# 後量子密碼學運用於無人飛行載具通訊鏈路安全之初探

作者／蔣河山


## 提要

一、無人飛行載具，越來越多被應用於許多具挑戰性和多樣化的領域，這些涵蓋了民用和軍事領域。在開放式無線通訊鏈路下運作，安全性和隱私問題也隨之上升。

二、隨著量子計算機的出現，當今廣泛使用於無人機通訊鏈路加密機制易受到量子計算攻擊，使得安全性和隱私也處於脆弱狀態。為了實現免受安全和隱私威脅的良好環境，已有調查研究奠定了基礎，即所謂後量子加密。

三、本文旨在分析PQC技術在UAV通訊安全應用方向，研究發現仍具有「運算資源需求」、「.延遲問題」、「兼容性與過渡期」及「安全性與抗攻擊性」等挑戰，未來研究可進一步針對UAV通訊架構的升級實作藉以驗證其可行性。


關鍵詞:密碼學、無人機、通訊鏈路、量子密碼學、PQC、Drone

## 前言

無人運輸載具（Unmanned Aerial Vehicles, UAVs）起源於1970年代由美國國防部發展使用於軍事用途，由早期人工手動操作發展到目前搭載微型飛行控制電腦與整合全球定位系統（Global Positioning System, GPS）和地面控制站(Ground Control Station, GCS)等，透過無線通訊系統導航。UAVs可以在各種設置中用作垂直組件，例如作為空中基地台、存取點(Access Point, AP)、中繼站(RelayStations)或飛行行動終端，提高覆蓋範圍和第六代行動通訊技術(SixthGenerationMobile Networks or Sixth Generation Wireless Systems, 6G)無線網路的能源效率。[1]由於UAVs可以與地面工作站和衛星進行通聯，形成空對地網路連結。

UAVs將其軍事範圍擴大到商業用途變得越來越普遍，隨之而來安全上的脆弱性以及載具上有限運算資源，出現UAVs通訊安全性和隱私之常規加密方法存有嚴重風險。這些風險包括未經授權的存取、資料外洩和網路實體攻擊之可能性

1 Khan, M.A.; Kumar, N.; Mohsan, S.A.H.; Khan, W.U.; Nasralla, M.M.; Alsharif, M.H.; Zywiołek, J.; Ullah,I Swarm of UAVs for ˙network management in 6G: A technical review. IEEE Trans. Netw. Service Manag.20 22, 20, 741–761.。

，[2]會危及無人機操作的機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)。[3]因此，通訊鏈路安全對於UAVs而言至關重要。

UAVs在傳統輕量級加密，[4]隨著量子電腦運算(Quantum Computing)出現了獨特漏洞和安全上的脆弱性，對於單位或組織運用，具有關鍵性之影響。無人機的通訊鏈路存在被攔截、資料被篡改以及未經授權存取的風險，使得執行關鍵任務時，敏感資訊會置於風險之中UAVs威脅通常針對無人機系統，包含了無人機、GCS或兩者之間的通訊鏈路。[5]

儘管過去幾年有不少學者提出了，解決UAVs的安全和隱私問題，這些進展與解決方案仍忽略了量子威脅，使得無人機通訊鏈路安全性仍處於脆弱狀態。因此，後量子加密（Post-Quantum Cryptography, PQC）在增強無人機通訊鏈路安全性方面之適用性，就是值得探討的主題，也是本研究動機。本文期望透過對目前常用傳統密碼機制進行討論與比較，在PQC環境中保持其安全性，提供未來無人機安全性挑戰，有初步

認識及納入判斷之指標與參考。

## 文獻探討

### 一、UAVs概要

#### (一)背景與架構

UAVs是機上沒有任何人類飛行員、機組人員或乘客的飛機，[6]通常被稱為無人機系統（Unmanned Aircraft System, UAS）、無人機（Unmanned Aerial Vehicle, UAV or Drone）、遙控飛機系統（Remotely Piloted Air System, RPAS）、遙控飛行器(Remotely Piloted Vehicle, RPV)、遙控飛機(Remotely Piloted Aircraft, RPA)。[7]UAV主要由三個部分組成，區分無人機、基地台/地面控制站(Ground Control Station, GCS)和連接它們的通訊系統(如圖1)。[8]

---

2 H. Wang et al., “Survey on unmanned aerial vehicle networks: A cyber physical system perspective ,” IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1027–1070, 2nd Quart., 2020

3 Khan, Muhammad Asghar, et al. "Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review."IEEE Transactions on Network and Service Management(2024)

4 輕量級加密（Lightweight Cryptography, LC）泛指一種運算量較傳統密碼學演算法小的密碼學演算法，旨在提供運算能力不強、對於能源效率有較高要求的裝置。

5 J. Whelan, A. Almehmadi, J. Braverman and K. El-Khatib, “Threat Analysis of a long range autonomous unmanned aerial system,” in Proc. 2020 Int. Conf. on Computing and Information Technology , Tabuk, Saudi Arabia, pp. 1–5, 2020

6 Ahmad, A., Ordoñez, J., Cartujo, P., & Martos, V. (2021). Remotely Piloted Aircraft (RPA) in Agriculture:A Pursuit of Sustainability. Agronomy, 11(1), 7.

7 Dalamagkidis, K.; Valavanis, K.P.; Piegl, L.A. On Integrating Unmanned Aircraft Systems into the National Airspace System: Issues, Challenges, Operational Restrictions, Certification, and Recommendations; Springer Science & Business Media: Berlin/Heidelberg, ermany, 2011; Volume 54.

8 J. Gertler, “US unmanned aerial systems,” Library of Congress Washington DC Congressional Research Service, vol. 1, no. 1, pp. 1–10, 2012.

最初，在二十世紀為軍事任務而開發，隨著控制技術改進和成本降低，它們的用途擴展到許多休閒和娛樂應用。此後，UAVs還有許多其他新興應用，包括航空攝影、農業、火災監測、環境保護、交通監控、搜索和救援、產品交付、娛樂等。2015年時Floreano等學者將UAVs根據其體積和飛行時間進行分類，區分固定翼和旋翼式，其中機身與結構相對較重的UAVs將有能力攜帶較重之有效載荷，並可執行自主和多項任務;另外考慮到空氣動力效率，定翼機比旋翼機可以有更多的飛行時間(如表1)[9]。

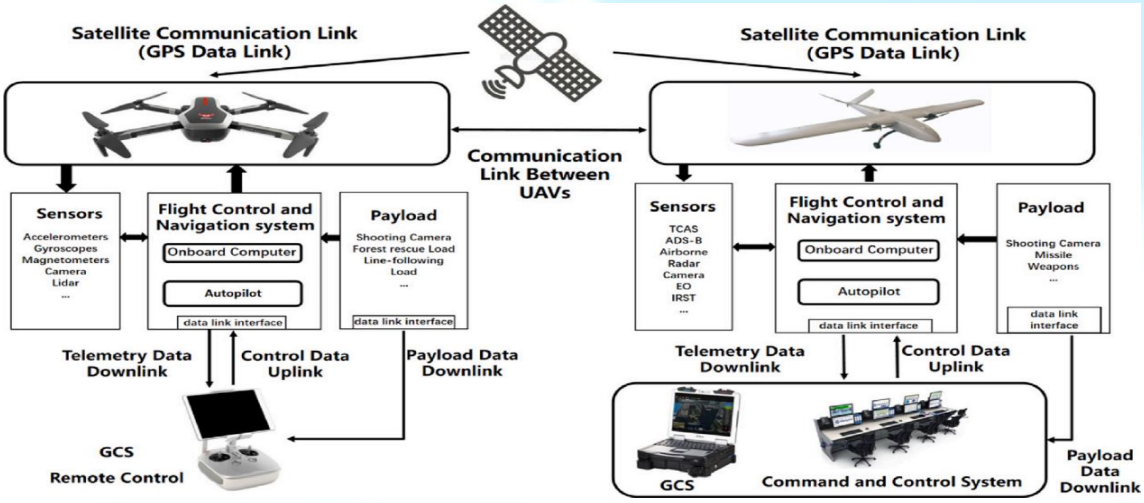


圖 1 UAV 架構

資料來源：Z. Wang, Y. Li, S. Wu, Y. Zhou, L. Yang, Y. Xu, T. Zhang, and Q. Pan, "A survey on cybersecurity attacks and defenses for unmanned aerial systems," Journal of Systems Architecture, vol. 138, p. 102870, 2023.

表 1 無人機區分類型

| Category | Weight | Altitude | Range | Payload |
|---|---|---|---|---|
| Nano | < 0.2 kg | < 90 m | < 90 m | < 0.2 kg |
| Micro | < 2 kg | < 90 m | < 5 km | < 0.5 kg |
| Mini | < 20 kg | < 900 m | < 25 km | < 10 kg |
| Small | < 150 kg | < 1500 m | < 100 km | < 50 kg |
| Tactical | > 150 kg | > 1500 m | > 100 km | > 50 kg |

資料來源：B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, ‘ ‘SoK－security and privacy int he age of drones: Threats, challenges, solution mechanisms, and scientific gaps,’ ’ 2

9 Dario Floreano and Robert J Wood. Science, technology and the future of small autonomous drones. Nature, 521(7553):460–466, 2015.

019, *arXiv:1903.05155*. [Online]. Available: http://arxiv.org/abs/1903.05155

(二)通訊類型

無人機通訊可以分為四種主要類型：[10]

1.無人機到無人機(Drone-to-Drone, D2D):用於多架無人機之間的直接通信，支持協同操作和編隊任務。

2.無人機到地面站(Drone-to-Ground Station, D2GS):用於無人機與控制地面站之間的通信，包括指令下達和數據回傳。

3.無人機到網絡(Drone-to-Network, D2N):通過無線蜂窩網絡（如4G/5G）進行通信，實現實時數據傳輸和遠程控制。

4.無人機到衛星(Drone-to-Satellite, D2S):通過衛星通信鏈路支持遠程或無覆蓋區域的操作。

(三)鏈路安全

無人機(UAV)通信主要依賴於MAVLink、SSL/TLS和IEEE 802.11等通訊協定，採用了傳統的加密機制來進行安全資料交換。[11]這些傳統加密機制，主要有對稱式加密和非對稱式加密等技術，來確保機密性和身份驗證(如圖2)。這些協定採用傳統加密方案，因此容易受到量子計算帶來的威脅影響。

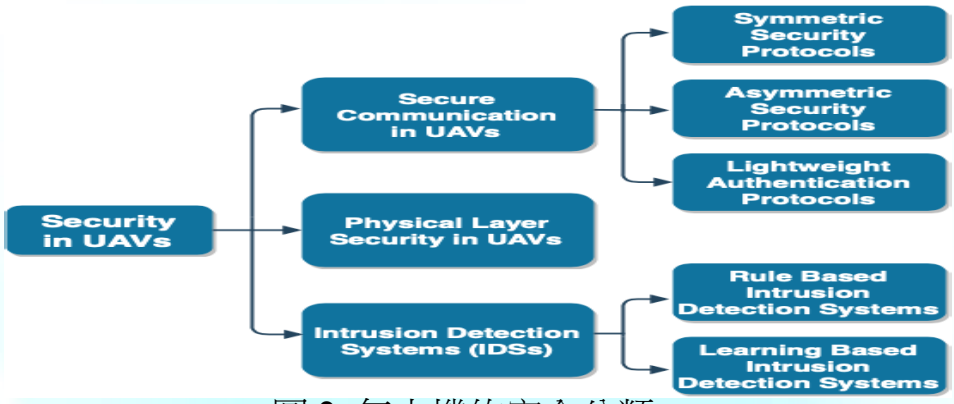


圖 2 無人機的安全分類

資料來源：A. Shafique, A. Mehmood, and M. Elhadef, "Survey of security protocols and vulnerabilities in unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 46927–46948, 2021.

## 二、密碼學在資訊安全運用

在傳統密碼學中，有兩種加解密方式，分別為「對稱式加密(Symmetric

10 J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," Internet Things, vol. 11, Sep. 2020, Art. no. 100218.

11 M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, "Future-proofing security for uavs with post-quantum cryptography: A review," IEEE Open Journal of the Communications Society, 2024.

Encryption)」與「非對稱式加密(Asymmetric Encryption)」(運作原理如圖3)。儘管加密具有許多優勢，但使用加密也存在一些缺點;其中最困難的問題是密鑰管理，加密資料的發送者和接收者必須交換並安全存儲密鑰。

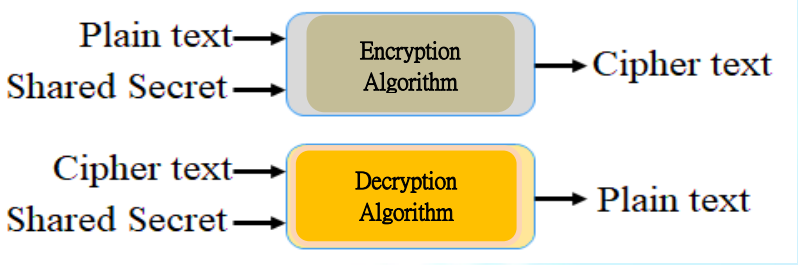


圖 3 傳統密碼機制運作原理

資料來源：E. E. Nithila, A. Rosi *et al*., "*A survey about post quantum cryptography methods*," *EAI Endorsed Transactions on Internet of Things*, vol. 10, 2024.

此外，加密過程可能需要大量的計算資源，這會降低大數據處理效率，導致處理速度變慢，區分如下:

(一)對稱式加密:1976年6月前公開的加密方式，是指發送方和接收方共用相同加、解密鑰匙（如圖4）。例如資料加密標準（Data Encryption Standard, DES）[12]和進階加密標準（Advanced Encryption Standard, AES），[13]其中的主要難度在於要如何找到在傳送方和接收方間，安全共用金鑰的方法。

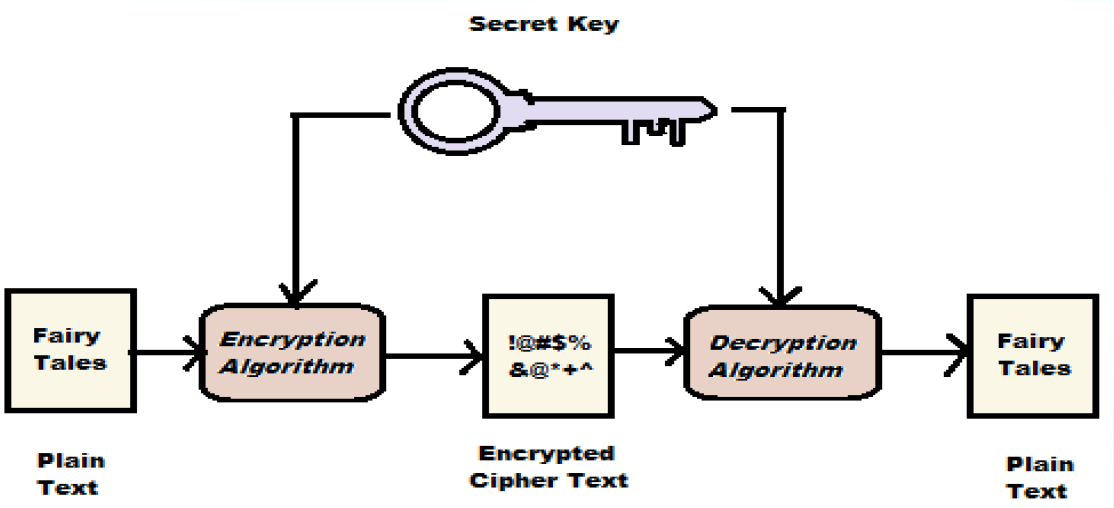


圖 4 對稱式加密

資料來源：S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in Proc. Int. Conf. Electron., Commun. Comput. Eng. (ICECCE), Nov. 2014, pp. 83–93.

12 Standard, NIST FIPS, Data Encryption Standard (DES). Federal Information Processing Standards Publication,1999, 46-3.

13 Standard, NIST FIPS, Advanced Encryption Standard (AES). Federal Information Processing Standards Publication, 2001, 197.

(二)非對稱式加密:此為一種更安全的加密技術，傳送方和接收方都各有兩把金鑰(公鑰和私鑰)。在此過程中，傳送方會使用接收方的公鑰來加密訊息，而接收方則會使用其私鑰來解密訊息和讀取訊息(如圖5)。RSA(Rivest–Shamir–Adleman)即是最常見的非對稱式加密方式。

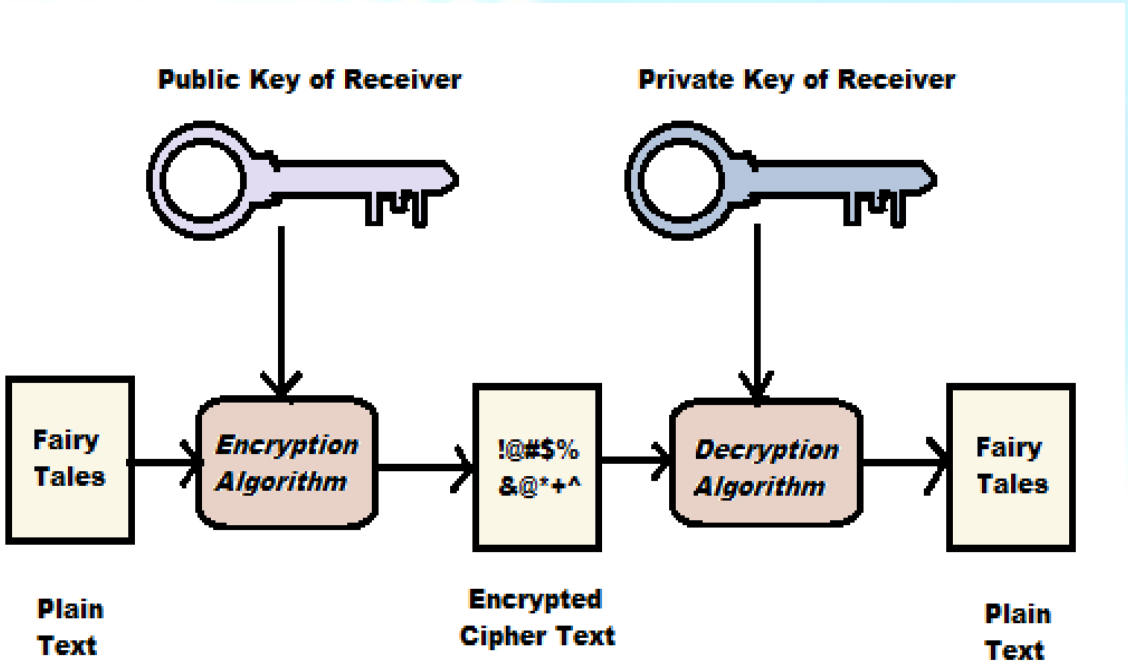


圖 5 非對稱式加密

資料來源：S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in *Proc. Int. Conf. Electron., Commun. Comput. Eng. (ICECCE)*, Nov. 2014, pp. 83–93.

## 三、量子運算與密碼

量子運算(Quantum Computing)主要是利用量子力學獨特屬性，[14]以目前傳統電腦無法實現的方式執行計算(等級比較如表2)，[15]其核心運作是基於量子位元(Qubits)，[16]與傳統位元(Bit)不同。量子位元可以同時處於0和1的多種狀態，這稱為量子疊加原理(Superposition)，此特性是使量子電腦能夠同時對多個可能的輸入進行計算，大幅提高計算能力(從Spartan Scytale到量子計算加密技術的發展過程如圖6)。

14 P. W. Shor, "Quantum computing," Documenta Math., vol. 1, no. 1000, p. 1, 1998
15 Nofer, M., Bauer, K., Hinz, O., van der Aalst, W., & Weinhardt, C. (2023). Quantum Computing. Business & Information Systems Engineering, 65(4), 361-367.
16 S. T. Marella and H. S. K. Parisa, "Introduction to quantum computing," Quantum Computing and Communications, 2020.

表 2 傳統加密機制與量子計算安全等級比較

| Crypto Scheme | Key Size | Effective Key Strength/Security Level (in bits) | |
|---|---|---|---|
| | | Classical Computing | Quantum Computing |
| RSA-1024 | 1024 | 80 | 0 |
| RSA-2048 | 2048 | 112 | 0 |
| ECC-256 | 256 | 128 | 0 |
| ECC-384 | 384 | 256 | 0 |
| **AES-128** | **128** | **128** | **64** |
| **AES-256** | **256** | **256** | **128** |

資料來源：V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, “The Impact o f Quantum Computing on Present Cryptography,” International Journa l of Advanced Computer Science and Applications, vol. 9, 2018.

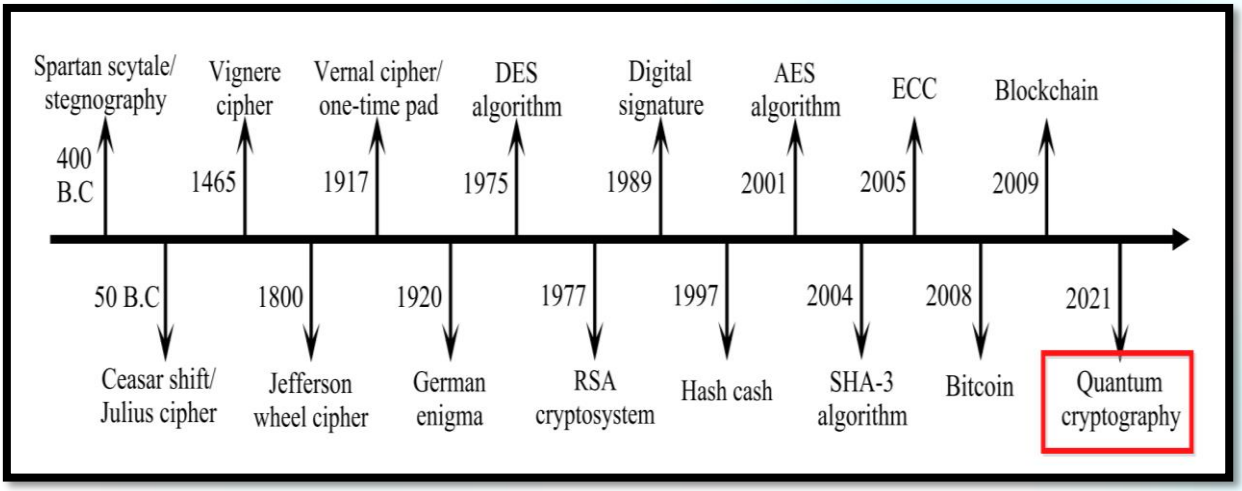


圖 6 量子計算加密技術演變過程

資料來源：V. K. Ralegankar, J. Bagul, B. Thakkar, R. Gupta, S. Tanwar, . Sharma, and I. E. Davidson, “Quantum cryptography-as-a-service for secure uav communication: Applications, challenges, and case study,” *IEEE Access*, 2021.

## 四、相關研究文獻

隨著軍事和商業運用無人機技術不斷進步和普及，它們經常攜帶竊聽者出於多種原因想要檢索的敏感資訊。無人機是由各種軟、硬體所組成，但這些模組中也可能存在潛在安全漏洞，[17]例如透過發動全球衛星定位系統(GlobalPositioning System, GPS)欺騙攻擊或無線網路（Wireless Fidelity,Wi-Fi）

17 Tychola, Kyriaki A., and Konstantinos Rantos. "Cyberthreats and Security Measures in Drone-Assisted Agri culture." Electronics 14.1 (2025): 149.

攻擊，竊聽者可以攔截目標無人機並存取所需資訊。

2016年Hayat等學者，從民用無人機飛行網路角度進行通訊系統透過網絡傳輸最少數據、相關任務參數和服務品質的調查。[18]2021年沙菲克等學者，研究了無人機安全措施且發現漏洞，提出增強安全性的方法。[19]2021年Wang等學者，研究了典型UAV通訊威脅，以制定安全需求。他們對提升無人機通訊安全性的現有安全對策，從實體和網路層進行深入評估。[20]2019年Nassi等學者，對商業用途無人機的安全與隱私問題進行全面探討，研究了學術界與業界在偵測和禁用無人機之方法。[21]Yaacoub等學者，探討網路攻擊興起以及商業無人機所面臨的挑戰，提出了強化無人機偵測與防禦之新方法和技術。同時，還討論了無人機網路的隱私與安全問題，指出其限制並提出相關建議。[22]在另一項研究中，2015年Shoufan等學者透過提出AES協定與硬體實現來保護GCS與UAV之間的通訊，主要針對機密性與身份驗證進行研究。[23]

有多種方法可以增加通訊鏈路之安全性，由於UAV中的連結是無線且網路拓撲具動態。因此排除運用實體連結方式進行保護的可能性，以目前使用密碼加密技術，是確保符合這些規範之通訊鏈路的最佳方式。隨著量子電腦提出的獨特漏洞和安全要求出現，UAV安全性問題仍然不斷在演變，從B5G(Beyond Fifth Generation)[24]甚至第六代行動通訊系統(Sixth Generation,6G)網路中的量子攻擊，後量子密碼學（Post-Quantum Cryptography, PQC）已成為確保無人機安全通訊以因應這項挑戰的解決方案。[25]因此傳統加密演算法需要經過修改以增強抗量子攻擊能力，或者採用能夠抵禦量子攻擊的新型演算法來取代現有方案。

PQC是一個新興研究領域，本研究探討PQC的複雜性及其在確保與預期量子時代軍事通訊安全之重要性。它有望提供能夠承受量子電腦強大功能的密碼解決方案。

---

18 S. Hayat, E. Yanmaz, and R. Muzaffar, “Survey on unmanned aerial vehicle networks for civil applications A communications viewpoint,” IEEE Commun. Surveys Tuts., vol. 18, no.4,pp. 2624–2661, 4th Quart.2016.

19 A. Shafique, A. Mehmood, and M. Elhadef, ‘Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles’, IEEE Access, vol. 9, pp. 46927–46948, 2021

20 L. Wang, Y. Chen, P. Wang, and Z. Yan, ‘Security Threats and Countermeasures of Unmanned Aerial Vehi cle Communications’, IEEE Communications Standards Magazine, vol. 5, no. 4, pp. 41–47, 2021.

21 B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, ‘SoK – Security and Privacy in the Age of Drones: Th reats, Challenges, Solution Mechanisms, and Scientific Gaps’, ArXiv, vol. abs/1903.05155, 2019.

22 J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, “Security analysis of drones systems: Attacks, limitat ions, and recommendations,” Internet Things, vol. 11, Sep. 2020, Art. no. 100218.

23 A. Shoufan, H. AlNoon and J. Baek, “ Secure communication in civil drones,” in Int. Conf. on Informatio nSystems Security and Privacy, cham, Springer, pp. 177–195, 2015.

24 B5G指的是在5G之上的增強型技術，其高速、低延遲及大容量的特性，提供更多設備和應用需求、更高的速度和更低的延遲率。B5G採用更高頻段的次太赫茲(100~300 GHz)，可擴大頻寬，降低延遲與縮短傳輸時間，並增加對聯網機器人、無人機控制。

25 Khan, Muhammad Asghar, et al. "Security and Privacy Issues and Solutions for UAVs in B5G Networks: AReview."IEEE Transactions on Network and Service Management(2024)

## 現行通訊機制安全與威脅

UAV飛行時間取決於不同因素，包括其軌跡、速度、重量和能源，可分為遙控無人機和完全自主無人機。最初無人機主要是為軍事而開發，操作安全優先於網路安全。然而隨著無人機越來越多地融入各行各業，對安全和隱私關鍵重要性認識也在不斷提高。目前無人機中的安全措施功能，如數據傳輸加密、實施安全認證機制及入侵檢測系統(Intrusion Detection Systems, IDS)等，能在一定程度上減少網路安全威脅。在下面章節中，將討論傳統加密技術應用安全與隱私威脅。

### 一、傳統密碼安全問題

(一)對稱式加密:此技術使用單一密鑰對資料進行加密和解密，密鑰由資料的發送者和接收者共同共享，特點是速度快且效率高；然而，它需要一個安全的通道來確保密鑰能夠安全地交換。[26]

(二)非對稱式加密:與對稱式加密相反，這種技術依賴於一對密鑰(公開密鑰和私密密鑰)來完成資料的加、解密。[27]雖然，非對稱式加密的密鑰長度通常較長，意味著需要較長運算時間，相對於對稱式加密較慢，但安全性較高。[28]表3顯示，RSA等非對稱式加密的速度比對稱式加密慢1,000倍，相較於DES、3DES和AES，則是安全性最低的演算法。

### 二、量子計算對傳統加密演算法威脅

量子計算對傳統密碼學之影響，源於其能夠以指數級的速度執行某些數學運算。不同於RSA和ECC加密演算法，其安全性是依賴於某些數學問題之高難度，例如整數分解和離散對數。然而量子電腦可以運用Grover和Shor演算法（尤其是Shor演算法）能有效地破解對稱式與非對稱式加密機制。[29]

(一)Grover搜尋演算法：透過平方根加速搜尋金鑰，在對稱式加密機制（如AES和3DES）中大幅縮短破解時間，為原始時間的平方根。[30]

(二)Shor因數分解演算法：能夠以多項式時間解決數學問題，輕鬆破解目前最廣泛使用的非對稱式加密機制(RSA)、橢圓曲線加密（ECC）和Diffie-Hellman等演算法，也證明量子電腦相對於傳統電腦的優勢(如圖7)。

然而非對稱式加密機制在資料和隱私保護方面擔任著重要角色，任何破解演算法的可能性都將構成重大挑戰。

---

26 M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, “Symmetric encryption algorithms: Review and e valuation study,” International Journal of Communication Networks and Information Security, vol. 12, no. 2 ,pp. 256–272, 2020.

27 B. Halak, Y. Yilmaz, and D. Shiu, “Comparative analysis of energy costs of asymmetric vs symmetric enc ryption-based security applications,” IEEE Access, vol. 10, pp. 76 707–76 719, 2022.

28 A. A.-R. El-Douh, S. F. Lu, A. A. Elkouny, and A. Amein, “Hybrid cryptography with a one–time stamp to secure contact tracing for covid–19 infection,” International Journal of Applied Mathematics and Comput er Science, vol. 32, no. 1, pp. 139–146, 2022.

29 D. J. Bernstein, “Introduction to post-quantum cryptography,” in Post-Quantum Cryptography, Berlin, Germa ny: Springer, 2009, pp. 1–14.

30 D. J. Bernstein and T. Lange, “Post-quantum cryptography,” Nature, vol. 549, no. 7671, pp. 188–194, 2017

表 3 RSA、DES、3DES 和 AES 安全性比較表

| Factors | RSA | DES | 3DES | AES |
|---|---|---|---|---|
| Created By | Ron Rivest, Adi Shamir, and Leonard Adleman In 1978 | IBM in 1975 | IBM IN 1978 | Vincent Rijmen, Joan Daemen in 2001 |
| Key Length | Depends on number of bits in the modulus n where n=p*q | 56 bits | 168 bits (k1, k2 and k3) 112 bits (k1 and k2) | 128, 192, or 256 bits |
| Round(s) | 1 | 16 | 48 | 10 - 128 bit key,12 - 192 bit key,14 - 256 bit key |
| Block Size | Variable | 64 bits | 64 bits | 128 bits |
| Cipher Type | Asymmetric Block Cipher | Symmetric Block Cipher | Symmetric Block Cipher | Symmetric Block Cipher |
| Speed | Slowest | Slow | Very Slow | Fast |
| Security | Least Secure | Not Secure Enough | Adequate Security | Excellent Security |

資料來源：G. Singh and Supriya, “A study of encryption algorithms (RSA (Rivest–Shamir–Adleman), des, 3des and aes) for information security,” International Journal of Computer Applications, vol. 67, pp. 33–38, 2013.

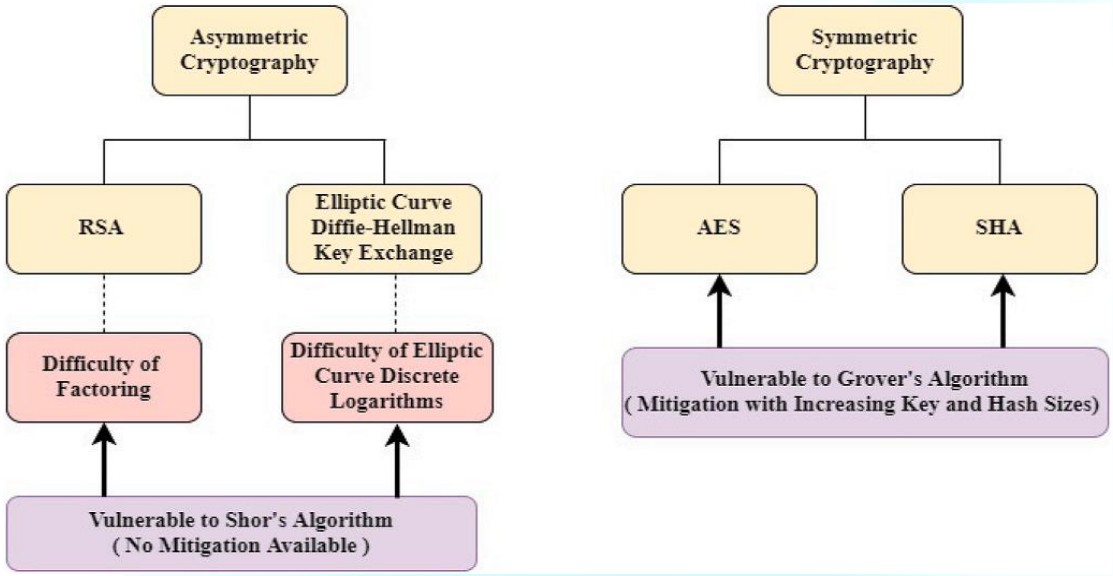


圖 7 Shor 和 Grover 演算法對傳統密碼的影響

資料來源：V. K. Ralegankar, J. Bagul, B. Thakkar, R. Gupta, S. Tanwar, . Sharma, and I. E. Davidson, “Quantum cryptography-as-a-service for secure uav communication: Applications, challenges, and case study,” IEEE Access, 2021.

另外根據Niraula等人研究，探討了量子計算對某些量子時代前的加密算法，如AES、RSA、數字簽名算法(DSA)、橢圓曲線Diffie-Hellman(ECDH)、SHA-2和SHA-3之影響。AES-128和RSA-2048能夠提供針對傳統攻擊的安全性，但無法抵禦量子攻擊。對於RSA擴展密鑰長度並沒有顯著影響；然而將AES密鑰長度加倍可以提供額外的128位安全性(如表4)。

表 4 量子計算對傳統密碼的影響

| Pre-quantum algorithm | Technique | QC impact | Quantum algorithm used |
|---|---|---|---|
| AES | Symmetric key | Larger Key size needed | Grover's algorithm |
| RSA | Asymmetric key | No longer secure | Shor's algorithm |
| DSA | Asymmetric key | No longer secure | Shor's algorithm |
| ECDH | Asymmetric key | No longer secure | Shor's algorithm |
| SHA-2, SHA-3 | Hash Function | Large output needed | Grover's algorithm |

資料來源：Don Jelle, et al. Security of the Fiat-Shamir Transformation in the quantum random-Oracle model. Advances in Cryptology – CRYPTO 2019 2019:356–83

因此UAV通訊鏈路面臨被攔截、資料篡改和未經授權存取的風險，從而危及關鍵任務操作與敏感資訊(如圖8)。

| Cryptographic Algorithm | Type | Purpose | Impact from large-scale quantum computer |
|---|---|---|---|
| AES | Symmetric key | Encryption | Larger key sizes needed |
| SHA-2, SHA-3 | ---------- | Hash functions | Larger output needed |
| RSA | Public key | Signatures, key establishment | No longer secure |
| ECDSA, ECDH (Elliptic Curve Cryptography) | Public key | Signatures, key exchange | No longer secure |
| DSA (Finite Field Cryptography) | Public key | Signatures, key exchange | No longer secure |

圖 8 量子計算對常見密碼演算法的影響

資料來源：L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone. NIST IR 8105: Report on post-quantum cryptography. Technical report, National Institute of Standards and Technology (NIST), April 2016.

## 通訊鏈路安全與需求

隨著無人機在不同應用領域需求的增加，製造商現在將安全功能納入設計中，以保護珍貴數據資料與避免潛在安全漏洞。由於無人機（UAV）透過無線通

訊來交換信息，易受到威脅和攻擊，主要針對三個部份：無人機本體、地面控制站，或兩者之間的通訊鏈路。[31]

**一、機體安全威脅:**

攻擊手段可能方式為軟殺(藉由各種手段增加飛行難度，如密集泡沫或固體物體群)、硬殺(屬直接攻擊類型，無人機低空飛行時，透過武器等方式將其擊落)、惡意硬體破壞(損壞或竊取硬體)和人為攻擊(如防禦系統)。

**二、地面控制站與通訊鏈路威脅:**

UAV與GCS之間的連接通常通過通訊協定進行通聯，例如MAVLink、Uranus Link和UAVCAN(如圖9)。

**三、無人機（UAV）與地面控制站（GCS）:**

根據美國空軍技術學院一份研究報告指出，[32] MAVLink (Micro Air Vehicle Link)協定未提供CIA機密性(Confidentiality)、完整性(Integrity)和可用性(Availability)安全服務也未對訊息進行加密，缺乏標準安全程序且存在多種漏洞，容易受到各類攻擊的威脅。任何駭客或攻擊者只需使用合適的發射裝置，即可與無人機進行相互通聯並植入指令，從而輕易攔截和操控通信內容，達到劫持無人機之目的。


圖 9 UAV 與 GCS 通訊鏈結架構

資料來源：Khan, N.A.; Jhanjhi, N.Z.; Brohi, S.N.; Almazroi, A.A.; Almazroi, A.A. A secure communication protocol for unmanned aerial vehicles. *CMC-COMPUTERS MATERIALS CONTINUA* 2022, *70*, 601–618.

由於UAV執行任務期間，多數時間是處於敵對環境中，入侵者可以通過標準介面或連接埠，攔截UAV或其數據，[33]藉由惡意攔截通訊信號、無人機載具或通

31 J. Whelan, A. Almehmadi, J. Braverman and K. El-Khatib, “Threat Analysis of a long range autonomous unmanned aerial system,” in Proc. 2020 Int. Conf. on Computing and Information Technology , Tabuk, Sa udiArabia, pp. 1–5, 2020.

32 J. A. Marty, “Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft ,”Air Force Institute of Technology, Tech. Rep., 2013.

33 M. Leccadito, T. Bakker, R. Klenke, and C. Elks, “A survey on securing UAS cyber physical systems,” IE EE Aerosp. Electron. Syst. Mag., vol. 33, no. 10, pp. 22–32, Oct. 2018

過篡改、破壞干擾其後續的操作功能和未經授權的存取，達到破壞資訊安全(CIA)，[34]成為誘餌(如圖10)。另一方面隨著科技進展無人機在空中監視和偵察能力，隱私問題也隨之產生，[35]此外根據這些攻擊進行分類(如表5)。

| Security objectives | System objectives | Attack methods |
|---|---|---|
| Confidentiality | Ground control station | Virus<br>Malware<br>Key loggers<br>Trojans |
| | UAV | Hijacking |
| | Communication link | Eavesdropping<br>Man-in-the-middle |
| Integrity | Communication link | Packet injection<br>Replay attack<br>Man-in-the-middle<br>Message detection |
| Availability | GCS<br>UAV<br>Communication | Denial of services (DoS)<br>Fuzzing<br>Jamming<br>Flooding<br>Buffer overflow<br>Denial of services |

圖 10 無人機通訊鏈路與安全需求（機密性、完整性、身份驗證、不可否認性）

資料來源：L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone. NIST IR 8105: Report on post-quantum cryptography. Technical report, National Institute of Standards and Technology (NIST), April 2016.

量子電腦的出現，能夠運用量子演算法對傳統密碼技術破解與影響。[36]傳統密碼主要缺點在於其系統之強韌性，完全依賴於所使用演算法的複雜性，而與通訊通道（傳統通道）無關。因此無法保證通訊鏈路之安全性，也無法檢測其中是否存在竊聽者，表5總結了無人機通訊協定、其相關加密機制及其在量子計算下的脆弱性。

傳統加密演算法需要被修改以增強抗量子攻擊的能力，或直接替換為能夠抵禦量子攻擊之後量子加密演算法(Post-Quantum Cryptography,PQC)作為相應措施。後量子加密(PQC)提供對量子攻擊的抵抗力，確保數據通訊和存儲長期安全性，成為發展抗量子攻擊演算法之關鍵領域(如圖11)。

34 H. Wang et al., “Survey on unmanned aerial vehicle networks: A cyber physical system perspective,” IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1027–1070, 2nd Quart., 2020.

35 A. Fitwi, Y. Chen, and S. Zhu, “No peeking through my windows: Conserving privacy in personal drones, ” in Proc. IEEE Int. Smart Cities Conf. (ISC2), Casablanca, Morocco, 2019, pp. 199–204.

36 KUBIGENOVA, AKKU, et al. "THE IMPACT OF QUANTUM COMPUTING (ALGORITHMS) ON CONTEMPORARY SECURITY SYSTEMS AND FUTURE. "Journal of Theoretical and Applied Information Technology, 102.15 (2024).

表5 UAV通訊協定、加密機制與量子攻擊綜合整理表

| Protocol | Cryptographic Scheme | Use in UAVs | Vulnerability to Quantum Attacks |
|---|---|---|---|
| MAVLink | RSA, AES | Secure UAV-GCS communication | RSA is vulnerable to Shor's Algorithm, AES to Grover's Algorithm. |
| SSL/TLS | RSA, ECC, AES | Encrypted data transmission between UAVs | RSA/ECC are vulnerable to Shor's Algorithm, AES weakened by Grover's Algorithm. |
| IEEE 802.11 | RSA, ECC, AES | Wireless communication between UAV and GCS | RSA/ECC are vulnerable to Shor's Algorithm, AES to Grover's Algorithm. |

資料來源：M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, "Future-proofing security for uavs with post-quantum cryptography: A review," IEEE Open Journal of the Communications Society, 2024.

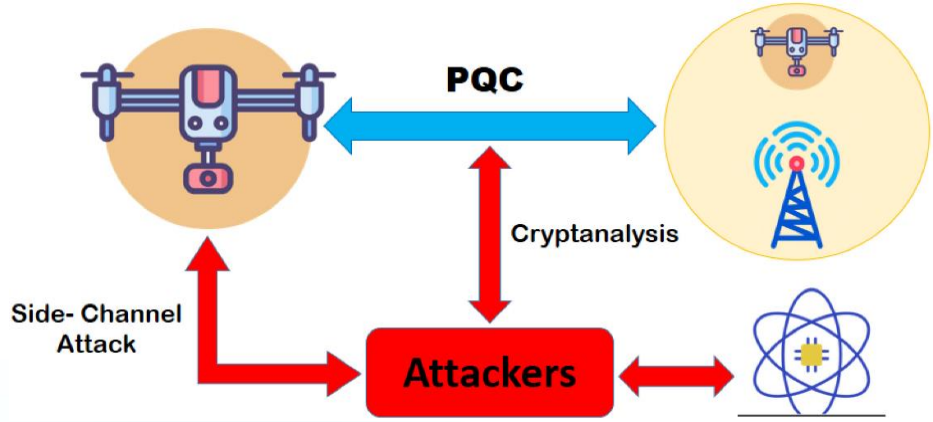


圖 11 量子計算機對無人機通訊的攻擊情境

資料來源：M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, "Futureproofing security for uavs with post-quantum cryptography: A review," IEEE Open Journal of the Communications Society, 2024.

## 後量子加密技術應用

PQC演算法涵蓋了一系列設計用於抵禦量子計算機攻擊的加密演算法，其主要包括基於格理論密碼學、代碼理論密碼學、雜湊函數密碼學、多元多項式密碼學，以及其他各類技術。以下針對PQC演算法背景與特性實施概述:

### 一、後量子加密標準化發展

美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)1970年代提出了選擇一種加密演算法作為全國通用標準的想法，並因此引入了數據DES演算法，於1997年被破解。隨後NIST再提案直到2000年，選定了AES作為對稱加密的標準並沿用至今。

量子計算機和量子密碼學的出現，威脅到了傳統密碼之安全性。美國國家安

全局（National Security Agency, NSA）2016年NIST啟動了一項標準化倡議，以選擇未來政府和行業可用的量子安全演算法，此提案被稱為「後量子密碼學」。

目前NIST標準化過程已進入第四輪評選階段，列入評選PQC演算法的條件是基於金鑰、密文和簽章之正確性、速度和大小，[37]目的在選出能夠抵抗量子計算能力的安全演算法。2022年NIST公布了PQC決選演算法，包括CRYSTALS-Kyber、CRYSTALS-Dilithium、FALCON（以NTRU為基礎的快速傅立葉格結構壓縮簽名）以及SPHINCS+，這些演算法因其在抗量子攻擊方面具備強大安全性、效率及確實可行性而被選中(PQC標準化過程如圖12所示)。[38]

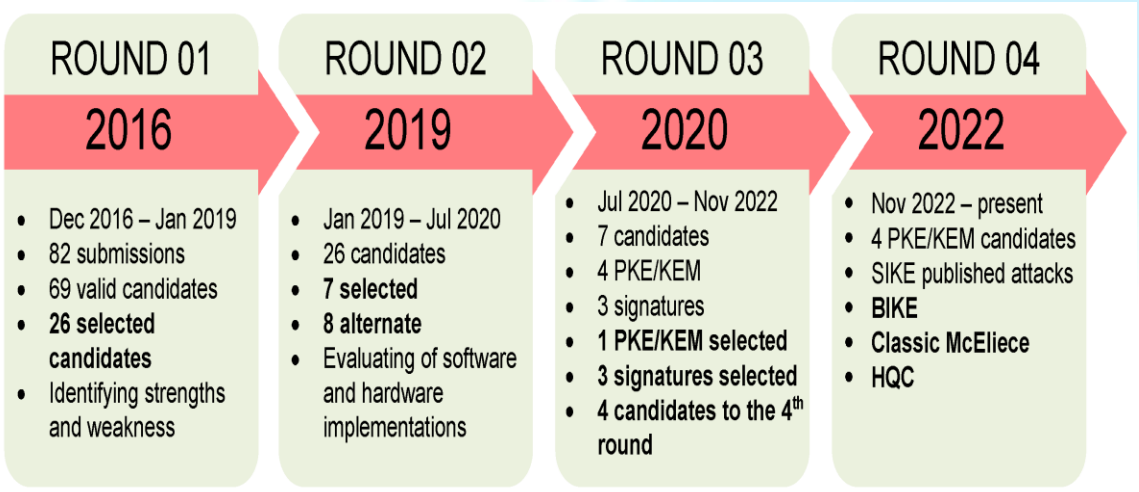


圖 12 NIST 的 PQC 標準化過程

資料來源：D. T. Dam, T. H. Tran, V. P. Hoang, C. K. Pham and T. T. Hoang, "A survey of post-quantum cryptography: Start of a new race", *Cryptography*, vol. 7, no. 3, pp. 40, 2023.

## 二、PQC技術適用性分析

PQC為因應量子計算，需要能抵禦的解決方案。以下是幾種主要加密技術(如圖13)與抗量子計算能力說明。[39]

(一)格基加密(Lattice-based Cryptography):[40]基於格理論的數學結構（如NTRUEncrypt和Kyber），提供了強大安全保障以及小型密鑰尺寸，具有高計算複

37 National Institute of Standards and Technology. (2016). Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

38 Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.-K.; Miller, C.; Moody, D.; et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process; Technical Report; National Institute of Standards and Technolog: Gaithersburg, MD, USA, 2022.

39 M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, “Future-proofing security for uavs with post-quantum cryptography: A review,” IEEE Open Journal of the Communications Society, 2024.

40 R. Overbeck and N. Sendrier, “Code-based cryptography. post-quantum cryptography/ed. bernstein dj, buchmann j., dahmene,” 2009.

雜度，適合無人機平台使用，已被廣泛研究和驗證。

(二)碼基加密(Code-based Cryptography):[41]基於糾錯碼的困難問題，(如McEliece和BIKE)提供了長期安全性和低計算開銷以其抗量子性著稱，非常適合資源受限的環境。

(三)雜湊基加密(Hash-based Cryptography):[42]利用安全的單向散列函數，特別適合數位簽章應用，結構簡單且易於分析安全性。

(四)多變量多項式加密(Multivariate Polynomial Cryptography):[43]基於多變量多項式方程求解的困難性，適合數位簽名和驗證用途。

(五)同態基加密(Isogeny-based Cryptography):[44]利用橢圓曲線同態映射的數學結構，具有較小的密鑰尺寸和高安全性。

(六)非交換性加密 (Non-commutative Cryptography):[45]基於非交換代數結構，如矩陣群和雙曲幾何結構，提供新型的安全框架。

(七)其他新興技術:包含混合模型與新型數學假設的研究方向，進一步強化抗量子攻擊能力。

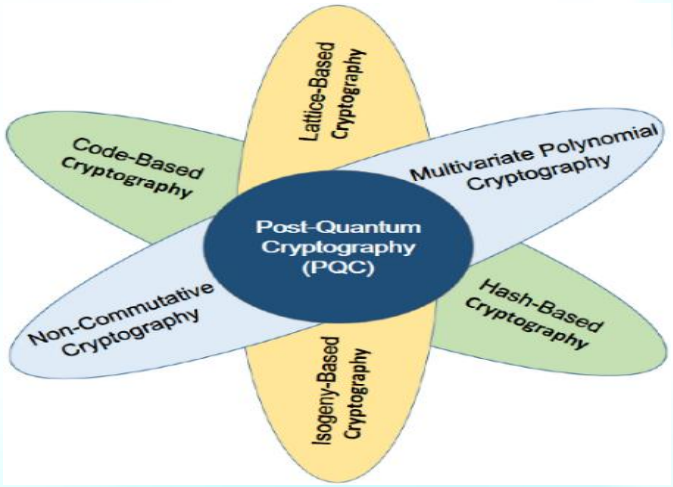


圖 13 PQC 的基本類型

資料來源：M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, "Future-proofing security for uavs with post-quantum cryptography: A review," IEEE Open Journal of the Communications Society, 2024.

41 V. Weger, N. Gassner, and J. Rosenthal, "A survey on code-based cryptography," arXiv preprint arXiv:2201 07119, 2022

42 J. Ding and A. Petzoldt, "Current state of multivariate cryptography," IEEE Security Privacy, vol. 15, no. 4,pp. 28–36, 2017.

43 C. Peng, J. Chen, S. Zeadally, and D. He, "Isogeny-based cryptography: a promising post-quantum techniq ue," IT Professional, vol. 21, no. 6, pp. 27–32, 2019.

44 S. Kanwal and R. Ali, "A cryptosystem with noncommutative platform groups," Neural Computing and Ap plications, vol. 29, pp. 1273–1278, 2018.

45 D. Deutsch, "Quantum theory, the church–turing principle and the univeRSA (Rivest–Shamir–Adleman)l qua ntum computer," in Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol100, no. 1818, 1985, pp. 97–117

## 三、傳統密碼與PQC比較

這些加密演算法，需根據指定參數與遵循NIST定義的安全等級，以確保能在一段時間內抵擋不同類型攻擊。

(一)功能性

PQC的目標是即使面對使用先進量子電腦進行攻擊的對手時，仍可保持原本安全加密基礎(Cryptographic Primitives)，[46]並提供以下優勢(如表6)：

1.抗量子攻擊能力:確保在量子電腦時代仍然有效。

2.保障長期安全性:確保數據通信與存儲的持久性與安全性，即使在量子計算能力大幅提升。

(二)安全性

傳統加密技術的安全性依賴於數學問題因式分解來實現安全性，從而抵禦量子計算攻擊。為了因應UAV中傳統加密漏洞，採用格、編碼或雜湊函數為基礎的量子安全加密技術(如Kyber和Dilithium)以抵禦量子攻擊，不僅提升了無人機通訊安全性，還提供可行解決方案。[47]

(三)主要區別：

密碼學之目標都是加密數據，確保其安全性、完整性和真實性。然而這些密碼技術在保護數據的方式上有著顯著差異。

1.數學複雜性與量子原理：

傳統密碼學和後量子密碼學依賴的是數學問題，這些問題對傳統計算機來說是計算困難的，而量子密碼學則利用量子力學之原理，提供與數學複雜性無關的優勢。

2.對量子計算的抵抗力：

後量子密碼學專門設計來抵抗量子計算的攻擊，利用量子計算無法高效解決之數學問題，而傳統密碼學本質上對量子演算法（如Shor演算法）存在脆弱性。

3.實用性與理論性：

傳統密碼學目前是主流，並廣泛應用於各種系統，而後量子密碼學則是為應對未來量子計算時代而提出的預防措施。量子密碼學目前處於實驗階段或早期部署階段，雖然QKD等技術正在測試中，但還未廣泛部署。

4.不同於量子密碼學(Quantum Cryptography, QC)或量子密鑰分配(Quantum Key distribution, QKD)，後量子密碼學使用現有電腦與網路，不依靠

46 T. R. N. G. S. Or and A. Q. AdveRSA (Rivest–Shamir–Adleman)ries, “Certifiable quantum dice,” 2012. [16] X. Wang, G. Xu, and Y. Yu, “Lattice-based cryptography: A survey,” Chinese Annals of Mathematics,Series B, vol. 44, no. 6, pp. 945–960, 2023.

47 Z. Liu, K.-K.-R. Choo, and J. Grossschadl, “Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography,” IEEE Commun. Mag., vol. 56, no. 2, pp. 158–162, Feb. 2018.

量子力學。

這些後量子加密方法為抗量子攻擊加密提供了多種可行途徑，表6提供了選定用於標準化的PQC並概述其主要特性、挑戰及當前狀態。[48]

表 6　PQC 主要特性

| Algorithm | Type | Key Features | Challenges | NIST Status |
|---|---|---|---|---|
| CRYSTALS-Kyber | KEM | Ring-LWE problem, efficient polynomial operations, compact key sizes, FFT | Side-channel attack susceptibility, complex implementation, cryptanalysis resistance | Finalist |
| CRYSTALS-Dilithium | Digital Signature | Module-lattice problems, efficient and fast signing/verification | Large signature sizes, side-channel vulnerabilities, cryptanalytic advances | Finalist |
| FALCON | Digital Signature | NTRU lattice problem, compact signature sizes, FFT | Side channel attack resistance, complexity of implementation, cryptanalysis resilience | Finalist |
| SPHINCS+ | Digital Signature | Hash-based, stateless, no number-theoretic assumptions | Large signatures and public keys, resource intensity, implementation complexity | Finalist |
| Classic McEliece | KEM | Code-based, uses Goppa codes, long-term reliability | Large public key sizes, computational complexity, adoption resistance | Alternate |
| SIKE | KEM | Supersingular isogenies, small key sizes | Slow performance, complex arithmetic operations, implementation difficulty, cryptanalysis advances | Alternate |
| BIKE | KEM | Syndrome decoding, QC-MDPC codes, robustness | Implementation efficiency, side channel resistance, cryptanalysis threats, error correction | Alternate |
| HQC | Public Key Encryption | Quasi-cyclic codes, strong security features | Performance and side-channel resistance | Alternate |

資料來源：Khan, Muhammad Asghar, et al. "Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review."IEEE Transactions on Network and Service Management(2024).

## 四、PQC效能與挑戰

(一)與現有UAV加密機制比較(如表7)

1.傳統加密演算法：基於傳統數學問題，如離散對數、整數分解和橢圓曲線離散對數，這些算法對傳統計算機來說是安全的。然而，隨著量子計算技術發展，這些算法將面臨來自量子算法（如Shor演算法）之重大挑戰，從而無法保證長期的安全性。

2.量子計算：量子計算能顯著提升某些數學問題的計算效率，對傳統的密鑰算法構成威脅。特別是Shor演算法可以高效解決整數分解和離散對數問題，

48 Khan, Muhammad Asghar, et al. "Security and Privacy Issues and Solutions for UAVs in B5G Networks:A Review."IEEE Transactions on Network and Service Management(2024).

對RSA、Diffie-Hellman 和ECDH等算法造成致命打擊。

3.後量子加密演算法：為了對抗量子計算的威脅，後量子密碼（如KYBER、NTRU、FrodoKEM）已經被提出並進入標準化過程。這些算法基於難以破解的數學問題，如格理論，對量子計算具有更強之抗性，並能在量子計算環境中保持長期的安全性。

後量子密鑰協商算法的實施，將能夠確保在量子計算普及後，依舊能夠保護數據免受攻擊，並且支持更安全之網絡通信和數據加密。

表 7 傳統、量子計算與後量子密碼演算法比較

| 區分 | 傳統密鑰協商算法 | 量子計算 | 後量子密鑰協商算法 |
|---|---|---|---|
| 算法類型 | 基於數學問題（如離散對數、整數分解、橢圓曲線） | 量子計算能夠解決傳統算法的基本數學問題 | 基於量子計算抗性的數學問題（如格理論、LWE） |
| 常見算法 | RSA, Diffie-Hellman, ECDH, ECDSA | Shor演算法能高效破解 RSA、Diffie-Hellman、ECDH | KYBER, NTRU, FrodoKEM, SIKE等 |
| 安全性基礎 | 離散對數問題、整數分解問題、橢圓曲線離散對數問題 | 量子計算能快速解決上述問題，威脅到傳統算法的安全性 | 基於格理論或其他量子抗性數學問題，不易被量子計算破解 |
| 密鑰長度 | RSA：3072 位元；DH：3072 位元；ECDH：P-384 | 量子計算使得這些密鑰長度不再足夠安全 | KYBER 512（相當於 AES-128）；KYBER 1024（相當於 AES-256） |
| 量子抗性 | 易受 Shor 演算法攻擊，特別是 RSA 和 DH | 量子計算可破解這些算法，導致數據洩露和身份偽造 | 強抗量子攻擊，能抵禦量子計算的解密和簽名偽造 |
| 運行效率 | 高效，廣泛應用於各種系統中 | 量子計算在某些情況下能實現更高效的解密，但需要高效的量子電腦 | 後量子算法如 KYBER 等在大部分情況下具有競爭力，並保持較高的性能 |
| 應用領域 | 用於現有的加密協定，如 TLS、VPN、電子支付等 | 量子計算尚未廣泛實現，但未來會對現有加密協定帶來威脅 | 用於未來的量子抗性加密協定和系統，特別是網絡通信和數據保護 |
| 未來發展 | 目前是主流，但面臨量子計算威脅 | 量子計算可能在未來 10-20 年內實現，改變現有加密方法 | 後量子密碼學已進入標準化過程，已經成為下一代加密方案 |

資料來源：作者整理

(二)未來挑戰：[49]

1.運算資源需求：PQC算法通常需要更高計算資源，這對於處理能力有限的UAV來說，可能會影響其性能和續航能力。

2.延遲問題：由於PQC算法可能涉及更複雜的計算過程，這可能導致通信延遲，對即時操作的UAV來說是一項挑戰。

3.兼容性與過渡期：目前大多數現有系統使用傳統的加密算法，導入PQC需要確保新的密碼學方法能夠與現有基礎設施兼容，並且在過渡期間保持安全性。

4.能效與功耗：PQC算法通常需要更多的計算資源，這可能會消耗更多能源，對於UAV續航能力會構成挑戰。

5.硬體支持：許多現有UAV平台並未設計來支持PQC算法，這可能需要額外的硬體升級或特殊設計，以確保加密過程之高效執行。

6.標準化與互操作性：PQC尚在標準化過程中，對於不同的UAV製造商和操作環境，確保跨平台的互操作性仍然是挑戰之一。

7.安全性與抗攻擊性：雖然PQC被認為能抵禦量子計算機之攻擊，但新算法的安全性和抗攻擊性仍需要在實際應用中進行測試和驗證。

## 結論

在當今網際網路普及環境中，隱私與通訊安全變得至關重要。然而隨著量子計算技術之發展，傳統公鑰加密機制（如RSA與ECC）將面臨被破解的風險，使得UAV通訊鏈路之安全性受到嚴重威脅。為此，PQC成為保護UAV通訊安全的重要研究方向。

本研究探討PQC在UAV通訊中的應用，分析傳統加密系統在量子計算機時代之脆弱性，並比較不同類型PQC演算法（如基於格、碼、哈希與多變數的方案）在UAV通訊環境中的適用性。本文針對UAV安全需求，包括戰場與災害應變環境下之通訊挑戰，以及UAV與地面控制站、其他UAV之間的通訊模式。我們進一步評估PQC技術之安全性與效能，並與現有加密機制進行比較。

PQC技術不僅能夠有效提升UAV通訊鏈路安全性，且部分基於格的密碼學方案（如CRYSTALS-Kyber）在資源受限的UAV環境下亦具備可行性。未來的研究可進一步探索PQC與輕量級加密技術的結合，並驗證其在實際UAV網路中部署之可行性。

49 M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, “Future-proofing security for uavs wit hpost-quantum cryptography: A review,” IEEE Open Journal of the Communications Society, 2024.

## 參考文獻


一、Khan, M.A.; Kumar, N.; Mohsan, S.A.H.; Khan, W.U.; Nasralla, M.M.; Alsharif, M.H.; Zywiołek, J.; Ullah, I. Swarm of UAVs for • network management in 6G: A technical review. IEEE Trans. Netw. Service Manag. 2022, 20, 741－761.。

二、D. Mishra, A. M. Vegni, V. Loscri, and E. Natalizio, "Drone Networking in the 6G Era: A Technology Overview," IEEE Communications Standards Magazine, vol. 5, no. 4, pp. 88－95, 2021.

三、B. Alzahrani, O. S. Oubbati, A. Barnawi, M. Atiquzzaman, and D. Alghazzawi, "UAV assistance paradigm: State-of-the-art in applications and challenges," Journal of Network and Computer Applications, vol. 166, p. 102706, 2020.

四、H. Wang et al., "Survey on unmanned aerial vehicle networks: A cyber physical system perspective," IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1027－1070, 2nd Quart., 2020

五、Khan, Muhammad Asghar, et al. "Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review."IEEE Transactions on Network and Service Management(2024).

六、J. Whelan, A. Almehmadi, J. Braverman and K. El-Khatib, "Threat Analysis of a long range autonomous unmanned aerial system," in Proc. 2020 Int. Conf. on Computing and Information Technology, Tabuk, Saudi Arabia, pp. 1－5, 2020

七、U. Challita, A. Ferdowsi, M. Chen, and W. Saad, "Machine learning for wireless connectivity and security of cellular-connected UAVs, " IEEE Wireless Commun., vol. 26, no. 1, pp. 28－35, Feb. 2019.

八、4Y. Mekdad et al., "A survey on security and privacy issues of UAVs," 2021, arXiv:2109.14442v2.

九、E. T. Michailidis and D. Vouyioukas, "A review on software-based and hardware-based authentication mechanisms for the Internet of Drones," Drones, vol. 6, no. 2, p. 41, 2022

十、Ahmad, A., Ordoñez, J., Cartujo, P., & Martos, V. (2021) . Remotely Piloted Aircraft (RPA) in Agriculture: A Pursuit of Sustainability. Agronomy, 11(1), 7

十一、Dalamagkidis, K.; Valavanis, K.P.; Piegl, L.A. On Integrating Unmanned Aircraft Systems into the National Airspace System: Issues, Challenges, Operational Restrictions, Certification, and Recommendations; Springer Science & Business Media: Berlin/Heidelberg, ermany, 2011; Volume 54.

十二、J. Gertler, "US unmanned aerial systems," Library of Congress Washington DC Congressional Research Service, vol. 1, no. 1, pp. 1－10, 2012.

十三、T. Samad, J. S. Bay and D. Godbole, "Network-centric systems for military operations in urban terrain: The role of UAVs," Proc. of the IEEE, vol. 95, no. 1, pp. 92－107, 2007.

十四、V. Roberge, M. Tarbouchi and G. Labonté, “Fast genetic algorithm path p lanner for fixed-wing military UAV using GPU,” IEEE Transactions on Aero space and Electronic Systems, vol. 54, no. 5, pp. 2105－2117, 2018.
十五、D. Orfanus, E. P. de Freitas and F. Eliassen, “Self-organization as a supp orting paradigm for military UAV relay networks,” IEEE Communications Le tters, vol. 20, no. 4, pp. 804－807, 2016.
十六、M. Saleh, N. Jhanjhi and A. Abdullah, “Proposing a privacy protection m odel in case of civilian drone,” in Proc. 2020 22nd Int. Conf. on Advanced Communication Technology, Phoenix Park, South Korea, pp. 596－602, 2020.
十七、G. Quiroz and S. J. Kim, “A confetti drone: Exploring drone entertainmen t,” in Proc. 2017 IEEE Int. Conf. on Consumer Electronics, Las Vegas, US A, pp. 378－381, 2017
十八、A. Gurtner, D. G. Greer, R. Glassock, L. Mejias, R. A. Walker et al., “I nvestigation of fish-eye lenses for small-UAV aerial photography,” IEEE Tra nsactions on Geoscience and Remote Sensing, vol. 47, no. 3, pp. 709－721, 2 009.
十九、D. Murugan, A. Garg and D. Singh, “Development of an adaptive approac h for precision agriculture monitoring with drone and satellite data,” IEEE Jo urnal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 10, no. 12, pp. 5322－5328, 2017.
二十、A. M. Jawad, H. M. Jawad, R. Nordin, S. K. Gharghan, N. F. Abdullah et al., “Wireless power transfer with magnetic resonator coupling and sleep/acti ve strategy for a drone charging station in smart agriculture,” IEEE Access, vol. 7, no. 1, pp. 139839－139851, 2019.
二一、E. Natalizio, N. R. Zema, E. Yanmaz , L. D. P. Pugliese and F. Guerriero , “Take the field from your smartphone: Leveraging UAVs for event filming, ” IEEE Transactions on Mobile Computing, vol. 19, no. 8, pp. 1971－1983, 2019.
二二、I. Bor-Yaliniz, S. S. Szyszkowicz and H. Yanikomeroglu, “Environment-aw are drone-base-station placements in modern metropolitans,” IEEE Wireless C ommunications Letters, vol. 7, no. 3, pp. 372－375, 2017.
二三、N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, R. S. A. Usmani and A. Nayyar, “Smart traffic monitoring system using unmanned aerial vehicles (UAVs),” C omputer Communications, vol. 157, no. 1, pp. 434－443, 2020
二四、A. N. Chaves, P. S. Cugnasca and J. Jose, “Adaptive search control appli ed to search and rescue operations using unmanned aerial vehicles (UAVs),” I EEE Latin America Transactions, vol. 12, no. 7, pp. 1278－1283, 2014.
二五、D. Wang, P. Hu, J. Du, P. Zhou, T. Deng et al., “Routing and schedulin g for hybrid truck-drone collaborative parcel delivery with independent and tru ck-carried drones,” IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10483

－10495, 2019
二六、Dalamagkidis, K.; Valavanis, K.P.; Piegl, L.A. On Integrating Unmanned Aircraft Systems into the National Airspace System: Issues, Challenges, Operational Restrictions, Certification, and Recommendations; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2011; Volume 54
二七、Dario Floreano and Robert J Wood. Science, technology and the future of small autonomous drones. Nature, 521(7553):460－466, 2015.
二八、Z. Wang, Y. Li, S. Wu, Y. Zhou, L. Yang, Y. Xu, T. Zhang, and Q. Pan, "A survey on cybersecurity attacks and defenses for unmanned aerial systems," Journal of Systems Architecture, vol. 138, p. 102870, 2023.
二九、B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, ' 'SoK－security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps,' ' 2019, arXiv:1903.05155. [Online]. Available: http://arxiv.org/abs/1903.05155
三十、M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, "Future-proofing security for uavs with post-quantum cryptography: A review," IEEE Open Journal of the Communications Society, 2024.
三一、R. Gupta, A. Nair, S. Tanwar, and N. Kumar, ' 'Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and hallenges,' ' IET Commun., vol. 15, no. 10, pp. 1352－1367, 2021
三二、A. Shafique, A. Mehmood, and M. Elhadef, ' 'Survey of security protocols and vulnerabilities in unmanned aerial vehicles,' ' IEEE Access, vol. 9, pp. 46927－46948, 2021.
三三、A. Shafique, A. Mehmood, and M. Elhadef, ' 'Survey of security protocols and vulnerabilities in unmanned aerial vehicles,' ' IEEE Access, vol. 9, pp. 46927－46948, 2021.
三四、Z. Hercigonja, "Comparative analysis of cryptographic algorithms," International Journal of Digital Technology & Economy, vol. 1, no. 2, pp. 127－134, 2016.
三五、P. Hämäläinen, M. Hännikäinen, and T. D. Hämäläinen, "Review of hardware architectures for advanced encryption standard implementations considering wireless sensor networks," in International Workshop on Embedded Computer Systems. Springer, 2007, pp. 443－453.
三六、S.-S. Wang and W.-S. Ni, "An efficient fpga implementation of advancedencryption standard algo rithm," in 2004 IEEE International Symposium on Circuits and Systems (ISCAS), vol. 2 IEEE, 2004, pp. II－597.
三七、E. E. Nithila, A. Rosi et al., "A survey about post quantum cryptography methods," EAI Endorsed Transactions on Internet of Things, vol. 10, 2024.
三八、Standard, NIST FIPS, Data Encryption Standard (DES). Federal Information Processing Standards Publication, 1999, 46-3.

三九、Standard, NIST FIPS, Advanced Encryption Standard (AES). Federal Information Processing Standards Publication, 2001, 197.
四十、S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, ‘‘A comparative survey of symmetric and asymmetric key cryptography,’’ in Proc. Int. Conf. Electron., Commun. Comput. Eng. (ICECCE), Nov. 2014, pp. 83–93.
四一、Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21(2), 120–126 (1978)
四二、P. W. Shor, ‘‘Quantum computing,’’ Documenta Math., vol. 1, no. 1000, p. 1, 1998
四三、Nofer, M., Bauer, K., Hinz, O., van der Aalst, W., & Weinhardt, C. (2023). Quantum Computing. Business & Information Systems Engineering, 65(4), 361-367.
四四、S. T. Marella and H. S. K. Parisa, “Introduction to quantum computing,” Quantum Computing and Communications, 2020.
四五、S. Chen, S. Sun and S. Kang, ” System integration of terrestrial mobile communication and satellite communication —the trends, challenges and key technologies in B5G and 6G,” in China Communications, vol. 17, no. 12, pp. 156-171, Dec. 2020.
四六、M. Moller and C. Vuik, “On the impact of quantum computing ¨ technology on future developments in high-performance scientific computing, ” Ethics and information technology, vol. 19, pp. 253–269, 2017.
四七、M. A. Nielsen and I. L. Chuang, “Quantum computation and quantum information,” Phys. Today, vol. 54, no. 2, p. 60, 2001
四八、V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The Impact of Quantum Computing on Present Cryptography, " International Journal of Advanced Computer Science and Applications, vol. 9, 2018.
四九、V. K. Ralegankar, J. Bagul, B. Thakkar, R. Gupta, S. Tanwar, . Sharma, and I. E. Davidson, “Quantum cryptography-as-a-service for secure uav communication: Applications, challenges, and case study,” IEEE Access, 2021.
五十、Tychola, Kyriaki A., and Konstantinos Rantos. "Cyberthreats and Security Measures in Drone-Assisted Agriculture."Electronics14.1 (2025): 149.
五一、S. Hayat, E. Yanmaz, and R. Muzaffar, “Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint,” IEEE Commun. Surveys Tuts., vol. 18, no. 4, pp. 2624–2661, 4th Quart.2016.
五二、A. Shafique, A. Mehmood, and M. Elhadef, ‘Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles’, IEEE Access, vol. 9, pp.46927–46948, 2021
五三、L. Wang, Y. Chen, P. Wang, and Z. Yan, ‘Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications’, IEEE Communicatio

ns Standards Magazine, vol. 5, no. 4, pp. 41－47, 2021.
五四、B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, ‘SoK － Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps’ , ArXiv, vol. abs/1903.05155, 2019.
五五、J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, ‘ ‘Security analysis of drones systems: Attacks, limitations, and recommendations,’ ’ Internet Things, vol. 11, Sep. 2020, Art. no. 100218.
五六、A. Shoufan, H. AlNoon and J. Baek, “Secure communication in civil drones,” in Int. Conf. on Information Systems Security and Privacy, cham, Springer, pp. 177－195, 2015.
五七、Khan, Muhammad Asghar, et al. "Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review. " IEEE Transactions on Network and Service Management(2024).
五八、R. Asif, "Post-Quantum Cryptosystems," MDPI, 29 January 2021
五九、K. Dalamagkidis, K. P. Valavanis, and L. A. Piegl, On integrating unmanned aircraft systems into the national airspace system: issues, challenges, operational restrictions, certification, and recommendations. springer science & Business Media, 2011, vol. 54.
六十、S. Javed et al., “ An efficient authentication scheme using blockchain asacertificate authority for the Internet of Drones,” Drones, vol. 6, no. 10, p. 264, 2022.
六一、S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, “Survey on collaborative smart drones and Internet of Things for improving smartness of smart cities,” IEEE Access, vol. 7, pp. 128125－128152, 2019.
六二、A. Ali et al., “A privacy-preserved Internet-of-Medical-Things scheme foreradication and control of dengue using UAV,” Micromachines, vol. 13, no. 10, p. 1702, Oct. 2022.
六三、N. S. Labib, M. R. Brust, G. Danoy, and P. Bouvry, “The rise of drones in Internet of Things: A survey on the evolution , prospects and challenges of unmanned aerial vehicles,” IEEE Access, vol. 9, pp. 115466－115487, 2021.
六四、M. U. Bokhari and Q. M. Shallal, “A review on symmetric key encryption techniques in cryptography,” International journal of computer applications,vol. 147, no. 10, 2016.
六五、K. Saranya, R. Mohanapriya, and J. Udhayan, “A review on symmetric key encryption techniques in cryptography,” International Journal of Science, Engineering and Technology Research (IJSETR), vol. 3, no. 3, pp. 539－544, 2014.
六六、M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, “Symmetric encryption algorithms: Review and evaluation study,” International Journal of Communication Networks and Information Security, vol. 12, no. 2, pp. 256－272,

2020.
六七、B. Halak, Y. Yilmaz, and D. Shiu, “Comparative analysis of energy costs of asymmetric vs symmetric encryption-based security applications,” IEEE Access, vol. 10, pp. 76 707－76 719, 2022.
六八、A. A.-R. El-Douh, S. F. Lu, A. A. Elkouny, and A. Amein, “Hybrid cryptography with a one－time stamp to secure contact tracing for covid－19 infection,” International Journal of Applied Mathematics and Computer Science,vol. 32, no. 1, pp. 139－146, 2022.
六九、J. Edney and W. Arbaugh, “Real 802.11 Security: Wi-Fi Protected Access and 802.11i”, Addison-Wisley, 2003.
七十、T. Hardjono and L. R. Dondeti, Security in Wireless LANS and MANS (Artech House Computer Security). Artech House, Inc., 2005.
七一、G. Singh and Supriya, “A study of encryption algorithms (RSA (Rivest－Shamir－Adleman), des, 3des and aes ) for information security,” International Journal of Computer Applications, vol. 67, pp. 33－38, 2013.
七二、D. J. Bernstein, “Introduction to post-quantum cryptography,” in Post-Quantum Cryptography, Berlin, Germany: Springer, 2009, pp. 1－14.
七三、D. J. Bernstein and T. Lange, “ Post-quantum cryptography,” Nature, vol.549, no. 7671, pp. 188－194, 2017.
七四、Don Jelle, et al. Security of the Fiat-Shamir Transformation in the quantumrandom-Oracle model. Advances in Cryptology － CRYPTO 2019 2019:356－83
七五、Gisin Nicolas, et al. Quantum cryptography. Rev Mod Phys 2002;74(1):145－95
七六、Banerjee Utsav, et al. Accelerating post-quantum cryptography using an Energyefficient TLS Crypto-Processor. 2020 IEEE International Symposium on Circuits and Systems (ISCAS) 2020.
七七、Roma, Crystal Andrea, et al. “Energy efficiency analysis of post-quantumcryptographic algorithms.” IEEE Access, vol. 9, 2021, pp. 71295－71317.
七八、L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone. NIST IR 8105: Report on post-quantum cryptography. Technical report, National Institute of Standards and Technology (NIST), April 2016.
七九、Niraula, Tohfa, Aditi Pokharel, Ashmita Phuyal, Pratistha Palikhel, and Manish Pokharel. " Quantum computers’ threat on current cryptographic measures and possible solutions." Int. J. Wirel. Microw. Technol 12, no. 5 (2022).10-20.
八十、P. S. Barreto et al., “A panorama of post-quantum cryptography,” in Open Problems in Mathematics and Computational Science, Cham, Switzerland: Springer, 2014, pp. 387－439.
八一、D. Joseph et al., “Transitioning organizations to post-quantum cryptography,” Nature, vol. 605, pp. 237－243, May 2022.
八二、H. J. Hadi, Y. Cao, S. Li, Y. Hu, J. Wang, and S. Wang, “Real-time collaborative intrusion detection system in uav networks using deep learning,” I

EEE Internet of Things Journal, 2024.
八三、H. J. Hadi and Y. Cao,” Cyber Attacks and Vulnerabilities Assessment fo r Unmanned Aerial Vehicles Communication Systems,” 2022 nternational Con ference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 20 22, pp. 213-218.
八四、J. Whelan, A. Almehmadi, J. Braverman and K. El-Khatib, “Threat Analys is of a long range autonomous unmanned aerial system,” in Proc. 2020 Int.C onf. on Computing and Information Technology, Tabuk, Saudi Arabia, pp. 1－5, 2020.
八五、M. Kratky and V. Minarik, “The non-destructive methods of fight against UAVs,” in Proc. Int. Conf. Mil. Technol., Brno, Czech Republic, 2017, pp.6 90－694.
八六、Z. Birnbaum, A. Dolgikh, V. Skormin, E. O’Brien, D. Muller, and C. Str acquodaine, “Unmanned aerial vehicle security using behavioral profiling,” i n Proc. Int. Conf. Unmanned Aircraft Syst., Denver, CO, USA, 2015, pp. 131 0－1319
八七、R. Altawy and A. M. Youssef, “Security, privacy, and safety aspects of c ivilian drones: A survey,” ACM Trans. Cyber-Phys. Syst., vol. 1, no. 2, pp.1 －25, 2017
八八、S. G. Casals, P. Owezarski, and G. Descargues, “ Generic and autonomou ssystem for airborne networks cyber-threat detection,” in Proc. IEEE/AIAA 3 2nd Digit. Avionics Syst. Conf., East Syracuse, NY, USA, 2013, pp. 4A4-1－ 4A4-14
八九、P. P. Angelov, Sense and Avoid in UAS: Research and Applications. Hobo ken, NJ, USA: Wiley, 2012
九十、J. A. Marty, “ Vulnerability analysis of the mavlink protocol for comman dand control of unmanned aircraft,” Air Force Institute of Technology, Tech. Rep., 2013.
九一、M. Leccadito, T. Bakker, R. Klenke, and C. Elks, “A survey on securing UAS cyber physical systems,” IEEE Aerosp. Electron. Syst. Mag., vol. 33, n o. 10, pp. 22－32, Oct. 2018
九二、H. Wang et al., “Survey on unmanned aerial vehicle networks: A cyber p hysical system perspective,” IEEE Commun. Surveys Tuts., vol. 22, no. 2, p p. 1027－1070, 2nd Quart., 2020.
九三、A. Fitwi, Y. Chen, and S. Zhu, “No peeking through my windows: Conse rving privacy in personal drones,” in Proc. IEEE Int. Smart Cities Conf. (IS C2), Casablanca, Morocco, 2019, pp. 199－204.
九四、A. Allouch, O. Cheikhrouhou, A. Koubâa, M. Khalgui, T. Abbes, MAVSec: Securing the MAVLink protocol for Ardupilot /PX4 unmanned aerial systems,i n International Wireless Communications & Mobile Computing Conference, IE

EE, 2019, pp. 621－628.
九五、N. A. Khan, S. N. Brohi and N. Z. Jhanjhi, “UAV’s applications, architecture, security issues and attack scenarios: A survey,” in Intelligent Computing and Innovation on Data Science. Berlin, Germany: Springer, pp. 753－760, 2020.
九六、Khan, N.A.; Jhanjhi, N.Z.; Brohi , S.N.; Almazroi, A.A.; Almazroi, A.A. A secure communication protocol for unmanned aerial vehicles. CMC-COMPUTERS MATERIALS CONTINUA 2022, 70, 601－618.
九七、KUBIGENOVA, AKKU, et al. "THE IMPACT OF QUANTUM COMPUTING (ALGORITHMS) ON CONTEMPORARY SECURITY SYSTEMS AND FUTURE. "Journal of Theoretical and Applied Information Technology, 102.15(2024).
九八、D. J. Bernstein, “Introduction to post-quantum cryptography,” in Post-quantum cryptography. Springer, 2009, pp. 1－14.
九九、D. J. Bernstein and T. Lange, “Post-quantum cryptography,” Nature, vol. 549, no. 7671, pp. 188－194, 2017.
一００、P. S. Barreto, F. Piazza Biasi, R. Dahab, J. C. Lopez-Hern andez, E. M. de Morais, A. D. S. de Oliveira, G. C. Pereira, and J. E. Ricardini, “A panorama of post-quantum cryptography,” Open Problems in Mathematics and Computational Science, pp. 387－439, 2014.
一０一、D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, “ransitioning organizations to post-quantum cryptography,” Nature, vol. 605, no. 7909, pp. 237－243, 2022.
一０二、M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, “Futureproofing security for uavs with post-quantum cryptography: A review,” IEEE Open Journal of the Communications Society, 2024.
一０三、National Institute of Standards and Technology. (2016). Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf
一０四、Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.-K.; Miller, C.; Moody, D.; et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process; Technical Report; National Institute of Standards and Technolog: Gaithersburg, MD, USA, 2022.
一０五、D. T. Dam, T. H. Tran, V. P. Hoang, C. K. Pham and T. T. Hoang, "A survey of post-quantum cryptography: Start of a new race",Cryptography, vol.7, no. 3, pp. 40, 2023.
一０六、R. Overbeck and N. Sendrier, “Code-based cryptography. post-quantum c

ryptography/ed. bernstein dj, buchmann j., dahmene,” 2009.
一0七、V. Weger, N. Gassner, and J. Rosenthal, “A survey on code-based cryp tography,” arXiv preprint arXiv:2201.07119, 2022
一0八、M. D. Noel, V. O. Waziri, S. M. Abdulhamid, and J. A. Ojeniyi, “Rev iew and analysis of classical algorithms and hash-based post-quantum algorith m,” Journal of Reliable Intelligent Environments, pp. 1 – 18, 2021
一0九、J. Ding and A. Petzoldt, “Current state of multivariate cryptography,” I EEE Security Privacy, vol. 15, no. 4, pp. 28 – 36, 2017.
一一0、C. Peng, J. Chen, S. Zeadally, and D. He, “Isogeny-based cryptography: a promising post-quantum technique,” IT Professional, vol. 21, no. 6, pp. 27 – 32, 2019.
一一一、S. Kanwal and R. Ali, “A cryptosystem with noncommutative platformg roups,” Neural Computing and Applications, vol. 29, pp. 1273 – 1278, 2018.
一一二、D. Deutsch, “Quantum theory, the church – turing principle and the univ eRSA (Rivest – Shamir – Adleman)l quantum computer,” in Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 100, n o. 1818, 1985, pp. 97 – 117
一一三、National Institute of Standards and Technology. Federal Information Proce ssing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules (with Change Notice 2). 2001. Available online: https://csrc.nist.gov/publications /detail/fips/140/2/final (accessed on 20 January 2025).
一一四、T. R. N. G. S. Or and A. Q. AdveRSA (Rivest – Shamir – Adleman)ries, “Certifiable quantum dice,” 2012. [16] X. Wang, G. Xu, and Y. Yu, “Lat tice-based cryptography: A survey,” Chinese Annals of Mathematics, Series B , vol. 44, no. 6, pp. 945 – 960, 2023.
一一五、Z. Liu, K.-K.-R. Choo, and J. Grossschadl, ‘ ‘Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography,’ ’ IEEE Commun. Mag., vol. 56, no. 2, pp. 158 – 162, Feb. 2018.
一一六、**Daniele Micciancio and Oded Regev. Lattice-based cryptography. I n Post-quantum cryptography, pages 147–191. Springer, 2009.**

## 作者簡介

蔣河山，國防大學資訊科學研究所碩士、國防大學國防科學研究所博士，曾任國防大學資訊部門主管。現任TASC臺灣應用軟體股份有限公司專業團隊成員，並兼任龍華科技大學資訊網路工程系助理教授。研究專長包括資通安全、資訊系統規劃與管理，以及自動化製造系統之應用等領域。