行政院國家科學委員會專題研究計畫成果報告

群體簽章與代理簽章之深入研究
Study of Group Signature and Proxy Signature

計畫編號：NSC 88-2213-E-032-003
執行期限：87 年 8 月 1 日至 88 年 7 月 31 日

主持人：顏嵩銘　國立中央大學 資訊工程系（淡江大學 電機工程系）
e-mail address:　yensm@csie.ncu.edu.tw
http://www.csie.ncu.edu.tw/~yensm/people/yensm/

一、中文摘要

在本計畫中，我們針對以下兩項重要之數位簽章系統進行完整之研究：
(1) 群體簽章 group signature[CvH91] (註:非通稱之群體導向簽章): 允許群體中的個別成員不具名的替群體簽署訊息，但事後若有需要或遇爭論時可被公開顯示簽署者的身分。
(2) 代理簽章 proxy signature: 有需要時，允許一個指定的人代替原來的簽署者進行簽名。

上述二種數位簽章在工業和商業上有很大的應用，然而，此二簽章系統於實際應用時仍存有若干缺點急待解決與改善。值得注意的是，群體簽章和代理簽章於概念上存在某種程度的相關連性。

關鍵詞：資訊安全、密碼學、數位簽章、群體簽章、群體導向簽章、代理簽章、身份驗證

Abstract

In this report, we investigate two useful extensions of digital signatures:
(1) Group signatures: which allow individual members of a group to anonymously sign messages on behalf of the group [CvH91].
(2)Proxy signatures: which allow a designated person to sign on behalf of the original signer.

Our main contribution is to point out the difficulty of coalition-resistance in group signature schemes. We also analyze several group signature schemes. We show that two schemes recently proposed by Tseng and Jan are universally forgeable. Furthermore, we show that the very efficient scheme due to W.-B. Lee and Chang and its improved version by Tseng and Jan are universally forgeable, as well. We finally prove the security of some (secret) relations in the weak model of Poupard and Stern.

Keywords: Information security, Cryptography, Digital signature, Group signature, Group oriented signature, Proxy signature, Authentication

二、緣由與目的

群體簽章和代理簽章於概念上存在某種程度的相關連性。群體簽章允許群體成員替群體簽名而代理簽章允許某一個人替原始的簽署者簽章。當考慮原始的簽署者是群體權力當局(authority)，則群體的成員便可被認為是代理簽章者。換句話

說，群體簽章可以被認為是一種完全授權式的代理簽章，而且代理簽署者是以匿名的型式出現。

本研究計畫形成之緣由與目的如前摘要所述乃為針對群體和代理簽章的研究邁進一步，徹底研究其特性與相關性並實際解決與改良諸多缺點。

三、結果與討論

In this report, we investigate two useful extensions of digital signatures:
(1)Group signatures: which allow individual members of a group to *anonymously* sign messages on behalf of the group [CvH91].
(2)Proxy signatures: which allow a designated person to sign on behalf of the original signer [MUO96a,MUO96b].

Our Main Contributions

Some material presented in this report has been submitted for publication. Our main contribution is to point out the difficulty of coalition-resistance in group signature schemes [AJT99] (see also [Joy98] and [Joy99]). This is a joint work with Giuseppe Ateniese and Gene Tsudik. We also analyze several group signature schemes. In [JKL99], jointly with Seungjoo Kim and Narn-Yih Lee, we show that two schemes recently proposed by Tseng and Jan are universally forgeable. Furthermore, with Narn-Yih Lee and Tzonelih Hwang, we show in [JLH99] that the very efficient scheme due to W.-B. Lee and Chang and its improved version by Tseng and Jan are universally forgeable, as well. We thank all our co-authors for their contribution. Of independent interest, we finally prove the security of some (secret) relations in the weak model of Poupard and Stern. We thank again Guillaume Poupard for commenting our proofs.

Content of the Research Report

We have completed a 50 page research report and the content of this report is organized as follows.

Chapter 2 introduces group signatures and motivates their usefulness through various applications. Moreover, it formally defines group signatures and the associated security properties. Previous and related works in group signatures are surveyed in Chapter 3. Chapter 4 is more technical and may be skipped at first reading. It presents some building blocks for demonstrating knowledge of a secret without revealing it. The blocks are constructed from the Schnorr signature scheme and proved secure under the Poupard-Stern model. It also defines the security parameters and discusses various versions of the Diffie-Hellman assumption. Chapter 5 introduces coalition attacks and illustrates how several (malicious) group members can produce an untraceable (but perfectly valid) group signature in various schemes. This clearly shows once more that ad-hoc constructions --- although seemingly robust -- certainly do not constitute a security proof and that their use always present some
risks. In Chapter 6, the security of the Camenisch-Stadler scheme and the Lee-Chang like schemes is investigated. It is shown that the security assumption made by Camenisch and Stadler is incorrect. The linkability problem in the Lee-Chang scheme is also discussed, and more importantly, it is

shown that both the Lee-Chang scheme and its improved version are universally forgeable. Finally, Chapter 7 presents the related idea of proxy signatures and exhibits the links between the two notions, that is, group signatures vs. proxy signatures.

四、計畫成果自評

綜觀以上 *計畫緣由與目的* 及 *結果與討論* 可以清楚地看出本研究計畫確實有其價值。

整體而言，本研究計畫在進度控制、研究內容、預期達成目標各方面均與原計畫相符。研究成果之內容已一部分發表於該領域相關之學術會議。

五、參考文獻

[BS97] M.Blaze and M.Strauss. Atomic proxy cryptography. Preliminary draft, 2 November 1997.

[Cam97] J.Camenish. Efficient and generalized group signatures. Advances in Cryptology -- Eurocrypt,'97, LNCS 1233, pp.465-479, Springer-Verlag, 1997.

[CS97] J.Camenish and M.Stadler. Efficient group signature schemes for large groups. Advances in Cryptology -- Crypto,'97, LNCS 1294, pp.410-424, Springer-Verlag, 1997.

[Cha91] D.Chaum. Zero-knowledge undeniable signatures. Advances in Cryptology -- Eurocrypt,'90, LNCS 473, pp.458-464, Springer-Verlag, 1991.

[CvH91] D.Chaum and E. van Heijst. Group signatures. Advances in Cryptology -- Eurocrypt,'91, LNCS 547, pp.257-265, Springer-Verlag, 1991.

[CP95] L.Chen and T.P. Pedersen. New group signature schemes. Advances in Cryptology -- Eurocrypt,'94, LNCS 950, pp.171-181, Springer-Verlag, 1995.

[Des93] Y.Desmedt. Threshold cryptosystems. Advances in Cryptology -- Auscrypt,'92, LNCS 718, pp.3--14, Springer-Verlag, 1993.

[KPW96] S.J. Kim, S.J. Park and D.H. Won. Convertible group signatures. Advances in Cryptology -- Asiacrypt,'96, LNCS 1163, pp.311-321, Springer-Verlag, 1996.

[KPW97] S. Kim, S. Park, and D. Won. Proxy signatures, revisited. Information and Communications Security, LNCS 1334, pp.223-232, Springer-Verlag, 1997.

[MUO96] M.Mambo, K.Usuda, and E.Okamoto. Proxy signatures for delegating signing operations. 3rd ACM Conference on Computer and Communications Security, pp.48-57, ACM Press, 1996.

[Mic96] M. Michels. Comments on some group signature schemes. Tech. report, TR-96-3-D, University of Technology Chemnitz-Zwickau, Germany, Nov. 1996.

[Ped91] T.P. Pedersen. A threshold cryptosystem without a trusted third party. Advances in Cryptology -- Eurocrypt,'91, LNCS 547, pp.522-526, Springer-Verlag, 1991.

[Pet97] H. Petersen. How to convert any digital signature scheme into a group signature scheme. Pre-proceedings of the 1997 Workshop on Security Protocols, Paris, 7-9th April 1997.

[Yen94] S.-M. Yen. Design and computation of public key cryptosystems. PhD Thesis, National Cheng-Kung University,Taiwan R.O.C., April, 1994.