**中國醫藥大學 人文與科技學院 數位健康創新碩士學位學程 碩士論文寫作格式**

**一、學位論文編印項目及順序**

What Should be Included in Your Thesis (In Order)

1. 封面 Front Cover
2. 空白頁 Blank Page
3. 書名頁（中文、英文）Thesis Title (Chinese, English)
4. 審定書Verification From the Oral Examination Committee
5. 授權頁CMU Thesis & Dissertation Copyright License Agreement
6. 研究生無違反學術倫理聲明書(本校) CMU Graduate Student Academic Ethics Statement
7. 誌謝辭 Dedication or Acknowledgments
8. 摘要（中文）及關鍵詞5-7個 Chinese Abstract and Keywords
9. 摘要（英文）及關鍵詞5-7個 English Abstract and Keywords English Abstract
10. 目次 List of Contents
11. 圖表目次 List of Figures/Illustrations
12. 正文 Body of The Thesis
13. 參考書目 Bibliographies/References

**二、本文撰寫格式：**

1.封面：內容包含研究所名、論文名稱、教授及本人姓名、提送日期等。

2.書名頁：包括論文中英文名稱，著者及指導教授中英文姓名、校名、所名、學位論文別、提送論文英文說明及地名、提送年月等。

3.口試委員會審定書。

4.中英文摘要：內容應說明研究目的、資料來源、研究方法及結果等，500-1000字，中英文橫式各一份，裝訂於論文內，格式如附件。

5.論文尺寸及紙張：以 210mm \*297mm 規格 A4 紙張繕製。封面、封底採用基重在 150g 以上布紋紙或卡紙，顏色由系所自訂，可詢問系辦。

6.版面規格：紙張頂端留邊2.54cm，左側留邊 3.81cm，右側留邊2.54cm，底端留邊 2.54cm，距版面底端 1cm 處中央繕打頁次。

7.文字規格：文章主體以標楷中文為主，英文則是Times New Roman使用14號字，自左至右，橫式以打字繕排，文句中引用之外語原文以()號附註。行距設定為1.5倍行高。

8.標題格式：標題以章（粗體18點，居中對齊）、節（大小粗體16點）、項（大小粗體14點）、壹、一、(一)、1.、(1)等層次。

凡例：

第一章 前言 （粗體18點，居中對齊）

第一節 研究動機與目的（大小粗體16點）

第二章 研究方法

第一節 研究設計

第一項 研究範圍 （大小粗體14點）

第二節 研究資料

第三章 研究結果

第四章 討論

第五章 結論與建議

第一節 結論

9. 頁次標示：

(1)由摘要(Abstract)至緒論(Introduction)之前以用i, ii, iii,連續編頁。

(2)論文第一章以至附錄，均以1，2，3等阿拉伯數字連續編頁。

10. 裝訂：自論文本左端裝訂，書背繕打學位論文別，論文名稱，校名、系所名、著者姓名。

11.表格：表的編號及標題皆粗體，位置在表的上方與表的「置中對齊」，編號和表的標題間空一個全型。標題與表之間不空行。表格內標題，以「置中」呈現。表的格線：只使用水平線，最下方的線用1 1/2 pt，其餘使用1/2 pt。

**三、參考文獻書寫範例：**

1. 參考書目之格式依各學門習慣使用為準，或採用IEEE格式。
2. 期刊文獻之書寫依序為：姓名、文章名稱、期刊名、卷別、期別、頁別、年代。
3. 範例：

[期刊論文格式]：Author, “Title,” *Journal*, vol. X, no. X, pp. X, Year.

[1] C. F. Cheng, E. T.-C. Huang, J.-T. Kuo, K. Y.-K. Liao, and F. J. Tsai, “Report of Clinical Bone Age Assessment using Deep Learning for an Asian population in Taiwan,” *BioMedicine*, vol. 11, no. 3, pp. 8, 2021.

[會議論文格式]：Author, “Title,” in Conference Name, Conference Location, Year, pp. X.

[2] C. H. Bennett, and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179.

**範 例**

中國醫藥大學

數位健康創新碩士學位學程

碩士學位論文

China Medical University

Master Program for Digital Health Innovation

Master Thesis

**量測回傳環境之認證式半量子金鑰分配協定**

**Measure-resend Authenticated Semi-****quantum Key Distribution Protocol**

指 導 教 授：楊竣崴 博士 Chun-Wei Yang

研 究 生：王鴻文 Hung-Wen Wang

中華民國111年6月

June 2006

中

國

醫藥

大

學

數位健康創新碩士學位學程

碩

士

學

位

論

文

：半量子金鑰分配協定

研究生

：

王

x

x

年

月

書背(最下面留3公分圖書館貼書標使用)

書背

**中國醫藥大學數位健康創新碩士學位學程碩士學位考試委員審定書**

 所撰之碩士論文

經本委員會審查通過。

|  |  |
| --- | --- |
| 論文考試委員會委員 |  |
|  |  |
|  |  |
|  |  |
| 指　導　教　授 |  |
|  |  |
| 學程主任 |  |

中華民國 年 月 日

**摘要**

量子金鑰分配協定起源於1984年，學者Bennett和Brassard提出第一篇基於單光子之量子金鑰分配協定。量子金鑰分配協定使兩位參與者能夠藉由量子物理特性來共享一把金鑰。然而，量子金鑰分配協定假設參與者皆擁有完整的量子能力，在量子設備仍然相當昂貴的現今是非常不切實際的。為了讓降低執行量子密碼協定之門檻，學者Boyer於2007年提出半量子金鑰分配協定。學者Boyer定義了在半量子環境之中，僅有一方擁有完整的量子能力，另一方則是假設為只有受限的量子能力之傳統使用者。儘管半量子金鑰分配協定降低執行量子密碼協定之門檻，但仍然需要透過傳統認證通道(即可以被竊聽但無法被竄改)認證參與者。若無傳統認證通道，則半量子金鑰分配協定無法抵擋偽冒攻擊。有鑑於此，學者Yu等人於2014年提出第一篇認證式半量子金鑰分配協定，達到不需傳統認證通道之目的。認證式半量子金鑰分配協定發表後，吸引了諸多學者們研究以及提出各種認證式半量子金鑰分配協定。

關鍵詞：量子密碼學、半量子、量測回傳環境、量子金鑰分配、認證

**Abstract**

The first quantum key distribution (QKD) protocol based on single photons was proposed in 1984 by Bennett and Brassard. The QKD protocols distribute keys between two participants based on quantum mechanics. However, QKD protocols typically assume that both participants have the requisite hardware, which is not a practical assumption as quantum computing hardware is prohibitively expensive. With an aim of increasing the accessibility of these protocols for everyone, Boyer et al. proposed the first semi-quantum key distribution (SQKD) protocol in 2007. Boyer et al. specified an environment that involves two types of participants: one with unlimited quantum capabilities and the other with classical capabilities and limited quantum capabilities, where the user Bob is considered a classical user and the user Alice possesses full quantum abilities. Although SQKD protocols increase the convenience of quantum protocols, the SQKD protocols cannot be secured without an authenticated classical channel (i.e., the transmitted classical messages can be eavesdropped upon but not modified). If an authenticated classical channel does not exist between Alice and Bob, then SQKD protocols can suffer from an impersonation attack. Mutual identity authentication is required to prevent impersonation attacks in SQKD protocols. In the light of this, Yu et al. proposed the first authenticated semi-quantum key distribution (ASQKD) protocol in 2014, which does not require authenticated classical channels. After the proposal, miscellaneous ASQKD protocols have been proposed.

Keywords: Quantum Cryptography, Semi-quantum, Measure-resend Environment, Quantum Key Distribution, Authentication

**誌謝**

論文寫到這一部份就代表著即將完成，對於在論文寫作過程中，指導教授．．．。

**目錄**

審定書 i

研究生無違反學術倫理說明書 ii

誌謝 iii

摘要 iv

Abstract v

目錄 vi

表目錄 viii

第一章 緒論 1

第二章 預備知識 6

第三章 雙簽章者的半量子簽章協定之安全性問題 10

第一節 Zhao學者等人的半量子簽章協定 10

第一項 初始階段 10

第二項 簽章階段 11

第三項 驗證階段 12

第四章 植基於貝爾糾結態的半量子簽章協定 16

第五章 結論與未來展望 23

參考文獻 24

iii

**圖目錄**

圖1 範例圖形 2

圖2 範例圖形 3

圖3 範例圖形 9

**第一章 緒論**

* 1. **研究動機**

**參考文獻**

1. C. F. Cheng, E. T.-C. Huang, J.-T. Kuo, K. Y.-K. Liao, and F. J. Tsai, “Report of Clinical Bone Age Assessment using Deep Learning for an Asian population in Taiwan,” *BioMedicine*, vol. 11, no. 3, pp. 8, 2021.
2. C. H. Bennett, and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179.