich 2004*]

ผู้นำกลุ่มวิจัย	สถานที่ในการวิจัย	หัวข้อหลักในการวิจัย
พี เอ็ดเวอร์ดส (P. Edwards)	มหาวิทยาลัยแคนเบอร์รา (University of Canberra) ประเทศออสเตรเลีย	การสื่อสารจากพื้นสู่ดาวเทียม
จี กิลเบอร์ต (G. Gilbert)	เอ็มไอทีอาร์อี (MITRE) ประเทศสหรัฐอเมริกา	การศึกษาทางด้านทฤษฎี
อาร์ ฮิวจ์ส (R. Hughes)	แอลเอเอ็นแอล (LANL) ประเทศสหรัฐอเมริกา	การสื่อสารจากพื้นสู่ดาวเทียม
ซี เคอร์ทซีเฟอร์ (C. Kurtsiefer)	มหาวิทยาลัยสิงคโปร์ (University of Singapore) ประเทศสิงคโปร์	การสื่อสารในแนวระยะสายตา (line of sight)
บี โลเวอส์น (B. Lowans)	คิเนติค (Qinetiq) ประเทศอังกฤษ	ระบบขนาดเล็ก
เจ แรริที (J. Rarity)	มหาวิทยาลัยบริสทอล (University of Bristol) ประเทศอังกฤษ	การสื่อสารจากพื้นสู่ดาวเทียม
ซี วิลเลียมส์ (C. Williams)	สถาบันทางมาตรฐานและเทคโนโลยีแห่งชาติ เกนสเตอส์เบิร์ก (National Institute of Standard and Technology : NIST, Gaithersburg) ประเทศสหรัฐอเมริกา	การกระจายกุญแจลับเชิงควอนตัมความเร็วสูง
เอช ไวน์ฟอร์เทอร์ (H. Weinfurter)	มหาวิทยาลัยมิวนิค (University of Munich) ประเทศเยอรมนี	การสื่อสารในแนวระยะสายตา (ผ่านอากาศ)
เอ ไซลิงเงอร์ (A. Zeilinger)	มหาวิทยาลัยเวียนนา (University of Vienna) ประเทศออสเตรีย	การสื่อสารในแนวระยะสายตา (ผ่านอากาศ)

ตารางที่ 6.4 กลุ่มวิจัยด้านการกระจายกุญแจลับเชิงควอนตัมด้วยแหล่งกำเนิดโฟตอนเดี่ยว [*Heinrich 2004*]

ผู้นำกลุ่มวิจัย	สถานที่ในการวิจัย	หัวข้อหลักในการวิจัย
วาย ยามาโมโต และ เจ โวโควิก (Y. Yamamoto and J. Vuckovic)	มหาวิทยาลัยสแตนฟอร์ด (Stanford University) ประเทศสหรัฐอเมริกา	แหล่งกำเนิดจากควอนตัมดอท (Quantum dot)
พี กรองจี (P. Grangier)	สถาบันดอปติค ซีเอ็นอาร์เอส (Institut d'Optique, CNRS) ประเทศฝรั่งเศส	แหล่งกำเนิดจากช่องว่างของอะตอมในผลึกเพชรระดับนาโน
พี เควียต (P. Kwiat)	มหาวิทยาลัยอิลลินอยส์ เออร์บานาแชมเปน (University of Illinois, Urbana-Champaign) ประเทศสหรัฐอเมริกา	แหล่งกำเนิดจากคู่โฟตอนพัวพัน แต่เลือกเพียงโฟตอนเดียว เพื่อยืนยันความเป็นโฟตอนเดี่ยวได้อย่างแท้จริง
เจ แรริที (J. Rarity)	มหาวิทยาลัยบริสทอล (University of Bristol) ประเทศอังกฤษ	แหล่งกำเนิดจากควอนตัมดอท
เอ มิกดอล และ ซี วิลเลียมส์ (A. Migdall and C. Williams)	สถาบันทางมาตราฐานและเทคโนโลยีแห่งชาติ (National Institute of Standard and Technology : NIST) ประเทศสหรัฐอเมริกา	แหล่งกำเนิดจากคู่โฟตอนพัวพัน แต่เลือกออกมาเพียงโฟตอนเดียว เพื่อยืนยันความเป็นโฟตอนเดี่ยวได้อย่างแท้จริง
เอ ชีลส์ (A. Shields)	ประเทศอังกฤษ	แหล่งกำเนิดจากควอนตัมดอท

เป้าหมายจากปี พ.ศ. 2547 สำหรับการวิจัยทางด้านนี้ (ตารางที่ 6.3) ในทศวรรษถัดมาคือ

- มีอัตราการส่งสัญญาณพัลส์มีความเร็วอย่างน้อย 1 กิกะเฮิรตซ์
- มีอัตราการกำเนิดกุญแจลับอย่างต่อเนื่องได้มากกว่า 100,000 บิตต่อวินาที
- สามารถจัดโครงข่ายแบบผู้ใช้หลายคนซึ่งครอบคลุมพื้นที่ระดับเมือง

6.1.1.3 การสื่อสารด้วยแหล่งกำเนิดโฟตอนเดี่ยว

การจัดการสื่อสารนี้เป็นระบบจากการจัดอุปกรณ์โดยใช้แหล่งกำเนิดโฟตอนที่ได้รับการประมาณว่าเป็นโฟตอนเดี่ยวอย่างแท้จริง ซึ่งสามารถยืนยันความปลอดภัยจากการถูกดักจับโฟตอนได้มากกว่าแหล่งกำเนิดที่อาศัยการลดทอนความเข้มแสง การจัดการสื่อสารในรูปแบบนี้มีกลุ่มวิจัยหลักแสดงดังตารางที่ 6.4 โดยเป้าหมายเวลา 10 ปี นับจากปี พ.ศ. 2547 สำหรับการวิจัยทางด้านนี้ คือ

- สามารถจัดชุดกระจายกุญแจลับเชิงควอนตัมด้วยแหล่งกำเนิดโฟตอนเดี่ยวได้ระยะทางในระดับ 100 กิโลเมตร ที่อัตราการส่งในระดับเมกะเฮิรตซ์
- สามารถจัดชุดกระจายกุญแจลับเชิงควอนตัมด้วยแหล่งกำเนิดโฟตอนเดี่ยวผ่านดาวเทียมได้

6.1.1.4 การสื่อสารด้วยแหล่งกำเนิดคู่โฟตอนพัวพัน

การใช้แหล่งกำเนิดคู่โฟตอนพัวพันที่มีความพัวพัน ทำได้โดยโฟตอนที่มีความพัวพันแรกจะถูกส่งไปที่ผู้ส่งข้อมูล โฟตอนที่สองจะถูกส่งไปที่ผู้รับปลายทาง จากนั้นผู้ส่งและผู้รับวัดสถานะของโฟตอนเพื่อกำหนดเป็นบิตข้อมูล ซึ่งหากมีผู้ดักจับโฟตอนระหว่างการส่งจะทำให้เกิดความผิดปกติขึ้นกับคู่โฟตอนที่พัวพันดังกล่าว การจัดการสื่อสารในรูปแบบนี้มีกลุ่มวิจัยแกนหลักดำเนินการไม่มากนักเนื่องจากเป็นเทคนิคขั้นสูง โดยกลุ่มบุกเบิกต่างๆ แสดงดังตารางที่ 6.5

ตารางที่ 6.5 กลุ่มวิจัยด้านการกระจายกุญแจลับเชิงควอนตัมด้วยแหล่งกำเนิดคู่โฟตอนพัวพัน [*Heinrich 2004*]

ผู้นำกลุ่มวิจัย	สถานที่ในการวิจัย	หัวข้อหลักในการวิจัย
เอ็น กีซิน (N. Gisin)	มหาวิทยาลัยเจนีวา (University of Geneva) ประเทศสวิตเซอร์แลนด์	การเพิ่มระยะทาง และประยุกต์ใช้งาน
เอ คอร์ลฌอน(A. Karlsson)	ราชวิทยาลัยเทคโนโลยี (The Royal Institute of Technology: KTH) ประเทศสวีเดน	การประยุกต์ใช้งาน
พี เควียต (P. Kwiat)	มหาวิทยาลัยอิลลินอยส์ เออร์บานา แชมเปน(University of Illinois, Urbana-Champaign) ประเทศสหรัฐอเมริกา	การพัฒนาประสิทธิภาพแหล่งกำเนิด และการประยุกต์ใช้งาน
เจ แรริที (J. Rarity)	มหาวิทยาลัยบริสทอล (University of Bristol) ประเทศอังกฤษ	การประยุกต์ใช้งาน
เอ เซอร์จีเอนโก (A. Sergienko)	มหาวิทยาลัยบอสตัน (Boston University) ประเทศสหรัฐอเมริกา	การพัฒนาประสิทธิภาพแหล่งกำเนิด และการประยุกต์ใช้งาน
เอช ไวน์ฟอร์เทอร์ (H. Weinfurter)	เอ็มพีคิว/แอลเอ็มยู มิวนิค (MPQ/LMU Munich) ประเทศเยอรมนี	การพัฒนาประสิทธิภาพแหล่งกำเนิด
เอ ไซลิงเงอร์ (A. Zeilinger)	มหาวิทยาลัยเวียนนา (University of Vienna) ประเทศออสเตรีย	การพัฒนาประสิทธิภาพแหล่งกำเนิด และการประยุกต์ใช้งาน

ตารางที่ 6.6 กลุ่มวิจัยด้านการกระจายกุญแจลับเชิงควอนตัมด้วยกระบวนการต่อเนื่อง [*Heinrich 2004*]

ผู้นำกลุ่มวิจัย	สถานที่ในการวิจัย	หัวข้อหลักในการวิจัย
พี กรองจี (P. Grangier)	ปารีส (Paris) ประเทศฝรั่งเศส	การใช้งานสำหรับการสื่อสาร
จี ลอยส์ (G. Leuchs)	แอร์ลางก์น (Erlangen) ประเทศเยอรมนี	การใช้งานสำหรับการสื่อสาร
อี จัคโกบิโน (E. Giacobino)	ปารีส (Paris) ประเทศฝรั่งเศส	การใช้งานสำหรับการสื่อสาร
เอ็น เซอร์ฟ (N. Cerf)	บรัสเซอร์ลส์ (Brussels) ประเทศเบลเยียม	การศึกษาทฤษฎีสำหรับการสื่อสาร
พี คูมาร์ (P. Kumar)	นอร์ทเวสเทิร์น (Northwestern) ประเทศสหรัฐอเมริกา	การใช้งานสำหรับการสื่อสาร
เจ พรีสคิล (J. Preskill)	สถาบันเทคโนโลยีแห่งแคลิฟอร์เนีย (California Institute of Technology : Caltech) ประเทศสหรัฐอเมริกา	การศึกษาทฤษฎีสำหรับการสื่อสาร

เป้าหมาย 10 ปี นับจากปี พ.ศ. 2547 สำหรับการวิจัยทางด้านแหล่งกำเนิดคู่โฟตอนพัวพัน (ตารางที่ 6.5) คือ

- สามารถทำหน่วยความจำเชิงควอนตัมที่เก็บข้อมูลได้นานถึงระดับ 1 วินาที
- สามารถจัดชุดกระจายกุญแจลับเชิงควอนตัมด้วยแหล่งกำเนิดคู่โฟตอนพัวพันผ่านดาวเทียมได้
- สามารถจัดทำต้นแบบระบบการสื่อสารผ่านเส้นใยแสงได้ระยะทางมากกว่า 100 กิโลเมตร
- สามารถจัดทำหน่วยย้ำสัญญาณเชิงควอนตัมที่มีอัตราการกำเนิดมากกว่า 1,000 คิวบิตต่อวินาที

6.1.1.5 การสื่อสารด้วยสถานะควอนตัมแบบต่อเนื่อง (Continuous-Variable QKD)

การจัดการสื่อสารระบบนี้เป็นการจัดอุปกรณ์ที่ใช้แหล่งกำเนิดแสงความเข้มสูงกว่าโฟตอนเดี่ยวโดยการกำหนดบิตเชิงควอนตัมด้วยการแบ่งเฟส แอมพลิจูด หรือโพลาไรเซชัน การจัดการสื่อสารในรูปแบบนี้มีกลุ่มวิจัยแกนนำต่างๆ แสดงดังตารางที่ 6.6 และสำหรับเป้าหมายในหนึ่งทศวรรษจากปี พ.ศ. 2547 สำหรับการวิจัยทางด้านนี้ คือ สามารถจัดชุดกระจายกุญแจลับเชิงควอนตัมแบบเต็มระบบด้วยระยะทางการสื่อสารในระดับ 100 กิโลเมตร

6.1.2 ภาพรวมงานวิจัยด้านวิทยาการรหัสลับเชิงควอนตัมทั่วโลก

การพัฒนาระบบวิทยาการรหัสลับเชิงควอนตัมได้รับความความสนใจจากสถาบันวิจัยและหน่วยงานต่างๆ ทั่วโลก ซึ่งความก้าวหน้าและสถานภาพงานวิจัยเด่นจากหน่วยงานทั่วโลกมีดังนี้

6.1.2.1 ทวีปยุโรป

สถาบันวิจัยแมกซ์พลังค์สำหรับควอนตัมเชิงแสง (Max Planck Institute for Quantum Optics) จากมหาวิทยาลัยลุกวิก แมกซิมิลเลียนส์แห่งมิวนิค (Ludwig Maximilians University of Munich) ประเทศเยอรมนี ร่วมกับนักวิจัยจากหลายสถาบันในสหภาพยุโรป ได้ทดสอบระบบวิทยาการรหัสลับเชิงควอนตัม โดยใช้โพลาไรเซชันของโฟตอนเดี่ยวตามเกณฑ์วิธี BB84 ส่งผ่านอากาศระยะทาง 144 กิโลเมตร ด้วยอัตราการส่งข้อมูล 12 บิต ต่อวินาทีใน พ.ศ. 2550 [*Schmitt-Manderbach และคณะ 2007*]

กลุ่มวิจัยจากมหาวิทยาลัยแห่งเวียนนา (University of Vienna) ประเทศออสเตรีย ทำการทดสอบระบบวิทยาการรหัสลับเชิงควอนตัมชนิดแหล่งกำเนิดชนิดคู่โฟตอนพัวพัน สำหรับการสื่อสารจริงในการทำธุรกรรมทางการเงิน ด้วยระยะทาง 1.45 กิโลเมตร ผ่านเส้นใยแสง ที่ความยาวคลื่น 810 นาโนเมตร ผลปรากฏว่ามีอัตราการส่งข้อมูล 80 บิตต่อวินาที ในปี พ.ศ.2547 ต่อมาในปี พ.ศ. 2550 มีความร่วมมือกับนักวิจัยจากหลายสถาบันในสหภาพยุโรป ทดสอบระบบวิทยาการรหัสลับชนิดแหล่งกำเนิดคู่โฟตอนพัวพัน สื่อสารผ่านอากาศด้วยระยะทาง 144 กิโลเมตร ด้วยอัตราการส่งข้อมูล 178 บิตภายในเวลา 75 วินาที [*Ursin และคณะ 2007*]

บริษัท ID Quantique ร่วมกับรัฐบาลประเทศสวิตเซอร์แลนด์ในการนำวิทยาการรหัสลับเชิงควอนตัมมาใช้งานสำหรับป้องกันการโจรกรรมระหว่างการส่งข้อมูลมายังหน่วยรวบรวมข้อมูลคะแนนเสียงเลือกตั้ง สำหรับการเลือกตั้งในวันที่ 21 ตุลาคม พ.ศ. 2550 ณ กรุงเจนีวา ประเทศสวิตเซอร์แลนด์ [*Election.NET*]

เครือข่ายกระจายกุญแจเชิงควอนตัมในยุโรป (Secure Communication based on Quantum Cryptography: SECOQC) เป็นกลุ่มงานวิจัยของทวีปยุโรป ได้ก่อตั้งกลุ่มวิจัยที่ประกอบด้วยสมาชิก 12 ประเทศด้วยงบประมาณกว่า 11 ล้านยูโร เพื่อแก้ปัญหาเรื่องความปลอดภัยของการส่งข้อมูลข่าวสารด้วยระบบวิทยาการรหัสลับเชิงควอนตัม กลุ่ม SECOQC ได้นำเสนอการสาธิตการทำงานแบบโครงข่ายของระบบวิทยาการรหัสลับเชิงควอนตัมแรกที่สมบูรณ์ประกอบด้วย 6 โหนด 8 เส้นทาง ในวันที่ 8-10 ตุลาคม พ.ศ.2551 ณ กรุงเวียนนา ประเทศออสเตรีย แสดงดังรูปที่ 6.2 [*Peev และคณะ 2009*]

รูปที่ 6.2 งานแถลงข่าวและสาธิตการทำงาน เครือข่ายกระจายกุญแจเชิงควอนตัมในยุโรป (SECOQC) ณ กรุงเวียนนา ประเทศออสเตรีย เมื่อวันที่ 8 ตุลาคม พ.ศ.2551

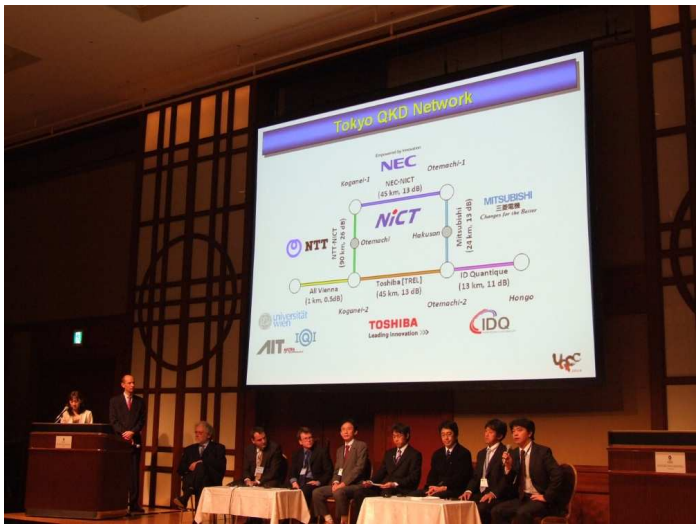
6.1.2.2 ทวีปอเมริกา

ประเทศสหรัฐอเมริกา มีหน่วยงานต่างๆ รวมกลุ่มสร้างโครงข่ายระบบวิทยาการรหัสลับเชิงควอนตัม โดยหน่วยงาน DARPA ซึ่งเป็นหน่วยงานของกระทรวงกลาโหมประเทศสหรัฐอเมริกา ให้ทุนในการสร้างเครือข่าย กลุ่มความร่วมมือของโครงการนี้ประกอบด้วยหน่วยงานหลักๆ คือ BBN Technologies เป็นบริษัทที่วิจัยและพัฒนาเทคโนโลยีชั้นสูงในประเทศสหรัฐอเมริกา สถาบันวิจัย Las Alamos ซึ่งเป็นสถาบันวิจัยแห่งชาติของประเทศสหรัฐอเมริกา National Institute of Standards and Technology (NIST) และ บริษัท QinetiQ จากสหราชอาณาจักร โดยมีเครือข่ายทั้งหมด 10 จุด และสามารถใช้งานได้อย่างสมบูรณ์ [*Elliott และคณะ 2005*]

6.1.2.3 ทวีปเอเชีย

สำนักงานเทคโนโลยีสารสนเทศและการสื่อสารแห่งประเทศญี่ปุ่น (National Institute of Information and Communications Technology: NICT) นำโดย ดร.มาซาฮิเดะ ซาซากิ (Masahide Sasaki) ร่วมกับบริษัทเอกชนและหน่วยงานที่เกี่ยวข้องได้จัดตั้งโครงการวิจัยระบบวิทยาการรหัสลับเชิงควอนตัม ดำเนินโครงการยี่สิบปี (พ.ศ. 2544 - 2563) เพื่อพัฒนาและสร้างระบบเครือข่ายความปลอดภัยระดับสูงด้วยเทคโนโลยีควอนตัมทั้งแบบโฟตอนเดี่ยว ควอนตัมเชิงพัวพัน รวมทั้งการกระจายรหัสลับเชิงควอนตัมผ่านดาวเทียม โดยเมื่อปี พ.ศ. 2548 ได้ร่วมกับบริษัท NEC ทดสอบและสาธิตเครือข่ายระบบวิทยาการรหัสลับเชิงควอนตัมได้ระยะทาง 16 กิโลเมตร ผ่านเส้นใยแสง ซึ่งเป็นการทดสอบต่อเนื่องระยะยาวนานที่สุด 2 สัปดาห์ และในปี พ.ศ. 2549 ได้ทดสอบการรับ – ส่งแสงจากดาวเทียมวงโคจรต่ำมายังภาคพื้นดินเพื่อเตรียมการสำหรับการกระจายกุญแจรหัสลับผ่านดาวเทียมในอนาคต [*NICT.NET*]

ประเทศญี่ปุ่น โดยหน่วยงาน NICT ร่วมกับสำนักงานส่งเสริมเทคโนโลยีสารสนเทศ ประเทศญี่ปุ่น (Information-technology Promotion Agency: IPA) และสถาบันพัฒนาวิทยาศาสตร์และเทคโนโลยีอุตสาหกรรมแห่งประเทศญี่ปุ่น (National Institute of Advanced Industrial Science and Technology: AIST) ร่วมกับบริษัท และสถาบันวิจัยจากหลายประเทศ สาธิตระบบวิทยาการรหัสลับเชิงควอนตัมและการสื่อสารเชิงควอนตัมที่ประกอบด้วย 6 โหนด 6 เส้นทาง ในวันที่ 18 - 20 ตุลาคม พ.ศ. 2553 ณ กรุงโตเกียว [*UQCC.NET*] แสดงดังรูปที่ 6.3



รูปที่ 6.3 งานแถลงข่าวและสาธิตการทำงานเครือข่ายรหัสลับเชิงควอนตัมของประเทศญี่ปุ่น ณ กรุงโตเกียว ในวันที่ 18 ตุลาคม พ.ศ. 2553

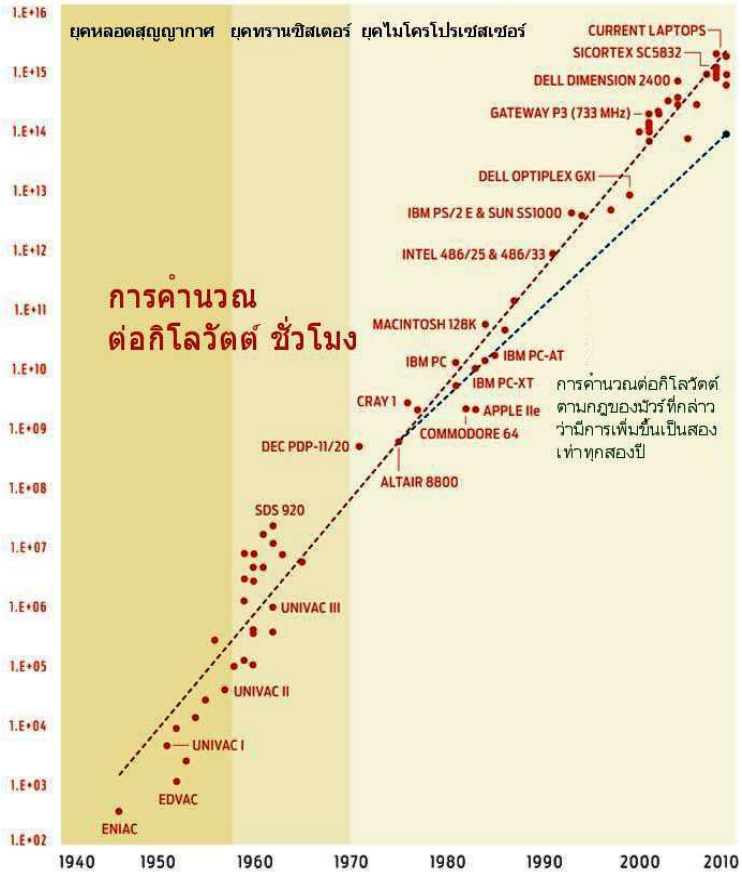
ประเทศสิงคโปร์ได้จัดตั้งศูนย์วิจัยเพื่อทำการวิจัยเกี่ยวกับเทคโนโลยีเชิงควอนตัม ณ มหาวิทยาลัยแห่งชาติประเทศสิงคโปร์ (The National University of Singapore) โดยได้รับงบประมาณ 150 ล้านเหรียญดอลลาร์สิงคโปร์ จาก Research Centre of Excellence (RCE) ในปี พ.ศ. 2550 [*Singapore.net*] ด้วยการลงทุนเชิญนักวิจัยที่มีชื่อเสียงระดับโลกเข้าร่วมงาน และวางแผนการสร้างเครือข่ายสื่อสารด้วยรหัสลับเชิงควอนตัมแรกบนเกาะสิงคโปร์ในอนาคต

ประเทศจีนโดยมหาวิทยาลัยวิทยาศาสตร์และเทคโนโลยี (University of Science and Technology of China: USTC) กลุ่มนักวิจัยได้ทดสอบระบบเครือข่ายวิทยาการรหัสลับเชิงควอนตัมสำหรับหน่วยงานรัฐบาลเพื่อใช้งานจริงสำหรับการเข้ารหัสภาพวีดีโอ เสียง และเอกสารต่างๆ ผ่านเส้นใยแสงที่ใช้ในเชิงพาณิชย์ทั่วไปทั้งหมดสี่โครงข่ายหลักในตัวเมืองอู๋หู มณฑลอานฮุย ประเทศจีน เพื่อเตรียมความพร้อมสำหรับการใช้งานภายในหน่วยงานของรัฐบาล [*Xu และคณะ 2009*]

6.1.3 ภาพรวมงานวิจัยด้านการคำนวณเชิงควอนตัมทั่วโลก

ตามคำทำนายของกอร์ดอน มัวร์ (Gordon E. Moore) ที่รู้จักในชื่อกฎของมัวร์ (Moore's law) สำหรับความก้าวหน้าด้านอุปกรณ์สารกึ่งตัวนำของโลกอิเล็กทรอนิกส์วงจรรวมเพื่อการคำนวณกล่าวว่า จำนวนของทรานซิสเตอร์ในวงจรรวมจะเพิ่มเป็นสองเท่าในช่วงเวลาประมาณ 2 ปี ทว่าบางกรณีกฎนี้ยังไม่แม่นยำพอ แต่เมื่อพิจารณาแทนด้วยประสิทธิภาพของคอมพิวเตอร์ (จำนวนครั้งของการประมวลผลต่อพลังงานที่ให้) กลับพบว่ามีความเป็นเชิงเส้นที่ชัดเจนกว่ากฎของมัวร์ [*Koomey 2010*] อีกทั้งการพิจารณายังไปครอบคลุมถึงการใช้งานหลอดสุญญากาศซึ่งเป็นช่วงที่ยังไม่มีการกำเนิดวงจรรวมด้วย ประสิทธิภาพดังกล่าวแสดงดังรูปที่ 6.4 ซึ่งมีแนวโน้มเพิ่มขึ้นเป็นสองเท่าทุก 1.5 ปี หากแต่ว่าแนวโน้มนี้จะไปถึงทางตันเมื่ออุปกรณ์อิเล็กทรอนิกส์มีขนาดเล็กลงมากจนถึงขนาดที่ทำให้คุณสมบัติเชิงควอนตัมของระบบแสดงผลขึ้นหรือไม่สามารถอธิบายด้วยหลักการเดิมได้ จึงต้องมีการพิจารณาถึงสาขาเทคโนโลยีควอนตัมด้านที่เกี่ยวข้องที่จะเข้ามารองรับการพัฒนาได้ในยุคต่อไป อาทิ อุปกรณ์ระดับควอนตัม (Quantum Devices) รวมทั้งสารสนเทศทั้งรหัสลับและการคำนวณเชิงควอนตัม อันหมายถึงการเตรียมความพร้อมทั้งอุปกรณ์และการใช้งาน

เมื่อพิจารณาจากพื้นฐานการคำนวณเชิงควอนตัม พัฒนาการงานวิจัยการคำนวณแขนงนี้บนพื้นฐานของอุปกรณ์หรือเครื่องมือยุคเริ่มต้นแบบต่างๆ จึงได้รับการสำรวจและนำเสนอ โดยมีกลุ่มและแนวทางวิจัยหลักที่สนใจการคำนวณเชิงควอนตัมจากทั่วโลก แสดงผลดังตารางที่ 6.7 และตารางที่ 6.8



รูปที่ 6.4 ประสิทธิภาพการคำนวณของคอมพิวเตอร์เทียบกับช่วงเวลา *(รูปดัดแปลงจาก [Koomey 2010] นำเสนอใน IEEE Spectrum, vol. 47, issue 3, p. 68, March 2010 ภายไทยโดย IEEE ComSoc Thailand)*

ตารางที่ 6.7 กลุ่มวิจัยทางด้านการคำนวณเชิงควอนตัมด้วยเอ็นเอ็มอาร์ [*Heinrich 2004*]

ผู้นำกลุ่มวิจัย	สถานที่วิจัย
ดี จี โครี และ ที แอฟ ฮาเวิล (D. G. Cory and T. F. Havel)	ภาควิชาวิศวกรรมนิวเคลียร์ สถาบันเทคโนโลยีแมสซาชูเซส (Nuclear Engineering, Massachusetts Institute of Technology : MIT) ประเทศสหรัฐอเมริกา
เอ็น เกอร์เชินฟีเอล และ ไอ เอล เชง (N. Gershenfeld and I. L. Chuang)	ห้องปฏิบัติการทางสารนิเทศ สถาบันเทคโนโลยีแมสซาชูเซส (Media Laboratory, Massachusetts Institute of Technology : MIT) ประเทศสหรัฐอเมริกา
เอส กลาเซอร์ (S. Glaser)	มิวนิค (Munich) ประเทศเยอรมนี
เจ เอ โจนส์ (J. A. Jones)	ออกซ์ฟอร์ด (Oxford) ประเทศอังกฤษ
เจ คิม (J. Kim)	ประเทศเกาหลี
เอ คูมาร์ (A. Kumar)	บังกาลอร์ (Bangalore) ประเทศอินเดีย
อี นีลล์ (E. Knill)	ห้องปฏิบัติการแห่งชาติลอส อลามอส (Los Alamos National Laboratory : LANL) ประเทศสหรัฐอเมริกา
อาร์ เลฟเฟลม์ม (R. Laflamme)	วอเทอร์ลู (Waterloo) ประเทศแคนาดา
เจิง (Zeng)	ประเทศจีน

ตารางที่ 6.8 กลุ่มวิจัยทางด้านการคำนวณเชิงควอนตัมด้วยการกักไอออน [*Heinrich 2004*]

ผู้นำกลุ่มวิจัย	สถานที่วิจัย	งานวิจัยที่เน้น (อะตอมที่นำมากัก)
ดี เบร์กแลนด์ (D. Berkeland)	ห้องปฏิบัติการแห่งชาติลอส อลามอส (Los Alamos National Laboratory : LANL) ประเทศสหรัฐอเมริกา	Sr+
อาร์ บลาตต์ (R. Blatt)	มหาวิทยาลัยอินซ์บรูค (University of Innsbruck) ประเทศออสเตรีย	Ca+
อาร์ เดอโว (R. Devoe)	ศูนย์วิจัยไอบีเอ็มอัลมาเดน (IBM Almaden Research Center) ประเทศสหรัฐอเมริกา	Ba+
เอ็ม ดรูเซนน์ (M. Drewsen)	ออร์ฮูส (Aarhus) ประเทศเดนมาร์ก	Ca+
พี กิลล์ (P. Gill)	ห้องปฏิบัติการวิจัยทางกายภาพแห่งชาติ เทดด์ดิงตัน (National Physical Lab (NPL), Teddington) ประเทศอังกฤษ	Sr+
บี คิง (B. King)	มหาวิทยาลัยแมคมาสเตอร์ แฮมินตัน ออนทาริโอ (McMaster University, Hamilton, Ontario) ประเทศแคนาดา	Mg+
ซี มอนโร (C. Monroe)	มหาวิทยาลัยแมรีแลนด์ (University of Maryland) ประเทศสหรัฐอเมริกา	Cd+
เอ สทีน (A. Steane)	ออกซ์ฟอร์ด (Oxford) ประเทศอังกฤษ	Ca+
ซี วุนเดอร์ลิช (C. Wunderlich)	ฮัมบูกก์ (Hamburg) ประเทศเยอรมนี	Yb+
เอช ไวล์เทอร์ (H. Walther)	สถาบันแมกซ์พลังค์ (Max-Planck Institute, Garching) ประเทศเยอรมนี	Mg+, In+
ดี ไวน์แลนด์ (D. Wineland)	สถาบันทางมาตราฐานและเทคโนโลยีแห่งชาติ โบล์เดอร์ (National Institute of Standard and Technology : NIST, Boulder) ประเทศสหรัฐอเมริกา	Be+, Mg+

นอกจากมหาวิทยาลัย และสถาบันวิจัยต่างๆ ดังตารางที่ 6.7 และ 6.8 แล้วบริษัท D Wave Systems สัญชาติแคนาดา ทุ่มเทวิจัยคอมพิวเตอร์เชิงควอนตัมเพื่อให้สามารถใช้งานได้จริง ได้ทำการทดสอบใช้งานเครื่องคอมพิวเตอร์เชิงควอนตัมที่ได้รับการพัฒนาขึ้นด้วยเงินทุนวิจัย 65 ล้านดอลลาร์สหรัฐ โดยทางบริษัทอ้างว่ากำลังทดสอบเครื่องคอมพิวเตอร์เชิงควอนตัมที่มีหน่วยประมวลผล 128 บิต จำนวนสามเครื่อง และต่อไปจะนำเครื่องดังกล่าวไปติดตั้งตามสถาบันต่างๆ เพื่อใช้ในงานวิจัย โดยโครงการนี้ได้รับผู้ร่วมงานจากองค์กรระดับโลกอย่าง Google และ NASA ซึ่งในที่สุดประสงค์จะพัฒนาให้เป็นศูนย์วิจัยเทคโนโลยีเชิงควอนตัมระดับโลก [*Guizzo 2010*]

มีการรายงานจากการที่บริษัท D Wave System พัฒนาเครื่องคอมพิวเตอร์เชิงควอนตัม ทำให้ Google ซึ่งเป็นผู้ให้บริการเวปไซต์สำหรับการสืบค้นข้อมูล ได้เล็งเห็นว่าคอมพิวเตอร์เชิงควอนตัมจะมีศักยภาพในการประมวลผลที่รวดเร็วขึ้นมากอันจะทำให้เกิดการสืบค้นข้อมูลในรูปแบบใหม่นั่นคือการสืบค้นด้วยรูปภาพแทนการสืบค้นจากประโยคตามมาได้ ซึ่งต้องอาศัยการ

คำนวณเพื่อแยกรูปภาพต่างๆ อย่างรวดเร็วเพียงพอมากกว่าการคำนวณด้วยคอมพิวเตอร์แบบปกติ [*Marks 2009*]

ทว่า การทำงานของคอมพิวเตอร์เชิงควอนตัมของบริษัท D Wave System ถูกตั้งข้อสังเกตโดยผู้เชี่ยวชาญว่า ไม่ได้แสดงคุณสมบัติเพียงพอที่จะเป็นคอมพิวเตอร์เชิงควอนตัมโดยสมบูรณ์ อีกทั้งทางบริษัทยังไม่ได้คำนึงถึงการควบคุมการเกิดสัญญาณรบกวนที่จะทำลายสถานะเชิงควอนตัม ซึ่งต้องมีการตรวจสอบข้อเท็จจริง [*Guizzo 2010*] เชิงวิทยาศาสตร์โดยลำดับต่อไป

6.2 พัฒนาการงานวิจัยด้านการสื่อสารและการคำนวณเชิงควอนตัมของประเทศไทย

งานวิจัยทางด้านการสื่อสารเชิงควอนตัมยังคงเป็นสาขาที่ใหม่ และมีผู้สนใจน้อยมากเช่นเดียวสาขาอุบัติใหม่อื่นๆ เนื่องจากต้องใช้งบประมาณสูง บุคลากรที่เกี่ยวข้องยังมีไม่เพียงพอ กอปรนโยบายการพัฒนาที่ยังคงต้องได้รับการผลักดันอย่างมาก และอื่นๆ เพื่อให้ประเทศไทยสามารถรองรับเทคโนโลยีสาขาใหม่นี้ได้ทันเวลา ลดการเสียเปรียบหรือเพิ่มโอกาสการแข่งขันทั้งด้านทางเศรษฐกิจ สังคม และการศึกษา จึงได้มีผลสำรวจเบื้องต้นและกิจกรรมอื่นๆ เพื่อวัตถุประสงค์ดังกล่าว โดยการศึกษาจากของต่างประเทศที่เกี่ยวข้อง จากประสบการณ์ของเทคโนโลยีแขนงใหม่อื่นๆในอดีต และจากทีมงานพัฒนานโยบายวิทยาศาสตร์และเทคโนโลยี ทยอยเริ่มดำเนินการมาโดยลำดับ เช่น โดยช่วงต้นของการดำเนินการของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ มีภารกิจหลักคือการวิจัยและพัฒนาระบบวิทยาการรหัสลับเชิงควอนตัม และติดตามความก้าวหน้าเทคโนโลยีการคำนวณเชิงควอนตัม ได้มีการจัดทำแผนที่นำทางเทคโนโลยีสำหรับประเทศไทย โดยดำเนินการนำเสนอจัดตั้งศูนย์กลางการอบรม วิจัย และพัฒนาวิทยาการรหัสลับเชิงควอนตัม (Testbed) เพื่อการใช้งาน ตรวจสอบ ทดสอบ ให้บริการปรึกษาของภาครัฐ เอกชน และภาควิชาการ เป็นต้น รวมทั้งการสร้างความร่วมมือกับหลายหน่วยงานในระดับนานาชาติ ดังเช่น

6.2.1 ประเทศญี่ปุ่น

สำนักงานเทคโนโลยีสารสนเทศและการสื่อสารแห่งประเทศญี่ปุ่น (National Institute of Information and Communications Technology : NICT) ประเทศญี่ปุ่น โดยกลุ่มวิจัย Quantum ICT Group (QICT) มีความร่วมมือในเรื่องการถ่ายทอดเทคโนโลยีด้านสารสนเทศเชิงควอนตัมผ่านอากาศ เพื่อเตรียมการกับแนวโน้มอนาคต เช่น การใช้งานดาวเทียมที่มีโมดูลการสื่อสารเชิงแสง เพื่อใช้สำหรับทดสอบการรับ-ส่งข้อมูลในงานวิจัยระบบวิทยาการรหัสลับเชิงควอนตัม และการแลกเปลี่ยนองค์ความรู้ในด้านรหัสแก้ไขความผิดพลาดสำหรับการสื่อสาร เป็นต้น

6.2.2 ประเทศสวิต

บริษัท id Quantique ซึ่งเป็นเป็นบริษัทที่จำหน่ายอุปกรณ์ด้านโฟโตนิกส์เชิงควอนตัม (Quantum photonics) ที่ใช้ในเครือข่ายความปลอดภัย โดยมีการลงนามบันทึกข้อตกลงความร่วมมือ และจะมีการร่วมพัฒนาโปรแกรมการกระจายกุญแจรหัสลับเชิงควอนตัม

6.2.3 ประเทศออสเตรเลีย

บริษัท Senetas ประเทศออสเตรเลีย ซึ่งเป็นบริษัทที่พัฒนาด้านการเข้ารหัสลับสำหรับเครือข่ายการสื่อสารปลอดภัยและผลิตอุปกรณ์สำหรับการเข้ารหัสลับ มีการลงนามบันทึกข้อตกลงความร่วมมือในการร่วมพัฒนาเครื่องเข้ารหัสลับสำหรับเครือข่ายการสื่อสารก้าวหน้าและปลอดภัยและการพัฒนาบุคลากร

6.2.4 ประเทศออสเตรีย

สถาบันเทคโนโลยีแห่งออสเตรีย (Austrian Institute of Technology : AIT) ประเทศออสเตรีย ซึ่งเป็นสถาบันวิจัยของรัฐบาลดำเนินการวิจัยและพัฒนาสหสาขาที่ใกล้เคียง (Foresight & Policy Development, Health & Environment, Safety & Security, Mobility และ Energy) ได้มีการลงนามบันทึกข้อตกลงความร่วมมือในการวิจัยและศึกษาเทคโนโลยีสารสนเทศเชิงควอนตัม

สถาบันทัศนศาสตร์เชิงควอนตัมและสารสนเทศเชิงควอนตัม (Institute for Quantum Optics and Quantum Information :

IQOQI) ประเทศออสเตรีย ซึ่งแบ่งงานวิจัยออกเป็น 2 กลุ่ม ได้แก่ กลุ่มที่เมืองอินส์บรุค (Section Innsbruck) และกลุ่มที่เมืองเวียนนา (Section Vienna) เพื่อดำเนินการวิจัยและทดลองด้านสารสนเทศเชิงควอนตัม (Quantum Information) และด้านทัศนศาสตร์ควอนตัม (Quantum Optic) ซึ่งกลุ่มที่เวียนนานำโดย อันตัน ไซลิงเงอร์ (Prof.Anton Zeilinger) เริ่มมีความร่วมมือในการแลกเปลี่ยนดูงานวิจัยและพัฒนาบุคลกร

6.3 วิเคราะห์ทิศทางงานวิจัยด้านเทคโนโลยีสารสนเทศเชิงควอนตัม

ภาพรวมของโลกงานวิจัยทางด้านเทคโนโลยีสารสนเทศเชิงควอนตัม เริ่มต้นมุ่งเน้นไปที่ระบบวิทยาการรหัสลับเชิงควอนตัมและการคำนวณเชิงควอนตัม สำหรับแนวทางงานวิจัยด้านเทคโนโลยีสารสนเทศเชิงควอนตัมในประเทศไทยที่ได้เริ่มดำเนินการเป็นความร่วมมือระหว่างสถาบันการศึกษา และหน่วยงานวิจัยต่างๆ รวมถึงบริษัทที่จำหน่ายเครื่องมือที่มีความเกี่ยวข้องกับระบบวิทยาการรหัสลับเชิงควอนตัม ทั้งภายในและต่างประเทศ มีแนวทางการวิจัยเน้นหนักไปที่เทคโนโลยีระบบวิทยาการรหัสลับเชิงควอนตัมในช่วงแรกและมีภาพรวมแนวโน้มการพัฒนาดังตารางที่ 6.9

ตารางที่ 6.9 แนวโน้มเทคโนโลยีการรักษาความปลอดภัยการสื่อสารยุคหน้าสำหรับประเทศไทย (ข้อมูลเพื่อการพิจารณาสำหรับแผนแม่บท ICT ของประเทศ โดย *ห้องปฏิบัติการวิจัย OQC/ เนคเทค - 2009*)

เทคโนโลยี	1-2 ปี (ค.ศ.2009 - 2010)	3-5 ปี (ค.ศ.2011 – 2012)	เกิน 5 ปี (ค.ศ.2013 ->)
เทคโนโลยีพื้นฐาน	• เทคโนโลยีพื้นฐาน (ลดทอนแสงจนได้โฟตอนเดี่ยว)	• การใช้งานแหล่งกำเนิดโฟตอนเดี่ยว • การใช้งานแหล่งกำเนิดคู่โฟตอนพัวพัน (Entangled photon)	
วิทยาการรหัสลับเชิงควอนตัม (Quantum Cryptography)	• กรอบความคิดศูนย์กลางการอบรม วิจัย และพัฒนาระบบวิทยาการรหัสลับเชิงควอนตัม (Testbed & Training Center) • ทดสอบระบบโครงข่ายต้นแบบของระบบวิทยาการรหัสลับเชิงควอนตัมระดับปฏิบัติการเพื่อทดสอบและเผยแพร่ความรู้ เพิ่มความตระหนักให้ผู้ใช้และสังคม • การสร้างความร่วมมือทั้งในและต่างประเทศเพื่อรับการถ่ายทอดเทคโนโลยี	• โครงข่ายระหว่างหน่วยงานเพื่อทดสอบระบบรหัสลับเชิงควอนตัมภาคสนาม • กลุ่มความเชี่ยวชาญเฉพาะทางระหว่างภาครัฐ ภาคการศึกษา และเอกชนผู้เกี่ยวข้องกับเครือข่ายความปลอดภัยสูง • ต้นแบบระดับภาคสนามเพื่อพัฒนาเทคโนโลยีพื้นฐานในประเทศ	• ศูนย์เชี่ยวชาญด้านความปลอดภัยของเครือข่ายด้วยรหัสลับเชิงควอนตัม (Center of Excellence) • เครือข่ายสื่อสารด้วยวิทยาการรหัสลับเชิงควอนตัมเพื่อการใช้งานทั่วไป ตรวจสอบ ทดสอบและให้บริการปรึกษาของภาครัฐ เอกชน และภาควิชาการ

บทสรุป

งานวิจัยด้านการสื่อสารและการคำนวณเชิงควอนตัมสามารถแบ่งได้เป็นสองส่วน คือการสื่อสารเชิงควอนตัมและการคำนวณเชิงควอนตัม เทคโนโลยีรหัสลับเชิงควอนตัมซึ่งเป็นส่วนหนึ่งของการสื่อสารเชิงควอนตัมนั้นมีการพัฒนาจนกระทั่งสามารถประยุกต์เพื่อใช้งานได้จริงและมีการใช้งานเชิงพาณิชย์ โดยเน้นที่การกระจายกุญแจลับเชิงควอนตัมให้มีความเหมาะสมในการใช้งาน และพัฒนาเป็นการสื่อสารเชิงควอนตัมรูปแบบอื่นๆ ต่อไปในอนาคต ส่วนงานวิจัยระดับสูงจะเป็นการวิจัยด้านการคำนวณเชิงควอนตัมที่อยู่ระหว่างการค้นคว้าทั่วโลกเพื่อหาแนวทางที่เหมาะสมโดยลำดับ

พื้นฐานสำหรับงานวิจัยทางด้านการกระจายกุญแจลับเชิงควอนตัมสามารถแบ่งตามวิธีการสร้างอุปกรณ์ได้เป็นห้าประเภท ประกอบด้วย การสื่อสารด้วยแหล่งกำเนิดแสงเลเซอร์ชนิดพัลส์ผ่านเส้นใยแสงและผ่านตัวกลางอากาศ การสื่อสารด้วยแหล่งกำเนิดโฟตอนเดี่ยว การสื่อสารด้วยแหล่งกำเนิดคู่โฟตอนพัวพัน และการสื่อสารด้วยสถานะควอนตัมแบบต่อเนื่อง ซึ่งทั้งหมดล้วนใช้โฟตอนเป็นสื่อในการสร้างระบบเชิงควอนตัมทั้งสิ้น ความก้าวหน้าของงานวิจัยทางด้านนี้จะกระจายอยู่ภายในประเทศที่มีเทคโนโลยีแนวหน้าทั่วโลก ทั้งทวีปยุโรป อเมริกาและเอเชีย

ด้านงานวิจัยสำหรับการคำนวณเชิงควอนตัมนั้น มีวิธีสร้างควอนตัมคอมพิวเตอร์ได้หลายแบบ แต่ยังไม่พบวิธีที่ดีที่สุด แม้ว่างานวิจัยด้านนี้ยังไม่มีแนวโน้มว่าจะใช้ได้อย่างแพร่หลายในเวลาอันใกล้ แต่ควอนตัมคอมพิวเตอร์ได้รับการคาดการณ์ถึงศักยภาพที่สูงมากในการแก้ปัญหาบางอย่างที่มีความซับซ้อน และจะมีประสิทธิภาพมากกว่าคอมพิวเตอร์แบบดั้งเดิมมาก นอกจากนี้ยังมีต้นแบบควอนตัมคอมพิวเตอร์ที่แสดงให้เห็นว่าแนวคิดด้านการคำนวณเชิงควอนตัมสามารถใช้ได้จริง ตั้งแต่ปีค.ศ. 2004 นักวิจัยทั่วโลกค้นพบรวมวิธีหลักๆของการสร้างวิธีคำนวณเชิงควอนตัมได้ห้าหลักการ ได้แก่ การคำนวณเชิงควอนตัมการสั่นพ้องแม่เหล็กนิวเคลียร์ การคำนวณเชิงควอนตัมโดยไอออนที่ถูกกัก การคำนวณเชิงควอนตัมด้วยสถานะของแสง การคำนวณเชิงควอนตัมโดยอะตอนที่เป็นกลาง และการคำนวณเชิงควอนตัมด้วยควอนตัมดอท

ส่วนงานวิจัยทางด้านการสื่อสารและการคำนวณเชิงควอนตัมภายในประเทศไทยยังอยู่ในช่วงเริ่มต้นที่ต้องอาศัยความร่วมมือกันระหว่างสถาบันวิจัยและสถาบันการศึกษา รวมถึงการสร้างความร่วมมือกับสถาบันวิจัยและบริษัทจากต่างประเทศ เช่นเดียวสาขาอุบัติใหม่อื่นๆ เนื่องจากต้องใช้งบประมาณสูง บุคลากรจำนวนมาก และนโยบายการพัฒนาที่ยังคงต้องได้รับการผลักดันและประเด็นสำคัญอื่นๆ เพื่อให้ประเทศไทยสามารถรองรับเทคโนโลยีสาขาใหม่นี้ได้ทันเวลา ลดการเสียเปรียบหรือเพิ่มโอกาสการแข่งขันทั้งด้านทางเศรษฐกิจ สังคม และการศึกษาได้ต่อไป

เอกสารอ้างอิง

[Election.NET] P. Marks, "Quantum cryptography to protect Swiss election," *NewScientist.com,* October 2007. **[**Online]. Available: http://www.newscientist.com/article/dn12786. [Accessed: January 2009]

[Elliott และคณะ 2005] C. Elliott, et al., "Current status of the DARPA Quantum Network," in *Proceedings SPIE The International Society for Optical Engineering*, 2005.

[Guizzo 2010] E. Guizzo, "Does not Quantum Compute," *IEEE Spectrum,* vol. 47, issue 1, pp. 42-43, January 2010.

[Heinrich 2004] T. Hughes, et al., "A quantum information science and technology roadmap," April 2004. [Online]. Available: http://qist.lanl.gov/ [Accessed: December, 2009].

[Koomey 2010] J. G. Koomey, "Outperforming Moore's Law," *IEEE Spectrum*, vol. 47, issue 3, p. 68, March 2010.

[Marks 2009] P. Marks, "Google demonstrates quantum computer image search," *New Scientist*, December 2009.

[NICT.NET] *National Institute of Information and Communications Technology,* **[**Online]. Available: http://www.nict.go.jp/about/mission_e.html. [Accessed: January 2009]

[OQC.NET] *Optical and Quantum Communications laboratory,* [Online]. Available: http://www.nectec.or.th/Optical&Quantum/. [Accessed: June 30, 2010]

[Peev และคณะ 2009] M. Peev, et al., "The SECOQC quantum key distribution network in Vienna," *New J. Phys.,* vol. 11, 2009.

[RAND.NET] "The Global Technology Revolution 2020, Executive Summary," *RAND Corporation,* [Online]. Available: http:// www.rand.org/pubs/monographs/MG475/ [Accessed: December 2009].

[Schmitt-Manderbach และคณะ 2007] T. Schmitt-Manderbach, et al., "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Phys. Rev. Lett.,* vol. 98, p. 010504, 2007.

[Singapore.net] "Annual report 2008," *National university of Singapore,* 2008. [Online]. Available: www.quantumlah.org/media/ presentation/annualreport2008.pdf. [Accessed: June 30, 2010]

[UQCC.NET] "Updating Quantum Cryptography and Communications 2010," *UQCC2010*, [Online]. Available: http://www.uqcc2010.org/index.html [Accessed: October 2010]

[Ursin และคณะ 2007] R. Ursin, et al., "Entanglement-based quantum communication over 144 km," *Nature Physics,* vol. 3, pp. 481 – 486, 2007.

[Xu และคณะ 2009] F. Xu, et al., "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chinese Science Bulletin,* vol. 54, no. 17, pp. 2991 – 2997, September 2009.

ดำถามท้ายบทที่ 6 (Questions and Answers)
และอภิปราย (Discussions) ปรับปรุง ณ
Blog: http://www.stks.or.th/blog/?p=14123

ภาคผนวก ก
พีชคณิตเชิงเส้นโดยสังเขป
(An introduction of linear algebra)

ก.1 ภาพรวม

พีชคณิตเชิงเส้น (linear algebra) เป็นคณิตศาสตร์ที่อธิบายสิ่งต่างๆ มีคุณลักษณะเชิงเส้น ความรู้จากพีชคณิตเชิงเส้นนี้นำไปประยุกต์ในการแก้ปัญหาระบบสมการเชิงเส้น และระบบสมการเชิงอนุพันธ์เชิงเส้น รวมทั้งปัญหาอื่นๆ ที่เป็นเชิงเส้น แต่ในที่นี้เน้นเฉพาะพีชคณิตเชิงเส้นที่สามารถนำมาประยุกต์ในสารสนเทศและการคำนวณเชิงควอนตัม โดยสิ่งที่นำมาใช้คือเวกเตอร์ในปริภูมิฮิลเบิร์ต (Hilbert spaces) ซึ่งใช้แทนสถานะควอนตัมทั้งหลายรวมไปถึงควอนตัมบิต และเรื่อง inner product ที่กำหนดค่าของ projection อันทำให้ทราบความน่าจะเป็นที่สถานะควอนตัมหนึ่งจะเปลี่ยนไปสู่สถานะหนึ่ง หรือบอกว่าความน่าจะเป็นที่ผลการวัดค่าจะเป็นค่าหนึ่ง โดยที่สถานะที่เข้ามาเป็นอีกค่าหนึ่ง เป็นต้น และจากการที่สมการชเรอดิงเงอร์ (Schrödinger's equation) ที่อธิบายการเปลี่ยนแปลงทางควอนตัมนั้น มีลักษณะเป็นเชิงเส้น กระบวนการทางพีชคณิตเชิงเส้นทั้งหลายจึงสามารถนำมาใช้อธิบายกลศาสตร์ควอนตัม รวมถึงสารสนเทศและการคำนวณทางควอนตัมได้

คุณสมบัติเชิงเส้น (linearity หรือ superposition)

การแปลง (transformation หรือ mapping) T: *V*--> *W* จากปริภูมิเวกเตอร์หนึ่งไปยังอีกปริภูมิเวกเตอร์หนึ่ง มีคุณสมบัติเชิงเส้น (linear) ก็ต่อเมื่อ $T(\vec{x}+\vec{y})=T(\vec{x})+T(\vec{y})$ และ $T(a\vec{x})=a\,T(\vec{x})$ โดยที่ $\vec{x}$ และ $\vec{y}$ เป็นเวกเตอร์ใด ๆ บนปริภูมิเวกเตอร์ *V* และ *a* เป็นปริมาณสเกลาร์ซึ่งนิยามบนปริภูมิเวกเตอร์นั้น

ก.2 เวกเตอร์

สิ่งที่เป็น object สำหรับการพิจารณาในพีชคณิตเชิงเส้น เรียกว่า เวกเตอร์ (vector) ซึ่งเป็นสมาชิกของเซตที่เรียกว่า ปริภูมิเวกเตอร์ (vector space) โดยเวกเตอร์ในที่นี้ มีความหมายกว้างกว่าเวกเตอร์ที่ชี้ใน 1 มิติ 2 และ 3 มิติ ซึ่งเป็นที่คุ้นเคยในการเรียนการสอนฟิสิกส์เรื่อง แรง ความเร็ว และความเร่ง เป็นต้น (เวกเตอร์ดังกล่าวถือเป็นชนิดหนึ่งตามความหมายของพีชคณิตเชิงเส้น) เวกเตอร์ในความหมายกว้างนั้น รวมไปถึง เมทริกซ์ ฟังก์ชันเชิงเส้น และอื่นๆ ที่สอดคล้องกับคุณสมบัติในนิยาม หรือ axioms เช่น ความมีอินเวอร์ส เป็นต้น

ปริภูมิเวกเตอร์ที่ใช้ในการคำนวณและสารสนเทศควอนตัม จะเป็นปริภูมิเวกเตอร์เชิงซ้อน (Complex vector space) โดยเวกเตอร์ที่อยู่ในปริภูมินี้ เรียกว่า เวกเตอร์เชิงซ้อน (complex vectors) แทนได้ด้วย

$$\begin{pmatrix} z_1 \\ z_2 \\ \cdot \\ \cdot \\ \cdot \\ z_n \end{pmatrix} \qquad \text{.....(ก.1)}$$

โดยที่ $z_1, z_2, \ldots, z_n$ เป็นจำนวนเชิงซ้อน และ *n* เป็นจำนวนมิติของปริภูมิเวกเตอร์นี้ (สำหรับคิวบิต *n*=2) และนิยามการบวกเวกเตอร์มีว่า

$$\begin{pmatrix} z_1 \\ z_2 \\ \cdot \\ \cdot \\ \cdot \\ z_n \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{pmatrix} = \begin{pmatrix} z_1 + w_1 \\ z_2 + w_2 \\ \cdot \\ \cdot \\ \cdot \\ z_n + w_n \end{pmatrix} \qquad \text{.....(ก.2)}$$

และการคูณด้วยสเกลาร์ (จำนวนเชิงซ้อน) นิยามว่า

$$\alpha \begin{pmatrix} z_1 \\ z_2 \\ \cdot \\ \cdot \\ \cdot \\ z_n \end{pmatrix} = \begin{pmatrix} \alpha z_1 \\ \alpha z_2 \\ \cdot \\ \cdot \\ \cdot \\ \alpha z_n \end{pmatrix} \quad \text{โดยที่} \quad \alpha \quad \text{เป็นจำนวนเชิงซ้อน} \qquad \text{.....(ก.3)}$$

เวกเตอร์แนวตั้ง หรือ เมทริกซ์ $n \times 1$ นี้ จะมีคู่ (dual vector) ของมันซึ่งเป็นคู่คอนจูเกตกัน เป็นเวกเตอร์แนวนอน หรือ เมทริกซ์ $1 \times n$ นิยามว่า

ถ้า $\vec{z} = \begin{pmatrix} z_1 \\ z_2 \\ \cdot \\ \cdot \\ \cdot \\ z_n \end{pmatrix}$ แล้ว คู่ (dual vector) ของ $\vec{z}$ จะมีค่าเท่ากับ $(z_1^*, z_2^*, \ldots, z_n^*)$

โดยเครื่องหมาย " * " หมายถึง complex conjugate ถ้า $z_1 = a + bi$ จะได้ว่า $z_1^* = a - bi$ โดยที่ $i = \sqrt{-1}$

ในกลศาสตร์ควอนตัมสถานะจะแทนด้วยสัญลักษณ์ $|\psi\rangle$ โดยที่ ψ แทนชื่อเรียก (label) และ $|\cdot\rangle$ แทนการบอกว่าสิ่งนี้เป็นเวกเตอร์ หรือ สิ่งนี้เป็นสัญลักษณ์ ซึ่งเป็นสัญลักษณ์ที่มีความหมายกว้าง แทนสถานะของระบบนั้น $|\psi\rangle$ สามารถแสดงได้ในรูปผลรวมเชิงเส้นของสถานะฐาน (basis states)

$$|\psi\rangle = \int_{-\infty}^{\infty} a_{(x)} |x\rangle \, dx \quad \text{สำหรับสถานะต่อเนื่อง (มิติเป็นอนันต์) และ}$$

$$|\psi\rangle = \sum_{0}^{n-1} a_i |i\rangle \quad \text{สำหรับสถานะไม่ต่อเนื่อง (มิติ n)}$$

โดยที่ x มีค่าเป็นจำนวนจริง และ i มีค่าเป็นจำนวนเต็มตั้งแต่ 0 ถึง $n-1$ อนึ่ง ในการคำนวณและการสารสนเทศทางควอนตัม สถานะที่ใช้จะเป็นสถานะไม่ต่อเนื่องเท่านั้น (เช่น $|0\rangle$ และ $|1\rangle$ รวมกันเชิงเส้น เรียกว่า คิวบิต) และสำหรับสถานะไม่ต่อเนื่อง $|\psi\rangle$ อยู่ในรูปสัมประสิทธิ์ของมันเพียงอย่างเดียว เช่น

$$|\psi\rangle \equiv \begin{pmatrix} a_0 \\ a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_{n-1} \end{pmatrix} \quad \text{หมายความว่า} \quad |\psi\rangle = a_0|0\rangle + a_1|1\rangle + \ldots + a_{n-1}|n-1\rangle$$

เวกเตอร์แนวตั้ง แทนด้วย $|\psi\rangle$ และเวกเตอร์แนวนอนซึ่งเป็นคู่กัน (dual) กับเวกเตอร์ดังกล่าว เป็นเวกเตอร์แนวนอน แทนด้วย $\langle\psi|$ โดยที่

$$|\psi\rangle = (a_0^*, a_1^*, \ldots, a_{n-1}^*)$$

เวกเตอร์ $\langle\cdot|$ เรียกอีกอย่างว่า "bra" และเวกเตอร์ $|\cdot\rangle$ เรียกว่า "ket" หากนำมาเรียงต่อกันจะเป็นสัญลักษณะ $\langle\cdot|\cdot\rangle$ เรียกว่า

“bracket” จะหมายถึงการนำเวกเตอร์สองตัวมาดำเนินการ inner product กัน โดย พอล ดิแรก (Paul Dirac) เป็นผู้เสนอสัญลักษณ์เหล่านี้ไว้ในการอธิบายกลศาสตร์ควอนตัม

นิยาม inner product

inner product หรือ scalar product หรือ dot product ระหว่างเวกเตอร์สองตัว $|\psi\rangle$ และ $|\varphi\rangle$ แทนด้วย $(|\psi\rangle,|\varphi\rangle)$ หรือ $\langle\psi|\varphi\rangle$ หรือ $\vec{\psi}\cdot\vec{\varphi}$ ตามสัญลักษณ์ของเวกเตอร์ที่แทนด้วยลูกศร สัญลักษณ์เหล่านี้มีความหมายเหมือนกัน แต่ในกลศาสตร์ควอนตัม มักใช้สัญลักษณ์ bracket $\langle\cdot|\cdot\rangle$

สำหรับเวกเตอร์ $|\psi\rangle=\begin{pmatrix} a_0 \\ a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_{n-1} \end{pmatrix}$ และ $|\varphi\rangle=\begin{pmatrix} b_0 \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_{n-1} \end{pmatrix}$ inner product ระหว่าง $|\psi\rangle$ และ $|\varphi\rangle$ นิยามว่า

$$\langle\psi|\varphi\rangle=(a_0^* \quad a_1^* \quad \ldots \quad a_{n-1}^*)\begin{pmatrix} b_0 \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_{n-1} \end{pmatrix} \qquad \text{.....(ก.4)}$$

$$=a_0^* b_0+a_1^* b_1+\ldots+a_{n-1}^* b_{n-1}$$

คุณสมบัติของ Inner product

- *ความเป็นบวก (possitivity)* $\langle\psi|\psi\rangle\geqslant 0$ *และเท่ากับศูนย์ก็ต่อเมื่อ* $|\psi\rangle=0$
- *skew symmetry* $\langle\psi|\varphi\rangle=\langle\varphi|\psi\rangle^*$
- *ความเป็นเชิงเส้น (linearity)* $\langle\psi|(a|\varphi_1\rangle+b|\varphi_2\rangle)=a\langle\psi|\varphi_1\rangle+b\langle\psi|\varphi_2\rangle$

ความสำคัญของ Inner product

ความสำคัญ	**สัญลักษณ์ bra และ ket**	**สัญลักษณ์แบบลูกศร**
นิยามขนาดของเวกเตอร์	$\|\|\|\psi\rangle\|\|=\sqrt{\langle\psi\|\psi\rangle}$	$\|\vec{A}\|=\sqrt{\vec{A}\cdot\vec{A}}$
นิยามมุมระหว่างเวกเตอร์[ก.1]	$\langle\psi\|\varphi\rangle=\|\|\psi\rangle\|\|\|\varphi\rangle\|\|\cos\theta$	$\vec{A}\cdot\vec{B}=\|\vec{A}\|\|\vec{B}\|\cos\theta$
นิยามความตั้งฉาก (orthogonality)	$\|\psi\rangle$ และ $\|\varphi\rangle$ ตั้งฉากกันก็ต่อเมื่อ $\langle\psi\|\varphi\rangle=0$	$\vec{A}$ และ $\vec{B}$ ตั้งฉากกันก็ต่อเมื่อ $\vec{A}\cdot\vec{B}=0$
นิยามโปรเจกชันของเวกเตอร์หนึ่ง ไปยังอีกเวกเตอร์หนึ่ง	โปรเจกชันของ $\|\psi\rangle$ บน $\|\varphi\rangle$ เท่ากับ $\frac{\langle\psi\|\varphi\rangle}{\|\|\varphi\rangle\|}$	โปรเจกชันของ $\vec{A}$ บน $\vec{B}$ เท่ากับ $\frac{\vec{A}\cdot\vec{B}}{\|\vec{B}\|}$

[ก.1] เนื่องจาก inner product มีค่าเป็นจำนวนเชิงซ้อน ดังนั้นมุม θ ที่ได้จะเป็นมุมในเชิงนามธรรม ซึ่งเป็นจำนวนเชิงซ้อน

ในกลศาสตร์ควอนตัม ความน่าจะเป็นที่สถานะหนึ่งจะเปลี่ยนไปเป็นอีกสถานะหนึ่ง (transition probability) แสดงได้ในรูป $Prob(a \rightarrow b) = |\langle b|a\rangle|^2$ หรือความน่าจะเป็นที่ผลการวัดสถานะจะออกมาเป็น $|0\rangle$ เมื่อสถานะที่เข้ามาเป็น $|\psi\rangle$ อยู่ในรูป $Prob(\psi \rightarrow 0) = P(0|\psi) = |\langle 0|\psi\rangle|^2$ เช่น $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ ความน่าจะเป็นที่สถานะจะถูกวัดออกมาเป็น $|0\rangle$ เท่ากับ $P(0|\psi) = |\langle 0|\psi\rangle|^2 = |\langle 0|(|\psi\rangle)|^2 = |\frac{1}{\sqrt{2}}\langle 0|0\rangle + \frac{1}{\sqrt{2}}\langle 0|1\rangle|^2 = \frac{1}{2}$ เนื่องจาก $\langle 0|1\rangle = 0$ เพราะ $|0\rangle$ และ $|1\rangle$ ตั้งฉากกัน

สัญลักษณ์ bra-ket นี้มีประโยชน์อีกประการหนึ่งคือ การที่เชื่อมโยงกับ conditional probability $P(0|\psi)$ ได้อย่างไม่สับสน

#----------#

ภาคผนวก ข
ทฤษฎีสารสนเทศ
(Information Theory)

ทฤษฎีสารสนเทศ (Information Theory) เสนอไว้ตั้งแต่ ค.ศ. 1948 โดย โคลด แชนนอน (Claude Shannon) ซึ่งถือได้ว่าเป็นบิดาของวิชาแขนงนี้ ทฤษฎีนี้ตอบปัญหาหลัก ๆ ของการสื่อสาร ได้แก่

ข.1 อัตราการบีบอัดสูงสุดที่ยังคงกู้ข้อมูลกลับคืนได้โดยสมบูรณ์นั้น คือเท่าใด (ไม่สามารถบีบอัดข้อความได้เล็กไปกว่าปริมาณสารสนเทศ (entropy) ของข้อความนั้น)

ข.2 อัตราการส่งสัญญาณสูงสุดผ่านช่องสัญญาณที่มีสัญญาณรบกวนเป็นเท่าใด (อัตราการส่งต้องไม่เกินค่าความจุของช่องสัญญาณ (channel capacity) เพื่อให้มีรหัสควบคุมความผิดพลาดที่ทำให้ความผิดพลาดลดเหลือน้อยเพียงใดก็ได้)

แชนนอนได้นิยามปริมาณสารสนเทศไว้ว่า $I_x = \log_2 \frac{1}{p_x}$ มีหน่วยเป็น บิต ซึ่งเป็นหน่วยพื้นฐานของการคำนวณและการสื่อสารแบบดั้งเดิม โดยที่ p_x คือความน่าจะเป็นที่จะเกิดเหตุการณ์ x เหตุการณ์ที่เกิดขึ้นแน่นอน ($p_x = 1$) จะมีปริมาณสารสนเทศเป็นศูนย์ (0) เหมือนกับว่าข่าวสารนั้นไร้ค่า เช่นประโยค “ยืนกลางฝนโดยไม่หาอะไรมาบังจะทำให้ตัวเปียก” ซึ่งเกิดขึ้นตามนั้นแน่นอน ($p=1$) ให้ค่าปริมาณสารสนเทศเป็น 0 และปริมาณสารสนเทศเฉลี่ย จะเรียกว่า เอนโทรปี (Entropy หรือ H) นิยามของแชนนอนนี้สามารถบ่งบอกในเชิงปริมาณถึงคุณค่าหรือปริมาณข่าวสารที่มีอยู่ในข้อความนั้น อันเป็นฐานไปสู่การพัฒนาด้านการสื่อสาร ตั้งแต่การบีบอัดข้อมูลไปจนถึงระบุขอบเขตด้านทฤษฎีของอัตราการส่งข่าวสารสูงสุดที่รหัสควบคุมความผิดพลาดยังสามารถช่วยควบคุมความผิดพลาดให้น้อยตามต้องการได้ ส่วนรหัสควบคุมความผิดพลาดนั้นจะมีลักษณะเฉพาะอย่างไรไม่ได้ระบุโดยทฤษฎีนี้

ในการคำนวณและการสื่อสารเชิงควอนตัม จอห์น ฟอน นอยมานน์ (John von Neumann) เป็นผู้นิยามปริมาณสารสนเทศในเทอมของสถานะผสม (mixed states) เรียกว่า ฟอน นอยมานน์ เอนโทรปี (von Neumann entropy) และมีผู้เสนอทฤษฎีการเข้ารหัสแหล่งกำเนิด (บีบอัดข้อมูล) สำหรับสารสนเทศควอนตัม รวมถึงการพัฒนาอื่น ๆ ด้วย

ภาคผนวก ฉ

นิยามความพัวพัน

(Entanglement concept)

สถานะ $|\psi\rangle$ จัดเป็นสถานะพัวพัน (entangled state) หรือสถานะที่แบ่งแยกไม่ได้ (non-separable state) ก็ต่อเมื่อ

$$|\psi\rangle \neq |\phi_1\rangle|\phi_2\rangle \quad \text{….....(ค.1)}$$

สำหรับสถานะ $|\phi_1\rangle$ และ $|\phi_2\rangle$ ใด ๆ

สถานะ $|\psi\rangle$ จัดเป็นสถานะไม่พัวพัน (non-entangled state) หรือสถานะที่แบ่งแยกได้ (separable state) ก็ต่อเมื่อ มีสถานะ $|\phi_1\rangle$ และ $|\phi_2\rangle$ ที่ทำให้

$$|\psi\rangle = |\phi_1\rangle|\phi_2\rangle \quad \text{….....(ค.2)}$$

ตัวอย่างในทางคณิตศาสตร์ เช่นสถานะ $|00\rangle+|01\rangle$ จัดเป็นสถานะที่แบ่งแยกได้ เพราะสามารถเขียนได้ในรูป $|00\rangle+|01\rangle=|0\rangle(|0\rangle+|1\rangle)=|\phi_1\rangle|\phi_2\rangle$ โดยที่ $|\phi_1\rangle=|0\rangle$ และ $|\phi_2\rangle=|0\rangle+|1\rangle$ ส่วนสถานะ $|00\rangle+|11\rangle$ ไม่สามารถเขียนได้ในรูป $|\phi_1\rangle|\phi_2\rangle$ ไม่ว่า $|\phi_1\rangle$ และ $|\phi_2\rangle$ จะเป็นอะไรก็ตาม เรียกว่าเป็นสถานะที่แบ่งแยกไม่ได้ (non-separable) หรือสถานะพัวพัน (entangled) ทันทีที่ทราบว่าอนุภาคที่สองอยู่ในสถานะ “1” สถานะรวมของสองอนุภาคจะเป็น $|11\rangle$ ซึ่งจะทราบทันทีว่าอนุภาคแรกมีสถานะ “1” เช่นเดียวกัน

เมื่อสถานะของอนุภาคที่หนึ่งและอนุภาคที่สองอยู่ในสภาพพัวพันกัน สถานะของอนุภาคที่หนึ่งไม่สามารถถูกอธิบายอย่างเป็นอิสระจากอนุภาคที่สองได้ หรือหากพยายามอธิบายสถานะของอนุภาคที่หนึ่ง ก็จะอยู่ในรูปสถานะผสม (mixed state) ซึ่งสูญเสีย relative-phase ไป เรียกกระบวนการเกิดการพัวพันระหว่างระบบที่สนใจกับสิ่งแวดล้อมว่า กระบวนการสูญเสียเฟส (*dephasing* หรือ *decoherence)*

ภาคผนวก ง

เกตลอจิกหนึ่งคิวบิตและสองคิวบิต

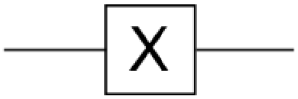
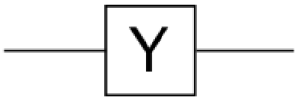
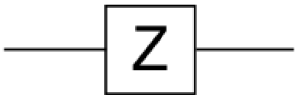
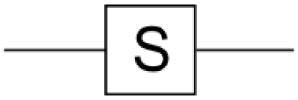
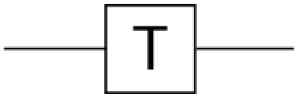
(Single and double qubit gate)

ง.1 เกตลอจิกหนึ่งคิวบิต (single-qubit gates)

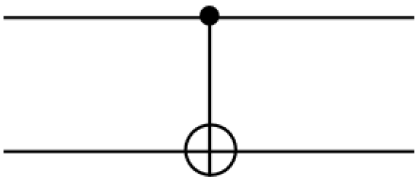
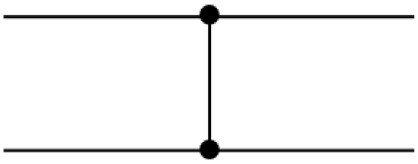
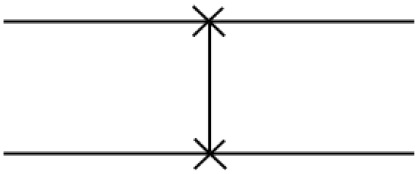
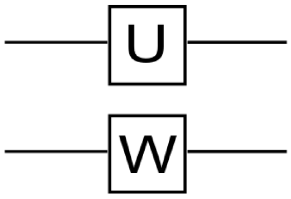
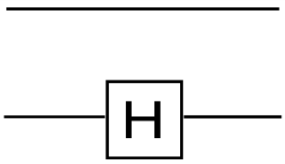
รูปแบบทั่วไปของเกตลอจิกหนึ่งคิวบิตแสดงได้ดังแผนภาพ

$$\begin{pmatrix} a_{out} \\ b_{out} \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} a_{in} \\ b_{in} \end{pmatrix}$$

นิยามของเกตลอจิกเชิงควอนตัมหนึ่งคิวบิตที่สำคัญสรุปได้ดังตาราง

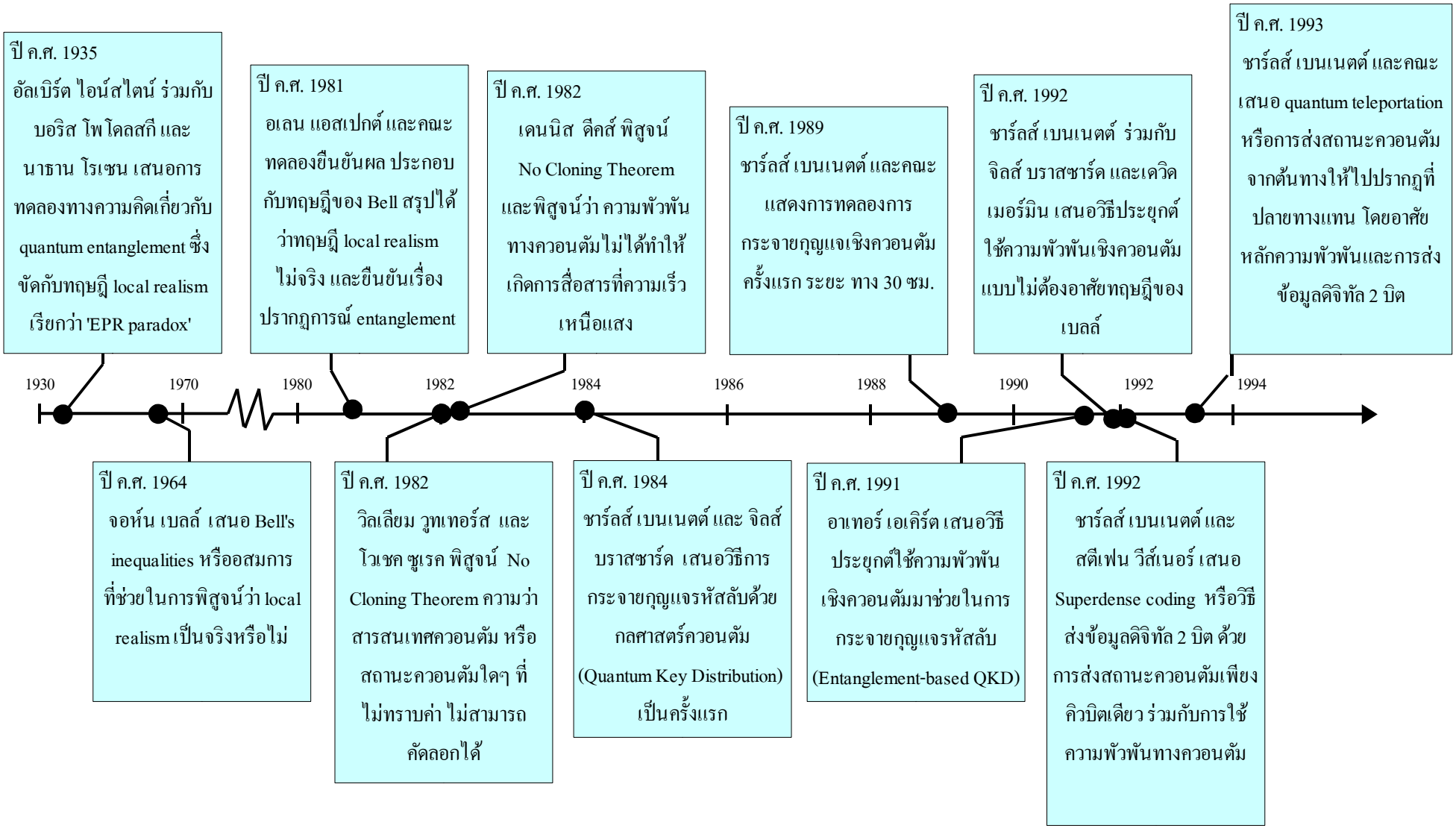
ชื่อเกตลอจิก	สัญลักษณ์	เมทริกซ์
Identity		$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Hadamard		$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
NOT (Pauli-X)		$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-Y		$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z		$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Phase		$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$\frac{\pi}{8}$ gate		$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$

ง.2 เกตลอจิกสองคิวบิต (two-qubit gates)

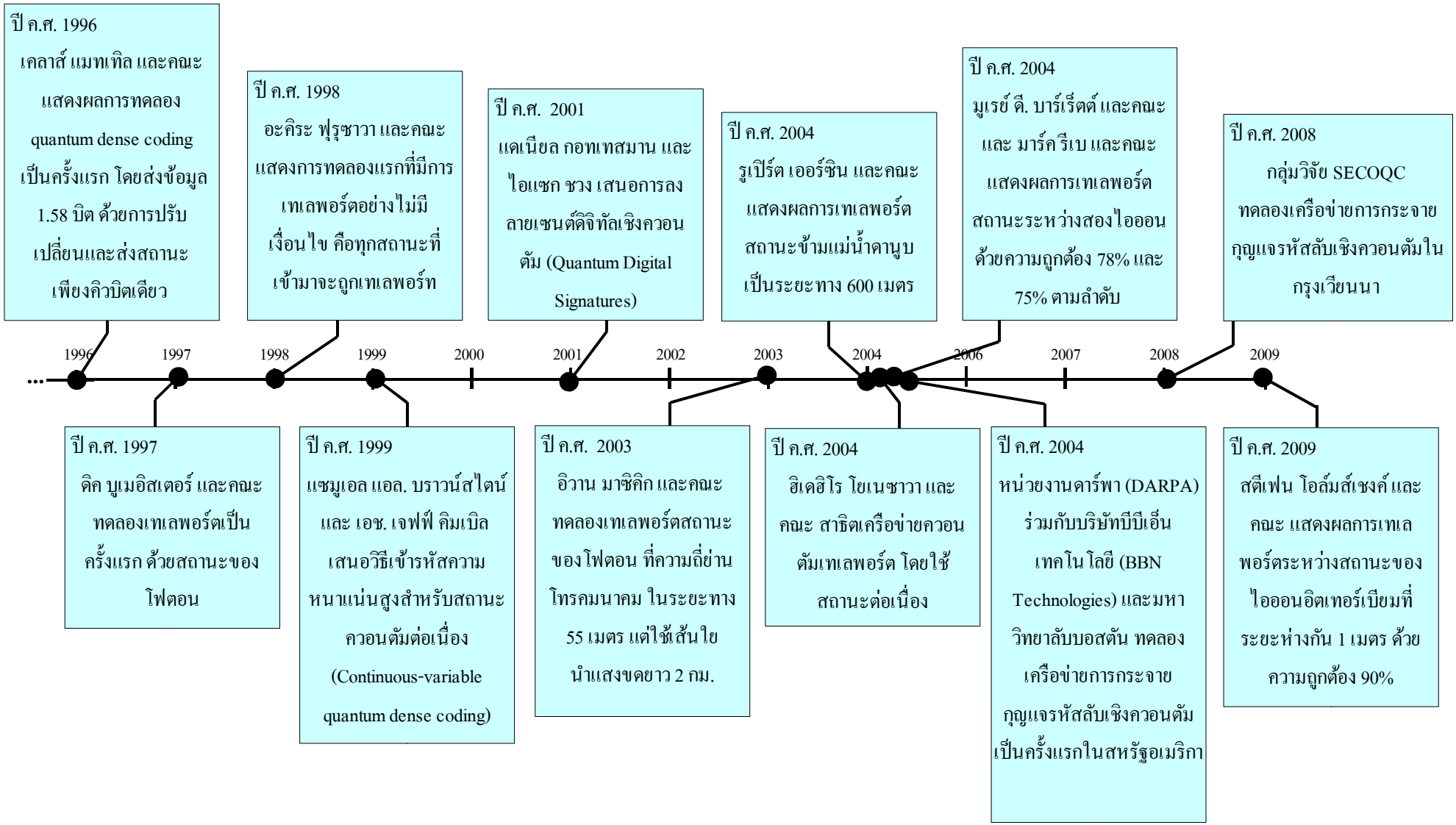
ชื่อเกตลอจิก	สัญลักษณ์	เมทริกซ์
Controlled-NOT *(interacting gate)*		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Controlled-Phase (CZ) *(interacting gate)*		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
SWAP *(interacting gate)*		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
U x W *(non-interating 2-qubit gate)*		$U \otimes W$ $\begin{pmatrix} u_{11}\begin{pmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{pmatrix} & u_{12}\begin{pmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{pmatrix} \\ u_{21}\begin{pmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{pmatrix} & u_{22}\begin{pmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{pmatrix} \end{pmatrix}$
1 x H (Hadamard on second qubit)		$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & -1 \end{pmatrix}$

ภาคผนวก ข

จดหมายเหตุการสื่อสารเชิงควอนตัม (Quantum Communications Milestones)

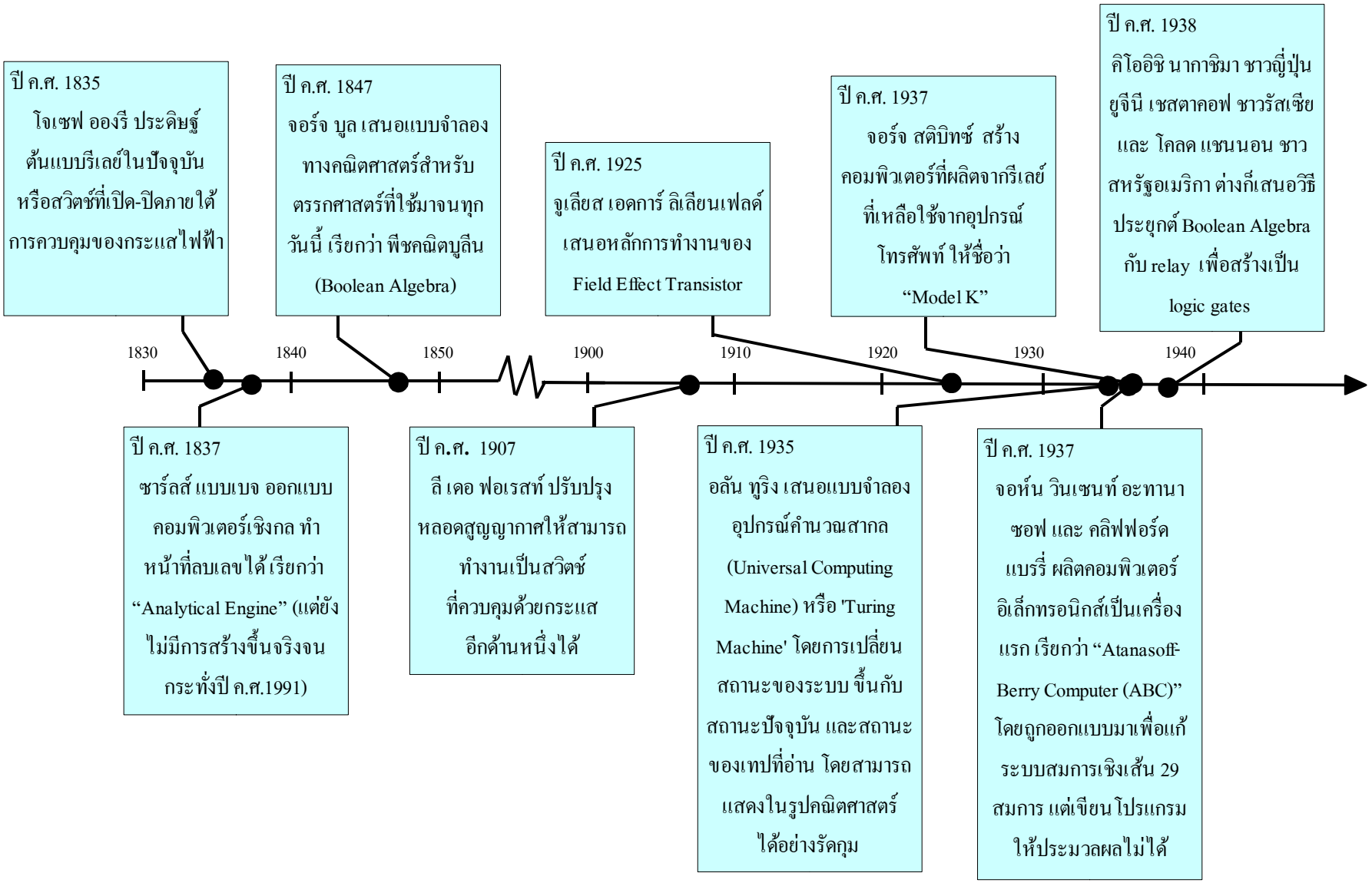


จดหมายเหตุการสื่อสารเชิงควอนตัม (Quantum Communications Milestones) (ต่อ)

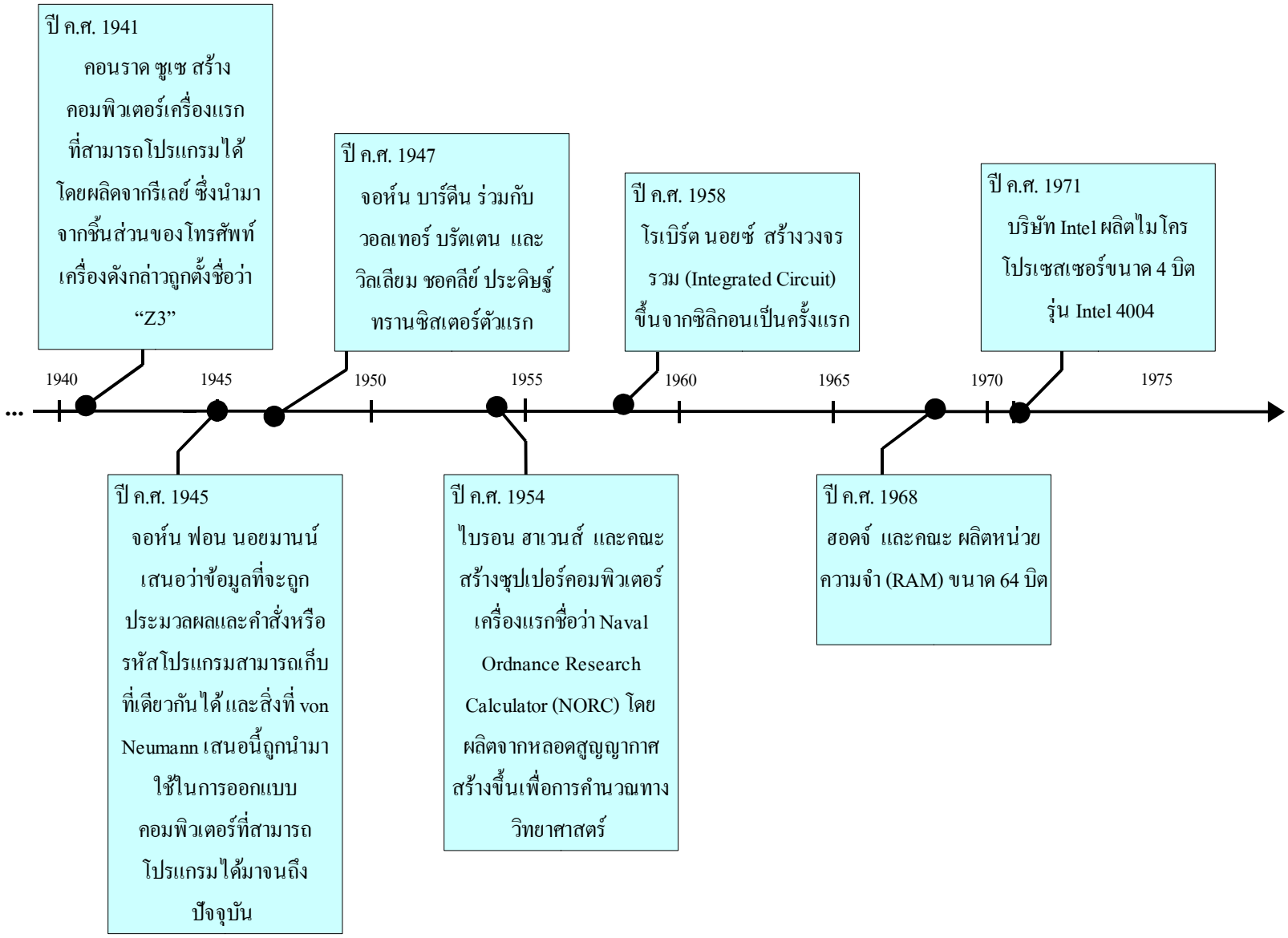


ภาคผนวก ฉ

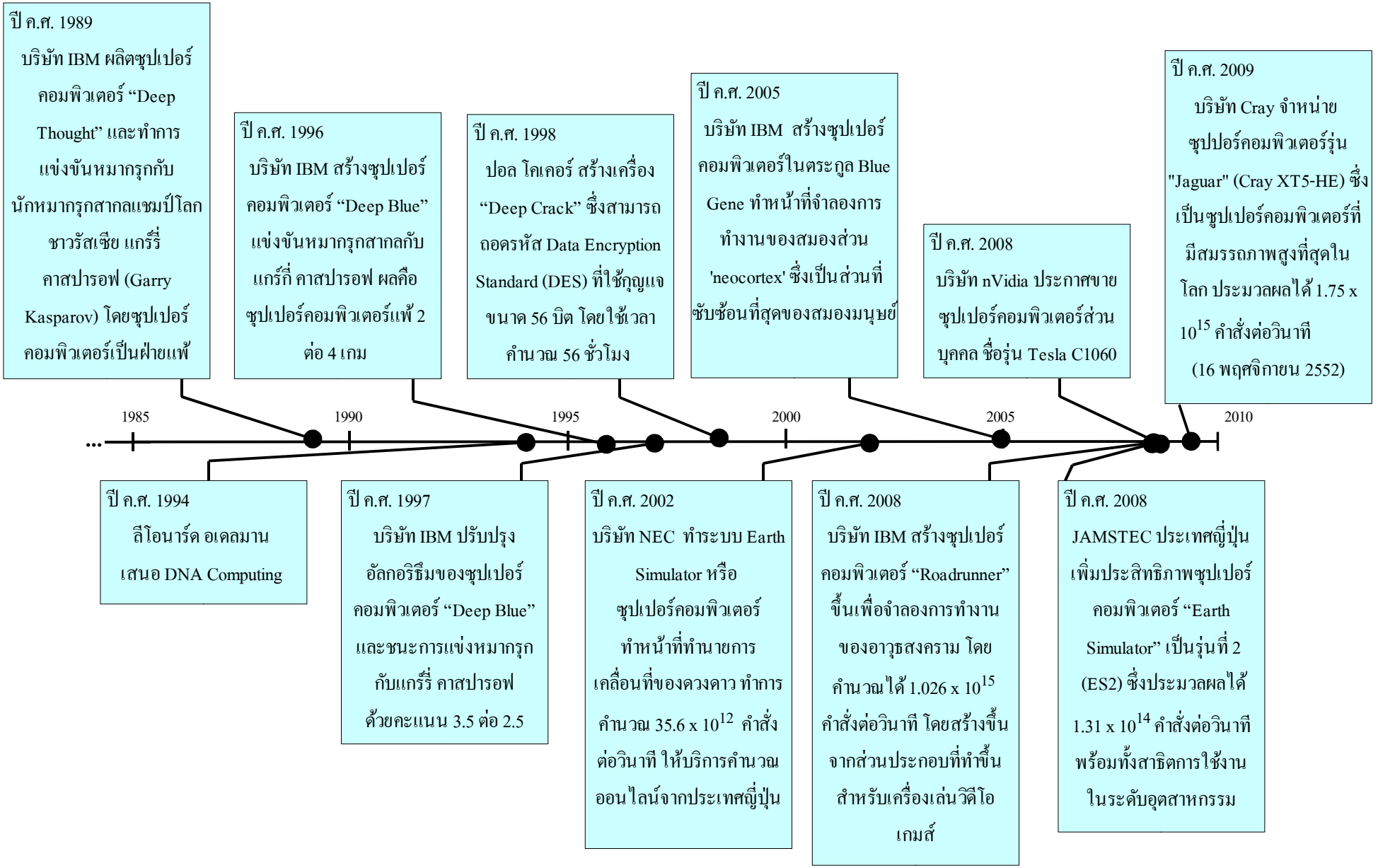
จดหมายเหตุการคำนวณเชิงดิจิทัล (Digital computing milestones)



จดหมายเหตุการคำนวณเชิงดิจิทัล (Digital computing milestones) (ต่อ)

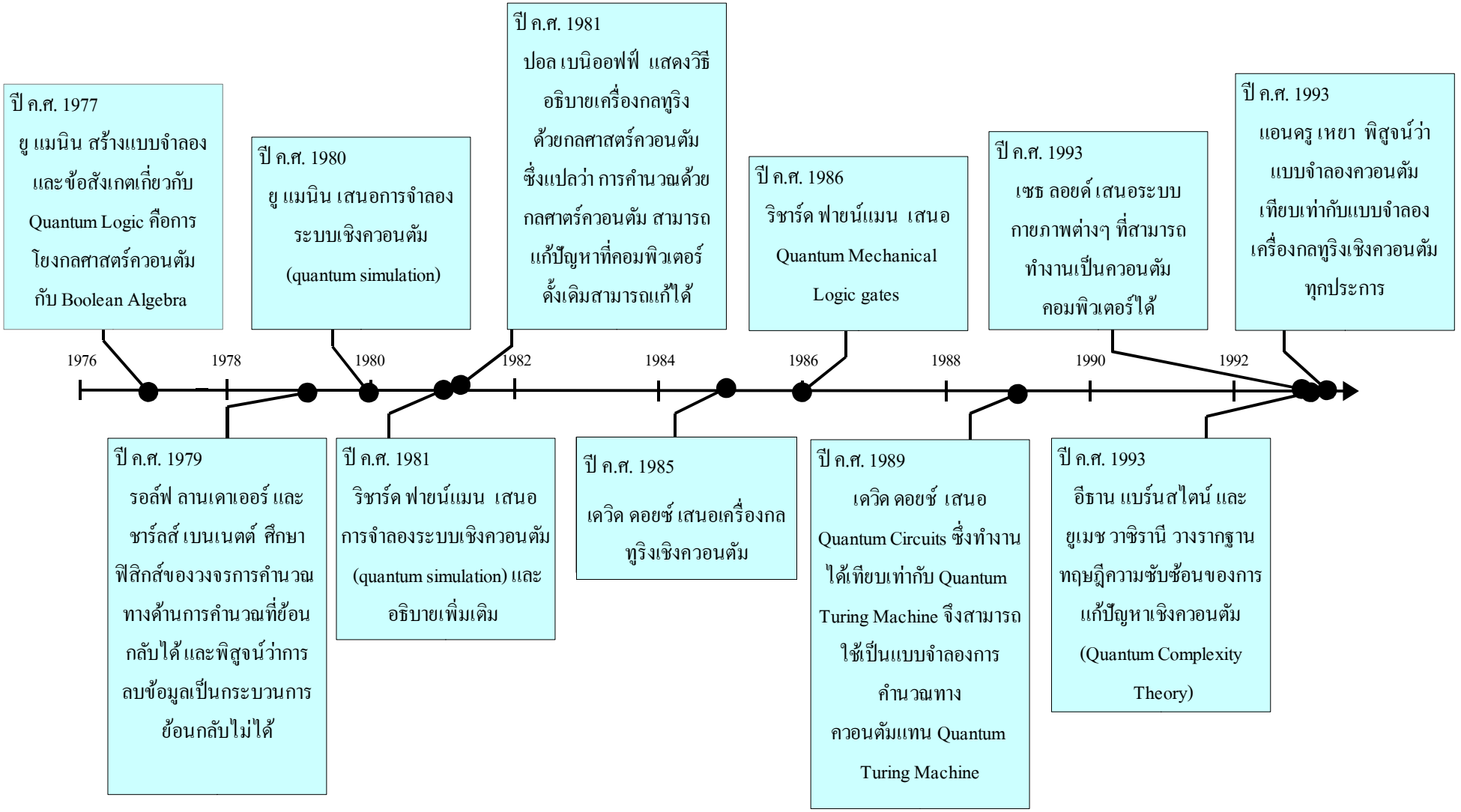


จดหมายเหตุการคำนวณเชิงดิจิทัล (Digital computing milestones) (ต่อ)

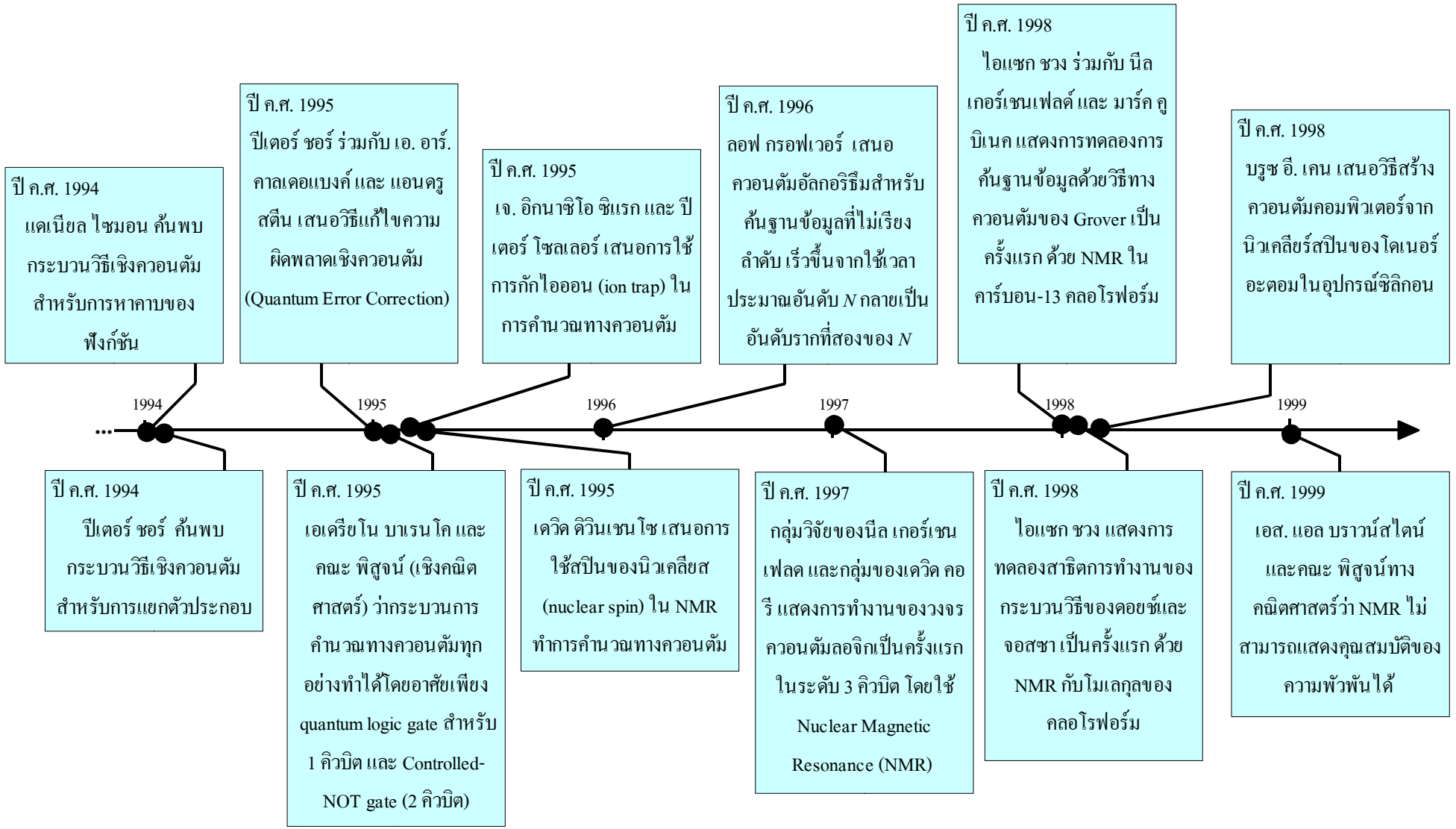


ภาคผนวก ช

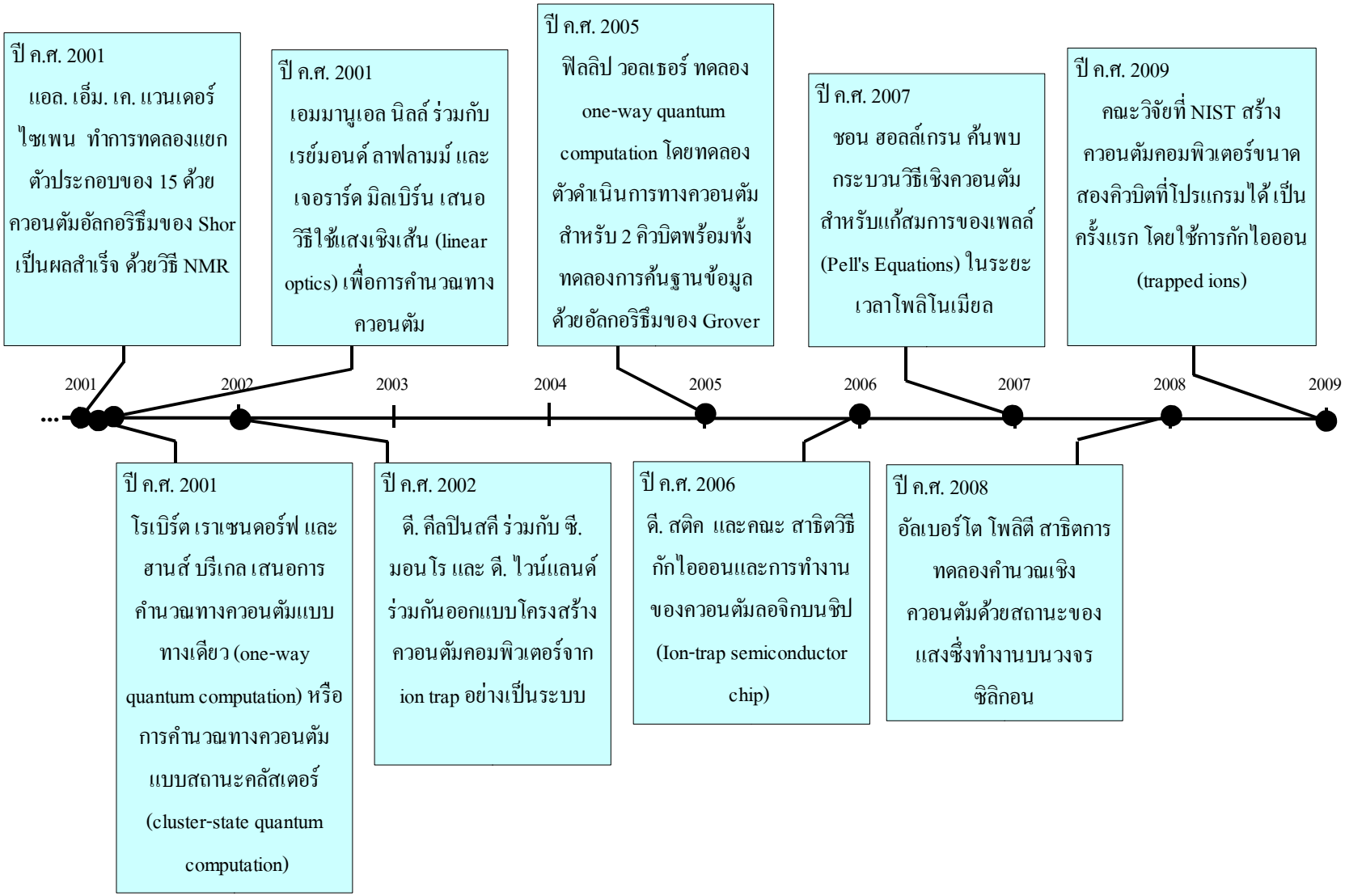
จดหมายเหตุการคำนวณเชิงควอนตัม (Quantum computing milestones)



จดหมายเหตุการคำนวณเชิงควอนตัม (Quantum computing milestones) (ต่อ)



จดหมายเหตุการคำนวณเชิงควอนตัม (Quantum computing milestones)



ชุดหนังสือสารสนเทศเชิงควอนตัม ฉบับที่หนึ่ง
พัฒนาการสารสนเทศเชิงควอนตัม (Development of Quantum Information)

วิทยาการสารสนเทศเชิงควอนตัม (Quantum Information Science) การคำนวณเชิงควอนตัม (Quantum Computing) รหัสย่อและการส่งถ่ายข่าวสารเชิงควอนตัม (Quantum Dense Codes/Quantum Teleportation) และรหัสลับเชิงควอนตัม (Quantum Cryptography) หรือเหล่าแขนงเทคโนโลยีสารสนเทศเชิงควอนตัม (Quantum Information Technology) มีพัฒนาการเติบขยายก้าวออกสู่ห้องตลาดเพื่อใช้งานจริงได้บ้างแล้ว รวมทั้งได้มีการคาดการณ์เทคโนโลยี (Technology Forecast/Foresight) และผลกระทบ (Impact) ทางสังคม การศึกษาและเกษตรกิจจากหลายสำนักและปรากฏอยู่ในวารสาร รายงาน หรือแผนแม่บทของหน่วยงานวิจัยของหลายประเทศ

Free Distribution

ISBN 978-616-12-0212-5