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(1/3)

計畫類別：整合型計畫

計畫編號：NSC91-2213-E-009-100-

執行期間：91年08月01日至92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：朱成康、劉世弘

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國　92年5月26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（1/3）
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　91－2213－E－009－100－
執行期間：　91 年　8　月　1　日至　92　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： 朱成康、劉世弘

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 92 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。

<u>關鍵詞</u>：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.

<u>Keywords</u>: **theoretical cryptography, zero-knowledge proof system, provable security, coding.**

一、緣起與目的

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。

二、研究成果

由於總計畫的經費被大砍，只剩 27 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. 子計畫三發現一個一般分散式金鑰產生演算法的安全漏洞，並提出補救的方法。成果『Distributed key generation as a component of an integrated protocols』發表在 ICICS 02 (Information and Communications Security) 國際會議上，LNCS 2513, Springer Verlag。

2. 子計畫二研究串流密碼器的核心元件—「組合布林函數」的建構，我們同時考慮了平衡性、相關免疫性、非線性杜、與傳播特徵等性質，設計出一些建構方法。這些成果將收錄在黃凱群同學的碩士論文中，並將整理成論文，投稿學術會議或期刊。

3. 子計畫二研究編碼理論與串流密碼的建構和攻擊之間存的關係，這些技術與理論如何整合，我們還在摸索中，目前有一些初步的成果 Jen-Chun Chang, Rong-Jaye Chen, Torleiv Klove, and Shi-Chun Tsai, “Distance-Preserving Mappings from Binary Vectors to Permutations,” IEEE Trans. on Info. Theory, Vol. 49, No. 4, APRIL 2003, pp. 1054-1059.

4. 子計畫一探討並設計新的 Extractor，探討 list coding 在密碼學的應用及 Extractor code 在記憶裝置的應用，相關結果正在寫成論文。

三、計畫成果自評

我們的研究結果發表了國際會議及期刊論文，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] N. Nisan and A. Ta-Shma. Extracting randomness : A survey and new constructions. Journal of Computer and System Sciences, 1998. To appear. Preliminary versions in [Nis96, TS96]

[2] Noam Nisan and Avi Wigderson. Hardness vs randomness. Journal of Computer and System Sciences, 49(2):149-167, October 1994.

[3] R. Raz, O. Reingold, and S. Vadhan. Extracting all the randomness and reducing the error in Trevisan's extractors. In Proceedings of the 31st ACM Symposium on Theory of Computing, pages 149-158, 1999.

[4] A. Ta-Shma and D. Zuckerman. "Extractor codes", In Proceedings of the 33rd Annual ACM Symposium on Theory of Computing, 2001.

[5] A. Ta-Shma, D. Zuckerman, S. Safra. "Extractors from Reed-Muller codes", Electronic Colloquium on Computational Complexity, Report No. 36 (2001).

[6] R. Shaltiel and C. Umans, "Simple Extractors for All Min-Entropies and a New Pseudo-Random Generator", IEEE Symposium on Foundations of Computer Science (FOCS'01)

[7] Luca Trevisan. Construction of extractors using pseudo-random generators. In Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing. Pages 141-148, Atlanta, Georgia, 1-4 May 1999.

[8] N. Nisan. Extracting randomness: How and Why. In Proceedings of the 11th IEEE Conference on Computational Complexity,page 44-58, 1996.

[9] N. Nisan and A. Wigdersn. Hardness vs randomness. Journal of Computer and System Sciences, 49149-167, 1994. Preliminary version in Proc. FOCS'98.

[10] R. Canetti, "Security and composition of multiparty cryptographic protocols", Journal of Cryptology 13(1), pp. 143-202, 2000.

[11] M. Fischlin, "A cost-effective pay-per-multiplication comparison method for millionaires", Proceedings of The Cryptographer's Track at RSA Conference 2001 (CT-RSA 2001), Lecture Notes in Computer Science 2020, pp.457-472, Springer-Verlag, 2001.

[12] Y. Frankel, P. MacKenzie, M. Yung, "Adaptively-secure optimal-resilience proactive RSA", Proceedings of Advances in Cryptology -- Asiacrypt 99, Lecture Notes in Computer Science 1716, pp.180-194, Springer-Verlag, 1999.

[13] M. Franklin, R.N. Wright, "Secure communication in minimal connectivity

models", Journal of Cryptology 13(1), pp.9-30, 2000.

[14] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems", Proceedings of Advances in Cryptology -- Eurocrypt 99, Lecture Notes in Computer Science, Springer Verlag, 1999.

[15] V. Shoup, "Practical Threshold Signatures", Proceedings of Advances in Cryptology -- Eurocrypt 2000, Lecture Notes in Computer Science 1807, pp.207-220, Springer-Verlag, 2000.

[16] Thomas Johansson and Fredrik Jönsson, "Fast Correlation Attacks Based on Turbo Code Techniques," Advances in Cryptoloty, Crypt'99, Springer-Verlag, 2000, Berlin, 181-197.

[17] 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.

[18] Jonsson, F.; Johansson, T., "Correlation attacks on stream ciphers over GF(2n)," Proceedings. 2001 IEEE International Symposium on Information Theory, 2001, pp. 140.

[19] Canteaut, A.; Trabbia, M., "Compared performance of fast correlation attacks an stream ciphers," IEEE International Symposium on Information Theory, 2000, pp. 213.

[20] Jonsson, F.; Johansson, T., "Theoretical analysis of a correlation attack based on convolutional codes," IEEE International Symposium on Information Theory, 2000, pp. 212.

[21] Johansson, T.; Jonsson, F., "Correlation attacks, convolutional codes, and iterative decoding," Proceedings of the 1999 IEEE Information Theory and Communications Workshop, 1999, pp. 58 –60.

[22] Menicocci, R.; Golic, J.Dj., "Correlation attacks on up/down and stop/go cascades," IEEE Transactions on Information Theory, Volume: 45 Issue: 2 , March 1999, pp. 486 –498.

[23] Simpson, L.; Dawson, E.; Golic, J.; Salmasizadeh, M., "Fast correlation attacks on the multiplexer generator," IEEE International Symposium on Information Theory, 1998, pp. 270.

[24] P. Hawkes and G. Rose. "Primitive specification and supporting documentation for SOBER-t16 submission to NESSIE." In Proceedings of the First Open NESSIE Workshop, 13-14 November 2000, Heverlee, Belgium.

[25] P. Hawkes and G. Rose. "Primitive specification and supporting documentation for SOBER-t32 submission to NESSIE." In Proceedings of the First Open NESSIE Workshop, 13-14 November 2000, Heverlee, Belgium.

[26] P. Sarkar and S. Maitra, “Construction of nonlinear Boolean functions with important cryptographic properties,” In Advances in Cryptology-EUROCRYPT 2000, Berlin, Germany:Springer Verlag, vol. 1807, pp. 485-506, 2000.

[27] P. Sarkar and S. Maitra, “Nonlinearity bounds and constructions of resilient boolean functions,” In Advances In Cryptology-CRYPTO 2000, Berlin, Germany:Springer-Verlag, 2000, vol. 1880, pp. 515-532.

[28] Y.V. Tarannikov, “On resilient Boolean functions with maximal nonliearity,” In Progress in Cryptology-INDOCRYPT 2000, Berlin, Germany:Springer Verlag, 2000, vol. 1977. pp. 19-30.

[29] Y. Zheng and X. M. Zhang, “Imoproved upper bound on the nonlineatity of high order correlation immune functions,” In Selected Areas in Cryptography-SAC 2000, Berlin, Germany:Springer-Verlag, vol. 2012, pp. 264-274, 2000.

[30] C. Carlet, “On the coset weight divisibility and nonlineatity of resilient and correlation immune functions,” In Sequences and Their Applications-SETA 2001, Berlin, Germany:Springer-Verlag, pp. 131-144, 2001.

[31] E. Pasalic, Smaitra, T. Johansson, and P. Sarkar, “New constructions of reilient 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, The Netherlands:Elseriver Science, vol. 6, 2001.

[32] S. Maitra, “Correlation immune boolean functions with very high nonlineatity,” Cryptology ePrint Archive[Online]. Available:eprint.iacr.org.

[33] S. Maitra and E. Pasalic, “Futher constructions of resilient boolean functions with very high nonlienariy,” IEEE Tran. On Info. Theory, Vol.48, No.7, 2002.