

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(2/3)

計畫類別：整合型計畫

計畫編號：NSC92-2213-E-009-034-

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：鍾季穎、莊吳祐、黃珮琳、張振偉

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 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
子計畫三：分散式門檻密碼系統的研究 (2/3)

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 92-2213-E-009-034-

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：鍾季穎、莊吳祐、黃珮琳、張振偉

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

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(第二年度)的研究成果如下：

1. 我們提出 GQ 簽章法的分散門檻簽章系統，並證明其安全性。論文已經在 ACNS 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。

強 RSA 問題是給定一合成數 n 及 $y \in \mathbb{Z}_n^*$ ，計算 α 及 $\beta \neq 1$ ，使得 $y = \alpha^\beta \pmod{n}$ 。我們證明我們設計的演算法和解強 RSA 問題一樣難。我們的分散式 GQ 簽名中，金鑰持份 (key share) 由一中心的 dealer 分配給各參與者 P_i ，因此公開金鑰為 $PK = (n, e, g, v)$ ，其中 g 是 $\mathbb{QR}_n^*$ 的 generator， $v = s^e \pmod{n}$ ， s 為私密金鑰是一多項式 $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_tx^t$ 的常數項 $s = g^{a_0}$ ；每一位參與者 P_i 的金鑰持份為 $SK_i = (n, e, g, s_i)$ ，其中 $s_i = g^{f(i)} \pmod{n}$ 。我們的分散式 GQ 簽名系統如下：

- (1) 所有的參與者執行 INT-JOIN-EXP-RVSS 以產生 $y = g^{\text{fr}(0)e} \pmod{n}$ ，每一 P_i 得到 $r_i = g^{\text{fr}(i)} \pmod{n}$ 。
- (2) 所有的參與者計算 $\sigma = H(y, M)$ 。
- (3) 所有的參與者執行 INT-JOIN-ZVSS 使得每一參與者 P_i 得到 $c_i = g^{L \cdot \sigma(i)} \pmod{n}$ 。
- (4) 每一參與者計算個別的部分簽名： $z_i = (r_i s_i^{\sigma})^L c_i \pmod{n}$ ，然後公布之。

然後由第三者將這些部分簽名整合成對 M 的簽名如下：

$$z' = \prod_{j=1}^{t+1} z_{ij}^{\lambda_{0,ij} L} \pmod{n}$$

其中 z_{ij} 為 $t+1$ 個有效的部分簽名， λ_{ij} 為 Lagrange 的係數。

簽名的驗證就如同 GQ 簽名的驗證一樣。

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。詳細方法及證明請參考所發表的論文。

2. 我們也正在研究分散式忘卻式傳輸 (OT) 的方法, 之前我們已經提出最有效率的 1-out-of-n OT 協定 (發表在 PKC 及 IEEE TC), 我們研究分散式 OT 系統, 目前已經可以將其擴展到 k-out-of-n 的情形, 非常有效率, 完成後將投稿發表。
3. 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 ACNS 會議論文, 論文集為 LNCS 系列 2846, 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. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.