行政院國家科學委員會專題研究計畫 成果報告

具個人隱私保護功能之電子簽名系統
研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 99-2221-E-004-009-
執 行 期 間 ：99 年 08 月 01 日至 100 年 07 月 31 日
執 行 單 位 ：國立政治大學資訊科學系

計 畫 主 持 人：左瑞麟

計畫參與人員：碩士班研究生-兼任助理人員：林欣瑤
碩士班研究生-兼任助理人員：陳漢光
碩士班研究生-兼任助理人員：吳承峰
碩士班研究生-兼任助理人員：邱士峰
碩士班研究生-兼任助理人員：朱致諺

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 100 年 09 月 08 日

具隱私保護之電子簽名系統

成果報告

前言

隨著電腦與網路科技的進步，許多的資訊可以透過網際網路瞬間取得或與他人共享。這固然顯示出電腦科技與網路發展趨勢之銳不可擋，但電腦與網路使用者的隱私權該如何保護，也成為不得不重視的重要課題。伴隨網路科技的進步，無形之中衍生了許多竊密、詐騙或偽造資訊等等的網路犯罪行為。一般民眾之個人資料隨時可能透過網路購物或線上轉帳，藉由電腦漏洞、木馬或網路釣魚等方式，在不知不覺的狀況下外洩個人資料。

為防範個人資料遭盜用或不當使用，在歐美日等先進國家，均針對個人隱私，分別訂定了相關的法令保護，以美國為例，在 50 州中已有 44 州立法規定，發生個資外洩事件的機關(構)或企業，依法必須通報其客戶以減少損害。另外，如德國的『聯邦個人資料保護法』以及日本的『政府資訊公開法』等。我國亦於民國八十四年訂定了『電腦處理個人資料保護法』，規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用。

但是，政策面或法律面的規範僅具赫阻效果及犯罪事件發生後的事後處理，而無法達到預防個資外洩等犯罪行為的發生。換句話說，利用網路從事電子商務等等的行為時，網路使用者其實必須相信對方的網管人員不會收集或濫用所得到的個人資訊。但近年來無論是國際或國內媒體陸續揭露政府機關與民間企業外洩客戶個人隱私資料的新聞，讓人們對於個人隱私能否再網路世界受到妥善保護，仍普遍缺乏信心。要達到防止個人資料的外洩，除了法律層面的規範之外，利用密碼學等技術層面，從人性的觀點考量，加以預防也是不可或缺的。

利用密碼學的技術達到保障個人隱私，最廣為人之的就是利用加解密的技術。配合數位簽章則可同時達到不可否認性。PGP 雖可提供資訊保密及數位簽章（防偽）的功能，但 PGP 的資訊保密僅針對資訊的傳輸過程中，用來防止非法竊聽者的竊聽或盜取機密資訊。針對資訊的收信端而言，並沒有任何的機制可以防止收信端濫用所收到資訊或洩密。舉例來說，針對企業內部的內部告發，若告發者不具名則告發內容之真實性會受到質疑。但若具名告發則又會擔心因資料外洩而遭到被告發者的報復。因此，個人身份一方面要能夠被確認，另一方面又要能夠確保不會被外洩。除了上述情況，個人身份需要受到保護之外，在電子投票，或網路線上公平遊戲如電子樂透等具金錢交易的遊戲中，個人身份亦同樣需要被確認，電子投票需確認投票者身份及是否為有權投票者;電子樂透遊戲則需確認樂透參加者身份以便日後領取獎金。但同時個人身份也需受到

保護，電子投票需保障投票人與所投之選票之關係不能被任何人找到，即投票之隱私性;電子樂透的參加者身份亦必須受到保護以免人身安全受到威脅。傳統的加解密機制或數位簽章無法提供此類保護個人隱私的功能。這一部份，在技術面來講，需要用到具個人隱私保護功能的數位簽章才能達到。

研究目的

資訊電子化既是未來的趨勢，關於電子資訊上相關個人資訊的保護問題，如電子證書簽名者身份，持有者身份以及證書之全部或部分內容之保護，實宜及早未雨綢繆，從技術面上著手，為未來安全，安心的電子化社會的及早實現而努力。本研究即以具個人隱私保護功能之電子簽名系統的設計，應用及其安全性分析為基礎，就個人隱私之保護及其相關課題等進行研究及探討。這個計畫，不論是在密碼學的理論研究或是未來因應電子化社會的實務應用的領域而言，都將是一個十分重要且極具挑戰性的研究。

鑑於資訊安全與保護個人隱私的技術已成為時下最重要的課題。本計畫的目的在研究具個人隱私保護功能之電子簽名系統，包括對既有（具個人隱私保護功能）方案的實用性分析，在應用層面如有不足的地方提供功能性的擴充，以及針對現有方案無法解決的問題，提出新的簽名系統以有效解決此些問題。另外，針對所提出的系統，提供完整及嚴格的安全性證明。

文獻探討

本計畫是以密碼學中的電子簽名為基礎，結合保護個人隱私的功能，以期能提供安全可靠又有效率的『具保護個人隱私功能之電子簽名系統』。此研究所需保護的個人隱私，其範圍包含了『簽名者身份』、『簽名使用者身份』及『被簽名之訊息的全部或部分內容』。以下僅就與本研究及研究成果相關的具個人隱私保護功能的簽名方案的研究作一個的介紹。

[1]. 環簽名與群簽名(Ring signatures and Group Signatures)：

環簽名(Ring signature)是一種保護簽名者的匿名簽名技術. Rivest 等人首先明確地提出了這一概念[17]。按照這一簽名技術,一個簽名者可以靈活地選擇一個包括自己在內的用戶集稱為環
(Ring),接著他可以代表這個環對某個消息進行簽名。驗證者確信這個簽名是由這個環的某個成員產生的,從而確定消息的真實性,但他沒有任何資訊能確定誰是真正的簽名者,從而又達到無條件匿名性. 環簽名的這種無條件匿名性在對

資訊需要長期保護的一些特殊環境中非常有用。Rivest 等人在他們所提出的環簽名論文，其標題即為『How to leak a secret』(如何洩漏一個秘密)。論文中所舉出的應用是當一個公司裡的一個成員，他想對外（如報章雜誌記者）洩漏公司內部消息或想檢舉公司內部的不法行為，但卻又不想讓公司集團內的成員或是驗證者知道是他對外洩漏消息，因此就提出了這個環簽名的概念。

群簽名(Group signature)[6]的概念和環簽名類似。群簽名使得群中任何一個成員均可以代表該群進行簽名，而不會暴露簽名者的身份。但群簽名中有一個系統管理者或稱群管理者，當爭議發生時，簽名者的身份可以通過群管理者而被公開。

環簽名及群簽名保障了訊息簽名者的身份不被洩漏。現實生活中可以找到許多例子讓我們知道群簽名或環簽名的重要性。關於個人，民間企業或政府部門的不法行為，如果我們可以在技術層面上確認檢舉的有效性，另一方面又能確保檢舉人的身份，私人權益及個人隱私不會被洩漏，則能夠激發組織之正義行為，使人人勇於檢舉不法，嚇阻舞弊犯罪事件並端正社會之不良風氣。

目前對於此類簽名技術已臻至成熟並發展出許多附加功能的方案。例如，針對內部告發者不是一個人而是多個人的情況,而有了有門檻(Threshold)的群簽名或環簽名[2,13,14,15]。為了解決傳統 PKI 的問題，亦即，對於傳統的公開金鑰體制下環簽名或群簽名,它的驗證者必須要首先驗證所有群或環成員的公開金鑰及憑證, 這需要花費大量的計算時間和空間，因而有了基於身分的(Identity-Based)群簽名或環簽名[8,10,15,21]。而由於 Identity-based 密碼系統有金鑰託管(key-escrow)，亦即，系統生成者知道所有使用者的密鑰的問題，所以有了免憑證(Certificateless)的環簽名(Certificateless ring signature)[9]。其他如 Constant sized ring signature[11],確保了簽名的長度不因簽名者的人數而改變。Ring signatures from a various of keys [1]，允許簽名者彼此間的公開/秘密鑰匙可以由不同系統所生成。Linkable ring signatures[18]可以讓簽名驗證者確認兩個環簽名是否由同一簽名者生成。

針對有門檻(threshold)的群簽名或環簽名，因為簽名者不只一人，而匿名簽名又通常是用在有參與重大事件上(如參與企業內不知告發等)，因此，在現實生活上，參與者事後改變決定而想要退出，或是有新的人想要加入是很有可能的。但現行方案皆未考慮到使用者中途退出或中途加入的情況。另一方面，群簽名或環簽名是保障簽名者的匿名性，而非保障資訊的隱私。這部分是否有兩者兼顧的方法是值得考慮的。

2.盲簽名(Blind signatures)

1.投票人：依據選票公開格式選定 m。再任選一亂數 R。 計算 C = (R^e)m mod n，將 c 送給選委會。 2.選委會：計算 T' = C^d mod n，將 T 送還給投票人。 3.投票人：計算 T = R^(-1)T' mod n = m^d mod n 。 4.各投票人可自行驗證 T 是否是選票 m 的數字簽名， 因為 T^e mod n = m

Table 1. 基於盲簽名的電子投票系統

盲簽名(Blind signature)是於 1982 年由 David Chaum 所提出的[5]。盲簽名的概念是讓簽名者在不知道文件具體內容的情況對文件進行簽名的動作。而送簽人在經過特定的計算後，可以的得到簽署人對原始文件的簽章。除了簽署人不知道所簽署文件的內容之外，盲簽名還具備了無關聯性或不可追蹤性(Untraceable)之特性。亦即，就算簽署者在日後取得此文件及其所對應的簽章，亦無法從中推導出此文件與當時盲簽名文件及簽名的相互關係。盲簽名因為具有盲性這一特點，可以有效保護所簽署消息的具體內容，所以在電子商務和電子投票等領域有著廣泛的應用。David Chaum 所提出的盲簽名是基於 RSA 簽名[16]。Table 1 介紹了其在電子投票上的應用。另外，

在電子商務的應用方面，因為在電子付款的機制當中，電子現金可以被視為一份電子文件，透過盲簽章的方式可以讓使用者取得銀行對於該電子現金的合法簽署，並在消費者使用其作交易時，商家及銀行街無法從此交易所付出的電子現金中追蹤出使用者的身份。

盲簽名的研究不斷深入，之後被細分為弱盲簽名(Weak blind signature)與強盲簽名(Strong blind signature)。弱盲簽名[23]具備可追蹤性，即簽名者可從事後公開的簽名及訊息中找出與原始盲簽名的關連。而強盲簽名則不具追蹤性。另外、部分盲簽名(Partially blind signature)的概念亦陸續被提出[3,4,7]。部分盲簽名通過在最終的簽名數據中包含簽名者和用戶協商一致的公用訊息(簽名發布日期, 電子貨幣的金額)來擴展了盲簽名的概念，以避免簽名者簽署到任何他不應該或不願意簽的文件。其他擴張如 Blind signature with message recovery[12]，提供了訊息可回復的盲簽名以節省傳輸過程中所需佔用的頻寬，基於身份的盲簽名(ID-based blind signature) [7,22,23] 以解決傳統公開金鑰體制下，驗證者必須要先驗證簽名者的公開金鑰及憑證，以及免憑證的盲簽名(Certificateless blind signature)[19]以解決 ID-based 方案中所產生的金鑰託管的問題等。

和群簽名或環簽名不一樣，盲簽名是用來保護簽名使用者的隱私，包括訊息本身以及使用者身份，而非保障簽名者的匿名性。另外，盲簽名基本上是針對簽名者與簽名使用者之間的機制，並無考慮到驗證者的部分。亦即，對驗證

簽名的第三方來說，簽名驗證和傳統的電子簽名並無任何不同。

研究方法

在本節中，我們就上一節中所討論到的問題，提出我們的想法，並指出本計畫的研究方向。

1.環簽名與群簽名

誠如前面所述，針對有門檻(threshold)的群簽名或環簽名，因為簽名者不只一人，而匿名簽名又通常是用在有參與重大事件上（如參與企業內不知告發等），因此，在現實生活上，參與者事後改變決定而想要退出，或是有新的人想要加入是很有可能的。但現行方案皆未考慮到使用者中途退出或中途加入的情況。另一方面，群簽名或環簽名是保障簽名者的匿名性，而非保障資訊的隱私。這部分是否有兩者兼顧的方法是值得考慮的。

在參與者中途退出或是中途加入的情況，目前最簡單的方法就是重新生成一個有門檻的群簽名或環簽名。此法雖一定可行，但較無效率可言，因為所有的參數都需重新計算。以環簽名為例，我們試想如果在有門檻的環簽名中，假設門檻為 k 而集合全部共有 n 個簽名者(entity)，亦即，一個 k out of n signature。如果此 k 個簽名者都只需要各自生成一個 1 out of n signature，而當這 k 個簽名集合起來，就能成為我們所要的 k out of n signature 的話，那中途退出或加入就變得容易多了。因為針對退出者，只需將他那一部份的 1 out of n signature 拿掉，就是我們所要的 k-1 out of n signature 了，而如果要加入，只需將新加入者算出的 1 out of n signature 和現有的 k out of n signature 作聯集(union)，就能得到所要的 k+1 out of n signature 了。關鍵在於如何確保每個簽名者只能生成唯一一個 1 out of n signature。如果這部分不能確保的話，就算 k 個簽名作聯集，也無法保證是 k out of n signature。因為，有可能 k 個 1 out of n signature 都是由同一個人作出來的。這部分我們預計可利用 hash function 的單向性(one way property)來達成。我們假設每個簽名者 U_i 的公鑰中包含了一個安全的 hash function H_i。在簽名者作簽名時，除了用到自己的簽名密鑰之外，另外需有一個 short term public/private key pair（一次性的公私鑰），公鑰為 z_i 私鑰為 r_i。其生成方式為

$$z_i = g_i^{r_i} - H_i(j)$$

其中 j 為 U_i 任選之一亂數，g_i 為 U_i 的公鑰之一。假設所有簽名者所選之亂數 j 皆不一樣，但 short term public key z_i 在每個 1 out of n signature 中都不會改變。為便於說明，假設 U_i 選亂數

j=i, 1 <= i <=k, 則

$$z_i = {g_i}^{r_{i_1}} - H_i(1) = \cdots = {g_i}^{r_{i_j}} - H_i(j) = \cdots$$
$$= {g_i}^{r_{i_i}} - H_i(i) = \cdots = {g_i}^{r_{i_k}} - H_i(k).$$

對於 z_i，基於離散對數問題及 hash function 的單向性，我們可以確認 U_i 只可能知道一個 short term private key r。我們只要確保簽名時一定要用到 r，而一個 r 只能用在一個 1 out of n signature，那我們就可以確定每個簽名者最多只能生成一個 1 out of n signature 了。因為同一個 z_i，簽名者 U_i 不可能知道一個以上的 r 對應同一個 z_i。目前我們以 Abe 等[1]的 1 out of n signature 為藍本，嘗試將此性質加進去而能得到我們要的 k out of n signature。

2.盲簽名

我們發現盲簽名結合代理簽名有不錯的應用，也有些學者在此方面作了些研究[18,46]。但我們尚未發現具免憑證的代理盲簽名。針對此部分我們的想法如下：

(1). Setup:

KGC 會執行下列幾個步驟：

- 首先生成系統參數G_1、G_2、q、e、P。
- 選擇一 $s \in Z_q^*$稱為 KGC 的 master-key，並且設定 KGC 的公鑰$P_{pub}=sP$
- 選擇兩個 hash functions

  $H1:\{0,1\}^* \rightarrow G_1$

  $$H2:\{0,1\}^* \times G_2 \rightarrow Z_q^*$$

接著 KGC 會公佈系統參數給使用者

$<G_1, G_2, q, e, P, P_{pub}, H1, H2>$

(2). Key-Generation

- 部分金鑰生成：

  KGC 利用原簽章者 A 的身分資訊ID_A、及代理簽章者的身分資訊ID_B，得出 $Q_A = H1(ID_A)$，$Q_B = H1(ID_B)$。

  接著 KGC 會利用剛剛選定的亂數 s，產生使用者分別的部分私鑰。

  $D_A = s \cdot Q_A$，$D_B = s \cdot Q_B$

  分別是 A 和 B 的部分私鑰

- Set-Secret-Number

  簽章者 A、代理簽章者 B 首先會分別選一亂數

  $X_A \in Z_q^*$，$X_B \in Z_q^*$

- Set-Secret-key

簽章者 A、代理簽章者 B 設定各自的私鑰

$S_A = X_A \cdot Q_A$，$S_B = X_B \cdot Q_B$

- Set-Public-Key

簽章者 A、代理簽章者 B 設定各自的公鑰

$P_{KA} = X_A \cdot P$，$P_{KB} = X_B \cdot P$

(3). Proxy-Phase

原始簽章者 A 會給代理簽章者 B 一個代理的授權m_w。

原始簽章者 A 計算下列各值：

$K_A \in Z_q^*$，$r_A = e(P,P)^{K_A}$，$h_A = H2(m_w, r_A)$

$\sigma_{proxy} = h_A \cdot (D_A + S_A) + K_A P$

接著傳送$(m_w, r_A, \sigma_{proxy})$給代理簽章者 B。

(4). Del-Verify

代理簽章者 B 得到了$(m_w, r_A, \sigma_{proxy})$後會執行、計算以下步驟，以確認這是由原簽章者 A 所簽發的

首先 B 先利用系統參數計算出：

$h_A = H2(m_w, r_A)$ 及 $Q_A = H1(ID_A)$，接著驗算下列式子是否成立：

$$e(\sigma_{proxy}, P) = e(Q_A, P_{KA} + P_{pub})^{h_A} \cdot r_A$$

Correctness：

$$\begin{aligned} E(\sigma_{proxy}, P) &= e(h_A \cdot (D_A + S_A) + K_A P, P) \\ &= e(h_A \cdot (D_A + S_A), P) \cdot e(K_A P, P) \\ &= e(D_A + S_A, P)^{h_A} \cdot r_A \\ &= e(s \cdot Q_A + X_A \cdot Q_A, P)^{h_A} \cdot r_A \\ &= e(Q_A, (s + X_A)P)^{h_A} \cdot r_A \\ &= e(Q_A, P_{KA} + P_{pub})^{h_A} \cdot r_A \end{aligned}$$

(5). Proxy-Key-Gen

代理簽章者 B 產生一代理簽章用的金鑰

d_{proxy}：$h_A \cdot (S_B + D_B) + \sigma_{proxy}$

(6). Sign

使用者 C 想要對一份文件 m 作簽章

代理簽章者 B 會執行以下步驟來對 m 作出一份代理 A 的簽章

$K_B \in Z_q^*$，$V_B = K_B \cdot H1(m)$，$U = K_B \cdot P$

$$S = d_{proxy} + V_B$$

最後產生對 m 的簽名為：$\sigma = (r_A, m_w, S, U)$

(7). Verify

驗證下列式子是否成立，可得此簽名是否為合法的簽名：

$$e(S,P) = (e(Q_A, P_{KA} + P_{pub}) \cdot e(Q_B, P_{KB} + P_{pub}))^{h_A} \cdot r_A \cdot e(H1(m), U)$$

以上為我們所設計之免憑證代理簽章。

結果與討論

首先，在學術成就上，
研究成果包括我們在上面提到的環簽名以及代理盲簽名，已以論文形式發表於以下之會議中。

A. Raylin Tso, Xun Yi. "Certificateless Proxy Signature and Its Extension to Blind Signature". 4th International Conference on Network and System Security (NSS 2010): 542-547, 2010. (EI)
B. Raylin Tso, Xun Yi, Tadahiko Ito, Takeshi Okamoto, Eiji Okamoto. "Design and Analysis of "Flexible" *k*-out-of-*n* Signatures". ATC 2010, Lecture Notes in Computer Science, Vol 6407, 255-267, 2010. (EI)

另外，有關環簽名的另一個研究成果亦已被接收並預計發表於以下之期刊中

A. Raylin Tso, "Convertible ring signatures with gradual revelation of non-signers", Computer and Communication Networks, to appear. (SCI)

on-line version:
http://onlinelibrary.wiley.com/doi/10.1002/sec.334/abstract

這些結果基本上解決了我們當初設想的問題，並且得到了很好的解決方案。這些成果在利用簽章來保護個人隱私上，提供了具體的想法與貢獻。經由實做，即可達成其實際的應用價值。例如使用在組織內之內部告發以預防不法之行為並保障告發者之人身安全。

另外，未來可考慮擴充其功能至其他環境中。例如，將本計畫提出之代理簽章及盲簽章應用於線上交易或電子投票之中。

參考文獻

[1]. M. Abe, M. Ohkubo and K. Suzuki," 1-out-of-n signatures from a variety of keys, Advances in cryptology --ASIACRYPT'02,Lecture Notes in Computer Science Vol. 2501, pp.415--432, 2002.

[2]. M. Abe, M. Ohkubo, and K. Suzuki, "Efficient threshold signer-ambiguoug signatures from variety of keys", IEICE Transactions, Vol.E587-A, No.2.

PP.471—479, 2004.

[3]. M. Abe and T. Okamoto, “Provably secure partially blind signatures, Advances in Cryptology --CRYPTO'00, Lecture Notes in Computer Science Vol. 1880, pp.271--286, 2000.

[4]. T. Cao, D. Lin, and R. Xue, “A randomized RSA-based partially blind signature scheme for electronic cash”, Journal of Computers and Security, Vol. 24, No. 1, PP.44—49, 2005.

[5]. D. Chaum, “Blind signatures for untraceable payments”, Advances in Cryptology --CRYPTO'82, Sringer-Verlag, pp.199--203,1983.

[6]. D. Chaum and E. van Heijst, “Group signatures”, Advances in cryptology --EUROCRYPT'91, Lecture Notes in Computer Science Vol.547, pp.257--265, 1991.

[7]. X. Chen, F. Zhang, and S. Liu, “ID-based restrictive partially blind signatures and applications”, Journal of Systems and Software, Vol.80, No.2, PP.164—171, 2007.

[8]. S. S. M. Chow, L. C. K. Hui and S. M. Yiu, “Identity based threshold ring signature”, Proceedings of ICISC'04, Lecture Notes in Computer Science Vol. 3506, pp.218--232, 2005.

[9]. S.S.M. Chow and W.S.Yap, “Certificateless ring signature”, available at http://eprint.iacr.org/2007/236.pdf

[10]. S. S. M. Chow, S. M. Yiu and C. K. Hui, “Efficient identity based ring signatures, Proceedings of ACNS'05, Lecture Notes in Computer Science Vol. 3531, pp.499--515, 2005.

[11]. Y. Dodies, A. kiayias, A. Nicolosi and V. Shoup,” Anonymous identification in ad-hoc groups”,Advances in cryptology --EUROCRYPT'04,Lecture Notes in Computer Science Vol. 3027, pp.609--626, 2004.

[12]. S. Han and E. Chang, “A pairing-based blind with message recovery”, In International Journal of Information Technology, Vol. 2, No. 4, 2005.

[13]. H. Kuwakado, and H. Tanaka,”Threshold ring signature scheme based on the curve”, In Proceedings of IEEE International Symposium on Information Theory (ISIT’03), pp. 139, 2003.

[14]. J. K. Liu, V. K. Wei,and D. S. Wong, “A separable threshold ring signature scheme”,
In Proceedings of ICISC'03, Lecture Notes in Computer Science Vol. 2971, pp.12--26, 2003.

[15]. C. Y. Lin, and T. C. Wu, “An identity-based ring signature scheme from bilinear pairings”, In Proceedings of the 18th International Conference on Advanced Information Networking and Applications (AINA’04), pp.282—285, 2004.

[16]. R. Rivest, A. Shamir; and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *Communications of the ACM* **21** (2): 120–126,

1978.

[17]. R. Rivest, A. Shamir and Y. Tauman,"How to lead a secret",Advances in cryptology --ASIACRYPT'01, Lecture Notes in Computer Science Vol. 2248, pp.552--565, 2001.

[18]. P. P. Tsang, V. K. Wei, T. K. Chan, M. H. Au, J. K. Liu and D. S. Wong, "it Separable linkable threshold ring signatures", In Proceedings of INDOCRYPT'04, Lecture Notes in Computer Science Vol. 3348, pp.384--398, 2004.

[19]. X. Yang, Z. Liang, P. Wei, and J. Shen, "A Provably Secure Certificateless Blind Signature Scheme," In Proceedings of the fifth International Conference on Information Assurance and Security(IAS'09), vol. 2, pp.643-646, 2009.

[20]. Y. L.Yu, and T. S. Chen, "An efficient threshold group signature scheme", Applied Mathematics and Computation 167(1): 362-371, 2005

[21]. F.Zhang and K.Kim, "Efficient ID-based blind signature and ring signature from pairings", In Proceedings of ASIACRYPT'02, pp533—547, 2002.

[22]. F.Zhang and K.Kim, "Efficient ID-based blind signature and proxy signature from bilinear pairings", In Proceedings of ACISP'03, pp312—323, 2003.

[23]. Z. Zhao, "ID-based weak blind signature from bilinear pairings", International Journal of Network Security, Vol. 7, No. 2, pp.265—2668, 2008.

國科會補助出席國際會議

心得報告書

報告人姓名	左瑞麟 Raylin Tso	學校/系所/職 稱	國立政治大學 資訊科學系 助理教授
會議名稱	ATC 2010 The 7th International Conferences on Autonomic and Trusted Computing		
會議時間	自 99 年 10 月 26 日 至 99 年 10 月 29 日	會議地點	中國西安
會議主辦 單位名稱	IEEE /西北工業大學		
擬發表之 論文題目	Design and Analysis of "Flexible" k-out-of-n Signatures		
會議相關連結	http://www.nwpu.edu.cn/atc2010/		

出席會議簡述：

本次會議自民國 99 年 10 月 26 日至 29 日於西安舉行。共有來自 20 個國家或地區的專家學者參與此盛會。此會議為一電腦科學領域相關之國際會議。會議主軸為自主計算(autonomic computing)以及可信計算(trusted computing)為主。其大致議題如下：

- AC/OC Theory and Models

Models, negotiation, cooperation, competition, self-organization, emergence, verification etc.

- AC/OC Architectures and Systems

Autonomic elements & their relationship, frameworks, middleware, observer/controller architectures, etc.

- AC/OC Components and Modules

Multi-core CPU, memory, storage, database, device, server, proxy, software, OS, I/O, etc.

- AC/OC Communication and Services

Networks, self-organized net, web service, P2P, grid, EaaS, could, semantics, agent, transaction, etc.

- AC/OC Tools and Interfaces

Tools/interfaces for AC/OC system development, test, monitoring, assessment, supervision, etc.

- Trust Models and Specifications

Models and semantics of trust, distrust, mistrust,
over-trust, cheat, risk, reputation, reliability, etc.

- Trust-related Security and Privacy

Trust-related secure architecture, framework, policy,
intrusion detection/awareness, protocols, etc.

- Trusted Reliable and Dependable Systems

Fault-tolerant systems, hardware redundancy,
robustness, survivable systems, failure recovery, etc.

- Trustworthy Services and Applications

Trustworthy Internet/web/P2P/grid/cloud services,
secured mobile services, novel applications, etc.

- Trust Standards and Non-Technical Issues

Trust standards and issues related to personality, ethics, sociology, culture, psychology, economy, etc.

此次會議的投稿篇數共有 68 篇，而其中只有 20 篇論文被錄取並收錄於由 Springer 出版的 Lecture Notes in Computer Science 會議論文集中。所以論文的錄取率為 29%。因為錄取率不高，所以每篇文章都有非常高的質量。很榮幸的我們的文章” Design and Analysis of “Flexible” k-out-of-n Signatures” 能夠被錄取並在此會議中發表。此文章被歸類在”Trusted-Related Security and Privacy”的議程中。此文章和計畫本身是非常相關的。我們在計畫書中提到了針對有門檻(threshold)的群簽名或環簽名，因為簽名者不只一人，而匿名簽名又通常是用在有參與重大事件上（如參與企業內不知告發等），因此，在現實生活上，參與者事後改變決定而想要退出，或是有新的人想要加入是很有可能的。但現行方案皆未考慮到使用者中途退出或中途加入的情況。而這篇文章，就是針對這樣的問題，提出了解決的方案。透過會議的報告，我們有機會將此成果展現在國外的專家學者面前，也得到了許多有用的意見以及和其他學者討論的機會。我們在演講完畢之後，獲得了許多迴響及建議。未來將針對這些建議，繼續改良我們的方案。

有幸參與 ATC2010 年會，與來自世界各地的專家學者齊聚一堂， 針對資訊安全與隱私保護的相關議題相互討論，彼此交流，分享成果及實務經驗，實在是獲益良多。

攜回資料

The proceedings of the 7 th International Conference on Autonomic and Trusted Computing (ATC2010 會議論文集)。此會議論文集收錄於 Springer 出版的 Lecture Notes in Computer Sciences 中。

ATC 2010

論文被接收證明文件

ATC2010 寄給 我 顯示詳細資料 10/7/2 回覆

Dear Raylin Tso,

we are pleased to inform you that your paper
Paper ID: 71
Title: Design and Analysis of ``Flexible'' k-out-of-n Signatures
submitted to the International Conference on Autonomic and Trusted Computing (ATC 2010) has been ACCEPTED.
The paper will subsequently be published in the proceedings volume as part of Springer's Lecture Notes in Computer Science (LNCS). Congratulations for your excellent work!

The reviews for your paper are included below. In order to achieve the highest quality proceedings, we urge you to carefully consider the reviewers' comments when preparing the final version of your paper.

Please note that the deadline for REGISTRATION and CAMERA-READY version submission is
** July 30, 2010 **.
By missing this deadline, you run the risk that your paper will not be included in the proceedings. It is advisable to send your final paper and register sooner rather than later.

Papers need to be formatted according to LNCS guidelines, as defined here: www.springer.com/computer/lncs?SGWID=0-164-7-72376-0
The maximum length of the camera ready papers in LNCS format is 15 pages. A maximum of two additional pages can be accepted, at an additional charge.

All detailed information on camera ready paper submission, registrations, and hotel reservation will be available on the conference web site: http://www.nwpu.edu.cn/atc2010/

Please note that at least one of the authors of accepted papers is required to register AND present the paper at the conference, otherwise the paper will have to be removed from the digital library after the conference.

Thank you again for helping to ensure the success of ATC 2010. We are looking forward to meeting you at the ATC 2010 conference in Xi'an.

Best regards,
Bing Xie, Juergen Branke, Masoud Sadjadi
ATC 2010 Programme Chairs

========== REVIEWS ==========

---------- REVIEW 1 ----------
PAPER: 71
TITLE: Design and Analysis of ``Flexible'' k-out-of-n Signatures

OVERALL RATING: 3 (strong accept)

The paper proposed a new (k,n)-ring signature based on the existing (1,n)-ring signature. The
new scheme allows the use of flexible threshold value for k. The idea seems interesting and useful. The paper is reasonably well-written. The following revisions are suggested to improve the

論文摘要

Design and Analysis of "Flexible" k-out-of-n Signatures

Raylin Tso[1], Xun Yi[2], Tadahiko Ito[2], Takeshi Okamoto[3], and Eiji Okamoto[3]

[1] Department of Computer Science, National Chengchi University, Taiwan
[2] School of Computer Science and Mathematics,
Victoria University, Australia
Graduate School of Systems and Information Engineering,
University of Tsukuba, Japan
[3] Faculty of Health Sciences, Tsukuba University of Technology, Japan
raylin@cs.nccu.edu.tw,
Xun.Yi@vu.edu.au,
tada@cipher.risk.tsukuba.ac.jp,
ken@cs.k.tsukuba-tech.ac.jp,
okamoto@cipher.risk.tsukuba.ac.jp

Abstract. This paper presents a new kind of (k, n)-threshold ring signature ((k, n)-ring signature) which is just a combination of k $(1, n)$-ring signatures. Our construction guarantees that a single signer can close at most one ring so the result of the combination is the required (k, n)-ring signature. This construction is useful in, for example, electronic negotiations or games where gradual revelation on how many people signed a given document is required. It also provides flexibility of the threshold k. The threshold-flexibility means that, in our scheme, we can change a (k, n)-ring signature into a (k', n)-ring signature for any $k' \leq n$ *without revoking* the original (k, n)-ring signature. This is useful for signers to withdraw their signatures afterward and/or is useful for new signers to add their (partial of the ring) signatures into the original ring signature. In addition, when $k' < k$, this modification requires no extra computation. The security of the proposed scheme is proved in the random oracle model based on the hardness of the discrete logarithm problem and the intractability of inverting cryptographic one-way hash functions.

Keywords: DL problem, threshold-flexibility, hash functions, threshold ring signature.

國科會補助出席國際會議

心得報告書

報告人姓名	左瑞麟 Raylin Tso	學校/系所/職 稱	國立政治大學 資訊科學系 助理教授
會議名稱	2010 FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA-10)		
會議時間	自 99 年 12 月 9 日 至 99 年 12 月 11 日	會議地點	韓國 光州
會議主辦 單位名稱	FTRA - Future Technology Research Association International		
擬發表之 論文題目	Convertible Ring Signatures with Gradual Revelation of Non-Signers		
會議相關連結	http://www.ftrg.org/acsa2010/		

出席會議簡述：

本次會議自民國 99 年 12 月 9 日至 11 日於韓國光州舉行。此光州就是發生於 1980 年 5 月 18 日至 27 日期間光州民主化運動或稱五一八光州事件的發生地。因此來到此地可以看到許多關於光州事件的歷史記錄或展示。因為自由得來不易，所以看起來特別有感觸。

ACSA 是一個非常大型的國際會議，會議主軸為關於未來計算方面的密碼學以及安全等的應用。是一個理論間實務並具的盛會。其大致議題如下：

Track 1. Cryptography and Information Security

- Encryption and cryptography
- Block/Stream Ciphers
- Hash Functions
- Mathematical and Algorithmic Foundations of Applied Cryptography
- Design and Analysis of Cryptographic Algorithms and Protocols
- Pairing Based Cryptography for FCS

- Provable Security for Cryptographic Primitives Suitable for FCS
- Information Security with Mathematical Emphasis for FCS
- Public Key Cryptosystems
- Side Channel Attack

Track 2. Security Protocols and Applications

- Authentication and Non-repudiation
- Access Control and Authorization
- Identity and Trust Management
- Database and System Security
- Intrusion Detection, Tolerance and Prevention
- Secure communications
- Information Hiding
- Digital Signatures
- Digital Right Management
- Watermarking and Steganography
- Critical infrastructure protection
- Digital rights management
- Computer Forensics
- Trust computing
- Security for M2M Platform
- Security and privacy issues for intelligent vehicular systems and communications

Track 3. Industrial Security & its Business and Services

- Information assurance
- Emergent challenges in security and assurance
- Theories, methods, tools and techniques in managing security
- Security and privacy standards
- Common Criteria
- Risk evaluation and security certification
- Security in E-commerce and E-business
- Security Policy
- Trust model and management
- Smartphone Security issues

- Security for Open convergence system
- IPTV security services in the BcN
- Security issues for Broadband convergence Network (BcN)

因為今年是第二屆，算是一個較新的會議，所以在資訊安全領域上，此會議並不算特別出名。但是經由參與會議，發表並聆聽其他學者的報告，仍可以感覺得出此會議具有一定的水準。而且可以感覺得出此會議希望達到的目標。例如，在邀請演講中，就請了許多國際知名的學者或者是有大型計畫並具前瞻性計畫的學者來報告。Open Remark 是由 Dr. Kiseon Kim, Professor, Director, ERC-UFON, GIST, Korea 介紹他目前在韓國執行的國家行計畫。其演講題目為" Challenges in Underwater Sensor Networks and the 3-dimensional Localization Issue Using Mobile Beacons"。在水下建立感應器的網路，從事監測的工作，這真的是一個非常具有挑戰性，但又非常實用的一個想法。因位址研究的重要性，所以能夠得到國家的權力支援。由這也可看出韓國對國家未來科技發展的重視。經由和這些大師的對話，讓我更深刻的體認研究一定要看長遠，並且要持續不斷的努力，不怕失敗，最終才能享受到成功的果實，並成為令人尊敬的學者。

我們在此次會議發表的論文題目為" Convertible Ring Signatures with Gradual Revelation of Non-Signers"。此研究為本次國科會計畫的相關研究的成果之一。在保護個人隱私方面，有時我們希望在一開始時是以匿名的方式公開某些事實，但也許為了某些因素，之後又希望能夠取消匿名，在原始簽名者的同意之下，公開關於此匿名簽名者的身份。除此之外，甚至可以達到不公開身份，但縮小可能簽名者的範圍。亦即，原本簽名者是 n 個人中的其中一個，我們的方案可以在不改變簽名的情況下，讓驗證者知道簽名者是 n' 中的其中一個。其中，$n' < n$。這一個新的成果，可以找到許多應用，所以非常適合在此一會議發表。透過會議的報告，得到了許多有用的意見。未來將針對這些建議，繼續改良我們的方案。

有幸參與此盛會，與來自世界各地的專家學者齊聚一堂，彼此交流，分享成果及實務經驗，實在是獲益良多。而我們的文章，在經過修改之後，也順利的被國際期刊 Security and Computer Networks (SCIE)所接收，這是我們在研究上的另一個收穫。

攜回資料

The proceedings of 2010 FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA-10)。

ACSA 2010

論文被接收證明文件

[ACSA 2010] Notification: Status of Paper 125

acsa@ftrai.org 寄給 我　　顯示詳細資料 10/9/8　回覆

Dear Raylin Tso

Congratulations!!

We are happy to inform you that your paper "Convertible Ring Signatures with Gradual Revelation of Non-Signers" has been accepted for being presented at The 2010 FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA 2010) (http://www.ftrai.org/acsa2010).

論文摘要

RESEARCH ARTICLE

Convertible Ring Signatures with Gradual Revelation of Non-Signers

Raylin Tso

Department of Computer Science, National Chengchi University, No.64, Sec.2, Zhi-Nan Rd., 11605, Taipei, Taiwan

ABSTRACT

A ring signature enables a member of a group to sign any message on behalf of the group while hiding the identity of the real signer. On the other hand, a convertible ring signature is a kind of ring signature in which the real signer can convert it into an ordinary signature. In this way, the real signer can prove the ownership of a ring signature if necessary. In this paper, we introduce a new convertible ring signature with an additional property. That is, before convert a ring signature into an ordinary signature, we allow the real signer to reveal the identity of non-signers gradually. In other words, if there are n possible signers in a ring, then, by revealing one non-signer, it will become a ring signature with $n-1$ possible signers. By revealing $n-1$ non-signers, then the ring signature comes to an ordinary signature and anyone can verify who is the real signer. This property is useful when some non-signers of a ring signature are not trusted by a verifier (ie., the signature will not be accepted if someone is a possible signer). Rivest, Shamir and Tauman first mentioned this problem and gave a solution as their modified ring signature scheme. However, their modified scheme can only guarantee computational anonymity. Our new scheme provides the same property on one hand and still guarantees unconditional anonymity on the other hand. The security is rigorously proved in the random oracle model according to the formal definition.

KEYWORDS

convertible ring signature; hash function; privacy protection; random oracle model; reveal non-signers; ring signature

國科會補助計畫衍生研發成果推廣資料表

日期:2011/09/07

國科會補助計畫	計畫名稱: 具個人隱私保護功能之電子簽名系統
	計畫主持人: 左瑞麟
	計畫編號: 99-2221-E-004-009- 學門領域: 資訊安全

無研發成果推廣資料

99 年度專題研究計畫研究成果彙整表

計畫主持人：左瑞麟	計畫編號：99-2221-E-004-009-
計畫名稱：具個人隱私保護功能之電子簽名系統	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	0%	篇	
		研究報告/技術報告	0	0	0%		
		研討會論文	0	0	0%		
		專書	0	0	0%		
	專利	申請中件數	0	0	0%	件	
		已獲得件數	0	0	0%		
	技術移轉	件數	0	0	0%	件	
		權利金	0	0	0%	千元	
	參與計畫人力（本國籍）	碩士生	0	0	0%	人次	
		博士生	0	0	0%		
		博士後研究員	0	0	0%		
		專任助理	0	0	0%		
國外	論文著作	期刊論文	1	1	100%	篇	
		研究報告/技術報告	0	0	0%		
		研討會論文	2	2	100%		
		專書	0	0	0%	章/本	
	專利	申請中件數	0	0	0%	件	
		已獲得件數	0	0	0%		
	技術移轉	件數	0	0	0%	件	
		權利金	0	0	0%	千元	
	參與計畫人力（外國籍）	碩士生	5	5	100%	人次	
		博士生	0	0	0%		
		博士後研究員	0	0	0%		
		專任助理	0	0	0%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	無

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：(以 100 字為限)

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）(以 500 字為限)

在學術成就上，研究成果已以論文形式發表於以下之會議中(1) 4th International Conference on Network and System Security (NSS 2010): 542-547, 2010. (EI) (2) ATC 2010, LNCS Vol 6407, 255-267, 2010. (EI). 另外，研究成果亦已被接收並預計發表於以下之期刊中 (1) Computer and Communication Networks. (SCI).這些成果在利用簽章來保護個人隱私上，提供了具體的想法與貢獻。經由實做，即可達成其實際的應用價值。例如使用在組織內之內部告發以預防不法之行為並保障告發者之人身安全。另外，未來可考慮擴充其功能至其他環境中。例如，將本計畫提出之代理簽章及盲簽章應用於線上交易或電子投票之中。