

行政院國家科學委員會專題研究計畫 期中進度報告

總計畫(2/3)

計畫類別：整合型計畫

計畫編號：NSC92-2213-E-009-033-

執行期間：92 年 08 月 01 日至 93 年 07 月 31 日

執行單位：國立交通大學資訊科學學系

計畫主持人：曾文貴

計畫參與人員：李尚辰、李惠龍

報告類型：精簡報告

處理方式：本計畫可公開查詢

中 華 民 國 93 年 5 月 27 日

行政院國家科學委員會補助專題研究計畫 ☐ 成果報告
☒ 期中進度報告

總計畫：理論密碼學與應用 (2/3)

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 92-2213-E-009-033-

執行期間：92 年 8 月 1 日至 93 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：李尚辰、李惠龍

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 93 年 5 月 31 日

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。密碼學的理论基礎包含很廣，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。

關鍵詞：密碼理論、零知識證明、可證明安全、編碼。

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.

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

一、緣起與目的

本計畫的主要目的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 (coding) 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。

二、研究成果

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。本年度(第一年度)的研究成果如下：

1. 子計畫一針對某些布林代數的建構方法進行研究，同時也提出一些新的建構方法，並探討其線性複雜度、相關免疫性、非線性度與函數的傳播特徵等性質。子計畫一亦針對基於 $GF(q)$ 上的串流密碼系統進行研究，探討構成系統的基本組成原件線性反饋移位暫存器、過濾函數、組合函數的特性，並對原有的必備性質加以分析研究，且針對串流密碼系統的攻擊方法：B-M 攻擊法、相關攻擊法、最佳仿射近似攻擊法與識別攻擊法的防範方式，以此建構出一個安全且有效率的串流密碼系統。我們證明了一些相關的定理，請見子計畫一的報告。子計畫一接著將系統實際的運用在無線通訊上，並給予安全性與效率分析。
2. 子計畫二到目前為止整理了一些串流密碼中關於擬隨機序列產生器的相關資料文獻，並實際撰寫了過濾產生器、組合產生器與鐘控產生器等擬隨機序列產生器模組的相關程式，且也同時撰

寫了頻率檢測法、連續檢測法、撲克檢測法、遊程檢測法及自動相關檢測法等統計檢測程式，並透過這些檢測程式，實際的測試每種擬隨機序列產生器的輸出二元序列是否通過檢測程式的統計檢測。本子計畫目前也正在著手研究其他相關測試序列隨機性的檢測方式；另外對於擬序列產生器中的布林函數，目前是沿用已知的布林函數，未來，也希望實際設計一個具有好的性質的布林函數來取代現有的布林函數。

3. 子計畫三提出 GQ 簽章法的分散門檻簽章系統，並證明其安全性。論文已經在 ACNS 03 國際會議上發表，論文集為 Lecture Notes in Computer Sciences 2846, pp. 137-150, Springer, 2003。

目前比較重要的數位簽章法有 RSA、ElGamal、DSA 及 GQ。其中 RSA、ElGamal 及 DSA 簽章法都已經有分散式門檻簽章系統，包含 DKG 及 TFE 兩部分。但是 GQ 簽章法的分散式門檻系統一直沒有解決，我們首先有了這項的突破。我們可以證明以上的分散式 GQ 簽名具有不可偽造性及強健性，有要沒有超過一半的參與者被攻擊，就可一產生有效的簽名出來。

三、計畫成果自評

我們的研究結果發表了國際會議刊論文，水準不錯，目前還有論文在投稿及撰寫中。以成果來看，我們達成了本計畫的目的。

參考文獻

- [1] C. Carlet, "On the coset weight divisibility and nonlinearity of resilient and correlation immune functions," in Sequences and Their Applications — SETA 2001 (Discrete Mathematics and Theoretical Computer Science). Berlin, Germany:

- Springer Verlag, pp. 131–144, 2001.
- [2] T. Johansson, and F. Jonsson, “Correlation attacks, convolutional codes, and iterative decoding,” Proceedings of the 1999 IEEE Information Theory and Communications Workshop, pp. 58–60, 1999.
 - [3] T. Johansson and F. Jönsson, “Fast Correlation Attacks Based on Turbo Code Techniques,” Advances in Cryptology, Crypto’99, Springer-Verlag, , Berlin, pp.181-197, 2000.
 - [4] S. Maitra and E. Pasalic, “Futher constructions of resilient Boolean functions with very high nonlienariy,” IEEE Tran. On Info. Theory, VOL.48, NO.7, JULY 2002.
 - [5] R. Menicocci, and J. Dj. Golic, , “Correlation attacks on up/down and stop/go cascades,” IEEE Transactions on Information Theory, VOL. 45, pp. 486–498, March 1999.
 - [6] E. Pasalic, T. Johansson, and P. Sarkar, “New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity,” In Workshop on Coding and Cryptography-WCC 2001, Published in Electronic Notes in Discrete Mathematics. Amsterdam, Elsevier Science, VOL. 6, 2001.
 - [7] E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar, “New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity,” Electronic Notes in Discrete Mathematic, VOL, 6, 2001.
 - [8] P. Sarkar and S. Maitra, “ Construction of nonlinear Boolean functions with important cryptographic properties,” In Advances in Cryptology-EUROCRYPT 2000, Berlin, Springer Verlag, VOL. 1807, pp. 485-506, 2000.
 - [9] P. Sarkar and S. Maitra, “Nonlinearity bounds and constructions of resilient boolean functions,” In Advances In Cryptology-CRYPTO 2000, Berlin, Springer-Verlag, VOL. 1880, pp. 515-532., 2000
 - [10] Seberry, etal., “Non-linearity balanced Boolean functions and their propagation characteristic,” Advances in Cryptology, Crypt’93, Springer-Verlag, Berlin, pp. 6-12, 1994.
 - [11] Y. Zheng and X. M. Zhang, “Improved upper bound on the nonlinearity of high order correlation immune functions,” In Selected Areas in Cryptography-SAC 2000, Berlin, Springer-Verlag, VOL. 2012, pp. 264-274, 2000.
 - [12] Golic, J.D., “Edit distances and probabilities for correlation attacks on clock-controlled combiners with memory,” IEEE Transactions on Information Theory, Volume: 47 Issue: 3, March 2001, 1032–1041.
 - [13] Jonsson, F.; Johansson, T., “Correlation attacks on stream ciphers over $GF(2^{\sup n})$,” Proceedings. 2001 IEEE International Symposium on Information Theory, 2001, pp. 140.
 - [14] Canteaut, A.; Trabbia, M., “Compared performance of fast correlation attacks an stream ciphers,” IEEE International Symposium on Information Theory, 2000, pp. 213.

- [15] Ran Canetti, Uriel Feige, Oded Goldreich, and Moni Naor, "Adaptively secure multi-party computation", In Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC '96), pages 639--648. ACM, 1996.
- [16] Ran Canetti, Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin, "Adaptive security for threshold cryptosystems," In Proceedings of Advances in Cryptology - CRYPTO '99, volume 1666 of LNCS, pages 98--115. Springer-Verlag, 1999.
- [17] Manuel Cerecedo, Tsutomu Matsumoto, and Hideki Imai, "Efficient and secure multiparty generation of digital signatures based on discrete logarithms, " IEICE Trans. Fundamentals, E76-A(4):532--545, 1993.
- [18] Yvo Desmedt, "Society and group oriented cryptography: A new concept", In Proceedings of Advances in Cryptology - CRYPTO '87, volume 293 of LNCS, pages 120--127. Springer-Verlag, 1987.
- [19] Yvo Desmedt and Yair Frankel, "Shared generation of authenticators and signatures," In Proceedings of Advances in Cryptology - CRYPTO '91, volume 576 of LNCS, pages 457--469. Springer-Verlag, 1991.
- [20] Olivier Delos and Jean-Jacques Quisquater, "An identity-based signature scheme with bounded life-span", In Proceedings of Advances in Cryptology - CRYPTO '94, volume 839 of LNCS, pages 83--94. Springer-Verlag, 1994.
- [21] Yair Frankel, Peter Gemmell, Philip D. MacKenzie, and Moti Yung, "Optimal-resilience proactive public-key cryptosystems," In Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS '97)}, pages 384--393. IEEE, 1997.
- [22] J. Benaloh, D. Tuinstra, "Receipt-free secret-ballot elections", Proceedings of the 26th ACM Symposium on the Theory of Computing (STOC), pp.544-553, 1994.
- [23] B. Barak, A. Herzberg, D. Naor and E. Shai, "The Proactive Security Toolkit and Applications", Proceedings of the ACM Conference on Computer and Communications Security, pp.18-27, 1999.