行政院國家科學委員會專題研究計畫　成果報告

總計畫(3/3)

計畫類別： 整合型計畫
計畫編號： NSC93-2213-E-009-008-
執行期間： 93 年 08 月 01 日至 94 年 07 月 31 日
執行單位： 國立交通大學資訊科學學系(所)

計畫主持人： 曾文貴

報告類型： 完整報告

處理方式： 本計畫可公開查詢

中　華　民　國 94 年 10 月 20 日

行政院國家科學委員會補助專題研究計畫 成果報告

總計畫：理論密碼學與應用（3/3）

Study of Theoretical Cryptography and Its Applications

計畫類別：□ 個別型計畫　　☑ 整合型計畫
計畫編號：NSC　93－2213－E－009－008－
執行期間：　　93 年 8 月 1 日至 94 年 7 月 31 日
全程計畫期間：91 年 8 月 1 日至 94 年 7 月 31 日

計畫主持人：曾文貴 教授
共同主持人：
計畫參與人員： 林蕙如、陳冠廷

成果報告類型(依經費核定清單規定繳交):□精簡報告　☑完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學 資訊科學系

中　華　民　國　94　年　10　月　25 日

目錄

中文摘要

近年來密碼研究非常重視理論的探討，從最近國際密碼會議所發表的論文來看，這趨勢將一直持續下去，因此密碼理論的研究是一個重要的課題。密碼學的理論基礎包含很廣，從計算模式、計算複雜度、電路複雜度、單向函數、密碼雜湊函數、布林函數、編碼理論、零知識證明系統到最新的量子計算等都包含在內。這些議題具有高度的相關性，總計畫將研究這些理論，再配合各子計畫專精的研究，加以整合，希望能夠得到一些好的成果。

總計畫包含三個子計畫：(1) 串列加密法的理論及實作、(2) 擬亂數產生器與編碼及其密碼之應用、及 (3) 分散式門檻密碼系統的研究。每一項子計畫有一個專精的議題，總計畫的研究比較廣泛，並包含子計畫沒有涵蓋的議題，綜合起來會有一個比較完整的成果。

本計畫的研究成果豐碩，共發表 5 篇不錯的國際會議論文（收錄於 LNCS 及 IEEE），5 篇 IEEE Transactions on Information Theory（IT）期刊論文，1 篇 IEEE Transactions on Wireless Communication 期刊論文，2 篇 IPL 期刊論文，2 篇 Designs, Codes, and Cryptography 期刊論文，和數篇國內會議及期刊論文

關鍵詞：密碼學、串流加密法、擬亂數產生器、分散式門檻密碼、預防式密碼。

英文摘要

Recent research on cryptography has been focusing on its theoretical foundation. This trend shall continue in the near future. Therefore, this project shall research on the theoretical foundation of cryptography, which consists of computation model, computational complexity, circuit complexity, one-way function, cryptographic hash function, Boolean function, coding theory, zero-knowledge interactive proof system and quantum computation, etc. These topics are closely related. This project shall study these topics in cooperation with its four sub-projects. We hope that through close cooperation with each other, we can produce satisfactory results.

This project consists of four sub-projects: (1) Stream cipher: theory and construction, (2) Pseudorandomness, codes and applications, and (3) Distributed threshold cryptography. Each sub-project has a special research topic. This project's goal is broader and covers cover the un-covered topics of the sub-projects.

This project has excellent results. In its three subprojects, we have published 5 international conference papers (its proceedings are in LNCS or IEEE), 5 papers in IEEE Transactions on Information Theory, 1 paper in IEEE Transactions on Wireless Communication, 2 papers in IPL, 2 papers in Designs, Codes and Cryptography. We also published several domestic conference and journal papers.

Keywords: theoretical cryptography, zero-knowledge proof system, provable security, coding.

1. 計畫緣起及目的

本計畫的主要目是從事密碼相關理論的研究,並尋找可能的應用,研究的重點為:

(1) 跨密碼議題的研究：總計畫將和三個子計畫分工合作，希望能過透過相互的激盪而得到一些不同議題之間相互應用的結果。

(2) 零知識交互證明的研究（zero-knowledge interactive proof system）：零知識交互證明系統不但是複雜度理論的重要議題，更是密碼協定設計與證明的最重要理論之一。目前的零知識交互證明系統已經發展出多種形式，例如非交互證明系統、多證明者證明系統等，每一種都在密碼領域得到很好的應用，我們將繼續研究之。

(3) 編碼理論在密碼學的應用：目前研究者漸漸發現傳統編碼（conding）與密碼的相關性，例如線性碼（linear code）就可以使用在叛逆者追蹤的問題上，除錯碼也可以使用在秘密分享上。最近資訊理論學者也發現編碼與擬亂數有密切的關係，因而導出 extractor code。因此在這個時間點上，我們要儘快的研究相關的議題。

(4) 密碼協定的設計與安全性研究：使用密碼技術來設計完成某些工作的協定一直是密碼研究的重點之一，例如電子商務的付款機制及安全的電子投票協定。我們將把我們在密碼理論研究的相關成果使用在密碼協定的設計上，並證明其安全性。

(5) 其他密碼相關理論的研究；密碼理論的基礎很多，並不能單獨研究一兩項，例如數位簽章就包含單向函數及密碼安全模式等的研究。我們希望能夠在綜合的成果上能有貢獻。

2. 計畫成果

由於總計畫的經費被大砍，只剩二十多萬元，因此總計畫的工作變為整合及支援各子計畫。茲分述各子計畫成果如下。

2.1. 子計畫一成果

1. Hwu, J. S., Chen, R. J., and Lin, Y. B.(2005)"An Efficient Identity-Based Cryptosystem for End-to-End Mobile Security," to appear in IEEE Trans. On Wireless Communication.
2. Hwu, J. S., Hsu, S. F., Lin, Y. B., and Chen, R. J.(2005)" End-to-end Security Mechanisms for SMS," to appear in International Journal of Security and Networks.
3. Lin, J. S., Chang, J. C., and Chen, R. J.(2005)"New Simple Constructions of Distance-Increasing Mappings from Binary Vectors to Permutations," to appear in Information Processing Letters.

4. Hwu J. S., Chen R. J., Lue H. S., Lin J. S. (2004) "Efficient Computation of the Weil Pairing in ID-based Cryptosystems," International Computer Symposium, Taipei, Taiwan, December, pp. 1297-1301.
5. Huang K. Q., Chang J. C., Chen R. J. (2004) "A new construction of resilient functions over GF(p) with good cryptographic properties," International Computer Symposium, Taipei, Taiwan, December, pp. 1213-1217.
6. Liang H. C., Chang J. C., Chen R. J. (2004) "New Efficient Constructions of Binary Asymmetric Error-Correcting Codes," International Computer Symposium, Taipei, Taiwan, December, pp. 1036-1038.
7. Liu, Wei-Ting, Chen Cheng-Kai, and Chen, Rong-Jaye (2005) "Experimental Linear Attacks on Substitution-Permutation Networks," Proceedings of the 15th National Conference on Information Security, Kaoshiung, Taiwan.
8. Liang, Han-Chang and Chen, Rong-Jaye (2005) "A Trichotomy Reaction Attack on McEliece Public-Key Cryptosystem," Proceedings of the 15th National Conference on Information Security, Kaoshiung, Taiwan.
9. Hwu, J. S., Chen, R. J., and Lin, Y. B.(2005) "Authenticated Public-Key Distribution over WLAN/Cellular Dual Networks." Proceedings of International Conference on Information Technology: Research and Education, Taiwan.

2.2. 子計畫二成果

子計畫二共有下列成果

A. Book Chapters

1. Jen-Chun Chang and Kai-Chun Hwang, "串流加密法的發展現況," Chapter 4 of 資通安全專輯, Eds. 官大智、曾文貴, 行政院國家科學委員會科學技術資料中心, Nov. 2004. (NSC93-2213-E-305-003-)
2. Jen-Chun Chang and Frank K. Hwang, "The reliability of consecutive-k systems," Chapter 3 of Handbook of Reliability Engineering, Ed. H. Pham, Springer, 2003. (NSC92-2213-E-415-006-)

B. Journal Paper Published

1. Jen-Chun Chang, "Distance increasing mappings from binary vectors to permutations," IEEE Transactions on Information Theory, Vol. 51, Jan. 2005, pp. 359-363. (SCI/EI) (IF=2.245) (NSC93-2213-E-305-003-)
2. Jen-Chun Chang, Rong-Jaye Chen, T. Klove and Shi-Chun Tsai, "Distance preserving mappings from binary vectors to permutations," IEEE Transactions on

Information Theory, Vol. 49, April 2003, pp. 1054-1059. (SCI/EI) (IF=2.245) (NSC91-2213-E-159-007-)

3. Jen-Chun Chang, Rong-Jaye Chen and Frank K. Hwang, "An efficient algorithm for the reliability of consecutive-k-n networks," Journal of Information Science and Engineering, Vol. 19, 2003, pp. 159-166. (SCI/EI) (NSC91-2213-E-159-007-)
4. Jyh-Shyan Lin, Jen-Chun Chang, and Rong-Jaye Chen, "New Simple Constructions of Distance-Increasing Mappings from Binary Vectors to Permutations,", to appear in Information Processing Letters. (SCI/EI) (NSC91-2213-E-159-007-)

C. Journal Paper Submitted

1. Jen-Chun Chang, "New algorithms of distance-increasing mappings from binary vectors to permutations by swaps," to appear in Designs, Codes and Cryptography. (SCI) (NSC93-2213-E-305-003-)
2. Jen-Chun Chang, "Distance increasing mappings from binary vectors to permutations that increase Hamming distance by at least two," to be published in IEEE Transactions on Information Theory. (SCI/EI) (NSC93-2213-E-305-003-)
3. Jen-Chun Chang, Kai-Chun Hwang and Rong-Jaye Chen, "Boolean functions with high nonlinearity and propagation characteristics," submitted to IEEE Transactions on Information Theory. (SCI/EI) (NSC93-2213-E-305-003-)
4. Jen-Chun Chang, Jun-Shiang Hu and Rong-Jaye Chen, "A construction of Boolean functions with propagation characteristics and resilient properties," submitted to IEEE Transactions on Information Theory. (SCI/EI)(NSC93-2213-E-305-003-)

D. Conference Paper

1. Jen-Chun Chang, Shiao-Fan Chang, "Constructions of Distance-Almost-Increasing Mappings from Binary Vectors to Permutations," International Computer Symposium, Dec 2004. (NSC93-2213-E-305-003-)
2. Han-Chang Liang, Jen-Chun Chang, Rong-Jaye Chen, "New Efficient Constructions of Binary Asymmetric Error-Correcting Codes," International Computer Symposium, Dec 2004. (NSC93-2213-E-305-003-)
3. Kai-Chiun Hunag, Jen-Chun Chang, Rong-Jaye Chen, "A new construction of resilient functions over GF(p) with good cryptographic properties," International Computer Symposium, Dec 2004. (NSC93-2213-E-305-003-)
4. Jen-Chun Chang, Rong-Jaye Chen, T. Klove and Shi-Chun Tsai, "Distance preserving mappings from binary vectors to permutations," IEEE International Symposium on Information Theory (ISIT 2003), Session: Coding Theory I, paper #9, 2003, pp. 14-15. (NSC92-2213-E-415-006-)
5. 羅世帆、張仁俊，"安全的 FTP 檔案傳輸協定的設計與實作"，第一屆流通與全球運籌論文研討會，Oct 2003。(NSC92-2213-E-415-006-)

6. 鄭凱仁、邱楷雯、張仁俊，"PDA 電子郵件安全收發系統之設計與實作"，第四屆產業資訊管理學術暨新興科技實務研討會，Nov 2003。(中華民國資訊管理學會主辦) (NSC92-2213-E-415-006-)

2.3. 子計畫三成果

子計畫三（NSC-91-2213-E-009-101, NSC-92-2213-E-009-034, NSC-93-2213-E-009-009）共發表以下論文：

1. L.-S. Liu, C.-K. Chu, W.-G. Tzeng. A threshold GQ signature scheme. In Proceedings of Applied Cryptography and Network Security Conference (ACNS 03), Lecture Notes in Computer Science 2864, pp. 137-150, 2003.
2. C.-K. Chu, W.-G. Tzeng. Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries. In Proceedings of International Workshop on Practice and Theory in Public-Key Cryptography (PKC 05), Lecture Notes in Computer Science 3386, pp.172-183, 2005.
3. S.-Y. Lin, W.-G. Tzeng. An efficient solution to the Millionaires' problem based on homomorphic encryption. In Proceedings of Applied Cryptography and Network Security Conference (ACNS 05), Lecture Notes in Computer Science 3531, pp.456-466, 2005.
4. C.-M. Hu, W.-G. Tzeng. Compatible Ideal Visual Cryptography Schemes with Reversing. In Proceedings of the 8th Information Security Conference (ISC 05), Lecture Notes in Computer Science 3650, pp.300-313, Springer-Verlag, 2005.
5. C.-J. Lee, C.-J. Lu, S.-C. Tsai and W.-G. Tzeng, Extracting Randomness from Multiple Independent Sources, IEEE Transactions on Information Theory 51(6), pp.2224-2227, 2005.
6. S.-C. Tsai, W.-G. Tzeng and H.-L. Wu, On the Jensen-Shannon Divergence and Variational Distance, IEEE Transactions on Information Theory 51(9), pp.3333-3336, 2005.

3. 成果自評

本總計畫下的三個子計畫共發表 5 篇不錯的國際會議論文（收錄於 LNCS 及 IEEE），5 篇 IEEE Transactions on Information Theory（IT）期刊論文，1 篇 IEEE Transactions on Wireless Communication 期刊論文，2 篇 IPL 期刊論文，1 篇 Designs, Codes, and Cryptography 期刊論文，和數篇國內會議及期刊論文。

IT 的水準非常高，impact factor 達 2.245，國內很少有論文在這期刊上發表，本計畫能夠發表 5 篇在這個期刊上，更顯得可貴。

綜合來說，本計畫成果豐碩，完全達成任務。