Elliptic Curve Discrete Logarithm Problem

Darrel Hankerson (Auburn University)
Alfred Menezes (University of Waterloo)

May 11, 2004

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and let $P \in E(\mathbb{F}_q)$ be a point of order n. Given $Q \in \langle P \rangle$, the elliptic curve discrete logarithm problem (ECDLP) is to find the integer l, $0 \leq l \leq n-1$, such that $Q = lP$.

The ECDLP is a special case of the discrete logarithm problem in which the cyclic group G is represented by the group $\langle P \rangle$ of points on an elliptic curve. It is of cryptographic interest because its apparent intractability is the basis for the security of elliptic curve cryptography.

If the order n of the base point P is composite and its factorization is known, then the Pohlig-Hellman algorithm [14] (see the discrete logarithm problem entry) can be used to efficiently reduce the ECDLP in $\langle P \rangle$ to instances of the ECDLP in proper subgroups of $\langle P \rangle$. Thus, the difficulty of the original ECDLP instance depends on the size of the largest prime factor of n. In order to maximize resistance to the Pohlig-Hellman algorithm, n should be prime, as we will henceforth assume.

1 Pollard's ρ method

Pollard's ρ method [15] (see Pollard's λ and ρ methods) is the best general-purpose algorithm known for solving the ECDLP. The algorithm, as improved by Teske [21], has an expected running time of $\sqrt{\pi n/2}$ elliptic curve operations and has negligible storage requirements. Van Oorschot and Wiener [22] showed how Pollard's ρ method can be effectively parallelized so that r processors could jointly work on solving one ECDLP instance with a net speedup by a factor of r. The processors do not have to communicate with each other, and only occasionally transmit data to a central processor. This method is also called parallel collision search (see discrete logarithm problem).

Gallant, Lambert and Vanstone [4] and Wiener and Zuccherato [23] observed that Pollard's ρ method can be modified to operate on equivalence classes determined by the negation map acting on points (which maps a point P to $-P$), rather than on points themselves. The running time of this modified version is

$$(\sqrt{\pi n})/2,$$

a speedup by a factor of $\sqrt{2}$.

Gallant, Lambert and Vanstone [4] and Wiener and Zuccherato [23] also observed that Pollard's ρ method can be accelerated by exploiting other efficiently-computable endomorphisms of an elliptic curve. For the two *Koblitz elliptic curves* (also known as *anomalous binary curves*) which are defined over $\mathbb{F}_2$ by the equations $y^2 + xy = x^3 + 1$ and $y^2 + xy = x^3 + x^2 + 1$, the *Frobenius map* $\phi : (x, y) \mapsto (x^2, y^2)$ is an endomorphism on $E(\mathbb{F}_{2^m})$ and can be efficiently computed. By operating on the equivalence classes of points determined by the negation and Frobenius maps, Pollard's ρ method for Koblitz curves can be accelerated further by a factor of $\sqrt{m}$ for a resulting running time of

$$(\sqrt{\pi n})/2\sqrt{m}.$$

The parallelized version of Pollard's ρ algorithm has been used in practice to solve several ECC challenges.

2 Index-calculus methods

Unlike the case of the discrete logarithm problem in the multiplicative group of a finite field, there is no index-calculus method known for solving the ECDLP that has a subexponential (or better) running time. No appropriate choice is known for the elements of the factor base required in the index-calculus method. In the case of elliptic curves over prime fields, the most natural choice for factor base elements is obtained by regarding an elliptic curve point as having coordinates in the field of the rational numbers, and selecting those points that have small *height*. Miller [13] and Silverman and Suzuki [19] presented convincing arguments why this approach is doomed to fail.

Silverman [18] proposed a different idea for attacking the ECDLP, which he termed *xedni calculus*. Shortly after, Jacobson et al. [7] gave compelling theoretical and experimental evidence why xedni calculus would be ineffective for solving the ECDLP.

3 Special-purpose algorithms

Algorithms that are faster than Pollard's ρ method for solving the ECDLP are known for some special classes of elliptic curves. When selecting an elliptic curve for use in a cryptographic scheme, one should verify that the elliptic curve chosen is not vulnerable to these special-purpose attacks.

3.1 Attack on prime-field anomalous curves

An elliptic curve E over a prime field $\mathbb{F}_p$ is said to be *prime-field anomalous* if the number of points in $E(\mathbb{F}_p)$ is equal to p. Satoh and Araki [16], Semaev [17], and Smart [20] showed that for such curves, the ECDLP in $E(\mathbb{F}_p)$ can be efficiently solved. Hence, when selecting an elliptic curve E over a prime field $\mathbb{F}_p$ for cryptographic use, it is important to verify that $\#E(\mathbb{F}_p) \neq p$.

3.2 Weil and Tate pairing attacks

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Menezes, Okamoto and Vanstone [10] and Frey and Rück [3] showed how the *Weil* and *Tate pairings* can be used to efficiently reduce the ECDLP in $E(\mathbb{F}_q)$ to the discrete logarithm problem in the multiplicative group of an extension field $\mathbb{F}_{q^k}$, where subexponential-time index calculus methods are known. The reduction is only useful for solving the ECDLP instance if the discrete logarithm problem in $\mathbb{F}_{q^k}$ is tractable—this imposes the restriction that k not be too large. Now, the smallest permissible value for the extension degree k is the smallest integer k such that n divides $q^k - 1$. Hence by verifying that n does not divide $q^k - 1$ for all integers $k \in [1, c]$ (where c is chosen so that the discrete logarithm problem in $\mathbb{F}_{q^c}$ is deemed to be intractable), the Weil and Tate pairing attacks can be circumvented.

3.3 Weil descent

Frey [2] proposed a general methodology using *Weil descent* for reducing the ECDLP in an elliptic curve E over a characteristic two finite field $\mathbb{F}_{2^m}$ to the discrete logarithm problem in the jacobian $J_C(\mathbb{F}_{2^n})$ of an algebraic curve C defined over a subfield $\mathbb{F}_{2^n}$ of $\mathbb{F}_{2^m}$. Gaudry, Hess and Smart [6] gave an explicit algorithm for the case where C is a hyperelliptic curve of genus g defined over $\mathbb{F}_{2^n}$; their method is called the *GHS attack*. Since subexponential-time algorithms are known for the discrete logarithm problem in high genus hyperelliptic curves (see [1] and [5]), the GHS attack can potentially solve the ECDLP faster than Pollard's ρ method.

Menezes and Qu [11] showed that the GHS attack is slower than Pollard's ρ method for all elliptic curves defined over finite fields $\mathbb{F}_{2^m}$ where m is prime and $m \in [160, 600]$. Thus the GHS attack is ineffective for elliptic curves over these fields.

The GHS attack for elliptic curves over $\mathbb{F}_{2^m}$ where m is composite has been extensively analyzed (see [8], [9] and [12]). This body of work shows that the GHS attack is indeed effective in solving the ECDLP for some elliptic curves over some fields $\mathbb{F}_{2^m}$ with m composite. In view of these attacks, it seems prudent to avoid use of elliptic curves over finite fields $\mathbb{F}_{2^m}$ where m is composite.

References

[1] L. Adleman, J. DeMarrais and M. Huang, "A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields", *Algorithmic Number Theory—ANTS-I*, Lecture Notes in Computer Science 877 (1994), Springer-Verlag, 28-40.

[2] G. Frey, "Applications of arithmetical geometry to cryptographic constructions", *Proceedings of the Fifth International Conference on Finite Fields and Applications*, Springer-Verlag, 2001, 128-161.

[3] G. Frey and H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of Computation* 62 (1994), 865-874.

[4] R. Gallant, R. Lambert and S. Vanstone, "Improving the parallelized Pollard lambda search on anomalous binary curves", *Mathematics of Computation* 69 (2000), 1699-1705.

[5] P. Gaudry, "An algorithm for solving the discrete log problem in hyperelliptic curves", *Advances in Cryptology—EUROCRYPT 2000*, Lecture Notes in Computer Science 1807 (2000), Springer-Verlag, 19-34.

[6] P. Gaudry, F. Hess and N. Smart, "Constructive and destructive facets of Weil descent on elliptic curves", *Journal of Cryptology* 15 (2002), 19-46.

[7] M. Jacobson, N. Koblitz, J. Silverman, A. Stein and E. Teske, "Analysis of the xedni calculus attack", *Designs, Codes and Cryptography* 20 (2000), 41-64.

[8] M. Jacobson, A. Menezes and A, Stein, "Solving elliptic curve discrete logarithm problems using Weil descent", *Journal of the Ramanujan Mathematical Society* 16 (2001), 231-260.

[9] M. Maurer, A. Menezes and E. Teske, "Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree", *LMS Journal of Computation and Mathematics* 5 (2002), 127-174.

[10] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory* 39 (1993), 1639-1646.

[11] A. Menezes and M. Qu, "Analysis of the Weil descent attack of Gaudry, Hess and Smart", *Topics in Cryptology—CT-RSA 2001*, Lecture Notes in Computer Science 2020 (2001), Springer-Verlag, 308-318.

[12] A. Menezes, E. Teske and A. Weng, "Weak fields for ECC", *Topics in Cryptology–CT-RSA 2004*, Lecture Notes in Computer Science 2964 (2004), Springer-Verlag, 366-386.

[13] V. Miller, "Use of elliptic curves in cryptography", *Advances in Cryptology—CRYPTO '85*, Lecture Notes in Computer Science 218 (1986), Springer-Verlag, 417-426.

[14] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance", *IEEE Transactions on Information Theory* 24 (1978), 106-110.

[15] J. Pollard, "Monte Carlo methods for index computation (mod p)", *Mathematics of Computation* 32 (1978), 918-924.

[16] T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves", *Commentarii Mathematici Universitatis Sancti Pauli* 47 (1998), 81-92.

[17] I. Semaev, "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p", *Mathematics of Computation* 67 (1998), 353-356.

[18] J. Silverman, "The xedni calculus and the elliptic curve discrete logarithm problem", *Designs, Codes and Cryptography* 20 (2000), 5-40.

[19] J. Silverman and J. Suzuki, "Elliptic curve discrete logarithms and the index calculus", *Advances in Cryptology—ASIACRYPT '98*, Lecture Notes in Computer Science 1514 (1998), Springer-Verlag, 110-125.

[20] N. Smart, "The discrete logarithm problem on elliptic curves of trace one", *Journal of Cryptology* 12 (1999), 193-196.

[21] E. Teske, "Speeding up Pollard's rho method for computing discrete logarithms", *Algorithmic Number Theory—ANTS-III*, Lecture Notes in Computer Science 1423 (1998), Springer-Verlag, 541-554.

[22] P. van Oorschot and M. Wiener, "Parallel collision search with cryptanalytic applications", *Journal of Cryptology* 12 (1999), 1-28.

[23] M. Wiener and R. Zuccherato, "Faster attacks on elliptic curve cryptosystems", *Selected Areas in Cryptography—SAC '98*, Lecture Notes in Computer Science 1556 (1999), Springer-Verlag, 190-200.