適用無線環境之橢圓曲線加速演算法研究

周智禾、曹偉駿

E-mail: 9222446@mail.dyu.edu.tw

摘 要

在1985年，Koblitz和Miller提出了橢圓曲線密碼系統，由於其所使用的金鑰大小可以大幅降低的特性，因此隨即受到了廣泛的重視。橢圓曲線密碼系統160位元金鑰長度的安全性，同等於RSA公開金鑰密碼系統的1024位元金鑰長度，故非常適合運用在具較小的記憶體與運算能力的裝置上，如智慧卡。IEEE、ANSI和ISO等都已經將橢圓曲線列為其標準，因此，我們預期它將是未來各種公開金鑰密碼系統的主流之一。 橢圓曲線密碼系統的效率依賴在純數積運算上，因此，基於效率上的考量，發展出其加速演算法是必要的。在1994年，Lim和Lee提出一個用在無線環境且較具彈性化的方法，有效的利用事先計算來加快指數運算的速度，其方法亦可使用在加速橢圓曲線的純數積運算上，我們稱之為LLECC方法。然而，LLECC方法使用在記憶體空間越小的裝置上，會越沒有效率，因此，在本篇論文中，我們將提出一個比LLECC方法更有效率的加速演算法。首先，我們將修改LLECC方法的演算法以降低事先運算所需花費的儲存空間，並進一步結合符號位元表示法及Multidoubling，以提出一套有效率的加速演算法，同時我們的方法亦可應用在加速橢圓曲線多點的乘法運算上。相較於LLECC方法，我們的方法不但降低了記憶體空間儲存量，並進一步地改善其運算效率，故本研究所提出之加速演算法較適用於無線的環境之下。根據我們的模擬結果，在有限場 及仿射座標系下之160位元的橢圓曲線密碼系統中，本方法可以減少11%的計算複雜度以及降低記憶體空間達21%。最後，在實作方面，我們將利用本研究所提出之演算法，來加速橢圓曲線數位簽章系統中的純數積運算於個人數位助理中。

關鍵詞 : 公開金鑰密碼系統、橢圓曲線密碼系統、純數積運算、點乘法、多點乘法。

目錄

Chapter I. INTRODUCTION..... 1 1.1 Backgrounds..... 1 1.2 Research Motivation..... 3 1.3 Thesis Organization..... 6 Chapter II. ELLIPTIC CURVE CRYPTOSYSTEMS..... 7 2.1 Introduction..... 7 2.2 Definition..... 8 2.3 Finite Fields..... 11 2.4 The Group Law..... .....13 2.5 Elliptic Curve Cryptosystems over.....16 2.6 Known Attacks..... .....18 Chapter III. PREVIOUS WORKS..... 21 3.1 Binary Method..... 21 3.2 m-ary Method..... 22 3.3 Window Methods..... 24 3.4 NAF..... 25 3.5 Addition Chain and Addition-Subtraction Chain.....27 3.6 Multi-Point Multiplication..... 28 3.7 Precomputation..... 30 3.7.1 BGMW..... .....31 3.7.2 LLECC Method..... .....32 3.7.3 Yang et al. Method..... 36 3.8 Multidoubling..... .....38 Chapter IV. THE PROPOSED EFFICIENT ALGORITHMS FOR SPEEDING UP ECC 40 4.1 Research Methods..... .....40 4.2 The Point Multiplication..... 42 4.3 The Multi-Point Multiplication.....47 4.4 Performance Analysis..... 51 Chapter V. IMPLEMENTATION..... 65 5.1 System Architecture..... 65 5.2 The ECDSA-like Scheme..... 67 5.3 User Interface..... .....69 Chapter 5. CONCLUSIONS..... .....76 Bibliography..... 78

參考文獻

[1] ANSI X9.31, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), 1998.

[2] ANSI X9.62, Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), 1999.

[3] ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Key Transport Protocols, Working Draft, 2000.

[4] I. F. Blake, G. Seroussi and N. P. Smart, Elliptic Curves in Cryptography, The Press Syndicate of the University of Cambridge, 1999.

[5] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology-Crypto'2001, Springer- Verlag, pp. 213-229, 2001.

[6] J. Bos and M. Coster, "Addition Chain Heuristics," Advances in Cryptology-Crypto'89, Springer-Verlag, Vol. 415, pp. 400-407, 1990.
[7] E. F. Brickell, D. M. Gordon, K. S. McCurley and D. Wilson, "Fast Exponentiation with Precomputation," Advances in Cryptology-Eurocrypto'92, Springer-Verlag, pp. 200-207, 1992.
[8] Certicom Corporation, URL: http://www.certicom.com/.
[9] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, Springer-Verlag, 1993.
[10] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Transactions in Information Theory, Vol. IT-22, pp. 644-654, Nov. 1976.
[11] P. Downey, B. Leony and R. Sethi, "Computing Sequences with Addition Chains," SIAM Journal of Computing, pp. 638-696, 1981.
[12] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472, 1985.
[13] FIPS 186-2, National Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-2, Available from http://csrc.nist.gov/encryption/, 2000.
[14] D. M. Gordon, "A Survey of Fast Exponentiation Methods," Journal of Algorithms, Vol. 27, pp. 129-146, 1998.
[15] J. Guajardo and C. Paar, "Efficient Algorithms for Elliptic Curve Cryptosystems," Advances in Cryptology-Crypto'97, LNCS, Springer-Verlag, Vol. 1294, pp. 342-356, 1997.
[16] Y. Han and P. C. Tan, "Direct Computation for Elliptic Curve Cryptosystems," Pre-proc. Cryptographic Hardware and Embedded Systems (CHES)'99, Springer-Verlag, pp. 328-340, 1999.
[17] IEEE P1363, Standard Specifications for Public-Key Crypto- graphy, http://grouper.ieee.org/groups/1363/index.html, 2000.
[18] ISO/IEC 14888-3, Information Technology-Security Techniques- Digital Signature with Appendix-Part 3: Certificate-based Mechanisms.
[19] ISO/IEC 15946 series, Information Technology-Security Techniq- ues-Cryptographic Techniques Based on Elliptic Curves, Working Draft, 1998.
[20] ISO/IEC 9796-4, Information Technology-Security Techniques- Digital Signature with Message Recovery-Part4: Discrete Logarithm-based Mechanisms.
[21] J. Jedwab and C. J. Mitchell, "Minimum Weight Modified Signed-Digit Representation and Fast Exponentiation," Electronic Letter, Vol. 25, No. 17, pp. 1171-1172, 1989.
[22] A. Juristic and A. J. Menezes, "Elliptic Curve and Cryptography," Dr. Dobb's Journal, pp. 26-35, 1997.
[23] D. E. Knuth, "Seminumerical Algorithms 2nd," The Art of Computer Programming, Vol. 2, Addison-Wesley, 1983.
[24] N. Koblitz, "Elliptic Curve Cryptosystems," Math. Comp., Vol. 48, No. 17, pp. 203-209, 1987.
[25] N. Koblitz, "Constructing Elliptic Curve Cryptosystems in Characteristic 2," Crypto'90, pp. 156-167, 1990.
[26] C. S. Laih and W. C. Kuo, "Speeding Up the Computations of Elliptic Curve Cryptoschemes," International Journal of Computers & Mathematics with Applications, Vol. 33, No. 5, pp. 29-36, March 1997.
[27] C. H. Lim and P. J. Lee, "More Flexible Exponentiation with Precomputation," Advances in Cryptology-Crypto'94, Springer- Verlag, pp. 95-107, 1994.
[28] G. W. Lo, The Study and Implementation on Elliptic Curve Digital Signature Schemes, Master Thesis, NCKU, Taiwan, 2000.
[29] A. J. Menezes and S. A. Vanstone, "Elliptic Curve Cryptosystems and Their Implementation," Journal of Cryptology, Vol. 6, No. 4, pp. 209-224, 1993.
[30] A. J. Menezes, T. Okamoto and S. A. Vanstone, "Reducing Elliptic Curve Logarithms to a Finite Field," IEEE Transactions on Information Theory, pp.1639-1646, 1993.
[31] V. Miller, "Uses of Elliptic Curves in Cryptography," Advances in Cryptology-Crypto'85, Springer-Verlag, pp. 417-426, 1985.
[32] A. Miyaji, T. Ono and H. Cohen, "Efficient Elliptic Curve Exponentiation (I)," IEICE Technical Report, ISEC97-16, 1997.
[33] F. Morain and J. Olivos, "Speeding Up the Computations on an Elliptic Curve Using Addition-Subtraction Chains," Info. Theory Appl., pp. 531-543, 1990.
[34] V. Muller, "Efficient Algorithms for Multiplication on Elliptic Curves," Proc. GI-Arbeitskonferenz Chipkarten 1998, TU Munchen, 1998.
[35] National Institute of Standards and Technology, "Digital Signature Standard," Communications of the ACM, Vol. 35, No. 7, pp. 36-40, July 1992.
[36] A. M. Odlyzko, "Discrete Logs in a Finite Field and Their Cryptographic Significance," Advances in Cryptology-Eurocrypt '84, Springer-Verlag, pp.224-314, 1985.
[37] P. Oorschot Van and M. Wiener, "Parallel Collision Search with Cryptanalytic Applications," Journal of Cryptology, pp. 1-28, 1999.
[38] J. Pollard, "Monte Carlo Methods for Index Computation ," Math. Comp., pp. 918-924, 1978.
[39] S. Pohlig and M. Hellman, "An Improved Algorithm for Computing Logarithms over and Its Cryptographic Significance," IEEE Transactions on Information Theory, pp.106-110, 1978.
[40] G. Poupard and J. Stern, "A Practical and Provable Secure Design of on the Fly Authentication and Signature Generation," Advances in Cryptology- proceedings of Eurocrypt '98, Springer-Verlag, pp.422-436, 1998.

[41] M. O. Rabin, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization," Technical Report LCS/TR212, MIT Laboratory for Computer Science, 1979.
[42] M. O. Rabin, "Probabilistic Algorithm for Testing Primality," Journal of Number Theory, Vol. 12, pp. 128-138, 1980.
[43] R. L. Rivest, A. Shamir and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, pp. 120-126, Feb. 1978.
[44] Y. Sakai and K. Sakurai, "Efficient Scalar Multiplications on Elliptic Curves without Repeated Doublings and Their Practical Performance," Information Security and Privacy, ACISP 2000, LNCS, Springer-Verlag, Vol. 1841, pp. 59-63, 2000.
[45] Y. Sakai and K. Sakurai, "Efficient Scalar Multiplications on Elliptic Curves with Direct Computation of Several Doublings," IEICE Transactions Fundamentals, Vol. E84-A, No. 1, pp. 120-129, 2001.
[46] Y. Sakai and K. Sakurai, "Speeding Up Elliptic Scalar Multiplication Using Multidoubling," IEICE Transactions Fundamentals, Vol. E85-A, No. 5, pp. 1075-1083, 2002.
[47] T. Satoh and K. Araki, "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves," Comm. Math. Univ. Sancti. Pauli., pp. 81-92, 1998.
[48] C. P. Schnorr, "Efficient Identification and Signature for Smart Cards," Advances in Cryptology-Crypto'89, New York, Springer-Verlag, pp. 239-252, 1990.
[49] SEC1, "Elliptic Curve Cryptography," Standards for Efficient Cryptography Group, Available from http://www.secg.org/ collateral/, 2000.
[50] SEC2, "Recommended Elliptic Curve Cryptography Domain Parameters", Standards for Efficient Cryptography Group, Available from http://www.secg.org/ collateral/, 2000.
[51] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.
[52] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994.
[53] N. P. Smart, "The Discrete Logarithm Problem on Elliptic Curves of Trace One," Journal of Cryptology, 1999.
[54] M. J. Wiener, "Cryptanalysis of Short RSA Secret Exponents," IEEE Transactions on Information Theory, Vol. IT-36, pp. 553-558, 1990.
[55] E. De Win, S. Mister, B. Prennel and M. Wiener, "On the Performance of Signature based on Elliptic Curves," Algorithmic Number Theory, Proceedings Third Intern. Symb., ANTS-III, LNCS 1423, Springer-Verlag, pp. 252-266, 1998.
[56] W. C. Yang, K. M. Lin and C. S. Laih, "A Precomputation Method for Elliptic Curve Point Multiplication," Journal of the Chinese Institute of Electrical Engineering, Vol. 9, No. 4, pp. 339-344, Nov. 2002.
[57] S. M. Yen, C. S. Laih and A. K. Lenstra, "Multi-Exponentiation," IEE Proceedings Part-E: Computers and Digital Techniques, Vol. 141, No. 6, pp. 325-326, Nov. 1994.
[58] S. M. Yen and C. S. Laih, "The Fast Cascade Exponentiation Algorithm and Its Application on Cryptography," Advances in Cryptology-Ausxrypt'92, New York, Springer-Verlag, pp. 447-456, 1993.
[59] 賴溪松、韓亮、張真誠，「近代密碼學及其應用」，松崗圖書資料公司，民國84年9月。