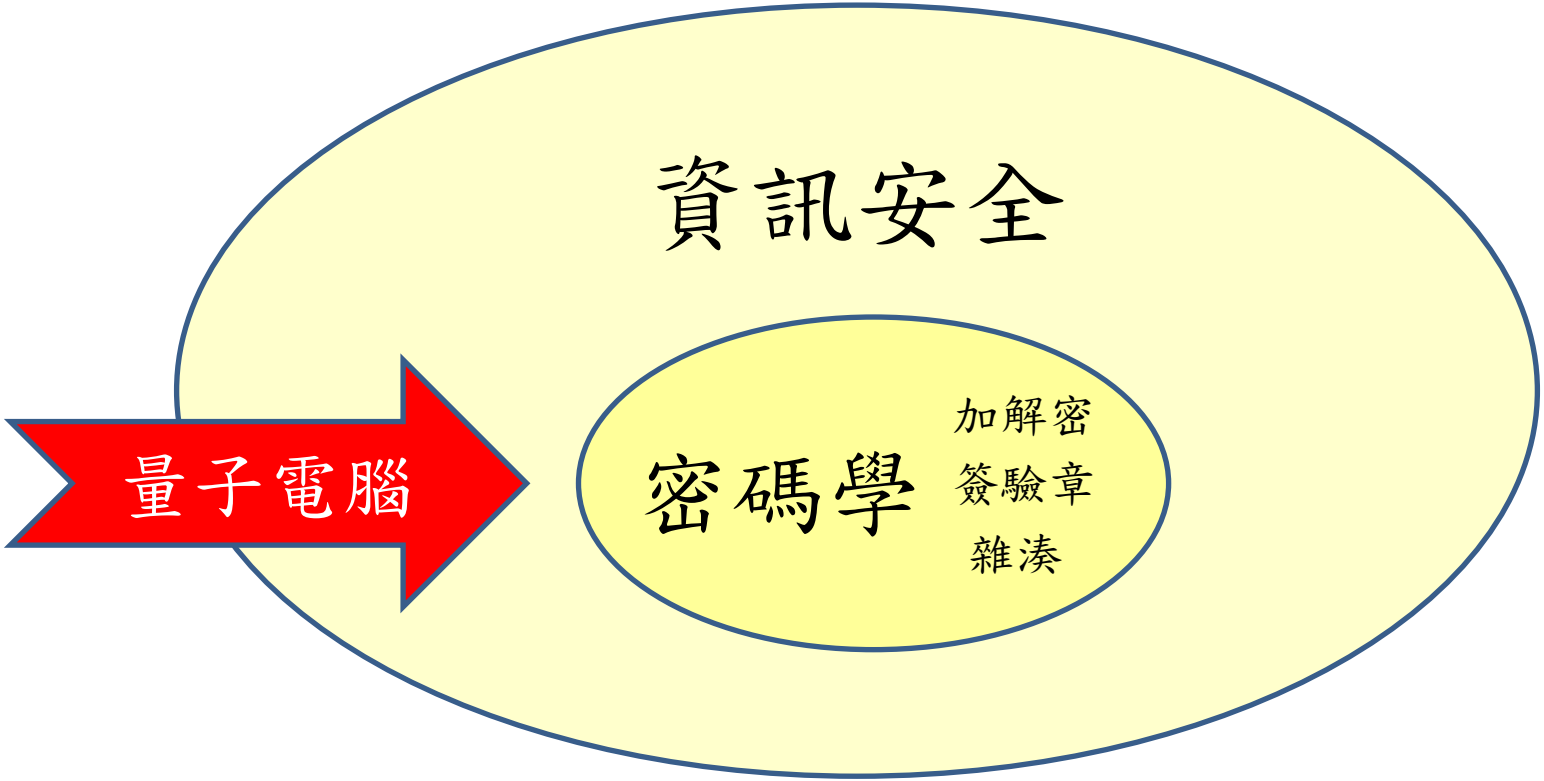
後量子密碼標準制定

陳君明 博士

匯智安全科技

台大數學系/EMBA

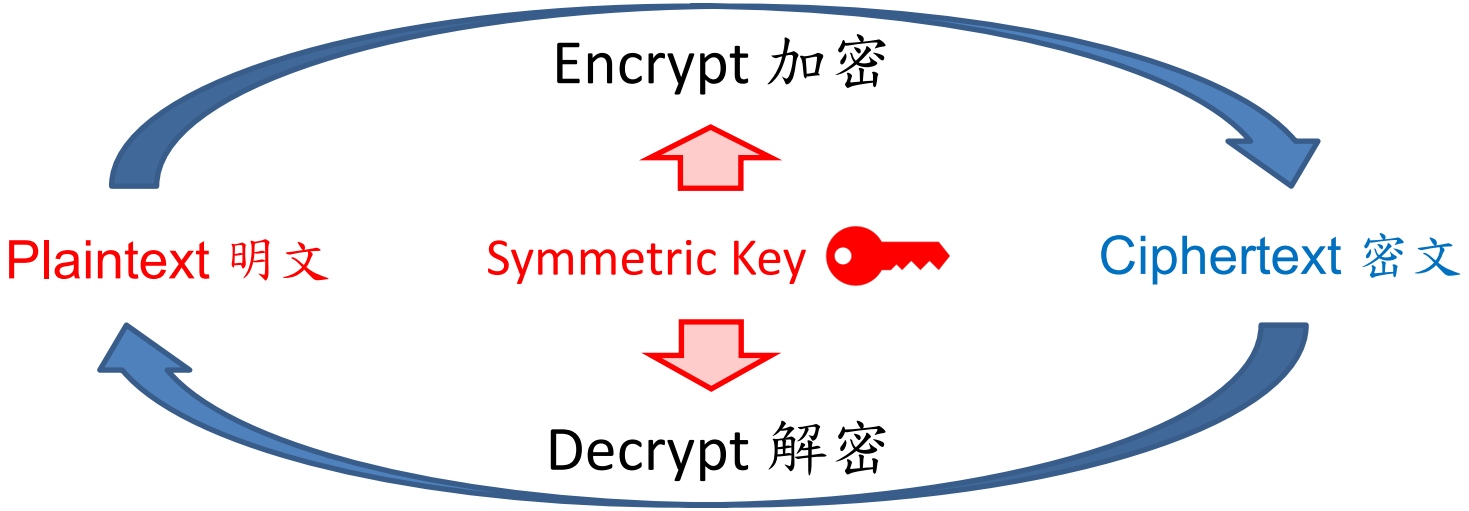
- 公鑰密碼系統 Public-Key Cryptosystem
- 量子計算 Quantum Computing
- 後量子密碼 Post-Quantum Cryptography
- 標準制定 Standardization
- 過渡至後量子 Migration to Post-Quantum


資訊安全
量子電腦
密碼學
加解密
簽驗章
雜湊

Caesar Cipher 凱撒加密

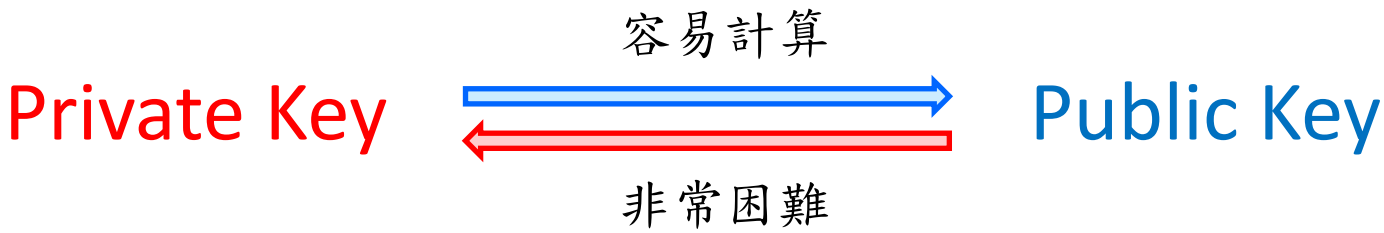
- Gāius Jūlius Caesar (100 BC – 44 BC)
  - 羅馬帝國軍事與政治領導人
- Caesar Cipher
  - 編碼 (Encode) : A ↔ 0, B ↔ 1, …, Y ↔ 24, Z ↔ 25
    - 明文 (Plaintext) : SPY (18 15 24)
    - 密文 (Ciphertext) : VSB (21 18 1)
  - 加密 (Encryption) : $c = p + 3 \mod 26$
  - 解密 (Decryption) : $p = c - 3 \mod 26$
    - 密鑰 (Key) : $k = 3$

Symmetric Cryptosystem 對稱密碼系統



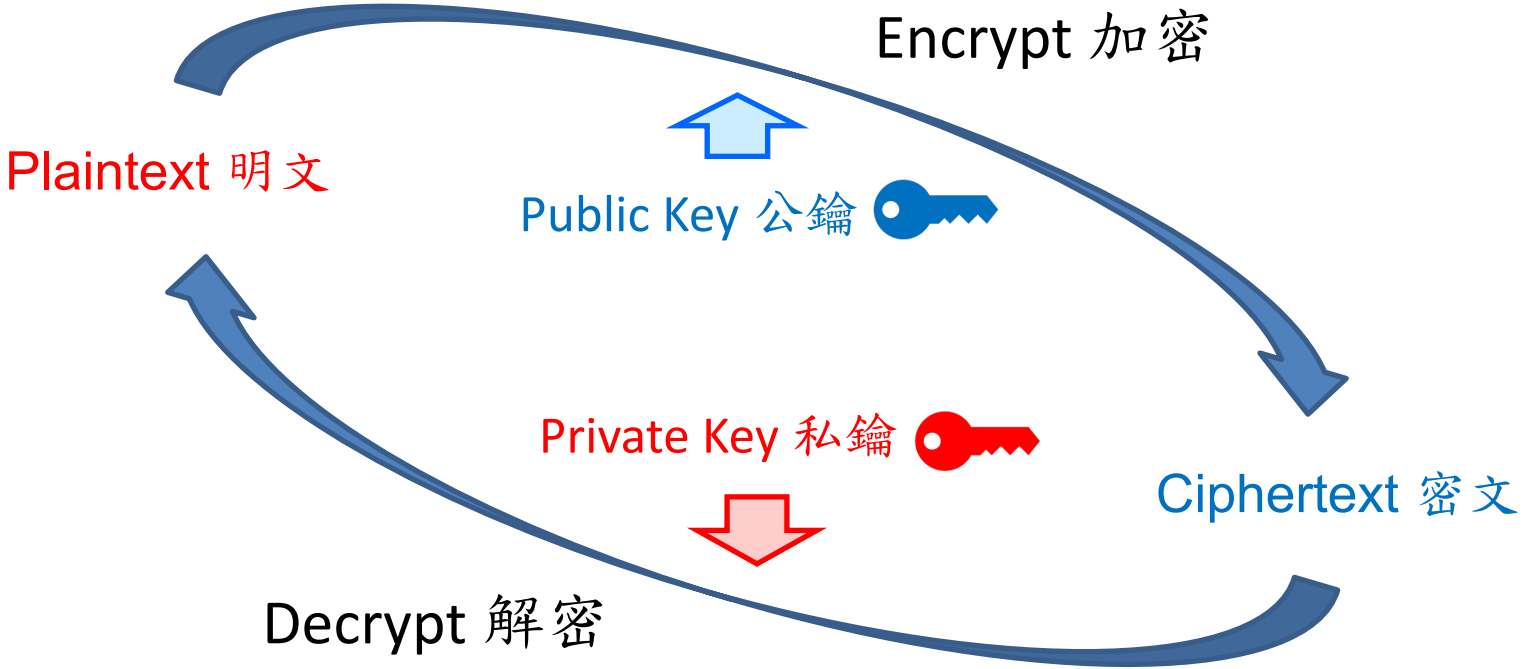
AES (Advanced Encryption Standard), DES (Data Encryption Standard)

私鑰 與 公鑰

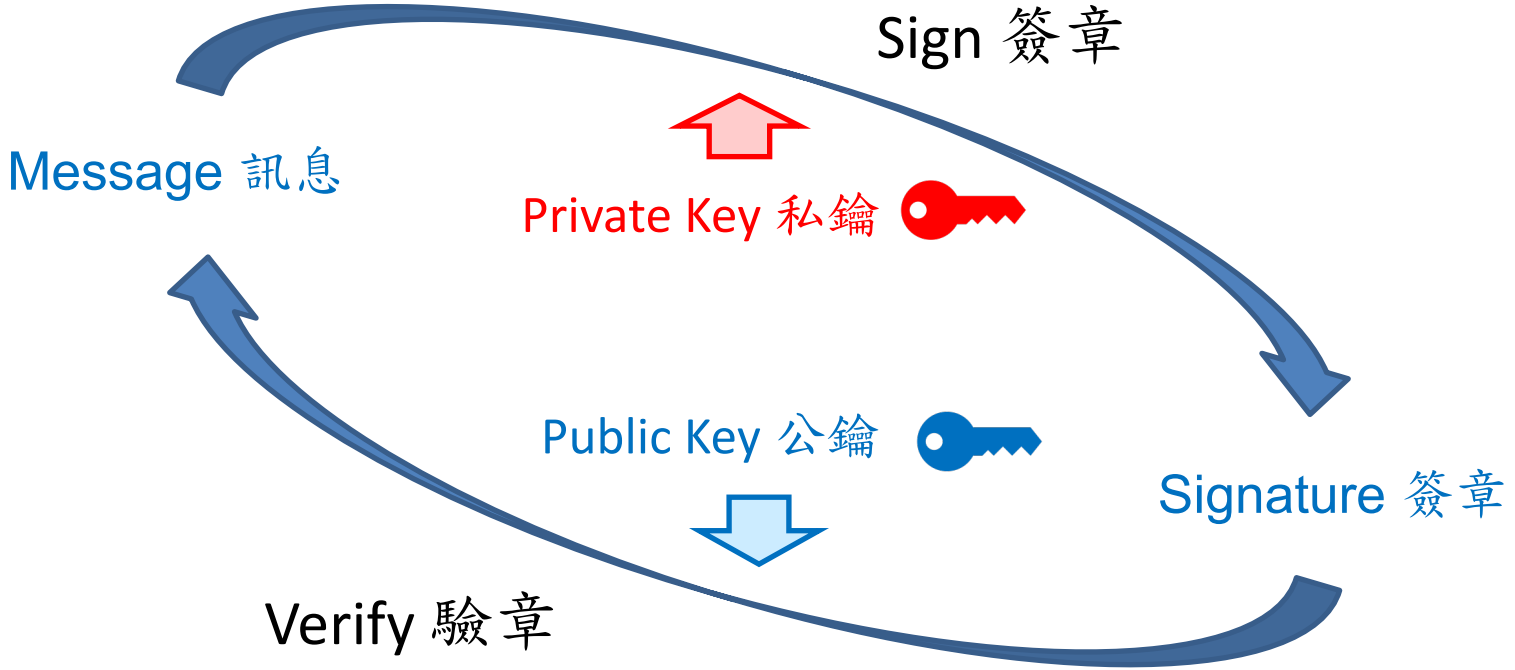


- 現今公鑰密碼系統的安全基礎為計算難題
  - 質因數分解：RSA
  - 離散對數：DHKE (Diffie-Hellman Key Exchange), DSA (Digital Signature Algorithm), ECDH 與 ECDSA 等 ECC (Elliptic Curve Cryptosystems)

Public-Key Cryptosystem 公鑰密碼系統



Digital Signature 數位簽章



- 公鑰密碼系統 Public-Key Cryptosystem
- 量子計算 Quantum Computing
- 後量子密碼 Post-Quantum Cryptography
- 標準制定 Standardization
- 過渡至後量子 Migration to Post-Quantum

量子 (Quantum)

- 「量子」是物理學家描述微觀世界的理論
- 「量子」非粒子本身，而是粒子的狀態或特性
- 某物理量若存在最小不可分割的基本單位，則它是不連續的(量子化的)，該基本單位稱為「量子」

量子疊加 (Superposition)

- 若一個物理系統可能處於許多狀態中的一種，那麼最一般的狀態是所有這些可能性的組合

0 1 0 1 既是 0 又是 1

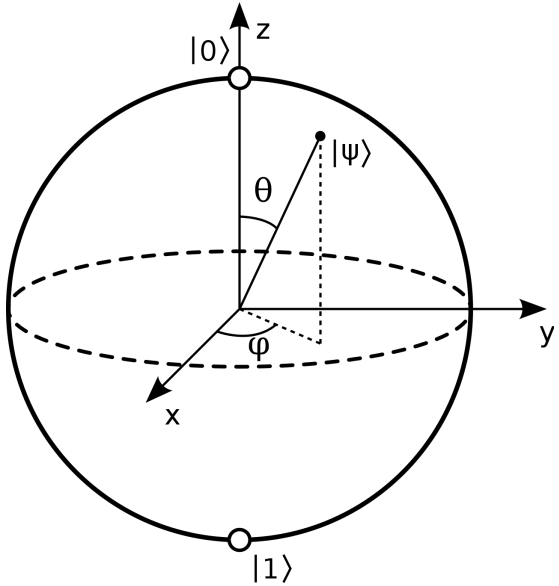
Bit 位元

Qubit 量子位元

量子位元 (Qubit)

Bit 位元

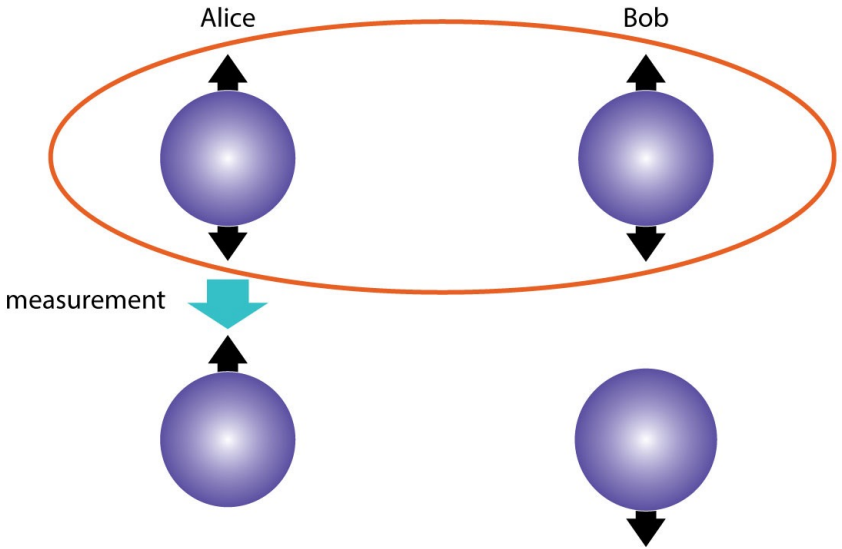
Qubit 量子位元



https://en.wikipedia.org/wiki/Qubit

量子糾纏 (Entanglement)

- 一對處於糾纏態的粒子，相隔甚遠仍可瞬間產生聯繫，量測其一即可確定另一者的狀態
- 百年前愛因斯坦稱之為
  “鬼魅般的超距作用”
  (spooky action at a distance)



量子計算 (Quantum Computing)

- 以粒子的「量子疊加」與「量子糾纏」特性為基礎，進行資訊處理的科學

傳統電腦：4 bits 的
16 種狀態依序跑一次

0000 0001 0010 0011
0100 0101 0110 0111
1000 1001 1010 1011
1100 1101 1110 1111

量子電腦：4 qubits
同時處理 16 種狀態

Shor's Algorithm

- Peter Shor (AT&T's Bell Labs) 1994 發現的演算法，未來若實現於成熟的大規模 (large scale, 2000+ qubits) 通用量子電腦，可破解現今所有標準公鑰密碼系統
- 歷史上首次執行 Shor 演算法於 2001 年，IBM 的 7-qubit 量子電腦分解 15 = 3 × 5

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

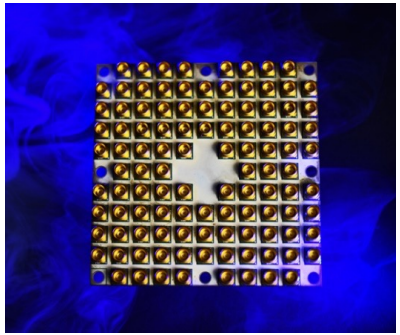
A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Grover's Algorithm

- Grover 量子演算法影響所有對稱式密碼系統，安全參數縮減一半，但不如 RSA / ECC / DHKE 於多項式時間被 Shor 演算法破解之威脅劇烈
- 若加長對稱式密鑰，量子計算並不構成威脅，例如 AES-256 仍有 128 位元的量子安全參數

近年量子電腦發展加速

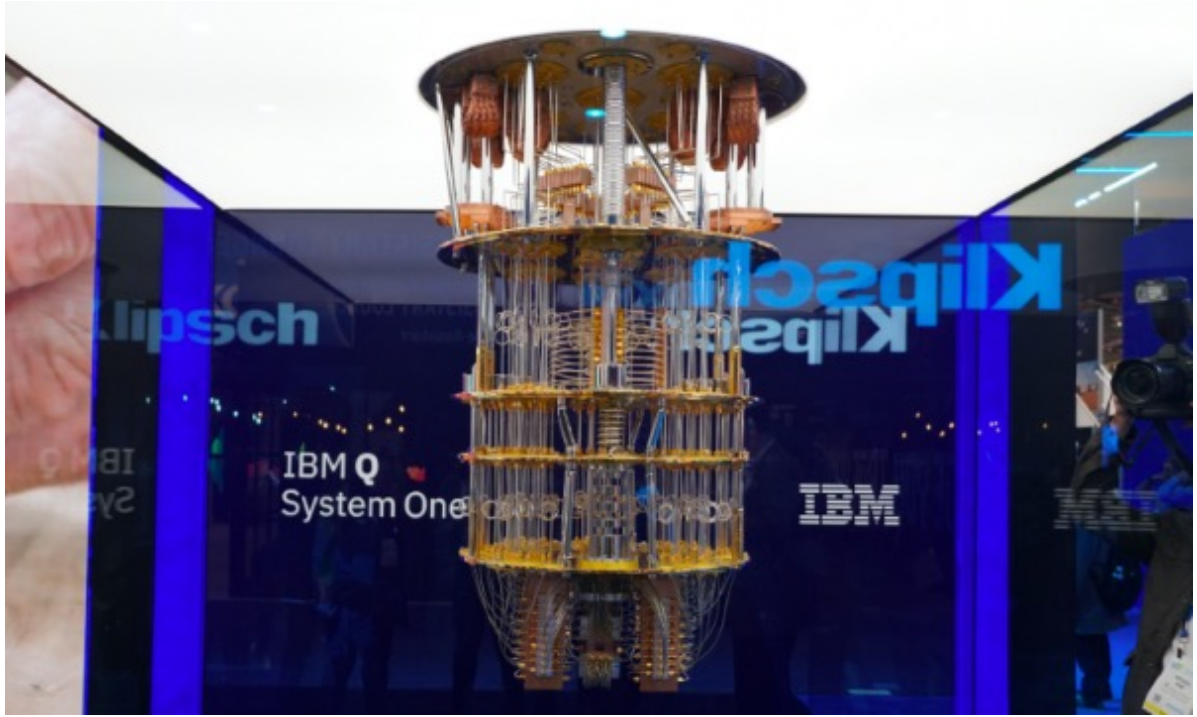
Intel's 49-qubit chip "Tangle-Lake"
January 2018



IBM's 50-qubit quantum computer
November 2017

Google's 72-qubit chip "Bristlecone"
March 2018

全球第一台商用通用量子電腦

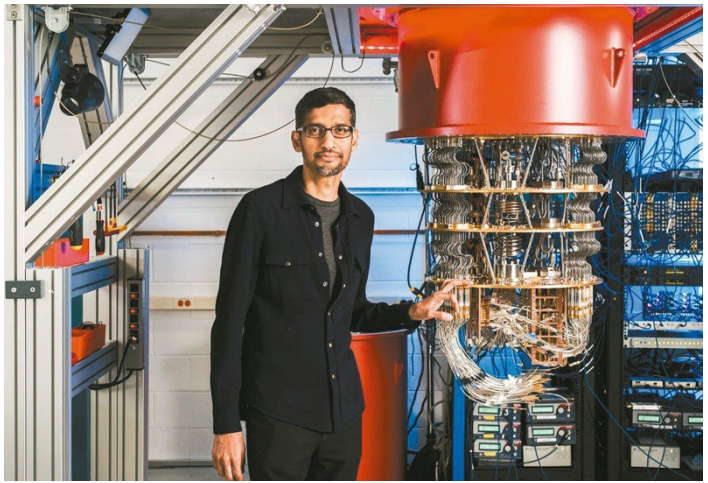


IBM's 53-qubit Quantum Computer

October 2019

量子霸權 (Quantum Supremacy)

- 以量子電腦完成一項運算，而該運算無法以任何傳統 (超級) 電腦在合理時間內完成
- Google 宣稱達到量子霸權



CEO Sundar Pichai with one of Google's quantum computers in the Santa Barbara lab.
October 2019

https://news.cgtn.com/news/2019-10-24/Google-unveils-quantum-computer-breakthrough-critics-say-wait-a-qubit-L2NlmoZVMA/index.html

- 公鑰密碼系統 Public-Key Cryptosystem
- 量子計算 Quantum Computing
- 後量子密碼 Post-Quantum Cryptography
- 標準制定 Standardization
- 過渡至後量子 Migration to Post-Quantum

PQC 後量子密碼學

- **後量子密碼學** (PQC, Post-Quantum Cryptography) 又稱**抗量子密碼學**，是現代密碼學的一個領域，專門研究可抵抗量子電腦攻擊的公鑰密碼系統
- 不同於量子密碼學 (QC, Quantum Cryptography) 或量子密鑰分配 (QKD, Quantum Key distribution)，**後量子密碼學**使用現有電腦與網路，不依靠量子力學，其基礎是公認無法被量子電腦有效解決的計算難題

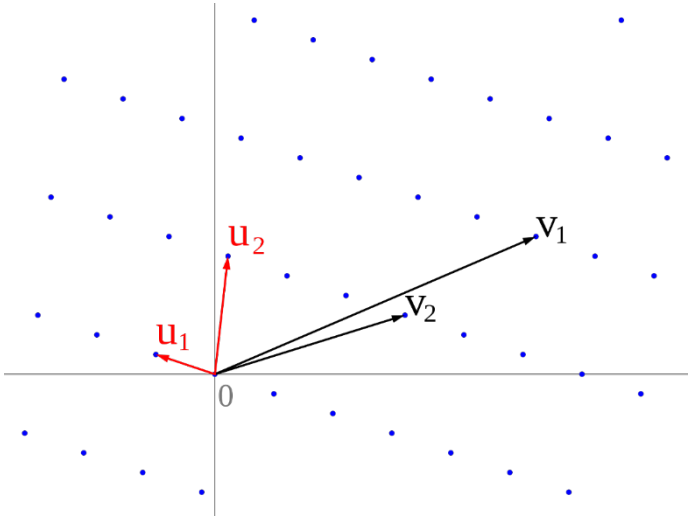
晶格 (Lattice) 上的計算難題

- Given a basis $B = \{b_1, b_2, \dots, b_n\}$ where $b_i \in \mathbb{R}^n$
- Lattice is a discrete subgroup of $\mathbb{R}^n$:

  $\Lambda(B) = B\mathbb{Z}^n = \{\sum_{i=1}^{n} m_i b_i \mid m_i \in \mathbb{Z}\}$
- Shortest Vector Problem (SVP) :

  Find a shortest $x \in \Lambda(B) \setminus \{0\}$
- Closest Vector Problem (CVP) :

  Find a closest $x \in \Lambda(B)$ to a given $y \in \mathbb{R}^n$



- Lattice basis reduction :

  Given a “bad” basis, find a “good” basis such that SVP or CVP is easier

President Biden Signed Memo

- Joe Biden, USA president, signed memorandum to combat quantum computing threat with PQC

THE WHITE HOUSE

BRIEFING ROOM

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3020175/president-biden-signs-memo-to-combat-quantum-computing-threat/

拜登簽署安全備忘錄，維繫美國於量子運算上的領導地位

美國總統拜登除了要全力發展量子資訊科學，也要將重大基礎設施及政府系統遷移到抗量子的密碼學系統

文/ 陳曉莉 | 2022-05-06 發表

美國總統拜登 (Joe Biden) 周三 (5/4) 簽署一國家安全備忘錄 (National Security Memorandum，NSM)，指示美國必須維繫於量子資訊科學上的主導地位，同時要求各政府機構必須將易受攻擊的密碼系統遷移到抗量子的密碼學系統上。根據該備忘錄，白宮認為量子電腦具備推動全美經濟創新的潛力，從材料科學、金融到能源等各領域都有可能受惠，而美國在技術與科學上的領導地位，至少有部分取決於國家在量子運算與量子資訊科學上保持競爭優勢。

然而，伴隨量子運算優點而來的還有對美國經濟與國家安全所帶來的風險，因為可用來執行密碼分析的複雜量子電腦 (Cryptanalytically Relevant Quantum Computer，CRQC)，將得以用來破解美國與全球數位系統所使用的公鑰密碼，一旦CRQC誕生，就可能危及民用與軍用的通訊，破壞重大基礎設施的監控與控制系統，並摧毀絕大多數基於網路之金融交易的安全協定。

為了平衡美國在量子運算上的競爭機會與潛在風險，拜登指示美國要持續投資量子運算，同時逐步將國家的密碼系統遷移到可對抗量子運算的密碼學系統上。

https://www.ithome.com.tw/news/150797

- 公鑰密碼系統 Public-Key Cryptosystem
- 量子計算 Quantum Computing
- 後量子密碼 Post-Quantum Cryptography
- 標準制定 Standardization
- 過渡至後量子 Migration to Post-Quantum

New Standards Developed by NIST

- Since 2015, NIST has been working with experts from around the world to develop new Post-Quantum Cryptography (PQC) standards that will work with our current computers — while being resistant to future quantum machines

https://csrc.nist.gov/Projects/post-quantum-cryptography

NIST PQC Standardization Timeline

- Aug. 2016 – Draft submission requirements & evaluation criteria
- Nov. 2017 – Deadline for submissions (69 algorithms)
- Jan. 2019 – 2nd Round announced (26 algorithms)
- Jul. 2020 – 3rd Round announced (7 Finalists and 8 Alternates)
- **Jul. 5, 2022** – Announcement of Candidates (4 algorithms) to be Standardized and 4th Round Candidates (4 algorithms)
- 2023-2024 – Draft standards available

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

Algorithms to be Standardized

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS–KYBER	CRYSTALS–Dilithium
	FALCON
	SPHINCS$^+$

Latttice-based

Hash-based

Candidates advancing to the Fourth Round

Public-Key Encryption/KEMs	Digital Signatures
BIKE	
Classic McEliece	
HQC	
SIKE	

(broken)

Code-based

Supersingular Isogeny

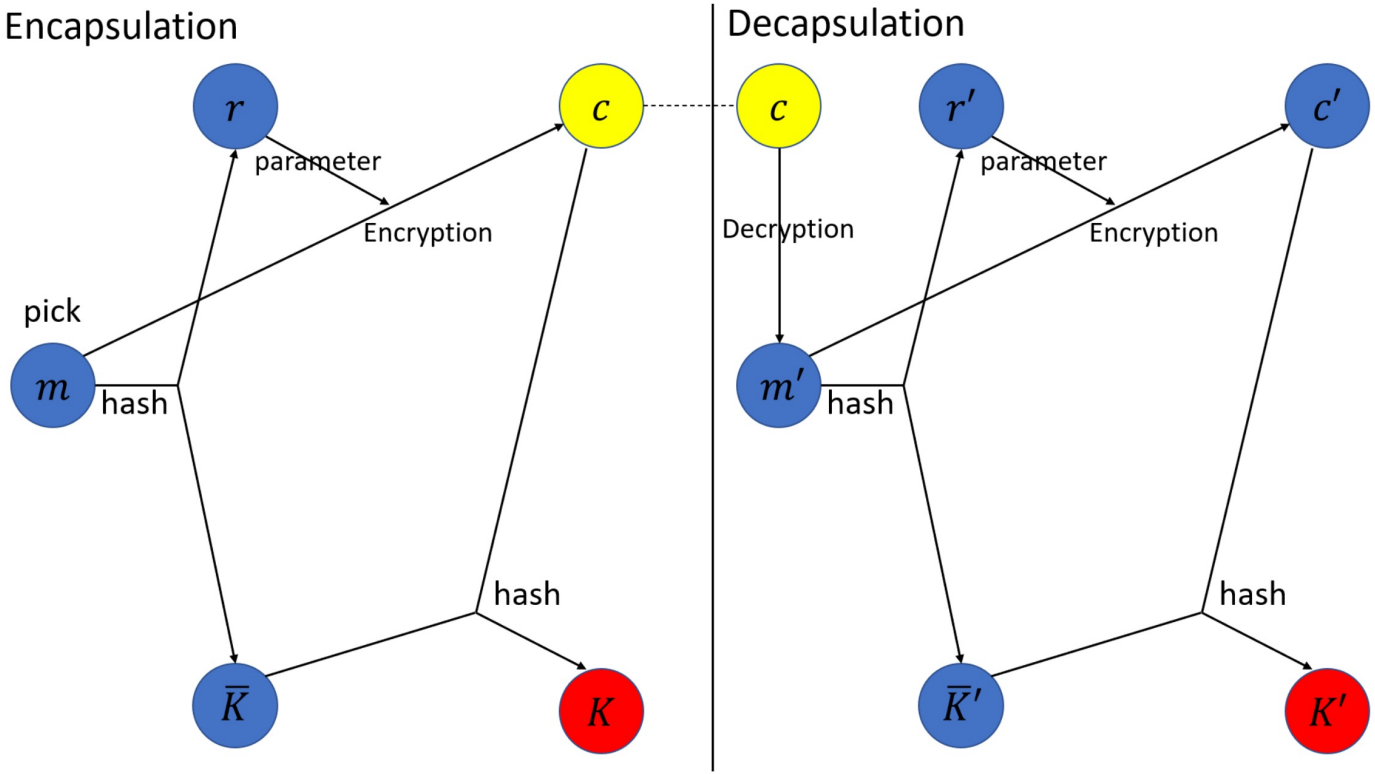
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

結構化晶格 Structured Lattices

- Kyber $Z_q[x]/(x^{256}+1)$ $q = 3329 = 13\times 2^8 + 1$
- Dilithium $Z_q[x]/(x^{256}+1)$ $q = 8380417 = 2^{23} - 2^{13} + 1$
- Falcon $Z_q[x]/(x^{256}+1)$ $q = 12289 = 12\times 2^{10} + 1$

Kyber

KEM : Key Encapsulation Mechanism



Candidate	Claimed Security	Public key	Private key	Ciphertext
KYBER512	Level 1	800	1632	768
KYBER768	Level 3	1184	2400	1088
KYBER1024	Level 5	1568	3168	1568
Classic McEliece348864	Level 1	261120	6492	128
Classic McEliece460896	Level 3	524160	13608	188
Classic McEliece6688128	Level 5	104992	13932	240
Classic McEliece6960119	Level 5	1047319	13948	226
Classic McEliece8192128	Level 5	1357824	14120	240
BIKE	Level 1	1540	280	1572
	Level 3	3082	418	3114
	Level 5	5122	580	5154
HQC-128	Level 1	2249	40	4481
HQC-192	Level 3	4522	40	9026
HQC-256	Level 5	7245	40	14469
SIKEp434	Level 1	330	374	346
SIKEp503	Level 2	378	434	402
SIKEp610	Level 3	462	524	486
SIKEp751	Level 5	564	644	596

Table 1: Key and ciphertext sizes (in bytes) for the KEM candidates.

Candidate	Claimed Security	Public key	Private key	Signature
Dilithium	Level 2	1312	2528	2420
	Level 3	1952	4000	3293
	Level 5	2592	4864	4595
FALCON-512	Level 1	897	7553	666
FALCON-1024	Level 5	1793	13953	1280
SPHINCS$^+$-128s	Level 1	32	64	7856
SPHINCS$^+$-128f	Level 1	32	64	17088
SPHINCS$^+$-192s	Level 3	48	96	16224
SPHINCS$^+$-192f	Level 3	48	96	35664
SPHINCS$^+$-256s	Level 5	64	128	29792
SPHINCS$^+$-256f	Level 5	64	128	49856

Table 2: Key and signature sizes (in bytes) for the signature candidates.

Candidate	Claimed Security	Key generation	Encapsulation	Decapsulation
KYBER512	Level 1	33856	45200	34572
KYBER768	Level 3	52732	67624	53156
KYBER1024	Level 5	73544	97324	79128
Classic McEliece348864	Level 1	46526112	43832	134184
Classic McEliece460896	Level 3	158155696	115540	270856
Classic McEliece6688128	Level 5	458561448	149080	322988
Classic McEliece6960119	Level 5	330214944	159116	300688
Classic McEliece8192128	Level 5	409854088	177480	325744
BIKE	Level 1	600000	220000	2220000
	Level 3	1780000	465000	6610000
	Level 5			
HQC-128	Level 1	83000	197000	349000
HQC-192	Level 3	200000	456000	740000
HQC-256	Level 5	400000	887000	1478000
SIKEp434	Level 1	5927000	9681000	10343000
SIKEp503	Level 2	8243000	13544000	14415000
SIKEp610	Level 3	14890000	27254000	27445000
SIKEp751	Level 5	25197000	40703000	43851000

Table 3: Runtime benchmarks (in cycles) for the KEM candidates.

Candidate	Claimed Security	Key generation	Signing	verification
Dilithium	Level 2	124031	259172	118412
	Level 3	256403	428587	179424
	Level 5	298050	538986	279936
FALCON-512	Level 1	19872000	386678	82339
FALCON-1024	Level 5	63135000	789564	168498
SPHINCS$^+$-128s	Level 1	84964790	644740090	861478
SPHINCS$^+$-128f	Level 1	1334220	33651546	2150290
SPHINCS$^+$-192s	Level 3	125310788	1246378060	1444030
SPHINCS$^+$-192f	Level 3	1928970	55320742	3492210
SPHINCS$^+$-256s	Level 5	80943202	1025721040	1986974
SPHINCS$^+$-256f	Level 5	5067546	109104452	3559052

Table 4: Runtime benchmarks (in cycles) for the signature candidates.

Side Channel Attack (SCA)

旁通道攻擊

PQC 實作也需要 SCA 防禦

- ECDSA Key Extraction from Mobile Devices: Fully extract secret signing keys from OpenSSL and CoreBitcoin running on iOS devices

https://www.tau.ac.il/~tromer/mobilesc

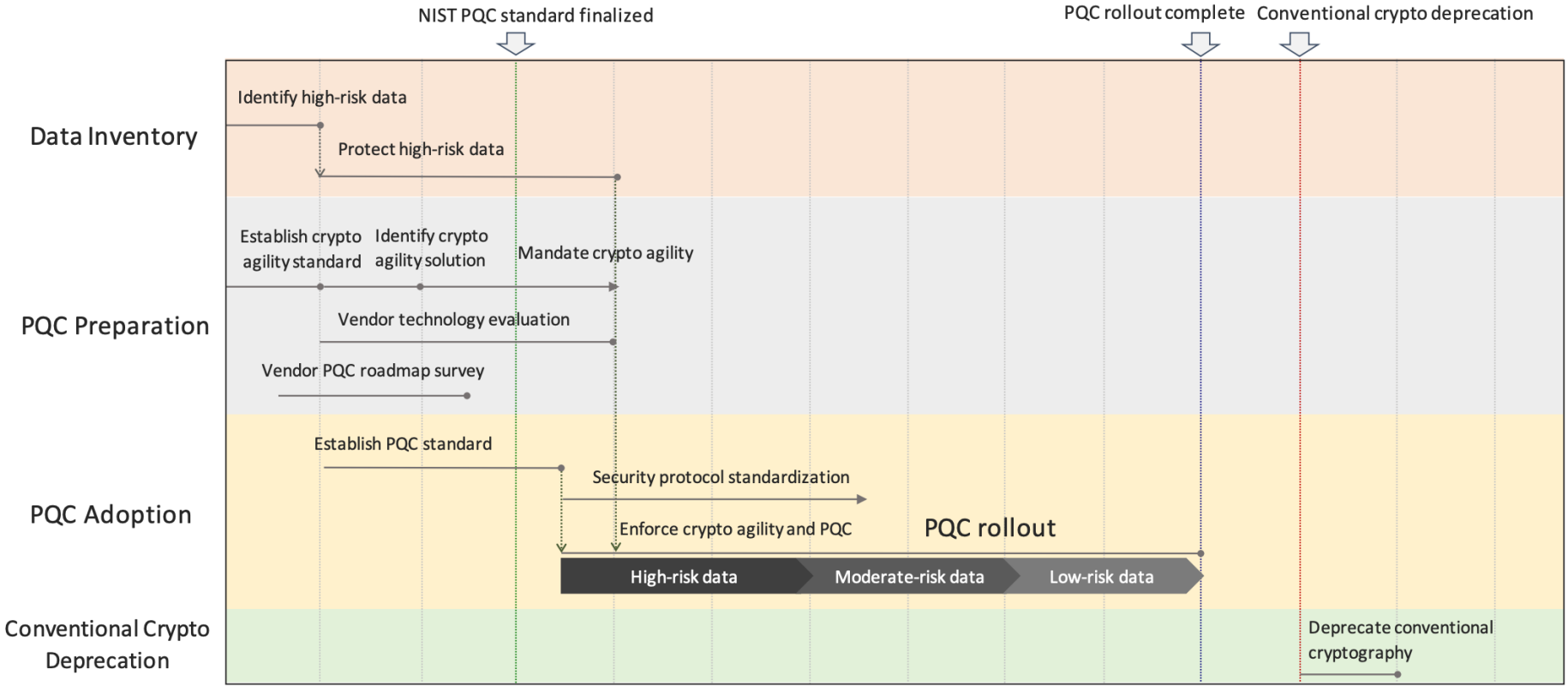
- 公鑰密碼系統 Public-Key Cryptosystem
- 量子計算 Quantum Computing
- 後量子密碼 Post-Quantum Cryptography
- 標準制定 Standardization
- 過渡至後量子 Migration to Post-Quantum

Virtual Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms

Wednesday, October 07, 2020

https://www.nccoe.nist.gov/sites/default/files/2021-10/6-Yassir-NIST-%2020200819-8.pdf
https://www.nccoe.nist.gov/get-involved/attend-events/virtual-workshop-considerations-migrating-post-quantum-cryptographic/post-workshop-materials

Reference PQC Transition Timeline



https://www.nccoe.nist.gov/sites/default/files/2021-10/6-Yassir-NIST-%2020200819-8.pdf

密碼敏捷 Cryptographic Agility

- **Crypto-Agility** is a practice paradigm in designing information security protocols and standards in a way so that they can support multiple cryptographic primitives and algorithms at the same time
- A security system is considered **crypto-agile** if its cryptographic algorithms or parameters can be replaced with ease and is at least partly automated
- The impending arrival of a quantum computer that can break existing asymmetric (public-key) cryptography is raising awareness of the importance of **cryptographic agility**

https://en.wikipedia.org/wiki/Cryptographic_agility

Project: Migration to PQC

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project, including background, goal, challenges, and potential benefits.

https://www.nccoe.nist.gov/sites/default/files/2022-06/Migration-to-PQC-05-16.pdf

Prepare for a New Cryptographic Standard to Protect Against Future Quantum-Based Threats

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Original release date: July 05, 2022

- Inventorying your organization's systems for applications that use public-key cryptography.
- Testing the new post-quantum cryptographic standard in a lab environment; however, organizations should wait until the official release to implement the new standard in a production environment.
- Creating a plan for transitioning your organization's systems to the new cryptographic standard that includes:
  - Performing an interdependence analysis, which should reveal issues that may impact the order of systems transition;
  - Decommissioning old technology that will become unsupported upon publication of the new standard; and
  - Ensuring validation and testing of products that incorporate the new standard.
- Creating acquisition policies regarding post-quantum cryptography. This process should include:
  - Setting new service levels for the transition.
  - Surveying vendors to determine possible integration into your organization's roadmap and to identify needed foundational technologies.
- Alerting your organization's IT departments and vendors about the upcoming transition.
- Educating your organization's workforce about the upcoming transition and providing any applicable training.

https://www.cisa.gov/uscert/ncas/current-activity/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum

首批NIST認可的PQC演算法出爐，美CISA建議即刻做好六大準備

美國NIST在今年7月初，公布了第一批入選後量子密碼學（PQC）標準的4款演算法，儘管標準要到2024年出爐，但美CISA與NIST強烈建議，企業組織現在就應為升級做準備，並提出六大準備要項可供依循，首先就是需盤點內部使用公鑰密碼的系統，並要制定PQC路線圖、找出優先轉換的系統、調查供應商等預先準備工作

文/ 羅正漢 | 2022-07-13 發表

美國政府已要求組織著手規畫轉換，並發布相關指引

不論如何，隨著量子運算的發展，公鑰密碼系統全面撤換已成大勢所趨。

雖然這是NIST為美國制訂的標準，但其影響也將形成全球的標準，臺灣企業也應留意並作好準備。

面對標準演算法的轉換，以及硬體設備與中介軟體升級，近期有許多密碼學專家已開始呼籲政府、組織與企業重視，建議大家可以先盤點已使用公鑰密碼系統的部分。

https://www.ithome.com.tw/tech/151925

Thank You!