Implementing a Feasible Attack against ECC2K-130 Certicom Challenge

Ahmad Lavasani*, Reza Mohammadi **

Department of Mathematics and Statistics, Concordia University

* ahmad.lavasani@gmail.com

Department of Mathematical Sciences, Sharif University of Technology

** remohammadi@gmail.com

June 12, 2008

Abstract

Popularity of Elliptic Curve Cryptography (ECC) is increasing compared to other common Public Key Cryptosystems such as RSA and DSA due to the more efficient cryptosystem scheme that they offer in the terms of memory and bandwith. In November 1997, Certicom introduced the ECC Challenge in order to appreciate the evaluation of ECC Cryptography. To date, all 109-bit ECC challenges have been solved and the easiest unsolved challenge is the ECC2K-130 problem.

The curve used in ECC2K-130 is the unique Koblitz Curve [5] defined over GF(2^{131}). The best known attack for a general elliptic curve is Parallel Pollard's Rho attack (known also as Pollard's Lambda) suggested by van Oorschot and Wiener [6]. This method can be improved significantly for Koblitz Curves using the method of Wiener and Zuccherato [7].

In this work, based on the implementation of Robert Harley and his team [8] who broke the last Koblitz Curve Challenge of Certicom, ECC2K-108, on April 2000 [9], we aim to mount a Pollard's Lambda attack to break ECC2K-130. We present different aspects of efficiently attacking ECC2K-130. In this way we employed new technological advancement such as SSE2 (Streaming SIMD Extensions 2) registers to speed up the arithmetic used in the attack. We also studied and compared different random walk functions and chose the function that exploits the Frobenius Automorphism while minimizing overhead in each iteration. We also improve some of critical algorithms, such as the bit-counting algorithm and GF(2^{131})-product to take advantage of CPU structure and our point representation.

By employing Berkeley Open Infrastructure for Network Computing (BOINC), we obtained a more interactive way to manage the distributed computation. This may improve the performance of the attack in several ways. For example, we can save the computation spent on a trail which does not terminate at a distinguished point. Another example is the

ability of centrally supervising clients' performances and adjusting clients' parameters individually to reach their optimum performance.

The practical results we obtained from our current running implementation suggest that the attack would successfully solve the challenge in a feasible amount of time (a conservative time estimate would be less than 2 years using 20,000 partially active computers).

References

[1] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48 (1987), pp. 203-209.

[2] J. Silverman, J. Suzuki, Elliptic curve discrete logarithms and the index calculus, Ad- vances in CryptologyASIACRYPT98, Beijing, October 1998, ed. by K. Ohta and D. Pei, Lecture Notes in Computer Science 1514, Springer-Verlag, Berlin, 1998, 110125

[3] http://www.certicom.com/index.php?action=company,press_archive&view=307

[4] http://www.certicom.com/index.php?action=ecc,ecc_challenge

[5] N.Koblitz.CMcurves with good cryptographic properties, Proc. Crypto 91, Springer-Verlag (1992) pp. 279 287

[6] P.C. van Oorschot, M.J. Wiener, Parallel collision search with cryptanalytic appli- cations, Journal of Cryptology, vol 12, num 1, pp 1-28, Winter 1999, Springer-Verlag.

[7] M. J. Wiener and R. Zuccherato, Faster Attacks on Elliptic Curve Cryptosystems, Selected Areas of Cryptography, Springer, LNCS 1556, pp. 190200, 1999.

[8] http://cristal.inria.fr/ harley/ecdl7/readMe.html

[9] http://www.inria.fr/presse/pre67.en.html

[10] http://www.certicom.com/index.php?action=ecc,ecc_challenge

[11] D. Hankerson, A. J. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer- Verlag, 2004.

[12] R.Gallant, R.Lambert,and S.Vanstone, Improving the parallelized Pollard lambda search on anomalous binary curves. Math. Comp. 69 (2000), no. 232, 16991705