行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※　　　　　　離散對數密碼系統之平行攻擊　　　　　　※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別： ¦個別型計畫　　æ整合型計畫

計畫編號： NSC89－2213－E－009－179－

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

離散對數密碼系統之平行攻擊

Parallel Attack on Discrete Logarithm-Based Cryptosystems

計畫編號：NSC 89-2213-E-009-179
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：黃凱群　國立交通大學 資訊工程學系
郭哲君　國立交通大學 資訊工程學系
林志信　國立交通大學 資訊工程學系
葉乃嘉　國立交通大學 資訊工程學系

一、中文摘要

1976 年，Diffie and Hellman 提出了一套金鑰分配方法，他們使用離散對數為高難度計算的假設，使得網路上兩個使用者可以安全且秘密的交換一把密鑰，之後離散對數的密碼系統被廣範的使用，如 Massey-Omura 密碼系統，ElGamal 公鑰密碼系統，及美國正式訂定的數位簽署標準 DSS.

在 ElGamal 公鑰密碼系統中，每個使用者都擁有兩把鑰匙--公鑰與私鑰，公鑰將公佈給所有的人知道，而私鑰則由自己秘密保存著，若甲方想要把訊息送給乙方，且不想讓其他人知到訊息的內容，甲方可以用乙方的公鑰將訊息加密後送出，此加密過的訊息，只有擁有私鑰的人--乙方，才能解開並讀到真正的內容．在正常的情形下，只有乙方一人知道這把解密的私鑰．

公鑰密碼系統的安全性，在於幾乎無法由公鑰去計算推導出私鑰，也就是靠這種計算不可行(computational infeasibility)才得以保密．假如藉計算推導確實不易取得私鑰，那麼我們才可以稱這個系統是安全的．ElGamal 公鑰密碼系統就是利用離散對數相當困難的這個事實來製造公鑰與私鑰．因為大家公認要找一個大的數字的某次方等於另一個數字是困難的，所以說 ElGamal 系統可說是相當安全的．

在本計畫中我們想要更深入的探討離散對數這個主題："為何我們需要解離散對數?" 早期人們認為大於 90 位的數字就不可能求解離散對數，但今日網際網路的爆炸，使得現在的電腦已有足夠的計算能力可以求解．解離散對數的進步主要歸功於硬體速度越來越快，網路越來越發達，及更多更快速的分解演算法被提出，目前著名的演算法有 Baby-step Giant-step 演算法，Pollard's Rho 演算法，Pohlig-Hellman 演算法，Tame & Wild Kangaroos 演算法，Index-calculus 演算法．由於上述解離散對數問題的演算法所花費的時間複雜度仍然很高，因此我們將向離散對數問題的困難度挑戰，設計一個有效率解離散對數的演算法，並且利用我們交大資工系 Intel 實驗室的分散式系統，使用平行運算結構來執行新設計的演算法，以期能夠迅速求解大型離散對數問題。

鑑於國內密碼學學術界對於基礎理論的研究並不多，我們將對這領域做深入的研究，設計出更有效率的大數分解演算法．在應用方面，我們也將發展出一套解離散對數的軟體，以供國內學界使用．

關鍵詞：ElGamal 公鑰密碼系統，離散對數，
Index-calculus 演算法，
Gaussian Integers，遺忘傳輸協定．

Abstract

In 1976, Diffie and Hellman use discrete logarithm problem to construct a key distribution system that provides a secure environment to distribute keys over public network. After that, many cryptosystems based on discrete logarithm problem such as Massey-Omura cryptosystem for message transmission, ElGamal public key cryptosystem, and DSS (Digital Signature Standard) were published.

ElGamal is a public key cryptosystem where each party holds two keys: a public key and a corresponding secret key. The public key is accessible by the public while the secret key is always kept secret. You can encrypt a message using the recipient's public key and only the recipient can decrypt the message with secret key. No other people know the secret key.

The security of the public key cryptosystem is ensured by the fact that it is too hard or, computationally infeasible, to derive the secret key from the public key. If a third party wants to decrypt the message, he should find power of a number that is part of the public key. Since discrete logarithm is commonly believed too hard, ElGamal utilizes this fact to produce the public key and the secret key to ensure security.

In this project we would like to explore discrete logarithm problem: "why we need to solve discrete logarithm problems?" In early years, people believed 90-digit numbers provided enough security, but now the computer can solve them efficiently. The progress

results from faster hardware and better algorithms. Currently the available solving discrete logarithm methods include baby-step giant-step method, Pollard's rho method, Pohlig-Hellman method, tame and wild kangaroos method, and index-calculus method. The time complexity of those mentioned algorithms for solving the problem is still too high. Therefore we challenge the difficulty of the discrete logarithm problem and design efficient parallel algorithms for it. We will implement the designed algorithms on the distributed system at Intel Laboratory in the Department of Computer Science and Information Engineering, National Chiao Tung University. We hope to solve efficiently large-scale discrete logarithm problems at the end of the project.

Since the basic theoretical research in cryptography is scarce in Taiwan, we dedicate ourselves to explore this area trying to design more efficient algorithms to solve discrete logarithm problem. For application purpose, we will develop software to solve discrete logarithm problems for academic users in the country.

Keywords: ElGamal public key cryptosystem, discrete logarithm, index-calculus, Gaussian Integers, oblivious transfer.

二、緣由與目的

自從美國正式訂定的數位簽署標準 DSS 被提出並且廣範應用於網際網路上後，解離散對數問題變成一件非常重要的事．目前很多密碼加解密方法，其安全度都是基於對解離散對數這個問題的困難度．在一個循環群中的所有數字，都可表示為 generator 的某次方．給定 generator 及次方數，可以很容易的算出這個數字，但反之，給定這個數字及 generator，卻很難將其次方求出．最直接的解離散對數演算法就是窮舉法(Exhaustive search method)，即對數字 n，用 generator 的 0 次方，1 次方，2 次方 ... 到φ(G)-1 次方去比對看是否相同，來求解離散對數．這個簡單的方法，對於 Group size 到 15 位左右的數就要耗費很多時間．在 40 年代電子計算機出現以前，儘管發明了許多解離散對數的方法，但由於需要手算，故即使幾位數左右也需好幾天時間，而對更大的數更是無能為力．隨著電子計算機的發明，人們開始利用這些歷史上留下來的方法並創造新的方法．到了 80 年代隨著離散對數在密碼學上有了重大的價值，數論學家與計算機專家們已深入的研究這個問題，而且得到了許多有效的方法．

目前著名的演算法有

1. Baby-step giant-step 演算法
2. Pollard's Rho 演算法
3. Tame & Wild Kangaroos 演算法
4. Pohlig-Hellman 演算法
5. Index-calculus 演算法

根據影響其執行效率的因素，我們可以將其分成兩大類，第一類的執行方式是是定性的(deterministic)，這類的演算法有 窮舉法，Baby-step giant-step 演算法[3]，Pollard's rho 演算法[4]，Pohlig-Hellman 演算法[5]．而第二類的執行時間跟機率(probabilistic)有關，這類演算法有 Tame & Wild Kangaroos 演算法[11]，Index-calculus 演算法[6]．這兩類的演算法跟據給的數字不同，而各有各的重要性．假設要求離散對數解的數對大小不會很大，則大部份都會先採用第一類的方法解離散對數，若使用第一類的方法時間太慢時導致無法解出時，再使用第二類的方法求其正確解答．

本計畫主要是研究有關離散對數的理論和實際應用，並依照不同的考量因素去改良與設計出不同的演算法：這些研究需要有現代代數，複雜度分析，演算法設計，以及數論等方面的知識並加以整合．在理論方面，我們將詳細研讀所有關於離散對數及數論的文獻，包括前述的各種解離散對數演算法．再者，我們也會透過網際網路得知世界上最新最快有關於解離散對數的問題和新的方法，以及它們在複雜度分析方面的結果．並且我們會測試我們目前現有的程式，並分析它們的優缺點．最後我們會嘗試把前述的演算法以及我們所設計的演算法做實際上軟體的撰寫；初期我們希望能有一個網際網路的介面供大家解離散對數，進而我們試著撰寫可供利用的函式庫(library)供有興趣的學者使用；在應用方面，目前實作上，我們使用離散對數去做遺忘傳輸協定(Oblivious Transfer)，遺忘傳輸協定是以密碼學上的公鑰密碼系統為基礎來實作，亦即在該系統中，每一位使用者必須自行產生自已所擁有的鑰匙對(key pair):一把公鑰與一把密鑰，並且將公鑰公佈於網路中，故此加密系統又稱"非對稱密碼系統(Asymmetric Cryptosystem)"．之後，使用者便可以利用這對鑰匙對，來進行遺忘傳輸．

鑑於國內密碼學學術界對於基礎理論的研究並不多，我們將對這領域做深入的研究，設計出更有效率的解離散對數演算法．在應用方面，我們也發展一套遺忘傳輸的軟體及解離散對數的函式庫，以供國內學界使用．

三、結果與討論

我們蒐集了到目前為止各種有關解離散對數的理論，及演算法的實作方法,整理完成代數體在整數分解及離散對數的應用[10]，並且對遺忘傳輸協定的設計做了研究及分析[12]，提供給國內密碼學學術界參考．

在實作方面，目前認為最有效率的解離散對數的演算法為 Index-calculus 使用 Gaussian Integers．基於硬體設備及時間等因素考量,我們以 100 位數左右的大數為目標，使用 Gaussian Integers 來分解．根據我們的實作，成功的解出了體大小約 30 位的離散對數問題．

據此，我們完成本計畫的目的，並在離散對數問題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離散對數理論研究的基礎；另外透過實作的過程，發展國內相關的基礎技術，除了應用在離散對數的領域外，未來更可以運用在密碼學上基本的計算及安全強度的分析．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] Diffie, W., and Hellmen, M.E., “New directions in cryptography,” IEEE Trans., IT-22, pp. 644-654, 1976

[2] ElGamal, T., “A public key cryptosystem and signature scheme based on discrete logarithms,” IEEE Trans., IT-31, (4), pp. 469-472, 1985

[3] Daniel Shanks, “Class number, a theory of factorization, and genera,” Proc. Symposium Pure Mathematics, American Mathematical Society, 1972

[4] J. M. Pollard, “Monte Carlo methods for index computation mod p,” Math. Comp. 32, 918-924, 1978

[5] Stephen C. Pohlig and martin E. Hellman, “An improved algorithm for computing logarithms over GF(p) and its cryptographic significance,” IEEE Trans. On Inform. Theory 24, 106-110, 1978

[6] L. M. Adleman, “A subexponential algorithm for the discrete logarithm problem with applications to cryptography,” Proc. Of the 20th Annual IEEE Symposium on Foundations of Computer Science, 55-60, 1979

[7] Kevin S. McCURLEY, “The Diserete Logarithm Problem,” Proceedings of Symposia in Applied Mathematics, Providence, Rhode Island, Vol. 42, American Mathematical Society, pp. 49-74, 1990

[8] L. Harn and Y.Xu, “Design of generalised ElGamal type digital signature schemes based on discrete logarithm,” ELECTRONICS LETTERS, Vol. 30, No. 24, pp. 2025-2026, 1994

[9] Neal Koblitz, “A Course in Number Theory and Cryptography,” Second Edition, 1994

[10] C. C. Kuo, “The Application of Number Field in Factorization and Discrete Logarithm Problems”, Master thesis, the National Chiao Tung University, (2001).

[11] E. Teske, “Speeding up Pollard’s Rho method for computing discrete logarithms,” A-3, p.541-554.

[12] J. C. Chang, W. C. Hsu, and R. J. Chen, (2001) “An Efficient Oblivious Transfer Scheme with Optimal Base,” Proceedings of the 11th National Conference on Information Security, Taiwan, pp. 241-248.

[13] B. A. LaMacchia and A.M. Odlyzko, “Computation of Discrete Logarithms in Prime Finite Fields,” Advances in cryptology-CRYPTO ’90 (Springer, Berlin, 1991)

[14] L. Harn, “Public-key cryptosystem design based on factoring and discrete logarithms”, IEE Proc. Comput. Digit. Tech., Vol. 141, No 3, 1994

[15] L. M. Adleman, and K. S. McCurley, “Open problems in number theoretic complexity,Discrete Algorithm and Complexity,” Proc. Of the Japan-U.S. Joint Seminar, Academic Press, Orlando, Florida, pp. 237-262, 1987

[16] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman, “The design and analysis of computer algorithms,” Addison-Wesley, Reading, MA, 1974

[17] Eric Bach, “Discrete logarithms and factoring,” Technical Report UCB/CSD 84/186, Computer Science Division (EECS), University of California, Berkeley, California, June, 1984

[18] I. F. Blake, R. Fuji-Hara, R. C. Mullin, and S. A. Vanstone, “Computing logarithms in fields of characteristic two,” SIAM J. Algebraic Discrete Methods 5(1984), 276-285.