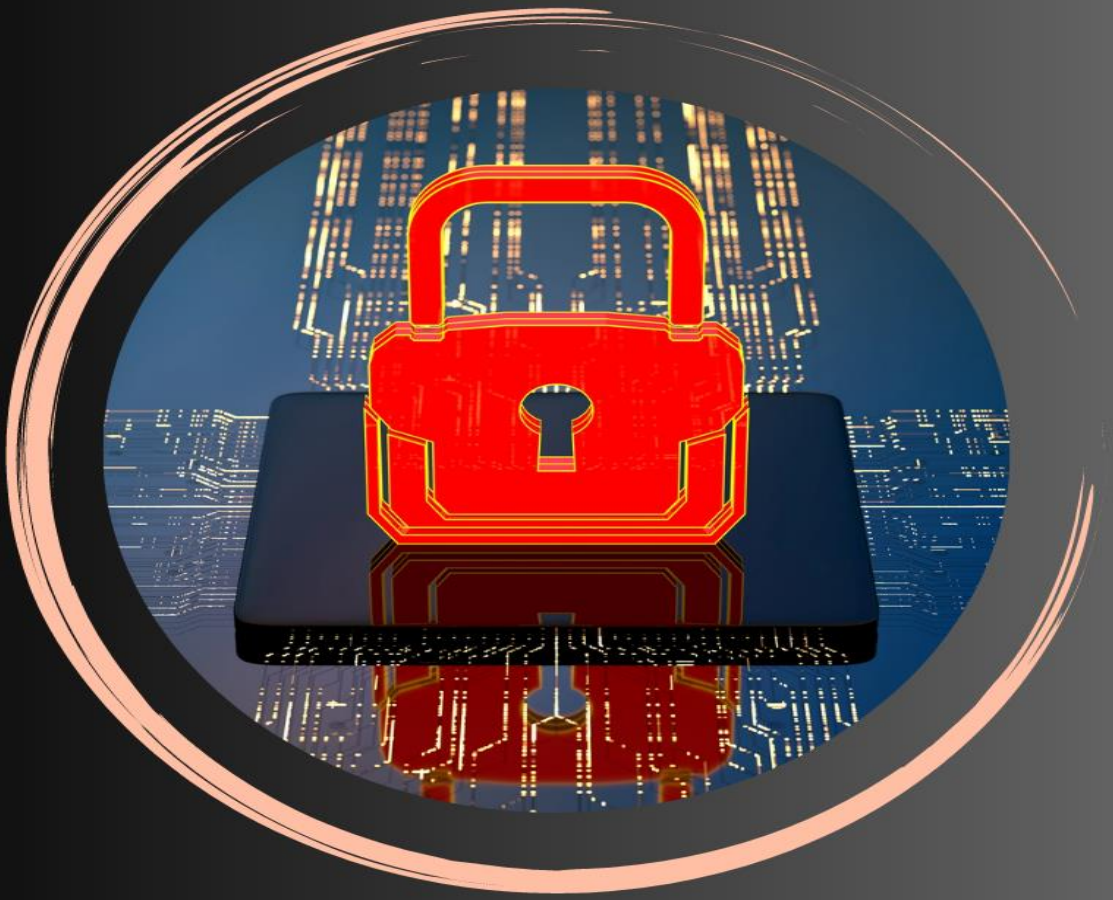
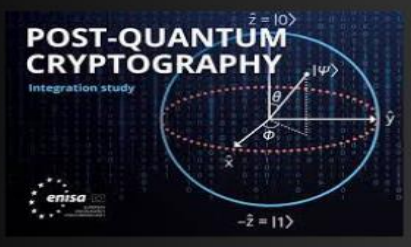
Post Quantum Cryptography





Cybersecurity Research Center
National Cyber Security Agency
NCSA

Post Quantum Cryptography

การเข้ารหัสยุคหลังควอนตัม (Post-Quantum Cryptography: PQC) คือ กระบวนการเข้ารหัสข้อมูลที่เกิดขึ้นมาเพื่อปกป้องข้อมูลจากการมาถึงของคอมพิวเตอร์ควอนตัม ซึ่งผู้เชี่ยวชาญและทำงานเกี่ยวข้องกับความปลอดภัยและการรักษาความลับข้อมูลต่างมีความกังวลว่าจะมีความสามารถเจาะผ่านเทคโนโลยีการเข้ารหัสแบบเดิมที่ใช้อยู่ได้อย่างง่ายดาย จึงแบ่งได้ออกเป็น 2 ส่วน คือ เทคโนโลยีการเข้ารหัส และการพัฒนาคอมพิวเตอร์ควอนตัม

เทคโนโลยีการเข้ารหัส (Cryptography)

เทคโนโลยีการเข้ารหัส เป็นแนวทางปฏิบัติในการปกป้องข้อมูลโดยใช้อัลกอริทึม แฮช และลายเซ็นเข้ารหัส ซึ่งข้อมูลนั้นอาจถูกพักเอาไว้ (เป็นไฟล์ในฮาร์ดดิสก์) อยู่ในระหว่างการส่งต่อ (ในเครือข่ายอิเล็กทรอนิกส์ที่มีการสื่อสารสองฝ่ายขึ้นไป) หรือใช้งานอยู่ (ระหว่างการประมวลผล) การเข้ารหัสมีเป้าหมายสำคัญอยู่ 4 ข้อ คือ

- การรักษาความลับ – ข้อมูลจะต้องใช้งานได้เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น
- การรักษาความถูกต้อง – ตรวจสอบได้แน่นอนว่าข้อมูลไม่ได้ถูกเปลี่ยนแปลง
- การยืนยันตัวตน – ยืนยันความถูกต้องของข้อมูลหรือระบุตัวตนผู้ใช้ได้
- การปฏิเสธความรับผิดชอบ – ป้องกันผู้ใช้ปฏิเสธความรับผิดชอบข้อมูลที่ส่งออกไป

ซึ่งส่วนประกอบหลักของเทคโนโลยีการเข้ารหัสก็คือ “การเข้ารหัสลับ(encryption)” และ “การถอดรหัสลับ (decryption)” โดยการเข้ารหัสลับคือการทำให้ข้อมูลที่อ่านได้ (plaintext) ไปทำการแปลงข้อมูล แปลงสภาพให้กลายเป็นข้อมูลที่อ่านไม่ได้ (ciphertext) ก่อนส่งต่อข้อมูลไปยังผู้รับปลายทางที่มีชุดเข้ารหัสที่ตรงกันทำการถอดรหัสลับ (decryption) ที่ครอบไว้ออกด้วยการถอดข้อมูล ให้ข้อมูลที่อ่านไม่ได้กลับมาเป็นข้อมูลที่อ่านได้เหมือนเดิม ซึ่งเทคโนโลยีการเข้ารหัสลับที่ใช้เป็นมาตรฐานและได้รับความนิยมมีด้วยกัน 2 แบบ คือ การเข้ารหัสลับแบบกุญแจสมมาตร (Symmetric Key Encryption) และการเข้ารหัสลับแบบกุญแจอสมมาตร (Asymmetric Key Encryption) ซึ่งความต่างของการเข้ารหัสสองแบบคือ แบบสมมาตรทั้งผู้ส่งและผู้รับจะมี

กุญแจรหัสเหมือนกัน ส่วนแบบอสมมาตรนั้น กุญแจจะแบ่งออกเป็นสองชุด คือ กุญแจส่วนตัว (Private Key) กับกุญแจสาธารณะ (Public Key) ซึ่งผู้ส่งกับผู้รับข้อมูลจะใช้คนละชุดเพื่อเข้ารหัสและถอดรหัส

เมื่อว่ากันด้วยเรื่องการเข้ารหัส สิ่งที่สำคัญก็คือรหัสที่ใช้มีความปลอดภัยแค่ไหน เราพิจารณาจากตัวแปรสองเรื่องคือ

- อัลกอริทึมที่ใช้เข้ารหัสมีความซับซ้อนแค่ไหน
- ความยาวของกุญแจรหัสมีขนาดเท่าไหร่

การเข้ารหัสจะมีหน่วยวัดจำนวนรหัสที่ใช้งานเรียกว่า “บิท (bit)” ยิ่งจำนวนบิทมากเท่าไหร่การเข้ารหัสก็ยิ่งมีความซับซ้อนและใช้เวลาทั้งการเข้ารหัสและถอดรหัสมากขึ้นตามไปด้วย ในตอนนี้ผู้เชี่ยวชาญด้านมาตรฐานความปลอดภัยในการเข้ารหัสแนะนำให้ใช้คือ 256 บิท

คอมพิวเตอร์ควอนตัม (Quantum Computer)

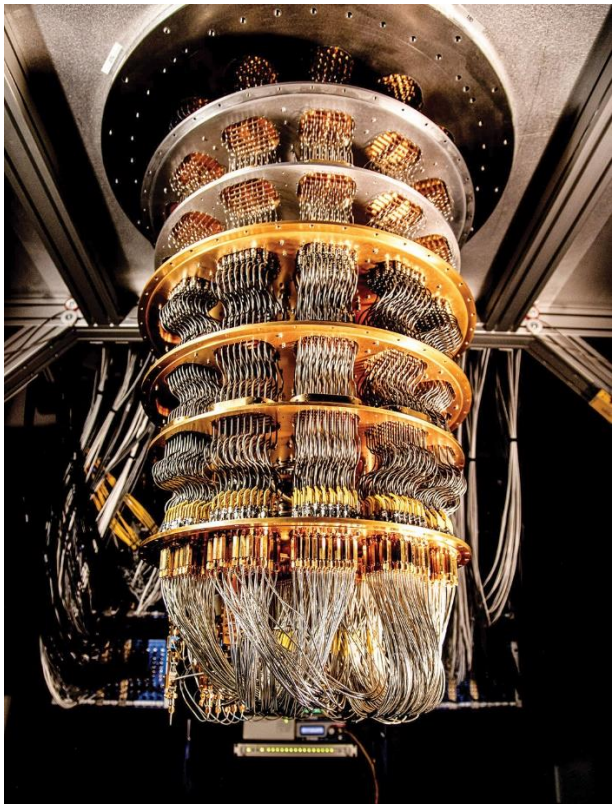
คอมพิวเตอร์ควอนตัม คือคอมพิวเตอร์ที่พัฒนาจากเทคโนโลยีการคำนวณแบบควอนตัม (Quantum Computing) ที่อาศัยคุณสมบัติเชิงควอนตัมของอนุภาคในระดับอะตอมมาเป็นต้นแบบในการพัฒนาเทคโนโลยีด้านนี้ขึ้น

ควอนตัมเป็นการศึกษากลไกของอนุภาคต่าง ๆ ภายในโครงสร้างอะตอมที่นักวิทยาศาสตร์เริ่มสนใจศึกษามาตั้งแต่ปลายศตวรรษที่ 19 จนเข้าสู่ศตวรรษที่ 20 ได้เริ่มมีแนวคิดทฤษฎีเกี่ยวกับควอนตัมออกมาอย่างต่อเนื่อง นักวิทยาศาสตร์ที่จุดประกายการศึกษาเกี่ยวกับควอนตัมที่สำคัญสองคนหลักก็คือ แวเนอร์ ไฮเซินแบร์ก (Werner Hisenberg) กับ แอร์วิน ชเรอดิงเงอร์ (Erwin Schrodinger) ได้พยายามอธิบายปรากฏการณ์ทางควอนตัมที่ไม่สามารถใช้ทฤษฎีหลักการเชิงกลศาสตร์แบบเดิมอธิบายได้อีกต่อไป คุณลักษณะที่เป็นเอกลักษณ์ของควอนตัมมีดังนี้

- เมื่อเราแยกอนุภาคของแสงออกจากกันและวัดค่าอนุภาคหนึ่ง อนุภาคที่แยกออกอีกตัวจะเปลี่ยนเป็นอีกค่าทันที ไม่ว่าอยู่ห่างกันแค่ไหนก็ตาม ปรากฏการณ์นี้เรียกว่า **การพัวพันเชิงควอนตัม** (Quantum Entanglement) เป็นต้นทางให้เกิดการพัฒนาเทคโนโลยีการสื่อสารควอนตัม (Quantum Communication) ขึ้น
- ทฤษฎีความไม่แน่นอนเชิงควอนตัม (Uncertainty Principle) หลักการข้อนี้มาจากข้อเสนอของ ไฮเซินแบร์ก ว่า เราไม่สามารถทราบตำแหน่งและวัดค่าโมเมนตัมของอนุภาคในเวลาเดียวกันได้อย่างแม่นยำ

- อนุภาคสามารถมีสถานะ “มากกว่าหนึ่ง” ได้ในเวลาเดียวกัน การทับซ้อนของสถานะของอนุภาคเรียกว่า “ซูเปอร์โพสิชัน (Superposition)”

ด้วยคุณสมบัติ “ซูเปอร์โพสิชัน” นี่เอง จึงมีการนำความรู้เกี่ยวกับควอนตัมมาใช้ในการพัฒนากระบวนการคำนวณควอนตัม จนเป็นที่มาของคอมพิวเตอร์ควอนตัมในปัจจุบัน (ภาพที่ 1)



ภาพที่ 1 ตัวอย่างคอมพิวเตอร์ควอนตัมที่อยู่ในการพัฒนาปัจจุบัน (ที่มา: science.org)

ความแตกต่างระหว่างคอมพิวเตอร์แบบเดิมที่ใช้กันทั่วไป กับคอมพิวเตอร์ควอนตัมที่ทั่วโลกกำลังพัฒนาขึ้น แตกต่างตั้งแต่พื้นฐานการประมวลผล ในคอมพิวเตอร์แบบเดิมนั้น เรียกหน่วยการประมวลผลว่า “บิท (bit)” ซึ่งอาศัยกระบวนการทางอิเล็กทรอนิกส์แสดงการประมวลผลออกมาเป็น 0 กับ 1 ค่าใดค่าหนึ่งเท่านั้น ในขณะที่คอมพิวเตอร์ควอนตัมเรียกหน่วยการประมวลผลว่า “คิวบิต (qubit)”อาศัยหลักการพัวพันทางควอนตัม และซูเปอร์โพสิชันของการหมุนอิเล็กตรอนหรือการเลี้ยวเบนของโฟตอน ซึ่งการแสดงผลในแบบควอนตัมสามารถแสดงออกมาเป็นทั้ง 0 1 หรือทั้งสองค่าเลยก็ได้ นอกจากนี้ความสามารถในการประมวลผลของคอมพิวเตอร์แบบเดิมจะเป็นสมการเชิงเส้น (linear) โดยประมวลผลตามลำดับ ต่างจากคอมพิวเตอร์ควอนตัมจะเป็นสมการเชิงพหุนาม (exponential) ทำให้ความเร็วและความสามารถในการประมวลผลข้อมูลแตกต่างกันมหาศาล

แม้ปัจจุบันจะยังเป็นช่วงเริ่มต้นของการพัฒนาคอมพิวเตอร์ควอนตัม ศักยภาพของเครื่องต้นแบบที่ออกมาก็สามารถเร่งการพัฒนาองค์ความรู้และเทคโนโลยีอุตสาหกรรมหลายด้านในระดับปฏิวัติองค์ความรู้ ไม่ว่าจะเป็นด้านการแพทย์ วัสดุศาสตร์ และการเงิน แน่นอนว่าผลกระทบด้านความปลอดภัยก็เริ่มส่งผลแล้วเช่นกัน

ทีมวิจัยของจีนได้รายงานการแยกตัวประกอบเลขด้วยคอมพิวเตอร์ควอนตัมแกะรหัส RSA ระดับ 48 บิท ด้วยคอมพิวเตอร์ควอนตัมขนาดเพียง 10 คิวบิท เท่านั้น และคาดว่าจะสามารถเจาะรหัส RSA-2048 ที่มีระดับความปลอดภัย 2048 บิท ได้ด้วยคอมพิวเตอร์ควอนตัมขนาด 372 คิวบิท แม้จะมีข้อโต้แย้งจาก สก็อต แอรอนสัน (Scott Aaronsion) นักวิจัยคอมพิวเตอร์ควอนตัม และผู้อำนวยการ Quantum Information Center ของมหาวิทยาลัยเท็กซัส ออกมาให้ความเห็นว่ารายงานของจีนฉบับนี้มีช่องโหว่ในการตั้งสมมุติฐานและยังไม่สามารถสรุปผลออกมาตามที่รายงานได้ แต่เป็นที่แน่ชัดแล้วว่า ระบบความปลอดภัยทางข้อมูลในปัจจุบันจะพบปัญหาแน่นอนเมื่อคอมพิวเตอร์ควอนตัมพร้อมใช้งานเชิงธุรกิจ จึงถือเป็นเรื่องเร่งด่วนที่ภาครัฐและเอกชนต่างพยายามพัฒนาระดับความปลอดภัยการเข้ารหัสข้อมูลให้สูงขึ้น

จุดเริ่มต้นของ Post-Quantum Cryptography

โจ ไบเดน (Joe Biden) ประธานาธิบดีสหรัฐอเมริกาออกคำสั่งแต่งตั้งคณะกรรมการที่ปรึกษาความคิดริเริ่มทางควอนตัมแห่งชาติ (National Quantum Initiative Advisory Committee – NQIAC) วัตถุประสงค์เพื่อกำหนดนโยบายด้านคอมพิวเตอร์ควอนตัมของสหรัฐอเมริกา โดยมีตัวแทนจากหน่วยงานวิจัยภาครัฐ สถาบันวิชาการ และภาคเอกชน เข้าร่วม

ในถ้อยแถลงการณ์แต่งตั้งคณะกรรมการ ดูเหมือนว่ารัฐบาลสหรัฐอเมริกา มีความกังวลถึงเรื่องความปลอดภัยของข้อมูลเมื่อเทคโนโลยีคอมพิวเตอร์ควอนตัมพัฒนาจนมีความเป็นไปได้ที่รหัสความปลอดภัยที่มีในปัจจุบันจะถูกเจาะได้ในที่สุด ภารกิจของคณะกรรมการชุดนี้จึงมีหน้าที่กำหนดนโยบายและแผนระยะยาวด้านโครงสร้างพื้นฐานไอทีของสหรัฐฯ ให้มีความแข็งแกร่งเพียงพอให้อนาคตรวมถึงการพัฒนาเทคโนโลยีการเข้ารหัสที่แข็งแกร่งเพียงพอจะรับมือควอนตัมคอมพิวเตอร์ได้ ด้านหน่วยงานวิจัยระดับชาติอย่าง สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standard and Technology: NIST) ได้เริ่มกำหนดมาตรฐานเทคโนโลยีการเข้ารหัสยุคหลังควอนตัมขึ้นมาระยะหนึ่งแล้ว

แนวคิดริเริ่มเกี่ยวกับการเข้ารหัสยุคหลังควอนตัม (PQC Initiative)

สำนักงานความมั่นคงปลอดภัยโครงสร้างพื้นฐานและไซเบอร์ (Cyber Security and Infrastructure Security Agency: CISA) แห่งประเทศสหรัฐอเมริกา ได้เสนอแนวคิดริเริ่มในการพัฒนาเทคโนโลยีการเข้ารหัสหลังยุคควอนตัม มีหลักการที่เป็นแนวทางให้การนำเทคโนโลยีมาใช้งานไว้ 4 ข้อคือ

- **การประเมินความเสี่ยง** ประเมินช่องโหว่ของระบบโครงสร้างพื้นฐานที่สำคัญของสหรัฐอเมริกา โดยประเมินความเสี่ยงใน 55 ฟังก์ชันสำคัญระดับชาติ (National Critical Functions: NCFs) การพิจารณาความสำคัญในระดับมหภาคของแต่ละฟังก์ชันของ NCF นั้น CISA จะประเมินจากความสำคัญของการข้อมูลที่ต้องได้รับการปกป้อง จุดที่มีความเสี่ยงสูง การเปลี่ยนแปลงระดับการเข้ารหัสหลังยุคควอนตัมว่าดำเนินการถึงจุดไหนแล้ว และสิ่งที่ต้องการการสนับสนุนจากรัฐบาลกลาง
- **การวางแผน** แผนที่ CISA ทำงานร่วมกับพันธมิตรควรมุ่งเน้นด้านทรัพยากรและการมีส่วนร่วมของผู้ประกอบการและผู้ปฏิบัติงาน ทั้งในภาครัฐและเอกชน
- **นโยบายและมาตรฐาน** ทำงานกับพันธมิตรเพื่อส่งเสริมการนำนโยบายด้านมาตรฐาน และข้อกำหนดไปใช้ในการปรับปรุงด้านความปลอดภัยของหน่วยงานบริหารพลเรือนของรัฐบาลกลาง (Federal Civilian Executive Branch: FCEB) รัฐ ท้องถิ่น พื้นที่ชนเผ่า รวมไปถึงดินแดน (SLTT) ในส่วนโครงสร้างพื้นฐานที่สำคัญ และเทคโนโลยีพื้นฐานที่สนับสนุน
- **การมีส่วนร่วมและตระหนักรู้** มีส่วนร่วมกับผู้มีส่วนได้ส่วนเสียในการพัฒนาแผนบรรเทาผลกระทบ และสนับสนุนการนำมาตรฐานไปใช้ทันที่พร้อมใช้งานทั้งในส่วน FCEB SLTT และโครงสร้างพื้นฐานสำคัญต่าง ๆ รวมถึงพัฒนาผลิตภัณฑ์ด้านเทคนิคเพื่อสนับสนุนพันธกิจเหล่านี้ให้ลุล่วง

ในส่วนการคัดกรองเทคโนโลยีตัวอย่างสำหรับเป็นมาตรฐานในการพัฒนาเทคโนโลยีการเข้ารหัสยุคหลังควอนตัมนั้น NIST ได้พิจารณาเทคโนโลยีให้ผ่านการพิจารณาในรอบที่สามได้แก่ CRYSTALS-KYBER CRYSTALS-Dilithium Falcon และ SPHINCS^{+} โดยแบ่งเป็นกลไกการเข้ารหัสแบบกุญแจลับ 1 และลายเซ็นดิจิทัล 3 แบบ

ตัวอย่างเทคโนโลยีการเข้ารหัสสำหรับยุคหลังควอนตัม

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) ได้พิจารณาเทคโนโลยีการเข้ารหัสยุคหลังควอนตัมรอบที่ 3 จนได้เทคโนโลยีผ่านมาตรฐานเข้ารอบนี้จำนวน 4 แบบได้แก่

Kyber เป็นกลไกลการห่อหุ้มคีย์ (Key Encapsulation Mechanism: KEM) ประเภท IND-CCA2 แบบหนึ่งซึ่งอ้างอิงหลักความปลอดภัยตามกระบวนการแก้ปัญหาแบบเรียนรู้จากข้อผิดพลาด (learning-with-error: LWE) กลไกชุดนี้แบ่งความซับซ้อนการเข้ารหัสออกเป็นสามระดับ Kyber-512 เน้นการรักษาความปลอดภัยในระดับ AES-128 Kyber-768 เน้นการรักษาความปลอดภัยในระดับ AES-192 และ Kyber-1028 เน้นการรักษาความปลอดภัยในระดับ AES-256

การใช้งาน Kyber ผู้พัฒนาแนะนำให้ใช้งานในลักษณะดังต่อไปนี้

- ใช้ Kyber ในลักษณะการเข้ารหัสแบบผสมผสาน (Hybrid Mode) ร่วมกับการเข้ารหัส "ยุคก่อนควอนตัม" ตัวอื่นเพื่อเสริมความปลอดภัย เช่นการใช้งานร่วมกับ Diffie-Hellmen
- ควรใช้งานตั้งแต่ระดับ Kyber-768 ขึ้นไป ซึ่งผ่านการวิเคราะห์เบื้องต้นมาแล้วว่าสามารถป้องกันการโจมตีในระดับ 128 บิทที่มีการใช้งานอยู่ได้ทั้งหมด ทั้งการโจมตีแบบทั่วไปและแบบควอนตัม

Dilithium เป็นลายเซ็นดิจิทัลที่มีการป้องกันขั้นสูงจากการโจมตีข้อความถูกเลือกไว้ โดยมีพื้นฐานโครงสร้างจากการแก้ปัญหาแบบแลตติซที่มีหลักการว่าผู้อื่นไม่สามารถสร้างลายเซ็นจากข้อความที่ยังไม่เห็นหรือไม่สามารถสร้างลายเซ็นอื่นได้แม้แต่จะเคยเห็นข้อความแล้วก็ตาม

การใช้งาน Dilithium ผู้พัฒนาแนะนำให้ใช้งานในลักษณะดังต่อไปนี้

- ใช้งาน Dilithium ในลักษณะการเข้ารหัสแบบผสมผสาน (Hybrid mode) ร่วมกับลายเซ็นดิจิทัลรุ่น “ก่อนควอนตัม” แบบอื่น
- แนะนำให้ใช้งาน Dilithium ในระดับ 3 ชั้น ซึ่งผ่านการวิเคราะห์เบื้องต้นมาแล้วว่าสามารถป้องกันการโจมตีในระดับ 128 บิทที่มีการใช้งานอยู่ได้ทั้งหมด ทั้งการโจมตีแบบทั่วไปและแบบควอนตัม

Falcon อัลกอริทึมลายเซ็นดิจิทัลที่พัฒนามาเพื่อป้องกันการโจมตีด้วยคอมพิวเตอร์ควอมตันที่มีพื้นฐานจากโครงสร้างแบบ NTRU lattices ซึ่งเป็นระบบการเข้ารหัสแบบโอเพนซอร์ส คุณสมบัติที่ Falcon ถูกนำไปพิจารณาให้เข้ารอบมีดังต่อไปนี้

- ความปลอดภัย การใช้กระบวนการสุ่มตัวอย่างแบบเกาส์เซียน (Gaussian Sampler) ภายในผู้พัฒนารับประกันโอกาสการรั่วไหลข้อมูลเข้ารหัสมีน้อยมากและปริมาณลายเซ็นใช้เข้ารหัสที่มีจำนวนมหาศาล (มากกว่า 2^{64} ตัวอย่าง)
- ความกะทัดรัด การใช้ NTRU lattices ทำให้ลายเซ็นมีความสั้นกว่าลายเซ็นดิจิทัลแบบอื่นมาก โดยรับประกันความปลอดภัยเทียบเท่ากับแบบอื่นที่มี public keys ความยาวใกล้เคียงกัน
- ความเร็วในการเข้ารหัส การใช้การสุ่มตัวอย่างแบบฟูริเยร์ (Fourier sampling) ช่วยให้การทำงานเป็นไปอย่างรวดเร็ว สามารถสร้างลายเซ็นนับพันต่อวินาทีด้วยคอมพิวเตอร์ใช้งานทั่วไป การยืนยันรหัสทำได้เร็วขึ้นห้าถึงสิบเท่าเมื่อเทียบกับวิธีก่อนหน้า
- ความสามารถในการขยายขนาด กระบวนการมีค่าใช้จ่ายที่ O(n log n) อัตราค่าใช้จ่ายในการรักษาความปลอดภัยในระยะยาวจะมีราคาไม่สูงมาก

- ประหยัด RAM อัลกอริทึมการสร้างรหัสลายเซ็นของ Falcon ใช้หน่วยความจำเพียง 30 กิโลไบท์ เมื่อเทียบกับลายเซ็นดิจิทัลแบบอื่นถือว่ามีขนาดเล็กและเป็นมิตรกับอุปกรณ์ใช้งานทั่วไป

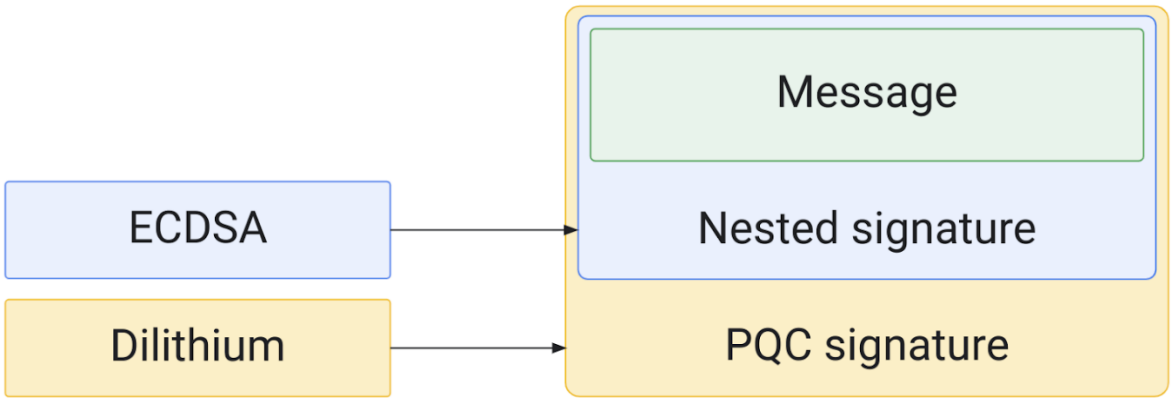
SPHINCS$^+$ เป็นอัลกอริทึมลายเซ็นดิจิทัลแบบไร้สถานะ พัฒนามาเพื่อส่งเข้าร่วมโครงการพัฒนาระบบเข้ารหัสหลังยุคควอนตัมของ NIST การออกแบบนี้อัลกอริทึมนี้พัฒนาต่อยอดมาจาก SPHINCS โดยมีเป้าหมายเพื่อลดขนาดลายเซ็นโดยเฉพาะ หลังจากพัฒนาได้แบ่งรูปแบบการพัฒนาออกมาเป็น 3 รูปแบบ

- SPHINCS$^+$-SHAKE256
- SPHINCS$^+$-SHAKE-256
- SPHINCS$^+$-Haraka

ทั้ง 4รูปแบบที่ผ่านการตัดสินในรอบที่ 3 ต้องกลับไปปรับปรุงการพัฒนาเพิ่มเติมหลายด้าน เช่นการไม่บังคับใช้สิทธิบัตรที่เกี่ยวกับการพัฒนาซอฟท์แวร์ที่พัฒนาจากอัลกอริทึมมาตรฐาน ซึ่งการปรับปรุงอัลกอริทึมเหล่านี้ต้องส่งให้คณะกรรมการดูการปรับปรุงภายในวันที่ 1 ตุลาคม พ.ศ. 2566 นี้

ในภาพรวมอัลกอริทึมที่ผ่านการคัดเลือกจาก NIST แม้จะผ่านการทดสอบเบื้องต้นมาได้ แต่ก็ยังต้องอาศัยการใช้งานแบบผสมผสานเพื่อรับรองความปลอดภัยของข้อมูลให้มากขึ้น รวมถึงแม้จะผ่านเกณฑ์เข้าร่วมพิจารณามาตรฐานจาก NIST ก็ยังมีรายงานอัลกอริทึมถูกโจมตีจนพบว่าสามารถถอดรหัสออกมาได้ ตัวอย่างเช่นกรณีของ SIKE ที่ผ่านการเข้าร่วมพิจารณามาตรฐานในรอบที่4

นอกเหนือจากหน่วยรัฐ ภาคเอกชนหลายแห่งก็เข้ามามีส่วนร่วมในพัฒนาเทคโนโลยีการเข้ารหัสยุคหลังควอนตัม ไม่ว่าจะเป็น Google ร่วมกับ ETH Zürich พัฒนาเฟิร์มแวร์กุญแจการเข้ารหัสยืนยันตัวตน FIDO รุ่นพิเศษ ที่ใช้การซ้อนลายเซ็นดิจิทัลแบบสองชั้นคือ ECDSA แบบดั้งเดิม ร่วมกับ Dilithium ที่ผ่านการพิจารณามาตรฐานจาก NIST เข้าด้วยกัน (ภาพที่2) ทางด้านบริษัทให้บริการด้านเน็ตเวิร์คอย่าง Cloudfare ได้ทดลองใช้อัลกอริทึมยุคหลังควอนตัมอย่าง Kyber มาใช้ในการเข้ารหัสข้อมูลของบริษัท กระบวนการเข้ารหัสที่เลือกใช้มีสองแบบคือ Kyber512Draft00 กับ Kyber768Draft00 ร่วมกับ X25519 เป็น X25519Kyber512Draft00 และ X25519Kyber768Darft00 โดยทั้งหมดยังเป็นการทดลองใช้งานในวงเฉพาะเท่านั้น



ภาพที่ 2 อธิบายเทคนิคการเข้ารหัสลายเซ็นดิจิทัล FIDO แบบพิเศษ (ที่มา: Google security blog)

จากการประชุมของนักพัฒนา คาดว่าอัลกอริทึมที่ผ่านมาตรฐานจะพร้อมใช้งานได้ในช่วงปี พ.ศ. 2567 แต่มาตรฐานที่ใช้อยู่ในปัจจุบันนั้นยังต้องปรับปรุงให้มีความซับซ้อนและใช้งานได้ง่ายขึ้น นักวิเคราะห์มองความเป็นไปได้ว่า คอมพิวเตอร์ควอนตัมจะสามารถใช้งานเชิงธุรกิจราวปี พ.ศ.2573 ซึ่งเมื่อถึงวันนั้น อัลกอริทึมที่พัฒนามาล่วงหน้าเหล่านี้จะได้พิสูจน์ความแข็งแกร่งว่าจะป้องกันการโจมตีในระดับควอนตัมได้จริงหรือไม่ และทนทานเพียงพอจะสร้างความมั่นใจในการรักษาความลับของข้อมูลผู้ใช้งานหรือเปล่า

บรรณานุกรม

ประณิธาน ธรรมเจริญพร. การเข้ารหัสลับ (Encryption) เบื้องต้นสำหรับนักพัฒนา. Big Data Thailand [อินเตอร์เน็ต]. 2566 [เข้าถึงเมื่อ 8 กันยายน 2566]; เข้าถึงได้จาก: https://bigdata.go.th/big-data-101/encoding-and-encryption-for-developers/

การเข้ารหัสคืออะไร. Amazon Web Service [อินเตอร์เน็ต]. 2566 [เข้าถึงเมื่อ 8 กันยายน 2566]; เข้าถึงได้จาก: https://aws.amazon.com/th/what-is/cryptography

Rahul_Roy. Conventional computing vs quantum computing. Geeks for Geeks [Internet]. 2022 [cited 2023 September 8]; Available from: https://www.geeksforgeeks.org/conventional-computing-vs-quantum-computing/

Breaking RSA with a Quantum Computer. Schneier on Security [Internet]. 2023 [cited 2023 September 12]; Available from: https://www.schneier.com/blog/archives/2023/01/breaking-rsa-with-a-quantum-computer.html

Scott Aaronson. Cargo cult quantum factoring. Shtetl-Optimized [Internet]. 2023 [cited 2023 September 12]; Available from: https://scottaaronson.blog/?p=6957

National quantum initiative advisory committee. Quantum.gov [Internet]. 2023 [cited 2023 September 12]; Available from: https://www.quantum.gov/about/nqiac/

Announcement: the end of the 3rd round - the first PQC algorithms to be standardized. Google Groups [Internet]. 2023 [cited 2023 September 12]; Available from: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/G0DoD7lkGPk?pli=1

Dilithium. CRYSTALS [Internet]. 2023 [cited 2023 September 12]; Available from: https://pq-crystals.org/dilithium/index.shtml

KYBER. CRYSTALS [Internet]. 2023 [cited 2023 September 12]; Available from: https://pq-crystals.org/kyber/index.shtml

Falcon. FALCON [Internet]. 2023 [cited 2023 September 12]; Available from: https://falcon-sign.info/

SPHINCS^{+}. SPHINCS [Internet]. 2023 [cited 2023 September 12]; Available from: https://falcon-sign.info/https://sphincs.org/

Dan Goodin. Post-quantum encryption contender is taken out by single-core PC and 1 hour. arsTechnica [Internet]. 2022 [cited 2023 September 12]; Available from: https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/

Elie Bursztein. Toward quantum resilient security keys. Google Security Blog [Internet]. 2023 [cited 2023 September 12]; Available from: https://security.googleblog.com/2023/08/toward-quantum-resilient-security-keys.html