ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, *25-27 June*, *2017*, *pp. 940-944*
doi: 10.18178/wcse.2017.06.163

Constructing Weak Curves ECDLP-Equivalent to Ordinary Curves via Elliptic Surfaces

Yuhong Zhang [1], Bo Peng [1] and Maozhi Xu [1+]

[1] LMAM, School of Mathematical Sciences, Peking University, No.5 Yiheyuan Rd., Haidian District, Beijing 100871

Abstract. The elliptic curve discrete logarithm problem(ECDLP) is the basis for the security of elliptic curve cryptography. Up to now, there is no subexponential algorithm for ECDLP. Only certain classes of weak curves exist whose standard ECDLP can be reduced to sample problems, like supersingular curves, anomalous curves etc. Elliptic surfaces are algebraic surfaces containing a pencil of elliptic curves (also means fibers). In order to reduce ordinary curves to weak curves using connections among these fibers, we define the ECDLP-equivalence of specialized-reduced points in the sense of the same section to elliptic surfaces (hereafter shortened as ECDLP-equivalence). We make a discovery that the ECDLP-equivalence is only related to the order of specialized-reduced points, and present an algorithm for constructing supersingular curves ECDLP-equivalent to ordinary curves via elliptic surfaces. In the end, we illustrate a 256-bit example.

Keywords: elliptic surfaces, ECDLP-Equivalence, supersingular curves, rank one lifting problem.

1. Introduction

The hardness of the elliptic curve discrete logarithm problem(ECDLP) is crucial to the security of elliptic curve cryptography. Elliptic curves suitable for cryptographic application are defined over binary or prime fields. Let $\tilde{E}$ be an elliptic curve over $\mathbb{F}_p$ (p is a prime) and points $\tilde{S}, \tilde{T}$, the ECDLP is to find the integer m satisfying $\tilde{T} = m\tilde{S}$. Elliptic surfaces are considered as one-parameter algebraic families of elliptic curves over function fields [2]. We aim at lifting ordinary curves to an elliptic surface over $\mathbb{Q}$. If the connections among the fibers exist, the designers are very likely to know more information about Elliptic Curve Cryptography, then the security of the whole system may be compromised.

Index Calculus, a lifting algorithm, can be used to solve the discrete logarithm problem (DLP) over finite fields in subexponential time. But two main approaches via lifting, Index Calculus and Xedni Calculus, cannot be efficient for the elliptic curves [3-6,9]. In order to find certainly linear dependence, the rank of the lifted curve $E/\mathbb{Q}$ should be lower than the number of lifted points, so it is not difficult to find the relation in $E(\mathbb{Q})$. Two points must be linearly dependent in the rank one case. Then ECDLP is equivalent to finding a good lifting. Using the good lifting and the relation of the lifted points, one can solve ECDLP for $\tilde{E}/\mathbb{F}_p$.

In [10-11], the authors proposed efficient algorithms to find dependence relation if they could lift two points to an elliptic curve over $\mathbb{Q}$ with rank one. Earlier similar work of [7] hoped to look for appropriate lifts among the family of curves over $\mathbb{Q}$. In William George's PhD thesis [8], the equivalence between rank one elliptic surfaces lifting problem and the ECDLP has been investigated in depth.

In this paper, we implement the algorithm to solve ECDLP assuming that the rank one lifting problem of the elliptic curves over $\mathbb{Q}(t)$ is solvable. Then we find a proposition that the ECDLP-equivalence of specialized-reduced points is only related to the order of these points. So we can make weak curves ECDLP-

+ Corresponding author. Tel.: 010-62753810; fax: 010-62753810.
E-mail address: mzxu@pku.edu.cn.

equivalent to ordinary curves by specialization-reduction maps. The rest of paper is organized as follows. We briefly describe the basic backgrounds in Section 2. After an example of rank one lifting, the details of ECDLP-equivalence and main proposition can be seen in Section 3 and the corresponding construction algorithm in Section 4. Then we cite an instance of constructing a 256-bit supersingular curve with the embedding degree 2, whose subgroup is ECDLP-equivalent to a 256-bit ordinary curve via the elliptic surface $y^2 = x^3 + b(t)$. In the end the conclusion is drawn and the future research direction proposed.

2. Preliminary

2.1. Elliptic surfaces

From [1,2], we can see that an elliptic surface has a proper connected morphism to an algebraic curve, almost all of whose fibers are elliptic curves.

Definition 1. Let C be a smooth projective curve. An *elliptic surface* $\mathcal{E}$ over C is a smooth projective surface with an elliptic fibration over C, i.e. a surjective morphism

$$\pi: \mathcal{E} \longrightarrow C$$

such that

- For all but finitely many points $t \in C(\bar{k})$, the fiber
$$\mathcal{E}_t: \pi^{-1}(t)$$
is a non-singular curve of genus 1;
- No fiber contains a curve of self-intersection number -1;
- Exists a section to π, namely a morphism
$$\sigma_0: C \longrightarrow \mathcal{E}$$
such that $\pi \circ \sigma_0 = id_C$, where σ_0 is called zero section.

The Mordell-Weil Theorem for function fields tells that the Mordell-Weil group $E(\mathbb{Q}(t))$ is a finitely generated abelian group, with the form

$$E(\mathbb{Q}(t)) \cong E(\mathbb{Q}(t))_{tors} \times \mathbb{Z}^r,$$

where the torsion subgroup $E(\mathbb{Q}(t))_{tors}$ is finite and the nonnegative integer r is called the rank of E.

Theorem 1 (Silverman's Specialization Theorem[1]). Let k be a number field, and C/k be a curve, and let E be an elliptic curve defined over the function field $k(C)$. Assume that E is nonconstant, i.e., $j(E) \notin k$. Then the specialization map of E at t

$$\sigma_t: E(\mathbb{Q}(t)) \to E_t(\mathbb{Q})$$

is well-defined and injective(called a specialization) for all but finitely many points $t \in C(k)$.

More generally, the set of points $t \in C(\bar{k})$ for which σ_t is not injective is a set of bounded height (these E_t's are also called exceptional specializations). Those E_t's with discriminant $\Delta \neq 0$ are called good specializations, and others degenerate specializations.

2.2. Lifting Problem of Elliptic Surfaces

Definition 2. Let $\tilde{E}/\mathbb{F}_p$ be an elliptic curve over $\mathbb{F}_p$ and $\tilde{P}_1, \tilde{P}_2, \cdots, \tilde{P}_l \in \tilde{E}(\mathbb{F}_p)$ be the points of $\tilde{E}(\mathbb{F}_p)$. The *lifting problem* for $(\tilde{E}, \tilde{P}_1, \cdots, \tilde{P}_l)$ is to find $(E, P_1, \cdots, P_l)$ which is defined as follows:

The elliptic curve to $\mathrm{E}/\mathbb{Q}(\mathrm{t})$ is the lifted curve of $\widetilde{\mathrm{E}}/\mathbb{F}_{\mathrm{p}}$: $\widetilde{\mathrm{E}}$ denotes the good reduction modulo p of E, i.e., $E \equiv \tilde{E}\ mod\ p$;

- $P_1, \cdots, P_l \in E(\mathbb{Q}(t))$ are the lifted points of $\tilde{P}_i$'s: i.e., $P_i \equiv \tilde{P}_i\ mod\ p$, $1 \leq i \leq l$.

Furthermore, if $P_1, \cdots, P_l$ are linearly dependent, we call $P_1, \cdots, P_l$ the good lifting.

Remark: If the rank r of $E(\mathbb{Q}(t))$ is strictly less than l, the linear dependence of $P_1, \cdots, P_l$ must be established. In this case we have a good lifting. So, without loss of generality, we can assume that the lifted points $P_1, \cdots, P_r$ are the generators of $E(\mathbb{Q}(t))/E(\mathbb{Q}(t))_{tors}$.

3. ECDLP-Equivalence by Specialization-Reduction Maps

3.1. ECDLP algorithm after finding a rank one lifting

Theorem 2. Let $E/\mathbb{Q}(t)$ be a rank one elliptic curve, and $S, T \in E\big(\mathbb{Q}(t)\big)$. Suppose there exist $k_1, k_2 \in \mathbb{Z}$ such that $\frac{\hat{h}(T)}{\hat{h}(S)} = \left(\frac{k_2}{k_1}\right)^2$ and $(k_1, k_2) = 1$, if k_1, k_2 are both positive/negative, $k_2S - k_1T \in E\big(\mathbb{Q}(t)\big)_{tors}$, else then $k_2S + k_1T \in E\big(\mathbb{Q}(t)\big)_{tors}$.

Proof: Let P_0 be the generator of E, then we can find $l_1, l_2 \in \mathbb{Z}$ and $S', T' \in E(\mathbb{Q}(t))_{tors}$ such that $S = l_1P_0 + S', T = l_2P_0 + T'$. So

$$\hat{h}(S) = l_1^2\hat{h}(P_0) \text{ and } \hat{h}(T) = l_2^2\hat{h}(P_0),$$

$\frac{\hat{h}(T)}{\hat{h}(S)}$ is a rational square.

Suppose we find k_1, k_2 satisfied above condition, then $\frac{k_2}{k_1} = \frac{l_2}{l_1}$ or $\frac{k_2}{k_1} = -\frac{l_2}{l_1}$. If $\frac{k_2}{k_1} = \frac{l_2}{l_1}$, then let $l_2 = dk_2$, $l_1 = dk_1$, so $S = dk_1P_0 + S', T = dk_2P_0 + T'$, hence $k_2S - k_1T = k_2S' - k_1T' \in E(\mathbb{Q}(t))_{tors}$.

Similarly, if $\frac{k_2}{k_1} = -\frac{l_2}{l_1}$, then

$$k_2S' + k_1T' \in E(\mathbb{Q}(t))_{tors}.$$

We can get the following Algorithm 1 assuming finding a rank one lifting elliptic surface:

Algorithm 1. ECDLP Algorithm after Finding a Rank One Lifting

Input: rank one good lifting $(E/\mathbb{Q}(t), S, T)$ of $(\tilde{E}/\mathbb{F}_p, \tilde{S}, \tilde{T})$;

Output: m such that $\tilde{T} = m\tilde{S}$.

1. Find $k_1, k_2 \in \mathbb{Z}$ such that $\frac{\hat{h}(T)}{\hat{h}(S)} = \left(\frac{k_2}{k_1}\right)^2$ and $(k_1, k_2) = 1$;
2. If $k_2S - k_1T \in E(\mathbb{Q}(\mathrm{t}))_{tors}$, then

$$m \equiv \frac{k_2 \bmod p}{k_1 \bmod p} \, mod\big(ord\big(\tilde{S}\big)\big),$$

3. else if $k_2S + k_1T \in E(\mathbb{Q}(\mathrm{t}))_{tors}$, then

$$m \equiv -\frac{k_2 \bmod p}{k_1 \bmod p} \, mod\big(ord\big(\tilde{S}\big)\big).$$

3.2. Main Proposition

According to Algorithm 1, we can draw a conclusion that the value of ECDLP on the fibers of an elliptic surface is only related to the order of the point $\tilde{S}$ in the period of mod p. So we can give our main proposition about the ECDLP-equivalence.

Definition 3. Let $\pi: \mathcal{E} \longrightarrow C$ be an elliptic surface, and let E/K be the associated elliptic curve, $K = k(C)$ is the function field of C. Let σ_t be the specialization map, and φ_p be the good reduction map:

$$\begin{matrix} E/K \overset{\sigma_t}{\to} E_t \overset{\varphi_p}{\to} \tilde{E}_t \\ P \longmapsto P_t \mapsto \tilde{P}_t \end{matrix},$$

then the composite mapping $\tau = \sigma_t \circ \varphi_p$ is called the specialization-reduction map from E/K to $\tilde{E}_t$, $\tilde{E}_t = \tau(E) = \varphi_p(\sigma_t(E))$ are called the specialized-reduced curves, $\tilde{P}_t = \tau(P) = \varphi_p(\sigma_t(P))$ called the specialized-reduced points.

Remark: The two specialized-reduced curves can be defined over two different base fields.

Definition 4. Using the specialization-reduction map τ, We call two specialized-reduced points $\tilde{P}_{t_1}, \tilde{P'}_{t_2}$ are section-equivalent(in the sense of the same section σ_P) if and only if $ord\big(\tilde{P}_{t_1}\big) = ord(\tilde{P'}_{t_2})$ shortened as section-equivalent, denoted by $\tilde{P}_{t_1} \sim \tilde{P'}_{t_2}$.

In particularly, if the two reduction maps φ_p are the same, we call two specialized-reduced points $\tilde{P}_{t_1}, \tilde{P}_{t_2}$ are section-equivalent over the same base fields, denoted by $\tilde{P}_{t_1} \sim \tilde{P}_{t_2}$.

Proposition 1. Using the specialization-reduction map τ, in the period of the reduction map, if the specialized-reduced points are ECDLP-equivalent, the specialized-reduced points have the same value of ECDLP.

The proof of this proposition is obvious, and is independent of the sequence of composite mapping.

According to Proposition 1, we can construct weak curves which are ECDLP-equivalent to the ordinary curves, such as supersingular curves, anomalous curves, and so on.

4. Constructing Weak Curves

4.1. Algorithm to construct supersingular curves

We know that the Algorithm 3.3 [14] is about the construction of supersingular elliptic curve. So, an algorithm to construct supersingular curves whose subgroups are section-equivalent to ordinary curves via elliptic surfaces can be stated as follows.

Algorithm 2. Algorithm for constructing supersingular curves

Input: an elliptic curve $E: y^2 = x^3 + b(t)$ over function filed $\mathbb{Q}(t)$, along with a point $P \in E(\mathbb{Q}(t))$;

Output: a supersingular specialized-reduced curve $\tilde{E}'_{t_2}/\mathbb{F}_{p_2}$, whose subgroup is section-equivalent to the ordinary specialized-reduced curve $\tilde{E}_{t_1}/\mathbb{F}_{p_1}$.

1. Find a prime $p \equiv 3(mod4)$, $p \not\equiv 5(mod6)$ and a t_1, such that $\tilde{E}_{t_1}/\mathbb{F}_{p_1}$ is an ordinary specializedreduced curve, with $\#(\tilde{E}_{t_1}(\mathbb{F}_{p_1})) = ord(\tilde{P}_{t_1}) = n$;
2. Find u such that $u * n - 1$ is a prime, and $u * n - 1 \equiv 5 \pmod 6$, then let $p_2 = u * n - 1$;
3. Find a specialization t_2, such that $\tilde{E}'_{t_2}/\mathbb{F}_{p_2}$ is a supersingular specialized-reduced curve, with $\#(\tilde{E}'_{t_2})/ord(\tilde{P}'_{t_2}) = u$, i.e., $ord(\tilde{P}_{t_1}) = ord(\tilde{P}'_{t_2}) = n$;
4. Return $\tilde{E}'_{t_2}/\mathbb{F}_{p_2}$.

4.2. A constructing example

So, we can construct weak curves via the elliptic surface

$$E: y^2 = x^3 + (2t^3 + 1)$$

with $P = (t^2, t^3 + 1) \in E(\mathbb{Q}(t))$ (implemented in Magma).

Let $S, T \in E$ be two points. Without losing generality, we choose the simple points representation, such as

$$S = 5 * P \text{ and } T = 13 * P,$$

$\tilde{E}_{t_1}, \tilde{E}'_{t_2}, \tilde{E}'_{t_3}$ are specialized-reduced curves, and $\tilde{P}_{t_1}, \tilde{P}'_{t_2}, \tilde{P}'_{t_3}, \tilde{S}_{t_1}, \tilde{S}'_{t_2}, \tilde{S}'_{t_3}, \tilde{T}_{t_1}, \tilde{T}'_{t_2}, \tilde{T}'_{t_3}$ are specialized-reduced points. Notice $\tilde{P}_{t_1}, \tilde{P}'_{t_2}, \tilde{P}'_{t_3}$ are all located in the same section σ_P. Correspondingly, $\tilde{S}_{t_1}, \tilde{S}'_{t_2}, \tilde{S}'_{t_3}$ are all located in σ_S, and $\tilde{T}_{t_1}, \tilde{T}'_{t_2}, \tilde{T}'_{t_3}$ in σ_T, where

- $t_1 = 2$,
  $p_1 = 57896044618658097711785492504343953926634992332820282019728792003956564820063$,
  $\tilde{E}_{t_1}/\mathbb{F}_{p_1}$ defined by
  $$y^2 = x^3 + 17$$
  is a 256-bit ordinary curve, and $\tilde{P}_{t_1} = \tau(P) = \varphi_{p_1}\left(\sigma_{t_1}(P)\right)$,
  $ord(\tilde{P}_{t_1}) = 57896044618658097711785492504343953926314260984279980125913588529494218755601$,
  Computer $m \equiv \frac{13}{5} \, mod\left(ord(\tilde{P}_{t_1})\right) = 23158417847463239084714197001737581570525704393711992050365435411797687502243$,
  So $\tilde{T}_{t_1} = m * \tilde{S}_{t_1}$.
- $t_2 = 6$,
  $p_2 = 11579208923731619542357098500868790785262852196855996025182717705898437511201$,
  $\tilde{E}'_{t_2}/\mathbb{F}_{p_2}$ defined by
  $$y^2 = x^3 + 433$$
  is a 256-bit supersingular curve (with the embedding degree 2), and $\tilde{P}'_{t_2} = \tau(P) = \varphi_{p_2}\left(\sigma_{t_2}(P)\right)$,

$ord(\tilde{P}'_{t_2}) = ord(\tilde{P}_{t_1})$,
Verify $\tilde{T}'_{t_2} = m * \tilde{S}'_{t_2}$, i.e. $\tilde{P}'_{t_2} \sim \tilde{P}_{t_1}$.

- $t_3 = 1$,
  $p_3 = 57896044618658097711785492504343953926634992332820282019728792003956564820109$,
  $\tilde{E}'_{t_3}/\mathbb{F}_{p_3}$ defined by
  $$y^2 = x^3 + 3$$
  is a 256-bit supersingular curve (with the embedding degree 2), and $\tilde{P}'_{t_3} = \tau(P) = \varphi_{p_3}\left(\sigma_{t_3}(P)\right)$,
  $ord(\tilde{P}'_{t_3}) \neq ord(\tilde{P}_{t_1})$,
  Verify $\tilde{T}'_{t_3} \neq m * \tilde{S}'_{t_3}$, i.e. $\tilde{P}'_{t_3} \nsim \tilde{P}_{t_1}$.

To summarize, $\because ord(\tilde{P}'_{t_2}) = ord(\tilde{P}_{t_1}),\ \therefore \tilde{P}'_{t_2} \sim \tilde{P}_{t_1}$,
on the other hand, $\because ord(\tilde{P}'_{t_3}) \neq ord(\tilde{P}_{t_1}),\ \therefore \tilde{P}'_{t_3} \nsim \tilde{P}_{t_1}$.

5. Conclusion

In this paper, we draw a conclusion that the ECDLP-equivalence (in the sense of the same section to elliptic surfaces) of specialized-reduced points is only related to the order of these points. To put theories to the test, we give an example of constructing a 256-bit supersingular curves with the embedding degree 2, whose subgroup is ECDLP-equivalent to a 256-bit ordinary curve via the elliptic surface $y^2 = x^3 + b(t)$.

6. References

[1] Silverman, J. H. The Arithmetic of Elliptic Curves, Graduate Texts in Math. Springer-Verlag, Berlin-Heidelberg-New York (1986).

[2] Silverman, J. H. Advanced topics in the Arithmetic of Elliptic Curves, Springer-Verlag, 1994.

[3] Jacobson, M., Koblitz, J. N., Silverman, J. H., Stein, A., and Teske, E. Analysis of the Calculus Attack, Designs, Codes and Cryptography 20 (2000), pp. 41-64.

[4] Miller, V. S. Use of elliptic curves in cryptography, Advances in Cryptology, CRYPTO'85, LNCS, 218 (1986), 417-426.

[5] Silverman, J. H. The Xedni calculus and the elliptic discrete logarithm problem, Designs, Codes and Cryptography, 20 (2000), 5-40.

[6] Silverman, J. H. and Suzuki, J. Elliptic curve discrete logarithms and the index calculus. ASIACRYPT 1998. LNCS, vol. 1514, pp. 110-125. Springer, Heidelberg (1998).

[7] Qi Cheng and Ming-Deh Huang, On partial lifting and the elliptic curve discrete logarithm problem, In Algorithms and computation, volume 3341 of Lecture Notes in Comput. Sci., pages 342-351. Springer, Berlin, 2004.

[8] George, W., Lifting Problems, Cross-fiberedness, and Diffusive Properties on Elliptic Surfaces, PhD thesis, University of Toronto, 2015, http://blog.math.toronto.edu/GraduateBlog/files/2015/08/George_Thesis.pdf.

[9] Kim, H. J., Cheon J. H., and Hahn, S. G. Elliptic curve lifting problem and its applications, Proc. Japan Acad. Ser. A Math. Sci, vol. 75(9), pp. 166-169, 1999.

[10] Cheon, J. H., Lee, D. H., Hahn, S. G., and Chee, S. Elliptic curve discrete logarithms and wieferich primes, Technical report of IEICE, ISEC, (1999), No. 584, 53-60.

[11] Daghigh, H., Didari, S., and Shahpar, F. S. Computing elliptic curve discrete logarithm via lifting, in 2013 10th International ISC Conference on Information Security and Cryptology (ISCISC). 2013: 1-4.

[12] Luijk, V. An elliptic K3 surface associated to Heron triangles. J. Number Theory 123 (2007), no. 1, 92-119.

[13] Cullinan, J., and Sekowski., C., On Quadratic Jacobi Polynomials, http://math.bard.edu/cullinan/papers/low_jac_submitted.pdf.

[14] Freeman, D., Scott, M., Teske, E. (2010). A taxonomy of pairing-friendly elliptic curves. Journal of Cryptology, 23(2), 224-280.

[15] Shioda, T., On the Mordell-Weil lattices, Comment. Math. Univ. St. Paul. 39 (1990), no. 2, 211240.