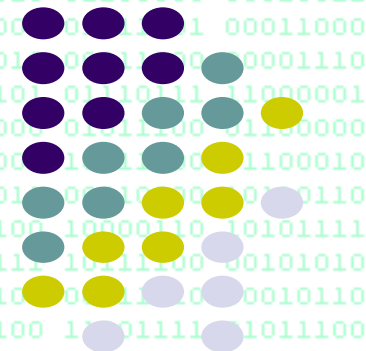


# 量子計算對資訊安全 的威脅與應對之道



陳君明

[jmchen@ntu.edu.tw](mailto:jmchen@ntu.edu.tw)



1. 資訊安全與密碼學

2. 量子計算對資訊安全的威脅

3. 量子電腦的發展

4. 美國 NIST 制定 PQC 國家標準

5. 美國 NSA 的公開聲明

6. 歐盟網路安全局的研究報告

7. PQC 應用實例

8. 過渡至 PQC 時代



# 資訊安全

量子電腦

密碼學

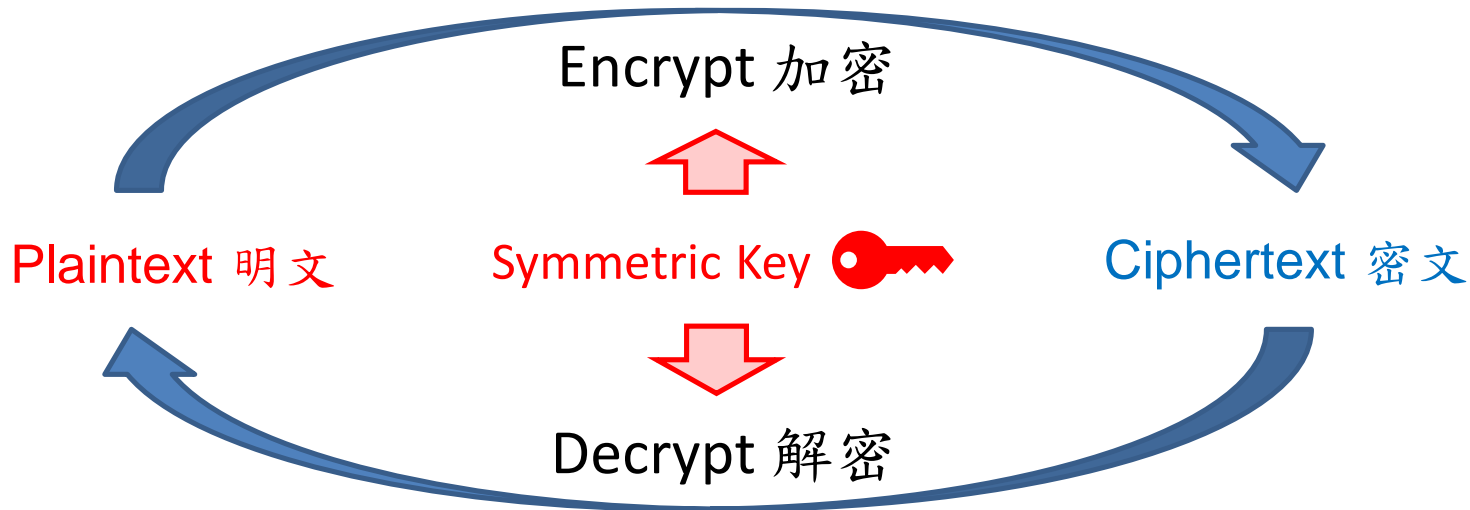
加解密  
簽驗章  
雜湊

# 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) :  $A \leftrightarrow 0, B \leftrightarrow 1, \dots, Y \leftrightarrow 24, Z \leftrightarrow 25$ 
    - 明文 (Plaintext) : SPY (18 15 24)
    - 密文 (Ciphertext) : VSB (21 18 1)
  - 加密 (Encryption) :  $c = p + 3 \pmod{26}$
  - 解密 (Decryption) :  $p = c - 3 \pmod{26}$ 
    - 密鑰 (Key) :  $k = 3$

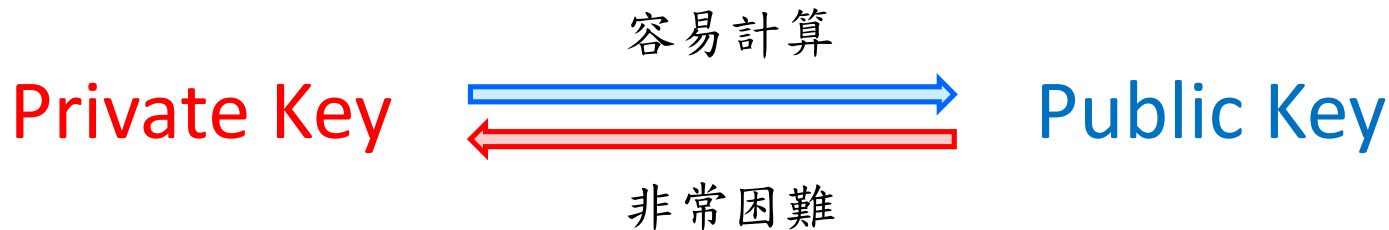


# Symmetric Cryptosystem 對稱密碼系統



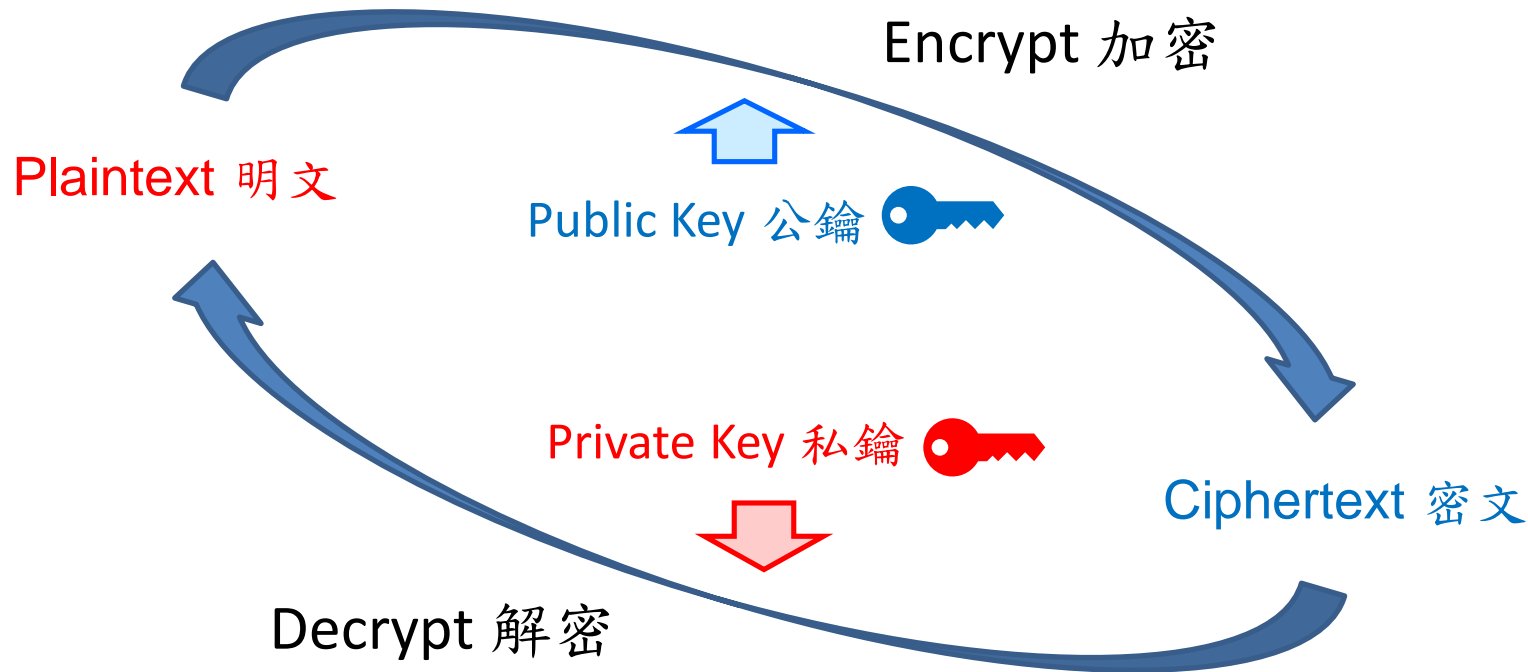
AES (Advanced Encryption Standard), DES (Data Encryption Standard)

# 私鑰 與 公鑰

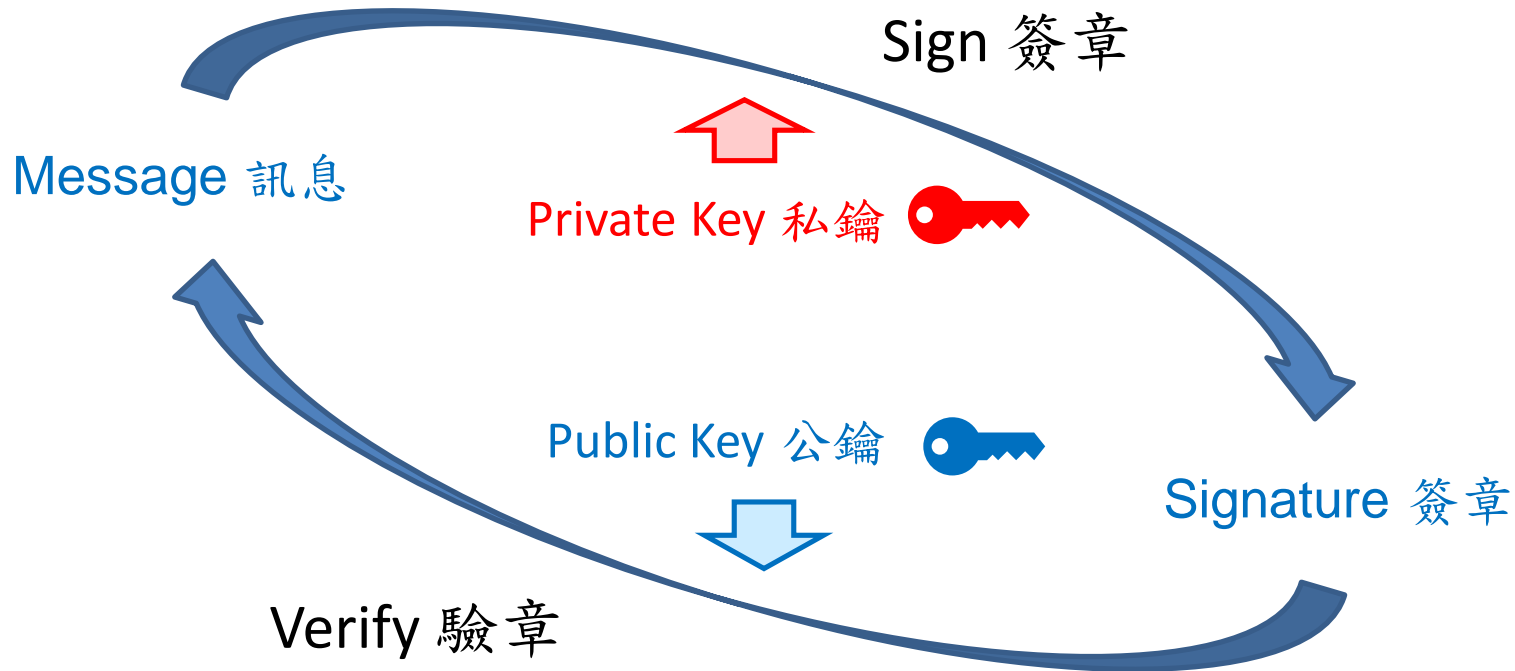


- 現今公鑰密碼系統的安全基礎為計算難題
  - 質因數分解：RSA
  - 離散對數問題：DHKE (Diffie-Hellman Key Exchange), DSA (Digital Signature Algorithm), ECDH 與 ECDSA 等 ECC (Elliptic Curve Cryptosystems)

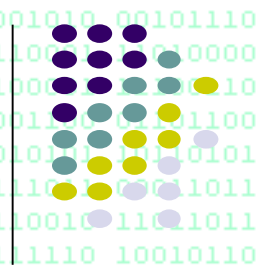
# Public-Key Cryptosystem 公鑰密碼系統



# Digital Signature 數位簽章







1. 資訊安全與密碼學
2. 量子計算對資訊安全的威脅
3. 量子電腦的發展
4. 美國 NIST 制定 PQC 國家標準
5. 美國 NSA 的公開聲明
6. 歐盟網路安全局的研究報告
7. PQC 應用實例
8. 過渡至 PQC 時代

# Quantum 量子

- Quantum Computing 量子計算
  - 利用量子力學特性進行計算
- Quantum Cryptanalysis 量子破密
  - 以量子計算破解密碼系統
    - Shor's algorithm → 公鑰密碼系統
    - Grover's algorithm → 對稱密碼系統
  - 防禦：QKD 或 PQC

# Shor's Algorithm

- Peter Shor (AT&T's Bell Labs) 於 1994 發現的演算法，未來若實現於成熟的大規模 (large scale, 2000+ qubits) 通用型 (universal) 量子電腦，可破解現今所有標準公鑰密碼系統
- 先將質因數分解或離散對數問題，轉化為 Order-Finding Problem (於特定的「群」(group) 尋找元素的「階」(order))，再利用量子傅利葉轉換 (Quantum Fourier Transform) 於多項式時間之內解出

# Grover's Algorithm

- 影響所有對稱式密碼系統，安全參數縮減一半，但不如 RSA/ECC 於多項式時間被破解之威脅劇烈
- 若使用夠長的對稱式密鑰，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
- 原理：給定布林函數，利用量子態疊加 (superposition) 特性，可達成同時平行運算的效果；再經由相位轉換 (phase inversion) 與對平均翻轉 (inversion about mean) 兩操作，改變疊加態中的係數，最後很可能得到答案

# QKD 量子密鑰分配

- 量子密鑰分配 (QKD, Quantum Key Distribution) 利用量子力學特性，使通訊雙方產生並分享隨機的、安全的密鑰，對訊息加密和解密
- 僅用於產生和分配密鑰，不傳輸任何實質訊息；實際運用上，QKD 常與 AES 等對稱式密碼系統一起使用
- 常與量子密碼學 (QC, Quantum Cryptography) 混為一談，因為它是量子密碼學中最著名的例子

# PQC 後量子密碼學

- 後量子密碼學 (PQC, Post-Quantum Cryptography) 又稱抗量子計算密碼學，是現代密碼學的一個研究領域，專門研究能夠抵抗量子電腦攻擊的公鑰密碼系統
- 不同於量子密碼學，後量子密碼學使用現有的電腦與網路，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

1. 資訊安全與密碼學

2. 量子計算對資訊安全的威脅

3. 量子電腦的發展

4. 美國 NIST 制定 PQC 國家標準

5. 美國 NSA 的公開聲明

6. 歐盟網路安全局的研究報告

7. PQC 應用實例

8. 過渡至 PQC 時代



# 質因數分解

- 歷史上首次執行 Shor 演算法於 2001 年
- IBM 的 7-qubit 量子電腦可分解  $15 = 3 \times 5$

## Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor  
AT&T Bell Labs  
Room 2D-149  
600 Mountain Ave.  
Murray Hill, NJ 07974, USA

### Abstract

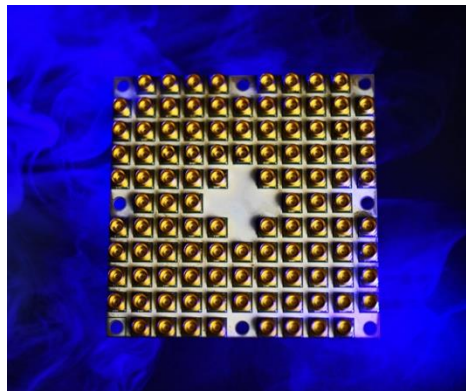
*A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum*

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum com-

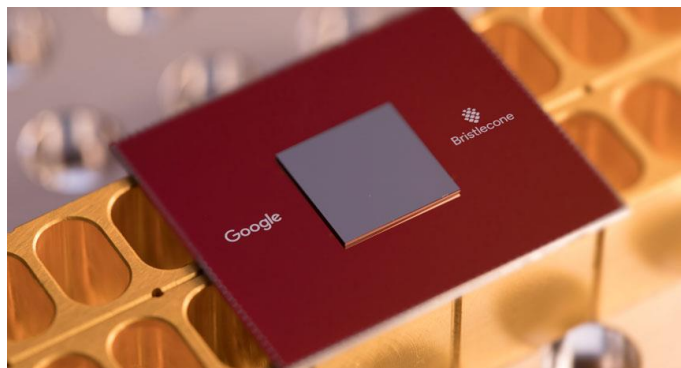


# 近年量子電腦發展加速



IBM's 50-qubit  
quantum computer  
November 2017

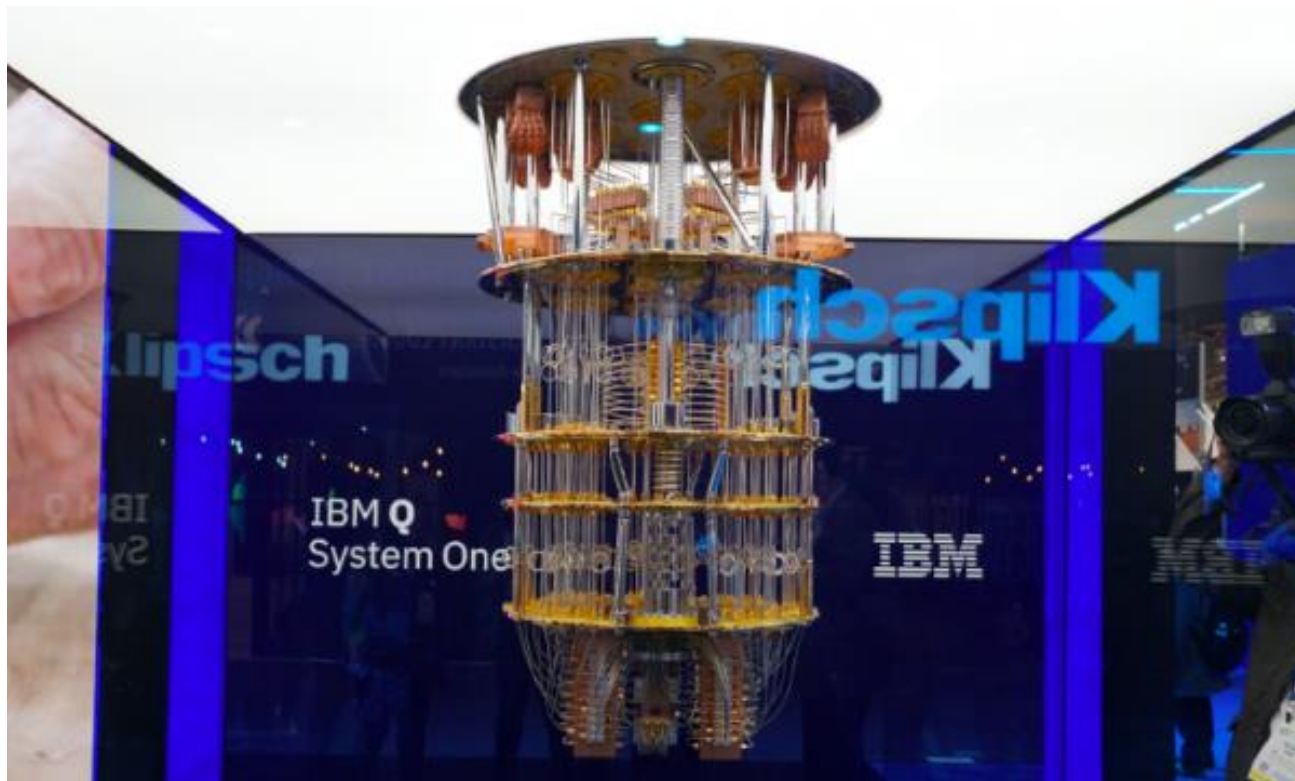
Intel's 49-qubit  
chip "Tangle-Lake"  
January 2018



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

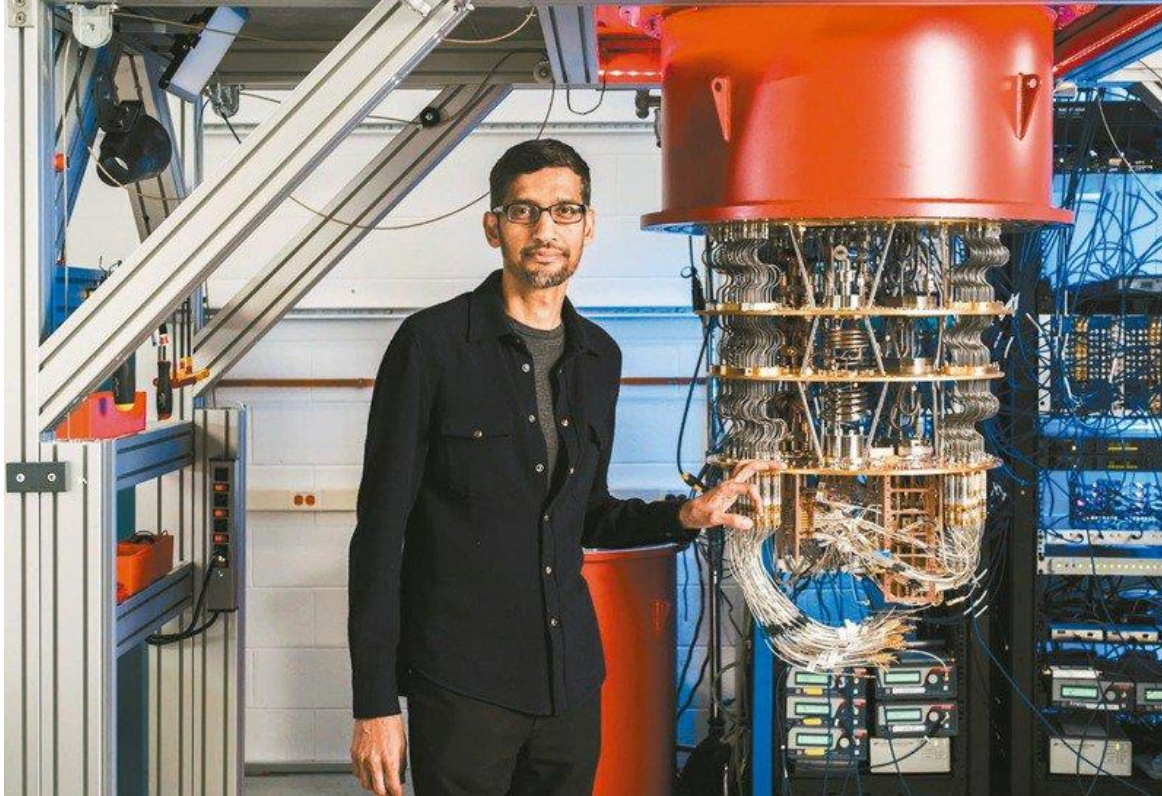


# 全球第一台商用量子電腦



IBM's 53-qubit  
Quantum  
Computer  
October 2019

# Google 宣稱量子霸權 (Supremacy) ?



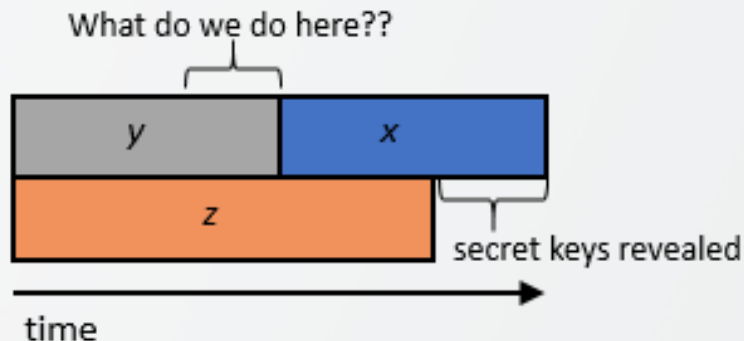
CEO Sundar Pichai with one of Google's quantum computers in the Santa Barbara lab. October 2019

# 未來量子電腦發展預測

- When will a (large-scale) quantum computer be built?
  - **“There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031.”**
  - Dr. Michele Mosca, (April 2015)

# 因應時程

Theorem (Mosca): If  $x + y > z$ , then worry!



- $x$  – time of maintaining data security
- $y$  – time for PQC standardization and adoption
- $z$  – time for quantum computer to be developed



- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

資訊安全與密碼學

量子計算對資訊安全的威脅

量子電腦的發展

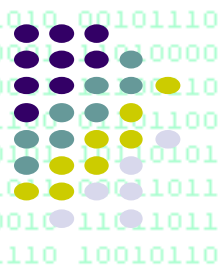
美國 NIST 制定 PQC 國家標準

美國 NSA 的公開聲明

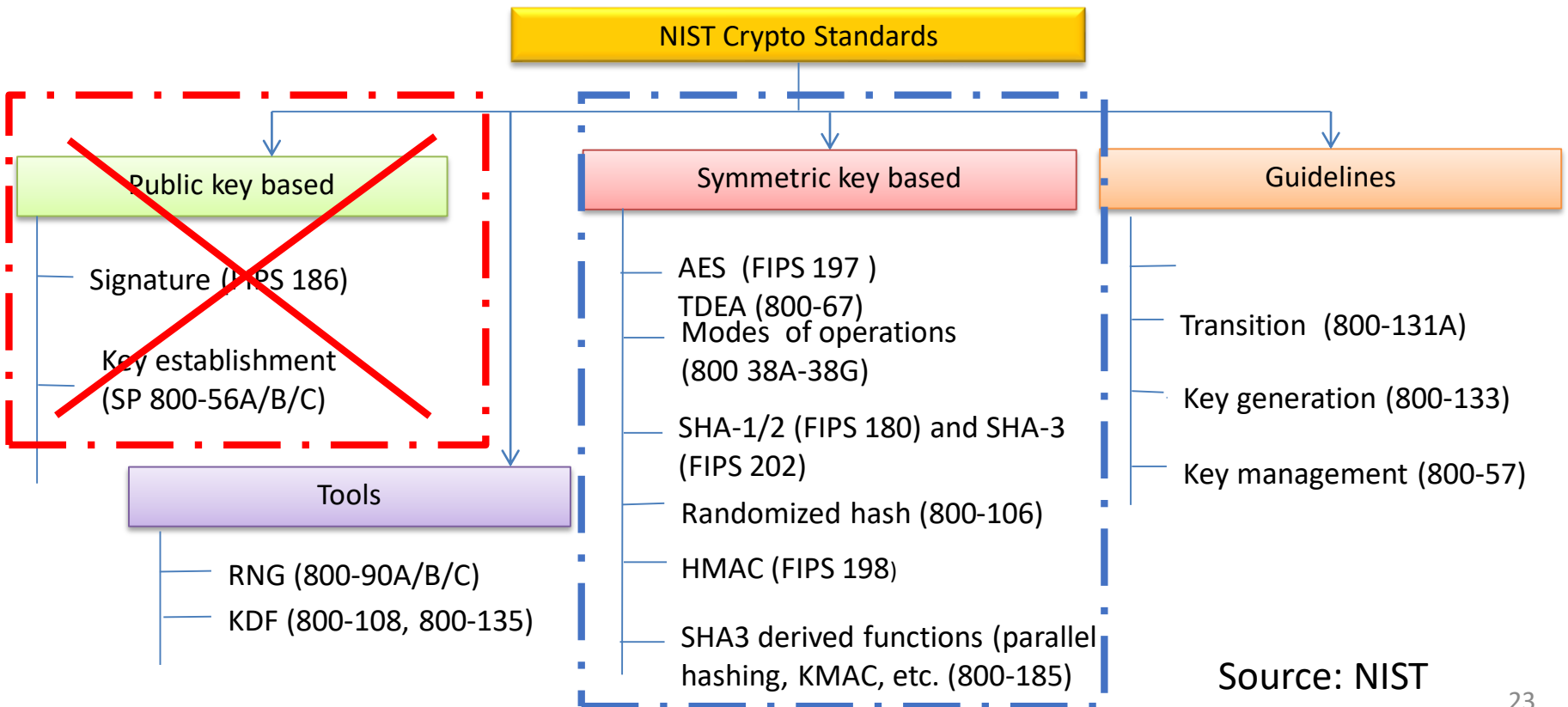
歐盟網路安全局的研究報告

PQC 應用實例

過渡至 PQC 時代



# 量子計算對美國現行國家標準的影響



# NIST PQC Standardization Timeline

- Aug 2016 – Draft submission requirements & evaluation criteria
- Dec 2016 – Final requirements and criteria
- Nov 2017 – Deadline for submissions (69 algorithms)
- Apr 2018 – 1<sup>st</sup> PQC Standardization Conference (Fort Lauderdale, FL)
- Jan 2019 – 2<sup>nd</sup> Round candidates announced (26 algorithms)
- Aug 2019 – 2<sup>nd</sup> PQC Standardization Conference (Santa Barbara, CA)
- **Jul 22, 2020** – 3<sup>rd</sup> Round candidates announced
  - **7 Finalists and 8 Alternates**
- **Jun 7-9, 2021** – 3<sup>rd</sup> PQC Standardization Conference (Virtual)
- 2022-2024 – Draft standards available



# Third PQC Standardization Conference



## REGISTRATION

The NIST Post-Quantum Cryptography Standardization Process has entered the third phase, in which 7 third round finalists and eight alternate candidates are being considered for standardization. NIST plans to hold a third NIST PQC Standardization Conference in June 2021 to discuss various aspects of these candidates, and to obtain valuable feedback for the final selection(s). NIST will invite each submission team of the 15 finalists and alternates to give a short update on their algorithm.

The conference will take place virtually.

### Call for Papers

- Submission deadline: **April 23, 2021**
- Notification date: **May 7, 2021**
- Conference Dates: **June 7-9, 2021**

Conference Inquiries: [pqc2021@nist.gov](mailto:pqc2021@nist.gov)

### **Registration Info**

**Registration Fee:** \$25.00 USD

### REGISTER

The link to attend the meeting will be sent to registered attendees on **June 3, 2021**.

<https://csrc.nist.gov/events/2021/third-pqc-standardization-conference>

# PQC Standardization Process: Third Round Candidate Announcement

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round. The seven third-round Finalists are:

## Third Round Finalists

### Public-Key Encryption/KEMs

Classic McEliece	Code-Based
CRYSTALS-KYBER	Lattice-Based
NTRU	Lattice-Based
SABER	Lattice-Based

### Digital Signatures

CRYSTALS-DILITHIUM	Lattice-Based
FALCON	Lattice-Based
Rainbow	Multivariate

## Alternate Candidates

### Public-Key Encryption/KEMs

BIKE;  
FrodoKEM  
HQC  
NTRU Prime  
SIKE

### Digital Signatures

GeMSS  
Picnic  
SPHINCS+ Hash-Based

NIST intends to select, at most, one Lattice-Based for the standard in each category

# 觀察與預測

- 美國的國家標準總是成為國際標準，全世界通用
- 為分散風險與配合不同應用，NIST 在兩個類別都很可能選擇至少兩個演算法作為國家標準
- 今年底或明年初，NIST 將公佈獲選的演算法
- NIST 或許在兩類別各先選其一，作為國家標準，未來再公佈兩類別的第二選擇
- 數位簽章類別，可能出現「敗部復活」

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

資訊安全與密碼學

量子計算對資訊安全的威脅

量子電腦的發展

美國 NIST 制定 PQC 國家標準

美國 NSA 的公開聲明

歐盟網路安全局的研究報告

PQC 應用實例

過渡至 PQC 時代




# NSA Cybersecurity Perspectives on Quantum Key Distribution and Quantum Cryptography

---

– In response to requests from mission customers, NSA is publicly sharing guidance on quantum key distribution (QKD) and quantum cryptography (QC) as it relates to securing National Security Systems (NSS). Sharing guidance that was previously kept within internal government channels represents one aspect of NSA's efforts to be more transparent in the way that we secure our nation's most sensitive systems and engage with the greater cybersecurity community.

<https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2394053/nsa-cybersecurity-perspectives-on-quantum-key-distribution-and-quantum-cryptogr/>

other system owners, but not for NSS. QKD is a method for using the physics of quantum mechanics to create a shared secret between two parties. While it has great theoretical interest and has been the subject of many widely publicized demonstrations, it suffers from limitations and implementation challenges that make it impractical for use in NSS operational networks. [For more details, please read NSA's QKD and QC guidance.](#) 

NSA considers cryptology based upon mathematical algorithms to be a better alternative for securing National Security Systems against the threat posed by future developments in quantum computing. The National Institute of Standards and Technology (NIST) is in the late stages of creating standards for public use. [For more details, please review NSA's Cybersecurity Perspective on Post-Quantum Cryptography Algorithms.](#) As these families of algorithms continue to evolve, NSA expects to select a single set of NIST standards for use by commercial products within NSS.

NSA Cybersecurity remains committed to supporting efforts to develop, adopt, and deploy secure post-quantum cryptography, which is vital to the defense of our nation.



## Technical limitations

1. **Quantum key distribution is only a partial solution.** QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e. entity source authentication). QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or preplaced keys to provide that authentication. Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better understood risk profile.
2. **Quantum key distribution requires special purpose equipment.** QKD is based on physical properties, and its security derives from unique physical layer communications. This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also lacks flexibility for upgrades or security patches.
3. **Quantum key distribution increases infrastructure costs and insider threat risks.** QKD networks frequently necessitate the use of trusted relays, entailing additional cost for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration.
4. **Securing and validating quantum key distribution is a significant challenge.** The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs. The tolerance for error in cryptographic security, however, is many orders of magnitude smaller than in most physical engineering scenarios making it very difficult to validate. The specific hardware used to perform QKD can introduce vulnerabilities, resulting in several well-publicized attacks on commercial QKD systems.<sup>2</sup>
5. **Quantum key distribution increases the risk of denial of service.** The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD.

## Conclusion

In summary, NSA views quantum-resistant (or post-quantum) cryptography as a more cost effective and easily maintained solution than quantum key distribution. For all of these reasons, NSA does not support the usage of QKD or QC to protect communications in National Security Systems, and does not anticipate certifying or approving any QKD or QC security products for usage by NSS customers unless these limitations are overcome.

過去從未見過「老大哥」NSA如此高度肯定或否定一項技術，公開講得這麼絕、這麼直白 .....



# 美国国家安全局重拳出击 量子通信工程被判出局



徐令予

一吨重的才华也抵不上一克重的勇气

2021.1.4

30 人赞同了该文章

## 美国国家安全局重拳出击 量子通信工程被判出局

当汽车沿着巴尔的摩与华盛顿之间的高速公路行驶，接近马里兰州的米德堡公园时，透过数百米远的森林，隐隐约约可以看到一片“神秘的迷宫”，其规模比中央情报局总部还大。那就是美国国家安全局(National Security Agency，简称为NSA)的总部所在地，又称国家保密局。它是1952年根据杜鲁门总统的一项秘密指令，把敌情捕获、解密的职能部门从当时的军事机构中独立出来，发展成为了美国情报机构的神经中枢。

NSA是全世界雇佣数学博士、计算机博士和语言学家最多的机构，也是美国最神秘的情报机构，“神秘机关初长成，养在深闺人未识。”很多美国人不知道这个重要机构，所以它的缩写NSA又被戏称为“No Such Agency（没有这个局）”。

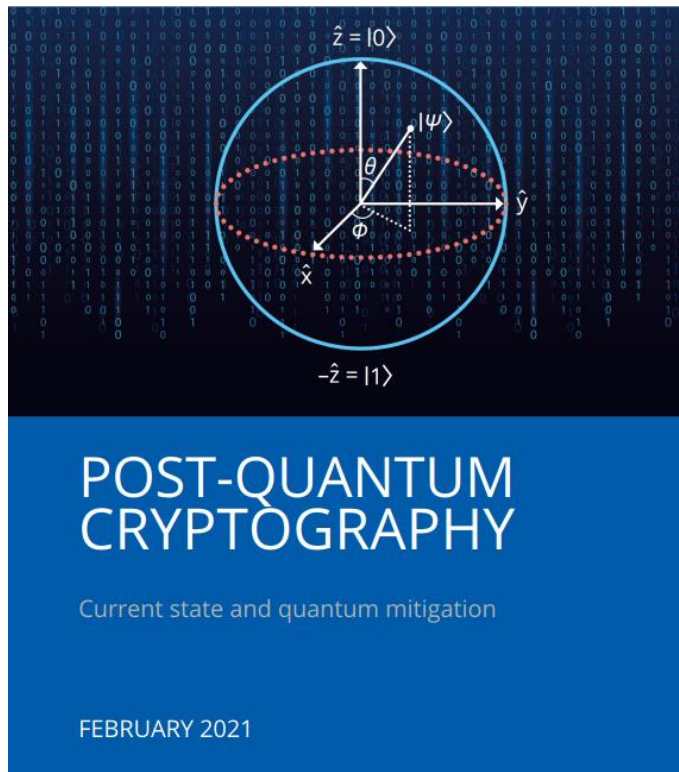
美国国家安全局才是谍中之谍，黑箱中的黑箱，是世界密码学发展的源头和风向标。2020年11月18日，美国国家安全局发表了一篇关于量子密钥分发和量子密码术《Quantum Key Distribution (QKD) and Quantum Cryptography(QC)》的政策报告。这份报告其实判定了量子通信QKD正式下架。

<https://zhuanlan.zhihu.com/p/341521614>

1. 資訊安全與密碼學
2. 量子計算對資訊安全的威脅
3. 量子電腦的發展
4. 美國 NIST 制定 PQC 國家標準
5. 美國 NSA 的公開聲明
6. 歐盟網路安全局的研究報告
7. PQC 應用實例
8. 過渡至 PQC 時代



# CONTENTS



<b>1</b>	<b>Introduction</b>	<b>6</b>
<b>2</b>	<b>Families of Post-Quantum Algorithms</b>	<b>8</b>
2.1	Code-based	8
2.2	Isogeny-based	8
2.3	Hash-based	9
2.4	Lattice-based	9
2.5	Multivariate-system based	10
2.6	The NIST Round 3 Candidates	10
<b>3</b>	<b>NIST Round 3 Finalists</b>	<b>12</b>
3.1	Encryption Schemes	12
3.1.1	Classic McEliece	12
3.1.2	Crystals-Kyber	13
3.1.3	NTRU	14
3.1.4	Saber	15
3.2	Signature Schemes	16
3.2.1	Crystals-Dilithium	16
3.2.2	Falcon	17
3.2.3	Rainbow	18
<b>4</b>	<b>Alternate Candidates</b>	<b>19</b>
4.1	Encryption Schemes	19
4.2	Signature Schemes	20
<b>5</b>	<b>Quantum Mitigation</b>	<b>22</b>
5.1	Hybrid schemes	22
5.2	Protective measures for pre-quantum cryptography	23
<b>6</b>	<b>Conclusions</b>	<b>25</b>
	<b>Bibliography</b>	<b>26</b>



[https://link.zhihu.com/?target=https%3A//www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/at\\_download/fullReport%23page20](https://link.zhihu.com/?target=https%3A//www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/at_download/fullReport%23page20)

# Long-Term Security 長期安全 (第五章)

若資料的保密必須超過十年，且攻擊者有機會接觸並儲存密文，則必須立即採取保護措施。否則，一旦攻擊者可使用大型量子電腦，安全性即受損害。鑑於 NIST 標準制定流程仍將運行幾年，基本上有兩項可行方法解決此問題：

1. 轉移 (migrate) 至組合前量子 (pre-quantum) 和後量子 (post-quantum) 公鑰密碼系統的混合實現 (hybrid implementation)
2. 概念上簡單，但實作複雜，將預共享 (pre-shared) 密鑰混合至藉由 (前量子) 公鑰密碼系統建立的所有密鑰中

The apt reader will have noticed the absence of mention of Quantum Key Distribution (QKD)<sup>1</sup> or of Quantum Cryptography in this text. This has been a deliberate choice. QKD is a quantum technology application that has been available for many years. It provides a guaranteed, by the laws of physics, secure way of distributing and sharing secret keys that are necessary for cryptographic protocols. It essentially offers key agreement services, but not authentication or message confidentiality; for these services we need to rely on math-based cryptography. In other words, QKD can complement a traditional cryptographic system and its setup relies on pre-established authenticated communications channels. However, the existence of such an authenticated channel, presupposes that communicating parties either have managed to privately exchanged a symmetric key in the past (e.g., by physically meeting) or are using public key cryptography. In the former case,

中譯：「聰明讀者會注意到，本文沒有提到量子密鑰分配 (QKD) 或量子密碼學。如此選擇是故意的。……」

後文解釋原因，和 NSA 說法不盡相同，但都否定 QKD。

[https://link.zhihu.com/?target=https%3A//www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/at\\_download/fullReport%23page20](https://link.zhihu.com/?target=https%3A//www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/at_download/fullReport%23page20)

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

資訊安全與密碼學

量子計算對資訊安全的威脅

量子電腦的發展

美國 NIST 制定 PQC 國家標準

美國 NSA 的公開聲明

歐盟網路安全局的研究報告

PQC 應用實例

過渡至 PQC 時代



# Google Security Blog

## Experimenting with Post-Quantum Cryptography

July 7, 2016

Posted by Matt Braithwaite, Software Engineer

Quantum computers are a fundamentally different sort of computer that take advantage of aspects of quantum physics to solve certain sorts of problems dramatically faster than conventional computers can. While they will, no doubt, be of huge benefit in some areas of study, some of the problems that they are effective at solving are the ones that we use to secure digital communications. Specifically, if large quantum computers can be built then they may be able to break the asymmetric cryptographic primitives that are currently used in TLS, the security protocol behind HTTPS.

<https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html>



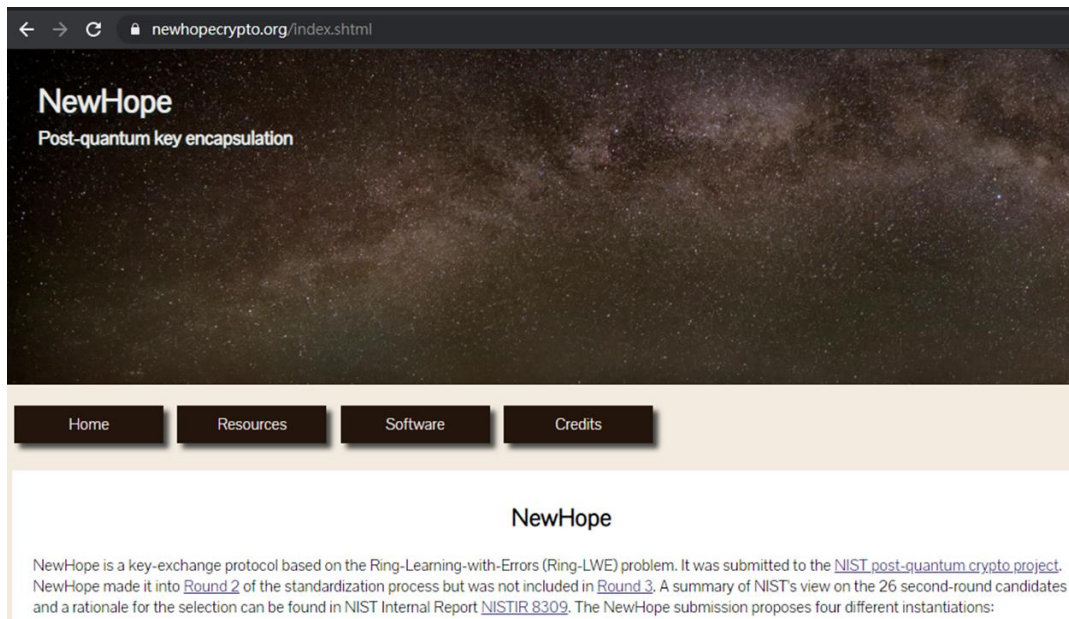
# Ready for tomorrow: Infineon demonstrates first post-quantum cryptography on a contactless security chip

May 30, 2017 | Business & Financial Press

Munich, Germany – 30 May 2017 – Due to their computing power, quantum computers have the disruptive potential to break various currently used encryption algorithms. Infineon Technologies AG (FSE: IFX / OTCQX: IFNNY), the leading provider of security solutions, is ready to provide a smooth transition from today's security protocols to next-generation [post-quantum cryptography](#) (PQC). The company has now successfully demonstrated the first PQC implementation on a commercially available contactless security chip, as used for electronic ID documents. This places Infineon in the pioneering position for encryption that withstands quantum computing power.

<https://www.infineon.com/cms/en/about-infineon/press/pressreleases/2017/INFCCS201705-056.html>



















<https://newhopecrypto.org/index.shtml>

Star Wars: Episode IV - A New Hope (1977)

- Google 瀏覽器和 Infineon 晶片實作的都是 NewHope
- NewHope 進入 NIST PQC 標準制定的第二輪，但未進入第三輪，因為有同類型演算法表現更好
- Google 已完成第二次實驗，採用第三輪決選者 NTRU

# ▲	Name	Price	24h %	7d %	Market Cap ⓘ	Volume(24h) ⓘ	Circulating Supply ⓘ	Last 7 Days
1	 Bitcoin BTC <span>Buy</span>	\$37,800.37	▲ 3.07%	▲ 4.64%	\$708,120,165,823	\$36,335,644,216 960,940 BTC	18,727,093 BTC	
2	 Ethereum ETH <span>Buy</span>	\$2,800.95	▲ 6.23%	▲ 12.54%	\$325,571,321,630	\$30,297,335,515 10,810,002 ETH	116,162,908 ETH	
3	 Binance Coin BNB <span>Buy</span>	\$422.32	▲ 11.84%	▲ 25.71%	\$64,965,772,373	\$4,170,046,980 9,848,607 BNB	153,432,897 BNB	
4	 Tether USDT <span>Buy</span>	\$1.00	▲ 0.09%	▲ 0.07%	\$62,276,083,917	\$76,853,206,334 76,770,735,077 USDT	62,209,255,385 USDT	
5	 Cardano ADA <span>Buy</span>	\$1.78	▲ 7.07%	▲ 18.81%	\$56,787,685,755	\$3,329,942,723 1,873,399,825 ADA	31,948,309,441 ADA	
6	 Dogecoin DOGE	\$0.3893	▲ 6.77%	▲ 25.49%	\$50,637,802,000	\$4,592,410,239 11,780,639,966 DOGE	129,898,176,108 DOGE	
7	 XRP XRP <span>Buy</span>	\$0.9938	▲ 5.27%	▲ 10.93%	\$45,854,756,211	\$3,393,091,791 3,415,013,783 XRP	46,151,013,329 XRP	



# Quantum Resistant Ledger

QRL



Quantum Resistant Ledger Price (QRL)

**\$0.2492**

▲ 4.30%

0.000006618 BTC ▲ 1.77%

0.00008926 ETH ▼ 1.40%

Rank #743

Coin

On 2,919 watchlists

Low: \$0.2241

High: \$0.3145

24h

Website

Explorers

Community

Chat

Source code

Whitepaper

Sponsored

Buy

Exchange

Gaming

Earn Crypto

Tags:

Mineable

PoW

Platform

Distributed Computing

View all

Market Cap

\$18,468,386

▲ 4.31%

Fully Diluted Market Cap

\$26,162,181

▲ 4.30%

Volume 24h

\$60,452

▼ 5.00%

Volume / Market Cap

0.003256

Circulating Supply

74,121,517.01 QRL

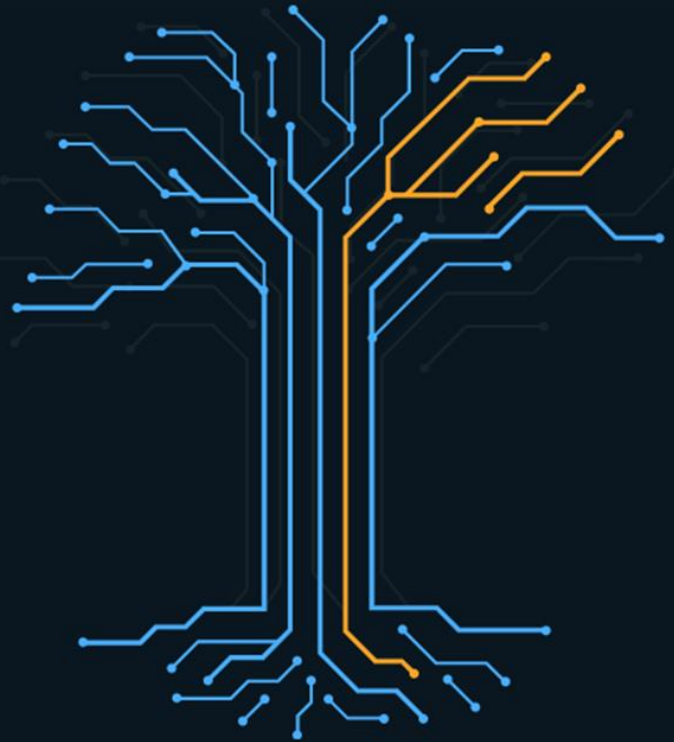
71%

Max Supply

105,000,000

Total Supply

74,121,517



## SECURITY BY DESIGN

A powerful blockchain  
platform secured by XMSS

XMSS is a [NIST-approved](#) post-quantum secure digital signature  
scheme

## Recommendation for Stateful Hash-Based Signature Schemes



Date Published: October 2020

### Author(s)

David Cooper (NIST), Daniel Apon (NIST), Quynh Dang (NIST), Michael Davidson (NIST), Morris Dworkin (NIST), Carl Miller (NIST)

### Abstract

This recommendation specifies two algorithms that can be used to generate a digital signature, both of which are stateful hash-based signature schemes: the Leighton-Micali Signature (LMS) system and the eXtended Merkle Signature Scheme (XMSS), along with their multi-tree variants, the Hierarchical Signature System (HSS) and multi-tree XMSS (XMSS<sup>MT</sup>).

### Keywords

cryptography; digital signatures; hash-based signatures; public-key cryptography

### Control Families

None selected

### DOCUMENTATION

#### Publication:

[SP 800-208 \(DOI\)](#)

[Local Download](#)

#### Supplemental Material:

[Comments received \(pdf\)](#)

#### Document History:

12/11/19: [SP 800-208 \(Draft\)](#)

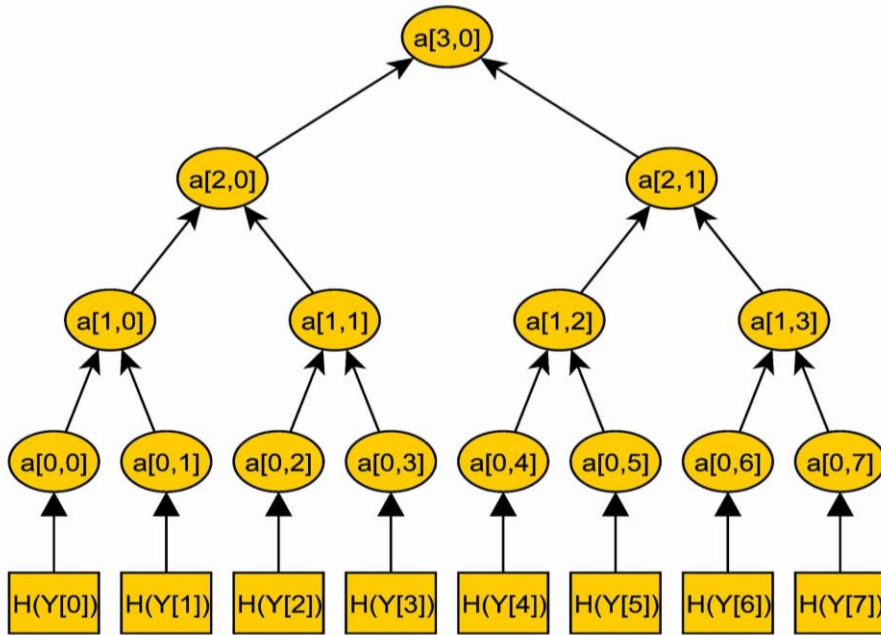
10/29/20: [SP 800-208 \(Final\)](#)

### TOPICS

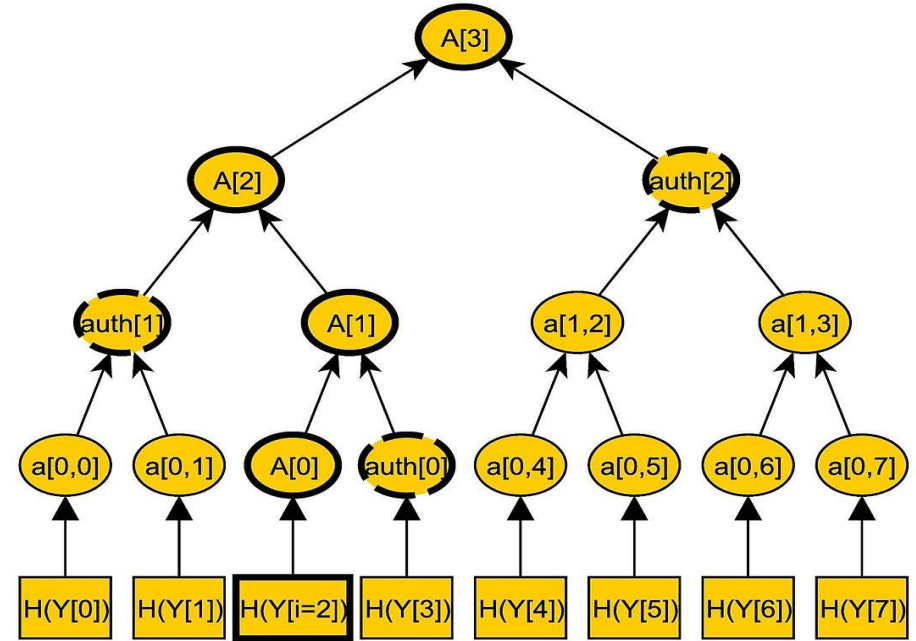
#### Security and Privacy

[digital signatures](#); [key management](#); [secure hashing](#)

# Merkle Tree in Merkle Signature (1979)



<http://commons.wikimedia.org/wiki/File:MerkleTree1.jpg>



<http://commons.wikimedia.org/wiki/File:MerkleTree2.jpg>



# Lattice 晶格

- 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) :

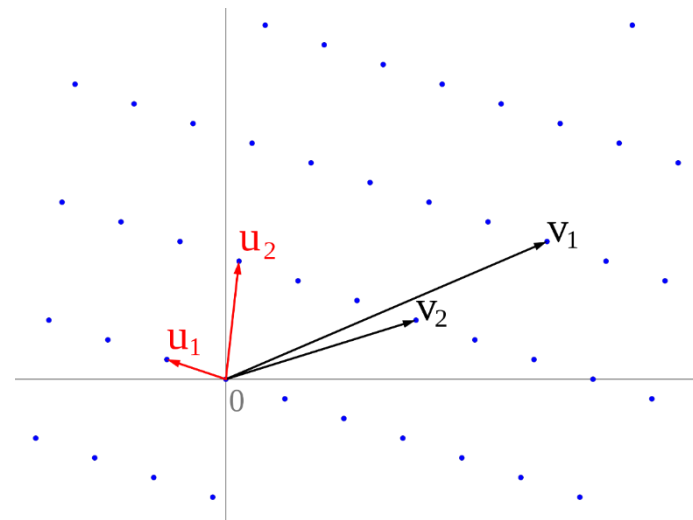
Find a shortest  $x \in \Lambda(B) \setminus \{0\}$

- 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



- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

資訊安全與密碼學

量子計算對資訊安全的威脅

量子電腦的發展

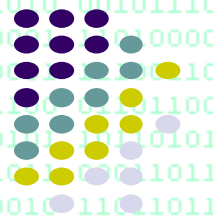
美國 NIST 制定 PQC 國家標準

美國 NSA 的公開聲明

歐盟網路安全局的研究報告

PQC 應用實例

過渡至 PQC 時代







## National Cybersecurity Center of Excellence



Accelerating the deployment and use of  
**secure, standards-based technologies**

### Addressing Visibility Challenges with TLS 1.3

Download the Final  
Project Description



### Migration to Post- Quantum Cryptography

Download the Final  
Project Description >

### How We Can Help You

Watch Our Video >

### Securing Picture Archiving and Communication System

View the Interactive  
Practice Guide >

# Crypto Agility: Considerations for Migrating to Post-Quantum Cryptographic Algorithms

## Building Blocks

5G Security

Adversarial Machine Learning

Applied Cryptography

Data Classification

Data Security

Derived PIV Credentials

Internet of Things

Mobile Device Security



## Download the Final Project Description

The NCCoE has released the final project description, *Migration to Post-Quantum Cryptography*. Use the buttons below to view the publication.

Download the PDF »

Virtual Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms  
Wednesday, October 7, 2020

Workshop Materials

Workshop Recording

## Current Status

National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence CoE has released the final project description, *Migration to Post-Quantum Cryptography*.

[w.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography](http://w.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography)



## White Paper

# Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms



**Date Published:** April 28, 2021

### Author(s)

William Barker (Dakota Consulting), W. Polk (NIST), Murugiah Souppaya (NIST)

### Abstract

Cryptographic technologies are used throughout government and industry to authenticate the source and protect the confidentiality and integrity of information that we communicate and store. The paper describes the impact of quantum computing technology on classical cryptography, particularly on public-key cryptographic systems. This paper also introduces adoption challenges associated with post-quantum cryptography after the standardization process is completed. Planning requirements for migration to post-quantum cryptography are discussed. The paper concludes with NIST's next steps for helping with the migration to post-quantum cryptography.

### DOCUMENTATION


---


#### Publication:

 [White Paper \(DOI\)](#)

#### Supplemental Material:

 [Local Download \(pdf\)](#)

 [NCCoE--Crypto Agility: Considerations for Migrating to Post-Quantum Cryptographic Algorithms \(web\)](#)

 [Post-Quantum Cryptography project \(other\)](#)

#### Document History:

05/26/20: [White Paper \(Draft\)](#)

04/28/21: White Paper (Final)

<https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final>

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

Wednesday, October 7, 2020

## Workshop Overview

The National Institute of Standards and Technology (NIST) hosted a virtual workshop on W workshop was to discuss the challenges and investigate the practical and implementable a of public key cryptographic algorithms to replacement algorithms that are resistant to quar complements the NIST post-quantum cryptography (PQC) standardization activities (<https://www.nccoe.nist.gov/events/virtual-workshop-considerations-migrating-post-quantum-cryptographic-algorithms>).

## Workshop Recording



## Post-Workshop Materials

Slide presentations are linked to the speaker.

<a href="#">Presentation #1</a>	NIST and NCCoE Overview Jeff Greene
<a href="#">Presentation #2</a>	Workshop Overview & Background Curt Barker
<a href="#">Presentation #3</a>	Status of NIST PQC Activity Dustin Moody
<a href="#">Presentation #4</a>	Challenges Session <ul style="list-style-type: none"><li>ETSI Cyber QSC WG, Migration to PQC<ul style="list-style-type: none"><li>Colin Whorlow, <a href="#">NCSC</a></li></ul></li></ul>
<a href="#">Presentation #5</a>	<ul style="list-style-type: none"><li>Integration Challenges<ul style="list-style-type: none"><li>Christian Paquin, <a href="#">Microsoft</a></li></ul></li></ul>
<a href="#">Presentation #6</a>	<ul style="list-style-type: none"><li>Customer Challenges<ul style="list-style-type: none"><li>Yassir Nawaz, <a href="#">JP Morgan Chase</a></li></ul></li></ul>
<a href="#">Presentation #7</a>	<ul style="list-style-type: none"><li>Challenge Overview<ul style="list-style-type: none"><li>Mike Boyle, <a href="#">NSA</a></li></ul></li></ul>

<https://www.nccoe.nist.gov/events/virtual-workshop-considerations-migrating-post-quantum-cryptographic-algorithms>



# QR Implementations and Standards

Mike Boyle  
Center for Cybersecurity Standards  
Cybersecurity Directorate, NSA

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



**CYBERSECURITY**

<https://www.nccoe.nist.gov/file/mike-boylemp4>

# NIST Introduction



- NSA Cybersecurity Directorate
- Center for Cybersecurity Standards
- Cybersecurity Directorate cryptanalysts continue analyzing the PQC candidates. Given the expected widespread usage (both in National Security Systems and by the public) of these algorithms, this is one of our highest priorities
- We find the lattice algorithms to be strong and well-studied
- We are concerned about the inclusion of Rainbow as a Round 3 Finalist as it has not received the same level of cryptanalytic scrutiny as the others, especially given the recent findings against it



# NIST Network Operators



- Start determining where you utilize public key in your network
  - Access Control, Authentication, PIV/CAC cards
  - VPNs, Webservers
- Some examples where you likely aren't using public key
  - Passwords / One Time Passwords
- Legacy Systems that will be around for a long time vs. new systems running your PKI. Easier to update key agreement than authentication.
  - Upgrade Key Agreement -> Most of your communications are secure.
  - Upgrade all but one of your authentication roots of trust -> all your systems are vulnerable.



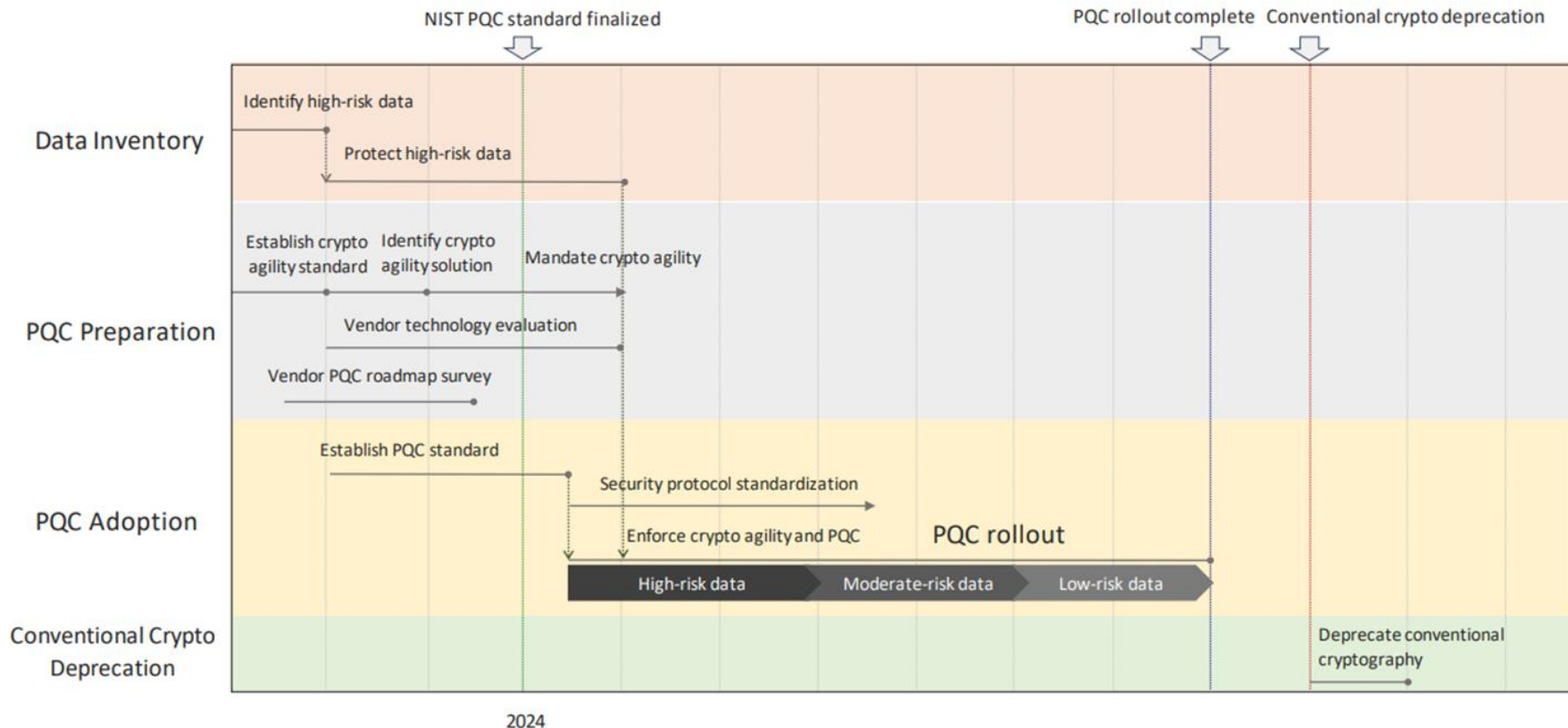
# Post-Quantum Crypto Transition for Global Financial Institutions

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

JPMORGAN CHASE & CO.

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

# Reference PQC Transition Timeline



# Challenges with Crypto Agility

## Crypto Agility Requirements

Crypto User (Application)	Crypto Provider (Solution)
<ol style="list-style-type: none"><li>1. Crypto User (“Application”) should be agnostic to the algorithm (e.g., AES) and configuration (e.g., key length) used in performing crypto operation.</li><li>2. Application should perform cryptographic operation without having to access raw keying material (e.g. master key, data key).</li><li>3. Application code refactoring is permitted for integration with another Solution or to take advantage of a new feature.</li><li>4. Application Owner should ensure Solution in use is supported throughout the application and its data lifecycle/lifespan.</li></ol>	<ol style="list-style-type: none"><li>1. Cryptographic Solution Provider (“Solution”) should provide crypto agnostic API to its client (or Application).</li><li>2. Solution should not provide Application with direct access to raw key material (e.g., data key, master key).</li><li>3. Solution should be committed to supporting future NIST crypto standards and guidelines, including the post-quantum cryptography standard.</li><li>4. Solution should maintain backward compatibility, i.e., a newer Solution version should be able to process ciphertext generated from an older version.</li><li>5. Interoperability with other Solutions is optional, but Solution should provide utilities or APIs to convert its ciphertext to another Solution’s.</li></ol>

# 量子計算威脅的應對之道

- 保持關注量子電腦的最新進展
- 持續追蹤後量子密碼標準制定
- 相關標準及法規與時俱進
- 評估並採用後量子密碼技術與產品
- 轉換至後量子密碼時代

