行政院國家科學委員會專題研究計畫　期中進度報告

子計畫三：分散式門檻密碼系統的研究(1/3)

計畫類別： 整合型計畫
計畫編號： NSC91-2213-E-009-101-
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

報告類型： 精簡報告
報告附件： 出席國際會議研究心得報告及發表論文
處理方式： 本計畫可公開查詢

中　華　民　國 92 年 6 月 23 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
子計畫三：分散式門檻密碼系統的研究（1/3）
Study of Distributed Threshold Cryptographic Protocol

計畫類別：□ 個別型計畫　　☑ 整合型計畫
計畫編號：NSC　91－2213－E－009－101－
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： 李佳蓉、張振偉、李尚辰、林坤杉、黃佩琳

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

本子計畫研究分散式門檻密碼方法的安全模式(security models)，定義合理的安全條件；我們設計有效率且可證明安全的分散式門檻密碼協定，我們也研究具預防性質的分散式門檻密碼協定。

關鍵詞：分散式門檻密碼、預防式密碼、安全模式。

英文摘要

The final security of cryptographic protocols resides on secret keys. How to protect secret keys is an important issue for the key-based information security. We can distribute the secret key into a set of users such that each user holds a share of the key. A set of users over a threshold t can perform the designated function, while the number of users under the threshold cannot get any information about the shared secret key. This constitutes the model for the distributed threshold cryptographic protocols. Under this model, the attacker need get at least t shares to break into the protocol. Nevertheless, the attacker has long time to obtain the shares. To deter this attack, users can renew their shares for each period of time, but the shared secret key remains unchanged. In a new period of time, the old shares of previous time periods are useless. Therefore, the attacker need get at least t shares during a period of time to break the protocol. Otherwise, when time migrates to the next period, the old shares that the attacker obtained become useless. This model is called “proactive” security.

In this project we research on the security models of distributed threshold cryptographic systems. We design efficient and provably secure distributed threshold cryptographic protocols. We also extend this research to the model of proactive security.

Keywords: threshold cryptography, proactive security complexity, security model.

一、計畫緣起及目的

密碼協定的最終安全落在私密金匙(secret key)上，如何保護金匙的安全是一

個重要的課題。分散式門檻密碼理論是將金匙分成幾個金匙分享值(shares)，分別由不同的使用者保管，在執行設定的功能時，必須有一定數目的使用者同時動作才能夠完成任務。這使得攻擊者必須同時擁有一定數目的金匙分享值才能夠破解密碼系統，這樣保障了基本的安全。我們可以更進一步要求這些使用者『定期』更新它們的金匙分享值，新的金匙分享值和舊的金匙分享值沒有任何關連，但是共享的私密金匙並沒有改變，使用新的金匙分享值能然能夠完成工作，但是攻擊者必須在『一定的時間』內得到一定數目的金匙分享值，否則一旦使用者更新了它們的金匙分享值，攻擊者得到的金匙分享值就沒有任何價值了。具有定期更新金匙分享值的密碼協定叫做『預防式』（proactive）的密碼協定。

本子計畫的目的是研究分散式門檻密碼系統的安全模式及設計安全的分散式門檻密碼系統，我們也研究預防式密碼系統。分散式門檻密碼系統可以增進將密碼系統的安全，藉由分散保有金匙及跨過一定門檻門檻既可執行工作的特性，達到安全的強固性。現在設計密碼系統的發展是走向『可證明安全』，強調密碼系統必須是在合理的假設下，可以經由嚴謹的推論方法證明其安全。本計畫將強調基礎研究，包含如何利用資訊科學的理論基礎來研究分散式門檻密碼密碼系統。我們希望三年內能夠達成下列目標：

1. 研究分散式門檻密碼系統的安全模式：利用理想模式為基礎，再研究可能的攻擊方式，我們希望能夠嚴謹的定義出合理的安全分散式門檻密碼模式。
2. 研究分散式門檻密碼系統的安全證明：正規的證明是目前設計密碼系統必要的前提，我們將熟悉及發展證明密碼安全的技巧；除此之外，我們還將研究資訊科學的理論，例如非交換性的零知識證明等。
3. 設計安全的分散式門檻密碼系統：我們將設計一些安全的分散式門檻密碼系統，例如簽章系統、拍賣系統及投票系統等。
4. 增進分散式門檻密碼系統的效率：我們將研究如何增進分散式門檻密碼系統的效率，特別是回合數的效率，以目前電腦強大的計算能力來看，使用者交換訊息所花的時間是協定效率的瓶頸，因此我們特別重視回合數的效率。
5. 增進和其他子計畫的整合的研究：本計畫和其他子計畫有一些相關性，我們將探討如何與其他子計畫整合，並將其他子計畫的研究成果應用在本計畫上。
6. 將研究成果應用在其它的問題上：本計畫的研究成果應該可以應用在其他密碼相關的問題上。

二、研究成果

本年度(第一年度)的研究成果如下：

1. 我們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。

   分散式金鑰系統包含兩的部分：一是分散式產生與分配金鑰持份

（DKG），二是執行門檻式函數（TFE）。以往做離散對數(DL)為基礎的 DKG 時，都是單獨討論如何產生及分配金鑰持份(key share)及其安全性，因此 DKG 演算法雖然符和單獨的安全要求，但是金鑰持份使用在 TFE 時卻發生了不安全的情形，我們首先指出這種安全上的漏洞。

我們接著使用預防式密碼的技巧改正了這項錯誤，並證明我麼提出的改正方法在同時考慮 DKG 及 TFE 時是正確且安全。

2. 我們提出 GQ 簽章法的分散門檻簽章系統，並證明其安全性。論文正在投稿中。

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，我們證明我們設計的演算法和解強 RSA 問題一樣難。

3. 我們研究分散式代理簽章系統，提出可以限制使用時間的金鑰代理方法。成果現正寫成孫狄雯的碩士論文，完成後將投稿發表。

4. 我們繼續改進去年的成果『Robust key-evolving public key encryption schemes』，提出更有效率的方法，論文正在撰寫中。

現今公開金鑰加密系統的公開及私密金鑰都是固定的，使用者一直使用他的私密金鑰直到過了有效期限或將金鑰廢止為止。我們提出一種可能會發生的情形，如果使用者的私密金鑰被偷走，但是使用者沒有發覺，因此繼續使用，如果是如此，偷竊者就可以一直解出送給使用者的加密資料。

為了解決上述的問題，我們提出金鑰演化的公開金鑰機加密法，使用者每隔一段時間就會將他的私密金鑰改變，同時舊有的私密金鑰就失去效用。即使使用者沒有發現私密金鑰遺失，到下一個時段更新私密金鑰之後，加密的安全性就恢復了。

當然加密時得做一些配合，我們將時間分為一些時段 T_i, $i \geq 1$，使用者的公開金鑰是固定的，加密時把公開金鑰 PK 現在時段 T_i 加以運算得到 PK_i，再利用 PK_i 加密資料，如此，使用者在 T_i 時段的私密金鑰就可以解密。

5. 我們和其他子計畫每週都有論文討論，和其他子計畫合作密切。建立了合作的機制。

三、計畫成果自評

我們的研究結果發表了一篇 ICICS 會議論文，水準還不錯，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. 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.
2. 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.

3. D. Boneh, M. Franklin. "Efficient generation of shared RSA keys". Proceedings of Advances in Cryptography -- Crypto 97, pp. 425-539, 1997.
4. R. Canetti, “Security and composition of multiparty cryptographic protocols”, Journal of Cryptology 13(1), pp. 143-202, 2000.
5. R. Canetti, R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Adaptive security for threshold cryptosystems", Proceedings of Advances in Cryptology -- Crypto '99, Lecture Notes in Computer Science 1666, pp.98-115, Springer-Verlag, 1999.
6. R. Canetti, R. Gennaro, A. Herzberg, D. Naor, "Proactive security: long-term protection against break-ins", CryptoBytes, 3(1), 1997.
7. R. Canetti, S. Halevi, A. Herzberg, "Maintaining authenticated communication in the presence of break-ins”, Journal of Cryptology 13(1), pp.61-106, 2000.
8. R. Canetti, E. Kushilevitz, R. Ostrovsky, A. Tosen, “Randomness versus fault-tolerance”, Journal of Cryptology 13(1), pp.107-142, 2000.
9. R. Cramer, M. Franklin, B. Schoenmakers, M. Yung, "Multi-authority secret-ballot elections with linear work", Proceedings of Advances in Cryptology -- Eurocrypt '96, Lecture Notes in Computer Science 1070, pp.72-83, Springer-Verlag, 1996.
10. R. Cramer, R. Gennaro, B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme", Proceedings of Advances in Cryptology -- Eurocrypt '97, Lecture Notes in Computer Science 1233, pp.103-118, Springer-Verlag, 1997.
11. Y. Desmedt, Y. Frankel, "Threshold cryptosystems", Proceedings of Advances in Cryptology -- Crypto 89, Lecture Notes in Computer Science 435, pp.307-315, Springer-Verlag, 1989.
12. 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.
13. 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.
14. M.K. Franklin, M.K. Reiter, "The design and implementation of a secure auction service", IEEE Transactions on Software Engineering 22(5), pp.302-312, 1996.
15. M. Franklin, R.N. Wright, “Secure communication in minimal connectivity models”, Journal of Cryptology 13(1), pp.9-30, 2000.
16. P. Gemmel, "An introduction to threshold cryptography", CrytoBytes 2(7), 1997.
17. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Robust Threshold DSS

Signature". Proceedings of Advances in Cryptology - Eurocrypt 96. Springer-Verlag Lecture Notes in Computer Science 1070, pp. 354-371, 1996.

18. 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.
19. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Robust and Efficient Sharing of RSA Functions". In Advances in Cryptology - Eurocrypt 96, pp. 354-371, Lecture Notes in Computer Science 1070, Springer-Verlag, 1996.
20. A. Herzberg, S. Jarcki, H. Krawczyk, M. Yung, "Proactive secret sharing, or how to cope with perpetual leakage", Proceedings of Advances in Cryptology -- Crypto 95, Lecture Notes in Computer Science 963, pp.339-352, Springer-Verlag, 1995.
21. M. Hirt, U. Muarer, “Palyer simulation and general adversary structures in perfect multiparty computation”, Journal of Cryptology 13(1), pp.31-60, 2000.
22. I. Ingemarsson, G.J. Simmons, "A protocol to set up shared secret schemes without the assistance of a mutualy trusted party", Proceedings of Advances in Cryptology -- Eurocrypt 90, Lecture Notes in Computer Science 473, pp.266-282, Springer-Verlag, 1990.
23. R. Ostrovsky, M. Yung, "How to withstand mobile virus attacks", Proceedings of the 10th ACM Symposium on Principles of Distributed Computing (PODC), pp.51-61, 1991.
24. T. Pedersen, "A threshold cryptosystem without a trusted party", Proceedings of Advances in Cryptology -- Eurocrypt 91, Lecture Notes in Computer Science 547, pp.522-526, Springer-Verlag, 1991.
25. T. Rabin, "A Simplified Approach to Threshold and Proactive RSA". Proceedings of Advances in Cryptology, Lecture Notes in Computer Science, Springer-Verlag, 1998.
26. K. Sako, "An auction protocol which hides bids of losers", Proceedings of Third International Workshop on Practice and Theory in Public Key Cryptography 2000 (PKC 2000), Lecture Notes in Computer Science 1751, pp.422-432, Springer-Verlag, 2000.
27. A. Shamir, "How to share a secret", Communications of the ACM 22(11), pp.612-613, 1979.
28. V. Shoup, "Practical Threshold Signatures", Proceedings of Advances in Cryptology -- Eurocrypt 2000, Lecture Notes in Computer Science 1807, pp.207-220, Springer-Verlag, 2000.