作戰參數資料庫安全機制之研究：以匿名資訊分享爲基礎

陳正鎔[1]　尹延齡[2]　林文彬[3]　洪有志[4]

[1]萬能科技大學資訊管理學系　[2,3,4]國防大學管理學院資訊管理學系

摘　要

隨著資訊科技的日新月異，因應海峽兩岸正邁入高科技作戰型態以及詭譎多變的國際情勢發展，正視國軍資訊系統安全機制之研究，實爲當前刻不容緩的議題。相對而言，戰場狀況瞬息萬變，建置三軍網絡化共享參數資料庫，整合三軍聯合作戰 C4ISR 指管通資情監偵之整體戰力，始能發揮統合戰力於無形。然國軍作戰參數數據庫爲三軍聯合作戰演訓之實戰經驗，參數資料除考量更新效能外，更應具備機密性、正確性、完整性、不可否認性以及情報蒐集者之身份隱密性。因之，本文導入群體簽章系統安全性，建置匿名資訊分享與分析機制，可有效降低資訊提供者身份曝光疑慮，確保個人隱私權。且透過群體中的管理者(group manager)統籌產生及分配合法成員私密金鑰，可充分追蹤簽署來源降低資安事件發生。再者，NTRU(N-th degree truncated polynomial ring)密碼系統深具商業化發展潛能，其快速運算能力更具數位化軍事作戰優勢，故本文進一步探討 NTRU 多項式數位簽章，並與其相較，藉此彰顯本簽章機制兼具安全與效率，進而提供爾後導入其加解密系統之先驅。

關鍵詞：ElGamal 數位簽章，群體數位簽章，NTRU(N-th degree truncated polynomial ring)

A Security Scheme for Combat Parameter Database —based on Anonymous Information Sharing

Jonathan Chen [1] Yen-Lin Yin [2] Wen-Pin Lin [3] Yu-Chih Hung[4]

[1]Department of Information Management, VANUNG University of Science and Technology, Taiwan, R.O.C.

[2, 3, 4] Department of Information Management, National Defense University, Taiwan, R.O.C.

Abstract

The ROC army has been involved in the applications of military simulation. Along with the development of war game models, we have to provide parameter values for weapons and performance indexes for engaged entities in the model. Therefore, there is a need to build a parameter database to support the modeling procedures. The share of parameters should conform to the general requirements for data security: secrecy, anonymity, integrity, authenticity, protection and unlinkability. By means of Group Digital Signature we propose an algorithm to realize anonymous information sharing among users of parameter database. The group manager is in charge of generating and distributing private keys for all authorized users of parameter database so that he or she can trace the source of every signature to inhibit any event that violates data security requirements. We also compare our algorithm with NTRU, a well-known multinomial digital signature, on the levels of security and computing time complexity and find that our algorithm is

more efficient in the respect of verification scheme on encryption and decryption signature.

Keywords: ElGamal Digital Signature, Group Digital Signature, NTRU (N-th degree truncated polynomial ring)

壹、前　　言

一、研究動機

隨著資訊科技的日新月異，社會網路犯罪案例刻正與日俱增，層出不窮。相較於此，海峽兩岸由於民族意識分歧以及政治意見相左，長期以來之軍事武力對峙已逐漸轉化成資訊武力競爭。近期，從報雜誌刊載海峽對岸官方網軍入侵國內軍事機敏處所以及個人電腦等資安事件，突顯出海峽對岸運用資訊戰力擷取國軍軍事情資之戰略手段。因之，面對近年來新一代高科技戰爭之作戰思維，國軍建構「網絡化」之現代化聯戰指揮機制，亦是現代化軍事事務革新之時勢所趨。換言之，提升國軍聯戰戰略思維，建立即時戰場決策管理知識庫，亦是有效遂行戰場管理之決勝手段。然而，爲有效整合三軍聯合作戰情資，統合資源共享與分析管道，建置聯戰共同參數資料庫勢必爲各軍種聯合作戰共用資源存取之重大基礎建設，亦爲整體作戰決策管理之核心。

因之，資訊正確性與來源可靠性以及傳遞即時性，即爲提升系統參數運用之價值，勝兵先勝之關鍵成功因素。故如何持恆確保系統能快速傳遞正確可靠之敵情動態參數，又可兼顧降低資料提供者身份洩密之顧忌，實爲值得探究之課題。總體而言，永續獲得參數資料之正確性與實用性，惟有提供情報分享人員身份隱密之作業環境，方可降低身份曝光之疑慮，確保人員安全無虞，間接提升分享意願。

二、研究目的

爲建置一套嚴謹綿密之參數資料保護機制，倘若參數資料傳遞作業機制滿足下列特性，必可實踐一個完善之參數交換共享機制。

(一)機密性(Secrecy or Privacy)

防止非法之接收者得知由資訊共享者所傳遞之參數資料明文。

(二)匿名性(Anonymity)

傳送者輸入資料庫參數數據，接收者可確定該訊息係合法成員所發出，惟不知是哪一位所發送。

(三)完整性(Integrity)

確保資料數據沒有被有意或無意之竄改，及被部分取代、加入或刪除等等。

(四)鑑定性(Authenticity)

確定所獲參數來源之合法性，亦此參數確由發送方所發送。而非他人所僞造，或利用以前的訊息來重送。

(五)保護性(Protection)

除傳送參數者外，組織內其他成員亦無法根據所攔截之訊息，從而整理出該文件係由哪一位傳遞者所傳送(除非組織中只有二位成員)；組織之部門主管亦無法於多項式時間內計算出發文者之所有秘密金鑰。因之，組織之主管沒有能力以特定傳送者之身份傳輸訊息。

(六)無關聯性(Unlinkability)

參數接收單位無法追蹤所簽署文件與傳送簽章者之關係，日後文件內容與簽署文公布出來，簽章者也無法追蹤文件與當時他所簽屬的文件之間之關係。

(七)追蹤性(Traceability)

倘若發現可疑參數數據時，接收單位持該參數向該單位主管反映，單位主管可據以查出係由哪一位傳送者所發出。

綜合上述參數交換共享機制之安全特性，運用公開金鑰系統之群體簽章密碼演算法，即可符合國軍資訊系統安全機制之需求。然而，對於安全的群體數位簽章，

匿名性是必然的，也就是說相同的參數訊息，不同的群體成員會產生不同的群體簽章。或者，同一位群體成員對於不同的參數訊息，也會產生不同的群體簽章，不可同時產生相同的群體簽章情勢，且除群體管理者外，其他人均無法辨識。然而，一些群體數位簽章採用 ElGamal 加密機制，普遍未具有匿名特性。2005 年 Zhou Sujing 和 Lin Dongdai，不但具備上述安全性特點，更進一步證明了 ACJT 群體簽章 (Ateniese et al. ,2000) 是 IND-CCA2 (indistinguishable against chosen ciphertext attacks, Section 2)，故符合匿名特性(Bellare, 2003) (Bellare, 2005) (Kiayias and Yung, 2004)(Kiayias and Yung, 2005)。因之，本研究基於 ElGamal 之密碼系統基本原理爲架構，藉由計算離散對數之假設之安全基礎，提出一套可變式群體數位簽章機制，俾利應用於匿名參數數據傳遞系統中，確保安全無虞。

貳、文獻探討

一、群體數位簽章

1991 年，學者 Chaum 及 Heyst 兩位學者率先提出群體簽章(group signature)之概念。顧名思義，主要概念即是允許群體中之合法成員，可以匿名之方式使用群體名義執行簽章行爲，其簽章特性如后：

(一)僅允許群體中的合法成員能執行簽署行爲。

(二)簽章接收者得到簽署文後，有能力驗證該簽章爲合法群體簽章，惟無法知悉爲何人簽署之。

(三)若日後有爭議情勢發生，該簽章仍可以被追蹤出原簽署文之簽章者身份。

其主要概念係群體中的管理者(group manager)負責管控及定義群體中之所有合法成員，並且產生及分配群體中之合法成員個人所屬私密金鑰，提供群體成員得隱匿個人身份，使用群體名義實施訊息簽章。換言之，群體中的任何一位成員即可代替整個群體來簽署有效之簽章。接收端若欲驗證此一訊息簽章之合法性，僅需透過群體對外公開之合法金鑰即可實施驗證，且接收者在驗證過程中無人可透過訊息明文或是對應之多筆簽署文追蹤簽章來源者身份。反之，爲有效防範有心人士利用群體簽章之匿名特性，衍生爭議事件等類案，群體管理者得追蹤訊息簽章來源者身份，確保群體數位簽章適得其用。

典型群體數位簽章之最佳寫照，即是廣泛運用於隱藏單位組織架構之需求或是降低驗證金鑰數量之時機。諸如，承辦人員可透過足以代表單位名義之金鑰實施簽署文件並公告招標事項，而領標公司僅需要使用一把採購單位公告之公開金鑰，即可不需知悉承辦人員身份之前提下，驗證該簽署公告是否具合法性，進而降低衍生採購弊案之可能性。總歸而論，彙整相關先進學者 (Zhang et al., 2005) (Cui et al., 2006)(Ge and Tate, 2006)(Chen et al., 2004) 學術研究，一個安全的群體簽章機制須滿足下列七點需求：

(一)不可僞造性(Unforgeability)

只有組織中合法的成員才可以代替該單位來簽署有效簽章。

(二)可辨明性(Exculpability)

沒有任何一位組織成員或是群體管理者可以代替其他成員簽署全體簽章。

(三)無法連結性(Unlinkability)

給定許多有效但不同的群體簽章，惟無法找出哪些簽章係由哪一位成員所簽署的。

(四)匿名性(Anonymity)

驗證者無法透過簽章訊息，進一步推演出成員身份。

(五)可追蹤性(Traceability)

群體管理者可以計算出有效群體簽章內之重要訊息，進而推導出眞正之簽署者。

(六)抗合謀性(Coalition- resistance)

群體成員之一個合謀子集不能產生出一個有效的不可追蹤簽署文。

二、ElGamal 數位簽章

近代公開金鑰密碼學已廣泛運用於軍事、金融等領域，其安全性大部分係基於解離散對數(discrete logarithms)之困難度上。其中，1985 年，ElGamal 所提出的模指數(modulo)運算數位簽章方法，即是此一公開金鑰密碼系統之代表作。該數位簽章是改良 1976 年 Diffie-Hellman 金鑰交換系統所提出基於單向暗門函數(one-way trapdoor function)之「公開金鑰密碼系統」觀念，並強化簽署訊息之加解密功能，使得密文傳輸更具安全性。其中，數位簽章及加解密技術對於每一個明文(plaintext)，即可產生許多不同的簽署文，故又稱是一種機率式的簽章加密技術。

(一)系統參數

假設系統(或網路中)存在一個很大的質數 P 以及一個模 P 之原根 g，使得解離散對數成爲相當困難的問題。

1. 私密金鑰：簽章者 A 任選一個整數 x，並滿足 $1<x<p-1$，作爲其私密金鑰。
2. 公開金鑰：簽章者 A 計算出其公開金鑰爲 $y=g^x \bmod p$。

(二)簽署階段

如果傳送者 A 欲簽署訊息 m，且滿足 $1 \le m \le p-1$，便可執行下列步驟：

傳送者 A 先任選一個整數 k，滿足 $GCD(k,(p-1))=1$

步驟一：傳送者 A 計算 $r=g^k \bmod p$

步驟二：傳送者 A

求出 $s=k^{-1}(m-xr) \bmod (p-1)$

或 $m=xr+ks \bmod (p-1)$

步驟三：傳送者 A 計算出相對應的數位簽章(r,s)

(三)驗證階段

傳送者 A 將訊息與數位簽章送給接收單位 B，當 B 收到 m 與數位簽章(r, s)後，便利用傳送者 A 的公開金鑰 y 來進行驗證步驟，驗證 $g^m ? \equiv y^r r^s \pmod p$，其中 $(g^m = g^{xr} g^{ks} = g^{xr+ks} \bmod p)$

如果上述成立，接收單位 B 便確定(r, s)確實爲傳送者 A 對訊息 m 所簽署的數位簽章，反之則屬非法簽署。

三、*NTRU*

NTRU 密碼系統起源於 1996 年，Joseph H. Silverman, Jeffrey Hoffstein, Jill Pipher and Daniel Lieman 等布朗大學(Brown University)四位數學學者(Hoffstein, 1998)提出，它是一個植基環 $R = Z[x]/x^N-1$ 之公開金鑰密碼系統。該密碼演算法與傳統公開金鑰密碼系統最大之異同在於，它的安全性架構已不再是植基於困難問題(N-P)。簡言之，公開金鑰之安全性不再是依賴的因數分解或離散對數所產生之難解問題，而是多項式因數分解問題。

NTRU 以 $R = Z[x]/x^N-1$ 的多項式加法與乘法爲基礎，產生三個整數(N, p, q)。其中，N 是質數，p 與 q 是相互關係的質數，滿足 gcd(p, q)=1 且 q>p。其中，加解密運算定理如下(Weichi et al., 2005)。

(一)運算元定義：

1. Z_p 代表 Z 在中執行(mod p)的模數環。
2. $Z_p[X]$代表 Z_p 在中唯一的變數多項式。
3. 一個唯一的變數多項式，能以一個向量表示，定義爲 $f ?x?? ? \sum_{i=0}^{n-1} f_i x^i ? ?f_0,f_1,....f_{n-1} ?? f$
4. f 與 g 的加法，定義爲 $h = f + g$。廣義而言，$h_k = f_k + g_k$ (其中 $0 \le k < n$)。
5. 級數 n 的 f 與 g 的乘積，定義爲 $h = f * g$。廣義而言 $h_k = \sum_{i+j \equiv k \pmod n} f_i g_j$，(其中 $0 \le i, j, k < n$)。
6. $L(d_1, d_2)$是一個唯一的變數多項式，在 $L((d_1, d_2)$中有 d_1 係數等同於 1, d_2 係數等同於 -1，其餘的係數等同於 0。
7. 在積模數環 $Z_p[X]/(X^n-1)$中，f 的反逆爲 f_p。換言之，$f_p * f \equiv 1 \pmod p$。其中，

對於隨機的 f，f_p 不一定永遠存在。

8. NTRU 基本參數爲$(n,p,q,d_f,d_g,d_\varphi)$。

(二)金鑰產生階段

使用者要產生公開金鑰，須完成下列過程。

1. 選擇一個私密金鑰，一個隨機的多項式 $f_p \in L(d_f, d_{f-1})$
2. 計算 f_p, f_q，假設其中一個或兩者不存在，則回到選項(1)。
3. 隨機選擇一個多項式 $g \in L(d_g, d_g)$
4. 計算 $h \equiv f_q * g \pmod q$
5. 私密金鑰爲(f, f_p)，公開金鑰爲 $L(d_1, d_2)$

(三)加密階段

1. 加密明文 m，選取隨機多項式 $\phi \in L(d_\phi, d_\phi)$，並使用公開金鑰 h 計算密文 e。
2. 計算 $e \equiv p\varphi * h + \pmod q$
3. 求得密文 e

(四)解密階段

1. 假設獲得密文 e，即可使用自己的私密金鑰 f 實施解密。
2. 計算 $a \equiv f * e \pmod q$
3. 計算 $m' \equiv f_p * a \pmod q$
4. 解密訊息爲 m'，假設沒有錯誤發生，則 m' =m

(五)公開金鑰演算法比較

1976 年，Diffie-Hellman 提出第一個公開金鑰加密系統後，許多主要著名的公開金鑰加密系統也如雨後春筍般地相繼提出，例如：RSA(Rivest et al., 1978)、ECC (Koblitz, 1987) (Menezes, 1993) 以及 NTRU，他們花費在執行的時間上，一般都是在執行模數乘法運算。這些模數乘法運算，包含了整數模數乘法運算、二進位多項式模數乘法運算或是在整數環上的多項式乘法運算。

2000 年，學者 P. Karu 和 J. Loikkanen 提出了 NTRU 與 RSA、ECC 三者間，在相對安全性層度上，其運算速度上之比較 NTRU 大於 RSA 與 ECC 兩者，且 NTRU 之速度更可藉由選擇不同的環(Ring)以及運用更有效率的線性參數變換來改善 (Hoffstein and Silverman, 2000, 2003) (效能分析表如表 1) 。

表 1 效能分析表

1024 bit RSA	
短指數	
模術乘法運算	17
時間(mst)	4.33
長指數	
模術乘法運算	1500
時間(mst)	382.25
160 bit ECC	
雙精度浮點數 (每次執行模術 9 倍數)	159
小數點加法 (每次執行模術 16 倍數)	53
模術乘法運算總和	2279
時間(ms)	15.26
503 NTRU	
時間(ms)	6.08

資料來源：O′Rourke and Sunar,2003

由表 1 可知，當NTRU之 N=503，相同的乘數能較算出值約爲 6ms 的多項式乘法運算。因之，若以相同安全性來分析 NTRU 執行效率較 RSA 與 ECC 較高。

參、系統架構與建置

一、前置動作

系統中心選取滿足下列式子之大質數 P_1。

$$P_1 = 4pq + 1 \quad (1)$$

其中，p,q 亦爲大質數

$$令\ n = p*q \quad (2)$$

再選取模(modulo) P_1，其序(order)爲 n 之一數 g

$$即\ g^{\frac{1}{2}n} ? ?1?\bmod p_1? \quad (3)$$

然後選取一數 $x_0 \in Z_n$，計算

$$y_0 ? g^{x_0} ? \bmod p_1 ? \quad (4)$$

由上述運算可得知，系統中心之公開金匙爲 p_1, n, g, y_0 ；系統中心之秘密金匙爲 p, q, x_0 。

二、使用者註冊

使用者 u_i 選取一數 $x_i \in Z_n$，計算

$$y_i ? g^{x_i} ? \bmod p_1 ? \quad (5)$$

u_i 傳送$\{y_i\}$向系統中心申請註冊，系統中心選取一數 $k_i \in Z_n$，計算

$$r_i ? g^{k_i} ? \bmod p_1 ? \quad (6)$$

$$s_i ? x_0 y_0 ? k_i r_i ? \bmod n ? \quad (7)$$

系統中心傳送 $\{r_i, s_i\}$ 予 u_i。

/* u_i 之公開金鑰爲 y_i，秘密金鑰爲 x_i

三、訊息傳送

假定 u_i 欲匿名傳送訊息 m，其演算步驟爲：

(一)選取一數$a \in Z_n$，計算

$$A_1 \equiv g^a (\bmod p_1) \quad (8)$$

$$A_2 \equiv (s_i + a r_i) A_1 (\bmod n) \quad (9)$$

$$A_3 \equiv A_1 y_i (\bmod p_1) \quad (10)$$

$$r'_i \equiv A_1 r_i (\bmod n) \quad (11)$$

(二)選取一數$b \in Z^*_n$ ，計算

$$B \equiv g^b (\bmod p_1) \quad (12)$$

$$m \equiv (x_i + a) B + b s'_i (\bmod n) \quad (13)$$

(三)傳送資料$\{m, A_2, B, r'_i, s'_i\}$予接收者 R

四、訊息驗證

接收者 R 驗證下列式子

$$g^{A_2} r_i^{? r_i ?} ? y_0^{? g^m B^{-s_i} ?^{B^{-1}} ? \bmod p_1 ?} ? \bmod p_1 ? \quad (14)$$

如果上列式子成立，則接受訊息 m，否則，拒絕接受

肆、安全性與複雜度分析

一、安全性分析

引理 1：$A_2 \equiv x_0 A_3 + (k_i + a) r'_i \pmod n$ (15)

証明：由式子(7)知

$$s_i + a r_i \equiv x_0 y_i + (k_i + a) r_i \pmod n \quad (16)$$

$$A_1(s_i + a r_i) \equiv x_0 (A_1 y_i) + (k_i + a)(A_1 r_i) \pmod n \quad (17)$$

$$A_2 \equiv x_0 A_3 + (k_i + a) r'_i \pmod n \quad (18)$$

依據式子(9)，(10)，(11)

所以，我們得到證明

引理 2：$g^m ? A_3^B B^{s_i ?} ? \bmod p_1 ?$ (19)

證明：本證明簡單，我們省略討論。

定理 1：如果 u_i 是誠實的，則式子(14)成立。

證明：由引理 1.可得知

$$g^{A_2} ? y_0^{A_3} r_i^{' r'_i} ? \bmod p_1 ? \quad (20)$$

由引理 2.知

$$A_3 ? ? g^m B^{? s_i ?} ?^{B^{-1}} ? \bmod p_1 ? \quad (21)$$

整理前面二個式子，得到下列式子

$$r_i^{? r_i ?} g^{A_2} ? y_0^{? g^m B^{-s_i} ? ? \bmod p_1 ?} ? \bmod p_1 ? \quad (22)$$

因此，我們得到證明。

接著我們就攻擊者針對式子(14)，所可能採取之攻擊進行討論。

狀況(1)：攻擊者任意選取 $\{A_2, B, r'_i, s'_i\}$ 參數企圖解出對應之訊息 m。

討論：由式子(14)知，攻擊者必須能解出(固定)參數 y_0 之指數。倘若就算能解出，他仍將面臨再度解析 $? g^m B^{-s'_i} ?^{B^{-1}} ? \bmod p_1 ?$之指數 m，其餘難度與破解離散對數之複雜度相同。

狀況(2)：攻擊者任意選取 $\{A_2, m, s'_i, B\}$ 參

數，企圖解出對應之參數 A_2

討論：本狀況與前述狀況類似，我們省略。

狀況(3)攻擊者任意選取{m, A_2, B , s'_i }參數，企圖解出對應之 r'_i

討論：整理式子(14)攻擊者可歸納出

$$r_i^{r_i'} \equiv y_0^{g^m B^{-s_i'} \bmod p_1 - 1} g^{-A_2} \bmod p_1$$

吾人知，上式解 r'_i 之複雜度，至少是解離散對數之複雜度。其他狀況，諸如攻擊者任選式子(14)中之部分參數而企圖解出其所對應之未知參數，攻擊者均有面臨破解離散對數之困境。

定理 2.攻擊者無法僞造式子(14)成立，除非他能破解離散對數之複雜度。

證明：由前述狀況(1)(2)(3)等之討論，我們可以得証。

二、複雜度分析

由方程式(9)(11)(12)(13)可以得知本系統複雜度分析爲 O(log n)。反之，經由 Joseph H. Silverman 等人之 NTRU 演算法簽章階段之多項式乘法運算得知，複雜度分析爲 O (N^3)。由此觀之，本系統具備高效率模式。

伍、結　論

隨著國軍資訊科技基礎建設日趨成熟，資訊戰士已是今後數位戰場決勝之先鋒部隊。面對二十一世紀之作戰型態，資訊系統已日漸取代傳統人力優勢，儼然成爲戰場關鍵成功因素之一。換言之，作戰參數資料庫更進一步扮演著戰場指揮官決策管理之智囊角色。因之，資訊系統參數資料庫之正確性與完整性維護，其重要性不容小覷。有鑑於此，透過本研究之改良式群體簽章密碼系統模組運算，可提供參數資料提供者安全無虞之使用者環境，且情傳人員可充分匿名個人身份，降低洩漏身份之疑慮，藉此提升情資分享意願。簡言之，面對網路駭客僞冒攻擊，透過本研究密碼模組安全性分析，可使攻擊者面臨分解離散對數之困難問題，充分達到嚇阻駭客入侵之優勢。

於國防管理之實務應用：以美國爲例，情資體系大部分由國防部部長所掌控，惟各情資單位經常不將高度機敏情資與對口單位分享，爲的是保護情資來源與取得方式。目前國軍刻正積極研發國防資訊分析及分享中心(**M-ISAC**)技術，其主要的功能即爲情資的分享，因此，運用本研究建立一個匿名情資分享平台，可促使各單位提供情資分享意願，並配合該系統其他蒐集情資管道，將可有效蒐整系統所需情資，俾利後續情資分析與運用。

參考文獻

Ateniese, G., J. Camenisch, M. Joye, and G. Tsudik, 2000. A practical and provably secure coalition-resistant group signature scheme," in Crypto'00, LNCS 1880, 255-270, Springer-Verlag.

Bellare, M., D. Micciancio, and B. Warinschi, 2003. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions, in Eurocrypt'03, LNCS 2656, 614-629, Springer-Verlag.

Bellare, M., H. Shi, and C. Zhang, 2005. Foundations of group signatures: The case of dynamic groups," in CT-RSA'05, LNCS 3376, 136-153, Springer-Verlag.

Chaum, D., and Heyst, van E., 1991. Group Signatures, Advances in Cryptology-EUROCRYPT, vol. 547, 257-265.

Chen, Z., J. Huang, D. Huang, J. Zhang, Y. Wang, 2004. Provably Secure and ID-Based Group Signature Scheme, AINA 2004, 18th International Conference on Advanced Information Net-

working and Applications, vol.2, 384-387.

Cui, S., C.W. Chan and X. Cheng, 2006. Practical Group Signatures from RSA, AINA'06, 111-115.

Diffie, W. and M.E. Hellman, 1976. New directions in cryptography. In IEEE Trans. On Information Theory, vol. 22, 644-654.

ElGamal T., 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. On Information Theory II-31 (4), 469-472.

Ge, H. and S.R. Tate, 2006. A group signature scheme with signature claiming and variable linkability, IPCCC 2006. 25th IEEE International, 497-504.

Hoffstein, J., J. Pipher and J. H. Silverman, 1998. NTRU: A Ring-Based Public Key Cryptosystem, Preprint.

Hoffstein, J. and J.H. Silverman, 2000. Optimizations for NTRU. In Public-key Cryptography and Computational Number Theory.

Hoffstein, J. and J.H. Silverman, 2003. Random small Hamming weight products with applications to cryptography. Discrete Applied Mathematics, vol. 130, 37-49.

Karu, P. and J. Loikkanen, 2000. Practical comparison of fast public-key cryptosystems.Seminar on Network Security, Telecommunications Software and Multimedia Laboratory, Kelsinki University of Technology. Available at http: //www.tml.hut.fi/Opinnot/Tik-110. 501/2000/papers.html.

Kiayias, A. and M. Yung, 2004. Group signatures: Provable security, efficient constructions and anonymity from trapdoor-holders, in http://eprint.iacr.org/2004/076/.

Kiayias, A. and M. Yung, 2005. Group signatures with efficient concurrent join, in Eurocrypt'05, LNCS 3494, 198-214, Springer-Verlag.

Menezes, A. J., 1993. Elliptic Curve Public Key Cryptosystems. Boston:Kluwer Academic.

N. Koblitz, 1987. Elliptic Curve Cryptosystems, Math. Computation, vol. 48, 203-209.

O'Rourke, C. and B. Sunar, 2003. Achieving NTRU with Montgomery Multiplication, IEEE Computer Society.

Rivest, R.L., A. Shamir and L. Adleman , 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Comm. ACM, vol. 21, 120-126.

Sujing, Z. and L. Dongdai, 2005. On Anonymity of Group Signatures, International Association for Cryptologic Research.

Yu, W., D. He and S. Zhu, 2005. Study on NTRU Decryption Failures, Information Technology and Applications, ICITA 2005.

Zhang, J., J. Zou and Y. Wang, 2005. A Group-Oriented Anonymous Signature scheme with Subliminal Channel, Networking, Sensing and Control, 2005 IEEE , 49-53.

相關研究專案

行政院國家科學技術發展基金會
九十六年度研究計畫
編號：NSC 96-3114-P-606-002-Y
【國防資訊分析及分享中心(M-ISAC)技術研發暨建置計畫】