行政院國家科學委員會專題研究計畫　成果報告

橢圓曲線密碼系統之加速運算

計畫類別：個別型計畫
計畫編號：NSC93-2115-M-164-002-
執行期間：93 年 08 月 01 日至 94 年 07 月 31 日
執行單位：修平技術學院資訊管理系

計畫主持人：姜文忠

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 94 年 9 月 2 日

橢圓形曲線密碼系統之加速運算

The faster computation on the elliptic curve cryptosystem

計畫編號：NSC 93-2115-M-164-002

執行期限：93 年 8 月 1 日至 94 年 7 月 31 日

主持人：姜文忠　　修平技術學院資訊傳播系

一、 中文摘要

近百年多來，橢圓曲線被廣泛應用於代數及幾何的領域中。1985 年由 Miller 與 Koblitz 首先引進密碼學中並提出一個新的公開金鑰密碼系統，稱為橢圓曲線密碼系統(ECC)，其安全性乃建立在橢圓曲線離散對數之問題上(ECDLP)。橢圓曲線密碼系統之所以被重視的原因主要在於相同的安全強度下，橢圓曲線密碼系統的金鑰長度遠短於其它公開金鑰密碼系統的金鑰長度，例如橢圓曲線密碼系統 160 位元的金鑰長度與 1024 位元的 RSA 或 Diffie-Hellman 有相同的安全強度，然而，大量減少的金鑰長度可直接節省硬體的運算成本。因此，不論是在儲存公開金鑰的能力、傳輸所佔的頻寬以及加密資料或數位簽章等方面，橢圓曲線系統都佔有較大的優勢。但是如果要應用於資源被限制的系統，例如智慧卡等，我們仍需要對 ECC 作改進。

ECC 的基本運算是對於在某個有限體(finite field)之橢圓曲線上的點作加法計算，而橢圓曲線密碼系統則是運用橢圓曲線離散對數問題(意即: 給予曲線上任意兩點 P, R，滿足 $nP = R$，欲找出 n。因為通常在實做時都會選取很大的 n，讓尋找 n 要花很多的成本與時間)以達到所謂的安全性。因此，橢圓曲線密碼系統中影響加、解密速度的關鍵在於對橢圓曲線上的點進行純量乘法(scalar multiplication)運算的效率(即具有 n 個橢圓曲線生成點(Generator)的進行純量乘法(nP)的運算)。

基於上述理由，本計畫提出一個快速的演算法來改善橢圓曲線純數積的運算速度，透過節省一個有限體的乘法(field multiplication)運算來加速橢圓曲線點乘法運算。此種做法相較一般傳統的橢圓曲線點乘運算，約可減少 4%到 7%的運算。

我們並將它應用到利用 Weil pairing 計算作為基礎的一些相關公鑰密碼系統或協定中，以提升實際應用之效率。

關鍵字：橢圓曲線密碼系統， 橢圓曲線離散對數問題，純量乘法，金鑰交換協定，Weil pairing.

Abstract

In 1985, Miller and Koblitz independently proposed a new public key cryptosystem, called elliptic curve cryptosystem (ECC), whose security is

based on the elliptic curve discrete logarithm problem (ECDLP). The key length of ECC is shorter than that of other public key cryptosystems in the same security strength, for instance, the key length of ECC with 160 bits and the key length of RSA or Diffie-Hellman with 1024 bits have the same security strength. Therefore, in the aspects of storing the ability of the public key, delivering the bandwidth had and encrypting the data etc., the ECC all occupies the bigger advantage. But for the application of constrained system, it still needs to be improved.

The basic operation in elliptic curve cryptosystem is the computation of scalar multiplication (nP) on the elliptic curve with order n over a finite field.

Therefore, we present a multiplication on a general an algorithm which speeds scalar multiplication on a general elliptic curve by an estimated 4% to 7% over the best known general methods when using affine coordinates. This is achieved by eliminating a field multiplication when we compute $2P+Q$ from given points P, Q on the curve.

We have applications to speed the computation of cryptosystem and key agreement protocol which base on the Weil pairing.

Keywords：elliptic curve cryptosystem, elliptic curve discrete logarithm problem, scalar multiplication, key agreement protocol, Weil pairing.

二、 緣由與目的

現今有許橢圓曲線密碼系統就是運用橢圓曲線離散對數問題中所提到，一個單向暗門函數(Trapdoor One-way Function)的觀念所設計來的。雖然，在橢圓曲線上的一個基本運算是橢圓曲線上的兩個點的加法運算(形成一個交換群 abelian group)，而實際上，運用在所謂的公開金鑰密碼系統上的公鑰其實就是：給予曲線上任意兩點 P, R，滿足 $nP = R$(其中，P 為一個橢圓曲線上的生成點 generator point，n 為私鑰，而 R 為公鑰)。也就是說，公鑰 R 是由生成點 P 連續作 n 次的加法運算而來。

傳統的金鑰交換協定大都建立在解離散對數的困難度上，然而，近年來由於橢圓曲線(Elliptic Curve)所衍生出的雙線性配對(Bilinear Pairings)密碼機制，提供了另一種新的金鑰交換協定方法。因此，利用 Weil pairing 之雙線性特性為基礎，以達到安全及有效的多方身份認證與金鑰交換亦是許多研究論文所探討的主題。Joux 在 2000 年首先利用 Weil pairing 的雙線性特性提出了三方的 Diffie-Hellman 金鑰協定(key agreement protocol)，在 Joux 的協定中，參與通訊的每個人僅需廣播一次公開的訊息，便可協議出一把共同加密的金鑰，有效減少各方通訊的次數。

綜觀上述，不論是在一般的橢圓曲線密碼系統要去解開所謂的密文(Ciphertext)以得到原始的明文(Plaintext)。還是更進一步地應用到做為多方通訊上的加密金鑰交換協定之上。均會面臨到一個問題，那就是如

何在這些密碼系統或協定中快速有效地計算出橢圓曲線上點的純量乘法運算。

三、 方法與結果

我們透過節省一個有限體的乘法(field multiplication)運算來加速橢圓曲線點乘法運算。舉例來說，給予橢圓曲線上任意兩點 P, Q, 當欲計算 $2P+Q$ (或 $2P-Q$)時，中間過程所產生的點(如 $2P$, $P+Q$ or $P-Q$)的座標不須計算出來，還是可以產生最後點 $2P+Q$ (或 $2P-Q$)的座標值。

以一般傳統的運算而言，已知在一個有限體 affine 座標內的橢圓曲線上的兩點相加 ($P+Q$) 或一個點的兩倍值($2P$) 或 ($2P+Q$)的, 它的基本運算結果如下:

	$2P$	$P+Q$	$2P+Q$
Multiplication	1	1	2
Squaring	2	1	3
Division	1	1	2

(此處 P, Q 為橢圓曲線上相異之兩點)

以 $2P+Q$ 的運算來說(其中 $P = (x_1, y_1)$, $Q = (x_2, y_2)$)，透過先計算($P+Q$)的結果，過程中，省略了($P+Q$)這個點的 y 座標計算(需要一個 Multiplication 運算)，因為這個 y 座標在下一階段計算 ($P+Q$)+P 的運算中並不需要利用到這個座標。因此，運算比上述一般的運算減少了一個 Multiplication 計算。詳細做法如下:

- 假設相異兩點 $P=(x_1, y_1)$, $Q=(x_2, y_2)$，且 $x_1 \neq x_2$，點($P+Q$)的座標為(x_3, y_3)。
- 透過橢圓曲線兩點和的計算:

  $\lambda_1 = (y_2-y_1)/ (x_2-x_1)$

  $x_3 = \lambda_1^2 - x_1 - x_2$

  $y_3 = (x_1-x_3)\lambda_1 - y_1$

- 將點($P+Q$)加到點 P 上, 即將座標(x_1, y_1)與(x_3, y_3)相加(此處 $x_3 \neq x_1$)，假設得到點($2P+Q$)其座標為(x_4, y_4)，結果如下:

  $\lambda_2 = (y_3-y_1)/ (x_3-x_1)$

  $x_4 = \lambda_2^2 - x_1 - x_3$

  $y_4 = (x_1-x_4)\lambda_2 - y_1$

- 若省略了 y_3 的計算 (y_3 僅用於計算 λ_2)，則λ_2 可以不使用 y_3 便可計算出來結果如下:

  $\lambda_2 = -\lambda_1 - 2y_1/ (x_3-x_1)$

綜合上述，總共節省了一個 Multiplication 計算(它使用在計算 y_3 時)。

同樣地，可運用於計算點 $3P$ 計算。而計算($3P+Q$)時，又如何呢? 可將它視為 $3P+Q=((P+Q)+P) + P$，即是利用上述的作法兩次，最後可節省兩個 Multiplication 計算。

最後我們可以將這整方法推廣到 kP 的計算(當 k 很大時)，例如計算 $1133044P$，又如何呢?

一般傳統計算:

	add	*div*	*squ*	*mul*
$4P = P+ 3P$	1	3	3	1
$35P= 8(4P) +3P$	1	3	4	4
$277P= 8(35P)-3P$	1	3	6	4
$2213P= 8(277P)-3P$	1	3	7	4
$283261P= 128(2213P)-3P$	1	7	9	5

1133044*P*= 4(283261*P*)	0	4	12	5
Total	**5**	**23**	**41**	**23**

本計畫結果:

	add	*div*	*squ*	*mul*
4*P* = *P*+ 3*P*	1	3	3	1
35*P*= 8(4*P*) +3*P*	2	3	4	3
277*P*= 8(35*P*)−3*P*	2	3	5	3
2213*P*= 8(277*P*)−3*P*	2	3	6	3
283261*P*= 128(2213*P*)−3*P*	2	7	9	4
283261*P*= 128(2213*P*)−3*P*	2	4	10	5
Total	**9**	**23**	**37**	**19**

相較一般傳統的橢圓曲線點乘運算點 1133044*P*, 總共需要(5*add* + 23*div* +41*squ* +23*mul*)，大約節省 5%。(此處假設 3*P* 是事先已算好的點)

四、 計畫成果自評

本計畫有效運用橢圓曲線上點座標及基本加法運算的特性，提出一個快速的演算法來改善橢圓曲線純數積的運算速度，利用兩次的點相加之過程中第一次產生知該點的 y 座標可以省略不用計算出的特性，以節省一個有限體的乘法運算來加速橢圓曲線點乘法運算。此種做法可有效降低一般傳統的橢圓曲線點乘運算。

再者，近來有許多的公鑰系統如加密系統、簽章系統及金鑰協定系統等紛紛利用 Weil pairing 計算來完成相關的機制或金鑰的計算，然而 Weil pairing 函數本身即是由橢圓曲線中基本的點乘運算而產生，因此，本計畫除能有效提升橢圓曲線點乘法運算外，倘若將它運用在以 Weil pairing 為基礎的密碼系統或協定上，更可大幅提升其計算之效能。

五、 參考文獻

[1] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. on Information Theory, Vol.IT-22, ,pp.638-654, Nov. 1976

[2] H. Cohen, A, Miyaji and T. Ono, "Efficient Elliptic Curve Exponentiation Using Mixed Coordinates," Advance in Cryptology-ASIACRYPT'98,LNCS 1514, Springer, pp. 51-65, 1997.

[3] E.F. Brickell and K.S. McCurley, "Interactive Identification and Digital Signatures," AT&T Technical Journal, pp.73-86, 1991.

[4] N. Koblitz, "Elliptic Curve Cryptosystems," Math. Computat., vol. 48, pp.203-209,1987.

[5] C. S. Laih and W. C. Kuo, "Speeding Up the Computations of Elliptic Curve Cryptoschemes," International J. of Computers & Mathematics with Applications, Vol. 33, no. 5, pp. 29-36, March 1997.

[6] K. Koyama and Y. Tsuruoka, "Speeding Up Elliptic Cryptosystems by Using a Signed Binary Window Method," Advances in Cryptology-Crypto'92, LNCS 740, springer-Verlag, pp. 345-357, 1993.

[7] P. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization", Math. Computat., vol. 48, pp.243-264, 1987.

[8] Pat. Morandi, Field and Galois Theory, Springer-Verlag, New York, 1996.

[9] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography, CRC Press, 1997.

[10] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, Boston, 1993.

[11] G. Menezes, R. Mullin, I. Onyszchuk and S. Vanstone, "An Implementation for Elliptic Curves Cryptosystem over," IEEE Journal on Seclected Areas in Communications, 11, pp. 1639-1646, 1993.

[12] A. J. Menezes, T. Okamoto, S. A. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," IEEE Trans. on Information Theory, Vol.39, No.5, pp.1639-1646, Sep 1993.

[13] S. Pohlig and M. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance", IEEE Transactions on Information Theory, Vol. 24, pp. 106-110, 1978.

[14] R. Schoof, "Nonsingular Plane Cubic Curves over Finite Fields", Journal of Combinat. Theory, vol. A 46, pp. 183-211, 1987.

[15] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106, Springer-Verlag, New York,1986.

[16] N. Smart, "The Discrete Logarithm Problem on Elliptic Curves of Trace One," to appear in Journal of Cryptology.

[17] J.H. Silverman, and J. Tate, Rational Points on Elliptic Curves, Springer-Verlag, New York, 1992.

[18] C.P. Schnorr, "Efficient Identification and Signatures for Smart Cards," Advanced in Cryptology -Crypto'89, LNCS 435, Springer-Verlag, pp. 239-252, 1990.

[19] I.F. Blake, G. Seroussi, N.P. Smart, Elliptic Curves in Cryptography, LMS 265 Cambridge University Press, 1999.

[20] Dan Boneh and Matt Franklin, Identity-based encryption from the Weil pairing, in Advances in Cryptology – Crypto 2001, J. Kilian (Ed.), LNCS 2139,

[21] Dan Boneh, Ben Lynn, and Hovav Shacham, Short signatures from theWeil pairing, in Advances in Cryptology – Asiacrypt 2001, C. Boyd (Ed.), LNCS 2248,

[22] IEEE Standard Specifications for Public-Key Cryptography, IEEE Std 1363–2000, IEEE Computer Society, 29 August 2000.

[23] Antoine Joux, The Weil and Tate

Pairings as building blocks for public

[24] David R. Kohel (Eds.), LNCS 2369, Springer-Verlag, 2002, pp. 20–32.

[25] Donald E. Knuth, The Art of Computer Programming, vol. 2, Seminumerical Algorithms, Addison-Wesley, 3rd edition, 1997.

[26] Applications in Elliptic Curve Cryptography, The 9th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2002, Dubrovnik, Croatia, September 15–18, 2002, vol. 3, pp. 1155–1158.

[27] Peter L. Montgomery, Speeding the Pollard and Elliptic Curve Methods of Factorization, Math. Comp., v. 48(1987), pp. 243–264.

[28] Yasuyuki Sakai, Kouichi Sakurai, On the Power of Multidoubling in Speeding up Elliptic Scalar Multiplication, in Selected Areas in Cryptography 2001, Toronto, Ontario, Serge Vaudenay and Amr M. Youssef (Eds.), LNCS 2259, Springer-Verlag, 2002, pp. 268–283.