Reducing Certain Elliptic Curve Discrete Logarithms to Logarithms in a Finite Field

Kyungah Shim

KISA (Korea Information Security Agency)
5th FL., Dong-A Tower, Seocho-Dong, Seocho-Gu, Seoul 137-070, Korea
kashim@kisa.or.kr

Abstract. We construct a variant of Weil pairing to reduce the elliptic curve discrete logarithm problem to the discrete logarithm problem in the multiplicative subgroup of a finite field. We propose an explicit reduction algorithm using a new pairing and apply the algorithm to the case of two trace elliptic curves.

Key words : Anomalous curve, supersingular curve, Weil pairing, elliptic curve discrete logarithm.

1 Introduction

The discrete logarithm problem for a general group G can be stated as follows: given $\alpha \in G$ and $\beta \in G$, find an integer x such that $\beta = \alpha^x$, provided that such an integer exists. The integer x is called the *discrete logarithm* of β to the base α. If we replace the group G by the elliptic curve group over a finite field then it is the elliptic curve discrete logarithm problem (ECDLP).

In [4] and [7], Koblitz and Miller independently propose how to use the group of points on an elliptic curve over a finite field to construct public key cryptosystems. The security of these cryptosystems is based upon the presumed intractability of computing logarithms in the elliptic curve group. The best algorithms known for solving this problem are the exponential square root attacks that can be applied to any finite group and have a running time that is proportional to the square root of the largest prime factor dividing the order of the group. In [7], Miller argues that the index-calculus methods, which produced dramatic results in the computation of discrete logarithms in the multiplicative subgroup of a finite field, do not extend to elliptic curve groups. Consequently, if the elliptic curve is chosen so that its order is divisible by a large prime, then even the best attacks take exponential time.

The integrity of ECDLP cryptographic tools would be widely accepted, however, there exist two exceptional families of elliptic curves (i.e., supersingular and anomalous curves) and for each case powerful cryptanalysis method has been invented. But both classes of elliptic curves may be easily avoided in practice.

At first Menezes, Okamoto and Vanstone [6] propose a subexponential time algorithm to solve the ECDLP over a supersingular elliptic curve E defined over a finite field F_q $(q = p^n,\ p > 3)$, the so-called MOV algorithm. It employed the Weil

V. Varadharajan and Y. Mu (Eds.): ACISP 2001, LNCS 2119, pp. 514–520, 2001.

pairing to reduce ECDLP to the discrete logarithm problem in a multiplicative subgroup of an extension field F_{q^k} of F_q, $k \leq 6$. By using a variant of the Tate pairing, Frey and Rück [2] gave a generalization of this the discrete logarithm over the divisor class group of curves, we call this algorithm the FR algorithm. Furthermore, Balasubramanian and Koblitz [1] showed that if we choose an elliptic curve at random over a prime finite field F_p whose number of F_p-rational points is prime, then the MOV algorithm on that curve is not effective with overwhelming probability.

Recently, Semaev [9], Smart [11], and Satoh and Araki [8] independently proposed a polynomial time algorithm (SSSA algorithm) for the ECDLP over an anomalous elliptic curve defined over a prime field F_p, i.e., an elliptic curve over F_p whose number of F_p-points is p. It is easy to see that we can also apply the SSSA algorithm to the discrete logarithm problem over the p-part of $E(F_q)$, where q is a power of p. Semaev employs an algebraic geometrical approach, while Smart and Satoh-Araki employ a number theoretical approach to reduce the ECDLP over E to the additive group F_p.

In this paper, we present the following results;

1. We construct a variant of Weil pairing to reduce the ECDLP defined over F_q to the discrete logarithm problem in F_q^*.
2. We propose an efficient reduction algorithm for ECDLP over elliptic curves with trace two, more generally, elliptic curves with even trace under a special condition.

2 Construction of Bilinear Pairing

We want to construct a certain variant of Weil pairing with simple computation. Let E be an elliptic curve defined over a finite field F_q where $q = p^n$ for some prime $p \neq 2, 3$. Let $E(F_q)$ be the group of rational points of E over F_q. Suppose that $E(F_q)$ contains a 2-torsion point and let a be a 2-torsion point in $E(F_q)$. If a divisor $D_1 = div(f)$ is principal, for any $D_2 = \sum_{i=1}^{r} n_i(a_i) \in \mathrm{Div}^0(E)_{F_q}$ such that $\mathrm{supp}(D_1) \cap \mathrm{supp}(D_2) = \emptyset$, we let $f(D_2) \equiv \prod_{i=1}^{r} f(a_i)^{n_i}$ where $\mathrm{Div}^0(E)_{F_q}$ is the group of divisors of degree zero whose components are F_q-rational. This value depends only on f since the constant disappears when taking the product over the points of a divisor of degree zero. We can define a bilinear pairing from $E(F_q) \times E(F_q)$ to F_q^* in the following way,

$$< \cdot, \cdot >_a : E(F_q) \times E(F_q) \to F_q^*, \; < P, Q >_a \equiv f_{\bar{P}}(\bar{Q}) / f_{\bar{Q}}(\bar{P}). \tag{1}$$

where $\bar{P}$ is a divisor $(P) - (O)$ corresponding to a point $P \in E(F_q)$ via an isomorphism from E to the divisor class group of E, $\mathrm{Pic}^0(E)$. We can deduce that $\bar{P}_a - \bar{P} = (P + a) - (a) - (P) + (O)$ is a principal divisor, by Cor 3.5 (pp. 67) of [10], namely, there exists a rational function $f_{\bar{P}}$ such that

$$div(f_{\bar{P}}) = (P + a) - (a) - (P) + (O).$$

Similarly, there exists a rational function such that

$$div(f_{\bar{Q}}) = (Q+a) - (a) - (Q) + (O).$$

These rational functions are uniquely determined up to constants. In fact, this pairing is similar to the Weil pairing on the group of m-torsion point of elliptic curve E.

Theorem 1. *For the pairing $< \cdot, \cdot >_a$ given in (1), we have the following properties.*

1. *$< \cdot, \cdot >_a$ depends only on the divisor class.*
2. *It is a bilinear pairing.*
3. *It is alternative, i.e.,$< P, Q >_a = < Q, P >_a^{-1}$.*

Proof. (1) Let $\bar{P}'$ be linearly equivalent to $\bar{P}$. Then we can express as $\bar{P}' = \bar{P} + (g)$ for some rational function g. Thus we get

$$(f_{\bar{P}'}) = \bar{P}'_a - \bar{P}' = \bar{P}_a - \bar{P} + (g)_a - (g) = (f_{\bar{P}}) + (g)_a - (g).$$

The value of $< P, Q >_a$ for $\bar{P}'$ is

$$\frac{f_{\bar{P}'}(\bar{Q})}{f_{\bar{Q}}(\bar{P}')} = \frac{f_{\bar{P}}(\bar{Q}) g(Q-a) g(-a)^{-1} g(0) g(Q)^{-1}}{f_{\bar{Q}}(\bar{P}) f_{\bar{Q}}((g))}.$$

Since a is a 2-torsion point, i.e., $a = -a$,

$$\frac{g(Q-a)g(O)}{g(Q)g(-a)} = \frac{g(Q+a)g(O)}{g(Q)g(a)} = g((f_{\bar{Q}})),$$

and by Weil reciprocity law in Lang [5], pp.172, we have $f_{\bar{Q}}((g)) = g((f_{\bar{Q}}))$. Hence we conclude that

$$\frac{f_{\bar{P}'}(\bar{Q})}{f_{\bar{Q}}(\bar{P}')} = \frac{f_{\bar{P}}(\bar{Q})}{f_{\bar{Q}}(\bar{P})},$$

namely, it is independent of the choice of a divisor in the same divisor class. Similarly, it is well-defined with respect to the second variable. If supp$((f_{\bar{P}})) \cap$ supp$(\bar{Q}) \neq \emptyset$, then we can find a divisor $\bar{Q}' = \bar{Q} + (g)$ such that supp$((f_{\bar{P}})) \cap$ supp$(\bar{Q}') = \emptyset$. Thus we can avoid the points at which the rational function are not defined.

(2) We show $< P_1 + P_2, Q >_a = < P_1, Q >_a < P_2, Q >_a$. Since $\overline{P_1 + P_2}$ is linearly equivalent to $\bar{P}_1 + \bar{P}_2$, we get

$$(P_1 + P_2) - (0) \sim (P_1) - (0) + (P_2) - (0)$$

by the square theorem [5]. Thus we have

$$\frac{f_{\overline{P_1+P_2}}(\bar{Q})}{f_{\bar{Q}}(\overline{P_1+P_2})} = \frac{f_{\bar{P}_1+\bar{P}_2}(\bar{Q})}{f_{\bar{Q}}(\bar{P}_1+\bar{P}_2)} = \frac{f_{\bar{P}_1}(\bar{Q}) f_{\bar{P}_2}(\bar{Q})}{f_{\bar{Q}}(\bar{P}_1) f_{\bar{Q}}(\bar{P}_2)} = < P_1, Q >_a < P_2, Q >_a .$$

It is also linear with respect to the second variable by the similar way.

(3) It is obvious by definition.

We can easily find our rational functions in computation of the pairing of (1) using the following algorithm.

Algorithm 1

[**Description**] Algorithm for finding a rational function over E with a given divisor.
[**Input**] A divisor of the form $(P+Q)-(P)-(Q)+(0)$ where $P, Q \in E(F_q)$.
[**Output**] A rational function g such that $(P+Q)-(P)-(Q)+(O)=(g)$.

1. Find a line equation $L: f(x,y,z) = ax+by+cz = 0$ in P^2 through P and Q where $a, b, c \in F_q$.
2. Compute R the point of intersection of L with E.
3. Find a line equation $L' : f'(x,y,z) = a'x+b'y+c'z = 0$ in P^2 through R and O where $a', b', c' \in F_q$.
4. Output $g = f'/f$.

How the algorithm yields an easy way to compute the rational function g; for a given divisor $\bar{P} = (P)-(O)$, let $f(x,y,z) = ax+by+cz = 0$ be the line L in P^2 through P and Q. Also let R be the point of intersection of L with E and $f'(x,y,z) = a'x+b'y+c'z = 0$ the line L' through R and O. Then, from the definition of addition on E and the fact that the line $z = 0$ intersects E at O with multiplicity 3, we have

$$div(f/z) = (P)+(Q)+(R)-3(O)$$

and

$$div(f'/z) = (R)+(P+Q)-2(O).$$

Hence

$$(P+Q)-(P)-(Q)+(O) = div(f'/f).$$

The rational function f'/f is the function for which we are looking.

Remark 2.2

1. In fact, for general elliptic curves the image of this pairing is very tiny. Let N be the order of the elliptic curve E then we have

   $$1 = < NP, NQ >_a = < P, Q >_a^{N^2} .$$

   Hence $< P, Q >_a$ has a order dividing $\gcd(N^2, q-1)$. Thus this technique is meaningful when $N = q-1$ or $\gcd(N, q-1)$ is of size almost that of q, as will be seen in the next section.
2. The similar procedure can be used to compute $< \cdot, \cdot >_a$ in the case J is the Jacobian variety of a hyperelliptic curve.

3 The Reduction

In fact, the condition of the extension degree for the FR algorithm is usually weaker than that for the MOV algorithm, theorem 4.2 in [3] shows that the condition $q^k \equiv 1 \pmod{l}$ is equivalent to the condition $E[\ell] \subset E(F_{q^k})$ if $\ell \not| q-1 \pmod{\ell}$, i.e., the effectiveness of the MOV algorithm is the same as that of the FR algorithm if $q \equiv 1 \pmod{\ell}$. The extension degree k is exponential in $\log q$ when $\ell \,|q-1$. We consider the case of $\ell \,|q-1$.

From a standard cryptographic view point, let $|E(F_q)| = 2 \cdot \ell$, we may assume that ℓ is around q, then it is easy to see $|E(F_q)| = q-1$ when $\ell \,|q-1$. Suppose that ℓ is a prime number. Let $P \in E(F_q)$ be an element of order ℓ and $R \in < P >$. Let $a \neq O$ be a 2-torsion point in $E(F_q)$. With the pairing described in section 2, we can obtain the following theorem.

Theorem 2. *There exists some point $Q \in E(F_q)$ such that the map $\phi_{Q,a}; < P > \longrightarrow G$ defined by $\phi_{Q,a}(R) = < Q, R >_a$ is a group isomorphism where G is a unique cyclic subgroup of F_q^*.*

Proof. There exists a unique 2-torsion point $a = -a$ since ℓ is prime. This we need not worry about the choice of the 2-torsion point. If we take Q be a non 2-torsion point in $E(F_q)$ then we have an one to one homomorphism $\phi_{Q,a} :< P > \longrightarrow F_q^*$ since $< P >$ has a prime order.

We can introduce the following algorithm to reduce the ECDLP when $|E(F_q)| = q-1 = 2 \cdot \ell$ where ℓ is a prime number, to the discrete logarithm problem in the multiplicative subgroup of a underlying finite field.

Algorithm 2

[**Description**] Reduction the discrete logarithm on $E(F_q)$ to the discrete logarithm in F_q^*
[**Input**] An element $P \in E(F_q)$ of order ℓ, $R \in < P >$.
[**Output**] An integer m such that $R = mP$.

1. Find $Q \in E(F_q)$ such that $\alpha = \phi_{Q,a}(P)$ has order ℓ.
2. Compute $\beta = \phi_{Q,a}(R)$.
3. Compute m, the discrete logarithm of β to the base α in F_q^*.

Note that the output of Algorithm 2 is correct since

$$\beta = \phi_{Q,a}(mP) =< Q, mP >_a =< Q, P >_a^m = \alpha^m.$$

Thus, in this case, the reduction step of Algorithm 2 takes polynomial time resulting in a probabilistic subexponential time algorithm for computing elliptic curve discrete logarithms in these curves. Thus, to select a secure elliptic curve, we must avoid elliptic curves of trace 2.

Remark 3.1

1. In our cases, which are important ones for cryptographic reasons, unlike Algorithm 2 in MOV reduction, which can choose a point Q probabilistically, we can determine a point Q easily, because every non 2-torsion point of $E(F_q)$ has a prime order ℓ. Consequently, (1) in Algorithm 2 is independent to the choice of a point Q such that $2Q \neq O$.
2. We can compare our pairing with Weil pairing and Tate-Lichtenbaum pairing. The fast algorithm used to compute the Weil pairing following V. Miller consists in a twofold computation of the Tate-Lichtenbaum pairing. But the Tate-Lichtenbaum pairing is computable in $O(\log q)$ steps, where one step is equivalent to the addition in $E(F_q)$. But the computation of our pairing is much simpler than that of Tate-Lichtenbaum pairing because the computation takes a constant number of multiplications in F_q^*.
3. In [3], Kanayama *et al.*, also proposed a reduction algorithm (KKSU algorithm) for the ECDLP over trace two elliptic curves. Their algorithm differ from the FR algorithm is faster than the FR algorithm. They confirmed that the reduction part of the proposed algorithm was 1.5 times faster than that of the FR algorithm. However the reduction part of our algorithm is faster than the KKSU algorithm since the computation of the pairing used to reduction consists of only a constant number of multiplications in F_q^*.
4. We know that, to resist the MOV attack, one only needs to check that n, the order of point P, does not divide $q^k - 1$ for all small k foe which the DLP in F_{q^k} is tractable- in practice, when $n > 2^{160}$ then $1 \leq k \leq 20$ suffices. More generally, the divisible check rules out all elliptic curves for which the ECDLP can be efficiently reduced to the DLP in some small extension of F_q. These include the elliptic curves of trace 2 as well as supersingular elliptic curves.

We conclude that the we can reduce the discrete logarithm problem on trace two elliptic curves defined over F_q to the discrete logarithm problem on the multiplicative subgroup of a underlying finite field F_q.

References

1. R. Balasubramanian and N. Koblitz, Improbability that an elliptic curve has subexponential discrete logarithm problem under the Menezes-Okamoto-Vanstone algorithm, Journal of cryptology, vol. 2, no. 11 (1998), pp. 141-145.
2. G. Frey and H. G. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Mathematics of Computation, vol. 62 (1994), pp. 865-874.
3. N. Kanayama, T. Kobayashi, T. Satoh and S. Uchiyama, Remarks on elliptic curve discrete logarithm problem, IEICE Transaction Fundamentals, vol. E83-A, no. 1 (2000), pp. 17-23.
4. N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, vol. 48 (1987), pp. 203-209.

5. S. Lang, Abelian varieties, Springer Verlag, New York, 1983.
6. A. J. Menezes, T. Okamoto and S. A. Vanstone, Reducing elliptic curve logarithms in a finite field, IEEE Transaction on Information Theory, vol. 39, no. 5 (1993), pp. 1639-1646.
7. V. Miller, Use of elliptic curves in cryptography, Advances in cryptology; Proceedings of Crypto'85, LNCS, 218 (1986), Springer-Verlag.
8. T. Satoh, K. Araki, Fermat quotients and the polynomial time discrete logarithm algorithm for anomalous elliptic curves, Proc. of algebraic number theory and its related topics, Koukyuuroku vol. 1026 (1998), pp. 139-150.
9. J. A. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curves in characteristic p, Mathematics of Computation, vol. 67 (1998), pp. 353-356.
10. J. H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, 1986.
11. N. P. Smart, The discrete logarithm problem on elliptic curves of trace one, Journal of Cryptology, vol. 12 (1999), pp.193-196.