行政院國家科學委員會補助專題研究計畫成果報告

橢圓曲線密碼模組 (II)

計畫類別：☑個別型計畫　　□整合型計畫

計畫編號：NSC 89－2115－M－032－014－

執行期間：89 年 08 月 01 日 至 90 年 07 月 31 日

主持人：陳燕美　淡江大學數學系

計畫參與人員：兼任助理　林安國　淡江大學數學系碩士生

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：淡江大學　數學系

中華民國 90 年 10 月 31 日

一、中文摘要：

令 E/F_p 是定義在有限體的橢圓曲線, S 和 T 是曲線上的兩點, 橢圓曲線離散對數問題是想要找到整數 m 滿足 $T=mS$。 在去年度的報告中我們已經給一個解決此一問題的方法。對於小的質數 p, 這個方法可以有效地解決我們的問題。在這份報告中, 我們將仔細分析此一方法的成功機率及其計算複雜度。

關鍵詞: 橢圓曲線, 有限體, 離散對數, 機率, 計算複雜度。

二、英文摘要(Abstract):

Let E/F_p be an elliptic curve defined over a finite field of odd characteristic, and let S and T be points in $E(F_p)$. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is the problem to find an integer m satisfying $T=mS$. In our last report, we gave a method to solve ECDLP. It has the advantage of working well for small values of prime p. In this report, we analyze the probability of success and the computational complexity of our method.

關鍵詞(Key Words): elliptic curves, finite field, discrete logarithms, probability, computational complexity.

三、計畫緣由與目的:

Elliptic Curve Cryptosystem was proposed independently by Miller and Koblitz in 1980's ([Mil1], [Kob1]). So far, there is no subexponential algorithm for ECDLP in practice except for particular cases of curves having the Frobenius trace -2,0 and 1 ([Fre1], [Men1], [Sem1]). In our last project, we gave a new method to solve ECDLP by lifting E over F_q to an elliptic curve E' over the function field F_q (t). In this project, we first estimate the computational complexity of the algorithm for the proposed new method, secondly we analyze the probability of success of our method. Finally, we do some computer experiment.

四、計畫結果與討論:

定理一：

The computation of the proposed new method can be done in a probabilistic algorithm with $O(\log q)$ operations in the finite field F_q.

定理二：

There exists an absolute constant C such that the probability of success of the proposed new method is less than C/q.

五、計畫成果自評

Although the proposed method has the advantage of working well for small values of primes p, the closer analysis in this project shows that it is still an impractical method asymptotically.

六、參考文獻

[Adl1] L. Adleman, *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, Proc. 20th IEEE Found. Comp. Sci. Symp., 1979, pp. 55-60.

[Cox1] David Cox and Walter R. Parry, *Torsion in Elliptic Curves over k(t)*, Compositio Mathmetica, Vol. 41, Fasc. 3, 1980, pp. 337-354.

[Evd1] S. Evdokimov, *Factorization of Polynomials over Finite Fields in Subexponential Time under GRH*, Lecture Notes in Computer Science, Vol. 877, 1994, pp. 209-219.

[Fre1] G. Frey and H.-G. Guck, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. 62(1994), 865-874.

[Kol1] N. Koblitz, *Elliptic curve cryptosystem*, Mathematics of Computation 48 (1987), 203-209.

[Jac1] M. Jacobson, N. Koblitz, J. Silverman, A. Stein, E. Teske, *Analysis of the Xedni Calcu;us Attack*, preprint, 1999.

[Men1] A. Menezes, T. Okamoto and S.A. Vanstone, *Reducing elliptic curves logarithms to logarithm in a finite field*, IEEE Trans. Info. Theory, 39, (1993) 1639-1646.

[Mil1] V.S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology CRYPTO'85, Springer-Verlag, 1986, pp. 417-426.

[Rab1] M.O. Rabin, *Probabilistic Algorithms in Finite Fields*, SIAM. J. Comput., Vol 9, No 2, 1980, 273-280.

[Sem] I. Semaev, *Evaluation of Discrete Logarithms in a Group of p-torsion Points of an Elliptic Curve in characteristic p*, Math. of Comp. 67(1998), 353-356.

[Sil1] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer--Verlag, 1985.

[Sil2] J. Silverman, *Computing Heights on Elliptic Curves*, Math. Comp., vol 51, 1988, pp. 339-358.

[Sil3] J. Silverman, J. Suzuki, *Elliptic curve discrete logarithms and the index calculus*, ASIACRYPT'98, to appear.

[Sil4] J. Silverman, *The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem*, preprint, 1998.

[Sil5] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer Verlag, 1994.