SCIS 2006 The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

Design and Implementation of an ECM-based Integer Factorization Tool with GMP-ECM on Windows Platforms

周秉慧*[1] 楊中皇*[2] 櫻井幸一†
Bin-Hui Chou Chung-Huang Yang Kouichi Sakurai

Abstract— Integer factorization is concerned with public-key cryptosystems, RSA. Most of the current factorization tools, which are not user friendly, are console-based software on the Linux environment. Consequently, we designed a GUI factorization tool with multiple algorithms, especially elliptic curve method, on Windows platform and implemented it by Dev-C++. Furthermore, the graphical interface doesn't lower the efficiency.

Keywords: integer factorization, ECM, RSA

1 Introduction

"The study of theoretical and practical aspects of factoring algorithms is of continuing interest for the analysis of various well known public-key cryptosystems [1]." In this paper we present our effort in the implementation of a GUI factorization tool equipped with several algorithms.

1.1 Integer factorization

"Integer factorization is a subject of great importance in cryptology, and a constant concern for cryptographers. [2]" In RSA, two large prime numbers, p and q are chosen and they are the two factors of n used in RSA encryption and decryption. P and q are kept secret whereas n is public. If n is broken and factorized to get p and q, the security of RSA will be doubted, and that is what integer factorization does.

There are a variety of algorithms that are designed to solve factorization problem, such as Pollard p±1, Pollard rho, quadratic sieve, elliptic curve method, and so on. Most of current factorization tools using these algorithms are console-based software with command line on Linux platforms (Table 1) whereas Windows occupies 95% market share.

Table 1. Current factorization tools

Name	Platform	Algorithm
CALC	Linux/Dos	MPQS, ECM
GMP-ECM	Linux	ECM, Pollard±1
LiDIA	Linux	Pollard rho, ECM, MPQS..
MIRACL	Linux/Dos	Pollard rho, ECM, MPQS..
PARI/GP	Linux	Pollard rho, ECM, MPQS..
UBASIC [3]	Dos	MPQS, ECM

1.2 Elliptic curve method

The ECM method is a probabilistic method. It can be viewed in some sense as a generalization of the Pollard p-1 and p+1 method and they are all two stage method. We lay stress on elliptic curve method (ECM) especially. ECM is currently the best algorithm known, among those whose complexity depends mainly on the size of the factor found. Elliptic curves are in the form: $y^2 = ax^3 + bx + c$ [4]. As coefficients changes, a new curve will be generated to try another factorization action.

2 Design

2.1 MIRACL

"MIRACL (Multiprecision Integer and Rational Arithmetic C/C++ Library) is a big number library that implements all of the primitives necessary to design big number cryptography into application. [5]" It contains not only some cryptographic techniques such as RSA public key cryptography, Diffie-Hellman key exchange, but integer factorization that is

*Institute of Information and Computer Education, National Kaohsiung Normal University, 116, Ho Ping First Road, Kaohsiung 802, Taiwan
http://crypto.nknu.edu.tw
[1] Email: b88107042@ntu.edu.tw
[2] Email:chyang@computer.org
†Faculty of Computer Science and Electrical Engineering, Kyusyu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581

highlighted in this paper. The latest version is 4.85.

The algorithms of factorization embedded in MIRACL are as follows: trial division, Brent-Pollard, Pollard p-1, Williams p+1, elliptic curve method, and multiple polynomial quadratic sieve (MPQS).

2.2 GMP-ECM

GMP-ECM [6] was developed by Jim Fougeron, Laurent Fousse, Alexander Kruppa, Dave Newman and Paul Zimmermann, and is related to ECMNET project [7]. The goal of ECMNET is to find large factors that are mainly contributed to Cunningham project by ECM. The latest version is 6.0.1.

GMP-ECM which relies on GMP (GNU Multiple Precision Arithmetic Library) is an ECM based factorization tool. GMP is a free library for arbitrary precision arithmetic, operating on signed integers, rational numbers, and floating point numbers. It is applied to cryptography application and research, Internet security applications, algebra systems, computational algebra research and so on.

The algorithms used in GMP-ECM are elliptic curve method and Pollard±1. The property of GMP-ECM is that elliptic curve method algorithms can be handled arbitrarily by the setting of numerous parameters. "Up from version 6.0, GMP-ECM prints the expected number of curves and expected time to find factors of different sizes in verbose mode. This makes it easy to further optimize parameters for a certain factor size if desired, simply try to minimize the expected time. [6]"

GMP-ECM has a great performance and precision in ECM, and MIRACL has much more algorithms. As a result, in this paper we integrate GMP-ECM with MIRACL to accomplish a GUI factorization tool with multiple algorithms on Windows platforms.

3 Implementation

Since GMP and GMP-ECM were all developed under Linux environment and included m4 and macro assembly language, we chose Dev-C++ 4.9.9.2 [8] and MSYS1.0.10 as a software tool to adapt Linux-like environment for Windows. "Dev-C++ is a full-featured integrated development environment for the C/C++ programming language, and uses MinGW port of GCC as its compiler." Moreover, we used GUI component—GTK 2.0 [9] to implement the interface.

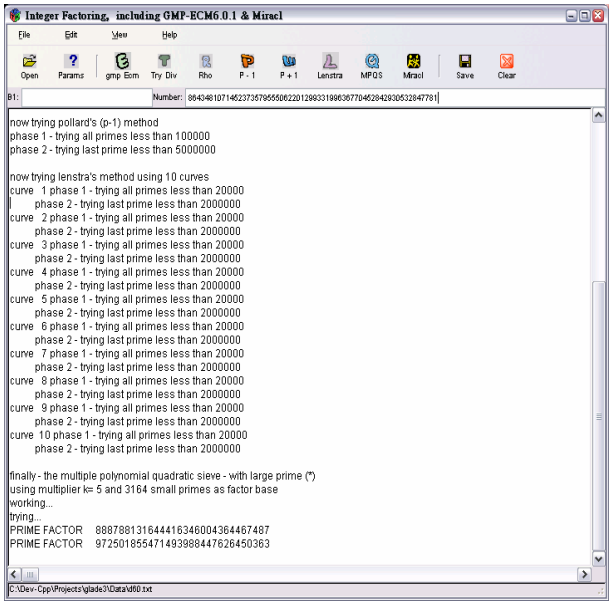

Figure 1. Implementation of GUI factorization tool

Figure 1 shows the tool we implemented. There are eight methods to factor a number in this tool. They are trial division, Brent-Pollard method, Pollard p-1, Williams p+1, MPQS, and ECM. Two elliptic curve methods can be chosen, and one is edited from GMP-ECM and the other is from MIRACL. The original function of MIRACL, factoring a number by running a series of algorithms like a relay race (trial division→Brent-Pollard→Pollard p-1→Williams p+1 → ECM→MPQS), is retained in the tool by clicking the "Miracl" button (Figure 1).

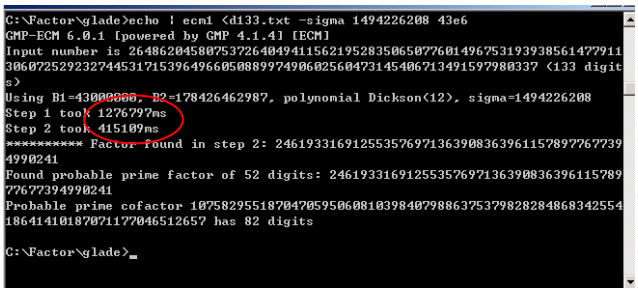

Figure 2. Factoring a133-digit number by GMP-ECM

The new tool is provided with user friendly interface and multiple algorithms on Windows Platform. Furthermore, we compared the graphical interface tool with original GMP-ECM and found that the graphical interface tool does not lower the efficiency. Figure 2 and 3 shows that the running time is almost the same. However, GMP-ECM may be quite memory expensive since its efficient algorithms use some large tables [6]. Figure 4 shows the setting of parameters of GMP-ECM. The memory usage can be reduced by increasing parameter "k".

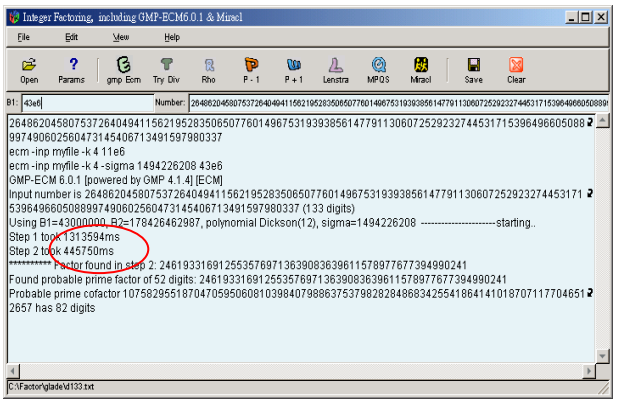

Figure 3. Factoring a 133-digit number by GUI tool

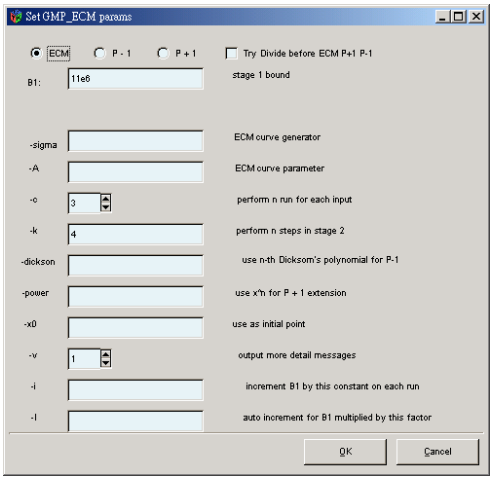

Figure 4. Parameter setting of ECM

4 Conclusions

The importance of integer factorization is undeniable because it accounts for the security of RSA that is still used prevalently. A secure and efficient key length will be changed and confirmed with the ability of integer factorization. In this paper, we have described our preliminary results on implementing an effective GUI factorization tool with multiple algorithms, like elliptic curve method, MPQS on Windows platform.

References

[1] B. Dixon, A. K. Lenstra, "Massively parallel elliptic curve factoring," Proc. Eurocrypt '92, Lecture Notes in Computer Science 658, 1993, p. 183-193

[2] A. K. Lenstra, M. S. Manasse, "Factoring with two large primes," Mathematics of Computation, vol. 63, 1994, p. 785-798

[3] Yuji Kida, "UBASIC", http://www.rkmath.rikkyo.ac.jp/~kida/ubasic.htm

[4] R. D. Silverman, Massively distributed computing and factoring large integers, Communications of the ACM, v.34 n.11, p.95-103, Nov. 1991

[5] Shamus Software Ltd., "MIRACL", http://indigo.ie/~mscott/

[6] P. Zimmermann et al., "GMP-ECM 6.0.1", http://www.komite.net/laurent/soft/ecm/ecm-6.0.1.html

[7] P. Zimmermann, "The ECMNET project", http://www.loria.fr/~zimmerma/records/ecmnet.html

[8] Bloodshed Software, "Dev-C++", http://www.bloodshed.net/devcpp.html

[9] GTK.org, "The GIMP Toolkit", http://www.gtk.org/