行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※　　　　演化式公開金匙密碼系統的研究　　　　※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：個別型計畫

計畫編號：NSC　90－2213－E－009－152－

執行期間： 90 年 8 月 1 日至 91 年 7 月 31 日

計畫主持人：曾文貴 教授

共同主持人：

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

執行單位：國立交通大學 資訊科學系

中　華　民　國　91 年　7 月　31 日

演化式公開金匙密碼系統的研究

Study on Key-Evolving Public-Key Encryption Schemes

計畫編號：NSC 90-2213-E-009-152
執行期限：90 年 8 月 1 日至 91 年 7 月 31 日
主持人：曾文貴 教授 交通大學 資訊科學系
執行機構：國立交通大學 資訊科學系
E-mail: tzeng@cis.nctu.edu.tw

一、中文摘要

在這個計畫中我們研究金匙演化的公開金匙加密系統，目的在於找到一種新的加密方法，這種加密方法是將時間切割成幾個區段，當時間由區段 T_i 進入 T_{i+1} 時，解密的金匙會改變，也就是解密金匙將由 SK_i 演化成 SK_{i+1}，但是公開金匙卻是不變的；這樣的加密系統的好處在於如果目前的解密金匙不小心被洩漏，並不會影響其他時間區段的通訊安全，這種加密系統的作法是類似前向安全（forward secure）的簽章系統。

在過去『前向安全』的密碼方法只有針對簽章做研究，而沒有針對加密方法做探討；因此，在此計畫中將研究具前向安全性的公開公匙加密系統，使得加密的訊息在各個時間區段是獨立的。我們將證明我們設計的系統可以抵擋被動攻擊及主動式選擇性的密文攻擊。

關鍵詞：金匙演化、前向項安全、公開金匙加密，可證明安全。

Abstract

In the project, we study key-evolving public-key encryption schemes. The goal is to propose new public key encryption schemes, which is like forward-secure digital signature schemes. Let time be divided into time periods such that at time period i, the decryptor holds the secret key SK_i, while the public key PK is fixed during its lifetime. When time makes a transit from period i to i+1, the decryptor updates its private key from SK_i to SK_{i+1} and deletes SK_i immediately. The key-evolving paradigm assures that compromise of the private key SK_i does not jeopardize the message encrypted at the other time periods.

In the past, forward-secure digital signatures have been studied, but the public key encryption schemes did not be studied. Therefore, we focus on the study of public key encryption schemes, which should satisfy semantically secure against passive adversaries and the adaptive chosen ciphertext attack under some cryptographic assumptions.

Keywords: key-evolving, key update, forward-secure, public-key encryption..

二、緣由與目的

過去已經有許多文章研究簽章系統，不過之前的研究都是針對固定金匙的簽章系統做研究。這些簽章系統有個特性就是，在有效的生命週期裡使用固定的一把金鑰對，一旦有一天，攻擊者取得了此私密金匙，將可以簽署（在此之前或之後的）任意的文件，這將危害到簽署人的權益。為了避免這種情況，保證不會任意製造在此之前任何文件的簽章，即使私密金匙被洩漏。因此有人利用金匙演化的技巧，來達到這個目的，也就是具有前向安全(forward secure)的簽章密碼系統。簽署者可以利用目前的私密金鑰去計算下一個區段的金鑰，但是利用目前的私密金鑰，卻無法推出之前時間的私密金鑰；如此，將使得一個攻擊者，如果取得目前的私密金鑰，可以簽署目前至往後的任意文件，卻無法偽造在此之前的時間之文件簽章。

Bellare 和 Miner 於 1999 年提出前向安全的簽章系統[20]，他們的方法是利用分解兩個大質數相乘是困難的問題(Factoring)，使得解二次方根也是困難的，來設計他們的簽章系統。之後，Abdalla 和 Reyzin 提出一個新的簽章系統[1]，基於解二的 1 次方根也是困難的，當然根本的問題也是分解兩個大質數相乘是困難的。2000 年，Abdalla 等人[1]，又將第一個簽章方法，改成分散式的方法，達到分散風險以及可以加入預防性的(proactive)

措施的方法。分散式的方式是個門檻值的方法[9][13][18][22]，只要低於某個門檻值的伺服器數目被攻擊，其餘的伺服器仍然可以正常工作，而且不會洩漏秘密金匙，因此比起單一使用者的系統，分散式的方法是比較安全的。分散式的作法可以進一步配合預防性的概念(proactive)，來達到更安全的境地。預防性的概念(proactive)[6][17][21]是假設一個攻擊者的能力是有限的，我們將主要秘密分享給超過 2t+1 個伺服器，然後將時間切成一段一段的，在一段時間之內攻擊者可以攻擊至多 t 個伺服器，將不會影響系統的安全，當時間進入下一個時段時，2t+1 伺服器的分享(share)會被更新，使得攻擊者所得到的分享，在下一個時區將是無用的。

計畫的目的是在研究金匙演化的公開金匙加密系統，希望系統能夠很有效率及達到可證明安全的目的。

三、結果與討論

本計畫依據密碼學的理論設計了可以證明為安全的演化式公開金鑰加密系統，在我們的系統中，有一個公正的第三者 TA 來幫使用者更新每個時間的解密金匙。

我們的系統具有下列特性：

1. **金匙演化：**新的加密系統達到公開金匙是固定，但是解密的金匙（即私密金匙）隨時間而演化。
2. **安全性的證明：**可以抵擋被動攻擊和主動攻擊，安全性的證明是基於密碼學上的知名假設，而且是嚴謹的證明，而不只是看起來安全而已。
3. **解密的金匙數目最少：**使用者只需一把私密金匙。
4. **有效率的密碼系統：**加密使用少量的計算，具有實用性。
5. **存在可信賴第三者：**此可信賴的第三者，主要協助解密者進行金匙演化，而在加密過程中，並不需要它的介入。
6. **分散式及預防式安全：**我們還將公正的第三者分散式化及預防式化，也就是使用者要更新金匙實，是透過分散式的系統與多個安全伺服器交換訊息以達到金匙演化的目的。各個安全伺服器間也會定期更新它們的金匙持份，只要攻擊者不在短時間內取的很多金匙持份，系統就是安全的。

我們的結果已經發表：

1. **W.-G. Tzeng, Zhi-Jia Tzeng. "Robust Key-Evolving Public-Key Encryption Schemes" In Proceedings of the 5th International Conference on Information and Communications Security (ICICS 02), Lecture Notes in Computer Science 2513, pp.61-72, Springer-Verlag, 2002.**

四、計畫成果自評

我們的研究結果發表了一篇國際會議論文、ICICS 國際會議水準不錯。我們也將把結果投到好的國際期刊上。以成果來看，我們達成了本計畫的目標。

五、參考文獻

[1] M. Abdalla, L.Reyzin, "A new forward-secure digital signature scheme", *Proceedings of Advances in Cryptology -- Asiacrypt 2000*, Lecture Notes in Computer Science 1976, pp.116-129, Springer-Verlag, 2000.

[2] M. Abdalla, S. Miner, C. Namprempre, “Forward security in threshold signature schemes”, manuscripts.

[3] J. Anzai, N. Matsuzaki, T. Matsumoto, "A quick group key distribution scheme with "entity revocation"", Proceedings of Advances in Cryptology -- Asiacrypt 99, Lecture Notes in Computer Science 1716, pp.333-347, Springer-Verlag, 1999.

[4] M. Bellare, P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols", Proceedings of the First ACM Conference on Computer and Communications Security, pp.62-73, 1993.

[5] D. Boneh, "The decisional Diffie-Hellman problem", Proceedings of the Third Algorithmic Number Theory Symposium, Lecture Notes in Computer Science 1423, pp.48-63, Springer-Verlag, 1998.

[6] R. Canetti, O. Goldreich, S. Halevi, "The random oracle methodology revisited", Proceedings of the 30th ACM Annual Symposium on Theory of Computing, pp.209-218, 1998.

[7] R. Canetti, R. Gennaro, A. Herzberg, D. Naor, "Proactive security: long-term protection against break-ins", CryptoBytes, 3(1), 1997.

[8] R. Cramer, V. Shoup, "A practical public key cryptosystem provably secure against adaptive

chosen ciphertext attack", Proceedings of Advances in Cryptology -- Crypto '98, Lecture Notes in Computer Science 1462, pp.13-25, Springer-Verlag, 1998.

[9] I. Damgard, "Towards practical public key cryptosystems secure against chosen ciphertext attacks", Proceedings of Advances in Cryptology -- Crypto 91, Lecture Notes in Computer Science 576, pp.445-456, Springer-Verlag, 1991.

[10] 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.

[11] W. Diffie, P.C. Van Oorschot, M.J. Weiner, "Authentication and authenticated key exchanges", Designs, Codes and Cryptography 2, pp.107-125, 1992.

[12] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory 31(4), pp.469-472, 1985.

[13] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing", Proceedings of the 28th IEEE Annual Symposium on the Foundations of Computer Science, pp.427-437, 1987.

[14] P. Gemmel, "An introduction to threshold cryptography", CrytoBytes 2(7), 1997.

[15] R. Gennaro, S. Jarecki, H. Krawczyk, R. Rabin, “Secure distributed key generation for discrete-log based cryptosystems, Proceedings of Advances in Cryptology – Eurocrypt 99, Lecture Notes in Computer Science 1592, pp. 295-310, Springer-Verlag, 1999.

[16] S. Goldwasser, S. Micali, "Probabilistic encryption", Journal of Computer and System Sciences 28, pp.270-299, 1984.

[17] R. Gennaro, M. Rabin, T. Rabin, "Simplified VSS and fast-track multiparty computations with applications to threshold cryptography", Proceedings of the 17th ACM Symposium on Principles of Distributed Computing(PODC), 1998.

[18] 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.

[19] 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.

[20] C.H. Lim, P.J. Lee, "Another method for attaining security against adaptively chosen ciphertext attacks", Proceedings of Advances in Cryptology -- Crypto 93, Lecture Notes in Computer Science 773, pp.420-434, 1993.

[21] M. Mellare, S.K. Miner, "A forward-secure digital signature scheme", Proceedings of Advances in Cryptology -- Crypto 99, Lecture Notes in Computer Science 1666, pp.431-448, Springer-Verlag, 1999.

[22] 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.

[23] 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.

[24] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing", Proceedings of Advances in Cryptology -- Crypto 91, Lecture Notes in Computer Science 576, pp.129-140, Springer-Verlag, 1991.

[25] D. Pointcheval, J. Stern, "Security proofs for signature schemes", Proceedings of Advances in Cryptology -- Eurocrypt 96, Lecture Notes in Computer Science 1070, pp.387-398, Springer-Verlag, 1996.

[26] C. Rackoff, D. Simon, "Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack", Proceedings of Advances in Cryptology -- Crypto 91, Lecture Notes in Computer Science 576, pp.433-444, Springer-Verlag, 1991.

[27] A. Shamir, "How to share a secret", Communications of the ACM 22(11), pp.612-613, 1979.