行政院國家科學委員會專題研究計畫成果報告

計算的組合學: Computational Combinatorics

計畫編號: NSC - 90 - 2115 - M - 032 - 006
執行期限: 2001 年 8 月 1 日至 2002 年 7 月 31 日

計畫主持人: 楊柏因　　淡江大學數學系

1　中文摘要

吾等應用計算機實驗於有限體結構上, 獲得對溫良變換方法 (TTM, Tame Transformation Method) 密碼系統的種種改進使其在不損及其安全性下能更快速, 更易於實際應用。並拓展其結果爲堪稱快速、安全、易彈性應用之數位簽章系統 TTS, 與安全可靠、有彈性的雜湊函數 TTH。其結果部份發表於去年在台灣, 由中華民國資訊安全協會主辦的亞太區公鑰密碼系統與下層結構研討會 (IWAP 2002), 部份正整理投稿到本年度美國密碼學大會 (Crypto 2003) 等會議與刊物。

關鍵字: 有限體, 多變量公鑰密碼系統, 數位簽章, 溫良變換方法, 溫良變換簽章

Abstract

Applying the power of computers in simulation and searching on the multivariate public-key cryptosystem TTM (Tame Transformation Method) and succeeded in enhancing its performance and security; we also extended an originally asymmetric scheme to digital signatures and proposed digital signatures scheme (Tame Transformation Signatures) TTS that combines high security (cryptanalytical complexity) and high performance. Some of the results were published in IWAP (International Workshop on Asian-Pacific Public-Key Infrastructure) 2002, held in Taiwan; another paper has been submitted to Crypto 2003; others are being prepared for publication.

Keywords: TTM, TTS, digital signature scheme, public key cryptosystem, finite field, hash function

2　緣由與目的

前幾年參與整合型計畫的工作時, 我們曾發表過這樣的看法, 認爲:

> **計算機可以幫助組合學家獲得很多新的方向與內涵; 根據 Moore's Law 日新又新的電腦技術, 使得我們有更多的東西可以模擬演練, 高度的平行化處理更是很多原本僅爲純理論性的技術現在可以有效的應用在實際上。**

根據幾年所獲得的經驗, 我們應用計算機實驗於種種離散數學的架構上。其間, 我們感到最有成效的部份係最近對溫良變換密碼系統 (Tame Transformation Method, TTM) 的研究上。根據代數幾何來的 TTM 系統係國人莫宗堅教授之創見([?]), 爲一種快速的多變量公鑰密碼系統 (Multivariate Public Key Cryptosystem) 吾等研究希望根據計算機實驗與搜尋獲得一種在密碼安全性複雜度 (cryptanalytical complexity) 與實際安裝使用 (implementational performance) 上均堪稱較爲優越的變形, 並發展出一種變式, 可以用爲數位簽章 (Digital Signature) 與一種安全的雜湊函數 (cryptographically secure hash function); 準此, 我們做了種種設計和一系列測試。

3　結果 (分兩大類敘述)

計算機科學上的主要結果是關於 TTM 系列的密碼系統。我們完成了研究目標, 發展出一種快速、安全的數位簽章稱之爲溫良變換簽章 (TTS, Tame Transformation Signatures), 與副產品, 高複雜度的雜湊函數 TTH (Topsy-Turvy Hash, 顛倒錯亂的雜湊函數), 另有其他零散的結果。

3.1 所謂溫良自同構: 介紹

所謂溫良自同構 (Tame Automorphism) 又稱溫良變換 (Tame Transformation) $\phi : \mathbf{x}(\in K^n) \mapsto \mathbf{y}(\in K^n)$ 形式如下, 式中, K 爲有限體, 諸 q 皆爲多項函數:

$$\begin{aligned}
y_1 &= x_1; \\
y_2 &= x_2 + q_2(x_1); \\
y_3 &= x_3 + q_3(x_1, x_2); \\
&\vdots \quad \vdots \quad\quad \vdots \\
y_i &= x_i + q_i(x_1, x_2, \ldots, x_{i-1}); \\
&\vdots \quad \vdots \quad\quad \vdots \\
y_n &= x_n + q_n(x_1, x_2, \ldots, x_{n-1});
\end{aligned}$$

此映射有下列的兩個性質:

1. 由 $\mathbf{y}$ 可以迅速的計算出 $\mathbf{x}$;
2. $\mathbf{x}$ 不易表爲 $\mathbf{y}$的明式多項式函數。因爲隨著迭次代入, 多項式的次數會迅速增加:

$$\begin{aligned}
x_1 &= y_1; \\
x_2 &= y_2 - q_2(x_1); \\
x_3 &= y_3 - q_3(x_1, x_2); \\
&= y_3 - q_3(y_1, y_2 - q_2(y_1)); \\
x_4 &= y_4 - q_4(x_1, x_2, x_3) \\
&= y_4 - q_4(y_1, y_2 - q_2(y_1), \\
&\qquad y_3 - q_3(y_1, y_2 - q_2(y_1))); \\
&\vdots \quad \vdots \quad\quad \vdots \\
x_n &= y_n - q_n(x_1, x_2, \ldots, x_{n-1}); \\
&= y_n - q_n(y_1, y_2 - q_2(y_1), \ldots \\
&\qquad y_{n-1} - q_{n-1}(\cdots)).
\end{aligned}$$

根據莫宗堅 (T. Moh) 的研究, 我們可以這樣的延伸溫良變換到一個 $K^n \to K^{n+k}$ 的映射 T_1: 先作 K^n 的標準嵌入到 K^{n+k}, 再做 K^{n+k} 的溫良變換, 等於在溫良變換後面加上若干條形如

$$\begin{aligned}
y_{n+1} &= q_{n+1}(x_1, x_2, \ldots, x_n); \\
y_{n+2} &= q_{n+2}(x_1, x_2, \ldots, x_n); \\
&\vdots \quad \vdots \quad\quad \vdots \\
y_{n+k} &= q_{n+k}(x_1, x_2, \ldots, x_n).
\end{aligned}$$

的式子, 當這樣的二次變換和另一個較高次的溫良變換 T_2 合成, 我們可讓它形如 $y_j = q_j(x_1, x_2, \ldots, x_n)$, $1 \le j \le n+k$. 而應用 K 爲有限體的條件讓各 q_j 皆爲二次, 在 T_1T_2 前後各加上一個可逆的線性映射成 $f = L_1T_1T_2L_2$, 就得到 f 爲嵌射, 已知各參數的值時可以迅速計算其反影, 但'無法' (即複雜度極高) 在只看到其二次多項式的形式時分解其爲原來的四個成份。此法[1] 滿足公鑰密碼系統 (Public Key Cryptosystem) 之要件, 而稱爲 TTM 系統, 或溫良變換方法密碼系統。

3.2 TTM 的改良

我們在這段時間內靠著模擬實驗和研究成功完成了對 TTM 的改進, 今天的 TTM 版本爲 $\mathrm{GF}(2^8)^{32} \to \mathrm{GF}(2^8)^{60}$, 而非原先的 $\mathrm{GF}(2^8)^{48} \to \mathrm{GF}(2^8)^{100}$, 加解密的速度爲原來的五到十倍, 如果在具有向量運算能力的電腦上, 如 Apple 的 PowerMac G4 之 AltiVec 向量技術, 其加密能力已達到每秒 15 Mb/s, 可做到即時加密傳輸再解密的程度 ([?]), 而非如以 RSA 爲基礎的傳統式公鑰傳輸, 需要用及所謂當次加密鑰匙 (session key) 的傳送。其主要弱點爲傳輸時膨漲率大, 不適合做軍用等於低頻寬的介質的傳輸。目前速度上的進展可見國人胡裕華等的研究報告([?])。

3.3 快速、安全的數位簽章 TTS

目前一般認爲安全的簽章需要有 160 位元即 20 個 byte, 每個byte 以一個 $K = \mathrm{GF}(2^8)$ 的元素代表, 則我們可以利用一個溫良變換和兩個線性變換合成爲驗證函數 $f = \phi_1 \circ \phi_2 \circ \phi_3$, 式中$\phi_1$ 與 ϕ_3 分別在 $\mathrm{GF}(2^8)^{28}$ 和 $\mathrm{GF}(2^8)^{20}$ 可逆線性, 而溫良變換 ϕ_2 把

$$\mathbf{x} = (x_0, \ldots, x_{27}) \in \mathrm{GF}(2^8)^{28}$$

送到

$$\mathbf{y} = (y_8, \ldots, y_{27}) \in \mathrm{GF}(2^8)^{20}:$$

[1] 爲 T. Moh 在 1997 年提出並申請專利在案。

$$
\begin{aligned}
y_8 &= x_8 + a_8x_0x_7 + b_8x_1x_6 \\
&\quad + c_8x_2x_5 + d_8x_3x_4 + e_8x_4^2; \\
&\vdots \quad \vdots \quad \vdots \\
y_k &= x_k + a_kx_{k-8}x_{k-1} + b_kx_{k-7}x_{k-2} \\
&+ c_kx_{k-6}x_{k-3} + d_kx_{k-5}x_{k-4} + e_kx_{k-4}^2; \\
&\vdots \quad \vdots \ \vdots \\
y_{20} &= x_{20} + a_{20}x_{12}x_{19} + b_{20}x_{13}x_{18} \\
&\quad + c_{20}x_{14}x_{17} + d_{20}x_{15}x_{16} + e_{20}x_{16}^2; \\
y_{21} &= x_{21} + a_{21}x_{13}x_0 + b_{21}x_{14}x_{19} \\
&\quad + c_{21}x_{15}x_{18} + d_{21}x_{16}x_{17} + e_{21}x_{17}^2; \\
y_{22} &= x_{22} + a_{22}x_{14}x_1 + b_{22}x_{15}x_0 \\
&\quad + c_{22}x_{16}x_{19} + d_{22}x_{17}x_{18} + e_{22}x_{18}^2; \\
y_{23} &= x_{23} + a_{23}x_{15}x_2 + b_{23}x_{16}x_1 \\
&\quad + c_{23}x_{17}x_0 + d_{23}x_{18}x_{19} + e_{23}x_{19}^2;
\end{aligned}
$$

函數 f 之反影 $f^{-1} = \phi_1^{-1} \circ \phi_2^{-1} \circ \phi_3^{-1}$, 在已知各 $a_i \cdots e_i$ 之後, 很容易分開三段做出, 即取亂數使 $x_0 \cdots x_7$ 爲 GF(2^8) 中均勻分布的隨機變數, 各 $y_0 = x_0, \ldots, y_7 = x_7$, 則 ϕ_2 爲溫良, ϕ_2^{-1} 不難求得也, 但要求得 f 分解爲該三段函數之合成非常麻煩, 計算上不可能, 故先公佈 f 於大眾之後, 任一信件 M 吾等可以用一個公開且安全的雜湊函數 (hash) 取得一個 GF$(2^8)^{20}$ 中的摘要段落 (message digest) $H(M)$, 再分三段取得 $S = f^{-1}(H(M)) \in$ GF$(2^8)^{28}$, 和 M 一起公佈, 此時任何人可以求出 $H(M)$ 並驗證 $f(S) = H(M)$, 以此爲原理的數位簽章, 稱之爲溫良變換簽章 (TTS), 計算速度遠勝現行的 RSA 簽章, 高於由法人 Courtois, Goubin, Patarin 提出的 SFLASH ([?]) 和 QUARTZ ([?]) 系統。TTS 有種種變式, 各有優缺點。速度上的進展可見 [?, ?] 與國人黃文俊等的研究報告([?])。

3.4 TTM/TTS 的安全性

自 Imai 和 Matsumoto ([?]) 與破解 I-M 系統的 Patarin ([?]) 以來, 目前多變量公鑰數位簽章系統之研究頗多, 標準的多變量數位簽章系統包含一個以上非線性映射夾在兩個線性映射之間, 此爲極普遍的架構, 近年公布的標準對稱加密系統 AES 亦採此設計 ([?, ?]), 而多變量二次聯立多項形式是一極受歡迎的課題, 故專文甚多。公鑰密碼學之開創者之一的 Shamir 亦對此多有發表。並提出針對 HFE 系統 ([?]) 的 relinearization 法, 此類方法和多項方程最常見的 Gröbner 基底法 ([?, ?]), 因代數幾何中的 Hilbert-Serre 理論對改良版 TTM 系 (含上述改良版 TTS) 無效 ([?, ?])。

即使解此等二次聯立多項方程組係 NP-hard ([?]) 法人 Courtois, Goubin, Patarin, 對此研究多年, 有專文([?, ?]) 討論硬解的可能性, 據其文中的公式可得其方法對 TTS/TTM 無效。

此外, Courtois, Goubin 更有一系列密碼的攻擊對 TTM 系均有設爲假想敵來考慮 ([?, ?, ?, ?, ?, ?, ?]), 尤其直指 TTM 系列不安全已被破解的 [?] 爲最, 莫宗堅在 [?] 說明其不正確。吾等記取其教訓而設計出目前, 現存各種解法都無效的 TTS 改良版本如上, 另有稍慢而更安全改良版本, 詳見 [?]。**目前 TTS 的安全性複雜度約 2^{130}。**

3.4.1 TTH

安全性複雜度約 2^{130} 的雜湊函數 TTH (Topsy-Turvy Hash, 顛倒錯亂的雜湊函數) 來自用 π 的十六進位展開做爲係數的二次多項式, 仿 DES 的方式用 Block Chaining Mode 造成 (詳 [?])。

3.5 其他

我們對其他的學科作了一些計算性工作, 結果尚在整理中。我們已經有所研究的 Wiener Polynomial (即圖形中頂點間距離的生成函數) 發現了一些非遞迴性的公式計算化學上有意義的圖, 包括七角鍊的 Wiener Number ([?]) 和一些其它。

目前我們最有興趣的計算性工作是一些組合設計和生成的問題, 事實上是上述 TTM/TTS 系統其係數與項的選取有安全性和可計算性的種種限制!

這些牽涉到線性代數和圖論且有其它應用, 結果整理中, 一個有趣的應用是, TTM/TTS 的變數個數應盡量避免爲六的倍數, 但方程數無妨, 故目前的 TTM 版本由 $36 \to 64$ 更爲 $32 \to 60$。

4 討論與計畫成果自評

我們最近的努力方向在使用組合學的概念於計算機領域, 但引入代數與分析學的技巧，希望藉由改換觀點來尋找一些問題的新處方 (prescription)。

簽章系統係很困難的課題, 除前述被破解的 I-M 系統外尚有 HFE 系統(被 [?, ?] 破解), 油醋系統 (被 [?] 破解, 有種種改版如 [?]) 等等, 由 Patarin 等人設計的 FLASH, QUARTZ 均在歐洲標準 (NESSIE, [?, ?]) 之候選之列, 其速度不如TTS, 而 QUARTZ 最慢, 而 FLASH 其安全性正受嚴苛考驗中, 目前經過三次改板, 到目前仍不被認爲安全 ([?, ?, ?, ?, ?]) TTS 在各方面均較其爲優。我們相信不論是理論或是實用性上來說，我們的結果都將相當有用。

我們亦棄 AES 系統等所用的 $GF(2^8)$ 乘法設計, 而選取組合上更優良的一種 $GF(2^8)$ 乘法, 可充分發揮子有限體的功能, 對於 smart card 可預見有相當應用。

5 參考文獻

References

[1] `http://csrc.nist.gov/encryption/aes` the AES homepage.

[2] M. Akkar, N. Courtois, R. Duteuil, and L. Goubin, *A Fast and Secure Implementation of SFLASH*, PKC 2003, LNCS V. 2567, pp. 267–278.

[3] J.-M. Chen and B.-Y. Yang, *On The Security and Efficiency of TTS Signature Scheme*, submitted.

[4] J.-M. Chen, B.-Y. Yang, B.-Y. Peng, *Tame Transformation Signatures with Topsy-Turvy Hashes*, pp. 313-320 Proc. IWAP 2002, but unabridged version at `http://www.usdsi.com/TTS.pdf`

[5] N. Courtois, *The Security of Hidden Field Equations (HFE)*, CT-RSA 2001, LNCS V. 2020, pp. 266–281.

[6] N. Courtois, *Generic Attacks and the Security of Quartz*, PKC 2003, LNCS V. 2567, pp. 351–364.

[7] N. Courtois, M. Daum, and P. Felke, *On the Security of HFE, HFEv-, and Quartz*, PKC 2003, LNCS V. 2567, pp. 337–350.

[8] N. Courtois, L. Goubin, W. Meier, and J. Tacier, *Solving Underdefined Systems of Multivariate Quadratic Equations*, PKC 2002, LNCS V. 2274, pp. 211–227.

[9] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, EUROCRYPT 2000, LNCS V. 1807, pp. 392–407.

[10] N. Courtois and J. Patarin, *About the XL Algorithm over GF(2)*, CT-RSA 2003.

[11] J. Faugère, *A New Efficient Algorithm for Computing Gröbner Bases (F4)*, Journal of Pure and Applied Algebra, 139 (1999), pp. 61–88.

[12] J. Faugère, *A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5)*, ACM Press, 2002.

[13] J. Faugère, private communication.

[14] M. Garey and D. Johnson, *Computers and Intractability, A Guide to the Theory of NP-completeness*, 1979, p. 251.

[15] W. Geiselmann, W. Meier, and R. Steinwandt, *An Attack on the Isomorphisms of Polynomials Problem with One Secret*, available at `http://eprint.iacr.org/2002/143`

[16] W. Geiselmann, R. Steinwandt, and T. Beth, *Attacking the Affine Parts of SFLASH*, 8th International IMA Conference on Cryptography and Coding, LNCS V. 2260, pp. 355–359.

[17] W. Geiselmann, R. Steinwandt, and T. Beth, *Revealing 441 Key Bits of* SFLASH^{v2}, Third NESSIE Workshop, 2002.

[18] H. Gilbert and M. Minier, *Cryptanalysis of SFLASH*, EUROCRYPT 2002, LNCS V. 2332, pp. 288–298.

[19] L. Goubin and N. Courtois, *Cryptanalysis of the TTM Cryptosystem*, ASIACRYPT 2000, LNCS V. 1976, pp. 44–57.

[20] Y. Hu, L. Wang, J. Chen, F. Lai, and C. Chou, *A Performance Report and Security Analysis of a fast TTM implementation*, preprint.

[21] W.-J. Huang, Y.-H. Hu, F. Lai, C.-Y. Chou, *A Performance Report of a Fast TTS Implementation*, pp. 157-162, Proc. IWAP 2002.

[22] "On Wiener numbers of Septagons", M.S. Thesis of C. Jiang under the direction of B.-Y. Yang, Tamkang University.

[23] A. Kipnis, J. Patarin, and L. Goubin, *Unbalanced Oil and Vinegar Signature Schemes*, CRYPTO'99, LNCS V. 1592, pp. 206–222.

[24] A. Kipnis and A. Shamir, *Cryptanalysis of the Oil and Vinegar Signature Scheme*, CRYPTO'98, LNCS V. 1462, pp. 257–266.

[25] A. Kipnis and A. Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization*, CRYPTO'99, LNCS V. 1666, pp. 19–30.

[26] B. Lucier, *Cryptography, Finite Fields, and AltiVec*, `http://www.simdtech.org/apps/group_public/download.php/22/Cryptography.pdf`

[27] T. Matsumoto and H. Imai, *Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption*, EUROCRYPT'88, LNCS V. 330, pp. 419–453.

[28] T. Moh, *A Public Key System with Signature and Master Key Functions*, Communications in Algebra, 27 (1999), pp. 2207–2222.

[29] T. Moh, *On The Method of XL and Its Inefficiency Against TTM*, available at `http://eprint.iacr.org/2001/047`

[30] T. Moh and J.-M. Chen, *On the Goubin-Courtois Attack on TTM*, available at `http://eprint.iacr.org/2001/072`

[31] *NESSIE Security Report, V1.0*, available at `http://www.cryptonessie.org`

[32] *Performance of Optimized Implementations of the NESSIE Primitives, V1.0*, available at `http://www.cryptonessie.org`

[33] J. Patarin, *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88*, CRYPTO'95, LNCS V. 963, pp. 248–261.

[34] J. Patarin, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*, EUROCRYPT'96, LNCS V. 1070, pp. 33–48.

[35] J. Patarin and L. Goubin, *Trapdoor One-Way Permutations and Multivariate Polynomials*, ICICS'97, LNCS V. 1334, pp. 356–368.

[36] J. Patarin, L. Goubin, and N. Courtois, *Improved Algorithms for Isomorphism of Polynomials*, EUROCRYPT'98, LNCS V. 1403, pp. 184–200.

[37] J. Patarin, L. Goubin, and N. Courtois, *C^*_{-+} and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai*, ASIACRYPT'98, LNCS V. 1514, pp. 35–49.

[38] J. Patarin, N. Courtois, and L. Goubin, *QUARTZ, 128-Bit Long Digital Signatures*, CT-RSA 2001, LNCS V. 2020, pp. 282–297. Updated version available at `http://www.cryptonessie.org`

[39] J. Patarin, N. Courtois, and L. Goubin, *FLASH, a Fast Multivariate Signature Algorithm*, CT-RSA 2001, LNCS V. 2020, pp. 298–307. Updated version available at `http://www.cryptonessie.org`

[40] Joan Daemen and Vincent Rijmen, *The Design of Rijndael, AES - The Advanced Encryption Standard.* Springer-Verlag, 2002.

[41] R. Steinwandt, W. Geiselmann, and T. Beth, *A Theoretical DPA-Based Cryptanalysis of the NESSIE Candidates FLASH and SFLASH*, ISC 2001, LNCS V. 2200, pp. 280–293.