SCBX QUANTUM OUTLOOK :
Post-Quantum Cryptography

SPECIAL EDITION
DECEMBER 2025

Content

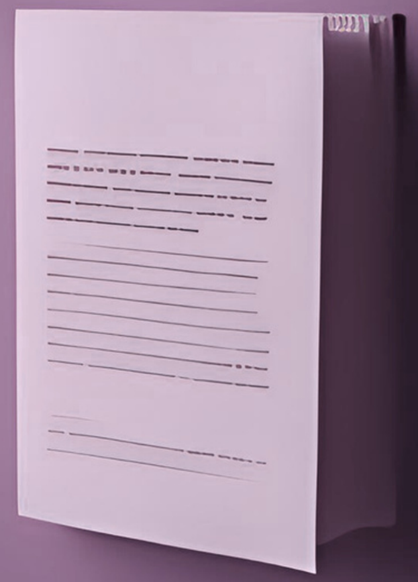
บทที่ 1

บทสรุปผู้บริหาร

บทสรุปผู้บริหาร

ภาพรวมใหญ่เกี่ยวกับภัยคุกคามจากควอนตัมและเหตุผลที่องค์กรต้องเตรียมพร้อม

ภัยคุกคามจากควอนตัมไม่ใช่สิ่งที่อยู่ไกลตัวอีกต่อไปแต่เป็นภัยคุกคามที่เกิดขึ้นแล้วในปัจจุบันความเสี่ยงเร่งด่วนที่สุด คือกลยุทธ์ Harvest-Now, Decrypt-Later (HNDL) ซึ่งผู้ไม่ประสงค์ดีจะดักจับและจัดเก็บข้อมูลในปัจจุบันจำนวนมหาศาลที่ถูกเข้ารหัสไว้ ข้อมูลเข้ารหัสเหล่านี้มักเป็นความลับที่จำเป็นต้องเก็บเป็นเวลาหลายปีหรือหลายทศวรรษ ตามระเบียบขององค์กรหรือข้อกำหนดทางกฎหมาย ซึ่งเป็นช่วงเวลาที่เรียกว่า ขอบเขตการรักษาความลับ (confidentiality horizon) เมื่อควอนตัมคอมพิวเตอร์ที่มีความสามารถเพียงพอในการถอดรหัส (Cryptographically Relevant Quantum Computer, CRQC) กำเนิดขึ้น ซึ่งคาดการณ์ว่าจะเกิดขึ้นระหว่างปี ค.ศ. 2030 ถึง 2035 ข้อมูลที่ถูกเก็บไว้เหล่านี้จะถูกถอดรหัสและรั่วไหลในวงกว้าง เหตุการณ์นี้จะเป็นจุดเปลี่ยนสำคัญที่เรียกว่า Q-Day การเตรียมพร้อมจึงไม่ใช่เพียงการอัปเกรดระบบอย่างรวดเร็ว แต่เป็นกระบวนการย้ายระบบเชิงกลยุทธ์ที่ใช้เวลานานนับทศวรรษองค์กรจึงต้องเริ่มดำเนินการตั้งแต่ตอนนี้ เพื่อลดความเสี่ยงจากการเปิดเผยข้อมูลและสร้างความคงทนของการดำเนินงานในอนาคต



ผลการศึกษา/ข้อเสนอแนะ

ภัยคุกคามจากกลยุทธ์ HNDL
ลำดับความสำคัญเร่งด่วนที่สุดคือการจัดทำบัญชีรายการและย้ายข้อมูลที่เป็นความลับระยะยาว (long-term secrets) ที่มีความเสี่ยงต่อการถูกดักจับข้อมูลในปัจจุบัน

ระเบียบมาตรฐาน
การเปลี่ยนผ่านสู่ PQC ในระดับโลกได้รับการขับเคลื่อนโดยกระบวนการจัดมาตรฐานของ NIST ซึ่งได้สรุปมาตรฐานชุดแรกแล้ว เช่น CRYSTALS-Kyber สำหรับการเข้ารหัส และ CRYSTALS-Dilithium สำหรับลายเซ็นดิจิทัล

การย้ายและการอัปเกรดระบบต้องเป็นแบบผสม
กลยุทธ์ที่ปลอดภัยและคงทนที่สุดคือการใช้งาน Hybrid Deployment ซึ่งหมายถึงการใช้อัลกอริทึมแบบคลาสสิกร่วมกับอัลกอริทึม PQC ใหม่ในเวลาเดียวกัน เพื่อคง backward compatibility และรับประกันความปลอดภัยต่อภัยคุกคามทั้งจากระบบคลาสสิกและระบบควอนตัมในอนาคต

ความคงทนในระยะยาว (PQC+QKD)
สำหรับการจัดการกุญแจระยะยาวและสภาพแวดล้อมของระบบที่ต้องการการปลอดภัยในระดับสูงสุด (เช่น ด้านความมั่นคงของชาติ หรือเครือข่ายสื่อสารระหว่างประเทศ) องค์กรที่เกี่ยวข้องควรพิจารณาการผสานรวมอัลกอริทึม PQC เข้ากับการแจกรหัสลับเชิงควอนตัม (Quantum Key Distribution, QKD) ซึ่ง PQC ใช้อัพเกรดระบบที่มีอยู่แล้ว ในขณะที่ QKD มอบหลักฐานการปลอมแปลงเชิงฟิสิกส์ (physics-based tamper evidence) เพื่อการเชื่อมต่อเฉพาะทาง เพื่อสร้างแนวป้องกันแบบหลายชั้นเพื่อรับมือกับภัยคุกคามในอนาคตทั้งหมด

Crypto-Agility เป็นสิ่งจำเป็น
ความสำเร็จในการเปลี่ยนผ่านขึ้นกับการฝัง crypto-agility ในโครงสร้างพื้นฐาน ซึ่งหมายถึงความสามารถทั้งในระดับองค์กรและระดับเทคนิคในการเปลี่ยนหรือปรับใช้อัลกอริทึมการเข้ารหัสได้อย่างรวดเร็วและมีประสิทธิภาพเพื่อตอบสนองต่อมาตรฐานใหม่หรือการโจมตีทางการวิเคราะห์รหัส (cryptanalytic attack) ที่ไม่คาดคิด

การกำกับดูแลการดำเนินงานเป็นสิ่งสำคัญ
การเปลี่ยนแปลงนี้เป็นความท้าทายด้านการบริหารความเสี่ยง ไม่ใช่แค่โครงการไอทีเพียงอย่างเดียว แต่จำเป็นต้องมีการกำกับดูแลการดำเนินงานในระดับคณะกรรมการ การนำแนวทางหรือกรอบนโยบายขององค์กรมาประสานให้เป็นไปในทิศทางเดียวกัน และการจัดทำรายการเพื่อติดตามสินทรัพย์เข้ารหัส (cryptographic assets) ทั้งหมดและขอบเขตการรักษาความลับที่เกี่ยวข้อง

บทที่ 2

บทนำ

วัตถุประสงค์และขอบเขตของเอกสาร

เอกสารฉบับนี้นำเสนอกรอบแนวทางที่ครอบคลุม เป็นกลางต่อผู้ให้บริการ และมีความสอดคล้องในระดับสากล เพื่อช่วยให้เข้าใจภัยคุกคามจากควอนตัม และดำเนินการเปลี่ยนผ่านสู่ PQC ได้อย่างมีประสิทธิภาพ วัตถุประสงค์หลักคือเพื่อขจัดความซับซ้อนทางเทคนิคอย่างเป็นกลาง โดยนำเสนอเส้นทางที่ชัดเจนสำหรับผู้บริหารระดับกลยุทธ์ในการตัดสินใจ ขอบเขตของเอกสารครอบคลุมตลอดช่วงเวลาของการเปลี่ยนผ่านสู่ PQC ตั้งแต่การอธิบายแนวคิดควอนตัมให้เข้าใจง่าย การจำแนกประเภทของอัลกอริทึมหลัก การอธิบายมาตรฐานสากล (เช่น NIST, ETSI, ISO/IEC) การกำหนดแผนการย้ายและอัปเกรดระบบแบบเป็นขั้นตอน ไปจนถึงการจัดการกับประเด็นที่ซับซ้อนด้านกฎระเบียบ การกำกับดูแล และการจัดการกุญแจ (key management) เอกสารนี้ให้ความสำคัญกับความจำเป็นในการประสานงานระดับภูมิภาค โดยเฉพาะในเอเชียและกรอบความร่วมมืออาเซียน (ASEAN framework)

กลุ่มเป้าหมาย

เอกสารแนะแนวฉบับนี้จัดทำขึ้นสำหรับสองกลุ่มหลักที่มีบทบาทสำคัญเท่าเทียมกัน ได้แก่

ผู้นำเชิงกลยุทธ์และผู้บริหารด้านการบริหารความเสี่ยง

ผู้บริหารระดับสูง กรรมการบริษัท ประธานเจ้าหน้าที่ด้านความปลอดภัยสารสนเทศ (CISO) และเจ้าหน้าที่กำกับความเสี่ยง ที่ต้องการความเข้าใจเชิงนโยบายเกี่ยวกับภัยคุกคามจากควอนตัม ผลกระทบต่อธุรกิจ และโครงสร้างการกำกับดูแลรวมถึงทรัพยากรที่จำเป็นต่อการย้ายและการอัปเกรดระบบอย่างปลอดภัย

สถาปนิกด้านความปลอดภัยและผู้เชี่ยวชาญด้านเทคนิค

วิศวกร นักพัฒนาแอปพลิเคชัน และเจ้าหน้าที่ฝ่ายปฏิบัติการด้านความปลอดภัยผู้รับผิดชอบการจัดทำบัญชีสินทรัพย์การเข้ารหัส การออกแบบสถาปัตยกรรมระบบ การนำมาตรฐานไปใช้ การทดสอบความเข้ากันได้ (interoperability testing) และการดำเนินการทางเทคนิคในแผนการเปลี่ยนผ่านสู่ PQC

ผลกระทบต่อการเข้ารหัสแบบคลาสสิก

รากฐานของความปลอดภัยทางดิจิทัลสมัยใหม่คือระบบการเข้ารหัสกุญแจสาธารณะที่อิงกับการแยกตัวประกอบของจำนวนเฉพาะขนาดใหญ่ (RSA) และการแก้ปัญหา discrete logarithm on Elliptic Curve Cryptography ซึ่งระบบเหล่านี้ถูกทำลายได้โดยกลไกของคอมพิวเตอร์ควอนตัมอย่างสิ้นเชิง ข้อมูลทั้งหมดที่ได้รับการปกป้องโดยอัลกอริทึมแบบคลาสสิก ไม่ว่าจะเป็นข้อมูลที่เก็บไว้ (data at rest) เช่น ในฐานข้อมูลหรือเซิร์ฟเวอร์ หรือข้อมูลที่กำลังส่งผ่านเครือข่าย (data in transit) ผ่านโปรโตคอลอย่าง TLS และ IPsec ต่างมีความเสี่ยงที่จะถูกถอดรหัสในอนาคต ดังนั้น การเปลี่ยนผ่านสู่ PQC จึงไม่ใช่ทางเลือก แต่เป็นสิ่งที่จำเป็นอย่างยิ่ง ต้องมีการทดแทนอัลกอริทึมที่เปราะบางเหล่านี้อย่างเป็นระบบในทุกจุดที่ใช้เพื่อการปกป้องข้อมูลระยะยาว code signing หรือการยืนยันตัวตน (identity authentication) ในบทต่อๆไป จะอธิบายถึงรายละเอียดของไทม์ไลน์ การกำหนดตัวเลือกอัลกอริทึม PQC และแนวทางปฏิบัติที่เป็นรูปธรรมสำหรับการบริหารจัดการการเปลี่ยนผ่านครั้งใหญ่ด้านการเข้ารหัสนี้อย่างมีประสิทธิภาพ

บทที่ 3

เทคโนโลยีควอนตัมสำหรับผู้เริ่มต้น

เทคโนโลยีควอนตัมสำหรับผู้เริ่มต้น

เมื่อเรายืนอยู่บนขอบของยุคเทคโนโลยีใหม่ เทคโนโลยีควอนตัมมีศักยภาพที่จะปฏิวัติการประมวลผล การตรวจวัด และการสื่อสารที่ปลอดภัยในรูปแบบที่ไม่เคยมีมาก่อน แตกต่างจากระบบคลาสสิกที่จัดการ bit เพียง 0 หรือ 1 ระบบควอนตัมใช้ประโยชน์จากพฤติกรรมเฉพาะของอนุภาคในระดับอะตอมเพื่อเปิดศักยภาพการประมวลผลแบบขนานและความสัมพันธ์ที่ไม่เคยมีมาก่อนสำหรับผู้บริหารและผู้เชี่ยวชาญที่ไม่มีพื้นฐานด้านฟิสิกส์ บทนี้ช่วยทำให้เข้าใจแนวคิดหลักได้ง่ายขึ้น อธิบายว่าทำไมควอนตัมจึงสำคัญในปัจจุบัน แสดงผลกระทบเชิงรูปธรรมต่ออุตสาหกรรมต่าง ๆ และสำรวจเหตุผลเชิงปฏิบัติที่ควรเริ่มเตรียมพร้อมตั้งแต่ตอนนี้ ทั้งเพื่อคว้าโอกาสเชิงกลยุทธ์และลดความเสี่ยงที่เกิดขึ้นใหม่ ในตอนท้ายของบทนี้ ผู้อ่านจะมีความเข้าใจถึงภาพรวมอย่างชัดเจนเกี่ยวกับเทคโนโลยีควอนตัมว่าทำไมถึงสำคัญ ผลกระทบต่อองค์กร และขั้นตอนที่จำเป็นในการเริ่มต้น

เทคโนโลยีควอนตัมคืออะไร?

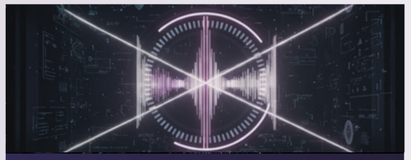
โดยแก่นแท้แล้ว เทคโนโลยีควอนตัมอาศัยพฤติกรรมของอนุภาคเมื่อถูกจำกัดในขนาดที่เล็กที่สุด แม้ว่าฟิสิกส์พื้นฐานเบื้องหลังอาจซับซ้อนทางคณิตศาสตร์ แต่มีผลกระทบหลักสามประการที่ขับเคลื่อนการประยุกต์ใช้งานทั้งหมด ได้แก่ superposition, entanglement และ quantum interference ส่วนนี้จะนิยามแต่ละปรากฏการณ์ในรูปแบบที่เข้าใจง่าย และอธิบายว่าคุณสมบัติเหล่านี้รวมกันอย่างไรเพื่อสร้างองค์ประกอบพื้นฐานของอุปกรณ์ควอนตัม โดยมุ่งเน้นหลักการสำคัญมากกว่ารายละเอียดทางเทคนิค เพื่อสร้างพื้นฐานความเข้าใจเกี่ยวกับระบบควอนตัมในโลกจริง

Superposition

Qubit สามารถอยู่ในหลายสถานะพร้อมกันได้ (ทั้ง 0 และ 1) แทนที่จะเป็นเพียงหนึ่งในสองสถานะเท่านั้น

Entanglement

Qubit สองตัวจะถูกเชื่อมโยงกัน ทำให้สถานะของตัวหนึ่งส่งผลต่ออีกตัวหนึ่งทันที ไม่ว่าจะอยู่ห่างกันเท่าใด



Quantum interference

ความน่าจะเป็นเชิงแอมพลิจูดของสถานะต่าง ๆ สามารถรวมกันในรูปแบบเสริมกันหรือหักล้าง ซึ่งทำให้ผลลัพธ์บางอย่างถูกเพิ่มขึ้นและบางอย่างลดลง

คุณสมบัติทั้งสามนี้ช่วยให้เกิดแนวทางใหม่ในการประมวลผล การตรวจวัด และการเข้ารหัสข้อมูล ซึ่งถูกนำไปใช้งานจริงใน superconducting circuits, trapped-ion arrays และ photonic networks

ทำไมต้องเทคโนโลยีควอนตัม?

ศักยภาพของเทคโนโลยีควอนตัมอยู่ที่ความสามารถเหนือกว่าระบบคลาสสิกในทุกมิติ ตั้งแต่การเร่งความเร็วของการคำนวณที่ซับซ้อน ไปจนถึงการตรวจวัดที่มีความแม่นยำสูงเป็นพิเศษ และการสร้างระบบสื่อสารที่ปลอดภัยต่ออนาคต เทคโนโลยีควอนตัมได้เปิดขอบเขตใหม่ของศักยภาพทางวิทยาศาสตร์และอุตสาหกรรม ส่วนนี้จะแบ่งข้อได้เปรียบหลักออกเป็นสามกลุ่ม ได้แก่ การประมวลผล (Computation), การตรวจวัด (Sensing & Metrology) และ ความปลอดภัยของข้อมูล (Security) พร้อมยกตัวอย่างการใช้งานที่เป็นรูปธรรม เพื่อช่วยให้องค์กรเข้าใจและสามารถวางแนวทางกลยุทธ์ที่สอดคล้องกับการเปลี่ยนผ่านสู่ยุคควอนตัม

1. พลังการประมวลผล

- **การเร่งความเร็วของปัญหาซับซ้อน** ปัญหาบางประเภท เช่น optimization, การจำลองทางเคมี , การจัดพอร์ตการลงทุน และการวางแผนโลจิสติกส์ อาจได้รับการเร่งความเร็วอย่างมหาศาลจากอัลกอริทึมควอนตัม
- **อัลกอริทึมใหม่** อัลกอริทึมควอนตัมใช้หลักการของ superposition และ entanglement เพื่อลดจำนวนขั้นตอนการคำนวณ ทำให้การจำลองที่เคยใช้เวลาหลายปีสามารถทำได้ภายในไม่กี่นาที

2.การตรวจวัดและมาตรวิทยา

- **การวัดที่มีความแม่นยำสูงเป็นพิเศษ** เซ็นเซอร์ควอนตัมสามารถตรวจจับสนาม แรง หรือช่วงเวลาที่ละเอียดกว่าระบบคลาสสิกหลายลำดับขั้น ซึ่งมีประโยชน์อย่างยิ่งในด้าน การนำทาง , การถ่ายภาพทางการแพทย์ และ การตรวจสอบวัสดุ
- **ตัวอย่างเช่น** นาฬิกาอะตอม และอุปกรณ์วัดสนามแม่เหล็กควอนตัม ถูกนำไปใช้เพื่อเพิ่มความแม่นยำของระบบ GPS และการตรวจวัดทางชีวการแพทย์

3.ความปลอดภัยของข้อมูล

- **การแจกรหัสลับควอนตัม** ใช้สถานะควอนตัมในการแลกเปลี่ยนกุญแจเข้ารหัสโดยมีคุณสมบัติสามารถตรวจจับการดักฟังได้จริงในทางฟิสิกส์
- **การเตรียมความพร้อมสู่ยุคหลังควอนตัม** เมื่อคอมพิวเตอร์ควอนตัมก้าวหน้าขึ้น ระบบเข้ารหัสแบบคลาสสิก เช่น RSA และ ECC จะไม่ปลอดภัยอีกต่อไป การใช้อัลกอริทึมที่ปลอดภัยต่อควอนตัม และ QKD จะช่วยปกป้องการสื่อสารทั้งในปัจจุบันและอนาคต
- **การโจมตีและการป้องกันด้วยควอนตัม** ผู้ไม่หวังดีอาจใช้ประโยชน์จากอัลกอริทึมควอนตัมเพื่อค้นหาช่องโหว่ใหม่ๆ ทั้งในระบบดิจิทัลและระบบสื่อสารควอนตัม รวมถึงสร้างการโจมตีแบบผสมที่มีประสิทธิภาพสูงขึ้น ขณะเดียวกันฝ่ายป้องกันสามารถใช้เทคโนโลยีควอนตัมเพื่อเพิ่มประสิทธิภาพการตรวจจับความผิดปกติและเฝ้าระวังภัยคุกคามแบบเรียลไทม์ ได้เช่นกัน

เทคโนโลยีควอนตัมจะส่งผลต่อชีวิตเราอย่างไร?

ศักยภาพในการปฏิวัติของเทคโนโลยีควอนตัมครอบคลุมเกือบทุกภาคส่วนของเศรษฐกิจโลก โดยการจับคู่ประโยชน์เฉพาะด้านของควอนตัมกับกรณีนำไปใช้งานจริง องค์กรสามารถระบุโอกาสในการเริ่มโครงการนำร่องและความร่วมมือเชิงกลยุทธ์ได้ ตารางด้านล่างสรุป 6 ภาคส่วนที่เทคโนโลยีควอนตัมเริ่มมีอิทธิพลต่อการวิจัยและพัฒนา พร้อมตัวอย่างเชิงรูปธรรมเพื่อแสดงให้เห็นว่าการพัฒนานี้นำไปใช้ได้จริงอย่างไร

ตัวเลือก	ผลประโยชน์ควอนตัม	ตัวอย่าง
เวชภัณฑ์	การจำลองโมเลกุลอย่างรวดเร็ว	การออกแบบการรักษามะเร็งแบบใหม่ผ่านแบบจำลองการพับโปรตีน
การเงินและโลจิสติกส์	การเพิ่มประสิทธิภาพเครือข่ายที่ซับซ้อน การเพิ่มประสิทธิภาพพอร์ตโฟลิโอ	การวางแผนเส้นทางแบบไดนามิกช่วยลดต้นทุนเชื้อเพลิงและลดความล่าช้า เพิ่มประสิทธิภาพการจัดสรรทรัพยากรสำหรับระบบที่ซับซ้อน
พลังงานและวัสดุ	การค้นพบตัวเร่งปฏิกิริยาและตัวนำยิ่งยวดใหม่	ตัวเร่งปฏิกิริยาการผลิตไฮโดรเจนที่มีประสิทธิภาพ
สุขภาพ	การถ่ายภาพความละเอียดสูงพิเศษ	การตรวจหาโรคตั้งแต่เนิ่นๆ ด้วย MRI ที่ปรับปรุงด้วยควอนตัม
โทรคมนาคม	การแลกเปลี่ยนกุญแจที่ปลอดภัยอย่างพิสูจน์ได้	ธุรกรรมทางการเงินและเครือข่ายรัฐบาลที่ปลอดภัยต่อควอนตัม
การผลิตและ AI	การฝึกอบรมแมชชีนเลิร์นนิงแบบเร่งรัด	การบำรุงรักษาเชิงคาดการณ์ที่ชาญฉลาดยิ่งขึ้น ช่วยลดเวลาหยุดทำงาน

ศักยภาพในการปฏิวัติของเทคโนโลยีควอนตัมครอบคลุมเกือบทุกภาคส่วนของเศรษฐกิจโลก โดยการจับคู่ประโยชน์เฉพาะด้านของควอนตัมกับกรณีใช้งานจริง องค์กรสามารถระบุโอกาสสำหรับ โครงการนำร่อง และควชามร่วมมือเชิงกลยุทธ์ได้ นอกจากนี้เทคโนโลยีควอนตัมยังจะเป็นแรงผลักดันให้เกิดความก้าวหน้าใน ปัญญาประดิษฐ์ (AI), ความปลอดภัยแห่งชาติ, และ วิทยาศาสตร์พื้นฐาน ซึ่งจะปรับโฉมตลาดและพลวัตการแข่งขัน

ทำไมเราต้องเตรียมตัวตั้งแต่ตอนนี้

การปฏิวัติของเทคโนโลยีควอนตัมจะไม่รอผู้ที่ล้าหลัง ผู้ที่เริ่มนำเทคโนโลยีไปใช้ก่อนจะได้เปรียบในด้าน นวัตกรรม, ตำแหน่งในตลาด, และการบริหารความเสี่ยง ในขณะที่องค์กรที่ไม่พร้อมจะเผชิญกับช่องว่างทั้งด้านยุทธศาสตร์และความปลอดภัย ส่วนนี้สรุป สี่เสาหลัก (Four Pillars) เพื่อเป็นแนวทางสำหรับผู้บริหารในการเตรียมความพร้อมด้านควอนตัม ได้แก่ กลยุทธ์, บุคลากร, โครงสร้างพื้นฐาน, และกฎระเบียบ พร้อมข้อเสนอเชิงปฏิบัติสำหรับการสร้างความสามารถและพันธมิตรด้านควอนตัมตั้งแต่วันนี้

1. ภาวะผู้นำเชิงกลยุทธ์

ข้อได้เปรียบของผู้เริ่มก่อน
กำหนดมาตรฐาน สร้างความร่วมมือที่มั่นคง และคว้าส่วนแบ่งตลาด

การลดความเสี่ยง
ป้องกันการรั่วไหลของข้อมูล ในอนาคตเมื่อการเข้ารหัสแบบคลาสสิกถูกคอมพิวเตอร์ควอนตัมทำลาย

2.บุคลากรและระบบนิเวศ

ความพร้อมของแรงงาน
พัฒนาผู้เชี่ยวชาญด้านวิศวกรรมควอนตัมและการออกแบบอัลกอริทึม

เครือข่ายความร่วมมือ
ร่วมมือกับสถาบันวิชาการ ห้องปฏิบัติการ และสตาร์ทอัพเพื่อถ่ายโอนเทคโนโลยี

3.การวางแผนโครงสร้างพื้นฐาน

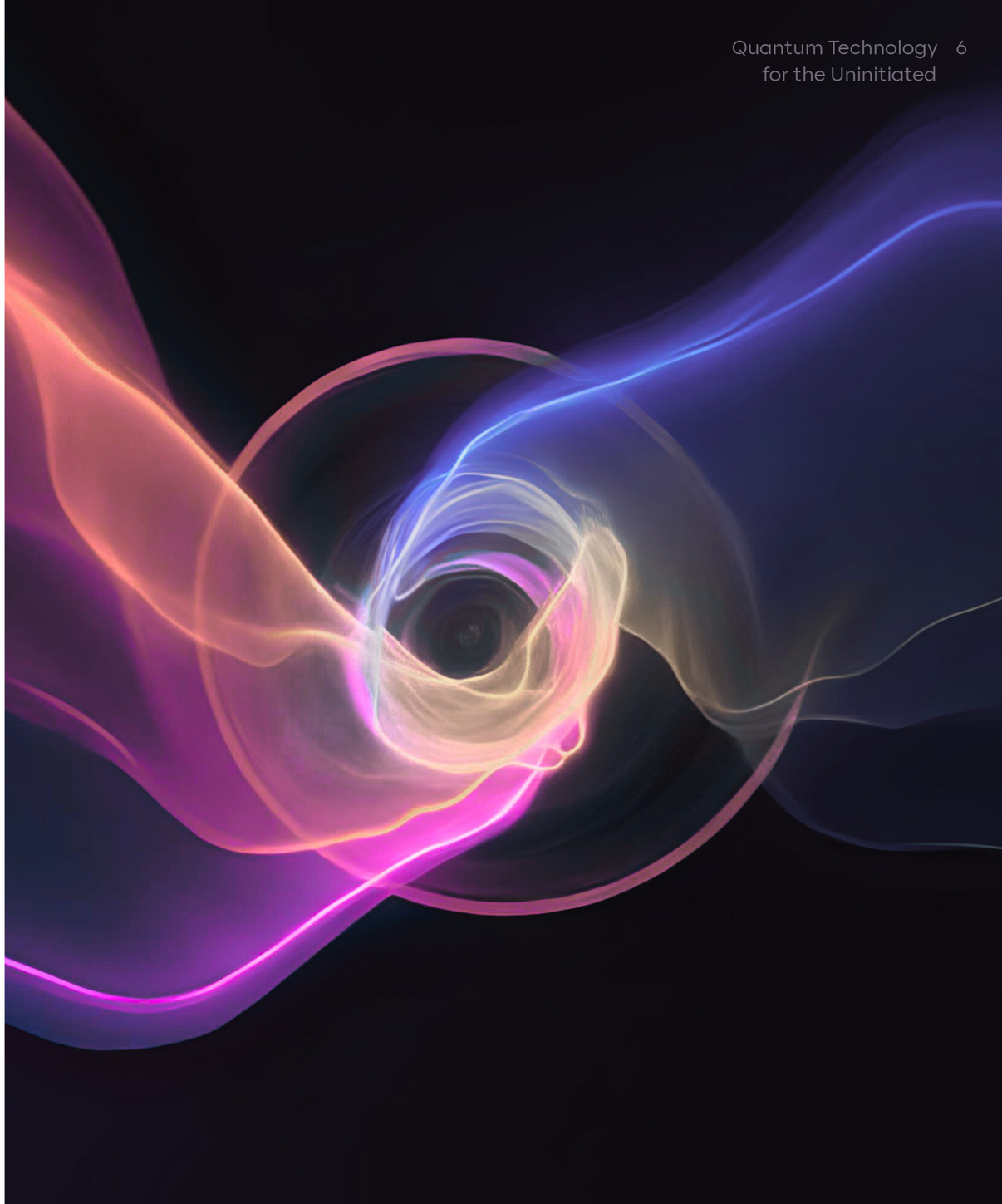
การระบุกรณีใช้งาน
ทดสอบโครงสร้างการทำงานแบบผสมคลาสสิกควอนตัมเพื่อตรวจสอบผลตอบแทนการลงทุน

การลงทุนแบบเป็นขั้นตอน
จาก proofs of concept ไปสู่ต้นแบบที่ขยายได้อย่างมีประสิทธิภาพ

4.การปรับตัวกับกฎระเบียบ

การมีส่วนร่วมในมาตรฐาน
มีอิทธิพลต่อกรอบการเข้ารหัสและความเป็นส่วนตัวของข้อมูลที่ปลอดภัยต่อควอนตัม

ความสามารถในการทำงานร่วมกัน
ปฏิบัติตามมาตรฐานตั้งแต่แรกเพื่อหลีกเลี่ยงการผูกติดกับผู้จำหน่ายและรับรองความเข้ากันได้ข้ามอุตสาหกรรม



บทที่ 4

ภาพของการคุกคาม จากคอมพิวเตอร์ควอนตัม

ภาพของการคุกคามจากคอมพิวเตอร์ควอนตัม

เมื่อคอมพิวเตอร์ควอนตัมก้าวจากทฤษฎีสู่การใช้งานจริง ศักยภาพในการปฏิวัติของมันสร้างทั้งโอกาสและความเสี่ยง ถึงระบบควอนตัมจะสามารถสร้างความก้าวหน้าในการจำลองและ optimazation แต่ก็ยังคุกคามรากฐานการเข้ารหัสข้อมูลปัจจุบัน ทำให้เกิดความเสี่ยงต่อการมีอยู่ต่อความปลอดภัยของข้อมูล ผู้บริหารจำเป็นต้องเข้าใจไม่เพียงแค่ความสามารถของ quantum machine ที่กำลังเกิดขึ้น แต่ยังรวมถึงไทม์ไลน์และขั้นตอนเชิงกลยุทธ์ที่จำเป็นในการป้องกันช่องทางโจมตีใหม่ๆ บทนี้ให้ข้อมูลเบื้องต้นเกี่ยวกับพลังการประมวลผลของคอมพิวเตอร์ควอนตัม, การกำหนด Q-Day milestones ที่คาดการณ์ไว้, อธิบายภัยคุกคามแบบ harvest-now/decrypt-later, และสรุปกรอบการกำกับดูแล เพื่อแนะนำแนวทางการกำหนดนโยบายและการลงทุนที่คงทน เมื่ออ่านบทนี้จบ ผู้อ่านจะเข้าใจความเร่งด่วนของกลยุทธ์ที่ปลอดภัยต่อควอนตัม และรู้วิธีปรับแนวทางป้องกันขององค์กรให้สอดคล้องกับมาตรฐานที่เปลี่ยนแปลงไป

เบื้องต้นเกี่ยวกับความสามารถของคอมพิวเตอร์ควอนตัม

คอมพิวเตอร์ควอนตัมทำงานบน qubit ที่ใช้คุณสมบัติ superposition, entanglement และ interference เพื่อทำการคำนวณบางอย่างได้เร็วขึ้นอย่างทวีคูณเมื่อเทียบกับคอมพิวเตอร์คลาสสิก อุปกรณ์ NISQ (Noisy Intermediate-Scale Quantum) ในปัจจุบัน ซึ่งมี qubit ตั้งแต่ 50 ถึง 150 ตัว ได้แสดงให้เห็น "quantum advantage" ในงานเฉพาะด้าน แต่ยังคงถูกจำกัดด้วยสัญญาณรบกวนและข้อจำกัดด้านการขยายระบบ การเข้าใจช่องว่างระหว่างแพลตฟอร์ม NISQ ปัจจุบันกับระบบ fault-tolerant เป็นสิ่งสำคัญสำหรับการประเมินว่าความเสี่ยงด้านการเข้ารหัสและการปฏิบัติการจะเกิดขึ้นเมื่อใด หน่วยประมวลผลควอนตัมใช้คุณสมบัติของ superposition, entanglement และ interference ในการแก้ปัญหาที่คอมพิวเตอร์คลาสสิกทำไม่ได้ ตัวอย่างเช่น หน่วยประมวลผล Willow ของ Google ที่มี 105 qubit ทำ random-circuit-sampling benchmark เสร็จในเวลา 5 นาที เทียบกับซูเปอร์คอมพิวเตอร์คลาสสิกที่ต้องใช้เวลาประมาณ 10^{25} ปี การขยายเกินขอบเขตของ NISQ จำเป็นต้องใช้การแก้ไขข้อผิดพลาดควอนตัม (quantum error correction) ซึ่งจะเข้ารหัส logical qubit หนึ่งตัวเข้าไปในหลายๆ physical qubit แผนงานของ IBM ตั้งเป้าให้มี 200 logical qubit ที่สามารถรัน 100 ล้านเกจ ได้ภายในปี 2029

ไทม์ไลน์ของ Quantum Capable Machine

การคาดการณ์ว่าเมื่อใดระบบควอนตัมจะเริ่มเป็นภัยคุกคามต่อระบบเข้ารหัสแบบคลาสสิกนั้น ต้องอาศัยการวิเคราะห์ข้อมูลจากแผนการดำเนินงาน (roadmap) ของผู้ผลิตควอนตัมคอมพิวเตอร์ รายงานจากภาครัฐ และความคิดเห็นจากผู้เชี่ยวชาญ (peer-reviewed forecasts) ตารางต่อไปนี้รวบรวม หมุดหมายสำคัญ (authoritative milestones) ตั้งแต่การสาธิตระบบควอนตัมยุคต้นแบบ NISQ ไปจนถึงสถาปัตยกรรม fully fault-tolerant architectures เพื่อช่วยให้ผู้บริหารสามารถวางแผนเชิงกลยุทธ์การลงทุนด้านความปลอดภัย และการปรับให้เป็นไปตามมาตรฐาน (standards compliance) ได้อย่างเป็นระบบตามตารางเวลาที่ชัดเจน

2024
Google Willow
105-qubit superconducting processor; first below-threshold error correction; 5 min random-circuit sampling vs classical ≈10^{25} yr.

2025
IBM Nighthawk
120-qubit square-lattice processor on IBM Quantum Cloud; >5000 two-qubit gates; integrates Quantum + HPC toolchains for error mitigation.

2026 - 2028
IBM Starling Prototype
Early error-corrected logical-qubit demos (200 qubits, 108-gate runs); pilot chemistry & optimization workloads via hybrid cloud access.

2030–2032
Cryptographically Relevant Runs
Controlled Shor's executions on moderate key sizes; NIST IR 8547 deprecates RSA-2048/ECC-256 by 2030 to counter these emerging risks

2035+
Fault-Tolerant Scale-Out
DOE Q-NEXT roadmap (10–15 yr horizon) targets mature interconnects and multi-million-qubit, fault-tolerant architectures for chemistry, AI, and logistics.

การทำความเข้าใจภัยคุกคามจากเทคโนโลยีควอนตัม จำเป็นต้องมีความเข้าใจในส่วนของ ฮาร์ดแวร์พื้นฐาน (underlying hardware) ที่ทำให้การวิเคราะห์ถอดรหัส (cryptanalysis) สามารถเกิดขึ้นได้ โดยแตกต่างจากคอมพิวเตอร์แบบคลาสสิกซึ่งใช้สัญญาณไฟฟ้าในการแทนข้อมูล ระบบควอนตัมใช้คุณสมบัติของวัสดุและโครงสร้างทางกายภาพที่หลากหลายเพื่อจัดการกับ qubits ซึ่งเป็นหน่วยข้อมูลพื้นฐานของการประมวลผลเชิงควอนตัม การนำไปใช้จริงทางกายภาพเหล่านี้ ซึ่งเรียกว่า modalities ต่างก็มีข้อได้เปรียบเฉพาะตัวในด้านประสิทธิภาพ ความคงทนของสถานะควอนตัม (หรือที่เรียกว่า coherence — ระยะเวลาที่สถานะควอนตัมสามารถคงอยู่ได้) และความสามารถในการขยายระบบ แต่ทุกแบบต่างก็ต้องเผชิญกับความท้าทายทางวิศวกรรมอย่างมหาศาล ตารางด้านล่างนี้สรุป รูปแบบหลักของการประมวลผลเชิงควอนตัม (quantum computing modalities) ที่กำลังอยู่ระหว่างการพัฒนา โดยเน้นให้เห็นถึง หลักการสำคัญ และ ความท้าทายหลัก ที่เป็นตัวกำหนดสถานะปัจจุบันของการแข่งขันด้านฮาร์ดแวร์ควอนตัม

การวิเคราะห์เชิงเปรียบเทียบรูปแบบการประมวลผลควอนตัมที่สำคัญ

Modality	Principle	Key Advantages	Major Challenges / Limitations	Representative Systems / Entities
คิวบิตตัวนำยิ่งยวด	Uses Josephson junctions and superconducting loops; microwave pulses manipulate qubit states	Fast gate operations, good compatibility with integrated electronics	Fast gate operations, good compatibility with integrated electronics	Google Sycamore, IBM, Rigetti
ไอออนกักเก็บ	Ions are trapped in vacuum; lasers drive transitions and coupling between ions	Very long coherence times, high-fidelity gates, all-to-all connectivity	Slower gate speeds, scaling to many ions, complexity of laser control	IonQ, Quantinuum
Photonic / Linear-optical	Qubits encoded in photon states (polarization, path, etc.), manipulated via beam splitters, phase shifters, etc.	Room-temperature operation, low decoherence from environment, good for communication	Photon loss, difficulty in deterministic photon sources and gates, detection inefficiencies	PsiQuantum, Xanadu, Jiuzhang (photonic quantum supremacy experiment)
Neutral-atom / Atomic arrays	Atoms are trapped (e.g. via lasers) and coupling between atoms (e.g. via Rydberg interactions) enables gates	Good scalability potential, relatively low sensitivity to stray charges	Precision control, weaker interactions, error rates, engineering complexity	QuEra, Pasqal
Quantum dots / Spin qubits	Use the spin or charge states in semiconductor nanostructures, manipulated by electric / magnetic fields	Potential compatibility with semiconductor fabrication, compact size	Decoherence (noise), coupling two qubits reliably, readout fidelity	Research in Intel, silicon qubit programs
Topological (Majorana)	Qubits stored in nonlocal (topological) degrees of freedom (e.g. Majorana zero modes), manipulated by "braiding" operations	Intrinsic error protection, robustness to local noise	Still mostly theoretical / experimental; creating and controlling topological states is extremely challenging	Microsoft's Majorana 1

ความเสี่ยงของ Harvest-Now/Decrypt-Later (HNDL)

หนึ่งในภัยคุกคามการเข้ารหัสที่เร่งด่วนที่สุดไม่ใช่การโจมตีควอนตัมในอนาคต แต่เป็นการรวบรวมข้อมูลที่เข้ารหัสอย่างเงียบๆ ในปัจจุบันสำหรับการถอดรหัสในวันข้างหน้า รู้จักกันในชื่อ HNDL กลยุทธ์นี้ใช้ประโยชน์จากอายุการเก็บรักษาที่ยาวนานของไฟล์ที่เก็บข้อมูลสำคัญ เช่น ข้อมูลทางการเงิน ข้อมูลทางการแพทย์ ทรัพย์สินทางปัญญา โดยการจัดเก็บข้อความเข้ารหัสจนกว่าระบบควอนตัมจะสามารถทำลาย RSA และ ECC ได้ การทำความเข้าใจลำดับการโจมตีและขั้นตอนการบรรเทาผลกระทบเป็นสิ่งสำคัญในการลดความเสี่ยงก่อนที่ Q-Day จะมาถึง

ลำดับการโจมตี (5 ขั้นตอน)

Passive Capture
บันทึกช่องสัญญาณที่เข้ารหัส (TLS, VPN, อีเมล, การสำรองข้อมูลบนคลาวด์) โดยไม่ต้องถอดรหัสแบบเรียลไทม์

Long-Term Archival
จัดเก็บข้อความเข้ารหัสในที่เก็บที่จัดทำดัชนีสำหรับการวิเคราะห์ในอนาคต

Quantum Maturation
รอการปรับปรุงฮาร์ดแวร์และการแก้ไขข้อผิดพลาดที่มีประสิทธิภาพ

Key Extraction
ใช้อัลกอริทึมของ Shor บนคอมพิวเตอร์ควอนตัมที่มีขนาดเพียงพอสำหรับการโจมตีทางเข้ารหัส เพื่อแยกตัวประกอบของจำนวนเต็มหรือแก้ปัญหา discrete logarithm

Bulk Decryption
ใช้กุญแจที่กู้คืนเพื่อถอดรหัสข้อมูลที่ถูกเก็บทั้งหมด

Mitigation Guidance

Inventory & Prioritize IR 8547 จาก NIST ตั้งค่าสถานะ HNDL ว่าเป็นความเสี่ยงร้ายแรง จัดทำรายการที่เป็นความลับระยะยาวและย้ายสินทรัพย์ที่มีความเสี่ยงสูงสุดไปยัง PQC

Hybrid Deployments Sectigo (พฤษภาคม 2025)[6] แนะนำให้ใช้อัลกอริทึมแบบคลาสสิกและ PQC ควบคู่กันและลดอายุการใช้งานของกุญแจผ่านการเปลี่ยนกุญแจที่เร็วขึ้น

การกำกับดูแลเทคโนโลยีควอนตัม

การก้าวสู่ยุควอนตัมอย่างมีประสิทธิภาพ จำเป็นต้องอาศัยมาตรฐาน กรอบกำกับดูแล และความร่วมมือในระดับต่าง ๆ ที่ประสานกันอย่างรอบคอบ เพื่อสร้างสมดุลระหว่าง นวัตกรรม กับ ความปลอดภัย หน่วยงานภาครัฐและองค์กรอุตสาหกรรมทั่วโลกต่างเผยแพร่แผนยุทธศาสตร์ กำหนดระยะเวลาในการเปลี่ยนผ่าน และส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชน เพื่อให้การนำเทคโนโลยีที่ปลอดภัยต่อควอนตัมมาใช้เป็นไปอย่างราบรื่น ส่วนนี้จะกล่าวถึง ความพยายามด้านการกำกับดูแล (governance efforts) และ best practices ที่สำคัญ เพื่อช่วยให้องค์กรต่าง ๆ สามารถปรับนโยบายและการลงทุนให้สอดคล้องกับข้อกำหนดที่กำลังพัฒนาอย่างต่อเนื่อง

แผนงานการเปลี่ยนผ่านของ NIST

- **IR 8547 (พฤศจิกายน 2024)** การโยกย้าย PQC เป็นระยะๆสอดคล้องกับเป้าหมายของ NSM-10 ในการนำไปใช้อย่างเต็มรูปแบบภายในปี 2035
- **"The Road Ahead" (มี.ค. 2025)[7]"** Updates on algorithm performance and integration guidance .
- **FIPS 203–205 (ส.ค. 2024)** Finalized PQC algorithms-CRYSTALS-Kyber, Dilithium, Falcon.

คำแนะนำของ CISA

- เอกสารข้อมูลความพร้อมด้านควอนตัม (Quantum-Readiness Fact Sheet, 2023): กำหนดให้หน่วยงานและผู้ให้บริการจัดทำแผนยุทธศาสตร์การเปลี่ยนผ่านสู่ระบบ PQC ดำเนินการ Hybrid Testing และจัดอบรมทีมงานด้านความปลอดภัยไซเบอร์ให้มีความรู้ความเข้าใจเกี่ยวกับความเสี่ยงจากเทคโนโลยีควอนตัม[9]

แผนงาน NICT Q-ICT (ญี่ปุ่น)[10]

- Metro QKD Links by 2025: ≥ 1 Mbps บนไฟเบอร์ 50 กม. ทดลองในโตเกียว
- QKD & Repeaters: R&D ใน > 100 กม. เชื่อมต่อรวมเข้ากับเครือข่าย Beyond 5G/6G

มาตรฐานยุโรป (CEN-CENELEC)

- แผนงานปี 2022: แผนงานที่สอดคล้องกันสำหรับ QKD, การเชื่อมต่อระหว่าง PQC และการทดสอบความสามารถในการทำงานร่วมกันระหว่างประเทศสมาชิกสหภาพยุโรป[11]

การประสานความร่วมมือและจริยธรรมระดับโลก (Global Coordination & Ethics)

- ข้อเสนอให้จัดตั้ง "การประชุมมาตรฐานควอนตัมระดับโลก (Global Quantum Standards Forum)" เพื่อสร้างความสอดคล้องของกฎระเบียบระหว่างประเทศ พร้อมทั้งการประเมินนวัตกรรมอย่างมีความรับผิดชอบ (responsible-innovation assessments) และส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชนอย่างโปร่งใส

บทที่ 5

ภาพรวมของ PQC

ภาพรวมของ (PQC)

เมื่อคอมพิวเตอร์ควอนตัมใกล้ถึงจุดที่จะสามารถทำลายโครงสร้างการเข้ารหัสแบบกุญแจสาธารณะที่ใช้อย่างแพร่หลาย (public-key schemes) องค์กรต่างๆจึงจำเป็นต้องเปลี่ยนไปใช้อัลกอริทึมเข้ารหัสที่คงทนต่อการโจมตีทั้งแบบคลาสสิกและควอนตัม[1] PQC ครอบคลุมกลุ่มอัลกอริทึมที่มีพื้นฐานทางคณิตศาสตร์ ซึ่งออกแบบมาให้สามารถทำงานร่วมกับโปรโตคอลและเครือข่ายที่มีอยู่แล้ว ในขณะที่ยังคงความปลอดภัยต่อผู้โจมตีที่มีคอมพิวเตอร์ควอนตัม[2] ในปี2016 NISTได้เผยแพร่เอกสาร IR 8105 เพื่อเริ่มกระบวนการกำหนดมาตรฐานหลายปี โดยประเมินข้อเสนอมากกว่า 70 รายการในห้ากลุ่มอัลกอริทึมหลัก[3] หลังจากผ่านการตรวจสอบสาธารณะอย่างเข้มงวด 3 รอบ NIST ได้สรุปมาตรฐานชุดแรกของอัลกอริทึมเข้ารหัส(CRYSTALS-Kyber)และลายเซ็นดิจิทัล (CRYSTALS-Dilithium, FALCON) ในเดือนสิงหาคม 2024 [4] ส่วนต่อไปจะอธิบาย เป้าหมายของ PQC และการสำรวจกลุ่มอัลกอริทึมหลัก ได้แก่ lattice-based, code-based, multivariate-based, hash-based, และ supersingular-isogeny-based schemes พร้อมยกตัวอย่างสำคัญและอธิบายคำศัพท์เฉพาะทางรวมถึงสมมติฐานที่เกี่ยวข้องทั้งหมด

คำจำกัดความและเป้าหมายของ PQC

PQC มีจุดมุ่งหมายเพื่อแทนที่อัลกอริทึมที่อ่อนแอต่อการโจมตีโดยคอมพิวเตอร์ควอนตัม เช่น RSA และ ECC ด้วยทางเลือกที่สร้างขึ้นบนปัญหาทางคณิตศาสตร์ซึ่งเชื่อว่าปลอดภัยต่อทั้ง อัลกอริทึมของ Shor สำหรับการแยกตัวประกอบและ อัลกอริทึมของ Grover สำหรับการค้นหาอย่างรวดเร็ว[3] เป้าหมายหลักของ PQC ประกอบด้วย

ความต้านทานต่อควอนตัม
ทำให้แน่ใจว่าไม่มีอัลกอริทึมควอนตัมที่ทราบอยู่ในปัจจุบันสามารถถอดรหัสได้อย่างมีประสิทธิภาพ โดยทั่วไปอาศัยปัญหาที่การโจมตีด้วยควอนตัมต้องใช้เวลาแบบ exponential-time เช่น การถอดรหัส noisy lattices หรือการแก้ปัญหา structured code [3]

ความสามารถในการทำงานร่วมกัน – ทำให้อัลกอริทึม PQC
ทำให้อัลกอริทึม PQC ใหม่สามารถเชื่อมต่อกับโครงสร้างพื้นฐานที่มีอยู่แล้ว เช่น TLS, SSH, IPsec ได้โดยไม่ต้องออกแบบโปรโตคอลใหม่ทั้งหมด ลดความซับซ้อนในการปรับใช้งาน [3]

ประสิทธิภาพ
ต้องคำนึงถึงขนาดของกุญแจและลายเซ็น, ภาระการคำนวณ (CPU cycles, หน่วยความจำ), และ network bandwidth เพื่อให้ PQC สามารถทำงานได้อย่างเหมาะสมบนฮาร์ดแวร์ปัจจุบัน ตั้งแต่เซิร์ฟเวอร์ไปจนถึงอุปกรณ์ IoT [2] เพื่อตอบสนองเป้าหมายเหล่านี้ได้PQC จึงมอบเส้นทางการอัปเกรดที่ราบรื่นและปลอดภัย ซึ่งยังคงรักษาความลับ ความสมบูรณ์ และการพิสูจน์ตัวตน(Confidentiality, Integrity, and Availability) ของข้อมูลในยุคที่คอมพิวเตอร์ควอนตัมกำลังใกล้เข้ามา

กลุ่มอัลกอริทึมหลัก

กระบวนการกำหนดมาตรฐาน PQC ของ NIST ได้จัดกลุ่มอัลกอริทึมที่เข้าชิงออกเป็น 5 กลุ่มหลัก โดยแต่ละกลุ่มอิงกับ hardness assumption ที่แตกต่างกัน[6] ตารางด้านล่างสรุป กลุ่มอัลกอริทึมเหล่านี้ ปัญหาพื้นฐานที่ใช้เป็นหลัก และมาตรฐานตัวอย่าง

Family	Core Assumption	Example Schemes
Lattice-based	Learning With Errors (LWE), Module-LWE, Short Integer Solution (SIS)	CRYSTALS-Kyber (KEM), Dilithium (SIG)
Code-based	Hardness of decoding random linear error-correcting codes	Classic McEliece (KEM)
Multivariate	Difficulty of solving large systems of multivariate (quadratic) polynomials	Rainbow (SIG)
Hash-based	Collision- and preimage-resistance of cryptographic hash functions	LMS & XMSS (stateful signatures)
Supersingular Isogeny	Difficulty of computing isogeny maps between supersingular elliptic curves	SIKE (KEM)

Main Algorithm Families

1. Lattice-Based

อัลกอริทึมกลุ่ม lattice-based ใช้ความยากของปัญหาที่นิยามบน จุด lattice หลายมิติ เป็นพื้นฐานด้านความปลอดภัย

- **Learning With Errors (LWE)** ให้เมทริกซ์สุ่ม A และเวกเตอร์ b = A·s + e (mod q) โดย s เป็นเวกเตอร์ลับ (secret vector) และ e เป็น noise การกู้คืน s ถือว่ายากแม้สำหรับคอมพิวเตอร์ควอนตัม
- **Short Integer Solution (SIS)** การหาเวกเตอร์ใน lattice ซึ่งเป็นจำนวนเต็มไม่เป็นศูนย์และมีขนาดสั้น โดยผลรวมของเวกเตอร์ต้องเท่ากับศูนย์

NIST เลือก CRYSTALS-Kyber สำหรับ Key Encapsulation Mechanism (KEM) และ CRYSTALS-Dilithium สำหรับลายเซ็นดิจิทัล ทั้งสองมีขนาดกุญแจและลายเซ็นระดับ kilobytes พร้อมการคำนวณพหุนามที่มีประสิทธิภาพ

- **Key ncapsulation** การเข้ารหัสกุญแจสมมาตรที่ถูกสุ่มด้วยกุญแจสาธารณะและส่งอย่างปลอดภัย
- **ลายเซ็นดิจิทัล** การพิสูจน์ความถูกต้องของข้อความแบบไม่สามารถปฏิเสธได้

2. Code-Based

การเข้ารหัสแบบ code-based ใช้ ปัญหา syndrome decoding เป็นพื้นฐาน

- **Random Linear Codes** รหัสแก้ไขความผิดพลาด เช่น Goppa codes สร้าง codewords จากการคูณ bit ข้อความกับ generator matrix สาธารณะและเพิ่มโครงสร้างที่มีความซ้ำซ้อน
- **Decoding Hardness** การกู้คืนข้อความต้นฉบับจาก codeword แบบสุ่มบวกกับ error ถือว่ายากมาก

Classic McEliece ใช้ Goppa codes แบบไบนารี ขนาดกุญแจสาธารณะใหญ่ (~1 MB) แต่การถอดรหัสและสร้างกุญแจทำได้เร็วมาก เหมาะสำหรับสถานการณ์ที่พื้นที่เก็บกุญแจไม่ใช่ปัจจัยสำคัญ[5]

3.Multivariate

อัลกอริทึม multivariate อาศัยความยากในการแก้สมการกำลังสองหลายตัวบนฟิลด์จำกัด (finite field)

- **Oil–Vinegar Equations** กุญแจสาธารณะเป็นเซตของพหุนามกำลังสองหลายตัวแปร การเซ็นคือการหาค่าเวกเตอร์ที่ทำให้สมการเป็นจริง
- **Rainbow** เวอร์ชั่นแบบหลายชั้นที่ผสมตัวแปร “Oil” กับ “Vinegar” ในแต่ละชั้น เพิ่มประสิทธิภาพและโครงสร้าง

Rainbow มีขนาดลายเซ็นเล็ก (ไม่กี่ kilobytes) และตรวจสอบเร็ว แต่กุญแจสาธารณะอาจใหญ่ และยังอยู่ในระหว่างการศึกษาต่อหลังการประเมินรอบที่ 3 ของ NIST

4.Hash-Based

ลายเซ็นแบบ hash-based ใช้คุณสมบัติของ ฟังก์ชัน cryptographic hash ที่เข้าใจดี

- **Collision Resistance** เป็นไปไม่ได้เชิงการคำนวณที่จะหาค่าข้อมูลสองชุดที่ได้ผลลัพธ์ hash เหมือนกัน
- **Preimage Resistance** การหาข้อมูลต้นฉบับใด ๆ จาก hash output นั้นถือว่ายาก

ตัวอย่างเช่น Leighton–Micali Signature (LMS) และ eXtended Merkle Signature Scheme (XMSS) ใช้ Merkle tree สร้างกุญแจใช้งานครั้งเดียวอย่างปลอดภัยและต้องจัดการ state อย่างระมัดระวังเพื่อหลีกเลี่ยงการใช้ซ้ำ[7]

- **Multi-tree variants (HSS, $XMSS_{(mt)}$)** ใช้หลาย Merkle tree เพื่อรองรับการเซ็นขนาดใหญ่

5. Supersingular Isogeny

Supersingular Isogeny Key Encapsulation (SIKE) ใช้องค์ประกอบดังนี้

- **Elliptic Curves** โค้งเชิงพีชคณิตบนฟิลด์จำกัดที่กฎการบวกบนจุดสร้างเป็นกรุป (group)
- **Isogeny Maps** ฟังก์ชันที่อนุรักษ์โครงสร้าง (morphisms) ระหว่าง elliptic curves การหาค่า isogeny ลับจากพารามิเตอร์เส้นโค้งสาธารณะถือว่ายากแม้สำหรับการโจมตีด้วยควอนตัม

จุดเด่นของ SIKE คือ กุญแจและ ciphertext ขนาดเล็ก (ไม่กี่ร้อย byte) แม้ประสิทธิภาพการเข้ารหัส/ถอดรหัสช้ากว่ากลุ่ม lattice- หรือ code-based ปัจจุบัน SIKE อยู่ในแผนสำรองของ NIST รอการวิเคราะห์เพิ่มเติม[8]

บทที่ 6
มาตรฐานและกระบวนการจัดทำมาตรฐาน

Standards & Standardization Process

มาตรฐานมีบทบาทสำคัญในการตรวจสอบ สร้างความร่วมมือ และการส่งเสริมอัลกอริทึมการเข้ารหัสที่สามารถต้านทานการโจมตีได้ทั้งจากคอมพิวเตอร์แบบคลาสสิกและคอมพิวเตอร์ควอนตัม มาตรฐาน PQC ของ NIST ได้กลายเป็นมาตรฐานอ้างอิงระดับโลก โดยเปิดให้ชุมชนนักวิจัยและผู้เชี่ยวชาญเข้ามามีส่วนร่วมผ่านการประเมินหลายรอบที่มีโปร่งใสและเข้มงวด หลังจากการแข่งขัน 3 รอบ และความคิดเห็นจากผู้เชี่ยวชาญทั่วโลก NIST ได้เผยแพร่มาตรฐาน FIPS ฉบับแรกในเดือนสิงหาคม 2024 ซึ่งระบุอัลกอริทึมทั้งสำหรับการเข้ารหัส (KEM) และการลงลายเซ็นดิจิทัล ที่พร้อมนำไปใช้งานจริงได้[4] นอกจากนี้ในเดือนกรกฎาคม 2022 NIST ได้อัปเดตชุดอัลกอริทึมลายเซ็นเพิ่มเติม โดยเพิ่ม SPHINCS+ และถอดอัลกอริทึมที่ถูกพบช่องโหว่จากการวิเคราะห์ทางปฏิบัติออกจากรายชื่อ [5] ในขณะเดียวกันหน่วยงานและองค์กรมาตรฐานอื่นทั่วโลก เช่น ETSI, ISO/IEC, KISA (เกาหลีใต้), ASEAN, SAC/TC 260 (จีน), NICT (ญี่ปุ่น), Rosstandart (รัสเซีย) และหน่วยงานจากสิงคโปร์อย่าง CSA, MAS และ IMDA ต่างได้ดำเนินการเพื่อให้เกิดความสอดคล้องและสามารถทำงานร่วมกันได้ในระดับภูมิภาค บทนี้จะเริ่มจากการทบทวน ระยะไทม์ไลน์ของ NIST จากนั้นนำเสนอโปรโตคอลที่ได้รับรองอย่างเป็นทางการพร้อมทั้งตัวเลือกอัลกอริทึมสำรองที่ผ่านการตรวจสอบ, และสรุปด้วยภาพรวมของความเคลื่อนไหวจากองค์กรพัฒนามาตรฐานอื่นๆทั่วโลก

โปรโตคอลมาตรฐานและโปรโตคอลสำรอง

ในเดือนสิงหาคม ปี 2024 NIST ได้ให้การรับรองโปรโตคอล KEM จำนวน 3 รายการ และโปรโตคอลลายเซ็นดิจิทัลอีก 3 รายการ ให้เป็นมาตรฐานภายใต้เอกสาร Federal Information Processing Standards (FIPS) 203–205 [4] เมื่อรวมกับการปรับปรุงในเดือนกรกฎาคม ปี 2022 แล้ว ชุดมาตรฐานดังกล่าวครอบคลุมสมมติฐานเชิงคณิตศาสตร์หลักทั้ง lattice-based และ hash-based พร้อมทั้งถอดถอนอัลกอริทึมที่ถูกพบช่องโหว่จากการวิเคราะห์ทางคริปโต [1] นอกจากนี้ NIST ยังได้ระบุชุดทางเลือกสำรองที่ผ่านการตรวจสอบอย่างเข้มงวด ซึ่งครอบคลุมแนวทาง lattice-, code-, และ hash-based เพื่อให้องค์กรต่าง ๆ สามารถพิจารณาใช้ในความต้องการเฉพาะทาง หรือในรอบการกำหนดมาตรฐานในอนาคต [1] ตาราง 6.2 แสดงการเปรียบเทียบระหว่างมาตรฐานปัจจุบันกับโปรโตคอลสำรองที่ได้รับการอนุมัติ

ประเภท	โปรโตคอลมาตรฐาน	ทางเลือกสำรอง
KEM (Encryption)	CRYSTALS-Kyber [4]	NTRU; SABER; Classic McEliece; BIKE; FrodoKEM; HQC [1]
Signatures	CRYSTALS-Dilithium; FALCON; SPHINCS+ [4][5]	Picnic [1]

ระยะและไทม์ไลน์ในการแข่งขัน PQC ของ NIST

กระบวนการกำหนดมาตรฐานของ NIST ได้เริ่มอย่างเป็นทางการด้วยรายงาน IR 8105 ในเดือนเมษายน ปี 2016 ซึ่งเป็นการประกาศ “Call for Proposals” และจัดเวิร์คช็อป PQC ครั้งแรก [16] จากกระบวนการประเมินแบบหลายขั้นตอนได้คัดกรองอัลกอริทึมจาก 69 ข้อเสนอแรกเริ่ม เหลือเพียง 26 รายการ และสุดท้ายได้คัดเลือกอัลกอริทึมหลักและอัลกอริทึมสำรองภายในเดือนกรกฎาคม ปี 2020 [1][2] ความคืบหน้าของการแข่งขันได้รับการรายงานผ่านเอกสารสถานะเป็นระยะๆ ได้แก่ IR 8240, IR 8309 และ IR 8545 ตลอดจนการประชุม PQC ซึ่งเผยแพร่ผลการประเมินด้านความปลอดภัย การทดสอบประสิทธิภาพ และความพร้อมในการใช้งานจริง
ตาราง 6.1 แสดงลำดับเหตุการณ์สำคัญของกระบวนการ PQC โดยสรุป

เม.ย. 2016
NIST IR 8105: การประชุมเชิงปฏิบัติการ PQC เบื้องต้นและรายงานที่พยายามเริ่มต้นในการกำหนดมาตรฐาน [16]

ธ.ค. 2016
ประกาศ "Call for Proposals" อย่างเป็นทางการ [16]

พ.ย. 2017
กำหนดส่งรอบที่ 1; ยอมรับข้อเสนอ 69 รายการ (สถานะใน IR 8240) [2]

พ.ย. 2019
ประกาศรายชื่อข้อเสนอรอบที่ 2 จำนวน 26 รายการ [2]

มี.ค. 2020
NIST IR 8309: รายงานสถานะรอบที่ 2 [3]

ก.ค. 2020
ประกาศข้อเสนอที่เข้ารอบสุดท้ายรอบที่สามและสำรอง [1]

ก.ค. 2022
เพิ่ม SPHINCS+; ถอด Rainbow, GeMSS, SIKE เนื่องจากการผลวิเคราะห์การเข้ารหัสในทางปฏิบัติ [5]

ก.ค. 2024
FIPS 203–205: การเผยแพร่มาตรฐาน PQC สามมาตรฐานแรก (การเข้ารหัสและลายเซ็น) [4]

องค์กรมาตรฐานอื่น ๆ: ETSI, ISO/IEC, และภูมิภาคเอเชีย

องค์กรกำหนดมาตรฐานในระดับภูมิภาคและระดับชาติ เช่น ETSI, ISO/IEC และหน่วยงานในเอเชีย มีบทบาทสำคัญในการส่งเสริมงานของ NIST เพื่อให้เกิดความสามารถในการทำงานร่วมกันได้ทั่วโลก ตอบสนองต่อข้อกำหนดเฉพาะของแต่ละประเทศ และสนับสนุนการทดสอบใช้งานเทคโนโลยีในสภาพแวดล้อมจริง โดย ETSI มุ่งกำหนดรายละเอียดของโปรไฟล์แบบ Hybrid Scheme ขณะที่ ISO/IEC ขยายขอบเขตของมาตรฐานความมั่นคงปลอดภัยหลัก ส่วน KISA และ SAC/TC 260 มีบทบาทในการจัดการแข่งขันระดับชาติและจัดทำแผนยุทธศาสตร์ด้าน ASEAN ส่งเสริมความร่วมมือพหุภาคีในระดับภูมิภาค ขณะที่ NICT สนับสนุนการประยุกต์เทคโนโลยีสารสนเทศและการสื่อสารควอนตัม ในขณะเดียวกัน Rosstandart ได้ปรับปรุงมาตรฐาน GOST ให้ทันสมัย และหน่วยงานของสิงคโปร์ได้แก่ CSA, MAS, และ IMDA ได้ขับเคลื่อนแนวทางและโครงการทดสอบในประเทศ องค์กรเหล่านี้ล้วนมีบทบาทเฉพาะในการพัฒนาระบบนิเวศของ PQC ให้เติบโตอย่างมั่นคงและเป็นมาตรฐานร่วมกันในระดับโลก

ETSI

- **TS 104 015 V1.1.1 "Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies"** (ก.พ. 2025)กำหนดแนวทางการรวม KEMs แบบคลาสสิก (เช่น X25519) เข้ากับ PQC KEMs (เช่น Kyber) ภายใต้ attribute-based policies [6]
- **TR 103 966 V1.1.1 "Deployment Considerations for Hybrid Schemes"** (ต.ค. 2024)วิเคราะห์ประเด็นการจัดการกุญแจ การปรับแต่งสมรรถนะ และการทดสอบแบบปฏิบัติตามข้อกำหนดสำหรับการปรับใช้การเข้ารหัสแบบผสมที่รองรับระบบ PQC [7]

ISO/IEC JTC 1/SC 27

- WG2 ปรับปรุงมาตรฐาน ISO/IEC 18033-3 (อัลกอริทึมการเข้ารหัส) เพื่อรวมชุดทดสอบ และค่าพารามิเตอร์สำหรับ KEM ที่ได้รับอนุมัติจาก NIST รวมถึงปรับปรุง ISO/IEC 19790 (ข้อกำหนดโมดูลการเข้ารหัส) เพื่อบังคับการตรวจสอบความถูกต้องของโมดูล PQC [8]
- เอกสารคณะกรรมการ SD11 (2024) ยืนยันว่าการรวม PQC เข้ามาเป็นส่วนหนึ่งของมาตรฐานถือเป็นวาระสำคัญที่สุดของ SC 27 [9]

เกาหลีใต้ (KISA)

- Quantum-Resistant Cryptography National Contest (KpqC) เริ่มในเดือนพฤศจิกายน 2021 ภายในธันวาคม 2023 มีอัลกอริทึม 16 รายการผ่านเข้าสู่รอบแรก และคัดเหลือ 4 รายสุดท้ายในเดือนมกราคม 2025 ตามแผนปฏิบัติการระดับชาติ [10]
- Quantum-Safe Cryptography Standardization Roadmap (2023) กำหนดให้มีการทดสอบ การรับรอง และการปรับใช้ PQC อย่างเป็นขั้นตอนในภาคส่วนสำคัญภายในปี 2026 [11]

อาเซียน

- ส่งเสริมการจัดเวิร์คช็อปด้าน PQC ระดับภูมิภาค การประเมินร่วมกัน และการออกแนวทางมาตรฐานที่สอดคล้องกัน เพื่อปรับใช้อัลกอริทึมที่ปลอดภัยต่อควอนตัมเข้าสู่กรอบความมั่นคงไซเบอร์ระดับชาติ [12]
- ประเทศสมาชิกยังดำเนินโครงการนำร่อง เช่น การทดลองสื่อสารข้อมูลปลอดภัยข้ามพรมแดน เพื่อเตรียมความพร้อมต่อภัยคุกคามจากควอนตัมในอนาคต

จีน (SAC/TC 260)

- ประกาศเรื่องข้อเสนอระหว่างประเทศด้านมาตรฐานความมั่นคงไซเบอร์และ PQC (23 ม.ค. 2025) เชิญชวนผู้มีส่วนร่วมภายในประเทศเข้าร่วมการจัดทำมาตรฐานร่วมกับ ISO/IEC เพื่อให้มาตรฐานไซเบอร์ของจีนสอดคล้องกับความพยายามระดับโลกด้าน PQC [13]

ญี่ปุ่น NICT)

- Q-ICT Roadmap (2023) วางแผนระยะการนำ QKD มาใช้งาน การใช้ PQC เข้ากับเครือข่ายยุคหลังจาก 5G และการสนับสนุนการกำหนดมาตรฐานสำหรับโครงข่ายควอนตัมในระดับเมืองและระยะทางไกล [14]

รัสเซีย (Rosstandart)

- ในฐานะสมาชิกที่เข้าร่วม ISO/IEC JTC 1/SC 27Rosstandart มีส่วนร่วมในการแก้ไขมาตรฐานการเข้ารหัส GOST R 34 เพื่อรวมอัลกอริทึม PQC และเผยแพร่แนวทางระดับชาติที่สอดคล้องกับพัฒนาการของ ISO/IEC [15]

สิงค์โปร (CSA, MAS, IMDA)

- CSA Quantum Security Guidelines (ธ.ค. 2024) จัดทำกรอบการวางแผนเพื่อการเปลี่ยนผ่านสู่ระบบที่ปลอดภัยต่อควอนตัม [17]
- MAS Advisory on PQC (2023) กำหนดให้สถาบันการเงินต้องตรวจสอบสินทรัพย์การเข้ารหัสที่ใช้ และเริ่มนำอัลกอริทึม PQC มาใช้งาน [18] นอกจากนี้ยังแนะนำการสร้าง QKD sandbox เพื่อประเมินการใช้งานจริงของ QKD[18]
- IMDA National Quantum-Safe Network Plus (NQSN+) Framework (มิ.ย. 2023) จัดตั้งการทดสอบโครงข่ายระดับประเทศและมาตรฐานอ้างอิงสำหรับเครือข่าย Hybrid QKD–PQC โดยร่วมมือกับ ITU-T และพันธมิตรภาคอุตสาหกรรม [19]

แนวทางเชิงปฏิบัติสำหรับประเทศไทยและอาเซียน

- การประสานงานของภาครัฐ:ประสานหน่วยงานที่เกี่ยวข้องของไทย (เช่น NCSA ด้านความมั่นคงไซเบอร์ระดับชาติ, NT ด้านโครงข่ายโทรคมนาคม หรือหน่วยงานกำกับดูแลด้านนั้น ๆ เช่น NBTC และ BOT) เพื่อจัดทำแผนการเปลี่ยนผ่าน (migration phase) ให้สอดคล้องกับกรอบนโยบายและรอบการรายงาน
- **โครงการนำร่องโครงสร้างพื้นฐานที่สำคัญ**เริ่มจากเครือข่ายที่รองรับบริการภาครัฐ การเงิน สาธารณสุข และสาธารณูปโภคโดยทดลองใช้ hybrid TLS/IPsec และ PQC-wrapped key envelopes ภายในระบบจัดการกุญแจ (KMS/HSM)
- **ความพร้อมของระบบนิเวศในประเทศ:**ร่วมมือกับมหาวิทยาลัยไทยและสตาร์ทอัพในภูมิภาค เพื่อทำการทดสอบการทำงานร่วมกัน (interoperability testing) การฝึกอบรม และโครงการนำร่อง

เพื่อลดความเสี่ยงในการใช้งานและเสริมสร้างขีดความสามารถในประเทศ

- **การทำงานร่วมกันข้ามพรมแดน:**การไหลเวียนข้อมูลภายในอาเซียน (คลาวด์ การชำระเงิน โลจิสติกส์) จะได้รับประโยชน์จากโปรไฟล์ hybrid ที่สอดคล้องกันจึงควรวางแผนความเข้ากันได้กับพันธมิตรต่างประเทศ เพื่อหลีกเลี่ยง vendor lock-in
- **การจัดซื้อและการปฏิบัติตามกฎ:**กำหนดคุณสมบัติ crypto-agility และแผนการรองรับ PQC ลงใน TOR/RFP และ SLAสำหรับหน่วยงานที่อยู่ภายใต้การกำกับ ควรเชื่อมโยงตัวชี้วัด (KPI) เข้ากับข้อกำหนดด้านการบริหารความเสี่ยงและความคงทนในการดำเนินงาน

ขั้นตอนต่อไปที่แนะนำสำหรับผู้มีส่วนได้ส่วนเสียในประเทศไทย

- จัดตั้ง คณะทำงานการเปลี่ยนผ่านสู่ PQC (PQC Migration Working Group) ร่วมระหว่างภาครัฐ ผู้ให้บริการเครือข่าย และผู้จำหน่ายระบบสำคัญ
- สร้าง แม่แบบบัญชีทรัพย์สินการเข้ารหัสสำหรับประเทศไทย (Thai-context cryptography inventory template) ทั้งภาษาอังกฤษและไทย โดยระบุอัลกอริทึม ความยาวกุญแจ เจ้าของระบบ ขอบเขต การรักษาความลับ และการเชื่อมโยงกับข้อบังคับ
- agency/enterprise security, NT/ISP partners, and critical vendors.
- จัดตั้ง คณะกรรมการกำกับดูแล (governance review) เพื่อติดตาม KPI ความพร้อมของผู้ผลิต และปัญหาความเข้ากันได้ข้ามพรมแดน โดยเฉพาะในโครงสร้างและบริการพื้นฐานสำคัญ

บทที่ 7

แผนในการย้ายระบบ / แบบปฏิบัติที่ดีที่สุด

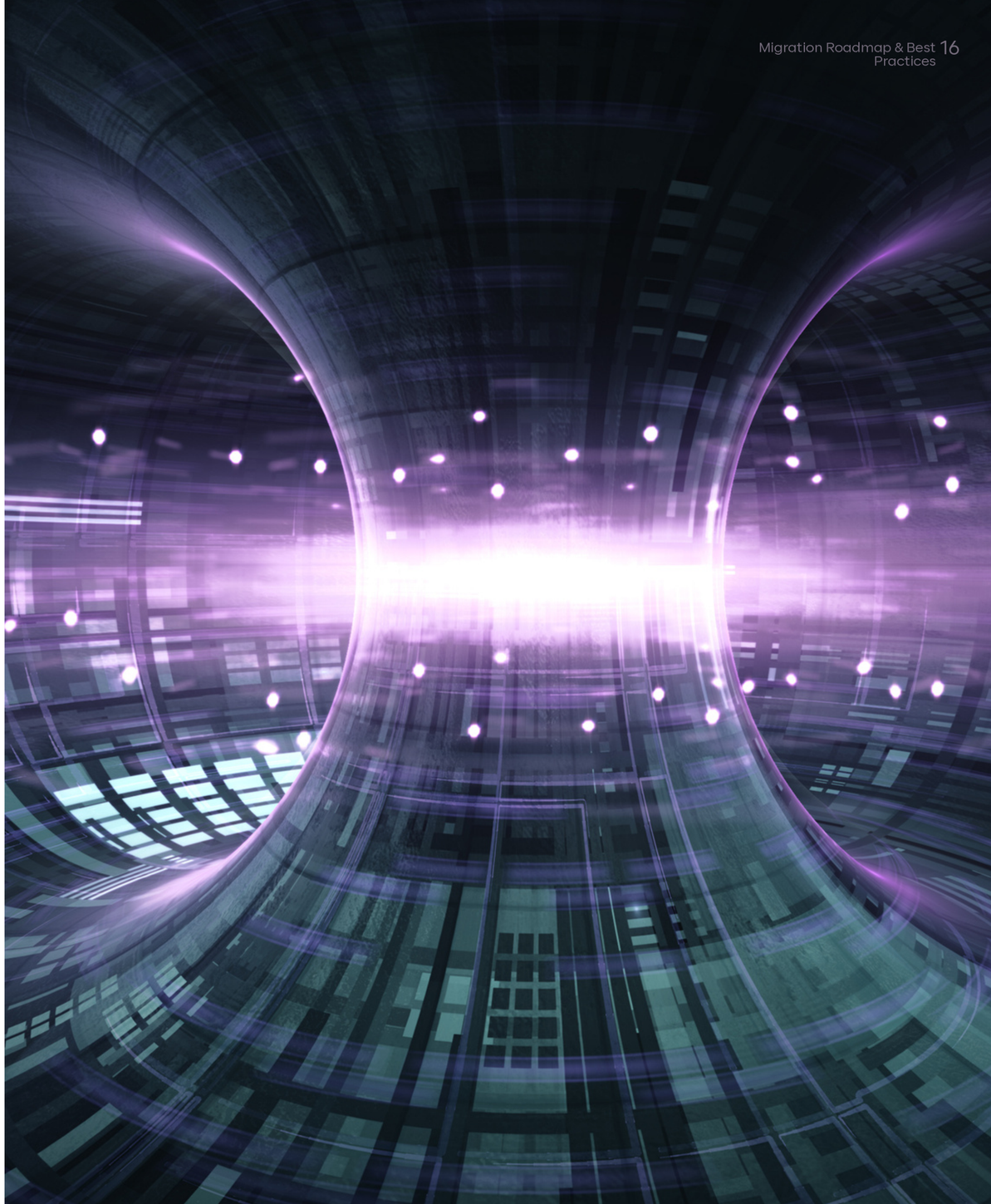
แผนในการย้ายระบบ / แบบปฏิบัติที่ดีที่สุด

การเปลี่ยนผ่านสู่ PQC เป็นความจำเป็นเชิงยุทธศาสตร์ซึ่งรวมถึงบุคลากร กระบวนการและเทคโนโลยี แผนปฏิบัติในการย้ายระบบจะประสบผลสำเร็จได้นั้น เริ่มต้นจากการทำรายการสินทรัพย์เข้ารหัสที่มีอยู่ ตามด้วย phased rollout เพื่อลดความเสี่ยงและยังทำให้ธุรกิจดำเนินไปได้ต่อเนื่อง [1][2] การทดสอบการทำงานร่วมกัน อย่างเคร่งครัดและการตรวจสอบความถูกต้องของโมดูลช่วยให้มั่นใจได้ว่าระบบ PQC พื้นฐาน สามารถผสานรวมกับระบบเดิมได้อย่างราบรื่นและเป็นไปตามข้อกำหนดในแผนปฏิบัติ [3][4] สิ่งที่สำคัญไม่แพ้กันคือ การพัฒนาความพร้อมของบุคลากร ทีมความปลอดภัยต้องเข้าใจคุณสมบัติของอัลกอริทึม หมั่นจัดการ key lifecycle และตอบสนองต่อปัญหาการผสานรวมระบบอย่างทันท่วงที [5][6] การใส่ความสามารถด้าน Crypto-Agility ช่วยให้สามารถแทนที่อัลกอริทึมได้อย่างรวดเร็ว และรองรับการตอบสนองต่อช่องโหว่ใหม่ๆ และการกำกับดูแลอย่างต่อเนื่องรับประกันว่าสินทรัพย์ที่เข้ารหัสจะปรับเปลี่ยนได้เมื่อเวลาผ่านไป [7][8][9]

การทำรายการและจำแนกประเภทสินทรัพย์เข้ารหัสที่มีอยู่

หนึ่งในรากฐานของการเปลี่ยนระบบการเข้ารหัสคือการทำรายการที่ถูกต้องและเป็นปัจจุบัน ตามมาตรฐาน IR 8547 ของ NIST แนะนำให้องค์กรจัดทำรายการทุกสิ่งที่มีการเข้ารหัส การใช้ลายเซ็นดิจิทัล หรือการแลกเปลี่ยนกุญแจ ครอบคลุมทั้งซิร์ฟเวอร์ แอปพลิเคชัน อุปกรณ์เครือข่ายและไลบรารีการเข้ารหัส [1] สำหรับสินทรัพย์แต่ละรายการ ให้บันทึกชื่ออัลกอริทึม (เช่น RSA-2048) ความยาวกุญแจ โหมดการทำงาน (เช่น RSA-OAEP สำหรับการห่อกุญแจ) และบริบทการใช้งาน (TLS, S/MIME, การลงนามโค้ด (code-signing), การเข้ารหัสฐานข้อมูล) ประเมิน dependency เช่น hardware security modules (HSM), KMS ที่จัดการโดยคลาวด์ และ SDK ของบุคคลที่สามเพื่อค้นหาการใช้งานที่ซ่อนอยู่ จัดประเภทสินทรัพย์ตามขอบเขตการรักษาความลับ ซึ่งเป็นช่วงเวลาที่ข้อมูลต้องถูกรักษาไว้อย่างปลอดภัย (เช่น เก็บ log ชั่วคราว 1 ปี เก็บข้อมูลทางการเงิน 10 ปี) เพื่อจัดลำดับความสำคัญของการย้ายระบบที่มีผลกระทบสูง [1] ท้ายสุด ให้เชื่อมโยงสินทรัพย์แต่ละรายการกับเจ้าของ และโปรไฟล์ความเสี่ยงเพื่อเพิ่มประสิทธิภาพการกำกับดูแล

- **เครื่องมือค้นหา** ใช้ประโยชน์จากการสแกนอัตโนมัติและเครื่องมือวิเคราะห์โค้ดเพื่อตรวจจับการเรียกใช้ API การเข้ารหัส และเก็บใบรับรอง
- **การแท็ค** ใส่คำอธิบายประกอบ (annotate) สินทรัพย์แต่ละรายการด้วย attribute ที่กำหนดเอง : การจำแนกประเภทข้อมูล ข้อควรปฏิบัติ (เช่น ข้อมูล GDPR) และขั้นตอนการกู้คืน
- **การให้คะแนนความเสี่ยง** ใช้แบบจำลองการให้คะแนนที่ให้น้ำหนักกับปัจจัยต่างๆ เช่น ความอ่อนไหวของข้อมูล attack surface และขอบเขตการรักษาความลับ



กลยุทธ์

Phased Rollout จะช่วยสร้างสมดุลระหว่างการลดความเสี่ยงต่อภัยคุกคามทางควอนตัมกับการรักษาเสถียรภาพของระบบ รายงาน NIST IR 8547 กำหนดแนวทาง โดยเริ่มต้นด้วยการตรวจสอบฟังก์ชัดการทำงานพื้นฐานบนระบบทดสอบ จากนั้นนำร่อง PQC ในบริการที่มีความเสี่ยงต่ำ ก่อนขยายไปสู่ระบบที่มีความสำคัญเชิงภารกิจ (mission-critical systems) [1] ข้อมูลเบื้องต้นของ CISA เน้นย้ำถึงการมีส่วนร่วมของผู้จัดจำหน่ายในการยืนยันล่วงหน้าว่าจะมีการสนับสนุน PQC ในแผนงานการสร้างผลิตภัณฑ์และการอัปเดตเฟิร์มแวร์ [2] แต่ละระยะควรรวมการวัดประสิทธิภาพ (performance benchmarks) การทดสอบเพื่อรับมือข้อผิดพลาด (error-handling tests) และแผนย้อนระบบ (rollback plans) การจดบันทึกสิ่งที่ได้เรียนรู้ในแต่ละรอบจะช่วยลดความเสี่ยงในการย้ายสินทรัพย์ที่มีมูลค่าสูง

- **ระยะที่ 1 Proof-of-Concept (PoC)** ปรับใช้ PQC ในสภาพแวดล้อมที่ถูกแยกไว้ต่างหาก ตรวจสอบการสร้างกุญแจ การเข้ารหัส/ถอดรหัส และลำดับการสร้างลายเซ็นดิจิทัล
- **ระยะที่ 2 การนำร่อง** เผสานรวม PQC เข้ากับจุดเชื่อมต่อกับระบบจริงบางกลุ่ม (เช่น เกตเวย์ VPN, API ขององค์กรพันธมิตร) วัดเวลาที่ใช้ของแฮนด์เชค (handshake) overhead ของ CPU/หน่วยความจำ และอัตราความผิดพลาด
- **Phase ระยะที่ 3 การปรับใช้ในวงกว้าง** ขยายไปยังบริการที่ลูกค้าใช้งาน (เช่น TLS บนเว็บ, แอปพลิเคชันมือถือ) บังคับใช้โหมดผสม (คลาสสิก+PQC) เพื่อรักษาความสามารถในการทำงานร่วมกัน
- **Phase ระยะที่ 4 การยุติการสนับสนุนและการตรวจสอบ** เมื่อตรวจสอบว่า PQC ถูกใช้จนครอบคลุมหมดแล้ว จึงค่อยนำอัลกอริทึมเก่าออก และดำเนินการตรวจสอบโดยบุคคลที่สามเพื่อยืนยันว่าเป็นไปตามแบบปฏิบัติ

การทดสอบการทำงานร่วมกันและกรอบการตรวจสอบ

การทดสอบช่วยยืนยันได้ว่าแผนพัฒนา PQC ที่แตกต่างกันสามารถสื่อสารได้อย่างถูกต้องในสถานการณ์จริง รายงาน NIST SP 1800-38C ให้กระบวนการทำงานที่มีประสิทธิภาพและสามารถทำงานร่วมกันได้ ประกอบด้วยชุดทดสอบ ตัวอย่างการตั้งค่า (sample configuration) และ failure-mode analysis [3] การตรวจสอบตามมาตรฐาน FIPS 140-3 ภายใต้ CMVP รับรองว่าโมดูลการเข้ารหัสเป็นไปตามความปลอดภัยที่กำหนดไว้และความต้องการการป้องกันทางกายภาพ [4] กรอบเหล่านี้ทำงานร่วมกันเพื่อลดความเสี่ยงของการติดตั้งโดยการตรวจจับปัญหารวมระบบ เช่น ชุดพารามิเตอร์ที่ไม่ตรงกันหรือ overflow จากขนาดของข้อความตั้งแต่เนิ่นๆ ของกระบวนการ

- **การตรวจเวกเตอร์ทดสอบ** ใช้แพ็คเกจเวกเตอร์ทดสอบ PQC ที่ออกเป็นทางการโดย NIST เพื่อให้แน่ใจว่าการใช้งานแต่ละครั้งจะสร้างข้อความเข้ารหัส ข้อมูลลับที่ใช้ร่วมกัน หรือลายเซ็นที่ถูกต้อง เมื่อรับข้อมูลที่กำหนด
- **ความสามารถในการทำงานร่วมกันของโปรโตคอล** ดำเนินการเชื่อมต่อ Hybrid TLS ที่รวมแบบคลาสสิก (เช่น X25519) และ PQC KEMs (เช่น Kyber) เข้าด้วยกัน บันทึกอัตราความสำเร็จของการเชื่อมต่อ เวลาที่ข้อมูลเดินทางไป-กลับ และการ fallback
- **การรับรองโมดูล** โมดูลฮาร์ดแวร์และซอฟต์แวร์ที่มี PQC ไปยังห้องปฏิบัติการทดสอบ FIPS 140-3 ตรวจสอบความถูกต้องของส่วนต่อประสานเชิงตรรกะ (logical interfaces) การจัดการสถานะ และการป้องกันจากช่องทางแฝง (side-channel resistance)

การฝึกอบรมและความพร้อมในการปฏิบัติงาน

บุคลากรคือหัวใจสำคัญของการย้ายระบบ PQC ให้สำเร็จลุล่วงไปได้ ในรายงาน NIST SP 800-50 และ SP 800-16 นำเสนอแนวทางในการสร้างโปรแกรมฝึกอบรมตามบทบาทหน้าที่ ตั้งแต่การบรรยายสรุปสำหรับผู้บริหารไปจนถึงห้องปฏิบัติการเชิงลึกสำหรับวิศวกรการเข้ารหัส [5][6] สำหรับเนื้อหาส่วน PQC หลักสูตรควรครอบคลุมหลักการอัลกอริทึม การเลือกพารามิเตอร์ (เช่น ระดับความปลอดภัย) การผสานรวมไลบรารี (เช่น OpenSSL, BoringSSL PQC forks) และขั้นตอนการตอบสนองเหตุการณ์ (incident response) เมื่อการเข้ารหัสล้มเหลว

- **ความตระหนักรู้ของผู้บริหาร** เวิร์กช็อปที่อธิบายภัยคุกคามทางควอนตัม ไทม์ไลน์การย้ายระบบ และผลกระทบทางธุรกิจ เพื่อให้มั่นใจว่าผู้นำองค์กรยอมรับ
- **เจาะลึกทางเทคนิค** การฝึกปฏิบัติที่วิศวกรจะนำ PQC KEM และ Signature API ไปใช้จริง แก้ไขข้อผิดพลาดตอนนำไปใช้ และประเมินประสิทธิภาพการทำงาน
- **คู่มือการปฏิบัติงาน** สร้างคู่มือการปฏิบัติงานที่ให้รายละเอียดเกี่ยวกับการสร้างกุญแจ PQC กำหนดการหมุนเวียน กระบวนการสำรองข้อมูล และขั้นตอนการย้อนระบบ
- **การฝึกซ้อมตอบสนอมเหตุการร์** จำลองความล้มเหลวในการเข้ารหัส (เช่น การใช้อัลกอริทึมที่เลิกใช้แล้ว) และฝึกฝนขั้นตอนการกู้คืนระบบ

Crypto-Agility และ การรวมเฟรมเวิร์ค

Crypto-agility คือความสามารถขององค์กรในการเปลี่ยนอัลกอริทึมและพารามิเตอร์การเข้ารหัสได้อย่างรวดเร็วเพื่อตอบสนองต่อช่องโหว่ใหม่ๆ หรือการอัพเดตมาตรฐาน ในรายงาน NIST SP 800-57 ตอนที่ 3 และ IR 8417 ระบุรูปแบบสถาปัตยกรรม เช่น ชั้นนามธรรม (abstraction layers) เอนจินนโยบาย (policy engines) และส่วนห่อหุ้มกุญแจเข้ารหัส (key envelopes) ที่แยกตรรกะของแอปพลิเคชันออกจากอัลกอริทึมเฉพาะ [7][8] เฟรมเวิร์คความปลอดภัยไซเบอร์ของ NIST 2.0 ที่กำลังเกิดขึ้นใหม่ ได้รวมการเข้ารหัสไว้ในฟังก์ชัน “ป้องกัน” “ตรวจจับ” และ “ตอบสนอง” โดยเน้นการตรวจสอบอัลกอริทึมอย่างต่อเนื่องและกลไกที่มาแทนที่ [9] ในมาตรฐาน ISO/IEC 27001 (มาตรการควบคุม A.10.1.2) และแนวทาง Crypto-Agility ของ ENISA ก็กำหนดแนวทางการวางแผนการย้ายอัลกอริทึมและการใช้งานการเข้ารหัสแบบโมดูลาร์ในทำนองเดียวกัน

- **Abstraction Layers** I พัฒนาการให้บริการการเข้ารหัส (cryptographic service providers: CSP) หรือ API เพื่อบริการการเข้ารหัสทั่วไป (เข้ารหัส ถอดรหัส ลงนาม ตรวจสอบ) โดยซ่อนรายละเอียดอัลกอริทึม
- **Policy Engines** จัดเก็บส่วนกำหนดอัลกอริทึม (algorithm preferences) และขั้นตอนการปรับค่าพารามิเตอร์ไว้ในไฟล์ภายนอกหรือฐานข้อมูลการตั้งค่า (configuration database) เพื่อหลีกเลี่ยงการเปลี่ยนแปลงโค้ดจากการสลับอัลกอริทึม
- **Key Envelopes** ห่อหุ้มกุญแจเข้ารหัสข้อมูล (data-encryption keys: DEK) ด้วยกุญแจสำหรับเข้ารหัสกุญแจ (key-encryption keys: KEK) ที่ผูกกับอัลกอริทึมเฉพาะ ทำให้การเข้ารหัสซ้ำจำนวนมากง่ายขึ้นเมื่ออัลกอริทึม KEK เปลี่ยนแปลง
- **Vendor Requirements** รวม Crypto-Agility ไว้ในสัญญาจัดซื้อจัดจ้าง และกำหนดให้มีการอัปเดตเฟิร์มแวร์หรือไลบรารีอย่างทันท่วงทีเพื่อรองรับอัลกอริทึมใหม่

การตรวจสอบ ประเมินผล และกำกับดูแลอย่างต่อเนื่อง

ความเสี่ยงด้านการเข้ารหัสเปลี่ยนแปลงอยู่ตลอด การโจมตีใหม่ๆ การเลิกใช้บางอัลกอริทึม หรือข้อบกพร่องจากการพัฒนาอาจเกิดขึ้นได้ทุกเมื่อ การหมั่นตรวจสอบและกำกับดูแลอย่างต่อเนื่องช่วยให้มั่นใจได้ว่าระบบการเข้ารหัสยังคงแข็งแรง ฟังก์ชัน "ตรวจจับ" และ "ตอบสนอง" ของ NIST CSF 2.0 กำหนดให้มีการแจ้งเตือนอัตโนมัติหากใช้อัลกอริทึมที่เลิกใช้แล้ว เกิดความผิดปกติในประสิทธิภาพของระบบ และความล้มเหลวในการตรวจสอบ (validation failure) [9] FIPS 140-3 revalidation cycles และ ISO/IEC 27002 A.12.6.1 ซึ่งเกี่ยวกับการตรวจทานทางเทคนิค (technical review) ของแอปพลิเคชัน บ่งชี้ถึงความจำเป็นในการตรวจสอบซ้ำ

- **Automated Alerts แจ้งเตือนอัตโนมัติ** รวม log จากโมดูลการเข้ารหัสเข้ากับระบบ SIEM และตั้งค่าการแจ้งเตือนสำหรับการใช้อัลกอริทึมที่เลิกใช้แล้วหรือการตรวจสอบใบรับรองที่ล้มเหลว
- **เกณฑ์มาตรฐานประสิทธิภาพ** รักษาตัวชี้วัดเกี่ยวกับเวลาในการเข้ารหัส/ถอดรหัส อัตราข้อผิดพลาด และการใช้ทรัพยากร ตรวจสอบความเบี่ยงเบนที่สำคัญ
- **Vulnerability Assessments ประเมินช่องโหว่** กำหนดการทดสอบเจาะระบบโดยบุคคลที่สามเป็นประจำทุกปี โดยมุ่งเน้นที่การใช้งานการเข้ารหัส รวมถึงช่องทางแฝงและ injection
- **ประเมินโดยคณะกรรมการกำกับดูแล**จัดตั้งคณะกรรมการกำกับดูแลการเข้ารหัสทุกไตรมาสเพื่อประเมินผลการตรวจสอบ วางแผนงานอัลกอริทึม รายงานการตอบสนองเหตุการณ์ (incident report) และอัปเดตแผนการย้ายระบบ

บทที่ 8

กฎระเบียบ การปฏิบัติ และการกำกับดูแล

กฎระเบียบ การปฏิบัติ และการกำกับดูแล

ในขณะที่องค์กรต่างๆ กำลังก้าวไปสู่การดำเนินงานที่ปลอดภัยต่อควอนตัม องค์กรเหล่านั้นต้องรับมือกับกรอบการทำงานที่ซับซ้อนของแนวทาง ข้อบังคับ และกรอบการกำกับดูแล กฎระเบียบในปัจจุบันได้สร้างแรงกดดันที่ขยายขอบเขตไปไกลกว่าความปลอดภัยของเทคโนโลยีสารสนเทศแบบคลาสสิก ไปสู่ความพร้อมด้านควอนตัม ซึ่งบังคับให้องค์กรต่างๆ ต้องผนวก Crypto-Agility เข้าไว้ในโปรแกรมการบริหารความเสี่ยงและแผนปฏิบัติ ในบทนี้จะพิจารณา (ก) แนวทางระดับโลกที่ตั้งความคาดหวังในภาพรวม (ข) ข้อบังคับเฉพาะอุตสาหกรรมที่กำหนดแผนปฏิบัติในแต่ละภาคส่วน (ค) กรอบการกำกับดูแลที่ครอบคลุมสำหรับนโยบาย การกำกับดูแล และการตรวจสอบ และ (ง) ระบบนิเวศของผู้จัดจำหน่าย รวมถึงหน่วยงานรับรอง ผู้บริหารสามารถปรับกลยุทธ์การเข้ารหัสหลังควอนตัม ให้สอดคล้องกับพันธกิจในปัจจุบันและพันธกิจที่เกิดขึ้นใหม่ได้ โดยการทำความเข้าใจองค์ประกอบเหล่านี้และคำศัพท์เฉพาะที่ใช้

แนวทางระดับโลก

แนวทางระดับโลกเป็นเครื่องมือภาพรวมทางนโยบาย ซึ่งมักเป็นคำแนะนำที่ไม่มีผลผูกพัน ซึ่งออกโดยรัฐบาลหรือองค์กรนานาชาติเพื่อประสานแนวปฏิบัติข้ามพรมแดน

- คำแนะนำของคณะกรรมาธิการยุโรปเกี่ยวกับการเข้ารหัสหลังควอนตัม กระตุ้นให้ประเทศสมาชิกพัฒนาแผนประสานงานสำหรับการย้ายไปยังอัลกอริทึมที่ต้านทานควอนตัมภายในปี 2026 (สำหรับโครงสร้างพื้นฐานทั่วไป) และปี 2030 (สำหรับระบบบริการสำคัญ) [1]
- การศึกษาของคณะกรรมการที่ปรึกษาด้านความมั่นคงแห่งชาติด้านโทรคมนาคมของสหรัฐอเมริกา (U.S. NSTAC) ว่าด้วยการเตรียมพร้อมระดับชาติสำหรับการเข้ารหัสหลังควอนตัม (สิงหาคม 2024) วิเคราะห์ช่องว่างด้านความปลอดภัยของโครงสร้างพื้นฐานสำคัญ รายงานของ NSTAC ให้ข้อมูลแก่นโยบายของประธานาธิบดี แต่ไม่ได้มีผลบังคับใช้ทางกฎหมาย [2]
- รายงาน NIST IR 8547 (“ฉบับร่างสาธารณะฉบับแรก”) กำหนดแผนงาน phased migration อย่างเป็นทางการ โดยกำหนดแนวคิดสำคัญต่างๆ เช่น ขอบเขตการรักษาความลับ (ระยะเวลาที่ข้อมูลต้องคงความปลอดภัย) และ hybrid deployment(การใช้อัลกอริทึมแบบคลาสสิกและแบบ PQC ควบคู่กัน) เพื่อสร้างมาตรฐานแนวทางปฏิบัติของรัฐบาลกลางสหรัฐอเมริกา [3]
- ETSI TS 104 015 V1.1.1 เป็นข้อกำหนดทางเทคนิคที่กำหนด hybrid key-exchange ที่รวมอัลกอริทึมคลาสสิก (เช่น X25519) กับ KEM (เช่น Kyber) ภายใต้ attribute-based access policies สำหรับการควบคุมการถอดรหัสแบบละเอียด [4]
- ITU-T Recommendation Y.3800 กำหนดกรอบสถาปัตยกรรมสำหรับ QKD โดยกำหนดคำศัพท์ต่างๆ เช่น QKD link, trusted node และ key-management layer เพื่อให้มั่นใจว่าสามารถทำงานร่วมกันได้ทั่วโลก [5]
- BIS (Bank for International Settlements) Paper No 158 เรื่อง “ความพร้อมด้านควอนตัมสำหรับระบบการเงิน: หมวดแผนงาน” ได้ให้กรอบโครงสร้างสำหรับธนาคารกลางและสถาบันการเงิน

ข้อบังคับเฉพาะอุตสาหกรรม

ข้อบังคับเฉพาะอุตสาหกรรม คือ ข้อกำหนดหรือมาตรฐานที่อยู่ในระบบการปฏิบัติเฉพาะภาคส่วน

ภาคการเงิน

- EBA (European Banking Authority) Guidelines on ICT (Information and Communications Technology) and Security Risk Management (EBA/GL/2019/04) กำหนดให้มีการประเมินความเสี่ยงด้านการเข้ารหัสและ key rotation policy ที่เข้มงวด แนวทางเหล่านี้เป็นส่วนหนึ่งของ DORA (Digital Operational Resilience Act) ของสหภาพยุโรป ซึ่งกำหนดให้สถาบันการเงินรักษาความสามารถด้าน Crypto-Agility กล่าวคือ ความสามารถในการปรับเปลี่ยนอัลกอริทึมได้อย่างรวดเร็ว เพื่อสนับสนุนการดำเนินการอย่างต่อเนื่อง [6][7]
- MAS (Monetary Authority of Singapore) Advisory MAS/TCRS/2024/01 ระบุถึงความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่เกิดจากการประมวลผลควอนตัม และแนะนำมาตรการต่างๆ เช่น การทำรายการอัลกอริทึม การใช้ hybrid-scheme และการอัปเดตการกำกับดูแลสำหรับสถาบันการเงิน [14]

ภาคสาธารณะสุข

- FDA (U.S. Food and Drug Administration) “Cybersecurity in Medical Devices” Guidance (มิถุนายน 2025) กำหนดให้ผู้ผลิตอุปกรณ์ต้องแสดงให้เห็นถึงความมั่นใจอย่างสมควร ว่าการควบคุมการเข้ารหัสยังคงมีประสิทธิภาพตลอดวงจรชีวิตผลิตภัณฑ์ และวางแผนสำหรับการปรับปรุงอัลกอริทึมหลังวางจำหน่าย [8]

ภาคโครงสร้างพื้นฐานสำคัญ

- CISA (Cybersecurity and Infrastructure Security Agency) Critical Infrastructure Cybersecurity Framework ได้รวมการค้นพบการประเมินช่องโหว่จากควอนตัมของ RAND มาใช้ โดยกระตุ้นให้ผู้ประกอบการพัฒนาแผนงาน PQC เฉพาะภาคส่วน และให้ quantum-hardening เป็นส่วนสำคัญในกิจกรรมด้านความคงทน [9]

กรอบนโยบายและการกำกับดูแล

เพื่อควบคุมการนำ PQC มาใช้ องค์กรต่างๆ ควรใช้ประโยชน์จากการกำกับดูแลและการปฏิบัติตามกฎระเบียบที่ได้กำหนดไว้แล้ว ดังนี้

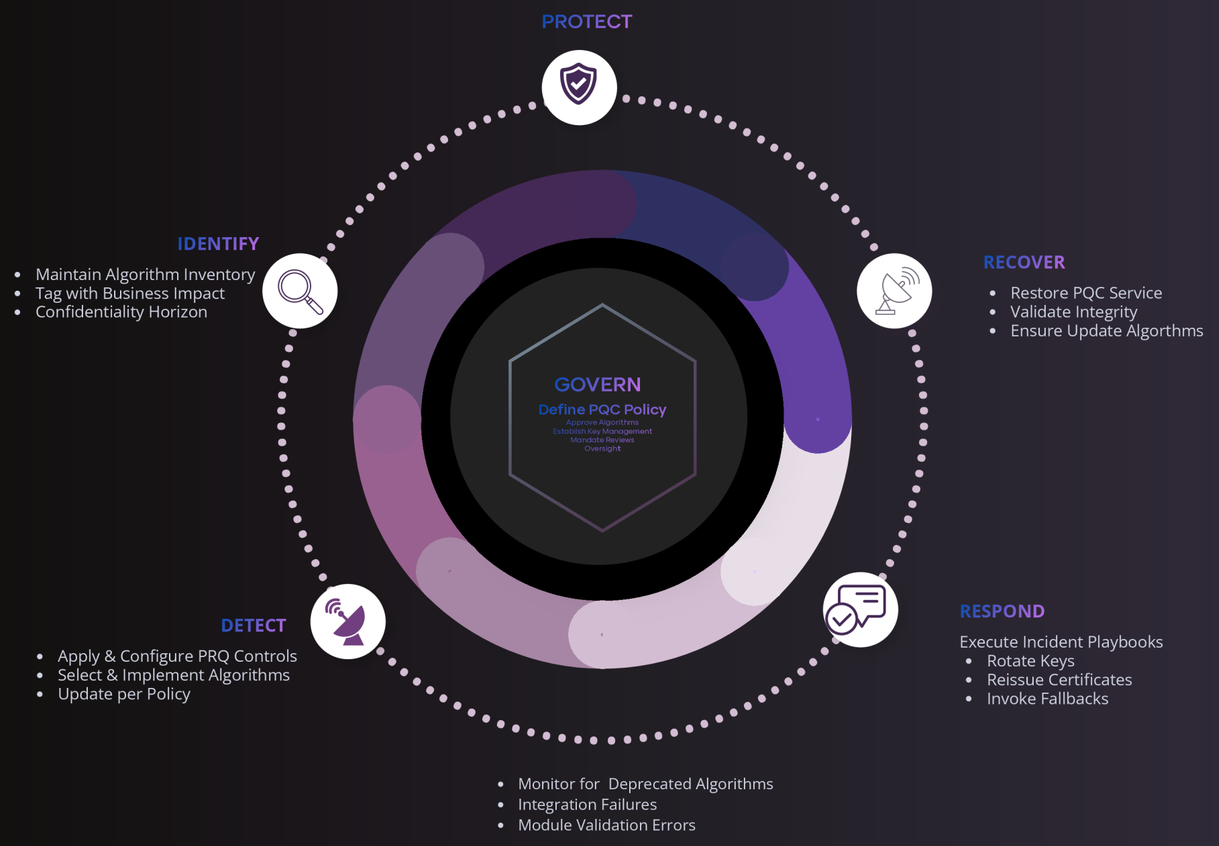
- **The NIST Cybersecurity Framework 2.0** (ฉบับร่าง มีนาคม 2024) ได้เพิ่มฟังก์ชันภาพรวมใหม่ชื่อว่า "Govern" เพื่อสะท้อนให้เห็นอย่างชัดเจนถึงความจำเป็นในการมีการกำกับดูแลขององค์กรและ การบริหารจัดการนโยบายของโครงการความปลอดภัยไซเบอร์ รวมถึงการ กำกับดูแลด้านการเข้ารหัสข้อมูล ภายใต้ Govern นี้ได้มีการกำหนดบทบาทและความรับผิดชอบสำหรับการอนุมัติการเลือกใช้อัลกอริทึม การกำหนดนโยบายการจัดการกุญแจ และการกำหนดให้มีการตรวจสอบเป็นระยะ จากนั้นฟังก์ชันทั้งห้าที่มีอยู่จะถูกนำไปประยุกต์ใช้กับการเข้ารหัสดังต่อไปนี้
    - **Identify (ระบุ)** รักษาบัญชีรายการอัลกอริทึมทั้งหมดให้ครบถ้วน พร้อมระบุผลกระทบทางธุรกิจ และขอบเขตการรักษาความลับ [3]
    - **Protect (ป้องกัน)** ใช้และกำหนดค่าตัวควบคุมการเข้ารหัส โดยเลือก ใช้งาน และอัปเดตอัลกอริทึมตามแต่ละนโยบาย
    - **Detect (ตรวจจับ)** ตรวจสอบการใช้อัลกอริทึมที่เลิกใช้หรืออ่อนแอลง ความล้มเหลวในการใช้งาน และข้อผิดพลาดในโมดูลตรวจสอบ
    - **Respond (ตอบสนอง)** ดำเนินการตามคู่มือรับมือเหตุการณ์ (incident playbook) ที่ได้รับการอนุมัติไว้ล่วงหน้า สำหรับการจัดการความล้มเหลวของระบบเข้ารหัส เช่น การเปลี่ยนกุญแจใหม่ การออกใบรับรองใหม่ และการเรียกใช้กลไกสำรอง
    - **Recover (กู้คืน)** กู้คืนบริการเข้ารหัส และตรวจสอบความสมบูรณ์ของระบบหลังเกิดเหตุ เพื่อให้มั่นใจว่าอัลกอริทึมที่อัปเดตแล้วถูกนำมาใช้

เมื่อรวมฟังก์ชัน Govern เข้ากับฟังก์ชันหลักทั้งห้า จะเกิดเป็น วงจรจัดการสินทรัพย์เข้ารหัสที่ต่อเนื่องและขับเคลื่อนด้วยตัวชี้วัด ครอบคลุมตั้งแต่การจัดทำรายการบัญชี การตรวจสอบความถูกต้อง การเลิกใช้งาน และการกำกับดูแล [10]

- ISO/IEC 27001:2013 ได้กำหนดระบบบริหารจัดการความปลอดภัยสารสนเทศ (Information Security Management System: ISMS) โดยในภาคผนวก Annex A.10 ระบุให้ต้องมีนโยบายด้านการเข้ารหัส ขั้นตอนการจัดการกุญแจ และการตรวจสอบกุญแจเป็นระยะ [11]
- ISO/IEC 27002:2013 เสนอแนวทางปฏิบัติ ที่ให้รายละเอียดมาตรการควบคุมต่าง ๆ เช่น Control 8.24 (การใช้การเข้ารหัส) ซึ่งกำหนดให้กลไกการเข้ารหัสต้องถูกออกแบบและใช้งานเพื่อปกป้องความลับ (confidentiality) ความสมบูรณ์ (integrity) และ ความถูกต้อง (authenticity) ของข้อมูล รวมถึงให้กระบวนการจัดการกุญแจรองรับวงจรการทำงานอย่างปลอดภัย [11]
- COBIT 2019 เป็นกรอบการกำกับดูแลที่เสนอวัตถุประสงค์ เช่น EDM05 (Ensure Risk Optimization) และ DSS05 (Manage Security Services) ซึ่งสามารถเชื่อมโยงเข้ากับกระบวนการกำกับดูแลด้านการเข้ารหัสและข้อกำหนดด้าน crypto-agility [12]

PQC Lifecycle

The NIST Cybersecurity Framework 2.0



ระบบนิเวศ (Ecosystem) และ Vendor Landscape

ระบบนิเวศของ PQC ประกอบด้วยผู้ให้บริการและการบริการหลายประเภท ซึ่งแต่ละส่วนมีบทบาทในการสร้างโครงสร้างพื้นฐานที่ปลอดภัยและมีคงทนสูง บทบาทสำคัญ กิจกรรมโดยทั่วไป และตัวอย่างต่าง ๆ ดังนี้

1.Crypto-Inventory Providers

- **บทบาท** ตรวจหาและจำแนกสินทรัพย์ทางการเข้ารหัสโดยอัตโนมัติ (เช่น อัลกอริทึม ความยาวกุญแจ บริบทของโปรโตคอล) ทั่วทั้งเครือข่าย แอปพลิเคชัน และอุปกรณ์ปลายทาง
- **กิจกรรม**
  - การสแกนเบื้องต้น โดยใส่คำอธิบายกำกับและ metadata เช่น ขอบเขตการรักษาความลับ ตาม NIST IR 8547
  - Continuous integration ด้วย configuration-management databases (CMDB) หรือแพลตฟอร์ม GRC (Governance, Risk, and Compliance)
- **ตัวอย่าง**
  - Venafi Crypto-Inventory Service
  - Thales CipherTrust Discovery

2. Threat-Register Services

- **บทบาท** ให้ข้อมูลข่าวกรองแบบเรียลไทม์เกี่ยวกับความก้าวหน้าใน cryptanalytic ช่องโหว่ใหม่ และการอัปเดตมาตรฐาน PQC
- **กิจกรรม**
  - เผยแพร่ข้อมูลแบบสมัครสมาชิก เช่น การโจมตีผ่านช่องทางแฝง การเลิกใช้อัลกอริทึม และการร่างมาตรฐานใหม่
  - เชื่อมโยงคำเตือนกับรายการสินทรัพย์ เพื่อระบุว่าสินทรัพย์ใดเสี่ยงและเรียกกระบวนการกำกับดูแล
- **ตัวอย่าง**
  - CISA Quantum-Readiness Alerts
  - Recorded Future PQC Intelligence

3. PQC Software Vendors

- **บทบาท** นำอัลกอริทึม PQC ที่ได้รับการอนุมัติจาก NIST ไปพัฒนาต่อ ทั้งในรูปของ reference code สำหรับ PoC และ SDKs สำหรับพัฒนาเชิงพาณิชย์
- **กิจกรรม**
  - ทดสอบความเข้ากันได้โดยใช้ไลบรารี เช่น liboqs (Open Quantum Safe)
  - ทดสอบประสิทธิภาพและผสานเข้ากับสภาพแวดล้อมนำร่อง
- **ตัวอย่าง**
  - PQShield SDK
  - ISARA Radiate
  - QuSecure Universe

4. Digital-Communication Hardware Vendors

- **บทบาท** รองรับ PQC ในอุปกรณ์ที่ใช้รักษาความปลอดภัยของข้อมูลขณะส่งผ่าน (data-in-transit) เช่น ไฟร์วอลล์ VPN เกตเวย์ หรือ HSMs (Hardware Security Modules)
- **กิจกรรม**
  - อัปเดตเฟิร์มแวร์เพื่อรองรับ hybrid key-exchange (เช่น X25519 + Kyber) ของ TLS หรือ IPsec
  - จัดเตรียมอินเทอร์เฟซสำหรับกำหนดค่าพารามิเตอร์ PQC และติดตาม handshake metrics
- **ตัวอย่าง**
  - ไฟร์วอลล์ และ VPN: Cisco Secure Appliance PQC Module, Palo Alto Networks TLS+Kyber Preview
  - HSMs: Thales nShield PQC Firmware, Utimaco CryptoServer PQC Edition

5. โอเพนซอร์ส vs. ระบบเชิงพาณิชย์

- **Open-Source Projects**
  - พัฒนาโดยชุมชน มีความโปร่งใสของซอร์สโค้ด (เช่น liboqs)
  - ใช้สัญญาอนุญาตแบบเปิด (permissive licenses)
  - ไม่มีการรับประกันบริการ (SLA) หรือการรับรองอย่างเป็นทางการ
- **ระบบเชิงพาณิชย์**
  - มี SLA
  - ให้บริการผสานระบบ
  - มีโมดูลที่ผ่านการรับรอง
  - มีเครื่องมือจัดการแบบกราฟิก
  - รับรอง policy engine
- **กิจกรรม** เริ่มจาก PoC ด้วยซอฟต์แวร์โอเพนซอร์ส แล้วจึงขยายสู่ระบบจริงบนระบบเชิงพาณิชย์
- **ตัวอย่าง** liboqs; Thales CipherTrust Manager with PQC plug-in; Venafi KeyProtect PQC.

6. ห้องปฏิบัติการรับรองและทดสอบความสอดคล้อง

- **บทบาท** ตรวจสอบและรับรองโมดูลการเข้ารหัสตามมาตรฐานด้านความปลอดภัยและการทำงานร่วมกัน
- **กิจกรรม**
  - การทดสอบตาม FIPS 140-3 ภายใต้ NIST CMVP เพื่อออกใบรับรองสำหรับการใช้งานสำหรับภาครัฐของสหรัฐฯ
  - การประเมินตาม Common Criteria (ISO/IEC 19790/24759) เพื่อกำหนด EALs (Evaluation Assurance Levels)
  - กิจกรรมทดสอบความเข้ากันได้ (interoperability events) เช่น ETSI Plugtests เพื่อยืนยันความสอดคล้องกับโปรไฟล์ PQC และสเปก hybrid-TLS
- **ตัวอย่าง**
  - NCC Group, TÜV Rheinland, A-LIGN (ห้องปฏิบัติการ CMVP)
  - BSI (เยอรมนี), ANSSI (ฝรั่งเศส) (หน่วยทดสอบ Common Criteria)

บทที่ 9

ตัวอย่างการใช้งาน และ Adoption Scenarios

Use Cases & Adoption Scenarios

บทนี้อธิบายถึงวิธีที่ PQC สามารถถูกประยุกต์ใช้ในสภาพแวดล้อมที่หลากหลาย เช่น ภาคการเงิน รัฐบาลและงานความมั่นคง Internet of Things (IoT) และ แพลตฟอร์มคลาวด์ เพื่อปกป้องแอปพลิเคชันสำคัญจากภัยคุกคามทางควอนตัมในอนาคต แต่ละส่วนจะอธิบายบริบทการดำเนินงาน ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีควอนตัม วิธีแก้ปัญหาด้วย PQC ในเชิงปฏิบัติ และตัวอย่างผลิตภัณฑ์หรือบริการในสถานการณ์จริง

ภาคการเงิน: การชำระเงินอย่างปลอดภัยและบล็อกเชน

สถาบันการเงินพึ่งพาการเข้ารหัสด้วยกุญแจสาธารณะอย่างมาก เช่น การใช้ TLS ในเครือข่ายการชำระเงิน, บัตรชิป EMV™, และ ลายเซ็นดิจิทัล ที่ใช้ในการทำธุรกรรมและ smart contracts คอมพิวเตอร์ควอนตัมที่สามารถรันอัลกอริทึมของ Shor ได้ จะสามารถแยกตัวประกอบของกุญแจ RSA หรือแก้ปัญหา elliptic-curve discrete logarithm ได้ ซึ่งจะทำให้ข้อมูลการชำระเงินและความถูกต้องของบล็อกเชนถูกถอดรหัสหรือปลอมแปลงได้ในอนาคต [4]

บริบทและความเสี่ยง

- การชำระเงินอย่างปลอดภัย (Secure Payments) Payment Card Industry (PCI) ใช้ RSA/ECDSA ในการตรวจสอบความถูกต้องของธุรกรรม ผู้โจมตีในแนวทาง HNDL สามารถบันทึกข้อมูลผู้ถือบัตรไว้ในปัจจุบัน และถอดรหัสเมื่อมีคอมพิวเตอร์ควอนตัมที่มีประสิทธิภาพเพียงพอในอนาคต [4]
- บล็อกเชน (Blockchain) สกุลเงินดิจิทัล เช่น Bitcoin และ Ethereum ใช้ ECDSA เพื่อควบคุมบัญชีผู้ใช้ หากมีคอมพิวเตอร์ควอนตัมขนาดใหญ่เพียงพอ ก็สามารถปลอมธุรกรรมและขโมยสินทรัพย์ดิจิทัลได้ [3]

แนวทางแก้ปัญหาด้วย PQC

- Hybrid TLS Deployment : การใช้งาน Hybrid TLS ที่รวมการแลกเปลี่ยนกุญแจแบบดั้งเดิม (เช่น X25519) เข้ากับ Key-Encapsulation Mechanism (KEM) เช่น CRYSTALS-Kyber จะช่วยรักษาความเข้ากันได้กับระบบเดิมในขณะที่เริ่มเปลี่ยนผ่านสู่ PQC [4]
- PQC-Enabled Payment SDKs : ชุดซอฟต์แวร์พัฒนา (SDK) สำหรับรองรับการชำระเงินด้วย PQC เปลี่ยนหรือเสริม authorization logic และการออกบัตร ด้วยลายเซ็น lattice-based เช่น Dilithium หรือ hash-based เช่น SPHINCS+

ตัวอย่าง

- FS-ISAC's "Future State" paper ได้กำหนดแผนงานระยะ 5–20 ปีเพื่อเตรียมความพร้อมสำหรับ PQC ในภาคการเงิน โดยแนะนำให้เริ่มโครงการนำร่องในระบบ card authorization และเกตเวย์การชำระเงินตั้งแต่เนิ่น ๆ [1]
- PCI DSS 4.0's requirement 12.3.3 กำหนดให้มี รายการสินทรัพย์ของชุดรหัสและโปรโตคอลการเข้ารหัสที่เป็นปัจจุบัน ซึ่งรวมถึงการวางแผนย้ายไปใช้ PQC ตาม best practice [2]
- The QRL Show panel เมื่อเดือนพฤศจิกายน 2023 ได้จัดเสวนาในหัวข้อ "Downtime Required for Bitcoin Quantum Safety" โดยเน้นถึงขั้นตอนเฉพาะในการปรับบล็อกเชนให้ปลอดภัยต่อควอนตัม เช่น กำหนดการหมุนเวียนกุญแจ (key rotation) และการอัปเกรดลายเซ็นดิจิทัล [3]
- PCI DSS 4.0's requirement 12.3.3 mandates an up-to-date "inventory of cryptographic cipher suites and protocols," which includes planning for PQC migration under best-practice guidance [2].
- The QRL Show's November 2023 panel detailed "Downtime Required for Bitcoin Quantum Safety," highlighting blockchain-specific migration steps such as key rotation schedules and signature-scheme upgrades [3].

รัฐบาล & งานความมั่นคง: การสื่อสารลับ & การเชื่อมต่อดาวเทียม

การสื่อสารที่เป็นความลับของรัฐบาลและงานความมั่นคงตั้งแต่ VPN ที่ปกป้องเครือข่ายลับไปจนถึงการเข้ารหัสการส่งข้อมูลทางดาวเทียม ขึ้นอยู่กับระบบกุญแจสาธารณะที่อาจถูกโจมตีโดยคอมพิวเตอร์ควอนตัม การรั่วไหลอาจทำให้ความลับระดับชาติถูกเปิดเผยหรือทำให้ช่องทางควบคุมและสั่งการสำคัญล้มเหลว [4][5]

บริบท และ ความเสี่ยง

- การสื่อสารลับ: IPsec VPN และช่องทาง TLS มักใช้ ECC-256 ซึ่งอัลกอริทึมของ Shor ที่ทำงานบนคอมพิวเตอร์ควอนตัมสามารถทำลายความลับของข้อมูลเหล่านี้ได้ทันที [4]
- การเชื่อมต่อดาวเทียม: การเข้ารหัสบนอวกาศ (Spaceborne encryption) (uplink commands, downlink telemetry) ใช้การเข้ารหัสแบบคลาสสิกที่ทำให้ปลอดภัยเพียงการห่อหุ้มกุญแจสาธารณะ ทำให้การดักฟังสัญญาณที่มีอายุยาวเหล่านี้มีความเสี่ยงสูงที่จะโดน HNDL [4][6]

แนวทางแก้ปัญหาด้วย PQC

- การตั้งค่า Hybrid IPsec ฝัง KEM ที่อิงกับ lattice (เช่น Kyber) ลงใน IKEv2 exchange เพื่อให้แม้ ECC ถูกทำลาย การสื่อสารก็ยังปลอดภัย
- ไลบรารี PQC สำหรับอวกาศ รองรับการห่อหุ้มกุญแจที่เข้ากันได้กับฮาร์ดแวร์ดาวเทียม ช่วยให้สามารถอัปเดต decryptor ของสถานีภาคพื้นดินหลังการปล่อยดาวเทียม

ตัวอย่าง

- **CISA's Post-Quantum Cryptography Initiative** ประสานงานหน่วยงานรัฐบาลกลางเพื่อจัดทำรายการสินทรัพย์ที่เปราะบาง และทดลองใช้ PQC ในเครือข่ายของรัฐบาล [5]
- **QuSecure ทดลองการเชื่อมต่อ PQC จากภาคพื้นสู่ดาวเทียม (Earth-to-satellite)** แบบสด โดยใช้ lattice-based KEM นับเป็นการส่งข้อมูลที่ทนต่อควอนตัมไปยังระบบหลายวงโคจรครั้งแรก [6]
- **U.S. General Services Administration (GSA)** เผยแพร่คู่มือสำหรับหน่วยงานรัฐบาลกลางในการนำการเข้ารหัสแบบไฮบริดไปใช้ในระบบสำคัญ รวมถึงการทดลองใช้ PQC ในเครือข่ายระดับชั้นความลับ [7]

IoT & ระบบฝังตัว (Embedded Systems)

อุปกรณ์ IoT เช่น เซนเซอร์ ตัวควบคุมในอุตสาหกรรม และมิเตอร์อัจฉริยะ (smart meters) มักถูกจำกัดด้วยพลังประมวลผล หน่วยความจำ และพลังงาน แต่หลายอุปกรณ์ก็ยังใช้ RSA หรือ ECC สำหรับอัปเดตเฟิร์มแวร์และการส่งข้อมูลที่ปลอดภัย ซึ่งเพิ่มช่องทางที่อาจถูกโจมตีจากคอมพิวเตอร์ควอนตัมอย่างมหาศาล [4]

บริบทและความเสี่ยง

- ข้อจำกัดของทรัพยากรทำให้ขนาดกุญแจ และความซับซ้อนของการคำนวณถูกจำกัด ทำให้การนำ PQC มาใช้แบบตรงไปตรงมาทำได้ยาก
- อายุการใช้งานของอุปกรณ์ที่ยาวนาน (5 – 10 ปี) หมายความว่า firmware-signed image ในปัจจุบัน อาจถูกโจมตีย้อนหลังผ่านการโจมตีแบบ HNDL [4]

แนวทางการแก้ปัญหา

- Lightweigth lattice schemes (เช่น NTRU, Saber) และโปรโตคอลแบบ code-based ที่ปรับให้เหมาะกับไมโครคอนโทรลเลอร์พลังงานต่ำ เพื่อให้สมดุลระหว่างความปลอดภัยและประสิทธิภาพ [8]
- Hybrid bootloaders ตรวจสอบลายเซ็นเฟิร์มแวร์โดยใช้ทั้ง ECDSA และ PQC signature (เช่น Dilithium) ทำให้การย้ายมาใช้ PQC เป็นไปอย่างราบรื่น

ตัวอย่าง

- Fernandez-Carames et al. สำรวจสถาปัตยกรรม IoT หลังควอนตัม และแนะนำให้ใช้ Saber และ NTRU-Prime ที่ปรับพารามิเตอร์แล้วสำหรับการใช้งานบนระบบฝังตัว [8]
- โมดูล Arm CryptoCell-P รองรับ dual-stack support ทำให้สามารถใช้ PQC สำหรับการแลกเปลี่ยนกุญแจควบคู่กับ ECC แบบดั้งเดิมบนอุปกรณ์ที่มีทรัพยากรจำกัดได้

บริการคลาวด์ & ข้อมูลที่เก็บอยู่ (Data at Rest)

แพลตฟอร์มคลาวด์เข้ารหัสข้อมูลที่เก็บอยู่โดย key-envelope: symmetric Data-Encryption Keys (DEKs) จะถูกห่อด้วย Key-Encryption Keys (KEKs) หากผู้โจมตีได้ DEKs ผ่าน KEK ที่ถูกโจมตีโดยคอมพิวเตอร์ควอนตัม ข้อมูลทั้งหมดที่เก็บไว้จะถูกเปิดเผยทันที [4]

บริบทและความเสี่ยง

- ความเสี่ยงของ Key-envelope: KEK แบบ RSA หรือ ECC ที่ใช้ใน Hardware Security Module (HSM) สำหรับการห่อหุ้ม DEK มีความเปราะบางทางควอนตัม ข้อมูลที่เก็บวันนี้อาจถูกโจมตีย้อนหลังได้ในอนาคตเมื่อมีคอมพิวเตอร์ควอนตัม [4]
- ความรับผิดชอบร่วมกัน: ลูกค้าคลาวด์ต้องมั่นใจว่ากุญแจที่ผู้ให้บริการจัดการ (provider-managed key) อยู่ถูกย้ายไปใช้ PQC ด้วย

แนวทางการแก้ปัญหา

- **PQC KEK integration** แทนที่ KEK แบบ RSA/ECC ใน HSM ด้วย lattice-based KEMs (เช่น Kyber) สำหรับห่อหุ้ม DEK โดยไม่ต้องเปลี่ยนการทำงานของ DEK ที่มีอยู่
- **การทดสอบความเข้ากันได้** NIST SP 1800-38C มีชุดทดสอบเทียบสำหรับ PQC ใน TLS, SSH และ HSM ช่วยให้ผู้ให้บริการคลาวด์ตรวจสอบการรองรับ PQC ได้ [9]

ตัวอย่าง

- ผู้ให้บริการคลาวด์หลายราย (AWS, Azure, Google Cloud) กำลังเปิดตัวฟีเจอร์เบื้องต้นสำหรับบริการ PQC key-envelope ทำให้ลูกค้าสามารถสร้าง และหมุนเวียน KEK ที่ห่อหุ้มด้วย Kyber ได้
- รายงาน Interoperability and Performance ของ NIST NCCoE มีคำแนะนำสำหรับการนำอัลกอริทึม PQC ไปใช้ใน virtualized HSM และ containerized TLS proxy [9]

บทที่ 10

ความท้าทายและคำถามปลายเปิด

ความท้าทายและคำถามปลายเปิด

เมื่อก้าวไปในการเปลี่ยนผ่านสู่ PQC องค์กรจะเผชิญกับความท้าทายด้านเทคนิค การปฏิบัติการ และการกำกับดูแลที่ยังไม่มีคำตอบชัดเจน คำถามปลายเปิดเหล่านี้ชี้ให้เห็นถึงประเด็นที่มาตรฐานยังอยู่ในช่วงกำลังพัฒนา โซลูชันที่กำลังถูกทดสอบ และคำตอบในระยะยาวที่ยังไม่ชัดเจน การรับมือกับประเด็นเหล่านี้จำเป็นต้องอาศัยความร่วมมืออย่างต่อเนื่องระหว่างภาคอุตสาหกรรม ภาควิชาการ และภาครัฐ

คอขวดด้านประสิทธิภาพในสภาพแวดล้อมที่มีข้อจำกัด

อัลกอริทึมเข้ารหัสยุคหลังควอนตัม (Post-Quantum Schemes) มักต้องใช้ขนาดกุญแจที่ใหญ่กว่า (ซึ่งเป็น mathematical "locks" ที่ใช้ในกระบวนการเข้ารหัส) และ การประมวลผลที่มากกว่า เมื่อเทียบกับอัลกอริทึมแบบดั้งเดิม ถึงแม้ฮาร์ดแวร์ระดับเซิร์ฟเวอร์จะสามารถรองรับภาระนี้ได้ แต่ อุปกรณ์ที่มีทรัพยากรจำกัด เช่น เซนเซอร์ IoT, embedded controllers และสมาร์ตมิเตอร์ อาจประสบปัญหาในการทำงาน

- **Latency and bandwidth**: Lattice-based KEMs (Key Encapsulation Mechanisms, โปรโตคอลที่สร้างกุญแจเข้ารหัสที่ใช้ร่วมกัน) อย่างเช่น Kyber สร้าง ciphertexts (ข้อความเข้ารหัส) ที่มีขนาดระดับ kilobyte ซึ่งอาจสร้างภาระให้กับการเชื่อมต่อแบบไร้สายหรือแอปพลิเคชันบนอุปกรณ์พกพา
- **การใช้พลังงาน** การคำนวณทางคณิตศาสตร์ที่เพิ่มขึ้นทำให้อายุการใช้งานแบตเตอรี่ของอุปกรณ์ปลายทาง (edge devices) ลดลง
- **Hardware acceleration** มีการพัฒนาแนวทางปรับปรุงประสิทธิภาพโดยใช้ชิปเฉพาะทาง เช่น GPU, FPGA หรือ ASICs แต่เทคโนโลยีเหล่านี้ยังไม่ได้ถูกใช้อย่างแพร่หลาย

คำถามปลายเปิด : PQC แบบที่เบาลง (เช่น Saber, NTRU-Prime) หรือ hybrid bootloader (เฟิร์มแวร์ที่รองรับทั้งลายเซ็นแบบคลาสสิก และ PQC) จะสามารถหาจุดสมดุลระหว่างความปลอดภัยและประสิทธิภาพได้หรือไม่ สำหรับการใช้งานในระบบ IoT ขนาดใหญ่?

Standard Maturity และ Algorithm Agility

แม้ว่า NIST จะประกาศชุดมาตรฐาน PQC ชุดแรกแล้ว แต่ cryptanalysis (การพยายามทำลาย ciphers) ยังคงดำเนินอยู่ อาจมีการค้นพบการโจมตีรูปแบบใหม่ที่เผยให้เห็นจุดอ่อน และในอนาคตอาจมีการออกอัลกอริทึมทดแทนเพิ่มเติม ดังนั้น องค์กรไม่ควรมองว่าการปรับใช้ PQC เป็น "ทำครั้งเดียวแล้วจบ"

- **Crypto-agility gaps** แอปพลิเคชันรุ่นเก่ามักฝัง "รหัสอ้างอิงอัลกอริทึมแบบตายตัว" (hard-code algorithm identifiers) เอาไว้ ทำให้ไม่สามารถเปลี่ยนหรืออัปเดตไปใช้อัลกอริทึมใหม่ได้อย่างราบรื่น
- **ความเข้ากันได้** ชุดพารามิเตอร์ที่แตกต่างกัน (ทางเลือกทางเทคนิคที่หลากหลายสำหรับอัลกอริทึมเดียวกัน) ระหว่างผู้ผลิตแต่ละราย ก่อให้เกิดการแยกย่อยของมาตรฐาน
- **แรงกดดันด้านกฎระเบียบ** หน่วยงานด้านข้อกำหนดและแบบปฏิบัติตาม (Compliance regimes) อาจกำหนดข้อบังคับตายตัวก่อนที่มาตรฐานจะพัฒนาเสร็จสมบูรณ์
- **คำถามปลายเปิด:** องค์กรจะออกแบบสถาปัตยกรรมอย่างไรให้ cryptographic primitives (องค์ประกอบพื้นฐานของการเข้ารหัส) เป็นโมดูลที่สามารถสลับเปลี่ยนได้ โดยไม่ต้องออกแบบระบบใหม่ทุกครั้ง?

คำถามปลายเปิด: PQC แบบที่เบาลง (เช่น Saber, NTRU-Prime) หรือ hybrid bootloader (เฟิร์มแวร์ที่รองรับทั้งลายเซ็นแบบคลาสสิก และ PQC) จะสามารถหาจุดสมดุลระหว่างความปลอดภัยและประสิทธิภาพได้หรือไม่ สำหรับการใช้งานในระบบ IoT ขนาดใหญ่?

กลยุทธ์การจัดการกุญแจในระยะยาว

การจัดการกุญแจ (วิธีที่องค์กรสร้าง แจกจ่าย และยกเลิกกุญแจเข้ารหัส) จะซับซ้อนขึ้นในยุค PQC ขนาดกุญแจที่ใหญ่ขึ้นทำให้โครงสร้างพื้นฐานของใบรับรอง (certificate infrastructures) ต้องรับภาระมากขึ้น และ stateful schemes (กุญแจต้องถูกติดตามอย่างระมัดระวังเพื่อป้องกันการใช้งานซ้ำ เช่น ลายเซ็นแบบ hash-based) จำเป็นต้องมีระเบียบปฏิบัติใหม่ในการดำเนินงาน

- **ระยะเวลาของใบรับรอง** : การหมุนเวียนกุญแจบ่อยขึ้นช่วยลดความเสี่ยงจากการโจมตีแบบ HNDL แต่ก็เพิ่มภาระงานด้านการบริหารจัดการมากขึ้น
- **Archival data :** ขอบเขตการรักษาความลับในระยะยาว (long-term confidentiality horizons) เช่น ข้อมูลทางการแพทย์หรือข้อมูลด้านการป้องกันประเทศที่ต้องปลอดภัยเป็นเวลาหลายทศวรรษ จำเป็นต้องมีกลยุทธ์ในการเข้ารหัสซ้ำ (re-encrypting) เมื่อมาตรฐานเข้ารหัสพัฒนาและเปลี่ยนแปลง
- **Integration with HSMs/KMS :** HSM (Hardware Security Modules) และ KMS (Key-Management Services) จำเป็นต้องมีการอัปเดตเฟิร์มแวร์และ API เพื่อรองรับ PQC โดยไม่กระทบต่อภาระงานหรือระบบเดิมที่มีอยู่

การรวมเข้ากับ Quantum Key Distribution (QKD)

QKD ใช้การแลกเปลี่ยนกุญแจที่อิงหลักฟิสิกส์ซึ่งสามารถนำไปเสริมกับ PQC ได้ แต่การรวมเข้ากับระบบที่มีอยู่ยังคงเป็นเรื่องท้าทาย เพื่อเป็นแนวทางในการตัดสินใจ องค์กรควรเข้าใจความแตกต่างพื้นฐานของแต่ละเทคโนโลยี องค์กรควรสร้างสมดุลในการนำ PQC และ QKD มาใช้งาน โดยอิงตามกรอบการป้องกันแบบหลายชั้น (layered defense) ที่ประเมินจากความเสี่ยง เช่น ใช้ PQC สำหรับความยืดหยุ่นและความสามารถในการขยายระบบ และเก็บ QKD ไว้สำหรับกรณีที่จำเป็นต้องมีการรับประกันความปลอดภัยตามหลักฟิสิกส์

PQC ควรเป็นเส้นทางการอัปเกรดหลัก สำหรับการต้านทานควอนตัมที่ครอบคลุมทั้งองค์กร

- **Software-Based Solution:** อัลกอริทึม PQC เป็นซอฟต์แวร์ และถูกออกแบบให้ รวมเข้ากับโปรโตคอลที่มีอยู่แล้วได้ง่าย เช่น TLS, IPsec และ SSH
- **Broad Coverage:** PQC เป็นวิธีที่คุ้มค่าและใช้งานได้จริง สำหรับระบบดิจิทัลแทบทุกประเภท รวมถึงเซิร์ฟเวอร์, สภาพแวดล้อมคลาวด์ และอุปกรณ์ IoT ที่นิยมในตลาด (mass-market IoT) ซึ่งมีข้อจำกัดด้านประสิทธิภาพและหน่วยความจำ
- **Mitigation of HNDL:** PQC เป็นสิ่งจำเป็น สำหรับการลดความเสี่ยงจาก การโจมตีแบบ Harvest-Now, Decrypt-Later (HNDL) ในข้อมูลที่ถูกเก็บระยะยาวทุกประเภท

QKD ควรถูกนำมาใช้ในข้อมูลที่มีมูลค่าสูงในสภาพแวดล้อมแบบ point-to-pointที่การแลกเปลี่ยนกุญแจจำเป็นต้องสามารถรับประกันโดยอาศัยหลักฟิสิกส์และ tamper-evident ตามความต้องการด้านความปลอดภัย

- **การเชื่อมต่อที่สำคัญ** รวมถึงการสื่อสารด้านการงานความมั่นคง, การสื่อสารลับของรัฐบาล, โครงสร้างพื้นฐานทางการเงินระหว่างธนาคาร, และการเชื่อมต่อข้ามพรมแดน
- **การลงทุนในโครงสร้างพื้นฐาน** QKD ต้องการการลงทุนสูง สำหรับช่องสื่อสารไฟเบอร์ออปติกเฉพาะทางหรือดาวเทียม ทำให้โดยทั่วไปไม่เหมาะสมและไม่คุ้มค่าสำหรับการใช้งานในองค์กรทั่วไป
- **Layered Resilience** การผสมผสาน PQC KEMs กับกุญแจที่ได้จาก QKD มอบความคงทนหลายชั้นและให้ความมั่นใจสูงสุดเท่าที่เป็นไปได้ แม้ว่าขณะนี้ โปรไฟล์มาตรฐานสำหรับ hybrid approach นี้ยังอยู่ในช่วงพัฒนา

กรอบงานใดที่จะช่วยรับประกันความต่อเนื่องของความน่าเชื่อถือ เมื่อมีการ re-signing archives หรือย้าย Root CA (Certificate Authorities) ไปใช้อัลกอริทึม PQC?

Decision-Making Framework

กรอบแนวคิดที่ใช้ในการกำหนดสมดุลที่เหมาะสมนี้ อิงตามการจำแนกข้อมูล และ ระดับความเสี่ยง โดยมี ขอบเขตของการรักษาความลับ เป็นตัวขับเคลื่อนหลัก

Factor	Guide for Decision-Making	Allocation
Data Sensitivity	How sensitive is the data? Does it have a long confidentiality horizon (decades)?	Higher sensitivity mandates PQC. Highest sensitivity (national security) may justify QKD for the link.
Risk Profile	Is the security requirement crypto-agility (PQC's strength) or physics-based assurance (QKD's strength)?	PQC for general agility; QKD for provable tamper-evidence.
Infrastructure	Is the environment constrained (IoT, mobile, cloud)? Can it support dedicated fiber?	PQC for constrained/cloud environments; QKD where dedicated trusted node infrastructure is feasible.

มีหลายแนวทางที่กำลังถูกศึกษาเพื่อ รับประกันความปลอดภัยทั้งในระยะสั้นและระยะยาว

1. **แนวทาง hybrid** การผสาน PQC KEMs เข้ากับกุญแจที่ได้จาก QKD อาจช่วยสร้าง ความคงทนแบบหลายชั้น (layered resilience) ได้ อย่างไรก็ตามโปรไฟล์มาตรฐาน (หรือกฎเกณฑ์กลางสำหรับการผสมผสานทั้งสองเทคโนโลยี) ยังอยู่ในช่วงเริ่มต้นของการพัฒนา
2. **ความพร้อมของโครงสร้างพื้นฐาน** QKD ต้องการช่องสัญญาณไฟเบอร์ออปติกเฉพาะ หรือระบบดาวเทียม ซึ่งเป็นการลงทุนที่สูงเกินงบประมาณขององค์กรส่วนใหญ่ในปัจจุบัน
3. **การกำกับดูแลและการรับรอง** กรอบการรับรองมาตรฐานสำหรับ QKD ยังอยู่ในระหว่างการพัฒนา ซึ่งทำให้เกิดข้อกังวลเกี่ยวกับความสามารถในการทำงานร่วมกัน และการตรวจสอบความถูกต้องอย่างอิสระ (auditability) ของระบบ

คำถามปลายเปิด

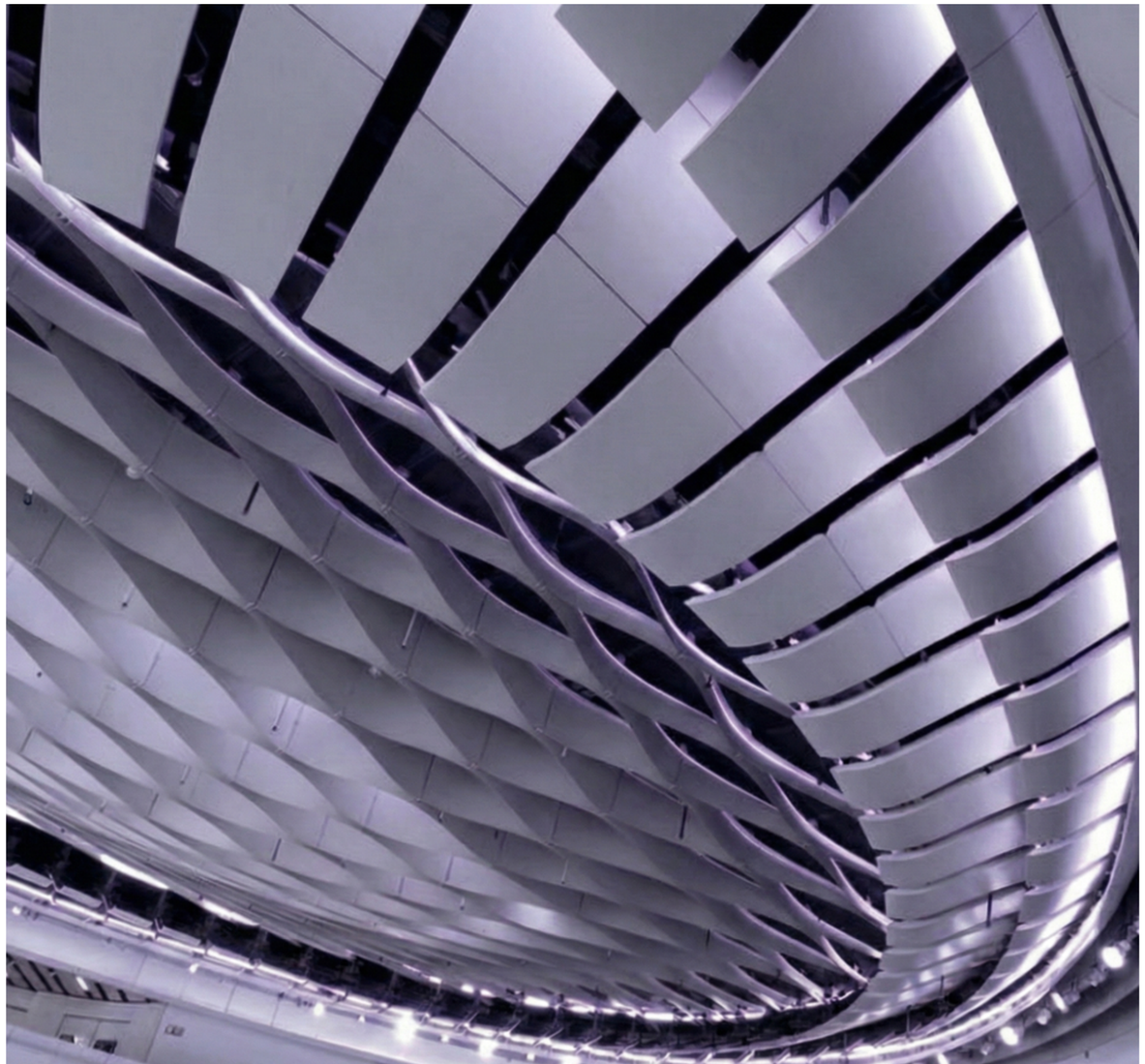
- องค์กรควรกำหนดสมดุลระหว่าง PQC และ QKD อย่างไร โดยใช้ PQC เป็นแนวทางอัปเกรดหลักสำหรับระบบดิจิทัลทั่วไป เพื่อให้ต้านทานควอนตัมได้ในวงกว้าง ในขณะที่สงวนการใช้ QKD ไว้สำหรับสภาพแวดล้อมที่ต้องการการรับประกันความปลอดภัยในระดับฟิสิกส์อย่างแท้จริง (เช่น ระบบป้องกันประเทศ เครือข่ายการเงินระหว่างธนาคาร หรือโครงข่ายสื่อสารข้ามพรมแดน)?
- กรอบแนวทางแบบใดที่สามารถช่วยให้องค์กรตัดสินใจได้อย่างเหมาะสมเพื่อให้แต่ละเทคโนโลยีถูกนำไปใช้ในบริบทที่สร้างคุณค่าได้สูงสุด?

บทที่ 11

ข้อเสนอแนะ และ Call to Action

ข้อเสนอแนะ และ Call to Action

ภัยคุกคามจากควอนตัมไม่ใช่เรื่องทางทฤษฎีอีกต่อไป ด้วยมาตรฐานในปัจจุบัน องค์กรต่าง ๆ จำเป็นต้องเริ่มดำเนินการเปลี่ยนผ่านตั้งแต่วันนี้ เพื่อปกป้องความปลอดภัยของข้อมูลในระยะยาว บทนี้นำเสนอแนวทางที่กระชับและสามารถปฏิบัติได้จริง สำหรับผู้บริหาร นักเทคโนโลยี และสมาคมอุตสาหกรรม



ข้อกำหนดในระดับผู้บริหาร

- **กำหนดนโยบายการกำกับดูแลการเข้ารหัส** จัดตั้งคณะกรรมการระดับบอร์ดที่รับผิดชอบด้านความเสี่ยงจากระบบเข้ารหัส และแต่งตั้งผู้บริหารที่มีความรับผิดชอบโดยตรง (เช่น "Chief Cryptography Officer" หรือผู้มีอำนาจเทียบเท่า)
- **ลงทุนในการตรวจสอบทรัพย์สินและโครงการนำร่อง** จัดสรรงบประมาณในการค้นหาทรัพย์สินดิจิทัลว่ามีการใช้ที่ไหนและอย่างไร รวมถึงสนับสนุนการใช้ hybrid deployments ที่รันระบบคลาสสิกและ PQC ควบคู่กัน พร้อมทั้งดำเนินการทดสอบความสอดคล้องตามมาตรฐาน
- **การรวมความเสี่ยงด้านควอนตัมเข้าสู่ความเสี่ยงขององค์กร:** มองการเปลี่ยนผ่านไปสู่ PQC เป็นส่วนหนึ่งของ operational resilience ไม่ใช่เพียงโครงการเสริมแยกต่างหาก
- **สร้างความร่วมมือกับหน่วยงานกำกับดูแลและพันธมิตร:** นำหน้าแบบปฏิบัติโดยยึดแนวทางจาก NIST IR 8547 (สหรัฐฯ), EU Quantum-Safe Roadmap, และข้อกำหนดเฉพาะในภาคการเงิน การแพทย์ และงานความมั่นคง

จุดตรวจสอบด้านเทคโนโลยีและกระบวนการ

- **การจัดทำบัญชีทรัพย์สินและการจำแนกประเภท** จัดทำบัญชีทรัพย์สินเข้ารหัส (cryptographic assets) ที่อัปเดตอยู่เสมอ พร้อมระบุ "ขอบเขตการรักษาความลับ" ของแต่ละชุดข้อมูล (กำหนดว่าข้อมูลใดต้องคงความปลอดภัยไว้นานเพียงใด)
- **การทดสอบนำร่องระบบแบบไฮบริด** เริ่มต้นจากการทดลองใช้ในโปรโตคอล TLS/IPsec (ซึ่งเป็นโปรโตคอลหลักของการเชื่อมต่ออินเทอร์เน็ตและ VPN อย่างปลอดภัย) โดยใช้ PQC KEMs ร่วมกับอัลกอริทึมแบบคลาสสิก
- **สถาปัตยกรรมที่รองรับ Crypto-Agility** ใช้ abstraction layers และ policy engines เพื่อแยกการทำงานของแอปพลิเคชันออกจากการเลือกใช้อัลกอริทึม
- **การตรวจสอบและการรับรองมาตรฐาน** ให้มั่นใจว่าโมดูลเข้ารหัสทั้งหมดผ่านการทดสอบ และรับรองตามมาตรฐาน FIPS 140-3 หรือ Common Criteria ซึ่งเป็นกรอบการประเมินอย่างเป็นทางการสำหรับผลิตภัณฑ์ทางการเข้ารหัส
- **การฝึกอบรมและความพร้อมของบุคลากร** จัดหลักสูตรเฉพาะตามบทบาท ระดับผู้บริหาร (สร้างความตระหนักเชิงกลยุทธ์), วิศวกร (เชิงเทคนิคและการพัฒนา), และผู้ปฏิบัติการ (การตอบสนองในงานประจำวัน)รวมถึงจัดการฝึกซ้อมตอบสนองเหตุการณ์ (incident response drills) สำหรับกรณีเกิดความล้มเหลวของระบบเข้ารหัส

การทำงานร่วมกันและการแบ่งปันภายในสมาคมอุตสาหกรรม

1. **กลุ่มทำงานตามภาคอุตสาหกรรม** เข้าร่วมสมาคมหรือกลุ่มทำงานภาคอุตสาหกรรม เพื่อแลกเปลี่ยนบทเรียนและประสบการณ์ที่ได้รับ
2. **การมีส่วนร่วมในโอเพนซอร์ส** สนับสนุนและมีส่วนร่วมในไลบรารี เช่น Open Quantum Safe Project เพื่อเร่งการพัฒนา เพิ่มความสมบูรณ์ของซอฟต์แวร์ และขยายขอบเขตการทดสอบ
3. **โครงการนำร่องข้ามพรมแดน** ร่วมมือในการทดลองใช้ PQC/QKD ระดับภูมิภาค เพื่อให้มั่นใจในความสามารถในการทำงานร่วมกัน และลดความแตกต่างระหว่างพรมแดน
4. **ระบบนิเวศการรับรอง** สนับสนุนการเติบโตของห้องปฏิบัติการทดสอบ และโปรแกรมการรับรองความสอดคล้อง เพื่อสร้างความเชื่อมั่นในการนำไปใช้งานจริง

Call to Action

เริ่มต้นการเปลี่ยนผ่านไปสู่ PQC ตั้งแต่วันนี้ เริ่มจากการจัดทำบัญชีทรัพย์สินเข้ารหัสและ hybrid pilot สร้างแนวปฏิบัติด้าน crypto-agility อย่างเป็นระบบ (ออกแบบระบบให้สามารถเปลี่ยนอัลกอริทึมเข้ารหัสได้อย่างรวดเร็ว) และสร้างความร่วมมือกับพันธมิตรในอุตสาหกรรมและหน่วยงานกำกับดูแล เพื่อกำหนดมาตรฐานที่สามารถทำงานร่วมกันได้ ผู้ที่เริ่มนำไปใช้อย่างรวดเร็วจะสามารถลดความเสี่ยงจาก การโจมตีแบบ HNDL และยังวางตำแหน่งตัวเองเป็นผู้นำในเศรษฐกิจควอนตัมที่กำลังเกิดขึ้น

แนวทางที่คงทนที่สุดคือ การป้องกันแบบหลายชั้น ด้วยการสร้างแนวปฏิบัติด้าน crypto-agility และดำเนินการทดลอง hybrid pilot ตั้งแต่ตอนนี้ องค์กรสามารถลดภัยคุกคามจาก HNDL ทันที และยังคงสอดคล้องกับมาตรฐานสากล

คำแปลศัพท์

คำศัพท์ (ภาษาอังกฤษ)	คำอธิบาย (สำหรับผู้อ่านทั่วไป)
Quantum Technology	เทคโนโลยีที่ใช้กฎของฟิสิกส์ควอนตัม (superposition, entanglement, interference) ในการสร้างรูปแบบใหม่ของการคำนวณ การสื่อสาร และการตรวจวัด
Quantum Computing	คอมพิวเตอร์ที่ใช้คิวบิต (qubits) แทนบิตแบบดั้งเดิม ทำให้สามารถแก้ปัญหาบางประเภทที่คอมพิวเตอร์ปกติไม่สามารถให้คำตอบได้ หรือใช้เวลานาน
Qubit	หน่วยของข้อมูลควอนตัมที่สามารถอยู่ในสถานะsuperposition ของ 0 และ 1
NISQ (Noisy Intermediate-Scale Quantum)	คอมพิวเตอร์ควอนตัมรุ่นปัจจุบัน (50–150 qubits) มีประสิทธิภาพสูง แต่มีแนวโน้มเกิดข้อผิดพลาดได้ง่าย
Post-Quantum Cryptography (PQC)	อัลกอริธึมการเข้ารหัสแบบใหม่ที่ออกแบบมาให้ทนต่อการโจมตีจากคอมพิวเตอร์ควอนตัม แต่ยังสามารถทำงานบนคอมพิวเตอร์แบบคลาสสิกได้
Harvest Now, Decrypt Later (HNDL)	วิธีการโจมตีโดยบันทึกข้อมูลที่ถูกเข้ารหัสไว้ในปัจจุบัน แล้วรอจนกว่าคอมพิวเตอร์ควอนตัมในอนาคตจะสามารถถอดรหัสได้
RSA / ECC	ระบบการเข้ารหัสแบบคลาสสิกที่ใช้อย่างแพร่หลาย ซึ่งมีความเปราะบางต่อการโจมตีจากคอมพิวเตอร์ควอนตัม
Lattice-based Cryptography	PQC ที่อิงกับปัญหาทางคณิตศาสตร์ที่ซับซ้อนใน lattices
Code-based Cryptography	PQC ที่อิงกับความยากของการถอดรหัสโค้ดแก้ข้อผิดพลาดแบบสุ่ม
Hash-based Cryptography	PQC ที่ใช้ hash ที่ปลอดภัยในการสร้างลายเซ็นดิจิทัล
Multivariate Cryptography	PQC ที่อิงกับการแก้สมการพหุนามหลายตัว
Supersingular Isogeny Cryptography	PQC ที่ใช้อิงกับปัญหาทางคณิตศาสตร์ที่ซับซ้อนบน elliptic curves.
KEM (Key Encapsulation Mechanism)	วิธีการแลกเปลี่ยนกุญแจเข้ารหัสอย่างปลอดภัย

คำศัพท์ (ภาษาอังกฤษ)	คำอธิบาย (สำหรับผู้อ่านทั่วไป)
Digital Signature	วิธีการเข้ารหัสที่ใช้พิสูจน์ความถูกต้องและความครบถ้วนของข้อความ
Crypto-Agility	ความสามารถของระบบในการเปลี่ยนอัลกอริธึมการเข้ารหัสได้อย่างรวดเร็วเมื่ออัลกอริธึมเดิมถูกเจาะหรือไม่ปลอดภัย
TLS / IPsec / SSH	โปรโตคอลความปลอดภัยหลักของอินเทอร์เน็ตที่จำเป็นต้องอัปเกรดเป็น PQC
HSM (Hardware Security Module)	อุปกรณ์ฮาร์ดแวร์ที่ปลอดภัยสำหรับเก็บและจัดการกุญแจเข้ารหัส
KMS (Key Management Service)	บริการที่จัดการ key lifecycle (การสร้าง การสับเปลี่ยน และการยกเลิก)
Certificate Authority (CA)	หน่วยงานที่เชื่อถือได้ซึ่งออกใบรับรองดิจิทัลเพื่อการสื่อสารที่ปลอดภัย
FIPS	มาตรฐานของสหรัฐฯ สำหรับข้อกำหนดด้านความปลอดภัยของโมดูลการเข้ารหัส
Common Criteria (CC)	มาตรฐานสากลสำหรับการประเมินความปลอดภัยของเทคโนโลยีสารสนเทศ
QKD (Quantum Key Distribution)	วิธีการแลกเปลี่ยนกุญแจอย่างปลอดภัยโดยใช้ฟิสิกส์ควอนตัม ซึ่งสามารถตรวจจับการดักฟังได้
Hybrid Cryptography	การใช้ทั้งอัลกอริธึมคลาสสิก (เช่น RSA, X25519) ควบคู่กับอัลกอริธึม PQC (เช่น Kyber) และระบบ QKD เพื่อให้การสื่อสารปลอดภัยทั้งจากภัยคุกคามคลาสสิกในปัจจุบันและภัยคุกคามควอนตัมในอนาคต
Confidentiality Horizon	ระยะเวลาที่ข้อมูลต้องคงความปลอดภัย
Governance	โครงสร้างการกำกับดูแลเพื่อให้มั่นใจว่าการเข้ารหัสถูกใช้อย่างปลอดภัยและได้รับการอัปเดตอย่างเหมาะสม

References

Chapter 4: Quantum Computing Threat Landscape
[1] Preskill, J. (2018). Quantum Computing in the NISQ Era and Beyond (arXiv:1801.00862).
[2] IBM Quantum Development & Innovation Roadmap. (2025). IBM.
[3] Mosca, M., & Piani, M. (2019). Quantum Threat Timeline. Global Risk Institute.
[4] National Institute of Standards and Technology. (2024, November). IR 8547: Transition to Post-Quantum Cryptography Standards (Initial Public Draft). NIST CSRC.
[5] U.S. Department of Energy. (2024, December). Quantum Information Science Applications Roadmap. U.S. DOE.
[6] Sectigo. (2025, May). Harvest Now, Decrypt Later Attacks & How They Relate to the Quantum Threat. Sectigo Resource Library.
[7] National Institute of Standards and Technology. (2025, March). The Road Ahead: Post-Quantum Cryptography Integration Guidance. NIST CSRC.
[8] National Institute of Standards and Technology. (2024, August). NIST Releases First Three Finalized Post-Quantum Encryption Standards (FIPS 203–205). NIST News.
[9] Cybersecurity and Infrastructure Security Agency. (2023). Quantum-Readiness: Migration to Post-Quantum Cryptography. CISA.
[10] National Institute of Information and Communications Technology. (2023). Q-ICT Roadmap: Quantum ICT for Future Networks. NICT.
[11] CEN-CENELEC. (2022). Standardization Roadmap on Quantum Technologies. CEN-CENELEC.

Chapter 5: Overview of Post-Quantum Cryptography (PQC)
[1] National Institute of Standards and Technology. Post-Quantum Cryptography. CSRC.
[2] National Institute of Standards and Technology. Report on Post-Quantum Cryptography (IR 8105). CSRC, 2016.
[3] National Institute of Standards and Technology. What Is Post-Quantum Cryptography? NIST, June 2023.
[4] National Institute of Standards and Technology. NIST Releases First Three Finalized Post-Quantum Encryption Standards (FIPS 203–205). NIST News, August 2024.
[5] Persichetti, E. Classic McEliece Update. NIST PQC Seminar #18, April 2024.
[6] Moody, D., & Robinson, A. Cryptographic Standards in a Post-Quantum Era. NIST, July 2022.
[7] National Institute of Standards and Technology. Recommendation for Stateful Hash-Based Signature Schemes (SP 800-208), October 2020.
[8] Seo, S., et al. "SIKE Round 2 Speed Record on Embedded Processors." NIST PQC Conference, 2018.

Chapter 6: Standards & Standardization Process
[1] NIST. (2020, July 22). PQC Third-Round Candidate Announcement. CSRC.
[2] NIST. (2019, Jan 31). IR 8240: Status Report on the First Round of the NIST PQC Standardization Process.
[3] NIST. (2020, Mar 9). IR 8309: Status Report on the Second Round of the NIST PQC Standardization Process.
[4] NIST. (2024, Aug). FIPS 203–205: First Three Finalized Post-Quantum Cryptography Standards. NIST News.
[5] NIST. (2022, July 5). Announcement of SPHINCS+ Addition; Removal of Protocols due to Cryptanalysis. CSRC.
[6] ETSI. (2025, Feb). TS 104 015 V1.1.1: Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies.
[7] ETSI. (2024, Oct). TR 103 966 V1.1.1: Deployment Considerations for Hybrid Schemes.
[8] ISO/IEC JTC 1/SC 27 WG 2. (2024). Proposed Updates to ISO/IEC 18033-3 and ISO/IEC 19790.
[9] ISO/IEC JTC 1/SC 27. (2024). Committee Document SD11: Structure, Members, and Work Programme.
[10] Korea Internet & Security Agency. (2023, Dec). Quantum-Resistant Cryptography National Contest (KpqC) Finalist Announcement.
[11] Korea Internet & Security Agency. (2023). Quantum-Safe Cryptography Standardization Roadmap.
[12] ASEAN Secretariat. (2022). ASEAN Cybersecurity Cooperation Strategy (2021–2025).
[13] SAC/TC 260. (2025, Jan 23). Notice on International Standard Proposals for Cybersecurity and PQC.
[14] National Institute of Information and Communications Technology (NICT). (2023). Q-ICT Roadmap.
[15] ISO/IEC JTC 1/SC 27. (2024). Membership and Contributions of the Russian Federation.
[16] NIST. (2016, Apr 28). IR 8105: Report on Post-Quantum Cryptography.
[17] Cyber Security Agency of Singapore. (2024). Quantum Security Guidelines.
[18] Monetary Authority of Singapore. (2023). Advisory on Post-Quantum Cryptography Adoption in Financial Institutions.
[19] Infocomm Media Development Authority. (2023, Jun 6). National Quantum-Safe Network Plus (NQSN+) Framework.

References

Chapter 7: Migration Roadmap & Best Practices

[1] National Institute of Standards and Technology. IR 8547: Transition to Post-Quantum Cryptography Standards (Initial Public Draft, Nov 2024). https://doi.org/10.6028/NIST.IR.8547.ipd

[2] Cybersecurity and Infrastructure Security Agency, National Security Agency, & National Institute of Standards and Technology. Quantum-Readiness: Migration to Post-Quantum Cryptography (Fact Sheet, Aug 21 2023). https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

[3] National Institute of Standards and Technology. SP 1800-38C: Migration to Post-Quantum Cryptography – Technology Interoperability and Performance Report (Preliminary Draft, Dec 2023). https://nccoe.nist.gov/projects/building-blocks/pqc-migration

[4] National Institute of Standards and Technology. FIPS 140-3: Security Requirements for Cryptographic Modules (Mar 22 2019). https://csrc.nist.gov/publications/detail/fips/140/3/final

[5] National Institute of Standards and Technology. SP 800-50: Building an Information Technology Security Awareness and Training Program (Aug 2003). https://doi.org/10.6028/NIST.SP.800-50

[6] National Institute of Standards and Technology. SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model (Feb 1998). https://doi.org/10.6028/NIST.SP.800-16

[7] National Institute of Standards and Technology. SP 800-57 Part 3: Transitioning Cryptographic Algorithms and Key Lengths (2019). https://doi.org/10.6028/NIST.SP.800-57pt3rev1

[8] National Institute of Standards and Technology. IR 8417: Report on Crypto-Agility (Nov 2023). https://doi.org/10.6028/NIST.IR.8417

[9] National Institute of Standards and Technology. Cybersecurity Framework 2.0 (Draft, Mar 2024). https://www.nist.gov/cyberframework

[10] International Organization for Standardization. ISO/IEC 27001: Information Security Management Systems – Requirements (2013).

[11] European Union Agency for Cybersecurity. Guidelines on Cryptographic Agility (ENISA, Aug 2022). https://www.enisa.europa.eu/publications/guidelines-on-cryptographic-agility

Chapter 8: Regulatory, Compliance & Governance

[1] European Commission. (2024). Commission Recommendation on Post-Quantum Cryptography. Official Journal of the European Union.

[2] Cybersecurity and Infrastructure Security Agency. (2024). NSTAC Study on National Preparedness for Post-Quantum Cryptography. U.S. Department of Homeland Security.

[3] National Institute of Standards and Technology. (2024). IR 8547: Transition to Post-Quantum Cryptography Standards (Initial Public Draft). NIST Computer Security Resource Center. https://doi.org/10.6028/NIST.IR.8547.ipd

[4] ETSI. (2025). TS 104 015 V1.1.1: Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies. European Telecommunications Standards Institute.

[5] ITU-T Study Group 13. (2019). Recommendation Y.3800: Overview on Networks Supporting Quantum Key Distribution. International Telecommunication Union.

[6] European Banking Authority. (2025). Guidelines on ICT and Security Risk Management (EBA/GL/2019/04). EBA.

[7] European Parliament & Council. (2025). Regulation (EU) 2024/xxxx: Digital Operational Resilience Act (DORA). Official Journal of the European Union.

[8] U.S. Food and Drug Administration. (2025). Cybersecurity in Medical Devices: Quality System Considerations and Premarket Submissions. FDA.

[9] RAND Corporation. (2022). Assessments of Quantum Computing Vulnerabilities of National Critical Functions. RAND.

[10] National Institute of Standards and Technology. (2024). Draft Cybersecurity Framework 2.0. NIST.

[11] International Organization for Standardization. (2022). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements. ISO.

[12] ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. ISACA.

[13] Bank for International Settlements. (2025). Quantum-Readiness for the Financial System: A Roadmap (BIS Paper No. 158). BIS.

[14] Monetary Authority of Singapore. (2022). Advisory on Addressing the Cybersecurity Risks Associated with Quantum Computing (MAS/TCRS/2024/01). MAS.

Chapter 9: Use Cases & Adoption Scenarios

[1] FS-ISAC. (2023). "Future State – Post-Quantum Cryptography (PQC) Working Group." FS-ISAC.

[2] Encryption Consulting. (2023). "PCI DSS 4.0's Role in Quantum-Safe Cryptography Transition.

[3] The QRL Foundation. (2023, November). The QRL show: Downtime required for Bitcoin quantum-safety https://www.theqrl.org/

[4] National Institute of Standards and Technology. (2024). "IR 8547: Transition to Post-Quantum Cryptography Standards" (Initial Public Draft). NIST CSRC.

[5] Cybersecurity and Infrastructure Security Agency. (2024). "Post-Quantum Cryptography Initiative." CISA.

[6] QuSecure. (2022). "Post-Quantum Satellite Protection Rockets Towards Reality."

[7] General Services Administration. (2025). "GSA and Post-Quantum Cryptography: Enabling a Secure Federal Future."

[8] Fernández-Cárames, T. M., et al. (2024). "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things." arXiv.

[9] National Cybersecurity Center of Excellence, NIST. (2023). "Interoperability and Performance of Post-Quantum Cryptographic Algorithms" (SP 1800-38C Preliminary Draft).

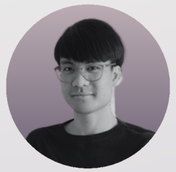
เกี่ยวกับ SCBX

SCBX เป็นบริษัทแม่ของกลุ่มธุรกิจเทคโนโลยีทางการเงิน โดยดำเนินงานครอบคลุมเสาหลักทางธุรกิจที่สำคัญ 3 ด้าน ได้แก่ ธุรกิจธนาคาร , ธุรกิจการเงินเพื่อผู้บริโภคและดิจิทัล , และธุรกิจแพลตฟอร์มและเทคโนโลยีนอกจากนี้ SCBX ยังมุ่งเน้นไปที่เทคโนโลยีด้านสภาพภูมิอากาศ โดยมีแรงบันดาลใจที่จะก้าวขึ้นเป็นกลุ่มบริษัทเทคโนโลยีทางการเงินระดับภูมิภาคที่น่าชื่นชมที่สุด' บริษัทดำเนินธุรกิจด้วยความยืดหยุ่นและรอบคอบในการกำกับดูแลกิจการและการบริหารความเสี่ยงและมีศักยภาพที่จะแข่งขันได้อย่างทัดเทียมในการแข่งขันระดับโลก

Authors

ดร.ทุตานนท์ สินธุประสิทธิ์
Head of R&D, SCBX

ดร.ภูมิพงศ์ ไชยวงศ์คต
Senior Research Fellow and Co-founder, QTFT



ณัฎฐ์ ชูกำแพง
Senior Research Scientist, SCBX

กรวิชญ์ สังข์แก้ว
AI Engineer, SCBX

อาทิตย์ ไทรงาม
Cloud and AI Technology Risk Specialist, SCBX

กวีวุฒิ เต็มภูวภัทร
Cheif Innovation Officer, SCBX
Cheif Executive Officer, SCB10X

ปริญญา จูตะเสน
Technology Risk Manager, SCB

นพปฎล สรงสระแก้ว
Head of Security Advisory, SCB

ขนิษฐา ศิวะโกเศศ
Head of Encryption Key Management & Application Deployment, SCB

Book Designer
ธัญกมล พยัคฆชนม์
Project Coordinator, SCBX

แปลโดย
ปารเมศ เอี่ยมทรงศักดิ์
ปัญญาทิพย์ ยี่เข่ง
ภูมิรัตน์ นวรัตน์
ณัฐธิดา แก้วอาจ
ณัฎฐ์ เหลืองสิรพรชัย

รายงานนี้เป็นความร่วมมือกันระหว่าง

SCBX

SCB QTFT

SCBX

www.scbx.com