行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※　　　具容錯能力的會議金匙系統的研究與製作　　　※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：個別型計畫
計畫編號：NSC　89－2213－E－009－180－
執行期間： 89 **年** 8 **月** 1 **日至** 90 **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 90 **年** 7 **月** 31 **日**

具容錯能力的會議金匙系統之研究與製作

Study on conference key agreement systems with fault tolerance

計畫編號：NSC 89-2213-E-009-180
執行期限：89 年 8 月 1 日至 90 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

當一群人想要在開放式的網路上召開一個會議時，為了安全，他們應該先建立起一把共同的會議金匙，再用此會議金匙加密所有的通訊內容，以保障安全。然而在建立會議金匙的過程中，可能有部份的參與者惡意地欺騙其他的參與者，使得誠實的參與者不能得到共同的會議金鑰值。

本計畫研究一個在沒有可信賴中心存在的分散式環境下，由所有參與者共同建立一會議金鑰的協定。且在惡意的參與者少於一半（或者任意多）的情況下，所有誠實的參與者可以建立起唯一的會議金鑰值，同時以零知識證明的方式證明此協定對於在一旁竊聽的旁觀者而言，將不會洩露出任何的資訊。

關鍵詞：多人會議金匙建立系統，密碼協定，可證明安全，容錯。

Abstract

When a group of members want to hold a conference over Internet, they should establish a common conference key so that the attackers cannot get the information of their communication. We consider not only the eavesdroppers, but also malicious members who try to spoil the conference sot that honest members cannot have a common conference key.

We proposed a distributed conference key agreement system. In our system, honest members can compute a common key no matter how many members are malicious. We also showed that an eavesdropper can not compute any information about the key.

Keywords: conference key agreement, secure multiparty computation, attack

二、緣由與目的

使用網路通訊已經是現在及未來不可或缺的工具，如何讓一群人能夠在網路上安全地召開一個會議(conference)，是有其研究的價值。在實際應用中，已有許多可以讓一群人在網路上溝通交談的工具，一如電子佈告欄(BBS)上的談天室，或是NetMeeting 等類似軟體，皆有非常多的使用者喜歡以此與他人溝通，不過通常運作的方式皆是集中式的方式，就是有一中心的伺服器(Server)存在，想要召開會議與參與會議的使用者，皆要連上此伺服器，所有的通訊皆是經由伺服器連繫，所以一旦伺服器失效，所有的通訊就無法繼續下去。此外，為了能保障通訊內容的安全，應該要能建立一個用以加密此次會議通訊內容的金鑰值，稱為會議金鑰(conference key)。同時希望此會議金鑰是分散式的產生，並非由一中心的伺服器，或是讓會議中某一位參與者決定之。這樣的好處是並不會有任一伺服器或參與者有相較於其他人較大權力，同時也不會有瓶頸發生於協定中某一參與者的情況。可是在這種情況下，每一位參與者的地位皆是相同的，都能影響最後產生的會議金鑰為何，在這樣沒有一個具公信力的第三者存在的情況下，參與者之間又產生了是否可以信賴對方的問題。既然大家是平等的，彼此之間並非完全地信任，也許其中有參與者採取不合作態度，試圖破壞會議金鑰的建立，使得參與會議的眾人不能得到一致的會議金鑰。或是其中有些參與者無法順利進行正常建立的步驟，在會議金鑰是由眾人所共同決定的情況下，只要有一參與者不願或不能正常執行，則建立會議金鑰的程序就失敗了。所以在此計畫中，將研究會議金鑰建立的程序中，加入檢測(detection)以及恢復(recovery)的機制，使得在有部份參與者沒有正常執行建立會議金鑰的情況下，正常運作的使用者依然可以排除這

些沒有遵循程序的參與者，然後安全地得到一共同的會議金鑰。

雖然過去有許多文章討論過這個議題，但是大部分的方法是不具有容錯性質的，或者有容錯性質，但是協定本身是很複雜的；另外有許多方法是無法證明它的安全性，因此我們希望提出的協定是有效率的，而且以正規的方法證明協定是安全的，並且達到認證，隱私性和具有容錯的能力。

要如何達到在一系統中，使得任一組群的參與者皆可以在需要的時候以一共同且私密的會議金鑰來進行一個會議。以最直觀的方法，就是由一具公信力的伺服器，為所有的可能的召開會議的組群皆產生一把會議金鑰。系統中的每一位參與者皆要私密地得知和保存所有的會議金鑰。在召開會議時，使用適當的會議金鑰。可想而知的，這種方式在伺服器可信任的情況下是安全的。但是伺服器和參與者所要產生和和儲存的金鑰值數量為 2^n-n-1，在系統中參與者很多的情況下，是一個很大的負擔。所以需要有更有效率的方法。

在"會議金鑰協定"的研究中，可以分為三類，第一種是為事先散佈(pre-distributed)，金鑰值完全是由每一位參與者事先持有的私密資訊決定。在使用此會議金鑰進行通訊前，此會議的參與者間不需互相交換訊息，然而此種方式的會議金鑰值就缺乏每次會議皆更新(fresh)的能力。第二種是為集中式(centralized)，金鑰值是由某一參與者決定，再安全地傳給其他參與者。此種方式可以達到更新及隨機的目的，但是將會有一參與者具有比其他參與者更大的權力，比其他參與者先得知會議金鑰值，同時也會有比其他參與者更大的負擔。而對其他的參與者而言，必須能完全相信此參與者是公正的。第三種是為分散式(distributed)，金鑰值是為每一位參與者在會議進行前經由通訊共同決定，具有更新與隨機的能力，且每一位參與者的權力和負擔是相同的。

本計畫研究在分散式環境下，設計一個具有容錯性質的會議金匙系統。我們考慮各種可能的攻擊，我們也證明我們系統的安全性。

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分散式會議密碼系統。在此研究的重點主要有兩個，第一個是希望整個協定是分散式(Distributed)的，第二個是希望能具有容錯(Fault-Tolerance)的能力。而此協定將會有下列的性質：

1. 效率(efficiency)：效率方面，我們分成兩方面來說，一是次數的效率(round efficiency)，另外為訊息量(message efficiency)的考量。我們希望所研究的成果能夠達到兩者之一，當然兩者均達到是理想的境界。
2. 認證(authentication)：只有合法的參與者可以廣播訊息，而不合法的參與者，即使廣播訊息，終究會被偵測出事非法的參與者，而被剔除，並且無法得到會議的金匙。
3. 私密的(privacy)：對於非此會議參與者而言，觀察公開傳遞的訊息並不能得到任何有關會議參與者的私密資訊，也不能求出最終建立的會議金鑰值。而對於此會議參與者而言，只要其有不遵循正確步驟的行為就會被檢測並排除，並且不能得知其它正確使用者的私密資訊。
4. 容錯的(fault-tolerant)：由於並非所有的參與者皆為善意的遵循協定步驟，協定中必須有機制可以檢驗出非善意的參與者，將其排除，並使得正確的參與者可以繼續建立金鑰的步驟，並求得一共同的會議金鑰。在廣播(broadcast channel)的網路情況下，只要發生錯誤或非善意的參與者人數少於一半或是任意數，則此協定依然能正確地執行下去，而誠實的參與者求出唯一且相同的會議金鑰值。
5. 更新(fresh)與隨機(random)：會議金鑰(conference key)是由眾參與者於每次會議召開前選則一隨機變數，再經由交換訊息而共同決定。而非由某一參與者或中心伺服器(server)所決定，也非由系統設定時

預先決定，是故每一次建立的會議金鑰值皆不相同，具有更新(fresh)及隨機(random)的性質。

6. 同步的(synchronized)：所有正確的參與者將可同時計算此會議金鑰的值，並沒有一參與者有能力比別的參與者先得知。
7. 可嚴謹證明的(rigid proof)：對於會議金鑰系統的安全性，能以零知識證明(zero-knowledge proof)的方式，嚴謹的方式證明將不會洩漏出任何的私密訊息。

我們的結果已經發表：

1. W.-G. Tzeng. "A provably secure fault-tolerant conference-key agreement protocol," IEEE Transactions on Computers (accepted), 2001.
2. W. Tzeng. “A practical and secure fault-tolerant conference-key agreement protocol” In Proceedings of 2000 International Workshop on Practice and Theory in Public-Key Cryptography (PKC 00), Lecture Notes in Computer Science 1751, pp.1-13, Springer-Verlag, 2000.
3. W. Tzeng, Z.-J. Tzeng. “Round-efficient conference-key agreement protocols with provable security”. In Proceedings of Advances in Cryptology - Asiacrypt 2000, Lecture Notes in Computer Science 1976, pp.614-618, Springer-Verlag, 2000.
4. 張德竟. “以密碼為基礎的動態會議金鑰系統.” 交通大學資訊科學系碩士論文. May, 2001.

四、計畫成果自評

我們的研究結果發表了兩篇會議論文、一篇期刊論文及一篇碩士論文。其中會議和期刊的論文都有相當有水準。以成果來看，我們達成了本計畫的目的。

五、參考文獻

1. M. Ben-Or, S. Goldwasser, A. Wigderson, ” Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation”, *Proceedings of the 20th ACM Symposium on the Theory of Computing*, pp. 1-10, 1988.
2. S. Berkovits, ”How to Broadcast a Secret”, *Advances in Cryptology: Proceedings of Eurocrypt ’91*, Lecture Notes in Computer Science 547, Springer-Verlag, pp. 535-541, 1991.
3. R. Blom, ”An Optimal Class of Symmetric Key Generation Systems”, *Advances in Cryptology: Proceedings of Crypto ’84*, Lecture Notes in Computer Science 196, Springer-Verlag, pp. 335-338, 1985.
4. C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, ”Perfectly-Secure Key Distribution for Dynamic Conferences”, *Advances in Cryptology: Proceedings of Crypto ’92*, Lecture Notes in Computer Science 740, Springer-Verlag, pp. 471-486, 1993.
5. M. Burmester, Y. Desmedt, ”A Secure and Efficient Conference Key Distribution System”, *Advances in Cryptology: Proceedings of Eurocrypt ’94*, Lecture Notes in Computer Science 950, Springer-Verlag, pp. 275-286, 1995.
6. R. Cramer, I. Damgard, B. Schoenmakers, “Proofs of partial knowledge and simplified design of witness hiding protocols”, *Advances in Cryptology: Proceedings of Crypto ’94*, Lecture Notes in Computer Science 839, Springer-Verlag, pp. 174-187, 1994.
7. R.Canetti, A. Herzberg, ”Maintaining Security in the Presence of Transient Faults”, *Advances in Cryptology: Proceedings of Crypto ’94*, Lecture Notes in Computer Science 839, Springer-Verlag, pp. 425-438, 1994.
8. C. C. Chang, C. H. Lin, ” How to Converse Securely in a Conference”, *Proceedings of IEEE Security Technology, 30th Annual 1996 International Carnahan Conference*, pp. 42-45, 1996.
9. C. C. Chang, T. C. Wu, C. P. Chen,”The Design of a Conference Key Distribution System”, *Advances in Cryptology: Proceeding of Auscrypt ’92*, Lecture Notes in Computer Science 718, Springer-Verlag, pp. 459-466, 1992.
10. G. H. Chiou, W. T. Chen, ”Secure Broadcasting Using the Secure Lock”, *IEEE Transactions on Software Engineering*, Vol. 15, No. 8, pp. 929-934,1989.
11. W. Diffie, M. Hellman, ”New Directions in Cryptography”, *IEEE Transaction of Information Theory*, Vol. IT-22, pp. 644-654, 1976.
12. U. Feige, A. Shamir, “Witness Indistinguishable and Witness Hiding Protocols”, *Proceedings of 27th ACM Symposium on the Theory of Computing (STOC)*, pp416-426, 1990.
13. M. Fitzi, M. Hirt, U. Maurer, ”Trading Correctness for Privacy in Unconditional Multi-Party Compution”, *Advances in Cryptology: Proceedings of Crypto ’98*, Lecture Notes in Computer Science 1462, Springer-Verlag, pp. 121-136, 1998.

14. Y. Frankel, P. Gemmell, P. D. MacKenzie, M. Yung, “Proactive RSA”, *Advances in Cryptology: Proceedings of Crypto ’97*, Lecture Notes in Computer Science 1294, Springer-Verlag, pp. 440-455, 1997.
15. A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M.Yung, ”Proactive Public Key and Signature Systems”, *Proceedings of the 4th ACM Symposium On Computer and Communication Security*, pp. 0-18, 1997.
16. A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, ”How to Cope with Perpetual Leakage, or “Proactive Security Sharing”, *Advances in Cryptology: Proceedings of Crypto’95*, Lecture Notes in Computer Science 963, Springer-Verlag, pp. 339-352, 1995.
17. T. Hwang, J. L. Chen, ”Identity-Based Conference Key Broadcast Systems”, *IEE Computers and Digital Techniques*, Vol. 141, No. 1, pp. 57-60, 1994.
18. I. Ingemarsson, D. T. Tang, C. K. Wong, ”A Conference Key Distribution System”, *IEEE transactions on Information Theory*, Vol. IT-28, No. 5, pp. 714-720, 1982.
19. K. Koyama, ”Secure Conference Key Distribution Schemes for Conspiracy Attack”, *Advances in Cryptology: Proceedings of Eurocrypt ’92*, Lecture Notes in Computer Science 658, Springer-Verlag, pp. 449-453, 1993.
20. K. Koyama, K. Ohta, ”Identity-Based Conference Key Distribution Systems”, *Advances in Cryptology: Proceedings of Crypto ’87*, Lecture Notes in Computer Science 293, Springer-Verlag, pp. 175-184, 1988.
21. K. Koyama, K. Ohta, ”Security of Improved Identity-Based Conference Key Distribution Systems”, *Advances in Cryptology: Proceeding of Eurocrypt ’88*, Lecture Notes in Computer Science 330, Springer-Verlag, pp. 11-19, 1988.
22. B. Klein, M. Otten, T. Beth, ”Conference Key Distribution Protocols in Distributed Systems”, *Proceedings of Codes and Ciphers-Cryptography and Coding IV*, IMA, pp. 225-242, 1995.
23. C. H. Lin, C. C. Chang, R. C. T. Lee, ”A Conference Key Broadcasting System Using Sealed Locks”, *Information Systems*, Vol. 17, No. 4, pp. 323-328, 1992.
24. T. Matsumoto, H. Imai, ”On the Key Predistribution System**:** A Practical Solution to the Key Distribution Problem”, *Advances in Cryptology: Proceedings of Crypto ’87*, Lecture Notes in Computer Science 293, Springer-Verlag, pp.185-193, 1988.
25. R. Ostrovsky, M. Yung, ”How to Withstand Mobile Virus Attacks”, *Proceedings of ACM Symposium on Principles of Distributed Computing (PODC)*, pp.51-61, 1991.
26. T. Rabin, M. Ben-Or, ”Verifiable Secret Sharing and Multiparty Protocols with Honest Majority”, *Proceedings of 26th ACM Symposium on the Theory of Computing (STOC)*, pp73-85, 1989.
27. B. Schoenmakers, “A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting”, *Advances in Cryptology: Proceedings of Crypto ’99*, Lecture Notes in Computer Science, Springer-Verlag, pp. 148-164, 1999.
28. A.Shamir, ”How to share a secret”, Communications of the ACM, Vol. 22, pp. 612-613, 1979.
29. A. Shimbo, S. I. Kawamura, ”Cryptanalysis of Several Conference Key Distribution Schemes”, *Advances in Cryptology: Proceedings of Asiacrypt ’91*, Lecture Notes in Computer Science 739, Springer-Verlag, pp. 265-276, 1993.
30. M. Stadler, “Publicly verifiable secret sharing”, *Advances in Cryptology: Proceedings of Eurocrypt’96*, Lecture Notes in Computer Science 1070, Springer-Verlag, pp. 190-199, 1996.
31. D. G. Steer, L. Strawczynski, W. Diffie, M. Wiener, ”A Secure Audio Teleconference System”, *Advances in Cryptology: Proceedings of Crypto ’88*, Lecture Notes in Computer Science 409, Springer-Verlag, pp. 520-528, 1990.
32. T. C. Wu, ”Conference Key Distribution System with User Anonymity Based on Algebraic Approach”, Proceedings of IEE Computers and Digital Techniques, Vol. 144, No 2, pp. 145-148, 1997.
33. Y. Yacobi, ”Attack on the Koyama-Ohta Identity Based Key Distribution Scheme”, Advances in Cryptology: Proceedings of Crypto ’87, Lecture Notes in Computer Science 293, Springer-Verlag, pp429-433, 1988.