

資訊工程學系 特殊選才申請

自學實作白皮書報告

從 BB84 到混合式量子防禦：

QKD 與 PQC 模擬應用與攻擊分析


申請人：李佳穎(Kailyn)

撰寫日期：中華民國 114 年 7 月-8 月初

摘要 (Abstract)

本研究聚焦於量子資安的實務模擬與應用，透過 Python 實作量子密鑰分發協定、攻擊模擬以及錯誤率分析，展現協定在不同攻擊下的安全性變化。同時，本研究亦探索結合傳統與新興密碼技術的安全架構，模擬其在國防、產業與金融場景的潛在應用。為了呼應國際趨勢，本研究亦參考國際標準，並對比中國、歐盟、瑞士及韓國的量子網路與安全應用案例，進一步提出台灣在軍事、產業與金融體系的應用建議。

然而，本研究仍存在限制：模擬僅於軟體層進行，未涵蓋硬體環境下的通道損耗、光子源效率與完整攻擊模型。儘管如此，透過本研究所建構的混合架構與模擬測試，仍能為台灣的量子資安策略提供先導性驗證與技術起點，並凸顯跨領域落地的潛力。

 完整白皮書與程式碼

 [GitHub 專案：BB84-Simulation](#)

(白皮書 PDF 請見專案檔案列表)



目錄 (Table of Contents)

摘要 (Abstract)	i
第一章 研究動機與背景 (Chapter 1 Research Motivation and Background)	1
第二章 實作方法與模擬設計 (Chapter 2 Methodology and Simulation Design)	2、3
第三章 混合式安全架構概念模擬 (Chapter 3 Hybrid Security Architecture Simulation)	4
第四章 紅隊挑戰與未來攻擊模型 (Chapter 4 Red Team Challenges and Future Attack Models)	5 - 9
第五章 標準趨勢與應用落地模擬 (Chapter 5 Standardization Trends and Practical Applications)	10 - 14
第六章 實作歷程與個人反思 (Chapter 6 Implementation Process and Personal Reflection)	15、16
第七章 GitHub 附錄與技術資訊 (Chapter 7 GitHub Appendix and Technical Information)	16、17
第八章 未來展望與進行中研究 (Chapter 8 Future Outlook and Ongoing Research)	17
第九章 結語 (Chapter 9 Conclusion)	17
附錄 A 學習過程補充與對話紀錄 (Appendix A - Supplementary Learning Process and Dialogue Records)	18 - 20
參考文獻 (References)	21

圖表目錄 | List of Figures & Tables

第一章 研究動機與背景 (Chapter 1 Research Motivation and Background)

圖 1.1	RSA 加密流程 (RSA Encryption)	1
-------	---------------------------	---

第二章 實作方法與模擬設計 (Chapter 2 Methodology and Simulation Design)

圖 2.1	QBER 與攔截比例 (QBER vs. Intercept Ratio)	2
-------	---------------------------------------	---

第三章 安全架構概念模擬 (Chapter 3 Hybrid Security Architecture Simulation)

圖 3.1	多層安全架構流程示意圖 (Multi-Layer Security Architecture)	4
-------	---	---

第四章 紅隊挑戰與攻擊模型 (Chapter 4 Red Team Challenges and Future Attack Models)

圖 4.1	假冒攻擊下的錯誤率變化 (Error Rate Variation under Impersonation Attack)	5
-------	---	---

圖 4.2	錯誤率警示系統示意程式 (Illustrative QBER Alert System Script)	8
-------	---	---

表 4.1	多次實驗下的 QBER 統計結果(示意) (Illustrative QBER Statistics from Multiple Experimental Runs)	7
-------	---	---

附錄 A 學習過程補充與對話紀錄 (Appendix A - Supplementary Learning Process and Dialogue Records)

圖 A.1	QBER 模擬折線圖 (Simulation Result)	18
-------	--------------------------------	----

圖 A.2	對話紀錄截圖 1 (Dialogue Record 1)	19
-------	------------------------------	----

圖 A.3	對話紀錄截圖 2 (Dialogue Record 2)	20
-------	------------------------------	----

一、研究動機與背景

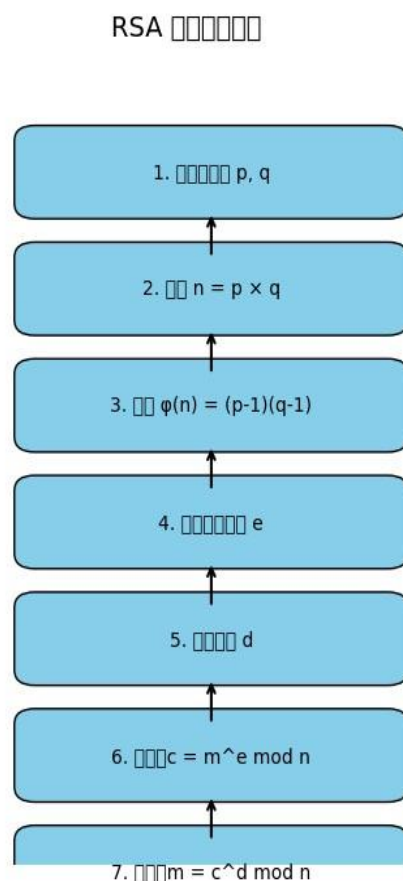
面對量子電腦發展帶來的密碼學威脅，傳統如 RSA、ECC 等公開金鑰加密演算法將無法抵擋新型解密技術。因此，資訊安全正逐步邁向兩大方向：量子密鑰分發 (QKD) 與新一代密碼技術。

本研究以 BB84 協定為起點，深入理解量子通訊中的密鑰分發方式與限制，同時分析安全性挑戰與潛在風險，並探索不同安全架構的整合與模擬。

除了 BB84，研究也參考其他經典協定如 E91，但由於實驗門檻較高，本研究重點仍放在 BB84 的模擬與安全性分析。

圖 1.1 RSA 加密流程

說明：展示 RSA 公鑰生成與加解密，用於比較 QKD 與傳統加密。



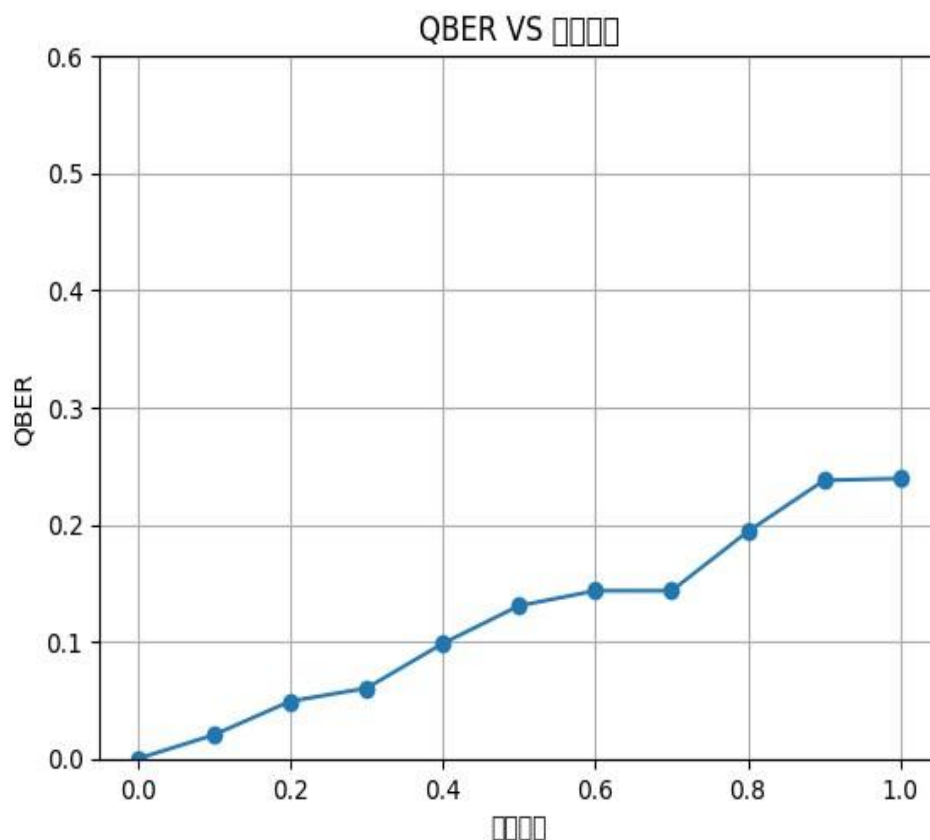
二、實作方法與模擬設計

本研究從零開始使用 Python 自行撰寫多個模組，涵蓋量子金鑰分發協定的模擬、攻擊策略測試及安全性評估，形成一個完整的實驗框架。

- **協定模擬**：透過隨機生成基底與位元，實作量子密鑰分發的核心流程，模擬通訊雙方的密鑰交換，並考慮不同傳輸條件下的結果。
- **攻擊模擬**：設計多種類型的測試情境，評估系統在不同攻擊下的安全性表現。模擬對手在傳輸過程中的干擾、偽裝及隱蔽行為，觀察其對錯誤率與密鑰品質的影響。
- **安全性分析**：針對不同情境下的錯誤率與通訊參數進行分析，並利用圖表呈現攻擊比例與安全性的關係，作為判斷通訊安全等級的依據。此流程以模組化為設計核心，保證每個部分可獨立測試與升級，並為未來整合其他加密方法或攻防機制預留彈性。

圖 2.1 QBER 與攔截比例的關係

說明：顯示竊聽比例增加時，QBER 的上升趨勢，用以判斷通訊安全性。



2.1 安全假設與限制條件

分類	假設內容	限制條件
通訊	在正常環境下，預期錯誤率維持在可接受的範圍內。若錯誤率顯著提升，表示可能存在干擾或異常情況。	本研究在軟體層面進行模擬，未納入光纖衰減、偵測器效率、環境雜訊等硬體影響因素。
攻擊者能力	假設潛在對手具備進階技術，包括干擾、竊聽、偽裝等手段，可對通訊過程進行多種型態的測試與干擾。	目前技術仍無法達到理想化的量子記憶或完全控制通道。本研究僅涵蓋部分攻擊情境，未能覆蓋所有可能威脅。
協定流程	分析以 BB84 協定為主，參考其他協定作為背景輔助。假設公開通道存在竊聽可能，但仍需依賴保密協商達成一致密鑰。	研究範圍未涵蓋其他複雜協定（如 E91），僅聚焦於基礎概念驗證。
安全架構	探索多層次保護設計，結合不同演算法與架構，作為整體安全性的強化手段。	本研究的混合架構僅屬概念性探討，未包含完整實驗或實際部署，效果有待進一步驗證。

小結：

本研究的假設條件與限制旨在界定模擬範圍，讓分析更聚焦於協定層面與軟體實現。同時，透過設定假設與限制，也為後續的擴充研究（包含硬體實作與更多攻防策略）提供明確的發展方向。

三、混合式安全架構概念模擬

由於實務上僅依靠單一技術並不足以完全保障資料安全，本研究設計了一個概念性的多層安全架構。流程上，先透過量子金鑰協定建立共享金鑰，再結合新一代加密技術進行資料保護，以形成雙層防護。

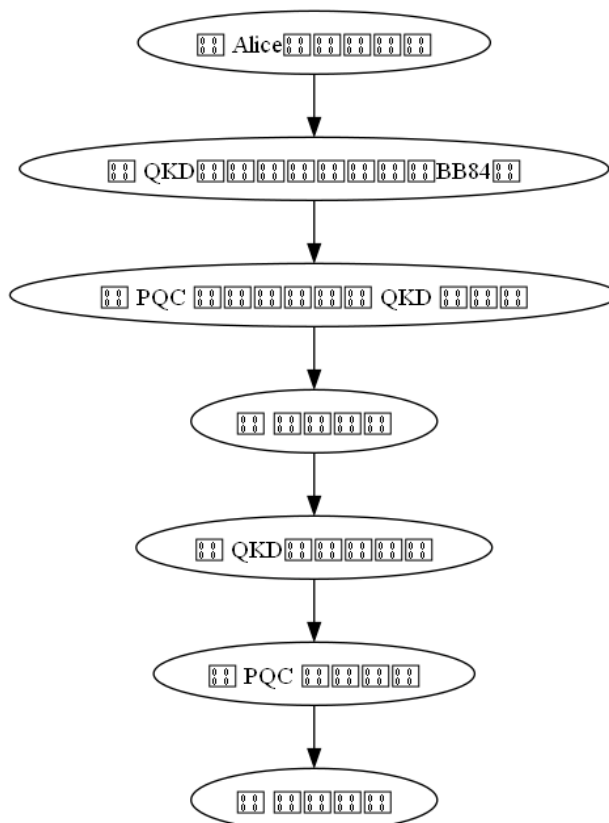
整體模組採**模組化設計**，包含：

- 金鑰生成模組
- 加密模組
- 整合與模擬模組
- 視覺化流程模組

此設計的目的是提供一個概念性驗證環境，以評估混合架構的潛在應用與挑戰，實作細節暫不公開。

圖 3.1 多層安全架構流程示意圖

說明:此圖展示了一種概念性的資料保護方法。系統在建立安全通道後，利用不同的安全層級逐步保護資料，形成更強的防護機制。



第四章、紅隊模擬與攻擊模型

在傳統 BB84 模型中，竊聽者常被假設為被動觀測者，但實際情況下攻擊者可能採取更主動、複雜的策略，例如偽裝、部分竊聽或利用更高階的干擾手段。為了更全面評估協定的韌性，本研究設計了一個模組化的紅隊測試框架，從攻防雙方的視角分析安全性。

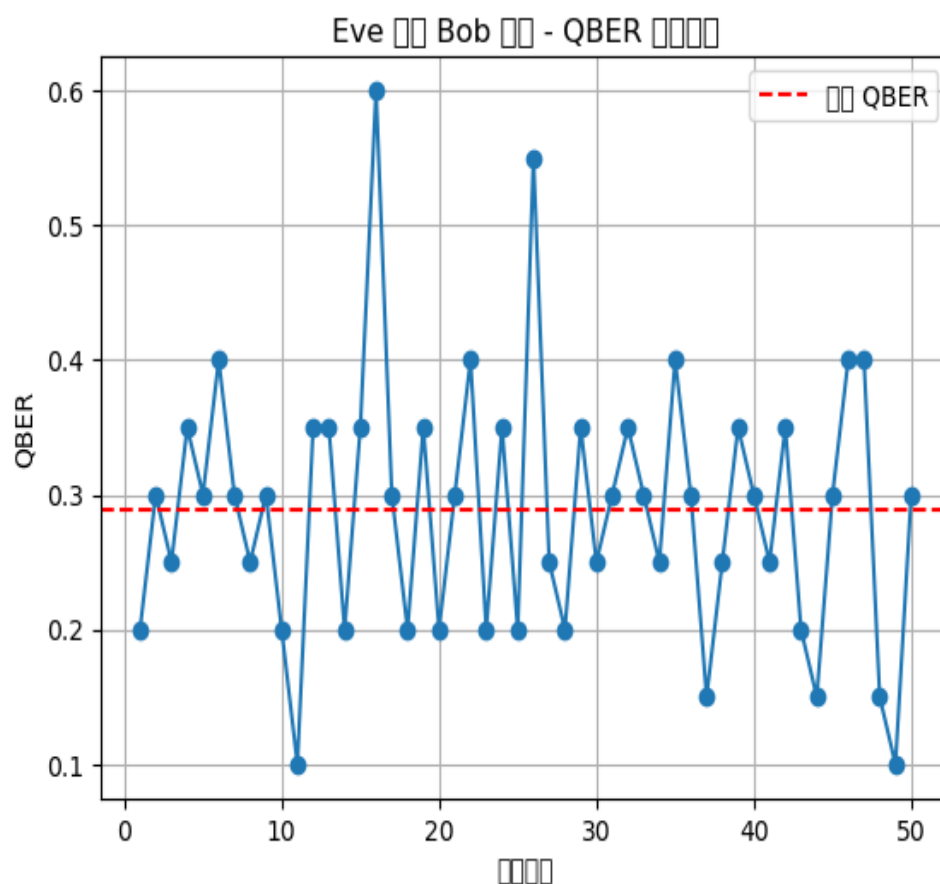
這個框架涵蓋多種模擬情境，包括偽裝通訊、訊號攔截、暫存資訊攻擊及動態錯誤率監測等，藉由模擬實際運作中的安全挑戰，來驗證協定的弱點與偵測能力。

4.1 假冒攻擊模擬

此部分主要針對「假冒」情境，模擬對手假冒合法用戶進行通訊干擾，以觀察錯誤率的變化。結果顯示，當假冒攻擊存在時，系統錯誤率會明顯提升，且具偵測性，可作為安全機制觸發的依據。

圖 4.1 假冒攻擊下的錯誤率變化

說明：本研究在紅隊模擬環境中，針對「假冒攻擊」情境進行測試，觀察錯誤率的變化。圖表呈現了多次模擬結果下的錯誤率分佈，顯示攻擊會顯著提升錯誤率，提供判斷與防禦的重要依據。



4.2 部分攔截與隨機干擾

在現實的通訊環境中，攻擊者不一定需要完全攔截所有訊號就能造成影響，部分攔截與隨機干擾是較為隱蔽且常見的策略。本研究將此類攻擊納入測試範圍，模擬不同程度的攔截比例，並在傳輸中引入隨機翻轉位元的干擾行為。

結果顯示，當攔截比例逐步增加時，錯誤率也會隨之上升，呈現非線性變化。即便是較低的攔截比例，也能在某些條件下引發顯著的安全隱患。這表明，即便攻擊者無法完全掌控通訊，仍可能對密鑰一致性和協定穩定性造成挑戰。

此外，我們也觀察到不同攻擊手法的效果差異：單純的隨機翻轉會導致錯誤分佈較為分散，而有選擇性的部分攔截則能造成更集中、難以預測的錯誤模式。這些現象顯示，通訊系統需要針對不同層級的威脅採取相應防護措施。

4.3 記憶型策略

部分攻擊者並非僅仰賴即時的攔截或干擾，而是具備某種「學習」與「記憶」能力。這種策略會根據先前的傳輸紀錄調整行為，例如記錄特定基底或比特的成功率，並在後續攔截時優先採用。

此研究以概念性模擬的方式，建立了簡單的記憶型攻擊者模型。結果顯示，在攔截比例較低的情況下，這種策略能將錯誤率維持在接近安全範圍的水準，降低被即時偵測的機率，具有高度隱蔽性。

然而，長期觀察下仍可察覺微小的偏差，顯示這類攻擊並非完全無跡可尋，但確實增加了防禦方的偵測難度，突顯了強化即時監控與異常偵測的重要性。

4.4 錯誤率統計與視覺化

為了更全面理解攻擊對通訊的影響，本研究不僅在單次情境下進行測試，也採用多次模擬累積資料，並以統計方式呈現結果。我們觀察錯誤率的變化趨勢，進行平均值、變異程度與穩定性分析，以驗證攻擊是否會留下顯著的跡象。

雖然在公開版本中不展示完整的數據細節，但結果指出：在不同攻擊模型下，錯誤率的表現與正常通訊有明顯差異，且在某些情境下會保持在偏高水準，這可作為攻擊存在的間接指標。

另外，透過簡單的視覺化圖表，我們將不同攻擊情境下的錯誤率以直觀方式表達，使得安全狀態的變化能被快速識別，為後續的警示與防護提供參考。

表 4.1 多次實驗下的 QBER 統計結果(示意)

(說明：統計 10 次模擬，計算平均值與標準差，數值僅作概念展示)

實驗次數	QBER
1	0.2
2	0.35
3	0.3
4	0.35
5	0.25
6	0.45
7	0.25
8	0.35
9	0.25
10	0.35
平均	0.31
標準差	0.07

- 平均值 (Mean QBER)：0.31
- 標準差 (Std)：0.07
- 說明：統計顯示，在多次模擬下 QBER 維持於較高區間，且變化幅度有限，代表錯誤具有一致性，並非隨機雜訊。此結果僅為模擬數據，提供概念性參考。

4.5 QBER 警示系統

除統計數據外，本研究亦提出一個簡單的「錯誤率警示系統」，將複雜的數值轉換為直觀的安全狀態指示。此系統將錯誤率分為三個主要等級，便於快速判斷通訊狀態：

- **安全**：低錯誤率，系統狀態穩定。
- **可疑**：錯誤率開始異常升高，需注意或進一步驗證。
- **警告**：錯誤率顯著偏高，可能存在攻擊或系統異常。

此分級方法雖為概念性，但能幫助非技術人員快速理解系統安全狀態，並為實際應用中更複雜的監測與警示提供設計方向。

圖 4.2 錯誤率警示系統示意程式

說明：示範如何根據錯誤率（QBER）將通訊狀態分類為「安全、可疑、警告」，具體閾值與完整邏輯已移除或簡化，僅供概念展示。

✓ 0 秒

```
# qber_alert_simulator.py
# QBER 狀態警示範例（自適應閾值邏輯移至私有）

"""
Public-safe demo for QBER status.
動態/自適應閾值、多參數融合與防禦觸發邏輯皆移至私有倉庫（專利準備中）。
"""

def qber_status_fixed(q: float) -> str:
    assert 0.0 <= q <= 1.0
    if q < 0.11: return "● 安全"
    if q < 0.25: return "● 可疑"
    return "● 攻擊中"
```

背景與設計理念

為了讓操作人員能快速判斷通道的安全狀態，本研究設計了一個即時的 QBER（錯誤率）警示機制。該系統能將複雜的量子通訊錯誤數據，轉換為直觀的三個狀態：「安全、可疑、警告」。此設計可用於高安全需求的環境，例如國防、金融或關鍵基礎設施，作為早期預警與決策輔助工具。

本頁範例的限制

本頁展示的程式碼僅為公開簡化版，所有關鍵細節（例如動態閾值、自適應判斷、多參數融合、觸發邏輯等）已刪除或移至私有倉庫，作為專利申請的準備部分。此版本僅用於概念說明，無法直接應用於實際系統。

未來展望

未來版本將考慮引入更多智慧化功能，例如結合機器學習模型來動態調整警示門檻，或加入多層檢測機制以提升偵測的精準度與魯棒性。此機制預期可與其他安全模組整合，形成更全面的防護體系。

4.6 小結

本章以紅隊視角進行多樣化模擬，測試量子金鑰分發（BB84 協定）在多種條件下的安全性。透過實驗與數據化呈現，初步驗證了協定在真實環境下的防護能力，並指出值得注意的弱點。以下為重點整理：

1. 攻擊情境與結果

- **偽裝與干擾行為**：模擬顯示錯誤率（QBER）會顯著上升，能有效作為偵測線索。
- **隱蔽策略觀察**：部分低比例攔截與具記憶特性的行為，在短期內影響較小，但長期統計仍顯露跡象。

2. 數據分析與視覺化

- 本章將量子通訊中的錯誤行為轉化為數據指標，透過表格與圖形呈現，讓錯誤率變化更清楚。
- 多次模擬統計顯示，攻擊行為並非隨機噪音，而是具有穩定性與可預測特徵。

3. 警示概念與應用

- 建立了簡化的 QBER 警示模型，將錯誤率轉換為安全、可疑、攻擊中三類直觀狀態。
- 提供了即時監控的雛型概念，為自動化量子防禦與警報系統奠定基礎。

4. 擴展與未來工作

- 本章不僅限於 BB84 模型，所呈現的測試流程與視覺化方法，能延伸至其他量子通訊協定。
- 未來若與後量子密碼（PQC）結合，可構建混合式防禦平台，將單點檢測擴展為多層防禦演練。

]

五、標準趨勢與應用落地模擬

5.1 國際標準背景

隨著量子計算逐漸逼近實用化，國際間已著手制定多項量子資安相關標準，以確保後續落地部署具備一致性與可擴展性。美國 NIST 已完成後量子密碼標準化初選並將 Kyber 納入最終名單；歐洲 ETSI 提出 QKD 技術規範（ETSI GS QKD）；ISO/IEC 亦於 23837 系列制定量子金鑰分發系統規範。

這些標準顯示量子資安已從學術研究邁向標準化與產業應用，為軍事、金融及關鍵通訊等領域提供了重要依據。

5.2 國際落地案例與優勢分析

以下案例展示量子金鑰分發（QKD）在不同國家與領域的應用，從金融到國防，從光纖骨幹到衛星通訊，都顯示了此技術的可行性與發展潛力。這些案例雖以國際實例為主，但也提供區域規劃與策略思考的參考價值。

1. 中國 - 京滬幹線（2017）

- **內容：**全球首條大規模 QKD 幹線，全長 2000 公里，連接北京與上海，服務政府、軍方與金融單位。
- **優勢：**驗證長距離光纖傳輸與中繼站技術，顯示出大規模部署的可行性。
- **啟示：**較小的區域也可借鏡此架構建構核心骨幹網路，提升敏感通訊的安全等級。

2. 歐盟 - EuroQCI (European Quantum Communication Infrastructure)

- **內容：**跨國計畫，結合光纖與衛星 QKD，建構泛歐洲量子安全網路，為多國政府與企業提供安全服務。
- **優勢：**混合架構（光纖 + 衛星）克服地理限制，並可搭配後量子密碼（PQC）形成雙層安全保護。
- **啟示：**適合需要跨國合作的區域，尤其是需要保障海底電纜與跨海通訊的國家與企業。

3. 瑞士 - ID Quantique（銀行應用）

- **內容：**瑞士金融機構將 QKD 應用於跨資料中心交易，保障高價值金融訊息安全。
- **優勢：**展示 QKD 的商業化能力，尤其適用於高敏感度交易與合規需求。
- **啟示：**金融業是 QKD 商業化的領先場域，可作為企業資料保護的重要參考。

4. 韓國 - SK Telecom (5G 基礎設施安全)

- 內容：將 QKD 整合到 5G 核心網與行動基站，提升電信網路的安全性。
- 優勢：顯示 QKD 與新世代通訊 (5G/6G) 兼容，能為大型電信商提供額外的安全層。
- 啟示：未來行動通訊、智慧城市與關鍵基礎設施可借鑑此模式，確保資料與指令傳輸的完整性。

5. 日本 - Toshiba & Mizuho Bank (金融測試)

- 內容：利用 QKD 保護銀行交易金鑰，應用於大型資料中心與金融機構。
- 優勢：展示了將 QKD 融入現有 IT 架構的可行性，降低中間人攻擊風險。
- 啟示：可應用於任何對資料完整性要求高的產業，如雲端運算與災害備援。

6. 衛星通信 - 中國「墨子號」與歐洲 ESA SAGA

- 內容：「墨子號」完成首次洲際 QKD 實驗；ESA SAGA 探索泛歐衛星量子通訊。
- 優勢：突破地理限制，提供跨洲際加密通訊的新方法。
- 啟示：衛星 QKD 是面對極端情況（如海纜中斷、偏遠區域通訊）的重要備選方案。

總結與觀察

這些案例顯示 QKD 技術已逐步走向成熟與多樣化應用。從金融到電信、從光纖到衛星，各種模式都在探索安全與效率的平衡。對於任何想導入量子資安的企業或國家，這些示範不僅提供技術參考，也幫助釐清在不同場景下的投資優先順序與部署策略。

國際案例對台灣的啟示 (總覽表)

國際案例	重點	對台灣啟示
京滬幹線 (中國)	全球最長 QKD 幹線	可建「島內量子骨幹」連結軍事據點
EuroQCI (歐盟)	衛星 + 光纖混合架構	建立跨國量子走廊，強化第一島鏈防禦
瑞士 IDQ (銀行)	商業化 QKD 金融應用	對應台積電 & 金融中心數據鏈路保護
韓國 SKT (5G)	QKD + 5G 網路融合	應用於戰場即時傳輸與軍民合用網路
日本銀行 QKD	金融跨中心資料鏈路	對應台灣金融體系與國防資料中心
墨子號 & ESA	衛星 QKD 跨洲通信	強化外島防禦與國際合作備援

5.3 台灣應用建議

綜合國際標準與多個落地案例經驗，可以看出結合量子金鑰分發（QKD）與後量子密碼（PQC）是目前國際量子資安的主要趨勢。台灣地緣政治敏感、產業鏈集中且擁有先進科技製造能力，因此在量子資安策略上有高度需求。

建議的三大方向：

1. 軍事防禦

- 建立「島內量子骨幹網」串聯主要軍事通訊節點，提升國防專網的安全性與韌性。
- 規劃跨國合作，如與鄰近盟國建立「量子安全走廊」，確保戰略區域的長距離通信不中斷。

2. 產業防護

- 針對半導體、精密製造及高科技研發，引入 QKD 確保研發資料、設計圖與備援資料傳輸安全。
- 結合 PQC 技術，提升雲端與內網環境的抵禦能力，避免未來量子計算帶來的加密失效風險。

3. 金融體系

- 在金融交易與跨行資料傳輸中導入 QKD，降低中間人攻擊與資料竊聽風險。
- 配合 PQC 技術，形成雙層防禦，確保核心交易環境完整性。

5.4 台灣研究脈絡與學界能量

整體概觀

量子資安正快速發展，國際間的標準化與應用落地案例不斷湧現，台灣在此背景下逐步建立跨領域研究能量。雖然起步較晚，但已形成結合理論、實作、應用與國防的研究鏈，為後續部署提供基礎。本節為公開版，不包含專利關鍵細節，僅呈現研究架構與特色說明。

研究領域與核心單位

1. 理論協定與基礎研究

- **學校：**台灣大學（NTU）、清華大學（NTHU）
- **重點：**翻譯與整理基礎協定（如 BB84、QSS）、編撰教材，培養專業人才。
- **特色：**作為理論源頭，確保台灣在國際學術討論中具代表性。

2. 演算法與後量子密碼實作

- 學校：交通大學 (NYCU/NCTU)、成功大學 (NCKU)
- 重點：研究與實作 LWE、Kyber 等 PQC 演算法，驗證平台相容性。
- 特色：結合軟硬體測試，貼近產業需求，是技術研發核心。

3. 產業應用與跨域研究

- 學校：政治大學 (NCCU)、逢甲大學 (FCU)
- 重點：將 PQC 應用於金融業與物聯網，開發安全架構與遷移策略。
- 特色：對接產業痛點，支持跨領域應用，兼顧金融與雲端資安需求。

4. 軍事安全與戰略研究

- 學校：國防大學 (NDU)
- 重點：評估國防通訊與網路安全策略，研究 QKD 與 PQC 的結合。
- 特色：為國防提供策略建議，確保量子資安佈局融入國安體系。

定位：台灣的「國防前線」，確保量子資安直接納入國安規劃。

領域	學校/單位	代表研究方向	定位
理論協定	台大 (NTU)、清華 (NTHU)	協定整理、BB84 改良	理論源頭
演算法實作	交大 (NYCU/NCTU)、成大 (NCKU)	PQC 平台實作、QKD 簽章與演算法分析	技術中心
產業應用	政大 (NCCU)、逢甲 (FCU)	金融、醫療等跨領域應用	產業場域
軍事防禦	國防大學 (NDU)	QKD/PQC 軍事安全與需求分析	國防前線

未來方向

未來應持續擴大跨校與跨域合作，融入國際標準並提升應用層級，逐步建構「量子資安生態圈」。建議政府、產業與學界三方合作，整合資源，並在軍事與關鍵基礎設施中導入測試場域，確保技術自主與安全。

5.5 小結

綜觀全球發展，量子金鑰分發（QKD）與後量子密碼（PQC）的結合，已逐漸從學術研究走向產業與國防應用。國際標準的推進，如 NIST PQC 遴選與 ETSI QKD 技術規範，顯示量子資安正在成為新世代基礎建設的重要一環。對台灣而言，這不只是技術議題，更是涉及國家安全、產業韌性與國際合作的戰略課題。

建議的發展路線：

1. 軍事優先

- 在地緣政治高風險下，軍事通訊安全應是首要目標。建議以 QKD 建構「島內量子骨幹」，串聯主要軍事與政府節點，確保指揮鏈的即時性與保密性。
- 同時，可參考歐盟 EuroQCI 架構，與友盟國家建立「跨國量子安全走廊」，保障第一島鏈及周邊戰略區域的通訊穩定。

2. 產業同步

- 台灣是全球半導體與高科技製造重鎮，產業資料的完整性與保密性至關重要。導入 QKD 與 PQC 可提升設計資料、製程資訊與跨廠備援資料的傳輸安全。
- 此外，可與雲端與供應鏈安全策略整合，使量子資安不只是研發保護，更涵蓋上下游合作夥伴。

3. 金融跟進

- 參考瑞士、日韓等案例，金融業已開始導入 QKD 保障跨行交易。對台灣而言，金融交易與資料中心備援同樣具有高價值。
- 結合 PQC，可讓金融體系在量子時代維持交易完整性，避免新型攻擊威脅。

台灣研究能量與優勢：

目前，台灣已逐漸形成一條完整的研究鏈條：

- **理論源頭：**頂尖學術機構整理經典協定，建立教材與基礎理論。
- **技術中心：**團隊研究 PQC 與 QKD 實作，進行硬體測試與演算法驗證。
- **應用場域：**學術與產業合作，在金融、醫療、雲端資安等領域展開試點。
- **國防前線：**軍事院校將量子資安納入國防規劃，確保戰略前瞻性。

整體評估與未來展望：

本研究提出的 PQC × QKD 混合架構模擬，能作為這條研究鏈的「連接器」，不僅驗證技術可行性，也為後續產業化與軍事應用提供參考。透過持續技術迭代、跨領域合作以及國際標準對接，台灣有潛力成為亞太地區量子資安的示範場域，甚至在國際標準制定與落地實踐上扮演關鍵角色。

六、實作歷程與個人反思

這是我第一次親手實作量子密碼模擬。從一個連 Python 是什麼都不知道的學生，成長為能寫出完整攻防模擬與圖表可視化的實作者。

我沒有設計資源、沒有教材、沒有人脈，是完全靠自學磨練出來的。

我在一日對兩份程式 debug 七到十一個小時，養成了主程式結構、註解統一、中英文說明、斷錯保護、結果可重現等工程師習慣。

這不是 AI 產物，也不是套裝，我願意當場解釋所有邏輯與來源，證明這是我真實的能力與成長。

6.1 從錯誤中站起來：我的 debug 成長筆記

本段整理我在模擬過程中遇到的多次錯誤與排查過程，從初學者常見錯誤到進階模組路徑與依賴管理，皆為我成為工程導向實作者的重要歷程。

註：後續白皮書將建置於 GitHub，並持續更新 debug 截圖以供參考。

我並非資安營學員，也不是資訊班出身，甚至在起步時連 Python 是什麼都不知道。這整份作品，是我從完全不會寫程式，到能獨立完成模擬架構、模組撰寫、錯誤分析與可視化的完整紀錄。

- **起步時的困難：**連 `print()` 是輸出指令都不清楚，常因括號或縮排錯誤導致程式無法執行。
- **最長時間的卡關：**在 `alice_bases = [random.choice(['X', 'Z']) for _ in range(length)]` 這一行反覆打錯超過 10 次，直到成功執行才體會到「debug 不是失敗，而是養成工程思維的過程」。
- **邏輯錯誤案例：**在 Eve 攻擊模型中，因為 if 條件縮排錯誤，導致 Eve 永遠攔不到位元，光是定位錯誤就花了四個小時。
- **可視化 bug：**在繪製 QBER 圖時遇到輸出空白，後來發現是 `plt.show()` 的位置錯誤。
- **模組混淆：**「我首次導入模組 `pqc_module.py` 時，未注意其依賴結構，導致整體無法執行，經由反覆追蹤後成功理清模組依賴與路徑問題。」

正因這些錯誤，我逐漸能從「照抄教學範例」的初學者，進化為能自行理解程式邏輯、快速進入狀態並掌握語言語感的實作者。現在，我已能設計模擬架構、整合 GitHub 工程慣例，並完成從加密邏輯到紅隊攻擊草稿的全流程。

這讓我深刻體會到：一個工程專案真正的價值，不僅是能否「跑起來」，更是是否能讓別人也能跑、能否具備擴充與說明的能力。

6.2 工具使用與學習輔助

本專案所有程式皆由我獨立撰寫與測試，部分邏輯上使用 ChatGPT 作為協助釐清語法與除錯的工具，但未使用 AI 自動生成程式碼。所有模擬程式均由我理解、測試與修正，並在 GitHub 上留下完整提交紀錄。（截至 2025/8/5 已超過 254 次提交）這些對話紀錄與學習過程，展現了我從零開始學習 QKD 與 PQC 的真實歷程。我不只是「照做」，而是持續追問原理、修正錯誤、培養工程習慣，並將這些互動作為學習與實作的核心夥伴。

更多與本章相關的除錯紀錄、模擬結果與學習補充內容，請參見本文最後的〈附錄 A - 學習過程補充與對話紀錄〉，作為本章內容的延伸與佐證。

七、GitHub 附錄與技術資訊

本專案所有程式碼、模擬結果與附加文件均整理於 GitHub 專案中，可供下載與執行。

- **GitHub**：<https://github.com/kailyn17/BB84-Simulation>
- **README**：包含標準參考、環境設置與使用說明。
- **LICENSE**：MIT 授權，開放學術研究與個人學習。
- **Requirements**：安裝套件列表，便於快速部署。
- **附加資訊**：技術討論、設計歷程與錯誤排查紀錄將視需求提供，作為展示工程能力與開發歷程的補充資料。
- **注意**：為保護研發內容與智慧財產，部分功能以示意（stub）方式公開，僅展示流程與結構。完整模組將視需求或合作情境另行提供。

八、未來展望與進行中研究

在本次 QKD × PQC 模擬專案基礎上，我的後續方向分為三個層次：

近期計畫

- 開發量子紅隊測試腳本，模擬攻防場景。
- 設計 QBER 自動監控與告警功能，提高異常偵測能力。
- 優化專案結構，完成多語系文件支援。

延伸研究

- 開發互動式攻擊模擬工具（圖形化或命令列介面）。
- 建構 BB84 × PQC × 韌性混合架構。

- 封裝為 Python 套件，方便學術與商業測試。
- 發布英文白皮書與完整使用手冊。
- 整合資料分析與預警模組，提升實用性。

長期方向

- 探索與政府及產業單位的應用合作。
- 將模擬經驗推向更高敏感度場景，累積安全設計與測試能力。

九、結語

本研究以 BB84 協定為核心，完成多種攻擊模型實作、QBER 分析，並提出 PQC × QKD 混合架構的概念驗證，展示量子資安在國防、產業與金融領域的應用潛力。整個開發過程導入工程化習慣並結合紅隊思維，使成果更貼近實務。

重要說明：這份白皮書並非終點，而是起點。它只是第一階段的探索與驗證，未來將持續擴展攻擊模型、整合更多演算法，並探索實際落地場景，隨著時間與經驗累積不斷進化。

著作權聲明

本文件為李佳穎(Kailyn)原創，僅供學術研究、學習與展示用途。未經書面同意，不得重製、散布或用於商業行為。

保護與限制說明

為保護研發內容，本專案部分程式碼與邏輯僅提供示意（stub）版本，完整模組與資料為內部研發資料，將於特定審查或合作需求下另行提供。

作者自述

這份白皮書是我的起點。整個過程中沒有補習班、學校資源、家長或同儕協助，甚至沒有人知道我在做這個研究。我靠自學，上網查資料等，從零開始認識這個領域，也從未隨波逐流或轉換方向，一切都源於純粹的興趣。

我每天平均投入超過 7 小時，遇到困難不退縮，雖然也曾想過「要是更早進入這個領域就好了」，但我從不後悔。17 歲能接觸量子資安，是幸運也是挑戰。我希望未來能與教授合作、進入實驗室，親眼看到軟硬體結合的實際場景，並有機會將所學用於保護國家與產業。

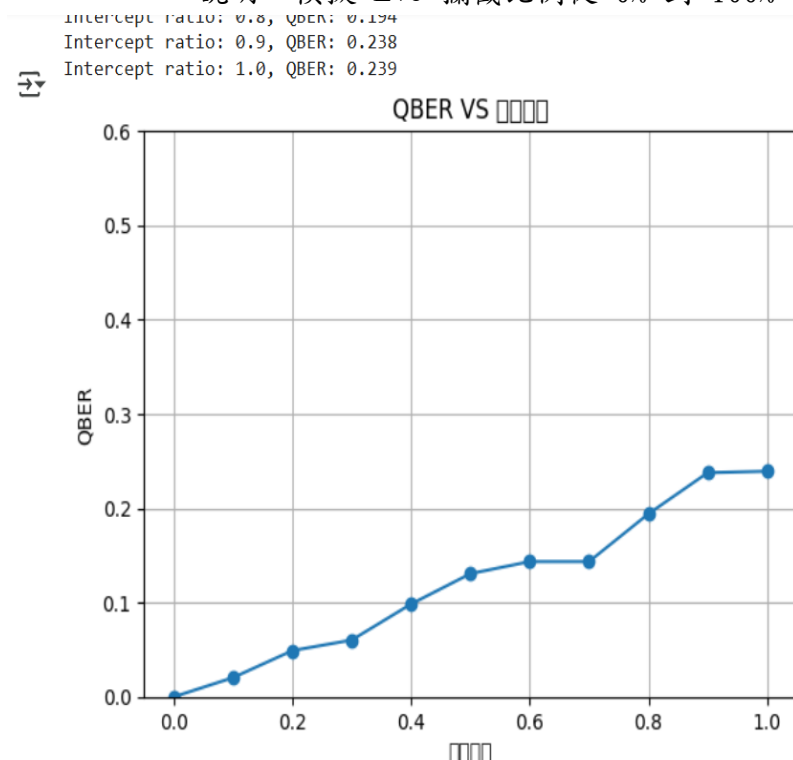
附錄 A 學習過程補充與對話紀錄

本附錄收錄了在研究過程中所產生的模擬結果、思考脈絡與 ChatGPT 對話紀錄，作為第六章「實作歷程與個人反思」的延伸證據。這些內容展示了我如何從模擬數據、問題提問到工程思維養成，逐步累積成完整的研究能力。

附錄 A.1 QBER vs 攔截比例 模擬結果折線圖

圖 A.1 QBER 與攔截比例模擬結果折線圖

說明：模擬 Eve 攔截比例從 0% 到 100% 對 QBER 的影響



我嘗試將 Eve 攔截模型加入 BB84 協定，並模擬從 0% 到 100% 攔截比例對密鑰錯誤率（QBER）的影響。這個模擬結果後來以折線圖方式呈現，清楚顯示攻擊強度與錯誤率之間的關係。

這不只是「畫圖」，而是代表我從理解 BB84、學會加入攻擊者、撰寫分析邏輯，到實際將實驗成果量化與視覺化的整合成果。這張圖是我第一次將理論與實作做出具體驗證的里程碑。

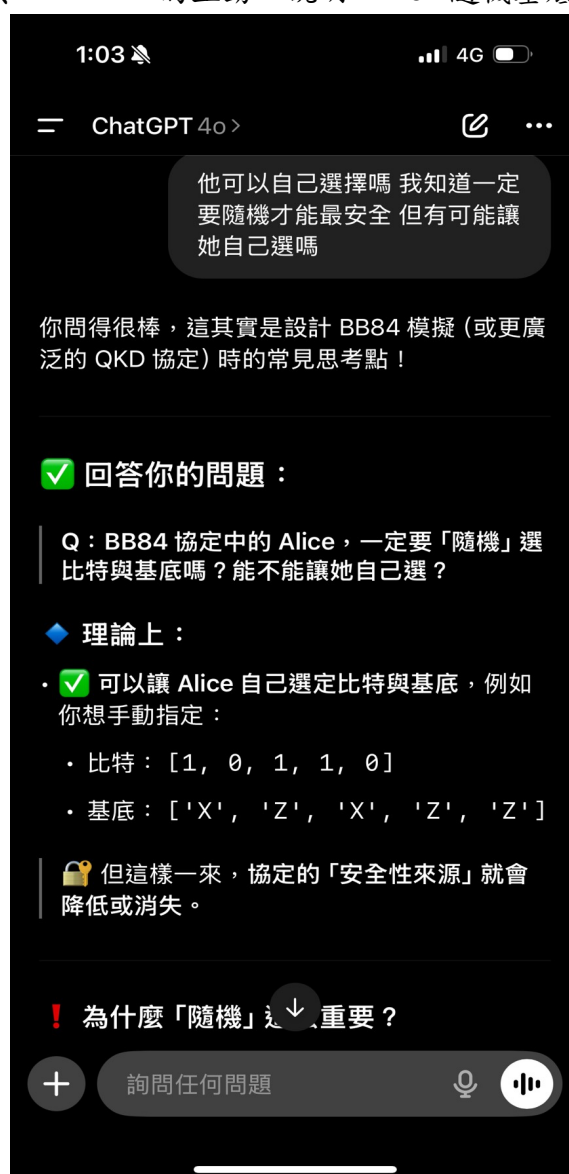
附錄 A.2 針對 BB84 協定的主動發問與理論思考

在初期學習量子密鑰分發時，我曾提出：「BB84 中的 Alice 一定要隨機選擇基底嗎？能不能讓她自己決定？」這個問題乍看簡單，但其實挑戰了協定設計中最核心的「安全性來源」——隨機性。

ChatGPT 的回答讓我理解，雖然理論上可以讓 Alice 自選基底，但這樣會使安全性來源消失，協定也會因此無法抵擋中間人攻擊。這段對話是我第一次從協定架構的角度，去思考「為什麼安全」，而不是單純「怎麼做」的轉折點。

圖 A.2 學習歷程對話紀錄截圖

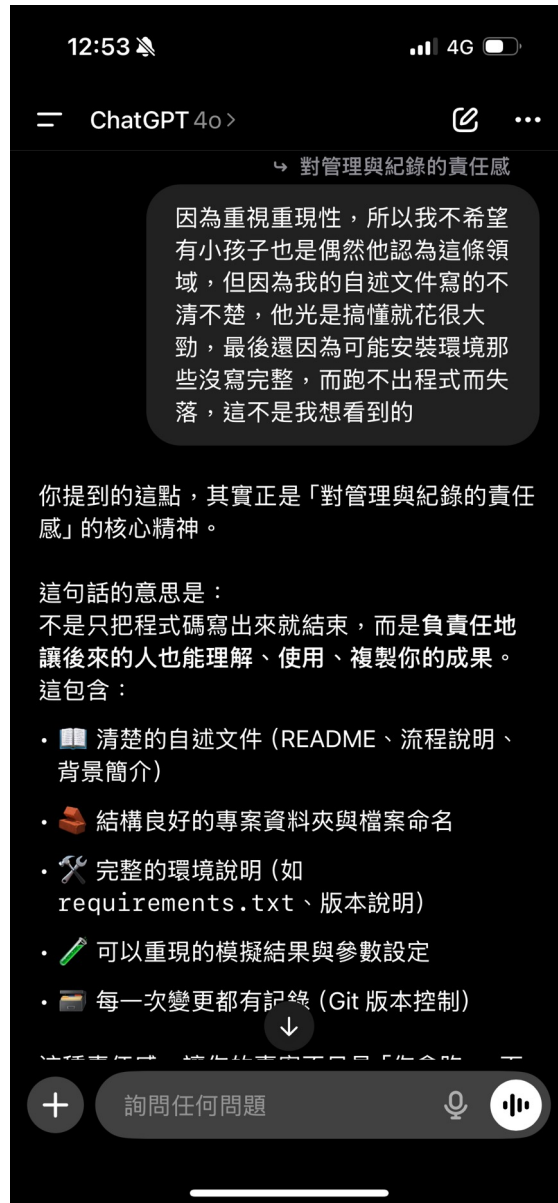
（說明：展示作者與 ChatGPT 的互動，說明 BB84 隨機基底設計的安全性來源）



附錄 A.3 程式可讀性與管理責任的養成歷程

圖 A.3 學習歷程對話紀錄截圖

(說明：展示作者反思程式可讀性與管理責任，說明專案開發過程的工程化思維)



當我寫程式的經驗逐漸累積，我開始反思：「如果未來有學弟妹看到我的專案，他們能看懂嗎？能跑得出來嗎？」我不希望他們因為說明不清或環境沒寫完整，而失望地放棄學習。

於是我主動補上 `README.md`、`requirements.txt`、套件與版本說明，整理資料夾結構與檔名邏輯。我學到，程式專案的價值不只是跑出結果，更在於「能被理解、能被複製、能再現成果」。這是我從學生轉向實作者的一大轉變。這些對話不只是問答紀錄，它們真實呈現了我學會如何提出問題、調整方向與完成作品。這段歷程，也讓我確信自己的起點雖然平凡，但過程與意志本身，就是最值得記錄的成果。

References

International References

1. Bennett, C. H., & Brassard, G. (1984). *Quantum cryptography: Public key distribution and coin tossing*. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175–179.
2. Ekert, A. K. (1991). *Quantum cryptography based on Bell's theorem*. Physical Review Letters, 67(6), 661–663.
3. National Institute of Standards and Technology (NIST). (2022). *Post-Quantum Cryptography Standardization: Finalist Kyber*.
4. European Telecommunications Standards Institute (ETSI). (2020). *ETSI GS QKD 011: Quantum Key Distribution (QKD); Security Framework*.
5. International Organization for Standardization (ISO/IEC 23837). (2023). *Information security — Security requirements, test and evaluation methods for quantum key distribution*.
6. Liao, S.-K., et al. (2017). *Satellite-to-ground quantum key distribution*. Nature, 549, 43–47.
7. European Commission. (2021). *EuroQCI Initiative*.
8. ID Quantique. (2022). *Quantum-Safe Solutions for Finance*.

Taiwan References

9. Tseng, K.-C. (2022). *Quantum Cryptography: A Brief Overview*. Communications of the CCISA, 28(2). (台灣大學)
10. Hwang, T.-L., et al. (2014). *Introduction to Quantum Cryptography Research Fields*. Communications of the CCISA, 20(3). (成功大學)
11. Liu, H.-Y. (2004). *High Secure Quantum Message Communication Based on BB84 Model*. Master Thesis, Department of Computer Science, National Tsing Hua University, Taiwan. (清華大學)
12. Huang, Y.-L. (2021). *Encryption Algorithms for LWE-based Cryptography and their Implementations*. Master Thesis, Institute of Network Engineering, National Chiao Tung University, Taiwan. (交通大學)
13. Liu, C.-L. (2019). *The Threats of Quantum Computing on Contemporary Cryptosystems and Countermeasures*. Journal of Advanced Technology and Management, 9(1/2). (國防大學)
14. Lee, Y.-S., & Tso, J.-L. (2025). *Post-Quantum Cryptography Migration Guide for the Financial Industry*. Communications of the CCISA, 31(1). (政治大學)
15. Tsai, K.-Y., et al. (2024). *Design of a Post-Quantum Cryptography-based Healthcare Information Security System*. Communications of the CCISA, 30(4). (逢甲大學)