

行政院國家科學委員會專題研究計畫 成果報告

離散代數結構之應用於計算與密碼學

計畫類別：個別型計畫

計畫編號：NSC93-2115-M-032-008-

執行期間：93年08月01日至94年07月31日

執行單位：淡江大學數學系

計畫主持人：楊柏因

計畫參與人員：楊柏因

報告類型：精簡報告

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 94 年 10 月 24 日

行政院國家科學委員會專題研究計畫 成果報告

代數與離散結構之應用於計算與密碼學： Computing and Crypto Applications of Discrete Algebraic Structures

計畫編號: NSC - 93 - 2115 - M - 032 - 008

執行期限: 2004 年 8 月 1 日至 2005 年 7 月 31 日

計畫主持人: 楊柏因 淡江大學數學系

中文摘要

吾人計畫所提出的目標分為計算與密碼學，於執行全程中，吾人根據當時提出的目標，持續進行研究，並分別在計算理論與密碼學方面各提出受本計畫補助的三篇論文。

在計算理論中，有所謂 Gröbner 基底法，為一種解非線性方程式的演算法，在有限體中解非線性方程組為一在密碼學上有極多應用的問題，亦眾所週知為所謂 NP-完備的問題，其定命性解法必為指數時間以上，但期望用時最短的演算法能做到多快則為一未解問題。五年前 Shamir 等人提出類似的 XL 演算法，Courtois 氏並聲稱其可以用以破解很多公鑰密碼系統，因之轟動一時，吾人去年在澳亞資訊安全與密碼學會議 (ACISP 2004) 首次公開提出 XL 在數學上的分析；在其後的計畫執行期間，分別在西班牙的國際資通安全會議 (ICICS 2004)，韓國的國際資訊安全與密碼學研討會 (ICISC 2004) 和義大利的代數幾何中的有效方法研討會 (MEGA 2005) 提出對解非線性方程組的分析，全文皆見於大會專刊，並否決了 Shamir 氏猜測，即 XL 類演算法能以多項式時間，在有限體上解出一般的非線性方程組。

另外，吾人在多變量密碼學上的研究，亦為去年的密碼學硬體與嵌入式系統國際研討會 (CHES 2004)，以及今年的公開金鑰密碼學國際研討會 (PKC 2005) 和澳亞資訊安全與密碼學會議 (ACISP 2005) 所接受，並刊登於電腦科學札記周刊 (Lecture Notes in Computer Science, Springer 公司出版) 的大會專刊。

多變量密碼學是目前研究很熱烈的一個新領域，由於其低資源、高效能的特性，和對量子電腦攻擊的抵抗力，吾人研究的系統自成一類，即所謂類溫良的多變量公鑰密碼系統，在效能和安全性上的推演有獨到之處，也受到國際密碼學界的肯定。

關鍵字: 密碼學, 非線性方程組, 演算法, 多變量公鑰密碼系統, 類溫良

Abstract

My project had dual aims in computing and cryptography. Accordingly, I conducted research and published three papers in each of these two areas.

It is well-known that solving nonlinear (equivalently quadratic) systems over a finite field is NP-complete, hence all deterministic solvers must be at least exponential. However, how quickly you can solve these systems on average and how is an important and long-standing problem.

Usually these equations are solved with Gröbner Bases. In 2000, Courtois, Klimov, Patarin and Shamir proposed the related XL method, a variant of which is claimed to solve a generic system in probabilistic polynomial time. I published the first mathematical analysis of XL last year at ACISP 2004. During the course of this project, I presented more results at ICICS 2004, ICISC 2004 and MEGA 2005, which refuted Shamir's claim. I also refuted Courtois' claims of using XL variants to cryptanalyze other public-key cryptosystems.

My other research was concentrated in the area of public-key cryptosystems. A subclass of public-key cryptosystems called multivariates or MQ schemes are attracting more attention because they are efficient for low-resource use and resists attacks using Quantum Computers. I proposed a new subclass of multivariates called *tame-like*, and analyzed their security. I also showed that they have desirable properties for efficiency, and this is well-received by the international cryptology community in general.

Keywords: cryptography, multivariate systems of quadratic equations, finite fields, algorithms, multivariate public-key cryptosystem, tame-like

1 緣由與目的

近年來我國政府致力推動網路商務與資訊安全體系，而網路與通訊安全中密碼系統當然為重要的一環。

一本廣為使用的密碼學教科書（“密碼學與網路安全”，[31]）說：所謂“沙灘難起高樓”，資訊安全奠基於密碼系統理論上的安全性，如果密碼系統不可靠，則資訊也無安全可言。

另一位有名的安全專家 Schneier 在他的近作 “Practical Cryptography” ([29]) 中警告大家，“一條鍊子只和它最脆弱的一環一樣強”，因此他說，“事實上大部份的密碼系統被攻破都不是因為理論上的漏洞”，不過他也強調，“但是在基本上就有問題，也就是理論上有漏洞的密碼系統，這當然不可能安全”。Schneier 同時也警告大家，在可以容許的速度下，安全性比速度重要。

即使如此，傳統的公鑰密碼系統也碰到的速度的瓶頸。自 Diffie-Hellman ([11]) 提出公鑰密碼學以來，公鑰密碼系統多在巨型代數結構上運算，故傳統式的公鑰密碼系統又稱為單變元公鑰密碼系統 (Univariate Public-Key Cryptosystem)，但其中的大代數結構如 RSA-1024 中的 128 位元組長整數，或 ECC 的橢圓曲線的計算本身都無可避免的都相當慢，且已研究日久較少新意。與此同時，RSA 在數論專家最新的攻擊手段下，被迫採用日漸加長的鑰匙，這對小型或嵌入式系統 (embedded system) 如智慧卡 (smart cards) 上的密碼學應用造成很大的負擔。

為了這個可以容許的速度，Matsumoto 與 Imai [23] 提出所謂的多變元公鑰密碼學 (Multivariate Public-Key Cryptography)。即在數位簽章或加密等系統上，利用多個多項式 (通常二次) 為驗證函數或加密函數，事實上，近年採納的標準對稱區塊加密系統：先進資料加密標準 (AES)，即 Rijndael 密碼，亦採仿多變量型式而設計 ([9])。由於它具有相同的設計安全性下較高效能，因此目下研究者日眾，吾人亦致力於彼。

要研究更好的多變元公鑰密碼系統，當然包括研究它的安全性，也就是說包含破密的方法。因此吾人也投注心力於演算法的分析與改良，其中自然包括『尋求最好的解高次方程組的演算法』，這也就是對多變元公鑰密碼系統所本的難題的原始攻擊方式。

2 研究成果

吾人於計畫進行中，共有六篇論文為知名的研討會中接受，略述於下：

CHES 2004 08.11-13, [40],
第6屆密碼學硬體與嵌入式系統國際研討會，美國波士頓 (M.I.T.)

ICICS 2004 10.27-29, [41],
第6屆國際資通安全會議，
西班牙馬拉加 (Malaga)

ICISC 2004 12.02-03, [38],
第7屆國際資訊安全與密碼學研討會，韓國首爾 (漢城)

PKC 2005 01.23-26, [34],
第7屆公開金鑰密碼學國際研討會，
瑞士雷第亞不列 (Les Diablerets)

MEGA 2005 05.27-01, [2],
第8屆代數幾何中的有效方法研討會，義大利亞格洛 (Alghero)

ACISP 2005 07.04-06, [39],
第10屆澳亞資訊安全與隱私權研討會，澳洲布理斯本 (Brisbane)

除 PKC 2005 由共同作者王立中教授代往發表之外，本人均前往與會並報告。

2.1 XL 解聯立方程組的研究

多年來解方程組的制式動作用就是 Buchberger 演算法，算出一套 Gröbner 基底。近年來這也有了變化——由數學家 Lazard 在 1983 提出的理論 ([21]) 最近被重新發揚光大，也就是 XL 和 F_4 - F_5 系列的解方程式演算法。

XL: XL (eXtended Linearization, 延伸線性化, [6]) 方法在 1999 年前後由 Courtois, Klimov, Patarin 與 Shamir 提出 (Ars 主張 XL 是 Lazard 早已發現的, [1])。在 2000-04 之間 Courtois 提出幾個變形, 其中最重要的是 FXL。

F₄-F₅: J.-C. Faugère 以 F₅ 演算法配合代數攻擊破解了 HFE 挑戰一號 ([14, 15, 16])。在澳洲發展出來的 MAGMA 系統使用改良式的 F₄ 演算法, 它號稱目前解方程組速度最快的商用數學軟體; 2004 年 12 月的今天可能有四五組人馬企圖自行開發 F₄ 或 F₅ 演算法。

XL 和變形們 (FXL, XLF, XFL, XSL, XL', XL2 — 可見 [4, 7, 8]) 從重線性化 (relinearization, [20]) 演化而來。XL 類操作的原理如次: 假設我們有基體 K 上的 n 個變數 $\mathbf{x} = (x_1, x_2, \dots, x_n)$ 的 m 個二次 (更高次也類似) 方程式 $l_1(\mathbf{x}) = l_2(\mathbf{x}) = \dots = l_m(\mathbf{x}) = 0$, 且 $n \leq m$, 那麼 D 次的 XL 操作如下:

1. 第一步驟是 X, X 表示乘或延伸 (eXtend), 我們以每一個單項 $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ (通常記作 \mathbf{x}^α , 而我們要求單項的次數 $\sum_i \alpha_i \leq D-2$), 乘以每一個方程式 $l_j = 0$;
2. 第二步驟是 L, L 表示線性化 (linearize), 把每個 D 次或更低的單項當成一個獨立的變數, 並把這樣求出來的 $m \binom{n+D-2}{n}$ 條方程式 (當 $q = |K| \leq D$ 時會變少) 做高斯消去法, 而變數的排序, 也就各單項式被消去的順序, 採用相反字典式 (reverse lexicographical order)。如此最後被消去的必定是第一個變數 x_1 的單項。
3. 如果獨立的方程式至少有 $\binom{n+D}{n} - D$ 條 (這個下限在 $|K| \leq D$ 時也會變少), 我們已消去含 x_1 以外任何變數的單項, 即得一 x_1 的方程式, 並在求出 x_1 後得到每個變數。

在 Courtois 等發明的 XL 的變形中, 根據申請人與陳君明等的最近研究 ([2, 37, 38, 41]), 最有用的是 FXL: 'F' 表示 Fix, 在 $m = n$ 時 XL 執行起來不理想。所以想到先猜 f 個變數讓變數的個數小些, 然後跑 XL 試試看, 發現沒有解就不再猜, Courtois 原本預測很小的 f 即可達到很好的結果, 吾人的研究發現對於一個一般性的方程組而言, 必需瞎猜一個和 n 大致成正比例的 f 個變數才是最佳的。其他幾個變化都不很有用。

Faugère 的 [14] 把 Buchberger 的 Gröbner 基底演算法理論推進一步, 他提出的 F₄ 法和 Courtois 提出來的 XL+XL2 有七分相似 ([8]), 即先消去高次項, 然後有系統的用各變數去乘消去後剩下來的低次方程式, 再重複消去的動作。F₅ 可說是 F₄ 的加強版, 也就是說在執行中靠 Frobenius 條件避免了生成出相依的方程式 ([15])。到今天為止商用程式中最佳的解方程組演算法是 Sydney 大學的 MAGMA ([22]), 使用改良的 F₄ 演算法, 但該軟體並不普及。

在有限體中解方程組目前重要問題是: F₅ 演算法中有嚴格限制的消去法是否可以用等同於 Lanczos 方法的速度做完? 若是, 則 F₅ 加上猜測變數 (吾人名此法為 FF₅, [38]) 當為對一般的方程組的最佳選擇, 如否, 則應採用 FXL。

2.2 XL 代數攻擊的主要定理

吾人將上節述及的主要結果略敘於下:

Theorem 1 (Yang-Chen, [37, 38]). 令 $[u]_s :=$ 為 u 在 s 的展式中的係數。

$$T = [t^D] \frac{(1-t^q)^n}{(1-t)^{n+1}}; \quad (1)$$

$$T - I = [t^D] \left(\frac{1}{1-t} \left(\frac{1-t^q}{1-t} \right)^n \left(\frac{1-t^2}{1-t^{2q}} \right)^m \right).$$

式中 T, I 分為單項與獨立的方程式的總數, 最後一式僅在諸 (l_i) 為半規則時成立, 所以右邊需要保持為正, 對大的體 ($q \gg 1$) 而言,

$$T - I = [t^D] ((1-t)^{m-n-1} (1+t)^m). \quad (2)$$

又據 C. Diem 的結果 [10], Fröberg 猜想為真時本定理必提供 $T - I$ 的下限。

Theorem 2 (Bardet-Faugère-Yang, [2, 37]). 在大的體上當 $\sqrt{m} \gg f \geq 2$,

$$\begin{aligned} D_{reg} &= \frac{m}{2} - (h_{f-1,1})\sqrt{\frac{m}{2}} + O(1) \\ &\sim \frac{m}{2} - \sqrt{fm}; \end{aligned} \quad (3)$$

又當 $f(\sim cm)$ 時

$$D_{reg} = \left(\frac{1}{2} - \sqrt{c} + \frac{c}{2}\right)m + O(m^{\frac{1}{3}}). \quad (4)$$

$h_{n,1} :=$ 為第 n 個 Hermite 多項式 H_n 的最大根 $= \sqrt{2n+1} + O(n^{-1/6})$ [32].

Theorem 3 (Yang-Chen, [38]). *FXL*, 即先猜 f 個變數再跑 *XL*, 是當 $m \sim n$ 的 *XL* 最佳用法, 且大致上最佳 $f \propto n$ 。

Theorem 4 (Yang-Chen, [37, 38]). 對 Courtois 氏提出的 *XFL*, *XL*, *XL2* and *XL'* 的方法, 吾人有: [4, 8]:

- *XFL* 等於以空間換取時間的 *FXL*。
- *XL* 和 *XL'* 永遠比 *FXL* 為劣。
- 如使用 *XL+XL2*, 對所有的變數操作並只消去最高次項, 等同於 F_4 。

Theorem 5 (Diem-Yang, 2004). Courtois-Shamir 猜想, 即 **FXL** 可在多項式時間內解出二次方程組 [6], 不真。

2.3 快速安全的數位簽章 TTS

標準的多變量公鑰系統包含一個以上非線性映射夾在兩個線性映射之間, 此為極普遍的架構, 公鑰在多變元密碼系統中皆代表一個映射以 $V: w \in K^n \xrightarrow{\phi_1} x \xrightarrow{\phi_2} y \xrightarrow{\phi_3} z \in K^m$ 形式存在; 式中, K 為一有限體, 即為所謂基體 (base field), $|K|=q$, 參數 n 與 m 分別為簽名或明文區塊 (signature or plaintext block) 和文摘或密文區塊 (digest or ciphertext block) 之維度, 映射 $\phi_1: w \mapsto M_1 w + c_1$ 與 $\phi_3: y \mapsto M_3 y + c_3$ 為平直(線性), ϕ_2

為非線性。一般而言, 吾人將 V 表現成 m 個 n 變元二次多項式, 即

$$z_k = \sum_i P_{ik} w_i + \sum_k Q_{ik} w_i^2 + \sum_{i<j} R_{ijk} w_i w_j,$$

而諸係數 P_{ik}, Q_{ik}, R_{ijk} 共 $mn(n+3)/2$ 個即為公鑰。矩陣 M_1^{-1}, M_3^{-1} , 向量 c_1, c_3 , 所有 ϕ_2 中的可調整參數為私鑰 (通常取 c_3 使 $V(0) = 0$)。密碼系統之安全性將繫於解 $V(w) = z$ 方程組與將 V 還原成其三部份 $\phi_3 \circ \phi_2 \circ \phi_1$ 之複雜度。

TTS (Tame Transformation Signature) 為一多變元公鑰簽章系統, 基本形狀如上。其特色在於使用類溫良 (tame-like) 的中央映射 (即上述 ϕ_2)。代數幾何中所謂溫良變換 (Tame Transformation), 係指平直, 或所謂 de Jonquiere 三角型映射, 亦即重排各成份順序後對每一 i 有 $y_i = x_i + p_i(x_1, \dots, x_{i-1})$ 的結構, 其中各 p_i 為多項式, 凡此則給定 y 可以按照順序解出 x 之各成份, 但其逆映射次數極高, 不容易以明式 (explicit form) 列出。此性質適合乎密碼學中作為所謂單向映射 (One-Way Trapdoor Map) 的概念。吾人推廣其為一多項式映射, 其參數少, 計算速度快, 且其反影在指定的集合上可以僅使用連續的代入與解一次方程式或聯立方程組而得到。

吾人目前的版本稱為 Enhanced TTS, 或稱 TTS/5 [39], 有多種可能參數, 當 $n = 28, m = 20$ 中心映射 ϕ_2 如下:

$$\begin{aligned} y_i &= x_i + \sum_{j=1}^7 p_{ij} x_j x_{8+(i+j \bmod 9)}, i = 8 \dots 16; \\ y_{17} &= x_{17} + p_{17,1} x_1 x_6 + p_{17,2} x_2 x_5 + p_{17,3} x_3 x_4 \\ &\quad + p_{17,4} x_9 x_{16} + p_{17,5} x_{10} x_{15} + p_{17,6} x_{11} x_{14} + p_{17,7} x_{12} x_{13}; \\ y_{18} &= x_{18} + p_{18,1} x_2 x_7 + p_{18,2} x_3 x_6 + p_{18,3} x_4 x_5 \\ &\quad + p_{18,4} x_{10} x_{17} + p_{18,5} x_{11} x_{16} + p_{18,6} x_{12} x_{15} + p_{18,7} x_{13} x_{14}; \\ y_i &= x_i + p_{i,0} x_{i-11} x_{i-9} + \sum_{j=19}^{i-1} p_{i,j-18} x_{2(i-j)-(i \bmod 2)} x_j \\ &\quad + p_{i,i-18} x_0 x_i + \sum_{j=i+1}^{27} p_{i,j-18} x_{i-j+19} x_j, i = 19 \dots 27. \end{aligned}$$

TTS/5 產生鑰匙對之程序: 隨機選出滿秩 (full-rank) 之方陣 M_1, M_3 , 向量 c_1 , 與非零之諸參數 $p_{ij}, i = 8 \dots 27$ 。計算 $V = \phi_3 \circ \phi_2 \circ \phi_1$ 並同時挑選 c_3 使 V 的常數項為 0, 計算 M_1^{-1}, M_3^{-1} , 與各參數和 c_1, c_3 合為私鑰 (1312 位元組), V 之係數為公鑰 (8680 位元組)。

TTS/5 由文件產生簽章之程序：

1. 先由雜湊函數取得文摘，令其為向量 $z \in K^{20}$ 之成份；
2. 使用私鑰中的資料生成 $y = M_3^{-1}(z + c_3) \in K^{20}$ (注意 y 之足標係由 $8 \dots 27$)；
3. 隨機取 $x_1, \dots, x_7 \in K$ ，並試解 x_8, \dots, x_{16} 至有解為止。
4. 解出後可依序解出 x_{17}, x_{18} 。而後隨機取 x_0 ，並試解 $x_{19}, \dots, x_{27} \in K$ ，重複試到可解為止 (最多僅 9 個 x_0 使行列式為零故終究有解)。
5. 計算 $w = M_1^{-1}(x + c_1) \in K^{28}$ 。

TTS/5 之驗章手續：收取文件與簽章組 (M, w) ，經 SHA-1 雜湊函數計算文摘 z ，驗證是否 $z = V(w)$ ，是則表示簽章為有效，否則為無效。

2.4 類溫良公鑰密碼系統種種

滿足和 TTS 相同條件的公鑰密碼系統，即中心多項式參數少且為疏落 (**sparse**)，並其反影在可以快速的根據某種逐次 (**recursive**) 的手續得到則稱為類溫良 (**tame-like**) 的系統。

類溫良型又稱馴類型，同屬於此類的系統還有 TRMS 和 MFE [18, 34]。類溫良的系統在私密映射 (**private map**) 速度上當然有其優勢，但是在生成金鑰的速度上也有好處。大體型 (C^* 和 HFE 的衍生物) 多變元公鑰密碼系統，生成公鑰最快的方式是 Wolf 的方法 [35]，其生成時間是 $\Theta(n^6)$ ，而...

Theorem 6 (Yang-Chen-Chen, [39, 40])。類溫良的公鑰密碼系統可以在 $o(n^5)$ 時間完成生成公鑰。

作法如下，對每對足標 $i < j$ ，可以同時 (對每一個 k) 算出每個

$$\bar{R}_{ijk} = \sum_{\pi_{x_\alpha x_\beta} \text{ in } y_k} [\pi((M_1)_{\alpha i}(M_1)_{\beta j} + (M_1)_{\alpha j}(M_1)_{\beta i})]$$

¹在此限制之內為提防 FXL/FF₅ [38]， v 越小越好。

再做乘上 M_3 的動作即可算出各 R_{ijk} ：

$$R_{ijk} = \sum_{\ell=n-m}^{n-1} \bar{R}_{ij\ell}$$

P 和 Q 仿此。此所以 TTS 與 TRMS 之能夠即時的 (**real-time**) 生成金鑰。

Theorem 7 (Yang-Chen, [39])。當類溫良型系統所需的安全度為 C ：

1. 當中心多項式能組合出最小的秩為 r 者，其對應到不同的核空間有 k 個，而 $\ell = \lceil m/n \rceil$ ，則

$$q^{r\ell} \cdot (m^2(n/2 - m/6) + mn^2) / k \geq C. \quad (5)$$

通常 r 為中心多項式中最小交叉項數之兩倍 [17]。

2. 當每個中心變數最少出現在 u 個方程式的交叉項中，則 [17]

$$q^u (un^2 + n^3/6) \geq C. \quad (6)$$

3. 令 v 為使每一個中心變換中的交叉項必有一足標在 $A \subset \{0 \leq i < n\}$ 中， A 能包含的最少變數個數，則¹

$$q^{2v-n-1}(n-v)^4 \geq C. \quad (7)$$

4. 令 $D_0 : \min\{D : [t^D]((1-t)^{k-1}(1+t)^m)\}$ ，與 $T := \binom{m-k+D_0}{D_0}$ ，則：

$$\min_k q^k \cdot m^{\gamma_0} T^\omega (c_0 + c_1 \lg T) \geq C. \quad (8)$$

其中 c_0, c_1, γ 為常數 [38]， ω 為解方程組的階數。

5. 中心多項式中不應有過份制約 (**overdetermined**) 的子方程組，否則會如王立中的 TRMC v2 [33] 一樣被 XL 類型的方法攻破 [19]。

2.5 其他

在本計畫執行期間內的其他研究，尚有其他次要成果與整理中者，不贅述。

3 討論與計畫成果自評

我們認為，TTS/5 在智慧卡上的功能相當優越，如下所述。同時，本計畫進行中發表的論文在質與量上都相當不錯，這當然是努力的成果，但自然也要感謝國科會對我的支援，以及一些好運氣的成份，總之，本計畫的研究方向值得繼續下去。特別是多變元的可證明安全性。

3.1 TTS/5 的性能

如要生成 key 的動作在卡上進行，需要使用具有 256 byte on-chip RAM 的 i8052，生成鑰匙和簽章的程式總共 3.1 kB，另須 2.7 kB EEPROM 記憶體位置，假設使用 8 kB EEPROM，則還剩 2.2 kB 做為系統用。公鑰無法一次生成，必須以 20 位元組 (byte) 為單位分成 434 次生成，以 120 或 240 bytes 一段一段由卡上送出，起始之後，建立鑰匙動作在 Intel 8052 AH 元件上約花四秒，此後共須 28 秒才能送出全部公鑰。若只討論簽章速度，則可見第9頁的表1:

此處各 μC 之性能對比茲解釋如下：有計算輔助器 (co-processor) 的智慧卡當然計算速度大幅度提升，成本(價錢)也大幅度上揚；同時，8051 系有一參數稱為“T數”，係代表常見指令使用幾個時脈，此值越小表示該 μC 越高檔，Intel 8051AH 或 8052AH 係極低檔者，為“12T”，表上所列 Winbond 牌元件為“4T”，同樣程式執行速度可快近三倍。Infineon SLE-66 元件為“3T”更好，Phillips 8051 元件則介乎其間為“6T”。由上可知，TTS/5 原型之實用速度較諸 SFLASH 更適合於低階智慧卡，希望能夠將其安全性更強化、證明後投入實用。

3.2 論文的質量評比

密碼與資訊安全專門期刊不多，整個領域處在日新月異的狀態下，多數新知均藉由研討會進行交換，密碼學與資訊安全的之研討會，特別是有口碑、有歷史

的重要研討會，LNCS 週刊照例都會為其出一本一大會專刊。而凡是論文將收入 LNCS 的論文集，Springer 都要求其每一篇必需經過三人以上專家審稿，並經由專家組成之議程委員會接受，再按照審議者的意見修整之後，始能刊出，故與一般數學期刊接受到刊登的過程除了不能向編輯抗告之外，並無二致。是故一般理論學門中重期刊而輕研討會的傾向當不適用於此。

密碼學的競爭最近變得白熱化，國際密碼學研究學會 (International Association for Cryptologic Research, IACR) 主辦的三大會 (亞密 Asiacrypt、歐密 Eurocrypt、美密 Crypto) 和三大研討會 (FSE, PKC, CHES) 被稱為密碼學的『主流大會』；但是不論是 IACR 的六個會議，或是有口碑的其他地區性、主題性的國際性研討會，只要是有 LNCS 論文集的會議，目前錄取率都在下降中。僅以我倖獲錄取的研討會為例 (請見第 10 頁表2)，我們可以看到錄取率的減少極為明顯。在計畫期間內，我一共投稿密碼學會議 14 次，九次失敗，五次成功 (MEGA 2005 係數學方面的研討會，茲不列入)，不論是以目前的密碼學會議的錄取率，和台灣其他密碼資安領域的研究者比較，或單就投入在這個領域的歷史來說，都要算是極高的了。

當然，這樣好運很難維持，但我仍在努力，期望以後即使沒有運氣幫忙，也能達成同等級或是更高的成就。

References

- [1] G. Ars, J.-C. Faugère, M. Sugita, M. Kawazoe, & H. Imai, *Comparison of XL and Gröbner Bases Algorithms over Finite Fields*. Asiacrypt 2004, LNCS v. 3329, p. 323-337.
- [2] M. Bardet, J.-C. Faugère, B. Salvy, & B.-Y. Yang, *Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems*, presentation at MEGA 2005 and a chapter of Ph.D. thesis by M. Bardet, 2004.

- [3] N. Courtois, *Generic Attacks and the Security of Quartz*, PKC 2003, LNCS v. 2567, p. 351–364. Also see E-Print Archive 2004/143.
- [4] N. Courtois, *Algebraic Attacks over $GF(2^k)$, Cryptanalysis of HFE Challenge 2 and SFLASH^{v2}*, PKC 2004, LNCS v. 2947, pp. 201–217.
- [5] N. Courtois, M. Daum, & P. Felke, *On the Security of HFE, HFE_v, and Quartz*, PKC 2003, LNCS v. 2567, p. 337–350.
- [6] N. Courtois, A. Klimov, J. Patarin, & A. Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, Eurocrypt 2000, LNCS v. 1807, p. 392–407.
- [7] N. Courtois & J. Pieprzyk, *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*, Asiacrypt 2002, LNCS v. 2501, pp. 267–287.
- [8] N. Courtois & J. Patarin, *About the XL Algorithm over $GF(2)$* , CT-RSA 2003, LNCS v. 2612, pp. 141–157.
- [9] J. Daemen & V. Rijmen, *The Design of Rijndael, AES - The Advanced Encryption Standard*. Springer-Verlag, 2002.
- [10] C. Diem, *The XL-algorithm and a conjecture from commutative algebra*, Asiacrypt 2004, LNCS v. 3329, pp. 338–353.
- [11] W. Diffie & M. Hellman, *New Directions in Cryptography*, IEEE Transactions in Information Theory, vol. IT-22, no. 6, pp. 644–654.
- [12] J. Ding and J. Gower. *Inoculating Multivariate Schemes Against Differential Attacks*, private communication and manuscript, E-Print Archive, 2005/255.
- [13] J. Ding and D. Schmidt, *Rainbow, a new Digital Multivariate Signature Scheme*, ACNS 2005, LNCS v. 3531, p. 164–175.
- [14] J.-C. Faugère, *A New Efficient Algorithm for Computing Gröbner Bases (F4)*, Journal of Pure and Applied Algebra, 139 (1999), p. 61–88.
- [15] J.-C. Faugère, *A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5)*, Proc. ISSAC, ACM Press, 2002.
- [16] J.-C. Faugère & A. Joux, *Algebraic Cryptanalysis of Hidden Field Equations (HFE) Cryptosystems Using Gröbner Bases*, Crypto 2003, LNCS v. 2729, p. 44–60.
- [17] L. Goubin and N. Courtois, *Cryptanalysis of the TTM Cryptosystem*, Asiacrypt'00, LNCS v. 1976, pp. 44–57.
- [18] Y.-H. Hu, F. Lai, L.-C. Wang, & B.-Y. Yang, *A “Medium-Field” Multivariate Public-Key Encryption Scheme*, to appear at CT-RSA'06, (Feb. 13–17, '06, San Jose CA) and LNCS v. .
- [19] A. Joux, S. Kunz-Jacques, F. Muller, P.-M. Ricordel, *Cryptanalysis of the Tractable Rational Map Cryptosystem*, PKC'05, LNCS v. 3386, pp. 258–274.
- [20] A. Kipnis & A. Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization*, Crypto'99, LNCS v. 1666, pp. 19–30.
- [21] D. Lazard, *Gröbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations*, EUROCAL '83, LNCS v. 162, pp. 146–156.
- [22] MAGMA project, University of Sydney, magma.maths.usyd.edu.au/users/allan/gb.
- [23] T. Matsumoto & H. Imai, *Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption*, Eurocrypt'88, LNCS v. 330, pp. 419–453.
- [24] NESSIE project, www.cryptoneessie.org
- [25] J. Patarin, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*, Eurocrypt 1996, LNCS v. 1070, p. 33–48.
- [26] J. Patarin, L. Goubin, & N. Courtois, *C_{-+}^* and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai*, Asiacrypt 1998, LNCS v. 1514, p. 35–49.

- [27] J. Patarin, N. Courtois, & L. Goubin, *QUARTZ, 128-Bit Long Digital Signatures*, CT-RSA 2001, LNCS v. 2020, p. 282–297. Update at [24].
- [28] J. Patarin, N. Courtois, & L. Goubin, *FLASH, a Fast Multivariate Signature Algorithm*, CT-RSA 2001, LNCS v. 2020, p. 298–307. Update at [24].
- [29] B. Schneier & N. Ferguson, *Practical Cryptography*, published John Wiley and Sons, Inc., New York, 2003.
- [30] P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, Proc. 35th Ann. Symp. on Foundations of Comp. Sci., IEEE Comp. Soc. Press (1994), pp. 124–134.
- [31] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd ed. Prentice Hall, 1998.
- [32] G. Szegő, *Orthogonal Polynomials, 4th ed.*, Amer. Math. Soc., Providence.
- [33] L. Wang, *Tractable Rational Map Cryptosystem*, see ePrint 2004/046.
- [34] L.-C. Wang, Y.-H. Hu, F.-P. Lai, C.-Y. Chou, & B.-Y. Yang, *Tractable Rational Map Signature*, PKC 2005, LNCS v. 3386, p. 244–257.
- [35] C. Wolf, *Efficient Public Key Generation for Multivariate Cryptosystems*, Int'l Workshop on Cryptographic Algorithms and their Uses 2004, pp. 78–93, also ePrint 2003/089.
- [36] C. Wolf and B. Preneel, *Taxonomy of Public-Key Schemes based on the Problem of Multivariate Quadratic Equations*, ePrint 2005/077.
- [37] B.-Y. Yang & J.-M. Chen, *Theoretical Analysis of XL over Small Fields*, ACISP 2004, LNCS v. 3108, pp. 277–288.
- [38] B.-Y. Yang & J.-M. Chen, *All in the XL Family: Theory and Practice*, ICISC 2004, LNCS v. 3506, p. 67–86.
- [39] B.-Y. Yang & J.-M. Chen, *Building Secure Tame-Like Multivariate Public-Key Cryptosystems: the New TTS*, ACISP 2005, LNCS v. 3574, p. 518–531. Older version at E-Print Archive 2004/061.
- [40] B.-Y. Yang, J.-M. Chen, & Y.-H. Chen, *TTS: High-Speed Signatures from Low-End Smartcards.*, CHES 2004, LNCS v. 3156, p. 371–385.
- [41] B.-Y. Yang, J.-M. Chen, & N. Courtois, *On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis*, ICICS 2004, LNCS v. 3269, p. 401–413.

Scheme	Platform (T number)	Clock	PrKey	Code	RAM	T_{sign}
TTS (20, 28)	Intel 8032AH (12)	3.57 MHz	1.4 kB	1.4 kB	256 B	144 ms
	Intel 8051AH (12)					170 ms
Winbond W77E58(4)	1.6 kB			128 B	64 ms	
					85 ms	
TTS (24, 32)					227 ms	
ESIGN	Intel 8051AH (12)		336 B	3.0 kB	800 B	12.0 s
SFLASH ^{v2}			2.4 kB	3.3 kB	344 B	1.07 s
RSA-PSS (1024 bits)	Infineon SLE66 (2)	10 MHz				59 ms
	NEC μ PD789828*(12)	40 MHz	320 B	N/A	≥ 1 kB	many s
RSA-2048	Infineon SLE66*(2)	5 MHz	640 B			100 ms
		10 MHz	21 B			230 ms
			24 B			1.1 s
ECDSA-163						159 ms
ECDSA-191						180 ms
NTRU-Sign	Philips 8051 (6)	16 MHz	100 B	5 kB	800 B	160 ms

Table 1: 8051 上各種簽章系統的實作資料

會議	年份→	'98	'99	'00	'01	'02	'03	'04	'05
PKC (年初)	投稿篇數	30	61	–	67	69	105	106	128
	接受篇數	15	25	–	30	26	26	32	32
	接受率%	50	41	–	45	38	25	31	25
ACISP (七月)	投稿篇數	66	53	81	91	94	158	195	185
	接受篇數	35	26	37	38	36	42	41	45
	接受率%	53	49	46	42	38	26	21	24
CHES (夏末)	投稿篇數	–	42	51	66	101	111	125	–
	接受篇數	–	27	25	31	39	32	32	–
	接受率%	–	64	49	45	39	29	26	–
ICICS (10月)	投稿篇數	–	87	62	134	161	176	248	–
	接受篇數	–	37	24	58	41	37	42	–
	接受率%	–	43	39	43	25	21	17	–
ICISC (12月)	投稿篇數	53	61	56	107	142	163	190	–
	接受篇數	18	20	20	32	35	34	34	–
	接受率%	34	33	36	30	25	21	18	–

Table 2: 最近一些國際密碼與資訊安全研討會的錄取率

Scheme	Signature	PublKey	SecrKey	Setup	Signing	Verifying
RSA-PSS	1024 bits	128 B	320 B	2.7 sec	84 ms	2.0 ms
ECDSA	326 bits	48 B	24 B	1.6 ms	1.9 ms	5.1 ms
ESIGN	1152 bits	145 B	96 B	0.21 sec	1.2 ms	0.74 ms
QUARTZ	128 bits	71.0 kB	3.9 kB	3.1 sec	11 sec	0.24 ms
SFLASH ^{v2}	259 bits	15.4 kB	2.4 kB	1.5 sec	2.8 ms	0.39 ms
TTS(20,28)	224 bits	8.6 kB	1.3 kB	1.5 ms	51 μ s	0.11 ms
TTS(24,32)	256 bits	13.4 kB	1.8 kB	2.5 ms	67 μ s	0.18 ms

Table 3: TTS 和NESSIE 計畫簽章系統決選者在 500MHz Pentium III 的比較