前瞻科技與管理 9 卷 1/2 期，4-21 頁（2019 年 11 月）
Journal of Advanced Technology and Management Vol. 9, No. 1/2, pp. 4-21 (November, 2019)
DOI:10.6193/JATM.201911_9(1_2).0002

量子計算對當代密碼系統之威脅及對策

劉江龍 *

國防大學理工學院電機電子工程學系教授

摘 要

由於近幾年來量子電腦技術快速的發展，以往基於量子特性所提出的破密演算法有可能在不久的將來得以實現，屆時不管是傳統的對稱式密碼技術或非對稱式密碼技術的安全均會受到威脅，其中尤以基於離散對數計算及質因數分解難題的金鑰分配協定或密碼系統所受的安全威脅最為嚴重。本文之目的即在說明 Grover 演算法及 Shor 演算法對當代密碼技術安全所造成的威脅，並提供對稱式密碼系統面對 Grover 演算法威脅的補強策略；此外，本文同時說明目前世界各國取代傳統金鑰分發技術所採取的量子密鑰分發（Quantum Key Distribution, QKD）技術及後量子密碼學（Post-Quantum Cryptography, PQC）的發展現況；最後針對國內未來在量子計算的威脅下提出相關建議，以供國內網路安全相關單位未來制定相關因應策略之參考。

關鍵詞：Grover 演算法、Shor 演算法、量子計算、量子密鑰分發、後量子密碼學

* 通訊作者：劉江龍
電子郵件：chianglung.liu@gmail.com
（收件日期：2019 年 7 月 17 日；修正日期：2019 年 7 月 25 日；接受日期：2019 年 7 月 25 日）

Journal of Advanced Technology and Management Vol. 9, No. 1/2, pp. 4-21 (November, 2019)
DOI:10.6193/JATM.201911_9(1_2).0002

Treats of Quantum Computing Occurring with Modern Cryptosystems and Possible Strategies to Conquer

Chiang-Lung Liu*

Professor, Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology, National Defense University

Abstract

With rapid development of quantum computing technology in recent years, the cryptanalytic algorithms based on quantum characteristics can be realized in the near future. Therefore, the security of the traditional symmetric or asymmetric cryptography may not be guaranteed as in the past, especially the key-distribution protocols and cryptosystems which are either based on the hard problems of calculating discrete logarithm or factoring. The purpose of this article is to explain how the Grover and Shor algorithms threat the security of the modern cryptography. Meanwhile, the strategy to enhance the security of the symmetric cryptography under the threat of Grover algorithm is also provided. Moreover, the development of the quantum key distribution (QKD) and the post-quantum cryptography (PQC), which will be used to replace the traditional key distribution techniques in the future, is also described. Related suggestions to deal with the threats of the quantum computing are also provided in this article for the references of the network security-related departments to establish the corresponding strategies.

Keywords: Grover algorithm, Shor algorithm, quantum computing, quantum key distribution, post-quantum cryptography

* Corresponding Author: Chiang-Lung Liu
E-mail: chianglung.liu@gmail.com

AECAST Ainosco Press

壹、前言

自從 John von Neumann（1903 ~ 1957）提出馮・諾依曼架構後，大從超級電腦，小至個人隨身手機，可以說都是依循著這個架構所發展而成，其運算架構是以電子訊號作為處理的對象，又稱之為傳統電腦或電子電腦（Electronic Computer）。然而在 1982 年 Richard Feynman 提出運用量子體系進行運算的想法後，引起了另一波電腦科技的革命，因其有別於以往之電子電腦的運作方式，如依量子計算所發展的電腦，則稱為量子電腦（Quantum Computer）。簡單來說，量子電腦是透過量子疊加（Superposition）與量子糾纏（Entanglement）兩項量子特性以進行有別於傳統電腦的運算，可以幫助人類在短時間內完成傳統電腦花上數十年才能解決的問題。

傳統電腦一般又稱為二進制電腦，也就是說，其訊息是以 0 或 1 組合而成，而且相同時間只能由 0 及 1 組合而成一組訊息。對於量子電腦而言，雖然也是使用 0 與 1 作為計量單位（稱為量子位元，Qubit）（Nielsen and Chuang, 2000），可是其是以機率方式存在。也就是說，量子位元在未被偵測前可能存在 0 或 1 之間任何一種狀態，稱之為量子疊加態。假設量子位元是以兩個基底態（或稱本徵態）$|0>$ 及 $|1>$ 表示，其量子態則可以這兩個基底態的線性組合表示，亦即 $|\psi> = \alpha|0> + \beta|1>$，其中 $|\alpha|^2$ 及 $|\beta|^2$ 分別是測得量子位元為 0 或 1 的機率。基於量子疊加的理論，Shor（1994）提出基於量子計算的演算法，巧妙地將分解質因數（Factoring）問題轉換成可透過量子計算的指數週期尋找（Period Finding）問題（Shor, 1997），同樣的技巧也可運用在解離散對數（Discrete Logarithm, DL）上，使得目前基於分解質因數、解 DL 或解橢圓曲線上的 DL（Elliptic Curve on DL, ECDL）等難題的公開金鑰密碼技術的安全面臨嚴重的挑戰，例如：Rivest-Shamir-Adleman（RSA）演算法（Stallings, 2010）、Diffie-Hellman（DH）金鑰交換協定（Diffie and Hellman, 1976）、ElGamal（ElGamal, 1985）、ECDH（Stallings, 2010）等，而這些公開金鑰密碼技術正是目前的網路運作的安全基礎。

雖然量子計算在指數運算上比傳統電腦更有效率，然而這些理論在 1980 年代及 1990 年代受限於科技的瓶頸，都只是在理論階段，甚至於在號稱世界上唯一銷售商用量子電腦的公司 D-Wave 2007 年公開示範其「量子運算系統」後，仍被各界認為只是基於運行量子退火演算法（Quantum Annealing）以解決最優化問題的技巧，不足以運行 Shor 演算法（Kayue, 2015）。直到 2016 年 IBM 公開基於五臺超導量子位元的通用型量子電腦（〈坐在家裏，你也可以體驗 IBM 量子電腦的威力〉，2016）後，包括美國國家安全局（National Security Agency, NSA）等掌管密碼機構才意識到現有的加密演算法的安全性已受到嚴重的威脅，必須趕緊採取因應之道（雷鋒網，2016）。事實證明 NSA 的顧慮不是沒有道理的，因為當量子組態可被更穩定操控後，就像傳統電腦的摩耳定律（Moore's Law）（Bailey, 2018）一樣，具有更多量子位元的量子電腦產生速度是可以預期的。例如：包括 IBM、Intel 及 Google 等電腦界的龍頭在量子電腦的發展上已有長足的進步，IBM 在 2017 年 11 月宣布研發出全世界第一臺 50 量子位元的量子電腦，並在 2019 年的美國消費電子展（Consumer Electronics Show [CES] 2019）發布了 20 個量子位元商用型量子電腦 IBM Q System One，而 Intel 在 CES 2018 也展示了 49 量子位元的測試晶片；另外，Google 量子 Artificial Intelligence（AI）實驗室

（Google Quantum AI Lab）在 2018 年 3 月公布了具備 72 個量子位元的處理器 Bristlecone。面臨量子電腦發展及足以破解公開金鑰密碼技術的演算法，目前密碼技術未來終將面臨安全上的極大威脅。本文之目的即在探討當代密碼技術所面臨的量子計算的威脅，並提出國內未來因應之道。

為說明當代密碼技術的安全問題，第貳章分別說明對稱式（Symmetric）及非對稱式（Asymmetric）密碼技術及其安全之基礎，其中以先進加密標準（Advanced Encryption Standard, AES）（Stallings, 2010）為例，說明對稱式密碼系統之安全基礎；在非對稱式密碼技術方面，則以 DH 及 RSA 為例，分別說明基於 DL 計算及質因數分解難題演算法的安全性。對於對稱式密碼技術，目前最具威脅的量子演算法公認為 Grover 演算法（Grover, 1997），而非對稱式密碼技術部分的威脅則來自 Shor 演算法，本文第參章分別說明其演算法之威脅性及因應之道。其中對稱式密碼技術可藉由加長金鑰位元長度以對抗 Grover 演算法之威脅，然而 RSA、DH 及 ECDH 等非對稱密碼技術則無法利用同樣的方法抵抗 Shor 演算法之威脅。為了建構在量子計算威脅下之安全金鑰分發途徑，目前朝向兩方面發展：量子密鑰分發（Quantum Key Distribution, QKD）及後量子密碼學（Post-Quantum Cryptography, PQC），第肆章及第伍章即分別說明 QKD 及 PQC 技術之發展；最後，本文將針對國內 QKD 及 PQC 提出未來發展的建議。

貳、當代密碼技術安全性解析

1976 年對於傳統密碼技術來說深具意義，這一年美國聯邦政府的國家標準局（Stallings, 2010）制定了資料加密標準（Data Encryption Standard, DES），其成為聯邦資料處理標準（Federal Information Processing Standards, FIPS）。雖然其被懷疑內含 NSA 的後門，可是一直未被證實，倒也相安無事。但由於其使用 56 位金鑰，以現代電腦運算速度來看，實在不足以抵抗暴力攻擊（Brute-Force Attack）。於是美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST，前美國國家標準局）在 1999 年版的標準（FIPS-46-3）中，則使用三次 DES 加密（稱為 3DES）取代單一次的 DES 加密方案。一方面提高其對暴力攻擊的抵抗能力，一方面則讓其在解密時可以與以往使用一次 DES 加密相容，預計 2030 年全面停止使用 DES。在使用 3DES 的同時，NIST 同時積極徵求新的 DES，並於 2001 公布使 Rijndael 加密演算法作為 AES。其共有三種長度的金鑰可供選擇，分別為 128 位元、192 位元及 256 位元等，相對於使用 56 位元的 DES 而言，不論是那一種金鑰長度，對暴力攻擊的抵抗能力均大幅提升。

除了對稱式密碼技術標準制定外，1976 年也是非對稱式密碼技術的紀元。對稱式密碼系統之所以稱為對稱式，是因為加解密雙方使用同一金鑰進行資料加解密。而如何使加解密雙方可以在網路上秘密進行金鑰的約定及更新，一直是管理人員頭痛的問題，又稱為金鑰管理問題。這個問題隨著 Diffie 與 Hellman（1976）提出的公開金鑰交換協定（簡稱 DH）才得以舒緩；另外，三位麻省理工學院的教授 Rivest、Shamir 與 Adleman（1978）則在隔年提出了赫赫有名的 RSA 密碼系統，這兩種方法的執行程相當簡潔，但卻是基於不同計算難題的安全。

由於非對稱式密碼技術之運算大部分為指數運算，如果對相同的資料進行加解密，其花費的運算時間約為單純使用邏輯運算的對稱式密碼系統的 1,000 倍。因此，如果用其進行大量資料的加解密，則不符合實際應用的效益。例如：在無線網路上使用非對稱式密碼系統進行大圖檔資料的傳輸，終將因耗時過久而形成效率的瓶頸。因此，目前大部分網路運作是採用對稱式及非對稱式密碼技術的混合作法，也就是先利用非對稱式密碼技術進行身分驗證及協議出一把臨時的對稱式金鑰，並利用這把臨時金鑰進行對稱式資料加解密。由於在混合式作法中，非對稱式金鑰加解密的對象只是數百位元的金鑰而已，而真正大資料的加解密還是使用對稱金鑰加密系統，不但可以解決金鑰管理問題，也同時避免了效率不彰的問題。另外，橢圓曲線密碼系統（Elliptic Curve Cryptosystem, ECC）在同樣安全的基礎上，具有比其他非對稱式密碼系統計算上的優勢，獲得學者在研究上的青睞，而 DH 金鑰交換協定可成功轉換到橢圓曲線領域（稱為 ECDH），以節省計算上的成本。以下各節將分別從傳統電腦計算能力的角度，針對對稱式密碼技術（AES）及非對稱式密碼技術（DH 及 RSA）進行安全性分析，以作為後續探討其面對量子演算法威脅之基礎。

一、對稱式密碼技術（AES）安全性分析

如同前述，AES 屬於對稱式密碼系統，亦即加解密雙方使用同一把金鑰進行資料的加解密。AES 屬於區塊加密法（Block Cipher），是將欲加密的原始文件區分為 128 位元（16 bytes）大小區塊的明文（Plaintext），並分別對不同區塊進行加密，分別得到 128 位元密文（Ciphertext）。AES 的加解密架構如圖 1 所示（Stallings, 2010），其屬於替代—排列架構（Substitution-Permutation Network, S-P Network），使用多回合（Round）簡單的替代及排列以達到混淆（Confusion）及擴散（Diffusion）的效果。AES 支援 128 位元、192 位元及 256 位元長度的金鑰，分別對應 10、12 及 14 回合等三種不同回合數的設計，而這把金鑰稱為主金鑰（Master Key），並透過金鑰生成程序（Key Scheduling）產生不同回合的子金鑰。以圖 1 的 128 位元主金鑰 Key 為例，其會生成 11 把子金鑰，分別為 w[0, 3]、w[4, 7]、……、w[40, 43] 等 4 × 4 位元組（128 位元），以供後續各回合之加解密使用。在加密部分，AES 的每回合均由 Substitute Bytes、Shift Rows、Mix Columns 及 Add Round Key 等四步驟組合（最後一個回合沒有 Mix Columns），其中各回合之 Add Round Key 步驟即是與上述相對之子金鑰進行混合運算；而在解密部分則透過反向運算，即可將密文解回原始明文。值得一提的是，AES 的 Substitute Bytes 是在葛洛依斯場（Galois Field）GF(2^8) 運作，具有非線性的替換特性，其運算過程亦可使用替換表取代，因此，除了安全性可清楚的受到檢驗外，並具有良好軟、硬體實作之特性。

對稱式密碼技術的安全檢驗可從其對兩大攻擊的抵抗程度著手，這兩大攻擊的方式分別為統計式攻擊（Cryptanalytic Attack）及暴力式攻擊。在 AES 發展之前，已有相當多的區塊加密演算法被提出來，而統計式攻擊的目的即在發現這些演算法中的弱點，並企圖透過其弱點推導出其使用之金鑰，其中最著名的攻擊應屬差分密碼分析（Differential Cryptanalysis）（Biham and Shamir, 1993）及線性密碼分析（Linear Cryptanalysis）（Matsui, 1994）。AES 的設計要求之一就是要能抵抗當時（西元 2000 年）已知對 DES 具有威脅性的統計式分析，

顯然 Rijndael 加密演算法在 AES 的評選階段已通過統計式分析的評估，而暴力攻擊則是 AES 必須考慮的關鍵。

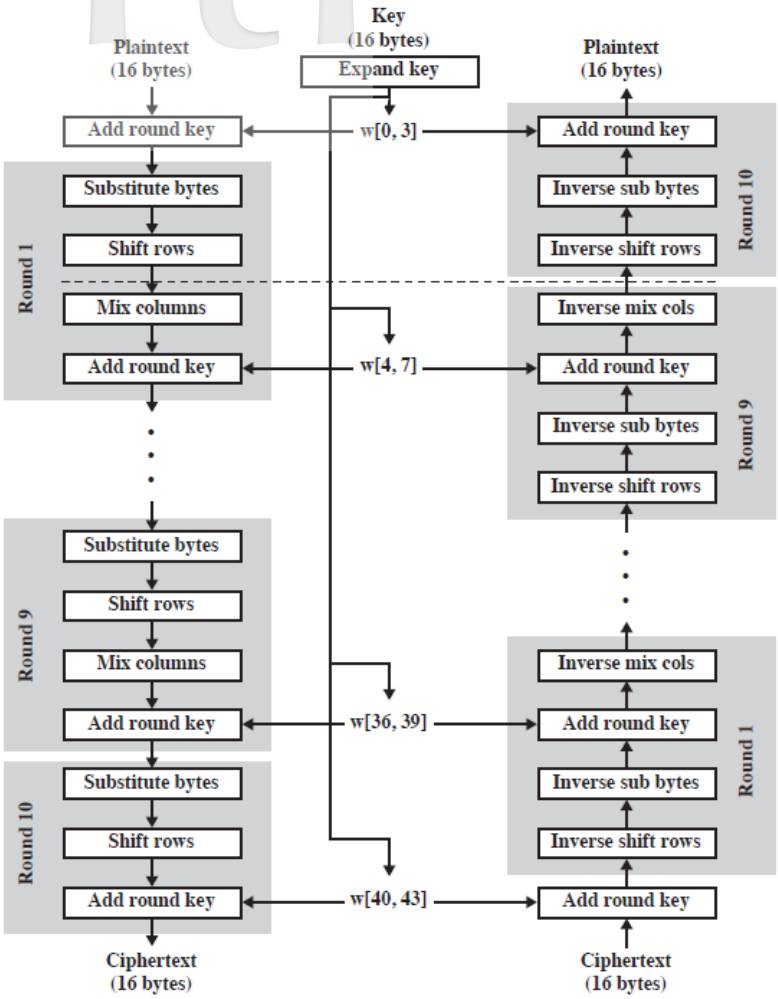

圖 1　AES-128 加解密架構

資料來源：Stallings（2010）。

暴力攻擊又稱為窮舉式搜尋（Exhaustive Search），就是窮舉所有可能的金鑰對特定密文進行解密。如果在解密過程中發現解密的結果產生具有意義的文字，則表示破密成功。假設某一加密技術所使用的可能金鑰總數是 N，若使用暴力攻擊法，平均嘗試 $N/2$ 金鑰後，有很大的機率可以找到正確的金鑰。因此，當金鑰的可能組合數目越大，則被破解的機率越小。這樣的攻擊法是所有的密碼系統都必須進行安全評估，並非只針對對稱式密碼系統。以使用 128 位元長度金鑰的 AES 為例，其所有可能的金鑰數目是 2^{128}（約等於 3.4×10^{38}）。如果以每秒可以窮舉 10^{12} 把金鑰計算能力的電腦進行破密運算，共需要 5.4×10^{18} 年的時間才能窮舉 2^{127} 金鑰，屆時這把被破解的金鑰已喪失其價值，以這樣加大金鑰空間來達到抵抗暴力攻擊的方式則稱之為計算上的安全（Computational Security）。依據上述的探討，如果僅以暴

力攻擊法進行對稱式密碼技術的安全性評估，從傳統電腦的計算能力來看，128 位元金鑰長度的 AES 是足夠的。

二、非對稱密碼技術安全性分析

（一）DH 金鑰交換協定安全性分析

DH 金鑰交換協定是美國密碼學家 Diffie 與 Hellman（1976）所提出，其目的是使用通訊雙方持有的私鑰（Private Key）建立起一把臨時通訊使用的對稱式金鑰，其進行步驟如下。

1. 假設通訊雙方（Alice 及 Bob）認同一個大質數 p 及原根 g，此為系統之公開參數。
2. Alice 使用其私鑰 a，計算 $A \equiv ga \bmod p$，並透過網路傳送給 Bob，其中「≡」表示同餘的意思。
3. Bob 使用其私鑰 b，計算 $B \equiv gb \bmod p$，並透過網路傳送給 Alice。
4. Alice 使用其私鑰 a 及 B，計算 $k \equiv Ba \bmod p$，得出 $k \equiv g\,ab \bmod p$。
5. Bob 使用其私鑰 b，計算 $k \equiv Ab \bmod p$，得出 $k \equiv g\,ab \bmod p$。

在上述步驟 4 及步驟 5 中，Alice 及 Bob 均可由自己的私鑰（a 及 b）及對方寄來的公開資訊（B 及 A），計算出共同的金鑰 k，並利用這把共同金鑰對後續通訊內容進行對稱式加密（例如：AES）。

在此系統中，假設大眾均可得到大質數 p 及原根 g，另外可從網路上得到上述步驟 2 及步驟 3 所計算得到的 A 及 B，因此可透過計算 $A \equiv ga \bmod p$ 或 $B \equiv gb \bmod p$ 以求解 a 及 b，此稱為解 DL 問題。如果 p 是一個超過 300 位整數的大質數，而且 a 和 b 均為超過 100 位的整數，以傳統最好的演算法解 DL 問題，將無法在合理時間內計算出 a 或 b，此為 DH 金鑰交換協定的安全基礎。換句話說，如果有一個演算法可以快速解決 DL 問題，則可在有效的時間內破解 k，則 DH 金鑰交換協定的安全性即不再存在。ElGamal（1985）所提出 ElGamal 公開金鑰加密演法即參考 DH 金鑰交換協定所制定，同樣繼承瞭解 DL 的安全性，在本文中不再贅述，有興趣的讀者可以參考文獻。

（二）RSA 加密演算法安全性分析

除瞭解 DL 問題被作為密碼系統安全的基礎外，另有一支公開金鑰密碼系統（Public-Key Cryptosystem）是以分解因數問題作為其演算法安全之基礎，其中最有名的是由三位麻省理工學院教授 Rivest et al.（1978）所提出的 RSA 加密演算法。

RSA 加密演算法是公開金鑰密碼系統，系統中的個人必須先產生一把公鑰（Public Key）及私鑰。假設系統中通訊雙方仍為 Alice 及 Bob，Alice 可使用以下的程序以產生其公鑰及私鑰。

1. 任意選擇兩個不同的大質數 p 及 q，並計算其乘積 $N = pq$。
2. 計算 $r = (p-1)(q-1)$。
3. 挑選小於 r 且與 r 互質的整數 e，並計算其模 r 的乘法反元素 d，亦即 $ed \equiv 1 \bmod r$。

4. 將 p 及 q 銷毀，公鑰（e, N）傳給 Bob，並將私鑰（d, N）存放在安全的地方。

Bob 獲得 Alice 的公鑰後，如果他想送訊息 m 給 Alice，可依下列步驟進行訊息加密及傳送。

1. 依照與 Alice 約定的格式，將 m 轉換為一個小於 N 的非負整數 n。
2. 計算密文 $c \equiv ne \bmod N$。
3. 將密文 c 直接在公開的網路上寄給 Alice。

當 Alice 獲得 Bob 的訊息後，可依下列步驟進行解密。

1. 計算明文 $n \equiv cd \bmod N$。
2. 將 n 依約定的格式轉回訊息 m。

上述解密步驟 1 可以用數學方法證明訊息 n 的確可以正確的還原，由於這不是本文的重點，有興趣的讀者可參考文獻（Stallings, 2010）。

由於 RSA 加密與解密的方式相當簡潔，因此受到廣大的使用。另外，RSA 如果反方向運用，還可以用來當作數位簽章（Digital Signature），亦即以私鑰加密（簽章），用公鑰解密（簽章驗證）。破密者若想從公開的資訊 c、e 及 N 以求得 d，必須求解 $ed \equiv 1 \bmod r$。由於 $r = (p - 1)(q - 1)$，其必須去分解 N，以求得 p 及 q。假設 p 及 q 均 300 位整數，以目前最好的演算法，破密者無法在合理的時間內從 N 分解出 p 及 q，這就是 RSA 所賴以安全的質因數分解難題。換句話說，如果有一個演算法可以快速解決大質數因數分解的難題，則可在有效的時間內從 N 分解出 p 及 q，則 RSA 的安全性即不再存在。

參、量子演算法的威脅及對策

雖然量子電腦可以藉由量子位元的疊加態特性以加速運算，但對於特定問題，必須設計相對量子演算法以達成量子加速運算的目的，而 Grover 演算法及 Shor 演算法就是分別針對破解對稱式密碼技術及非對稱式密碼技術所提出的量子演算法，本文將分別說明 Grover 演算法及 Shor 演算法的運作方式及其對對稱式密碼技術及非對稱式密碼技術所產生之威脅。

一、Grover 演算之威脅及對策

Grover 演算法適用的對象為所有的對稱式密碼系統。簡單來說，如果我們要從 N 個房間內找尋一件物品，以傳統的作法，只能一間間房間開門進去看，直到找到我們想要的物品。平均來說，如果打開 $N/2$ 間房間後，有很大的機率可以找到那件物品，我們稱這種方法的時間複雜度為 $O(N)$，而 Grover 演算法則是利用量子特性，把搜尋方法的時間複雜度降至 $O\left(\sqrt{N}\right)$。

Grover 演算法的原理是藉由量子態疊加的特性，同時對某一個布林函數 $f(x)$ 進行平行運算；接著再經由相位轉換（Phase Inversion）及對平均翻轉（Inversion about Mean）操作來改變疊加態當中的係數，而經過這樣的操作後，最後會有很高的機率可以得出正確答案。

如果我們擁有一組明文—密文對，則可運用 Grover 演算法進行對稱式密碼技術的破解。可定義 x 為密鑰，$f(x)$ 為明文—密文對的比對函數，若比對成功，則 $f(x)$ 輸出 1；若比對不成功，則 $f(x)$ 輸出 0。其後再將 $f(x)$ 經由 Grover 演算法，即可求得正確答案。由於 Grover 演算法中與量子計算相關理論的推導因非本文之重點，有興趣的讀者可以參考文獻（Grover, 1997）。

目前最好的傳統搜尋演算法的時間複雜度為 $O(N)$，而 Grover 演算法則可達成平方倍的加速效果。換句話說，若密鑰全部的可能數量為 N，Grover 演算法只需要的計算時間便可有很大的機率找到正確的金鑰。因此，如果有一天量子電腦發展成功，在 Grover 演算法的威脅下，現有的對稱式密碼技術必須把金鑰的位元數加長一倍，以達到同樣的安全性。以使用 128 位元金鑰的 AES（AES-128）為例，未來必須使用 256 位元的金鑰（亦即 AES-256），才能達到同樣的安全性。

二、Shor 演算法之威脅及對策

嚴格來說，Shor 演算法主要是針對分解因數而設計，目的在破解 RSA 密碼系統。Shor 演算法包含傳統計算程序及量子計算程序兩部分。傳統計算程序是將質因數分解問題轉換成指數週期尋找問題以分解質因數，而指數週期尋找正是利用量子特性的快速計算程序。簡單來說，我們可以設計一量子傅立葉轉換（Quantum Fourier Transform）電路（Beauregard, 2003），然後透過反覆操作反量子傅利葉轉換，就可以得到特定量子的相位，此稱為相位估測（Phase Estimation），再巧妙地設計具有特徵向量 $|\phi\rangle$ 的么正（Unitary）矩陣 U，就可以得到 $ax \equiv 1 \bmod N$ 的解 x，其中與量子計算相關理論的推導因非本文之重點，有興趣的讀者可以參考文獻（Shor, 1994）。

結合指數週期尋找的量子程序，Shor 演算法可以描述為以下步驟。

1. 在 2 至 $N-1$ 的範圍內隨機選取一個整數 a。
2. 計算 $gcd(a, N)$。若不為 1，則輸出 $gcd(a, N)$，分解成功。
3. 利用量子部分計算 $ax \equiv 1 \bmod N$ 的解。若 x 為奇數，則回到步驟 1。
4. 計算 $gcd(ax/2 + 1, N)$。若僅得到 1 或 N，則回到步驟 1；否則，輸出 $gcd(ax/2 + 1, N)$，分解成功。

依據 Shor 演算法，若欲破解的大小約為 n 個位元的私鑰，則 Shor 演算法的計算時間為 $O(n3 \log n)$。換句話說，Shor 演算法可在有效時間內完成大質數的因數分解，即使 RSA 使用兩個約 1,024 個位元的大質數乘積，也會很快被具備足夠量子位元的量子電腦破解。Shor 演算法同樣可仿照破解 RSA 的作法進行 DH 及 ECDH 的破解，其作法是將 DL 問題、ECDL 問題轉化為 Order Finding 問題，再利用量子傅利葉轉換於多項式時間內解決 Order Finding 問題。

上述表示，如果具備足夠量子位元的量子電腦發展成功，目前在網路上使用的金鑰交換系統將面臨嚴重威脅，因此必須要有替代方案以進行金鑰交換。目前金鑰交換的替代方案朝向兩方向發展，一為使用量子計算特性的 QKD 技術，一為使用傳統計算方式的 PQC，下二章將分別介紹這兩種技術目前的發展及應用的趨勢。

肆、QKD 技術之發展

目前網路通訊所使用的訊息加密金鑰，一般是使用公開金鑰密碼技術所協議出來的一次性密鑰（One-Time Pad）。當此次連線結束後，此密鑰也跟著失效，如此可確保當密鑰在未來某個時間點被破解時，不會影響之前及之後通訊內容之安全。可是當公開金鑰密碼技術有問題時，表示破密者可以很輕易破解網路上的任一次通訊密鑰，如此網路的通訊就不再安全了。同樣的，未來有一天，當 Shor 演算法開始在量子電腦上運行時，基於 DL 及質因數分解難題的公開金鑰密碼技術就不能像現在一樣保障網路通訊的安全了。QKD 技術則是基於量子力學特性所發展的密鑰交換技術，其可在通訊開始之初藉由「資訊協調」（Information Reconciliation）和「隱私增強」（Privacy Amplification）等技巧，使通訊雙方擁有一把共同密鑰，而且無論攻擊者擁有多少資訊，均無法破解這把密鑰。以下各節將介紹 QKD 的運作方式及在世界各國發展的狀況。

一、QKD 運作原理與程序

QKD 已發展出許多協定及其變形，但基本的運作方式大致相同。其是假設通訊雙方擁有一組可驗證身分的傳統通道（例如：公開的網路），以及一條可以傳送量子態的量子通道。QKD 協定運作方式如下：協定開始時，通訊雙方先經由量子通道傳送一連串的量子資訊，接著再經由傳統通道比對及修正資訊，藉以獲得一把共同密鑰。假設在協定運行期間，攻擊者可竊聽傳統通道上的所有訊息及使用任何方式竊聽量子通道，但由於量子力學的「資訊獲得必然造成干擾」與「不可複製原理」（No-Cloning Theorem）特性，可確保通訊期間通訊雙方發現量子通道上的任何竊聽及干擾。另外，通訊雙方可使用「資訊協調」與「隱私增強」手段，確保在干擾程度低於一定的門檻值下，可協議出一把共同密鑰。以下舉目前最簡單且效率高的 BB84 協定說明 QKD 的運作方式。

BB84 是由兩位物理學家 Brassard 與 Bennett（1984）所提出的協定，為最早提出利用量子力學特性進行密鑰傳輸的協定，其使用光子作為量子態的載體。BB84 假設通訊雙方（Alice 與 Bob）透過公開的網路進行身分驗證，並透過光纖進行光子的量子態傳送。假設 Alice 為送方，其在光纖上有兩種頻道可供選擇，分別為⊕及⊗。當 Alice 選擇頻道⊕時，可以發送兩種偏振態的光子，其中 0 度偏振態的光子代表位元 1，90 度偏振態的光子代表位元 0；當 Alice 選擇頻道⊗時，同樣可以發送兩種偏振態的光子，其中 45 度偏振態的光子代表位元 1，135 度偏振態的光子代表位元 0。在接收方，Bob 可以選擇兩種頻道進行測量。當 Bob 使用⊕頻道來測量時，只會得到 0 度或是 90 度偏振態的光子；當 Bob 使用⊗頻道時，只會得到 45 度或 135 度偏振態的光子。由於量子的特性，當 Bob 使用與送方相同的頻道測量時，一定可以得到正確的資訊；但若他使用錯誤的頻道測量時，便有一半的機會得到錯誤的資訊。由於 Alice 都可以任意選擇兩種頻道來傳輸光子，所以 Bob 每次接收到光子時，只能猜 Alice 是使用哪一種頻道。當 Bob 全部接收完光子後，會把自己對每一顆光子選用的頻道放上公開的網路上；而當 Alice 看到後，則透過公開的網路告訴 Bob 錯誤選用的頻道，接著雙方同時把錯誤的結果拋棄，僅留下正確結果的部分。

在上述的光子傳輸過程中，如果遭到攻擊者攔截，光子會有一半的機會改變其原本的偏振態角度。由於此時攻擊者並不知道 Alice 使用何種頻道，只能如同 Bob 一般，在⊕及⊗兩種頻道中進行選擇。若是攻擊者使用了正確的頻道進行測量，光子就會保持原本的樣子；若是攻擊者使用了錯誤的頻道，光子的偏振態就會發生變化，例如：使用⊕頻道測量 45 度偏振態的光子，光子的偏振態就會變成 0 度或是 90 度。為了驗證光子在傳輸時沒有被攻擊者竊聽，Alice 和 Bob 只要從先前確定的正確頻道中選擇幾個位元的測量結果放上公開的網路比對即可。若是比對結果完全相同，表示其被攻擊者竊聽的機率很低；若是比對結果的相異值超過一定的門檻值，則可合理懷疑其被攻擊者竊聽。此時，Alice 和 Bob 可決定放棄這次協定，另重新運作協定的過程。另外，若是比對結果雖然有差異，可是在可容忍的門檻值以下，則可利用「資訊協調」及「隱私增強」來建立共同的密鑰。

根據以上對 QKD 原理及過程的描述，QKD 可綜整為以下程序。

1. Alice 送出 4 種偏振態的光子。
2. Bob 隨機在 2 種頻道中選擇一種頻道進行測量，並記錄選用的頻道與測量結果。
3. Bob 在網路上公布其測量各光子所使用頻道的狀況。
4. Alice 通知 Bob 哪些頻道是錯誤的。
5. Alice 及 Bob 同時拋棄錯誤頻道的光子，僅留下正確頻道的光子。
6. Alice 及 Bob 從正確頻道的光子中，選擇部分光子在公開的網路上進行位元值比對。若比對錯誤率超過預設的門檻值，則放棄此次協商的密鑰，回到步驟 1，重啟另一次 QKD；若是錯誤率在容忍範圍內，則利用「資訊協調」及「隱私增強」來建立共同的密鑰。

二、國際 QKD 技術之發展

面對未來成熟量子電腦的到來，一個成熟而且可在量子計算威脅下提供密鑰協商的安全技術已刻不容緩，而 QKD 技術正是這樣的一個技術。目前許多國家的政府或民間公司已投入相關產品的開發，而包括美國、中國大陸、歐洲、日本、澳洲也都已建立 QKD 通訊網路。

美國早在西元 2000 年就已啟動建立 QKD 網路，是最早建立 QKD 網路的國家。其是由國防高等研究計畫署（Defense Advanced Research Projects Agency, DARPA）與 BBN 科技公司合作，在哈佛大學、波士頓大學、BBN 科技公司等三個節點之間建立世界上第一個 QKD 網路（Elliott, Colvin, Pearson, Pikalo, Schlafer, and Yeh, 2005），如圖 2 所示，並於 2005 年完成建立，全長 10 公里。在民間產業方面，美國的 MagiQ 公司有一款 QKD 產品（QPN 8505），其主要銷售對象為美國軍方及政府單位，並受到美國高科技出口政策限制。

基於量子密碼的安全通訊計畫（Secure Communication based on Quantum Cryptography, SECOQC）（Alléaume, 2007）是歐洲發展的大型 QKD 網路計畫，從 2004 年執行到 2008 年，參與者計歐盟、瑞士與俄羅斯等。SECOQC 共規劃連接 41 個政府與學術單位，並於 2008 年 10 月 6 日，由奧地利西門子公司（SIEMENS）負責，將八條 QKD 連線整合在量子骨幹上，於奧地利維也納完成第一次 QKD 密鑰傳輸，並進行視訊會議展示。歐洲的民間 QKD 產業在銷售上較沒有美國那麼多限制，瑞士 ID Quantique 的 QKD 產品 Clavis 於 2004 年首度進

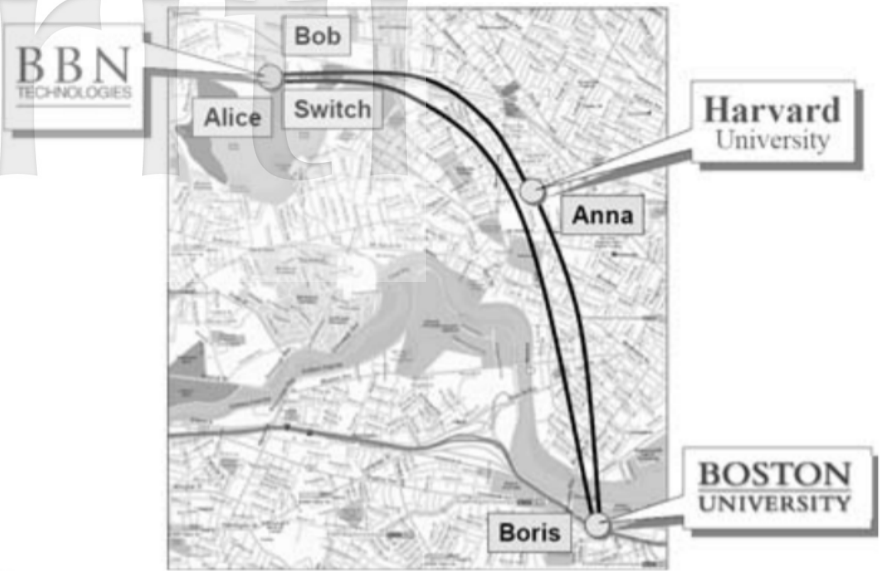

圖 2　由 DARPA 與 BBN 科技公司合作建立的 QKD 網路示意圖

資料來源：Elliott et al.（2005）。

行商業銷售，而該公司最新的 QKD 系統 Clavis 3 的密鑰傳輸效率則可在 50 公里的距離內，可達到超過每秒 3 kbits 的傳輸率。2010 年日本立行政法人資訊通訊研究機構（National Institute of Information and Communications Technology, NICT）於日本學術網路 JGN2plus 上的四個據點設置金鑰分配裝置，構建了 10～90 公里的量子密碼網路（東京 QKDNetwork），並以每秒 10 萬個位元的速度，完成加密影像的傳輸。

中國量子安全骨幹計畫（China Quantum Secure Backbone Project）（Courtland, 2016）是中國大陸因應 QKD 通訊需求所執行的一項基礎建設，從 2013 年執行到 2016 年，預計建造一條從北京，經濟南、合肥，至上海，全長達 2,000 公里的量子通道，如圖 3 所示。

上述所建構的 QKD 網路均為地面上的實作，且使用光子作為量子位元的載體，並透過光纖傳輸。由於光子的能量在光纖中傳輸會造成能量的消耗，而且在訊息傳輸過程中，因量子態不可複製與干擾的特性，無法將訊號放大，使得光子有效傳輸距離均在 100 公里以內。如同中國量子安全骨幹計畫這樣超過 1,000 公里級的傳輸距離，必須透過中間很多節點的接續傳輸（Relay）才能達成。另一可達 1,000 公里級傳輸的可能作法是利用衛星傳輸。由於大氣層以上幾乎為真空，光子訊號不易衰減，使得星地傳輸距離可達上千公里遠。基於此假設，中國大陸於 2016 年 8 月 16 日發射了一顆量子科學實驗衛星（稱為「墨子號」），以進行長距離的量子通訊實驗（〈量子科學實驗衛星〉，2018）。

「墨子號」是由中國科學院負責建造，重量為 631 公斤，規劃在兩年內進行多項量子相關實驗，其中與 QKD 相關的實驗有「星地高速量子密鑰分發實驗」、「廣域量子通信網絡實驗」及「星地雙向糾纏分發實驗」等。為了建構這樣的實驗環境，其在中國大陸境內及奧地利維也納建立了許多量子通信地面站，包括河北興隆、新疆烏魯木齊南山、青海德令哈、雲南麗江、西藏阿里及維也納和格拉茨（距離維也納 199 公里）等子通信地面站，如圖 4 所

圖 3　中國量子安全骨幹計畫示意圖

資料來源：Courtland（2016）。

示。其中規劃興隆與南山之間及興隆與維也納之間進行「量子密鑰分發實驗」；南山與德令哈之間及德令哈與麗江之間進行「量子纏結分發實驗」；而衛星與阿里之間則進行「星地雙向纏結分發實驗」。而在阿里的「量子隱形傳態實驗站」部分，其主要在測試一對糾纏光子在遠距離分隔的狀況下，如果改變其中一個光子的量子態，是否會引起另一個光子量子態的對應改變。雖然此實驗曾經在 2012 年在長達 97 公里的青海剛察湖兩岸之間實現過（Knapp,

圖 4　參與「墨子號」量子通訊實驗的量子通信地面站示意圖

資料來源：〈量子科學實驗衛星〉（2018）。

2012），但相隔數千公里長的距離下的實驗卻是第一次。根據報導（Castelvecchi, 2017），「墨子號」於 2017 年 6 月 16 日進行的「量子纏結分發實驗」中，成功實現兩個糾纏光子被分發超過 1,200 公里距離後，仍可保持其量子糾纏的狀態。最近一次被披露的實驗為「墨子號」分別與河北興隆及奧地利格拉茨地面站進行了「星地量子密鑰分發」展示（大陸中心，2018）。在實驗中，「墨子號」分別傳輸給興隆地面站與格拉茨地面站之間通訊所需的共享密鑰，並結合 AES-128 加密技術，以每秒更新一次種子密鑰的方式，在北京到維也納之間展示圖片加密傳輸的實驗。據統計，此次實驗中，共計傳輸了將近 800 kbits 的共享密鑰。

伍、PQC 之發展

為了確保成熟的量子電腦問世後，有足夠能抵抗量子計算的密碼系統可繼續保護網路安全，NIST 於 2016 年 12 月開始公開徵求 PQC，以取代現有受到量子演算法威脅的公開金鑰密碼系統。如前所述，當前之非對稱式密碼無法抵抗量子計算的原因，是由於 Shor 演算法可以藉由量子特性快速解決 DL 問題，而 PQC 則是在傳統非對稱式密碼學中具有抵抗類似 Shor 演算法潛力的密碼學理論，如果經過評估證實其可抵抗量子計算的攻擊，在量子電腦問世後，其可用來取代目前類似 DH 或 RSA 演算法，在網路上進行私密金鑰交換。PQC 可概分為五大類，分別是網格密碼學（Lattice-Based Cryptography）、多變數密碼學（Multivariate Cryptography）、雜湊密碼學（Hash-Based Cryptography）、編碼密碼學（Code-Based Cryptography），以及橢圓曲線同源密碼學（Supersingular Elliptic Curve Isogeny Cryptography），而密碼學界每年均會定期針對這些 PQC 進行研討，以分析其安全性及實務上的效率，以下將簡介各 PQC 的原理及應用方向。

網格密碼學首見於 1980 年代，但網格問題上的「最壞情況到一般情況」（Worst-Case to Average Case）直到 1997 年才獲得證實（Ajtai and Dwork, 1997），此表示網格密碼系統具有高度的安全性。一般網路安全上會用到的密碼基本元件包括公鑰加密、數位簽章、雜湊函數（Hash Function）等系統，而網格幾乎可建構所有密碼學的基本元件，例如：NTRU 公鑰密碼系統即是建構在網格基礎上的密碼系統。NTRU 是將其所依賴的數學難題轉化為網格理論中的最短向量問題（Shortest Vector Problem, SVP），或是最接近向量問題（Closest Vector Problem, CVP），因此可確保其加密及解密理論上的安全。目前微軟公司在 2016 年發布基於網格密碼的函式庫（LatticeCrypto），其號稱可以提供 128 位元量子電腦計算安全性；另外，美國安全創新公司（Security Innovation）則擁有 NTRU 演算法的專利，並有開源及商業兩種授權。

多變量密碼學是由 Matsumoto and Imai（1988）所提出，其安全性是建構於解有限體上的多變量多項式上。由於在解二次以上的多項式難度等同於 Nondeterministic Polynomial 完全（NP-Complete）問題，引發學者們熱烈的討論，因此也是在 PQC 中被研究最澈底的一支。多變量密碼學可建構公開金鑰密碼系統、數位簽章、雜湊函數及串流密碼系統，與其他 PQC 比較，基於多變量密碼學的數位簽章機制則具有很高的效率。

雜湊密碼學是基於雜湊函數為基礎所建立密碼體系，例如：Lamport 一次性簽章與 Merkle

簽章均是基於雜湊密碼學所發展的簽章機制。雜湊密碼學的安全性不是依賴特定的數學難題，因此在計算上相對較具效率，在安全上也較容易分析。但也因為如此，基於雜湊密碼學的密碼系統只能用以建構數位簽章，而其他諸如公開金鑰密碼系統及密鑰交換系統則無法使用此密碼學系統建立。

編碼密碼學是於 1980 年代所發展基於錯誤更正碼（Error Correcting Code）建構的密碼系統。錯誤更正碼原本是附加在訊息上的額外資訊，可用來檢查訊息傳遞過程中是否發生錯誤，同時在其有限的能力下修正錯誤。而編碼密碼學即是藉由在一個錯誤更正碼的碼字（Code Word）加入一些錯誤，以計算出其癥狀（Syndrome），並藉此建構公開金鑰密碼系統或數位簽章系統。McEliec 公開金鑰密碼系統（McEliece, 1978）是最早利用編碼密碼學所建構的加解密系統，然而包括 McEliece 公開金鑰密碼系統及其改進的方法均已被破解。因此，在相同的安全性要求下，基於編碼密碼學所建構的公開金鑰密碼系統所使用的公、私鑰都較其他的 PQC 所使用的金鑰對來得大，例如：Niederreiter 公鑰加解密系統即使用相當大位元長度的金鑰對，以維持其安全性。

超奇異橢圓曲線同源密碼學是由 Jao 與 De Feo（2011），屬於較晚期所發展的 PQC。其是採用超奇異橢圓曲線系統進行 DH 密鑰交換機制，又稱為超奇異同源 DH 密鑰交換機制（Supersingular Isogeny DH Key Exchange, SIDH）。在 PQC 中，SIDH 可提供最小位元長度密鑰以達到與其他後量子密碼系統相同的安全性，其同時相容於 DH 或 ECDH 系統，是很好的金鑰交換系統，可惜必須付出高計算量的代價。

陸、國內未來發展之建議

本文已簡要說明在量子演算法威脅下，世界各組織為了維持網路通訊安全所採取的可行方案，包括 QKD 及採用 PQC 等。在這兩方案中，由於 QKD 為直接採用量子力學的特性所架構的密鑰分發管道，可以達到理論上的安全，因此世界上各政府組織及民間機構已進行相關的計畫以驗證其理論的可行性，而相關端點量子設備也已產品化。預測未來當成熟的量子電腦問世後，其將扮演維持網安全的第一線角色；在 PQC 方面，具有成為未來標準潛力的五大後量子密碼類別，目前密碼學界正熱烈討論中，其中考量的重點莫過於安全與實作效率兩大問題。面對量子計算對現有未來密碼系統安全之衝擊，個人覺得在有限的資源下，國內可以朝以下之方向發展。

一、科技部從 2018 年起，計畫每年投入臺幣 7,000 萬經費，以 3 ~ 5 年時間，結合半導體產業，輔導團隊研發量子電腦，可是並無對於量子通訊專款的研究經費投入。建議科技部應比照量子電腦研發，設立專款，並結合國內民間產業及國防工業等相關資源，在國內大學設有量子研究中心，單位內培養量子通訊相關人才。目前國內包括臺灣大學、中央大學、清華大學、交通大學及成功大學等知名大學均成立量子相關研究單位，以進行量子前瞻科技之研究。由於國內在量子通訊研究起步較其他國家晚，為了能迎接未來量子計算的挑戰，在國家層級應整合國內具有研發能量的產官學界一起努力，以加速國內量子通訊的發展。基於此，國內也應加快腳步進行 QKD 相關基礎之建設。

二、在安全上，目前看似安全的 PQC，難保未來沒有對應具有威脅性的量子演算法出現。因此，作為來後量子密碼標準的 PQC，應該能提出確切的理論基礎，以作為其面對量子計算之安全評估標準，而目前有些 PQC 則沒有這樣的理論存在；在實務上，為了達到與現有密碼系統同樣的安全性，後量子密碼系統必須使用很大位元數的金鑰對，一般都在千位元組的大小，甚至有系統必須使用百萬位元組長度的金鑰對，均是未來實務上必須面對的問題。以上所列舉 PQC 的安全與效率問題，未來均有賴國際相關組織進一步討論與評估，而在國內則建議由政府部門結合包括中央研究院、國防部各軍事學院、中山科學研究院及國內各大學具有密碼學研究師資人才，成立智庫，並提供相關科研經費，補助參加國際知名 PQC 研討，以掌握國際標準制定之發展，未來可適時提供政府及關心國內網路安全單位制定相關因應策略之參考。

參考文獻

大陸中心，2018 年 1 月 22 日，〈墨子號完成量子保密洲際通話——全球首次成功 75 分通信會議〉，《ETtoday新聞雲》，https://www.ettoday.net/news/20180122/1097878.htm#ixzz5cr6ple2Z（瀏覽日期：2019 年 1 月 16 日）。

〈坐在家裏，你也可以體驗 IBM 量子電腦的威力〉，2016 年 5 月 6 日，《端聞》，https://theinitium.com/article/20160505-dailynews-IBM（瀏覽日期：2019 年 1 月 16 日）。

〈量子科學實驗衛星〉，2018 年 9 月 9 日，《維基百科》，https://zh.wikipedia.org/wiki/%E9%87%8F%E5%AD%90%E7%A7%91%E5%AD%A6%E5%AE%9E%E9%AA%8C%E5%8D%AB%E6%98%9F（瀏覽日期：2019 年 1 月 16 日）。

雷鋒網，2016 年 2 月 14 日，〈量子計算過於強大，NSA：加密演算法必須因應升級才安全〉，《科技新報》，https://technews.tw/2016/02/14/nsa-says-it-must-act-now-against-the-quantum-computing-threat（瀏覽日期：2019 年 1 月 16 日）。

Kayue，2015 年 12 月 11 日，〈Google 的量子電腦比普通電腦快 1 億倍？專家表示言之尚早〉，《關鍵評論》，https://hk.thenewslens.com/article/32489（瀏覽日期：2019 年 1 月 16 日）。

Ajtai M., and Dwork C., 1997, “A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence,” in *Proceedings of the Twenty-Ninth STOC*, El Paso, TX: Association for Computing Machinery, 284-293. doi:10.1145/258533.258604

Alléaume R., 2007/1/22, *SECOQC White Paper on Quantum Key Distribution and Cryptography,* Version 5.1, Austrian Research Centers GmbH.

Bailey B., 2018/10/29, “The Impact of Moore’s Law Ending,” *Semiconductor Engineering*, https://semiengineering.com/the-impact-of-moores-law-ending (accessed January 16, 2019).

Beauregard S., 2003, “Circuit for Shor’s Algorithm Using 2n+3 Qubits,” *Quantum Information and Computation*, 3(2), 175-185.

Biham E., and Shamir A., 1993, *Differential Cryptanalysis of the Data Encryption Standard*, New

York, NY: Springer-Verlag. doi:10.1007/978-1-4613-9314-6

Brassard G., and Bennett C. H., 1984, "Quantum Cryptography: Public Key Distribution and Coin Tossing," In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India: Steering Committee, 175-179.

Castelvecchi D., 2017/6/15, "China's Quantum Satellite Clears Major Hurdle on Way to Ultrasecure Communications," *Nature*, https://www.nature.com/news/china-s-quantum-satellite-clears-major-hurdle-on-way-to-ultrasecure-communications-1.22142?WT.ec_id=NEWS-DAILY-20170616#/b1 (accessed January 16, 2019).

Courtland R., 2016/10/26, "China's 2,000-km Quantum Link Is Almost Complete," *IEEE Spectrum*, https://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete (accessed January 16, 2019).

Diffie W., and Hellman M. E., 1976, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 22(6), 644-654. doi:10.1109/TIT.1976.1055638

ElGamal T., 1985, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, 31(4), 469-472. doi:10.1109/TIT.1985.1057074

Elliott C., Colvin A., Pearson D., Pikalo O., Schlafer J., and Yeh H., 2005, "Current Status of the DARPA Quantum Network," in *Proceedings of the Defense and Securit*y, Orlando, FL: Society of Photo-Optical Instrumentation Engineers, 138-149. doi:10.1117/12.606489

Grover L. K., 1997, "Quantum Mechanics Helps in Searching for a Needle in a Haystack," *Physical Review Letters*, 79(2), 325. doi:10.1103/PhysRevLett.79.325

Jao D., and De Feo L., 2011, "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," in *Proceeding of the PQCrypto 2011*, Taipei, Taiwan: Springer-Verlag, 19-34. doi:10.1007/978-3-642-25405-5_2

Knapp A., 2012/5/11, "Chinese Researchers Quantum Teleport Photons Over 60 Miles," *Forbes*, https://www.forbes.com/sites/alexknapp/2012/05/11/chinese-researchers-quantum-teleport-photons-over-60-miles/#2d7a0e5035eb (accessed January 16, 2019).

Matsui M., 1994, "Linear Cryptanalysis Method for DES Cipher," in *Proceedings of 93 EUROCRYPT*, Heidelberg, Germany: Springer, 386-397.

Matsumoto T., and Imai H., 1988, "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption," in *Proceedings of 88 EUROCRYPT*, Heidelberg, Germany: Springer, 419-453. doi:10.1007/3-540-45961-8_39

McEliece R. J., 1978, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," *Coding Thv*, 4244, 114-116.

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

Rivest R., Shamir A., and Adleman L., 1978, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM*, 21(2), 120-126. doi:10.1145/359340.359342

Shor P. W., 1994, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM: Institute of Electrical and Electronics Engineers, 124-134. doi:10.1109/SFCS.1994.365700

Shor P. W., 1997, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computer*, 26(5), 1484-1509. doi:10.1137/S0097539795293172

Stallings W., 2010, *Cryptography and Network Security: Principles and Practice*, 5th ed., Upper Saddle River, NJ: Prentice Hall Press.