LETTER Special Section on Discrete Mathematics and Its Applications

Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems

Taiichi SAITO[†], *Member*, Fumitaka HOSHINO[†], *Nonmember*, Shigenori UCHIYAMA[†], *and* Tetsutaro KOBAYASHI[†], *Members*

SUMMARY This paper provides methods for construction of pairing-based cryptosystems based on non-supersingular elliptic curves.

key words: *non-supersingular elliptic curve, pairing-based cryptosystem, the Weil and the Tate pairings*

1. Introduction

Since the discovery by Joux and Nguyen [13], of the existence of point groups on supersingular elliptic curves in which the DDH problem is easy, and the works of Sakai, Ohgishi and Kasahara [18] and Joux [11], *pairing-based cryptosystems* have been becoming one of the most active area of research in cryptography. However the underlying elliptic curves for many pairing-based cryptosystems have been often restricted to be supersingular.

This paper provides methods that allow us to use *non-supersingular* elliptic curves in pairing-based cryptosystems.

1.1 Related Works

The intractability of the Decision Diffie-Hellman (DDH) problem, the DDH assumption, has been receiving increasing attention as an underlying assumption in the design of provably secure schemes since the resulting schemes are often more efficient than others [6].

Let $\mathbb{G}$ be a cyclic group generated by P; P has prime order l. The *Decision Diffie-Hellman problem in* $\mathbb{G}$ is for given (P, aP, bP, cP) to decide whether or not $c = ab \bmod l$ holds (see [6]).

However Joux and Nguyen [13] pointed out that the DDH problem in a $\mathbb{F}_q$-rational point group $\mathbb{G}$ of prime order on a special class of supersingular elliptic curves over $\mathbb{F}_q$ with the so-called distorsion map ψ (see [21]) is easy. In their proof, they constructed a non-degenerate bilinear map $\hat{e}$ from $\mathbb{G}$ to $\overline{\mathbb{F}}_q^{\times}$ by combining the Weil pairing e with the distorsion map ψ as follows:

$$\hat{e}(\cdot,\cdot) = e(\psi(\cdot),\cdot) : \mathbb{G}\times\mathbb{G} \to \overline{\mathbb{F}}_q^{\times}$$
$$; (P_1, P_2) \mapsto \hat{e}(P_1, P_2) = e(\psi(P_1), P_2).$$

Joux and Nguyen's result on the DDH problem and the ideas of the Sakai-Ohgishi-Kasahara [18] and the Joux [11] papers have led us to a new field in cryptography, *pairing-based cryptosystems*, in the construction of which the bilinear map is used as building block, and recently pairing-based cryptosystem is one of the most active fields of research in cryptography.

Many pairing-based cryptosystems are based on the above type of non-degenerate bilinear maps (i.e., the domain consists of the direct product of two copies of *a cyclic group*). On the other hand, for any cyclic group $\mathbb{G}$ and for any $P_1, P_2 \in \mathbb{G}$, the value of the Weil pairing e is constant (i.e., $e(P_1, P_2) = 1$). Then, in order to make pairing non-degenerate, the distorsion map has been used, which maps points in $\mathbb{G}$ to points in other cyclic group, and combination of the Weil pairing and the distorsion map achieves the property of non-degeneracy. However it is known that there exists no distorsion map on non-supersingular elliptic curves and then the underlying elliptic curves for pairing-based cryptosystems have beenoften restricted to be supersingular.

Remark 1: Barreto, Kim, Lynn and Scott [3] pointed out that a few pairing-based cryptosystems do not require distorsion maps and in such systems, pairings on non-supersingular curves can be used as building block. Miyaji, Nakabayashi and Takano [15], Barreto, Lynn and Scott [5] and Dupont, Enge and Morain [10] discussed constructions of non-supersingular elliptic curves for pairing-based cryptosystems. Barreto, Lynn and Scott [4] discussed how to select distinct two cyclic groups in non-supersingular elliptic curves so that pairing is non-degenerate (Similar results were proposed in [14], [16]).

Remark 2: It is also shown in [13] that the DDH problem on a special class of non-supersingular elliptic curves, *the trace-2 curves*, is easy.

Verheul [21] showed the existence of point groups on non-supersingular elliptic curves in which the DDH problem is easy. The technique is related to our selection of point groups and construction of the map for non-degenerate bilinear map.

Remark 3: The non-existence of distorsion map on non-supersingular elliptic curve was shown implicitly in [22] and explicitly in [19], and recently rediscovered in [21].

Manuscript received August 22, 2003.
Manuscript revised November 10, 2003.
Final manuscript received January 5, 2004.

[†]The authors are with NTT Information Sharing Platform Laboratories, Kanagawa-ken, 239-0847 Japan.

1.2 Preliminaries

In this paper, we follow the notation and definition in *Silverman's book* [20] for elliptic curves. Let E be a non-supersingular elliptic curve over a finite field with q elements, $\mathbb{F}_q$, and ϕ denote the q^{th}-power Frobenius endomorphism on E. Let $P \in E(\mathbb{F}_q)$ be a point of order l and $E[l]$ denote the l-torsion points group.

In this paper, we assume that the order l is odd prime number other than the characteristic of $\mathbb{F}_q$ and that $l \nmid (q-1)$, which imply $E[l] \not\subset E(F_q)$ and *the trace of* $\phi \neq 2$. Let k denote the smallest positive integer such that $l | (q^k - 1)$. Then it follows that $E[l] \subset E(\mathbb{F}_{q^k})$ (see [2]).

Since $l \nmid (q-1)$, a $\mathbb{Z}/l\mathbb{Z}$-linear representation of (the action of) ϕ on $E[l]$ has two distinct eigenvalues, 1 and $q \bmod l$, and then there is a point $Q(\neq O) \in E[l]$ such that $\phi(Q) - [q \bmod l]Q = O$. Thus we see that $E[l]$ is decomposed as $E[l] = \langle P \rangle \oplus \langle Q \rangle$ and that the cyclic groups $\langle P \rangle$ and $\langle Q \rangle$ are the eigenspaces corresponding to the eigenvalues 1 and $q \bmod l$, and annihilated by $(\phi - 1)$ and $(\phi - [q \bmod l])$, respectively. Moreover we have the following group isomorphism:

$$\begin{aligned}(\mathrm{proj}_1, \mathrm{proj}_2) &: E[l] \to \langle P \rangle \times \langle Q \rangle \\ &; r_1 P + r_2 Q \mapsto (r_1 P, r_2 Q)\end{aligned}$$

where we define proj_1 and proj_2 as

$$\begin{aligned}\mathrm{proj}_1 &: E[l] \to \langle P \rangle; R \mapsto \mathrm{proj}_1(R) \\ &= [(1-q)^{-1} \bmod l] \circ (\phi - [q \bmod l])R \\ \mathrm{proj}_2 &: E[l] \to \langle Q \rangle; R \mapsto \mathrm{proj}_2(R) \\ &= [(q-1)^{-1} \bmod l] \circ (\phi - 1)R.\end{aligned}$$

There are $l + 1$ subgroups of order l in $E[l]$, which consist of the two eigenspaces $\langle P \rangle$ and $\langle Q \rangle$, and the other $l - 1$ groups different from the eigenspaces, $G_1, \ldots, G_{l-1}$. The Frobenius endomorphism ϕ sends any group G_i to other group G_j (i.e., $\phi(G_i) = G_j$ and $i \neq j$). Verheul [21] showed the DDH problem in any non-eigenspace G_i is easy, where it was used that for the Weil or the Tate pairing e, $e(\phi(\cdot), \cdot)$ is a non-degenerate bilinear map from G_i to $\mathbb{F}_{q^k}^{\times}$.

On the other hand, the endomorphisms proj_1 and proj_2 send any G_i to the eigenspaces $\langle P \rangle$ and $\langle Q \rangle$, respectively. Then, by constructing a non-degenerate bilinear map of the form $e(proj(\cdot), \cdot)$ from G_i to $\mathbb{F}_{q^k}^{\times}$, we obtain the same result on the DDH problem as in [21].

Note: Since proj_1 and proj_2 commute with any endomorphism, each eigenspace of the Frobenius endomorphism is stable by the action of any endomorphism α (i.e., $\alpha(\langle P \rangle) \subset \langle P \rangle$ and $\alpha(\langle Q \rangle) \subset \langle Q \rangle$ for any $\alpha \in \mathrm{End}(E)$). Then for any α, $e(\alpha(\cdot), \cdot)$ should not be non-degenerate on $\langle P \rangle$ nor $\langle Q \rangle$. Hence the techniques of combination of the Weil or the Tate pairings with endomorphism cannot be applied to the DDH problems in the eigenspaces, $\langle P \rangle$ and $\langle Q \rangle$.

2. Pairing-based cryptosystems on non-supersingular elliptic curves

Almost pairing-based cryptosystems require that the domain of the underlying bilinear map be the direct product of two copies of a cyclic group, and such bilinear maps have been constructed by combining the Weil or the Tate pairing with distorsion map. Joux pointed out in his survey on pairing-based cryptosystems [12] that since the distorsion maps exist only on supersingular elliptic curves and not on non-supersingular curves, *"it is usually more practical to use supersingular curve"* in pairing-based cryptosystems.

However there is a concern that supersingular elliptic curves may not be as secure as non-supersingular ones (see [3], [15]). Additionally, while the so-called embedding degree [3] for supersingular curves is restricted to be less than or equal to 6, non-supersingular has no such restriction. Then it may be desirable to adopt non-supersingular elliptic curve as the underlying curve of pairing-based cryptosystems.

This section suggests methods that allow us to use *non-supersingular* elliptic curves in pairing-based cryptosystems: a selection of cyclic point groups on the curves, a method to verify that a point is in the group, a method to randomly choose a point from the group and a construction of non-degenerate bilinear map from the direct product of two copies of the cyclic group to finite field.

The selection of cyclic point groups: Let P, Q be as in the previous section. Use a cyclic group generated by R, $\langle R \rangle$, such that the generator R has the form of $R = r_1 P + r_2 Q$ and $r_1, r_2 \in (\mathbb{Z}/l\mathbb{Z})^{\times}$.

When P, Q are given, such R can be constructed by choosing $r_1, r_2 \in (\mathbb{Z}/l\mathbb{Z})^{\times}$ and computing $R = r_1 P + r_2 Q$. Alternatively, we can generate R by randomly choosing a point $R \in E[l]$ and verifying $\mathrm{proj}_1(R) \neq O$ and $\mathrm{proj}_2(R) \neq O$ hold.

Polynomial-time recognition of $\langle R \rangle$: Given the generator R, we can construct a polynomial-time algorithm that decides whether or not a given $R' \in E[l]$ is in $\langle R \rangle$.

We can decide $R' \in E[l]$ is in $\langle R \rangle$ or not by computing the Weil pairing $e(R, R')$ since $e(R, R') = 1$ iff $R' \in \langle R \rangle$.

Polynomial-time samplable uniform distribution on $\langle R \rangle$: Given the generator R, we can construct a probabilistic polynomial-time algorithm whose output is randomly and uniformly distributed on $\langle R \rangle$.

The algorithm randomly chooses $r \in \mathbb{Z}/l\mathbb{Z}$ and outputs $R' = [r]R$.

The construction of of non-degenerate bilinear map: We can construct a non-degenerate bilinear map b from $\langle R \rangle \times \langle R \rangle$ to $\mathbb{F}_{q^k}^{\times}$.

For the Weil or the Tate pairing e and any endomorphism $\alpha \in \{\mathrm{proj}_1, (\phi - [q \bmod l]), \mathrm{proj}_2, (\phi - 1)\}$, the following b is non-degenerate bilinear map:

$$b(\cdot,\cdot) : \langle R \rangle \times \langle R \rangle \to \mathbb{F}_{q^k}^{\times}$$
$$; (R_1, R_2) \mapsto b(R_1, R_2) = e(\alpha(R_1), R_2)$$

It is easy to see that $\mathrm{proj}_1(\langle R \rangle) = (\phi - [q \bmod l])(\langle R \rangle) = \langle P \rangle$ and $\mathrm{proj}_2(\langle R \rangle) = (\phi - 1)(\langle R \rangle) = \langle Q \rangle$. Since $\langle R \rangle \neq \langle P \rangle, \langle Q \rangle$, the map b is non-degenerate.

Using these methods, we can construct variants of the key agreement protocols in [1], [11], [21] and the verifiable random function in [9] based on the cyclic group $\langle R \rangle$ and the non-degenerate bilinear map b[†]. On the other hand, our cyclic group $\langle R \rangle$ seems not directly applicable to other important areas of pairing-based cryptosystems, identity-based cryptosystems [7] and signature schemes [8], since embedding identities into the group and constructing hash function that outputs elements in $\langle R \rangle$ and behaves as truly random function seem difficult.

Remarks: The groups $\langle R \rangle$ that appear in the above selection are the same as the groups the DDH problem on which were shown to be easy by Verheul [21]. Moreover, based on the way by Verheul [21] of transforming $\langle R \rangle$ to other group with the Frobenius endomorphism ϕ, we can also construct other bilinear map c on $\langle R \rangle$ as $c(\cdot,\cdot) = e(\phi(\cdot),\cdot)$ and also apply it to pairing-based cryptosystems.

The evaluation of $\mathrm{proj}_1(R')$ and $(\phi - [q \bmod l])(R')$ requires almost the same computation complexity as scalar multiplication, $O((\log q^k)^3)$. While $\phi(R')$ is not $\mathbb{F}_q$-rational for $R' \in \langle R \rangle \setminus \{O\}$, $\mathrm{proj}_1(R')$ and $(\phi - [q \bmod l])(R')$ are $\mathbb{F}_q$-rational. Then the computation of the pairing e for the bilinear map b is comparable with that for the bilinear map c.

3. Conclusion

This paper provided methods that allow us to use non-supersingular elliptic curves in pairing-based cryptosystems, which realizes some key agreement protocols and a verifiable random function based on non-supersingular curves.

[†] Joux [11] presented a key agreement protocol which also does not require the underlying curve to be supersingular (see the Sakai-Mitsunari-Kasahara paper [17]). Their protocol is secure under the co-BDH assumption [7], which is an extension of the BDH assumption [7]. On the other hand, the key agreement protocol based on our bilinear map is secure under the BDH assumption, and then can be considered as a special case of [17].

References

[1] S.S. Al-Riyami and K.G. Paterson, "Authenticated three party key agreement protocols from pairings," `http://eprint.iacr.org`

[2] R. Balasubramanian and N. Koblitz, "Improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm," J. Cryptol., vol.2, no.11, pp.141–145, 1998.

[3] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," Proc. Crypto 2002, LNCS 2442, pp.354–368, Springer-Verlag, 2002.

[4] P.S.L.M. Barreto, B. Lynn, and M. Scott, "On the selection of pairing-friendly groups," `http://eprint.iacr.org`

[5] P.S.L.M. Barreto, B. Lynn, and M. Scott, "Constructing elliptic curves with prescribed embedding degrees," Proc. SCN'2002, LNCS 2576, pp.257–267, Springer-Verlag, 2003.

[6] D. Boneh, "The decision Diffie-Hellman problem," Proc. ANTS-III, LNCS 1423, pp.48–63, Springer-Verlag, 1998.

[7] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," Proc. Crypto 2001 and full version, LNCS 2139, pp.213–229, Springer-Verlag, 2001.

[8] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing," Proc. Asiacrypt 2001, LNCS 2248, pp.514–532, Springer-Verlag, 2001.

[9] Y. Dodis, "Efficient Construction of (Distributed) Verifiable Random Functions," Proc. PKC'2003, LNCS 2567, pp.1–17, Springer-Verlag, 2003.

[10] R. Dupont, A. Enge, and F. Morain, "Building curves with arbitrary small MOV degree over finite prime fields," `http://eprint.iacr.org`

[11] A. Joux, "A one round protocol for tripartite Diffie-Hellman," Proc. ANTS IV, LNCS1838, pp.385–394, Springer-Verlag, 2000.

[12] A. Joux, "The Weil and tate pairings as building blocks for public key cryptosystems," Proc. ANTS 2002, LNCS2369, pp.20–32, Springer-Verlag, 2002.

[13] A. Joux and K. Nguyen, "Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups," `http://eprint.iacr.org`

[14] N. Kanayama, T. Kobayashi, T. Saito, and S. Uchiyama, "Remarks on elliptic curve discrete logarithm problems," IEICE Trans. Fundamentals, vol.E83-A, no.1, pp.17–23, Jan. 2000, `http://search.ieice.or.jp/index-e.html`

[15] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," IEICE Trans. Fundamentals, vol.E84-A, no.5, pp.1234–1243, May 2001, `http://search.ieice.or.jp/index-e.html`

[16] T. Saito and S. Uchiyama, "A Remark on the MOV algorithm for non-supersingular elliptic curves," IEICE Trans. Fundamentals, vol.E84-A, no.5, pp.1266–1268, May 2001, `http://search.ieice.or.jp/index-e.html`

[17] R. Sakai, S. Mitsunari, and M. Kasahara, "Cryptographic schemes based on pairing over elliptic curve," ISEC2001-29, 2001.

[18] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," Proc. SCIS 2000, 2000.

[19] R. Schoof, "Nonsingular plane cubic curves over finite fields," J. Comb. Theory A, vol.46, pp.183–211, 1987.

[20] J.H. Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, 1986.

[21] E.R. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems," Proc. Eurocrypt 2001, LNCS 2045, pp.195–210, Springer-Verlag, 2001.

[22] W.C. Waterhouse, "Abelian varieties over finite fields," Ann. Sci. École Norm. Sup., Ser. 2, no.4, pp.521–560, 1969.