行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　　　　　　※
※　　**橢圓曲線加密與簽章及串流加密之分析與製作**　　※
※　　　　　　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：¦個別型計畫　　æ整合型計畫

計畫編號：NSC89－2213－E－009－155－

執行期間：89 年 08 月 01 日至 90 年 07 月 31 日

計畫主持人：陳榮傑

共同主持人：

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

執行單位：國立交通大學資訊工程學系

中　華　民　國　90 年　10 月　30 日

行政院國家科學委員會專題研究計畫成果報告
橢圓曲線加密與簽章及串流加密之分析與製作
Analyses and Implementations on EC Encryption, EC Digital Signature and Stream Cipher Encryption

計畫編號：NSC 89-2213-E-009-155
執行期限：89 年 08 月 01 日至 90 年 07 月 31 日

主持人：陳榮傑　國立交通大學 資訊工程學系
計畫參與人員：張仁俊　國立交通大學 資訊工程學系
胡鈞祥　國立交通大學 資訊工程學系
吳緯凱　國立交通大學 資訊工程學系
王偉全　國立交通大學 資訊工程學系

一、中文摘要

虛擬私人網路(Virtual Private Network；VPN)可以提供企業用戶在公共的網際網路上架設專屬且安全的網路系統，節省企業租借專用線路的大筆經費，因而成為網路應用中的新貴。VPN 的核心技術包括通道工程(tunneling)、資料加密(encryption)、身份認證(authentication)以及存取控制(access control)等，尤其以資料加密為一切的基礎。目前加密的系統分為密鑰密碼系統和公鑰密碼系統，前者包括區塊密碼(Block cipher)和串流密碼(Stream cipher)，區塊密碼常見的包括 DES、IDEA、RC4 等，串流密碼常用的為線性反饋移位暫存器(LFSR)；至於公鑰密碼系統常見的有 RSA、Diffie-Hellman、ElGamal 等技術。

過去的公鑰密碼系統大都基於 n 模餘群(modulo n)上的兩大難題：大數分解與離散對數問題；前者以 RSA 密碼系統為代表，後者則包括 ElGamal 密碼系統、Diffie-Hellman 金鑰交換以及 DSA 數位簽章系統。1985 年 Neil Koblitz 和 Victor Miller 觀察到橢圓曲線中存在另一個難題--橢圓曲線離散對數問題，並提出將其運用在公鑰密碼系統上的可能性。橢圓曲線密碼系統的優點在於它提供與 RSA 及其他公鑰密碼系統相同的安全性，且使用的公鑰長度較短(160 位元的 ECC 大約與 1024 位元的 RSA 具有相同的安全性)；因此不論在公鑰儲存的能力、傳輸所佔的頻寬以及加密資料或數位簽章的長度等方面，橢圓曲線密碼系統都佔有較大的優勢。至於運算速度方面，由於 ECC 所用的公鑰相對的較短，透過軟體和硬體的實作，採用橢圓曲線系統的算術運算會比 modulo 算術運算來的簡單。由於橢圓曲線密碼系統具有密鑰長度短、安全性佳、容易用硬體製作、運算速度快、可同時運用在加密及簽章技術等優點，而成為現代密碼學研究的重點。

以線性反饋移位暫存器為基礎的串流密碼系統是目前串流密碼的主流，其特性為結構簡單、加密速度快，並且已有理想的數學工具如頻譜理論和代數理論來做安全性的分析。線性複雜度為最初串流密碼系統強度的重要指標。之後，相關攻擊與最佳仿射逼近攻擊的提出，產生如相關免疫函數與 Bent 函數等指標的研究。接著重量複雜度、球體複雜度、變複雜度距離、定複雜度距離、球面週期、球體週期函數穩定性和信源碼穩定性指標的引入，建立了串流密碼穩定性的新理論，使得串流密碼系統強度問題研究得到了重大的突破。這一新領域的探討將對公鑰密碼系統和傳統分組密碼穩定性的研究起到積極的推動作用。目前網路安全之應用常需要快速加密，串流密碼具有此特性，於是設計安全性高的串流加密系統將是一個重要的課題。

本計畫將針對橢圓曲線的理論基礎，配合現行存在的公鑰密碼系統及各種攻擊方式，製作橢圓曲線加密和簽章系統，將其架構在 VPN 的通訊協定上。另外，針對帶 memory 與不帶 memory 的串流加密技術，發展出一套安全性高的串流密碼系統，專門處理 VPN 中即時資料的加解密。

關鍵詞：橢圓曲線、橢圓曲線密碼系統、串流密碼

Abstract

Virtual Private Network (VPN) provides a company with a secure communication channel over the public Internet with lower cost than leased-line networks. The kernel technologies of VPN include tunneling, encryption, authentication, and access control. All of them are based on the cryptographic system. Cryptosystems are generally classified into secret-key systems and public-key systems depending on if encryption key and decryption key are identical. Secret-key cryptosystems can further divided into block cipher (such as DES, IDEA, RC4 etc.) and stream cipher (LFSR, for example). Public-key cryptosystems contain several systems such as RSA, ElGamal encryption, Diffie-Hellman key exchange and DSA etc.

Over the years, most proposed public-key cryptosystem are classified according to the

mathematical problems they are based on as the Integer Factorization (RSA is the best known example) or the Discrete Logarithm (such as ElGamal encryption, Diffie-Hellman key exchange and DSA). In 1985, Neil Koblitz and Victor Miller proposed the Elliptic Curve Cryptosystem (ECC) whose security relies on the discrete logarithm over the points on an elliptic curve. ECC can be used to provide both an encryption scheme and a digital signature scheme. It provides security equivalent to existing public-key systems, such as RSA, but with shorter key lengths. Shorter key length means smaller bandwidth and storage are required while data is transmitted on the Internet and can be a crucial superiority over other public-key systems. Moreover, the most efficient implementations of ECC are faster than comparable RSA systems in terms of relative security (160 bits ECC vs. 1024 bits RSA). Because of the above advantages, ECC has been the subject of intensive research in cryptography.

LFSR (Linear Feedback Shift Register)-based stream cipher systems are the most important ones which feature simple structures and high-speed encryption. Besides, there have been some ideal mathematical tools, such as spectrum theory and algebraic theory, to do the security analysis for stream cipher. Linear complexity is an important indicator for the security level of the original stream cipher. The proposals of correlation attack and best affine approximation attack have invoked several studies, such as correlation immune function and Bent function. Moreover, the introduction of weight complexity, fixed-complexity distance and variable-complexity distance etc. establishes a new theory on stream cipher stability, which results in a significant development on the security level issues. Currently, to meet the need of high-speed encryption on the network, designing a stream cipher system with high security level will be an important task.

We start by studying the mathematical basis of elliptic curve cryptography to identify suitable elliptic curves for ECC. We then survey all proposed public-key systems and attack methods in order to design an efficient elliptic curve encryption scheme and a digital signature scheme. By applying theoretical proof and practice attacks, we will analyze the security of our schemes and implement them on VPN. In addition, we will develop a highly secure stream cipher based on LFSR with/without memory to deal with the encryption of real time data on VPN.

Keywords: Elliptic Curve, Elliptic Curve Cryptosystem, Stream Cipher

二、緣由與目的

過去的公鑰密碼系統大都基於 n 模餘群(modulo n)上的兩大難題：大數分解(Integer Factorization)與離散對數問題(Discrete Logarithm Problem，DLP)；前者以 RSA 密碼系統為代表，後者則包括 ElGamal 密碼系統、Diffie-Hellman 金鑰交換以及 DSA 數位簽章系統。1985 年 Neil Koblitz 和 Victor Miller 觀察到橢圓曲線中存在另一個難題--橢圓曲線離散對數問題(Elliptic-curve Discrete Logarithm Problem，ECDLP)，並提出將其運用在公鑰密碼系統上的可能性。

橢圓曲線在代數及幾何學上已被廣泛的研究長達 150 年之久，並有豐富且深奧的理論基礎。在橢圓曲線中，橢圓曲線群(Elliptic-curve Group)是一個集合，集合內的元素是滿足橢圓曲線方程式的數對(x, y)，其中 x 和 y 可以屬於 R 實數系或是 Z_p(p 是質數)或 GF(2^m)的有限體(finite field)等不同數系，群內並有自行定義的群加法運算。其中基於 R 的橢圓曲線提供了直覺簡單的群加法運算的概念，而基於 Z_p 或 GF(2^m)的橢圓曲線則由於具有橢圓曲線離散對數問題的特性，適合用來設計不同的密碼系統。

在橢圓曲線群中點(元素)的個數決定了有限群的大小，也和設計出來的橢圓曲線密碼系統的安全度有關，Hasse 定理證明，如果在 $E_{a,b}(Z_p)$ 上共有#E 個點，則#E 介於 $p+1-2\sqrt{p}$ 與 $p+1+2\sqrt{p}$ 之間，Schoof 也提出一個需要多項式時間的演算法來計算#E。除了元素個數的計算之外，關於橢圓曲線方程式及產生子的選擇也是一個重要的課題，目前來說，我們把數系定在 Z_p 或是 GF(2^m)上，然而即便是在同一個數系下，也有很多的方程式可供選擇，Miyaji 討論一些基於不同數系下，適合用來設計密碼系統的橢圓曲線。Menezes 更證明滿足某些條件的橢圓曲線(稱為 supersingular elliptic curve)內的橢圓離散對數問題能 reduce 到有限體上的離散對數問題，而會遭受到一些次指數(subexponential)演算法如 Index calculus method 的攻擊，表示如果我們希望設計出來的密碼系統更安全的話，應該要避免選到 supersingular 橢圓曲線，除此之外，也有另外一類稱為 Anomalous 橢圓曲線也由 Smart 證明這類的 ECDLP 很容易解。Koblitz 後來又提出架構在 Hyperelliptic curve 上的密碼方法，這些都是和橢圓曲線密碼系統有關的理論研究。

在實際設計橢圓曲線密碼演算法方面，有多篇論文針對橢圓曲線群設計資料加密方法和數位簽章技術，這些方法大都是修改原有的系統如 RSA、ElGamal、DSA 和 Diffie-Hellman 等，把原來在 n 模餘群(modulo n)上的乘法和指數運算改變為相對在橢圓曲線群上的加法和乘法的運算，以達到較短的金鑰長度，仍然有相同的安全度。至於這些密碼系統的安全性分析，則大多沿用目前一些有效率的攻擊法來做安全上的評估。另外在運算速度方面，由於基於 GF(2^m)的橢圓曲線具有元素為 m 位元二元字串的特性，因此可以透過軟體或硬體的方式，加速加解密的動作。在橢圓曲線密碼系統中，不同數系的選擇會影響到橢圓曲線群內元素的個數、計算速率和相對應離散對數問題的困難度；當橢圓曲線群運用在密碼系統上時，不同的數系則會影響到公鑰的大小、計算元件以及保密性。這種設計上的多元性，使得橢圓曲線更適合來製作公鑰密

碼系統。

本計畫首先針對有關橢圓曲線密碼系統的理論基礎，包括橢圓曲線的分類，如何驗證選擇的橢圓曲線適合用來架構密碼系統以及產生子的選取等課題，蒐集整理最新的研究報告。另外為了使設計出來的加密方法有很高的安全性，我們有必要整理目前已知的各種攻擊法，瞭解其攻擊模式，進而設計出新的橢圓曲線加密方法。

另外我們會對橢圓曲線的理論基礎進行研究，包括 supersingular EC、anomalous EC 及 hyperelliptic curve 等不同種類橢圓曲線的特性以及其他用來判斷安全密碼系統橢圓曲線的指標，定義橢圓曲線選擇的演算法。並針對目前已經有的橢圓曲線加密方法加以改良，設計安全且有效率的加密演算法，接著用目前已知的攻擊法(如 Pohlig-Hellman 演算法、Index calculus 方法等)加以分析，以驗證加密方法的安全性。我們希望能利用硬體製作技術的改良，加快橢圓曲線加密的速度；另一方面，配合現有的通訊協定，將我們設計出來的演算法參數化，使其容易運用在不同的通訊協定上。

由於橢圓曲線運算速度方面，相較於一般的公鑰密碼系統，其運算方式要來的複雜。1988 年，Mullin、Onyszchuk、Vanstone 與 Wilson1 提出以正規基底（normal basis）取代原先多項式基底（polynomial basis）的運算模式，進而加快了橢圓曲線平方運算的速度，此種方法我們簡稱為 NB 方法；若基於某個正規基底下，NB 方法所需的計算量最少，則我們給予此方法另一個名稱：最佳 NB 方法（optimal normal basis）。之後 Bailey 與 Paar 於 1997 年提出了另一種加快橢圓曲線運算速度的方式，簡稱為 OEF 方法。OEF 方法是建立一個架構於最佳擴展體（optimal extension fiend）上的橢圓曲線密碼系統，並於多項式基底下進行運算，且可根據電腦暫存器所能提供之位元數大小進行多位元的同步運算，以增快橢圓曲線運算速度。有鑑於橢圓曲線運算速度在實際應用上的需求，我們計畫分析目前已有之加速運算演算法，透過實作分析，提供國內密碼學學術界有關橢圓曲線密碼系統實作上參數選擇的參考。

三、結果與討論

我們蒐集了目前為止有關橢圓曲線密碼系統的理論基礎及安全性分析，以及不同有限體系下的實作方式，整理完成橢圓曲線密碼系統的基礎理論與實作技巧[13]，提供給國內密碼學學術界參考。

在實作方面，如何加快有限體上的算術運算速度是一個重要的研究課題。目前提出來最有效率的方法有兩種，分別是基於正規基底下的運算模式以及架構於最佳擴展體下的運算模式。我們將兩種方法分別實作在不同的機器平台下，分析比較其執行效能，並整理歸納出不同的環境平台下選擇運算模式的標準以及最佳的參數[14]，對於實作橢圓曲線密碼系統有相當的貢獻。

據此，我們完成本計畫的目的，並在橢圓曲線密碼系統的領域上提供一個理論與實作並重的研究報告。

四、計畫成果自評

依上節所提之結果，我們達成了此計劃預期的目標。此計畫的研究結果除了為國內密碼學術界提供橢圓曲線密碼系統的基礎；另外透過實作分析的過程，針對不同的機器平台，發展不同有限體系上算術運算的基礎技術，除了應用在橢圓密碼系統相關的領域外，也可以運用在密碼學上其他密碼系統基本的算術運算(有限體上)。成果極具有學術上的價值與貢獻，相當適合學術期刊上發表。

五、參考文獻

[1] G. Agnew, R. Mullin, and S. Vanstone, “An implementation of elliptic curve cryptosystems over $F_{2^{155}}$,” *IEEE Journal on Selected Areas in Communications*, to appear.

[2] D. V. Bailey and C. Paar, “Optimal extension fields for fast arithmetic in public-key algorithms,” *Crypto’98*, pp. 472-285, 1998.

[3] A. Bender and G. Castafnoli, “On the implementation of elliptic curve cryptosystems,” *Advances in Cryptology - CRYPTO ’89*, Lecture Notes in Computer Science, 435, pp. 417-426, Springer-Verlag, 1990.

[4] G. Harper, A. Menezes and S. Vanstone, “Public-key cryptosystems with very small key lengths”, *Advances in Cryptology EURO -CRYPT ’92*, to appear.

[5] N. Koblitz, “Elliptic curve cryptosystem”, *Math. Comp.* 48, 1987.

[6] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1987.

[7] N. Koblitz, “Hyperelliptic cyrptosystems”, *Journal of Cryptology*, 1 (1989), 139-150.

[8] K. Koyama, U. Maurer, T. Okamoto and S. Vanstone, “New public-key schemes based on elliptic curves over the ring Zpq”, *IEEE Transactions on Information Theory*, to appear.

[9] K. Koyama and Y. Tsuruoka, “Speeding up elliptic cryptosystems using a signed binary window method”, *Advances in Cryptology - CRYPTO ’92*, to appear.

[10] A. J. Menezes, Elliptic Curve Public Key Cryptossytems, Kluwer Academic Publishers, 1993.

[11] A. Menezes, T.Okamoto and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field”, *IEEE Transactions on Information Theory*, to appear.

[12] V, Miller, “Use of elliptic curves in cryptography,” *Abstracts for Crypto 85*, 1985.

[13] A. Miyaji, “Elliptic curves over Fp suitable for cryptosystems”, *Advances in Cryptology – AUSCRYPT ’92*, to appear.

[14] F. Morain, “Building cyclic elliptic curves modulo large primes,” *Crypto’98*, pp. 472-285,

1998.
[15] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, "Optimal normal bases in GF(p^m)," *Discrete Applied Math*, vol. 22, pp. 149-161, Elsevier Science Publishers North-Holland, 1988.
[16] S. H. Yang, *The Implementation and Performance Analysis on Elliptic Curve Cryptosystems*, Master thesis, the National Chiao Tung University, (2001).
[17] S. H. Yang, J. S. Hwu, K. C. Huang and R. J. Chen, "Performance Analysis for Arithmetic in Finite Field GF(p^n)," *Proceedings of the 11th National Conference on Information Security*, Taiwan, pp. 185-192.