The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences

Kristin E. Lauter[1] and Katherine E. Stange[2,*]

[1] Microsoft Research, One Microsoft Way, Redmond, WA 98052
klauter@microsoft.com
[2] Department of Mathematics, Harvard University, Cambridge, MA 02138
stange@math.harvard.edu

Abstract. We define three hard problems in the theory of elliptic divisibility sequences (*EDS Association*, *EDS Residue* and *EDS Discrete Log*), each of which is solvable in sub-exponential time if and only if the elliptic curve discrete logarithm problem is solvable in sub-exponential time. We also relate the problem of EDS Association to the Tate pairing and the MOV, Frey-Rück and Shipsey EDS attacks on the elliptic curve discrete logarithm problem in the cases where these apply.

1 Introduction

The security of elliptic curve cryptography rests on the assumption that the *elliptic curve discrete logarithm problem* is hard.

Problem 1 (Elliptic Curve Discrete Logarithm Problem (ECDLP)). Let E be an elliptic curve over a finite field K. Suppose there are points $P, Q \in E(K)$ given such that $Q \in \langle P \rangle$. Determine k such that $Q = [k]P$.

In this article, we explore several related hard problems with a view to expanding the theoretical foundations of the security of ECDLP as a hard problem. Our research is inspired by work of Rachel Shipsey in her thesis [1], relating the ECDLP to elliptic divisibility sequences (EDS). An elliptic divisibility sequence is a recurrence sequence $W(n)$ satisfying the relation

$$W(n+m)W(n-m) = W(n+1)W(n-1)W(m)^2 - W(m+1)W(m-1)W(n)^2.$$

We relate Shipsey's work to the MOV and Frey-Rück attacks and explain their limitations from the EDS point of view. We also point to a specific avenue for attacking ECDLP by analysing the quadratic residuosity of elliptic divisibility sequences.

The study of elliptic divisibility sequences was introduced by Morgan Ward [2]. Let Ψ_n denote the n-th division polynomial of an elliptic curve E over the

* The second author was supported by NSERC Award PGS D2 331379-2006, and this work was performed during an internship of the second author at Microsoft Research.

rationals. The sequence $W_{E,P} : \mathbb{Z} \to \mathbb{Q}$ of the form $W_{E,P}(n) = \Psi_n(P)$ for some fixed point $P \in E(\mathbb{Q})$ is an elliptic divisibility sequence, and Ward showed that almost all elliptic divisibility sequences arise in this way. This relationship is the basis of our work here.

The general theory has been developed by Swart [3], Ayad [4], Silverman [5][6], Everest, McLaren and Thomas Ward [7] and, more recently, generalised to higher rank *elliptic nets* by Stange [8][9]. For an overview of research, see [10]. Sections 2 and 3 provide brief background on elliptic divisibility sequences and elliptic nets, more information about which can be found in [8][9][11].

The hard problems for elliptic divisibility sequences we consider are:

Problem 2 (EDS Association). Let E be an elliptic curve over a finite field K. Suppose there are points $P, Q \in E(K)$ given such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, and $\mathrm{ord}(P) \geq 4$. Determine $W_{E,P}(k)$ for $0 < k < \mathrm{ord}(P)$ such that $Q = [k]P$.

Problem 3 (EDS Residue). Let E be an elliptic curve over a finite field K. Suppose there are points $P, Q \in E(K)$ given such that $Q \in \langle P \rangle$, $Q \neq \mathcal{O}$, and $\mathrm{ord}(P) \geq 4$. Determine the quadratic residuosity of $W_{E,P}(k)$ for $0 < k < \mathrm{ord}(P)$ such that $Q = [k]P$.

Problem 4 (Width s EDS Discrete Log). Given an elliptic divisibility sequence W and terms $W(k)$, $W(k+1)$, …, $W(k+s-1)$, determine k.

Problem 4 was considered by Shipsey [1, §6.3.1] and Gosper, Orman and Schroeppel [12, §3]. Problem 2 is also implicit in [1, §6.4.1] and [12, §3].

A perfectly periodic elliptic divisibility sequence is one which has a finite period n and whose first positive index k at which $W(k) = 0$ is $k = n$. If a sequence is not perfectly periodic, then it has period $n > k$. In Section 10, we prove the following theorem.

Theorem 1. *Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$ of characteristic $\neq 2$. If any one of the following problems is solvable in sub-exponential time, then all of them are:*

1. *Problem 1: ECDLP*
2. *Problem 2: EDS Association for non-perfectly periodic sequences*
3. *Problem 3: EDS Residue for non-perfectly periodic sequences*
4. *Problem 4 ($s = 3$): Width 3 EDS Discrete Log for perfectly periodic sequences*

Section 4 relates Problems 4 and 2 to the ECDLP. Section 6 expands on Problem 2. Sections 7 and 8 discuss Problem 3. Section 9 remarks on Problem 4. Section 10 proves Theorem 1. The relation with the MOV and Frey-Rück attacks is discussed in Section 5.

The authors would like to thank the referees for their helpful suggestions.

2 Background on Elliptic Nets

In this section we state the background definitions and results on elliptic divisibility sequences and elliptic nets that are needed for the rest of the paper. For details and examples, see [8][9][11].

Definition 1 (Stange [8, Def. 2.1][9, Def. 3.1.1]). *Let K be a field, $n > 0$ and integer. An* elliptic net *is any map $W : \mathbb{Z}^n \to K$ such that the following recurrence holds for all $p, q, r, s \in \mathbb{Z}^n$:*

$$\begin{aligned} W(p+q+s)\,W(p-q)\,W(r+s)\,W(r) \\ + W(q+r+s)\,W(q-r)\,W(p+s)\,W(p) \\ + W(r+p+s)\,W(r-p)\,W(q+s)\,W(q) = 0 \quad (1) \end{aligned}$$

We refer to n as the rank *of the elliptic net. An elliptic net of rank one is called an* elliptic divisibility sequence*.*

One always has $W(-\mathbf{v}) = -W(\mathbf{v})$ and $W(\mathbf{0}) = 0$, and a restriction of an elliptic net to a sublattice of $\mathbb{Z}^n$ is again an elliptic net. The important fact for our purposes is that any elliptic curve E over K and points $P_1, \ldots, P_n \in E(K)$ gives rise to a unique elliptic net $W_{E,P_1,\ldots,P_n} : \mathbb{Z}^n \to K$. The principal theorem is as follows.

Theorem 2 (Stange [8, Thm. 6.1][9, Thm. 7.1.1]). *Let $n > 0$ be an integer. Let*

$$E : f(x,y) = y^2 + \alpha_1 xy + \alpha_3 y - x^3 - \alpha_2 x^2 - \alpha_4 x - \alpha_6 = 0$$

be an elliptic curve defined over a field K. Let $\mathbf{e}_i$ be the i^{th} standard basis vector. For all $\mathbf{v} \in \mathbb{Z}^n$, there are functions $\Psi_{\mathbf{v}} : E^n \to K$ in the ring

$$\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6][x_i, y_i]_{i=1}^n \left[(x_i - x_j)^{-1}\right]_{1 \le i < j \le n} \Big/ \langle f(x_i, y_i) \rangle_{i=1}^n \subset K(E),$$

such that

1. *$W(\mathbf{v}) = \Psi_{\mathbf{v}}$ satisfies the recurrence (1).*
2. *$\Psi_{\mathbf{v}} = 1$ whenever $\mathbf{v} = \mathbf{e}_i$ for some $1 \le i \le n$ or $\mathbf{v} = \mathbf{e}_i + \mathbf{e}_j$ for some $1 \le i < j \le n$.*
3. *$\Psi_{\mathbf{v}}$ vanishes at $\mathbf{P} = (P_1, \ldots, P_n) \in E^n$ if and only if $\mathbf{v} \cdot \mathbf{P} = \mathcal{O}$ on E (and $\mathbf{v}$ is not one of the vectors specified in 2).*

In the case of rank $n = 1$, the $\Psi_{\mathbf{v}}$ are the familiar *division polynomials* of an elliptic curve [13, p. 105]. Since the $\Psi_{\mathbf{v}}$ satisfy the elliptic net recurrence (1), we may make the following definition.

Definition 2 (Stange [8, Def. 6.1][9, Def. 7.2.1]). *For any elliptic curve E defined over K and non-zero points $P_1, \ldots, P_n \in E(K)$ such that no two are equal or inverses (or, if $n = 1$, P_1 is not a 2- or 3-torsion point), the map $W_{E,P_1,\ldots,P_n} : \mathbb{Z}^n \to K$ defined by*

$$W_{E,P_1,\ldots,P_n}(\mathbf{v}) = \Psi_{\mathbf{v}}(P_1, \ldots, P_n)$$

is an elliptic net called the elliptic net associated to $E, P_1, \ldots, P_n$.

Nearly all elliptic nets arise in this way (see [8][9]). For the remainder of this article, any elliptic net or elliptic divisibility sequence will be assumed to have this form.

Elliptic nets or elliptic divisibility sequences are arrays or sequences of values of K. The zeroes in this array are particularly important.

Definition 3. *The zeroes of an elliptic divisibility sequence or elliptic net appear as a sublattice of the lattice of indices. We call this sublattice the* lattice of zero-apparition. *In the case of a sequence, this sublattice is specified by a single positive integer – the smallest positive index of a vanishing term – and this number is called the* rank of zero-apparition.

The rank of zero-apparition of an elliptic divisibility sequence associated to a point P will equal the order of the point P. In the case of an array associated to points $P_1, \ldots, P_n$, the zeroes $(v_1, \ldots, v_n)$ correspond to linear combinations $\mathbf{v} \cdot \mathbf{P}$ that vanish.

Suppose $T : \mathbb{Z}^s \to \mathbb{Z}^t$ is a $\mathbb{Z}$-linear transformation. The following theorem relates the elliptic net associated to $\mathbf{P} \in E^s$ to that associated to $T(\mathbf{P}) \in E^t$.

Theorem 3 (Stange [8, Prop. 5.6][9, Thm. 6.2.3]). *Let T be any $t \times s$ integral matrix. Let $\mathbf{P} \in E^s$ and $\mathbf{v} \in \mathbb{Z}^t$. Then*

$$\begin{aligned} W_{E,\mathbf{P}}(T^{tr}(\mathbf{v})) &= W_{E,T(\mathbf{P})}(\mathbf{v}) \\ &\times \prod_{i=1}^{t} W_{E,\mathbf{P}}(T^{tr}(\mathbf{e}_i))^{v_i^2 - v_i(\sum_{j\neq i} v_j)} \prod_{1\le i<j\le t} W_{E,\mathbf{P}}(T^{tr}(\mathbf{e}_i+\mathbf{e}_j))^{v_i v_j} \end{aligned} \tag{2}$$

This has several useful corollaries. For proofs see the cited references.

Theorem 4 (Ward [2, Thm. 8.1], Stange [9, Thm. 10.2.3][14]). *Suppose that $W_{E,P}(m) = 0$. Then for all $l, v \in \mathbb{Z}$, we have*

$$W_{E,P}(lm+v) = W_{E,P}(v) a^{vl} b^{l^2}$$

where

$$a = \frac{W_{E,P}(m+2)}{W_{E,P}(m+1)W_{E,P}(2)}, \qquad b = \frac{W_{E,P}(m+1)^2 W_{E,P}(2)}{W_{E,P}(m+2)}.$$

Furthermore, $a^m = b^2$. Therefore, there exists an $\alpha \in \bar{K}$, the algebraic closure of K, such that $\alpha^2 = a$ and $\alpha^m = b$, and so

$$W_{E,P}(lm+v) = W_{E,P}(v)\alpha^{(lm+v)^2 - v^2}.$$

Theorem 5 (Stange [9, Thm. 10.2.3][14]). *Suppose $\mathbf{r} = (r_1, r_2) \in \mathbb{Z}^2$ is such that*
$W_{E,P,Q}(\mathbf{r}) = 0$. For $l \in \mathbb{Z}$ and $\mathbf{v} = (v_1, v_2) \in \mathbb{Z}^2$ we have

$$W_{E,P,Q}(l\mathbf{r}+\mathbf{v}) = W_{E,P,Q}(\mathbf{v}) a_{\mathbf{r}}^{lv_1} b_{\mathbf{r}}^{lv_2} c_{\mathbf{r}}^{l^2}$$

where

$$a_{\mathbf{r}} = \frac{W(r_1+2, r_2)}{W(r_1+1, r_2)w(2,0)}, \ b_{\mathbf{r}} = \frac{W(r_1, r_2+2)}{W(r_1, r_2+1)W(0,2)}, \ c_{\mathbf{r}} = \frac{W(r_1+1, r_2+1)}{a_{\mathbf{r}} b_{\mathbf{r}} W(1,1)}.$$

3 Perfectly Periodic Sequences and Nets

Definition 4. *An elliptic divisibility sequence is called* perfectly periodic *if it is periodic with respect to its rank of zero-apparition. An elliptic net is called* perfectly periodic *if it is periodic with respect to its lattice of zero-apparition.*

Definition 5. *Let $f : \mathbb{Z}^n \to K^*$ be a quadratic function, and $k \in K^*$ a constant. Two elliptic nets W and W' are called* equivalent *if $W'(\mathbf{v}) = kf(\mathbf{v})W(\mathbf{v})$.*

As an example, let W be an elliptic divisibility sequence with rank of zero-apparition m. In one variable ($n = 1$), quadratic functions to K^* have the form $f(n) = \alpha^{n^2}$ for some $\alpha \in K^*$. Suppose we use α as defined by Theorem 4, i.e. $\alpha^2 = a, \alpha^m = b$, and let take $k = \alpha^{-1}$. Then $W'(n) = \alpha^{n^2-1}W(n)$, and this sequence is perfectly periodic. Suppose that $K = \mathbb{F}_q$ and $\gcd(q-1, m) = 1$. In this case the conditions of Theorem 4 determine such an α uniquely, and it lies in K. Otherwise (if $\gcd(q-1, m) \neq 1$), two such α's will exist, equal up to sign. The two resulting perfectly periodic sequences will be equal at even-indexed locations and equal up to sign at odd-indexed locations.

The moral of the last paragraph is that any elliptic divisibility sequence is equivalent to a perfectly periodic one. We can give an explicit expression for such a perfectly periodic sequence.

Theorem 6. *Let K be a finite field of q elements, and E an elliptic curve defined over K. For all points $P \in E$ of order relatively prime to $q-1$ and greater than 3, define*

$$\phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q-1+\mathrm{ord}(P))} \right)^{\frac{1}{\mathrm{ord}(P)^2}}. \tag{3}$$

For a point P of order relatively prime to $q-1$ and greater than 3, the sequence $\phi([n]P)$ is a perfectly periodic elliptic divisibility sequence equivalent to $W_{E,P}(n)$. Specifically,

$$\phi([n]P) = \phi(P)^{n^2-1} W_{E,P}(n). \tag{4}$$

More generally, let $\mathbf{P} \in E(K)^n$ be a collection of nonzero points, no two equal or inverses, and all elements of a single cyclic group and having order greater than 3. The n-array $\phi(\mathbf{v} \cdot \mathbf{P})$ (as $\mathbf{v}$ ranges over $\mathbb{Z}^n$) forms a perfectly periodic elliptic net equivalent to $W_{E,\mathbf{P}}(\mathbf{v})$. Specifically,

$$\phi(\mathbf{v} \cdot \mathbf{P}) = W_{E,\mathbf{P}}(\mathbf{v}) \prod_{i=1}^{n} \phi(P_i)^{v_i^2 - v_i(\sum_{j \neq i} v_j)} \prod_{1 \leq i < j \leq n} \phi(P_i + P_j)^{v_i v_j}.$$

Proof. The proof uses Theorem 3. We will demonstrate the method of proof in the rank one case before proceeding to the general case. Take $T = (l)$, so

$$W_{E,[l]P}(n) W_{E,P}(l)^{n^2} = W_{E,P}(nl).$$

By symmetry,

$$W_{E,[n]P}(l) W_{E,P}(n)^{l^2} = W_{E,P}(nl).$$

Let $m = \mathrm{ord}(P)$. Thus, combining the above and using $l = q-1$ and $q-1+m$ in turn,

$$\frac{W_{E,[n]P}(q-1)W_{E,P}(n)^{(q-1)^2}}{W_{E,P}(q-1)^{n^2}} = W_{E,[q-1]P}(n) = W_{E,[q-1+m]P}(n)$$
$$= \frac{W_{E,[n]P}(q-1+m)W_{E,P}(n)^{(q-1+m)^2}}{W_{E,P}(q-1+m)^{n^2}}$$

Rearranging,

$$\phi([n]P) = \phi(P)^{n^2-1}W_{E,P}(n).$$

Therefore, $\phi([n]P)$ is an elliptic divisibility sequence. By definition, $\phi([n]P)$ has period $\mathrm{ord}(P)$ which is equal to the rank of apparition of $W_{E,P}$ and $\phi([n]P)$. So $\phi([n]P)$ is perfectly periodic.

For the rank n case, let m be the order of the cyclic group containing all the points under consideration. In Theorem 3, let $t = 1$ and $s = n$ and take $T = (v_1 \quad v_2 \quad v_3 \quad \cdots \quad v_n)$ to obtain

$$W_{E,\mathbf{P}}(l\mathbf{v}) = W_{E,\mathbf{v}\cdot\mathbf{P}}(l)W_{E,\mathbf{P}}(\mathbf{v})^{l^2}.$$

Now take $t = s = n$ in Theorem 3 , and $T = l\mathrm{Id}_\mathrm{n}$ to obtain

$$W_{E,\mathbf{P}}(l\mathbf{v}) = W_{E,l\mathbf{P}}(\mathbf{v})\prod_{i=1}^{n} W_{E,\mathbf{P}}(le_i)^{v_i^2-v_i(\sum_{j\neq i} v_j)} \prod_{1\leq i<j\leq n} W_{E,\mathbf{P}}(le_i+le_j)^{v_iv_j}.$$

Note that

$$W_{E,\mathbf{P}}(le_i) = W_{E,P_i}(l), \qquad W_{E,\mathbf{P}}(le_i+le_j) = W_{E,P_i+P_j}(l).$$

Combining the above, we have

$$W_{E,l\mathbf{P}}(\mathbf{v}) = \frac{W_{E,\mathbf{v}\cdot\mathbf{P}}(l)W_{E,\mathbf{P}}(\mathbf{v})^{l^2}}{\prod_{i=1}^{n} W_{E,P_i}(l)^{v_i^2-v_i(\sum_{j\neq i} v_j)}\prod_{1\leq i<j\leq n} W_{E,P_i+P_j}(l)^{v_iv_j}}.$$

Comparing this in the case of $l = q-1$ and $l = q-1+m$ gives the required result, as before.

In light of this theorem we will use the convenient notation

$$\widetilde{W}_{E,P}(n) = \phi([n]P).$$

and call this the *perfectly periodic elliptic divisibility sequence associated to E and P*. The attractive property of a perfectly periodic sequence is formula (3): $\widetilde{W}_{E,P}(n)$ can be calculated *as a function of the point $[n]P$ on the curve* without knowledge of n.

Corollary 1. *Suppose that E is an elliptic curve over a field $K = \mathbb{F}_q$ and $P \in E(K)$ is of order $m \geq 4$. The period of the sequence $W_{E,P}$ is $m\,\mathrm{ord}_{K^*}(\phi(P))$.*

Proof. First, $\phi([n]P)$ has period exactly m. Since, if the period were $m' < m$, then $W_{E,P}(m') = 0$, a contradiction. The result now follows from equation (4).

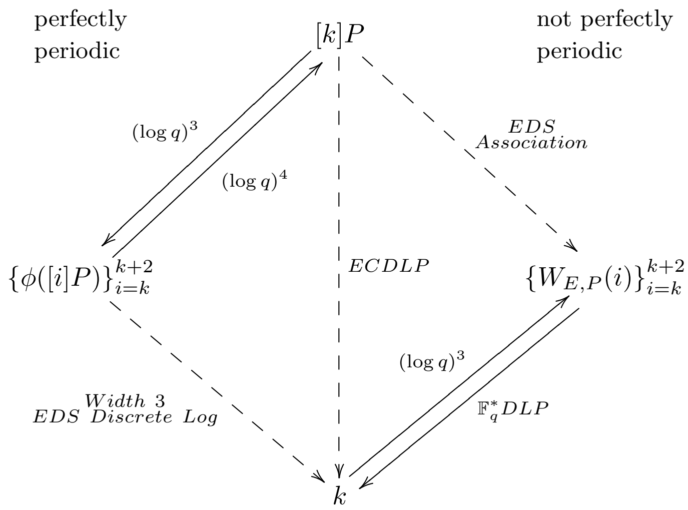
The ratio between the period and the rank of zero-apparition, which we've demonstrated to be $\mathrm{ord}_{K^*}(\phi(P))$, is called τ by Morgan Ward [2, Thm. 11.1].

4 The Hard Problems

As we have seen, elliptic nets are closely related to the points on an elliptic curve. In this section, we will see specifically how to compute them, and how they relate, algorithmically, to the points.

The choice of segment $0 < k < \operatorname{ord}(P)$ is not crucial in Problem 2 (EDS Association): it could be restated for any segment $i \operatorname{ord}(P) < k < (i+1) \operatorname{ord}(P)$. This problem is trivial for a perfectly periodic sequence or net (since $\widetilde{W}(k) = \phi(Q)$ is computable in $\log q$ time). For the non-perfectly periodic case, the problem appears to be much harder. As for Problem 4 (EDS Discrete Log), on the other hand, for non-perfectly periodic elliptic divisibility sequences, it can be solved by computing an $\mathbb{F}_q^*$ discrete log. For this problem, it is the case of perfect periodicity that seems very difficult.

We will see that these hard problems are related according to the following diagram.



We demonstrate the complexity of solving the problems associated to the solid lines in the following series of theorems. The solid line labelled $\mathbb{F}_q^*$DLP has the complexity of a discrete logarithm problem in $\mathbb{F}_q^*$ (this is sub-exponential by index calculus). No sub-exponential algorithms are known for the dotted lines.

Since our concern is polynomial time vs. non-polynomial time, in the following we assume naive arithmetic in $\mathbb{F}_q$, i.e. we bound the time to do basic $\mathbb{F}_q$ operations by $O((\log q)^2)$ for simplicity.

Lemma 1. *Let E be an elliptic curve defined over K, and $P \in E(K)$ be a point of order not less than 4. The x-coordinate of $[n]P$, $x([n]P)$, can be calculated in $O((\log q)^2)$ time from the three terms $W_{E,P}(n-1)$, $W_{E,P}(n)$, and $W_{E,P}(n+1)$ or from the three terms $\widetilde{W}_{E,P}(n-1)$, $\widetilde{W}_{E,P}(n)$, and $\widetilde{W}_{E,P}(n+1)$.*

Proof. See [9, Lemma 6.2.2] for the following identity:

$$\frac{W_{E,P}(n-1)W_{E,P}(n+1)}{W_{E,P}(n)^2} = x(P) - x([n]P). \tag{5}$$

The left-hand side of (5) is invariant under equivalence, and so the same calculation applies if we put tilde's on the W's.

Theorem 7 (Shipsey [1, Thm 3.4.1]). *Let E be an elliptic curve over K, and $P \in E(K)$ a point of order not less than 4. Given a value t, the term $W_{E,P}(t)$ in the elliptic divisibility sequence associated to E, P can be calculated in $O((\log t)(\log q)^2)$ time.*

Proof. For completeness, we give a simplified version of Shipsey's algorithm here. Following Shipsey, denote by $\langle W_{E,P}(k)\rangle$ the segment or *block centred at k* of eight terms $W_{E,P}(k-3)$, $W_{E,P}(k-2)$, ..., $W_{E,P}(k+3)$, $W_{E,P}(k+4)$ of the sequence. The block centred at t can be calculated from the block centred at 1 via a double-and-add algorithm based on an addition chain for t. The calculation of the new block from the previous depends on two instances of the recurrence (one such calculation for each term of the new block):

$$\begin{aligned} W(2i-1,0) &= W(i+1,0)W(i-1,0)^3 - W(i-2,0)W(i,0)^3 \ , \\ W(2i,0) &= \big(W(i,0)W(i+2,0)W(i-1,0)^2 \\ &\qquad - W(i,0)W(i-2,0)W(i+1,0)^2\big) / W(2,0) \ . \end{aligned}$$

To begin we must calculate the block centred at 1. Recalling that $W(0) = 0$, $W(1) = 1$ and $W(-n) = -W(n)$, we must calculate $W(i)$ for $i = 2, 3, 4$. Precise formulae in terms of the coordinates of P and the Weierstrass coefficients for E can be found in [13, p. 105] or for long Weierstrass equations in [15, p. 80]. This algorithm takes $O(\log t)$ steps, each of which involves a fixed number of $\mathbb{F}_q^*$ multiplications and additions, which take $O((\log q)^2)$ time at worst.

Theorem 8. *Let E be an elliptic curve over $\mathbb{F}_q$, and $P \in E(\mathbb{F}_q)$ a point of order relatively prime to $q-1$ and greater than 3. Given a point $Q = [k]P$, the term $\phi(Q) = \widetilde{W}_{E,P}(k)$ can be calculated in $O((\log q)^3)$ time without requiring knowledge of k.*

Proof. We use equation (3). Using Theorem 7 to calculate the ratio of terms inside the parentheses takes $\log(q-1+\mathrm{ord}(Q))+\log(q-1)$ steps. Since $\mathrm{ord}(Q)$ is on the order of q, this is $O((\log q)^3)$ time at worst. The other necessary operation in (3) is to find the inverse of $\mathrm{ord}(Q)^2$ modulo $q-1$, and to raise to that exponent. Both these are also $O(\log q)$ operations.

Theorem 9. *Let E be an elliptic curve over $\mathbb{F}_q$, and $P \in E(\mathbb{F}_q)$ a point of order relatively prime to $q-1$ and greater than 3. Given the $\widetilde{W}_{E,P}(k)$, $\widetilde{W}_{E,P}(k+1)$ and $\widetilde{W}_{E,P}(k+2)$, the point $Q = [k]P$ can be calculated in probabilistic $O((\log q)^4)$ time without requiring knowledge of k.*

Proof. Calculate $x([k+1]P)$ by Lemma 1. We can calculate the corresponding possible values for y in probabilistic time $O((\log q)^4)$ [16, §7.1-2]. To determine which of the two points with this x-coordinate is actually $[k+1]P$, first take one of the two candidate points, and proceed on the assumption that it is $[k+1]P$. Using the addition formula for elliptic curves, calculate $x([k+1]P+P) = x([k+2]P)$. Compare this with (5) to determine $\widetilde{W}(k+3)$. Also determine $\widetilde{W}(k+4)$ in this manner. Then, if the terms $\widetilde{W}(k), \ldots, \widetilde{W}(k+4)$ satisfy the recurrence instance

$$\widetilde{W}(k+4)\widetilde{W}(k) = \widetilde{W}(k+1)\widetilde{W}(k+3)\widetilde{W}(2)^2 - \widetilde{W}(3)\widetilde{W}(1)\widetilde{W}(k+2)^2,$$

our assumption about the point we chose is correct. If this recurrence does not hold, then the point we chose was incorrect, and the other one is the point $[k+1]P$ we seek. For, it is impossible that both points cause the above equation to be satisfied: any sequence of four consecutive terms in an elliptic divisibility sequence determines the entire sequence uniquely. Finally, knowing $[k+1]P$, we can calculate $Q = [k]P = [k+1]P - P$.

The following theorem is implicit in the work of Shipsey; see Section 5.2 for an explanation.

Theorem 10. *Suppose P has order relatively prime to $q-1$ and greater than 3, and $\phi(P)$ is a primitive root in $\mathbb{F}_q^*$. Given $W_{E,P}(k), W_{E,P}(k+1), W_{E,P}(k+2)$, where it can be assumed that $0 < k < ord(P)$, calculating k can be reduced to a single discrete logarithm in $\mathbb{F}_q^*$ in probabilistic $O((\log q)^4)$ time.*

Proof. We can deduce the x-coordinate of the point $Q = [k]P$ by Lemma 1. Compute the two corresponding y-coordinates, which takes probabilistic time $O((\log q)^4)$ [16, §7.1-2]. Choosing one of the two possible y-coordinates, we have either $Q = [k]P$ or $Q = [-k]P$. To determine which is correct, use the trick of the proof of Theorem 9. Suppose it is the former; then, from Theorem 6, we have

$$\frac{\phi([k+1]P)}{\phi([k]P)} = \phi(P)^{2k+1}\frac{W_{E,P}(k+1)}{W_{E,P}(k)}. \tag{6}$$

So k satisfies an equation of the form $A = B^{2k+1}$ where A and B are known, and B has order $q-1$ by assumption. Therefore, we are reduced to solving a discrete logarithm of the form $A = B^x$ for $0 \leq x < q-1$, with the understanding that k will be one of $(x-1)/2$ or $(x+q-1)/2$. (In fact, if $q-1 < m$, there may be at most two other possible values of k to check: the above values shifted by $q-1$.)

Remark 1. Let $m = \mathrm{ord}(P)$. Suppose that $\gcd(m, q-1) = 1$. As an integer k ranges over representatives of a single coset in $\mathbb{Z}/m\mathbb{Z}$, it ranges over all possible cosets of $\mathbb{Z}/(q-1)\mathbb{Z}$. Therefore, we cannot expect to find the set of k such that $Q = [k]P$ (i.e. a coset in $\mathbb{Z}/m\mathbb{Z}$) by solving an equation of the form $A = B^k$ in $\mathbb{F}_q^*$ (i.e. solving modulo $q-1$). One solution to this problem is to attempt to solve for an *integer* k (instead of a coset) – say, for example, the smallest non-negative k with $Q = [k]P$. This is in essence what the preceeding theorem does. With this in mind, we set some terminology.

Definition 6. *Let Q be a multiple of P on an elliptic curve E. The* minimal multiplier *of Q with respect to P is the smallest non-negative value of k such that $Q = [k]P$.*

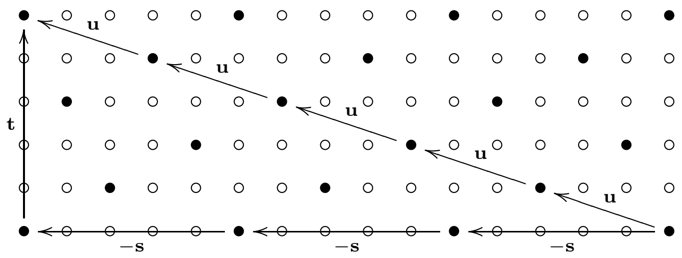
Note that the minimal multiplier satisfies $0 \leq k < \mathrm{ord}(P)$.

5 $\mathbb{F}_q^*$ Discrete Logarithm, The Tate Pairing and MOV/Frey-Rück Attack

Theorem 10 uses terms of the elliptic divisibility sequence to give a discrete logarithm problem in $\mathbb{F}_q^*$. We demonstrate some variations on this theme, and relate these types of equations to the Tate pairing, and to an ECDLP attack given by Shipsey [1].

5.1 An $\mathbb{F}_q^*$ DLP equation of the form $A = B^k$ from periodicity properties

The $\mathbb{F}_q^*$ DLP equations we consider are consequences of Theorem 3, but many can be conveniently understood in terms of its corollary Theorem 5. The following example involves the terms $W_{E,P}(k)$ and $W_{E,P}(k+1)$, and requires knowledge of $Q = [k]P$. The following diagram is suggestive for the discussion.



In this picture of $\mathbb{Z}^2$, $\mathbf{u} = (-3, 1)$, $\mathbf{s} = (5, 0)$ and $\mathbf{t} = (0, 5)$. Vectors $\mathbf{u}$ and $\mathbf{s}$ generate the lattice of zero-apparition Λ for some elliptic net W associated to points P and $Q = [3]P$ of order 5. The vector $\mathbf{t}$ is also in Λ. One coset of $\mathbb{Z}^2$ modulo Λ is shown as the solid discs.

Theorem 5 shows the transformation relative to translation by a vector $\mathbf{r} \in \Lambda$: it relates $W(\mathbf{v} + \mathbf{r})$ to $W(\mathbf{v})$ for each $\mathbf{v}$. This Lemma can be applied repeatedly, and different 'paths' from one point to another must agree. In the picture above, the translation property which relates $W(\mathbf{v}+(-15, 5))$ to $W(\mathbf{v})$ can be calculated by applying the transformation associated to $\mathbf{u}$ five times (the diagonal path) or by applying the transformation associated to $-\mathbf{s}$ three times followed by that associated to $\mathbf{t}$ once (the sides of the triangle).

In the general case, we have $Q = [k]P$. Then the lattice of zero-apparition Λ for $W = W_{E,P,Q}$ includes vectors $\mathbf{u} = (-k, 1)$, $\mathbf{s} = (m, 0)$ and $\mathbf{t} = (0, m)$.

Suppose $\mathbf{r} = (r_1, r_2)$ is an element of Λ for $W = W_{E,P,Q}$. By Theorem 5, we have for all $l \in \mathbb{Z}$ and $\mathbf{v} \in \mathbb{Z}^2$,

$$W(l\mathbf{r} + \mathbf{v}) = W(\mathbf{v}) a_{\mathbf{r}}^{lv_1} b_{\mathbf{r}}^{lv_2} c_{\mathbf{r}}^{l^2} \tag{7}$$

where

$$a_{\mathbf{r}} = \frac{W(r_1+2, r_2)}{W(r_1+1, r_2)W(2,0)},\ b_{\mathbf{r}} = \frac{W(r_1, r_2+2)}{W(r_1, r_2+1)W(0,2)},\ c_{\mathbf{r}} = \frac{W(r_1+1, r_2+1)}{a_{\mathbf{r}} b_{\mathbf{r}} W(1,1)}.$$

We expect appropriate relationships between $a_{\mathbf{u}}$, $b_{\mathbf{u}}$, $c_{\mathbf{u}}$, $a_{\mathbf{s}}$, $b_{\mathbf{s}}$, etc. The $\mathbb{F}_q^*$ DLP equation we seek is one such relationship. We have

$$a_{\mathbf{s}} = \frac{W(m+2,0)}{W(m+1,0)W(2,0)},\ a_{\mathbf{t}} = \frac{W(2,m)}{W(1,m)W(2,0)},\ a_{\mathbf{u}} = \frac{W(2-k,1)}{W(1-k,1)W(2,0)}.$$

For each $i \in \mathbb{Z}$, we apply (7) to obtain

$$\frac{W(-ik+1, i-1)W(0,-1)}{W(1,-1)W(-ik, i-1)} = a_{\mathbf{u}}^i \tag{8}$$

Set $i = m$ in (8), and apply (7) four times:

$$\begin{aligned} a_{\mathbf{u}}^m &= \frac{W(-mk+1, m-1)W(0,-1)}{W(1,-1)W(-mk, m-1)} \\ &= \left(\tfrac{W(-mk+1,m-1)}{W(-mk+1,-1)}\right)\left(\tfrac{W(-mk+1,-1)}{W(1,-1)}\right)\left(\tfrac{W(0,-1)}{W(-mk,-1)}\right)\left(\tfrac{W(-mk,-1)}{W(-mk,m-1)}\right) \\ &= \frac{a_{\mathbf{t}}^{-mk+1} b_{\mathbf{t}}^{-1} c_{\mathbf{t}}^1 a_{\mathbf{s}}^{-k} b_{\mathbf{s}}^k c_{\mathbf{s}}^{k^2}}{a_{\mathbf{t}}^{-mk} b_{\mathbf{t}}^{-1} c_{\mathbf{t}}^1 a_{\mathbf{s}}^0 b_{\mathbf{s}}^k c_{\mathbf{s}}^{k^2}} = a_{\mathbf{t}} a_{\mathbf{s}}^{-k} \end{aligned}$$

Setting $i = 1$ in (8), we obtain an expression

$$a_{\mathbf{u}} = \frac{W(-k+1,0)W(0,-1)}{W(1,-1)W(-k,0)} = -\frac{W_{E,P}(k-1)}{W_{E,P}(k)W(1,-1)}$$

which, when substituted into the last calculation, yields

$$\left(\frac{W(m+1,0)W(2,0)}{W(m+2,0)}\right)^k = \left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)}\right)^m \left(-\frac{W(1,m)W(2,0)}{W(2,m)W(1,-1)^m}\right). \tag{9}$$

5.2 An $\mathbb{F}_q^*$ DLP equation from Shipsey's Thesis

The possibility of such an equation was observed by Rachel Shipsey in her thesis [1, (6.3)]. She uses one-dimensional periodicity properties to derive the following equation:

$$\frac{W_{E,P}((m+1)(k+1))W_{E,P}(k)}{W_{E,P}((m+1)k)W_{E,P}(k+1)} = W_{E,P}(m+1)^{2k+1} \tag{10}$$

Shipsey then argues that without knowledge of k the left hand side can be calculated up to a factor of

$$\left(\frac{W_{E,P}(k)}{W_{E,P}(k-1)}\right)^{m(m+2)}.$$

This is very much of the same spirit as equation (9), and in fact, Theorem 3 can be used to rewrite (10) in this form:

$$\frac{W_{E,P,Q}(m+1,m+1)}{W_{E,P,Q}(0,m+1)}\left(\frac{W_{E,P}(k+1)}{W_{E,P}(k)}\right)^{m(m+2)} = W_{E,P}(m+1)^{2k+1}. \qquad (11)$$

By Lemma 1, knowledge of $Q, W_{E,P}(k), W_{E,P}(k-1)$ determines $W_{E,P}(k+1)$, and so this is very much equivalent to Shipsey's analysis. Note that the unknown terms in (11) are raised to the exponent $m+2$. At first blush, this may appear to lead to an ECDLP attack for $q-1 = m+2$ (where the unknown terms will disappear). However, this is not allowed by Remark 1. In fact, it turns out that if $q-1 = m+2$, then $W_{E,P}(m+1) = 1$ (this eventually follows from Theorem 3 also).

5.3 $\mathbb{F}_q^*$ DLP equations and the Tate pairing

Choose $m \in \mathbb{Z}^+$. Let E be an elliptic curve defined over a finite field K containing the m-th roots of unity. Suppose $P \in E(K)[m]$ and $Q \in E(K)/mE(K)$. Since P is an m-torsion point, $m(P) - m(\mathcal{O})$ is a principal divisor, say $\mathrm{div}(f_P)$. Choose another divisor D_Q defined over K such that $D_Q \sim (Q) - (\mathcal{O})$ and with support disjoint from $\mathrm{div}(f_P)$. Then, we may define the Tate pairing

$$\tau_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$$

and Weil pairing

$$e_m : E(K)[m] \times E(K)[m] \to \mu_m$$

by

$$\tau_m(P,Q) = f_P(D_Q), \qquad e_m(P,Q) = f_P(D_Q) f_Q(D_P)^{-1}.$$

Both are non-degenerate bilinear pairings, while the Weil pairing is alternating. For details, see [17][18].

The Tate pairing and Weil pairing are used in the MOV [19] and Frey-Rück [20] attacks on the ECDLP. These use the Weil and Tate pairings, respectively, to translate an instance of the ECDLP into an $\mathbb{F}_q^*$ DLP equation, where index calculus methods may be used. The basic idea, illustrated here for the Tate pairing, is that $Q = [k]P$ implies $\tau_m(Q,S) = \tau_m(P,S)^k$ by bilinearity. If S can be chosen so that $\tau_m(P,S)$ is non-trivial, and if the Tate pairing takes values in a manageably small finite field, then index calculus methods can be used to determine k. In particular, this attack applies for curves E over $\mathbb{F}_q$ where $m = q-1$.

In (11) and (9), all the terms may be calculated from knowledge of m, P and Q except for $W_{E,P}(k)$ and $W_{E,P}(k-1)$. However, notice that these unknown terms are raised to the power m. Therefore, in the case that $m = q-1$, no extra information is needed and the ECDLP is reduced to an $\mathbb{F}_q^*$ DLP; this works in exactly the cases that the MOV or Frey-Rück attack applies.

These sorts of 'alternate versions' of the MOV/Frey-Rück attack do have a relation to the Tate pairing.

Theorem 11 (Stange [9, Thm. 17.2.1][11, Thm. 6]). *Let E be an elliptic curve, $m \geq 4$, and $P \in E[m]$. Let $Q, S \in E$ be such that $S \notin \{\mathcal{O}, Q\}$. Let W be an elliptic net of rank n, associated to points $\mathbf{T} \in E(K)^n$. Let $\mathbf{s}, \mathbf{p}, \mathbf{q} \in Z^n$ be such that*

$$P = \mathbf{p} \cdot \mathbf{T}, \qquad Q = \mathbf{q} \cdot \mathbf{T}, \qquad S = \mathbf{s} \cdot \mathbf{T}.$$

Let $\tau_m : E[m] \times E/mE \to K^*/(K^*)^m$ be the Tate pairing. Then

$$\tau_m(P, Q) = \frac{W(m\mathbf{p} + \mathbf{q} + \mathbf{s})W(\mathbf{s})}{W(m\mathbf{p} + \mathbf{s})W(\mathbf{q} + \mathbf{s})}.$$

Now equations (9) and (11) can be re-written as statements in terms of the Tate pairing.

Equation (9)**:** Use Theorem 11 with $\mathbf{p} = (1, 0), \mathbf{q} = (-1, 0), \mathbf{s} = (2, 0)$ for the left-hand side and $\mathbf{p} = (0, 1), \mathbf{q} = (-1, 0), \mathbf{s} = (2, 0)$ for the right. This rewrites (9) as

$$\tau_m(P, -P)^k = \tau_m(Q, -P).$$

Equation (11)**:** This is somewhat more complicated. From Theorem 4 with $m = q-1$ and Theorem 11 with various parameters,

$$W_{E,P}(m+1)^2 \tau_m(P, P)^{-2} = \left(\frac{W_{E,P}(m+1)^2 W_{E,P}(2)}{W_{E,P}(m+2)} \right)^2 = b^2 = a^m = 1,$$

$$\tau_m(P, Q) = \frac{W_{E,P,Q}(m+1, 1)W_{E,P,Q}(1, 0)}{W_{E,P,Q}(m+1, 0)W_{E,P,Q}(1, 1)},$$

$$\tau_m(Q, P) = \frac{W_{E,P,Q}(1, m+1)W_{E,P,Q}(0, 1)}{W_{E,P,Q}(0, m+1)W_{E,P,Q}(1, 1)},$$

$$1 = \tau_m(P, \mathcal{O}) = \tau_m(P, [m]Q) = \frac{W_{E,P,Q}(m+1, m+1)W_{E,P,Q}(1, 1)}{W_{E,P,Q}(m+1, 1)W_{E,P,Q}(1, m+1)}.$$

All of which, taken together, rewrites (11) as

$$\tau_m(P, Q)\tau_m(Q, P) = \tau_m(P, P)^{2k}.$$

Equation (4) (with $n = k$) does not, however, lend itself to this sort of re-writing in terms of pairings in the case $m = q-1$, as the very definition of $\phi(P)$ requires the assumption that $\gcd(m, q-1) = 1$.

6 ECDLP through EDS Association

The previous sections have demonstrated that there are a variety of ways to translate an ECDLP into an $\mathbb{F}_q^*$ DLP. The $\mathbb{F}_q^*$ DLP equation is in terms of elements of the sequence $W_{E,P}$. For example in (9), the elements are $W_{E,P}(k)$ and $W_{E,P}(k-1)$. The problem of finding these terms (with knowledge of $Q = [k]P$ but not k) is *EDS Association*. In this example, however, it is only their quotient that is needed. Depending on the form of the $\mathbb{F}_q^*$ DLP equation, different information (certain terms or ratios of terms) suffices. We formalise the most general statement of this in the following theorem.

Proposition 1. *Fix an elliptic curve E defined over $\mathbb{F}_q$, and $P \in E(\mathbb{F}_q)$ of order greater than three and relatively prime to $q-1$. Suppose $\phi(P)$ has order $q-1$ in $\mathbb{F}_q^*$. With knowledge of any product*

$$\prod_{i=1}^{N} W_{E,P}(p_i(k))^{e_i}, \tag{12}$$

where the $e_i \in \mathbb{Z}$, and $p_i(x) \in \mathbb{Z}[x]$ of degree at most D, and $t(x) = \sum_{i=1}^{N} e_i p_i(x)^2$ is a non-constant polynomial of degree at most 2 in $\mathbb{Z}[x]$, the value of k can be determined in subexponential time in q, with constants depending on D and N.

Proof. Combine appropriate instances of equation (4) of Theorem 6 in such a way that $t(k)$ satisfies an equation in $\mathbb{F}_q^*$ of the form $A = B^{t(k)}$. That is, combine one instance for each $n = p_i(k)$ with multiplicities given by the respective e_i, and obtain an equation of the form

$$\frac{\prod_{i=1}^{N} \widetilde{W}_{E,P}(p_i(k))^{e_i}}{\prod_{i=1}^{N} W_{E,P}(p_i(k))^{e_i}} = (\phi(P)^{-1})^{t(k)}$$

(Perhaps it is easier to demonstrate this concept by example: suppose that $1 = e_1 = -e_2$, $p_1(k) = k+1$, and $p_2(k) = k$, so that $t(k) = 2k+1$, and obtain equation (6) (note the product (12) appears on the right side) from combining equation (4) for $n = p_1(k) = k$ and $n = p_2(k) = k+1$ with multiplicities given by $e_1 = 1$ and $e_2 = -1$.)

The left hand side A includes the known product (12) as well as terms of the form $\phi([p_i(k)]P)$, while $B = \phi(P)^{-1}$. The N points $[p_i(k)]P$ can each be calculated from knowledge of P and $Q = [k]P$ without knowledge of k in $O(D \log D)$ curve operations. Then the various ϕ terms can be computed in time time $O((\log q)^3)$ by Theorem 8. Thus we have computed A and B.

Solving the discrete logarithm $A = B^{t(k)}$ for $t(k)$ can be done sub-exponentially by index calculus methods. Solving for k from $t(k)$ is sub-exponential [16, §7.1-2].

It is evident that the most costly step is the index calculus step, which in many cases has run time $r(q) = \exp(c(\log q)^{1/3}(\log\log q)^{2/3})$ [21, p.306].

7 ECDLP and Quadratic Residues

We will show that determining only one bit of information – the residuosity – about a term $W_{E,P}(k)$ may suffice to solve the ECDLP. First, we observe a hypothetical method of attack for ECDLP.

Proposition 2. *Let P be a point of odd order relatively prime to $q-1$. Given an oracle which can determine the parity of the minimal multiplier of any non-zero point Q in $\langle P\rangle$ in time $O(T(q))$, the elliptic curve discrete logarithm for any such Q can be determined in time $O(T(q)\log q + (\log q)^2)$.*

Proof. Suppose that k is the minimal multiplier of Q with respect to P. The basic algorithm is:

1. If $Q = P$, stop.
2. Call the oracle to determine the parity of k. If k is even, find Q' such that $[2]Q' = Q$. If k is odd, find Q' such that $[2]Q' = Q - P$.
3. Set $Q = Q'$ and return to step 1.

In Step 2, since the cyclic group $\langle P\rangle$ has odd order, there is a unique Q'. It can be found in $O(\log q)$ time (see [22] for methods). Furthermore, $Q' = [k']P$ where

$$k' = \begin{cases} k/2 & k \text{ even} \\ (k-1)/2 & k \text{ odd} \end{cases}.$$

Then k' is the minimal multiplier for Q' with respect to P. At the end of this process, the value of the original k can be deduced from the sequence of steps taken. For each even step, record a '0', and for each odd step a '1', writing from right to left, and adding a final '1': this will be the binary representation of k. The number of steps is $\log_2 k = O(\log q)$.

Proposition 3. *Fix an elliptic curve E defined over $\mathbb{F}_q$ of characteristic not equal to two, and $P \in E(\mathbb{F}_q)$ of order greater than three and relatively prime to $q-1$. Suppose that $\phi(P)$ is a quadratic non-residue. Then, with knowledge of the quadratic residuosity of any product of the form*

$$\prod_{i=1}^{N} W_{E,P}(p_i(k))^{e_i}, \tag{13}$$

where the $e_i \in \mathbb{Z}$, and $p_i(x) \in \mathbb{Z}[x]$ of degree at most D, and $t(x) = \sum_{i=1}^{N} e_i p_i(x)^2$ is not constant as a function $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, the parity of k can be determined in time $O(N(D(\log D)(\log q)^2 + (\log q)^3))$.

Proof. By Theorem 6, the value $t(k)$ satisfies an equation in $\mathbb{F}_q^*$ of the form $A = B^{t(k)}$ (exactly as in the proof of Proposition 1). The quadratic residuosity of A can be calculated in time $O(N(D(\log D)(\log q)^2 + (\log q)^3))$ as in the proof of Proposition 1. Now, $B = \phi(P)$ is a quadratic non-residue. The parity of $t(k)$ can be calculated from these values in constant time (i.e. consider the question in K^* modulo $(K^*)^2$). The parity of k is determined by checking the parity of $t(0)$ and $t(1)$. This final step takes time $O(D)$.

Corollary 2. *Let E be an elliptic curve over a field of characteristic not equal to two. Let P be a point of odd order such that $\phi(P)$ is a quadratic non-residue, and let k be the minimal multiplier of a multiple Q of P. Given P, Q and an oracle which can determine the quadratic residuosity of $W_{E,P}(k)$ in time $O(T(q))$, the elliptic curve discrete logarithm for any such Q can be determined in time $O((\log q)(T(q) + (\log q)^3))$.*

Proof. This follows from Proposition 3 with $N = 1, e_1 = 1, p_1(x) = x$ and Proposition 2.

A few remarks are in order.

1. If $\phi(P)$ is a quadratic residue, one solution to this obstacle is to replace the initial problem of $Q = [k]P$ with the equivalent problem of $[n]Q = [k]([n]P)$ for any n such that $\phi([n]P)$ is a quadratic non-residue. The sequence $\widetilde{W}_{E,P}(n)$ can be calculated term-by-term until such an n is found. The existence of such an n is guaranteed when -1 is a quadratic non-residue in $\mathbb{F}_q$, in which case $\phi([m-1]P) = -\phi(P)$ suffices. Other cases are less clear.
2. The condition that the order of P is relatively prime to the even quantity $q-1$ is required in several ways. First, for the very definition of ϕ (Theorem 6). Furthermore, if the order m of the group $\langle P \rangle$ is even, multiplication by 2 is not an automorphism, and so there is no unique 'half' of a point (this is the same difficulty that prevents this sort of parity attack on an $\mathbb{F}_q^*$ discrete log). However, if $m|(q-1)$ is odd, then k satisfies a discrete logarithm equation of the form $A = B^k$ in the group $K^*/(K^*)^m$, which has an odd number of elements. Therefore, this does not determine the parity of k.
3. Similarly, if $q-1$ is odd (i.e. $\mathbb{F}_q$ has characteristic 2), then $A = B^k$ does not carry information about the parity of k.

8 The EDS Residue Problem

In light of the preceeding section, it is natural to define the problem of EDS Residue (Problem 3). In Section 10 we will show that it is equivalent to the elliptic curve discrete logarithm in sub-exponential time. How might one determine the quadratic residuosity of $W_{E,P}(k)$? Our first observation is that knowledge of the residuosity of one term $W_{E,P}(k)$ would determine the residuosity of the next term.

Proposition 4. *Suppose Q is a known element of $\langle P \rangle$, but that its minimal multiplier k is unknown. The quadratic residuosity of $W_{E,P}(k+1)/W_{E,P}(k)$ can be calculated in $O((\log q)^3)$ time.*

Proof. From (4) with $n = k$ and $n = k+1$, we have

$$\frac{\phi(Q)}{\phi(Q+P)} = \phi(P)^{2k+1} \left(\frac{W_{E,P}(k+1)}{W_{E,P}(k)} \right).$$

The calculation of the terms $\phi(P), \phi(Q)$, and $\phi(P+Q)$ each take $O((\log q)^3)$ time.

Therefore, based on knowledge of Q but not k, the sequence

$$S(n) = \left(\frac{W_{E,P}(n)}{q}\right)\left(\frac{W_{E,P}(k)}{q}\right)$$

for $n = k, \ldots, k+N$ may be calculated in $O(N \log q)$ time. Then the sequence

$$\left(\frac{W_{E,P}(n)}{q}\right)$$

is either $S(n)$ or $-S(n)$. To determine which is to determine the quadratic residuosity of $W_{E,P}(k)$.

Therefore, if some bias, or some pattern, for quadratic residues of the elliptic divisibility sequence $W_{E,P}(n)$ were known, then the correct choice of the two sequences above could be determined. However, as yet we have no evidence to suggest that the ratio of quadratic residues among the terms is not $1/2$ in general.

9 ECDLP through EDS Discrete Log in the case of Perfect Periodicity

Problem 4 (EDS Discrete Log) is less unusual in flavour than the other problems considered here: general discrete logarithm attacks will apply. Recall the proof of Theorem 7, in which *blocks centred at* k are defined – denote this as $B(k)$. From $B(k)$, the recurrence relation can be used to calculate $B(2k)$ or $B(2k+1)$. In fact, Shipsey goes further, and shows how two blocks $B(k), B(k')$ can be added to obtain a block $B(k+k')$ in a similarly efficient manner (see [1, p. 23]). This means that the sequence of blocks $B(n)$ is a sequence along which we can move easily by addition and $\mathbb{Z}$-multiplication. Therefore, algorithms such as Baby-Step-Giant-Step and Pollard's ρ can be applied to this problem.

10 Equivalence of Hard Problems

Proof (Proof of Theorem 3). (3) $\implies$ (1)**:** Corollary 2. (1) $\implies$ (2)**:** If k is known, we can assume $0 < k \leq \mathrm{ord}(P)$, and then $W_{E,P}(k)$ can be calculated in $O((\log k)(\log q)^2) = O((\log q)^3)$ time. (2) $\implies$ (3)**:** Residuosity of a value in $\mathbb{F}_q^*$ can be determined in sub-exponential time (see [23] for algorithms). (1) $\implies$ (4)**:** Theorem 9. (4) $\implies$ (1)**:** Theorem 8 allows calculation of $\phi([k]P)$, $\phi([k+1]P)$, and $\phi([k+2]P)$ in sub-exponential time.

References

1. Shipsey, R.: Elliptic Divibility Sequences. PhD thesis, Goldsmiths, University of London (2001)
2. Ward, M.: Memoir on elliptic divisibility sequences. Amer. J. Math. **70** (1948) 31–74

3. Swart, C.: Elliptic curves and related sequences. PhD thesis, Royal Holloway and Bedford New College, University of London (2003)
4. Ayad, M.: Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques. Ann. Inst. Fourier (Grenoble) **43**(3) (1993) 585–618
5. Silverman, J.H.: Common divisors of elliptic divisibility sequences over function fields. Manuscripta Math. **114**(4) (2004) 431–446
6. Silverman, J.H.: p-adic properties of division polynomials and elliptic divisibility sequences. Math. Ann. **332**(2) (2005) 443–471 (Addendum 473–474)
7. Everest, G., Mclaren, G., Ward, T.: Primitive divisors of elliptic divisibility sequences. J. Number Theory **118**(1) (2006) 71–89
8. Stange, K.E.: Elliptic nets and elliptic curves. `http://arxiv.org/abs/0710.1316v1`, submitted (2007)
9. Stange, K.E.: Elliptic nets and elliptic curves. PhD thesis, Brown University (May 2008)
10. Everest, G., Poorten, A.v.d., Shparlinski, I., Ward, T.: Elliptic Divisibility Sequences. In: Recurrence Sequences. American Mathematical Society, Providence (2003) 163–175
11. Stange, K.E.: The Tate pairing via elliptic nets. In: Pairing-Based Cryptography - PAIRING 2007. Volume 4575 of Lecture Notes in Comput. Sci. Springer, Berlin (2007) 329–348
12. Gosper, R. W., O.H., Schroeppel, R.: Using somos sequences for cryptography
13. Silverman, J.H.: The arithmetic of elliptic curves. Volume 106 of Graduate Texts in Mathematics. Springer-Verlag, New York (1992) Corrected reprint of the 1986 original.
14. Stange, K.E.: Elliptic nets, generalised Jacobians and bi-extensions. In preparation
15. Frey, G., Lange, T.: Background on curves and Jacobians. In: Handbook of elliptic and hyperelliptic curve cryptography. Discrete Math. Appl. (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL (2006) 45–85
16. Bach, E., Shallit, J.: Algorithmic number theory. Vol. 1. Foundations of Computing Series. MIT Press, Cambridge, MA (1996) Efficient algorithms.
17. Duquesne, S., Frey, G.: Background on pairings. In: Handbook of elliptic and hyperelliptic curve cryptography. Discrete Math. Appl. (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL (2006) 115–124
18. Galbraith, S.D.: Pairings. In: Advances in elliptic curve cryptography. Volume 317 of London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge (2005) 183–213
19. Menezes, A.J., Okamoto, T., Vanstone, S.A.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inform. Theory **39**(5) (1993) 1639–1646
20. Frey, G., Rück, H.G.: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comp. **62**(206) (1994) 865–874
21. Crandall, R., Pomerance, C.: Prime numbers. Springer-Verlag, New York (2001) A computational perspective.
22. Kenny Fong, Darrel Hankerson, J.L., Menezes, A.: Field inversion and point halving revisited. Technical Report, CORR 2003-18, Department of Combinatorics and Optimization, University of Waterloo, Canada (2003)
23. Itoh, T., Tsujii, S.: An efficient algorithm for deciding quadratic residuosity in finite fields GF(p^m). Inform. Process. Lett. **30**(3) (1989) 111–114