社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

非特異楕円曲線上の一方向性関数の提案

齊藤　泰一[†]　　星野　文学[†]　　内山　成憲[†]　　小林鉄太郎[†]

[†] NTT 情報流通プラットフォーム研究所 〒 239–0847 横須賀市光の丘 1-1
E-mail: †{taiichi,fhoshino,uchiyama,kotetsu}@isl.ntt.co.jp

あらまし　本稿は、非特異楕円曲線上のある種の自己準同型写像を用いて構成した一方向性関数を提案し、その一方向性の傍証をいくつか与える。

キーワード　一方向性関数, ペアリングに基づく暗号系, distorsion map, Weil 対, Tate 対, Frobenius 自己準同型, co-Diffie-Hellman 問題

Candidate One-Way Functions on Non-Supersingular Elliptic Curves

Taiichi SAITO[†], Fumitaka HOSHINO[†], Shigenori UCHIYAMA[†], and Tetsutaro KOBAYASHI[†]

[†] NTT Information Sharing Platform Laboratories, 1-1 Hikari-no-oka, Yokosuka-shi, 239-0847, Japan
E-mail: †{taiichi,fhoshino,uchiyama,kotetsu}@isl.ntt.co.jp

Abstract　This paper proposes candidate one-way functions constructed with a certain type of endomorphisms on non-supersingular elliptic curves and presents several pieces of evidence of the conjectured one-wayness.

Key words　one-way function, pairing-based cryptosystem, distorsion map, the Weil and the Tate pairings, the Frobenius endomorphism, the co-Diffie-Hellman problem

1. Introduction

One way functions are the most fundamental primitive in cryptography. While there has been no proof for the existence of one-way functions, there are some candidate functions believed to be one-way, such as the RSA, the Rabin and the exponentiation functions; the first two are based on the intractability of a computational number-theoretic problem, the integer factoring problem while the last is of another problem, the discrete logarithm problem. The discrete logarithm problem can be defined on any efficiently computable cyclic group and recently, as the underlying group of problem, the group of rational points on elliptic curves has been receiving much attention.

In this paper we propose other number-theoretic candidates for one-way functions, whose one-wayness is related to the discrete logarithm problem on elliptic curves but which are not exponentiation functions themselves. Several pieces of evidence as to their one-wayness are presented. The candidates are constructed with a certain type of endomorphism on *non-supersingular elliptic curve*.

We also show that their one-wayness is equivalent to special cases of the *co-Diffie-Helman assumption* [8], [9] and that if the one-wayness is breakable, we can construct identity-based cryptosystems and signature schemes [7], [9] even if the Diffi-Hellma problem on non-supersingular elliptic curves is used.

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]. However, Joux and Nguyen [18] 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 [28]) is easy.[1] 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:

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

Joux and Nguyen's result on the DDH problem and the ideas of the Sakai-Ohgishi-Kasahara [24] and the Joux [16] papers have led us to a new field in cryptography, *pairing-based cryptosystems*, which use the bilinear map as building block. Recently pairing-based cryptosystems are one of the most active fields of research in

[1] It is also shown in [18] that the DDH problem on a special class of non-supersingular elliptic curves, *the trace-2 curves*, is easy.

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 equal to 1 (i.e., $e(P_1, P_2) = 1$). The distorsion map has been used in order to make the pairing non-degenerate. It maps points in $\mathbb{G}$ to points in another cyclic group, and combination of the Weil pairing and the distorsion map achieves the property of non-degeneracy. However, it is known that there are no distorsion maps on non-supersingular elliptic curves[2] so the underlying elliptic curves for pairing-based cryptosystems have been often restricted to be supersingular.

Verheul [28] showed there exist point groups on non-supersingular elliptic curves in which the DDH problem is easy. We will discuss whether such groups can be applied to pairing-based cryptosystems. It is shown that if the one-wayness of our candidates is breakable, we can construct identity-based cryptosystems and signature schemes based on the Diffi-Hellma problem on non-supersingular elliptic curves.

Boneh, Lynn and Shacham [9], in addition to the basic pairing-based cryptosystem constructed on supersingular curve, presented another modified cryptosystem that uses non-supersingular curves. Boneh, Gentry, Lynn and Shacham [8] presented cryptosystems that directly use the Weil or Tate pairing instead of the above type of bilinear map and can be constructed with non-supersingular curves. Their cryptosystems are based on an extension of the Diffie-Hellman problem, the *co-Diffie-Hellman problem*, which is defined with a pair of groups of the same order. We will see that the one-wayness of our candidates is equivalent to special cases of the co-Diffie-Helman assumption.

Miyaji, Nakabayashi and Takano [21], Barreto, Lynn and Scott [5] and Dupont, Enge and Morain [11] discussed constructions of non-supersingular elliptic curves for pairing-based cryptosystems using the complex multiplication theory. Barreto, Lynn and Scott [4] discussed how to select two distinct cyclic groups of the same order in non-supersingular elliptic curves for pairing-based cryptosystems (Similar results are proposed in [19], [23]; see **Appendix 2**). We use their results as a building block in constructing our candidate one-way functions.

2. Background

In this paper, we follow the notation and definition in *Silverman's book* [26] 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 an odd prime number other than the characteristic of $\mathbb{F}_q$ and that $l \nmid (q-1)$. These 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 $Q (\neq \mathcal{O}) \in E[l]$ such that $\phi(Q) - [q \bmod l]Q = \mathcal{O}$. Thus we see that $E[l]$ is decomposed into $E[l] = \langle P \rangle \oplus \langle Q \rangle$ 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:

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

where we define proj_1 and proj_2 as

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

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 [28] showed the DDH problem in any non-eigenspace G_i is easy, where, for the Weil or Tate pairing e, $e(\phi(\cdot), \cdot)$ was used as the 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 the 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 [28].

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 combining the Weil or Tate pairing with endomorphism cannot be applied to the DDH problems in the eigenspaces, $\langle P \rangle$ and $\langle Q \rangle$.

By using non-eigenspace $\langle R \rangle$ and the non-degenerate bilinear map $e(\mathrm{proj}_1(\cdot), \cdot)$, we can construct variants of the key agreement protocols in [1], [16], [28] and the verifiable random function in

[2] The non-existence of a distorsion map on non-supersingular elliptic curves was shown implicitly in [29] and explicitly in [25], and recently rediscovered in [28].

[10].[3] On the other hand, our cyclic group $\langle R\rangle$ would not be directly applicable to other important areas of pairing-based cryptosystems, identity-based cryptosystems and signature schemes (e.g, [7], [9]), 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. Indeed, instead of the problems in such groups, the cryptosystems based on non-supersingular curves in [7], [9] adopt other problems (the co-BDH and co-DH problems) as the underlying problems (see also **Section** 3. 3).

Remark: We will see that if the one-way function $\mathcal{F}$ in next section is breakable, we can realize identity-based cryptosystems and signature schemes based on $\langle R\rangle$.

3. Candidate one-way functions

This section suggests the use of two types of endomorphism as candidates of one-way functions, discusses several pieces of evidence of their conjectured one-wayness, and presents other properties. We follow *Goldreich's book* [14] and *Goldwasser and Bellare's note* [15] on one-way functions.

As well as most popular one-way function candidates, the candidates suggested in this paper also are described as collections of functions; A *collection of functions* is an infinite set of indexed functions $\{f_i\}$ such that each function f_i operates on a finite domain D_i and all functions share a single evaluation algorithm F which, given as input a representation (*index*) i of function f_i and element x in domain D_i, returns the value $f_i(x)$ (i.e., $F(i,x)=f_i(x)$).

In addition, a collection of *one-way* functions is required such that any efficient algorithm, when given an index i and $f_i(x)$, cannot retrieve x, except with negligible probability. Formally:

(Collection of one-way functions):

A collection of one-way functions $\{f_i\}$ is called **one-way** if there exist three probabilistic polynomial-time algorithms I, D and F such that the following conditions hold:

(1) Easy to sample and compute:

I, on input 1^n (n: security parameter), outputs an index i.

D, on input i, outputs $x \in D_i$.

F, on input i and $x \in D_i$, outputs $F(i,x)=f_i(x)$.

(2) Hard to invert:

For any probabilistic polynomial-time algorithm A, there exists a negligible function μ_A such that

$$\Pr\left[\begin{array}{l} A(i,y)=x\ ;\ i \leftarrow I(1^n), \\ \qquad\qquad x \leftarrow D(i), y=F(i,x) \end{array}\right] \leqq \mu_A(n)$$

where the probability is taken over the coin-tosses of A, I, and D.

3. 1 A candidate collection of one-way functions $\mathcal{F}$

We suggest a candidate collection of one-way functions $\mathcal{F}=(I,D,F)$ which consists of three probabilistic polynomial-time algorithms: an index generation algorithm I, a domain sampling algorithm D, a function-evaluation algorithm F:

Index generation algorithm I:

On input 1^n (n: security parameter), the index generation algorithm I outputs an index $i=\overline{(E,\mathbb{F}_q,l,\mathbb{F}_{q^k},R)}$, a polynomial-size representation of $(E,\mathbb{F}_q,l,\mathbb{F}_{q^k},R)$. We assume that $(E,\mathbb{F}_q,l,\mathbb{F}_{q^k},R)$ satisfy the following:

- E is a non-supersingular elliptic curve over $\mathbb{F}_q$.
- l is a prime number coprime to q.
- l divides $\#E(\mathbb{F}_q)$ and does not divide $(q-1)$.
- k is the smallest positive integer such that $l|(q^k-1)$.
- R is an $\mathbb{F}_{q^k}$-rational point of order l such that $\mathrm{proj}_1 R \neq \mathcal{O}$ and $\mathrm{proj}_2 R \neq \mathcal{O}$.
- There is a polynomial $p(\cdot)$ such that the size of q and l is upper-bounded by $p(n)$ and the size of k is upper-bounded by $\log p(n)$.

I can be constructed by using the methods of non-supersingular curve generation in [5], [11], [21] and the methods of group selection in [4], [19], [23] or in **Appendix 2**.

Domain sampling algorithm D:

The domain sampling algorithm D takes index i as input and outputs point R' which is randomly and uniformly distributed over $\langle R\rangle$. D can be realized by randomly choosing $r \in \mathbb{Z}_q$ and outputting $R'=[r]R$.

Function-evaluation algorithm F:

The function-evaluation algorithm F takes index i and point $R' \in \langle R\rangle$ as input and returns $f_i(R')(=F(i,R'))$ and f_i is constructed as follows:

$$\begin{aligned} f_i(\cdot) \ = \ F(i,\cdot) : \ &\langle R\rangle \rightarrow \langle P\rangle \\ &;\ R' \mapsto f_i(R')=(\phi-[q \bmod l])R' \end{aligned}$$

where P denotes an $\mathbb{F}_q$-rational point of order l.

The conjectured one-wayness of $\mathcal{F}=(I,D,F)$ is described as follows: For any probabilistic polynomial-time algorithm A, there exists a negligible function μ_A such that

$$\Pr\left[\begin{array}{l} A(i,P')=R' \\ \qquad ;\ i=\overline{(E,\mathbb{F}_q,l,\mathbb{F}_{q^k},R)} \leftarrow I(1^n), \\ \qquad\quad R' \overset{R}{\leftarrow} \langle R\rangle, P'=(\phi-[q \bmod l])R' \end{array}\right] \leqq \mu_A(n)$$

where the probability is taken over the coin-tosses of A, I and the choices of R'.

[3] Note that $\langle R\rangle$ is polynomially recognizable and that the uniform distribution over $\langle R\rangle$ is polynomially samplable.

Instead of $(\phi - [q \bmod l])$, we can use other efficiently computable endomorphisms that induce isomorphisms from $\langle R\rangle$ onto $\langle P\rangle$, such as proj_1 and $\mathrm{Tr} = \sum_{i=0}^{k-1} \phi^i$.

[Evidence of one-wayness of $\mathcal{F}$]

Here we discuss several pieces of evidence of the one-wayness of $\mathcal{F}$.

- *There is no endomorphism of E that maps $\langle P\rangle$ onto $\langle R\rangle$*
  Since any endomorphism commutes with ϕ, $\mathrm{End}_{\overline{\mathbb{F}}_q}(E) = \mathrm{End}_{\mathbb{F}_q}(E)$ holds [25], [28], [29].
- *The DDH assumption in $\langle P\rangle$ implies the one-wayness of f_i*
  It is easy to see that if the one-wayness of f_i does not hold, then the DDH assumption in $\langle P\rangle$ is not valid.
  On the other hand, Verheul [28] showed that there is no distorsion map that sends $\langle P\rangle$ to another group. Then the construction of a non-degenerate bilinear map by combining pairing with a distorsion map cannot be applied to this case. Thus the DDH assumption in $\langle P\rangle$ still remains valid.
- *The skewed-DH assumption is equivalent to the one-wayness of $\mathcal{F}$.*
  Here we consider a variant of the usual DH problem, *the skewed-DH problem*.
  Let P an Q be eigenvectors corresponding to the eigenvalues 1 and $q \bmod l$, respectively. Let P' be a random point in $\langle P\rangle$.
  The *skewed-DH problem* is
  given P, Q, P', to find $Q' \in \langle Q\rangle$ such that
  $\log_P P' = \log_Q Q'$.
  We say the *skewed-DH assumption* holds if the skewed-DH problem is intractable. The skewed-DH assumption is equivalent to the one-wayness of our proposed candidate (See **Appendix 1** for detail).

As we have seen, the one-wayness of f_i is strongly related to the hardness of the problems on $\langle P\rangle$. We also note that the one-wayness of f_i implies the discrete logarithm assumption in $\langle P\rangle$.

[Properties of f_i]

In addition to the conjectured one-wayness, f_i has the following properties:

- *(Commutative) random self-reducibility*
  Since f_i is an isomorphism, the relation $R_i = \{(f_i(y), y) | y \in \langle R\rangle\}$ is (commutative) random self-reducible [22], [27].
- *Isomorphism from the Gap-DH group to the DDH group*
  The DDH problem in $\langle R\rangle$ is easy and the DH problem seems intractable. As we have discussed, the DDH problem in $\langle P\rangle$ still remains intractable. Then f_i is conjectured to map the Gap-DH group to the DDH group.
- *Efficiency*
  Boneh and Franklin [7] and Verheul [28] discussed the one-wayness of bilinear map induced by the Weil or the Tate pairing. It also are conjectured to be maps from the Gap-DH group to the DDH group.
  While the evaluation of bilinear maps require the costly computation of pairings, f_i is efficiently computable endomorphism.
- *Efficiently recognizable domain and range*
  We see that $R'(\in E[l])$ is in $\langle R\rangle$ if and only if $e(R, R') = 1$ for the Weil pairing e. Then the domain $\langle R\rangle$ is polynomially recognizable.

3. 2 Another candidate of collection of one-way functions $\mathcal{F}'$

Another candidate collection of one-way functions $\mathcal{F}' = (I, D, F')$ consists of the same index generation algorithm I and the same domain sampling algorithm D as of the previous candidate, and another function-evaluation algorithm F'.

The function-evaluation algorithm F' takes index i and point $R' \in \langle R\rangle$ as input and returns $f'_i(R')(= F'(i, R'))$; f'_i is constructed as follows:

$$f'_i(\cdot) = F'(i, \cdot) : \langle R\rangle \to \langle Q\rangle;\ R' \mapsto f'_i(R') = (\phi - 1)R'$$

where Q denotes an $\mathbb{F}_{q^k}$-rational point of order l such that $(\phi - [q \bmod l])Q = \mathcal{O}$.

Instead of $(\phi - 1)$, we can use other efficiently computable endomorphisms that induce isomorphisms from $\langle R\rangle$ onto $\langle Q\rangle$, such as proj_2.

[Evidence of one-wayness of $\mathcal{F}'$]

Here we discuss several pieces of evidence of the one-wayness of $\mathcal{F}'$.

- *There is no endomorphism of E that maps $\langle Q\rangle$ onto $\langle R\rangle$*
  Since any endomorphism α commutes with $(\phi - [q \bmod l])$, $\langle Q\rangle$ is stable by the action of α (i.e., For any α and $Q' \in \langle Q\rangle$, $\alpha(Q') \in \langle Q\rangle$ holds).
- *The DDH assumption in $\langle Q\rangle$ implies the one-wayness of f'_i*
  Since there is no endomorphism that sends $\langle Q\rangle$ to another group, the construction of a non-degenerate bilinear map by combining pairing with distorsion map cannot be applied to this case. Thus the DDH assumption in $\langle Q\rangle$ still remains valid.
- *A variant of the skewed-DH assumption is equivalent to the one-wayness of $\mathcal{F}'$.*
  Here we consider a variant of the *skewed-DH problem* defined in the previous subsection.
  Let P an Q be eigenvectors corresponding to the eigenvalues 1 and $q \bmod l$, respectively. Let Q' be a random point in $\langle Q\rangle$.
  The variant of the skewed-DH problem is
  given P, Q, Q', to find $P' \in \langle P\rangle$ such that
  $\log_P P' = \log_Q Q'$.
  The intractability of this problem is equivalent to the one-wayness of $\mathcal{F}'$.

f'_i has almost the same properties as shown on f_i in the previous subsection. We note that the range of f_i' is efficiently recognizable since $Q'(\in E[l])$ is in $\langle Q\rangle$ if and only if $(\phi - [q \bmod l])Q' = \mathcal{O}$.

3.3 The co-Diffie-Hellman problem

The skewed-DH problem and the variant in the previous subsections can be seen as special cases of the *co-Diffie-Hellman problem* [8], [9].

The co-Diffie-Hellman (co-DH) problem on $(\mathbb{G}_1, \mathbb{G}_2)$
Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be cyclic groups of order l generated by P_1 and P_2, respectively. The *co-Diffie-Hellman problem* on $(\mathbb{G}_1, \mathbb{G}_2)$ is given (P_1, aP_1, P_2) to compute aP_2.

In addition to the GDH signature, which is constructed on supersingular curves and was proven to be unforgeable under the Diffie-Hellman assumption, Boneh, Lynn and Shacham [9] also presented a modification of the GDH signature, the *co-GDH signature*.

The co-GDH signature (basic scheme)

Key generation

Pick a random $a \in \mathbb{Z}/l\mathbb{Z}$ and compute $V = aP_1 \in \mathbb{G}_1$. The public key is V and the secret key is a.

Signing

Given secret key a and message m, compute hash value $H = H(m) \in \mathbb{G}_2$ and $S = aH \in \mathbb{G}_2$. The signature of m is S.

Verification

Given public key V, message m and signature S, compute hash value $H = H(m) \in \mathbb{G}_2$. Output "valid" if and only if $e(S, P_1) = e(H, V)$ where e denotes the Weil or Tate pairing.

The co-GDH signature was proven to be secure under special cases of the co-DH assumption. More precisely, under the setting

$$(\mathbb{G}_1, \mathbb{G}_2) = (\langle R\rangle, \langle P\rangle),$$

there exist efficient isomorphisms f from $\mathbb{G}_1$ onto $\mathbb{G}_2$ (e.g., the trace map, proj_1) and then the unforgeability of the corresponding co-GDH signature can be proved in the random oracle model by letting a hash value and the corresponding signature be $[r] \circ f(P_1)$ and $[r] \circ f(aP_1)$ for random r, respectively, in the simulations of signing and random oracles. Note that the co-GDH signature uses points in $\mathbb{G}_1$ to define public keys and embeds conventional hash values into the $\mathbb{F}_q$-rational point group $\mathbb{G}_2$.

Interestingly, even though the unforgeability of the co-GDH signature under the setting

$$(\mathbb{G}_1, \mathbb{G}_2) = (\langle Q\rangle, \langle P\rangle)$$

cannot be proved in the same way because there are no endomorphisms that induce isomorphisms from $\mathbb{G}_1$ onto $\mathbb{G}_2$, it can be derived from the unforgeability of the co-GDH signature under the setting

$$(\mathbb{G}_1, \mathbb{G}_2) = (\langle R\rangle, \langle P\rangle).$$

The skewed-DH problem for $\mathcal{F}$ and the variant skewed-DH problem for $\mathcal{F}'$ can be seen as special versions of the co-DH problem as follows:

The skewed-DH problem for $\mathcal{F}$	$(\langle P\rangle, \langle Q\rangle)$
The variant problem for $\mathcal{F}'$	$(\langle Q\rangle, \langle P\rangle)$
The underlying problem of the co-GDH signature	$(\langle R\rangle, \langle P\rangle)$

It is easy to see that the co-DH assumptions on $(\langle R\rangle, \langle Q\rangle)$ and $(\langle R\rangle, \langle P\rangle)$ imply the skewed-DH and the variant assumptions, respectively. Then it is concluded that the co-GDH signature should adopt the variant skewd-DH assumption (i.e., setting of $(\mathbb{G}_1, \mathbb{G}_2) = (\langle Q\rangle, \langle P\rangle)$).

Remark 1: The challenges given to the adversaries against the one-wayness of our candidates can be also seen as special cases of the co-Diffie-Hellman problem as follows:

The challenge against $\mathcal{F}$	$(\langle P\rangle, \langle R\rangle), f_i(P_2) = P_1$
The challenge against $\mathcal{F}'$	$(\langle Q\rangle, \langle R\rangle), f_i'(P_2) = P_1$

Remark 2: Note that the co-GDH signature uses a pair of groups on which the *Decision co-Diffie-Hellman problem* is easy.

The Decision co-Diffie-Hellman problem on $(\mathbb{G}_1, \mathbb{G}_2)$ Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be cyclic groups of order l generated by P_1 and P_2, respectively. The *Decision co-Diffie-Hellman problem* on $(\mathbb{G}_1, \mathbb{G}_2)$ is given (P_1, aP_1, P_2, bP_2) to decide whether or not $a = b \bmod l$ holds.

We easily see that unless $\mathbb{G}_1 = \mathbb{G}_2 = \langle P\rangle$ nor $\langle Q\rangle$, the Decision co-DH problem on $(\mathbb{G}_1, \mathbb{G}_2)$ is easy.

4. Conclusion

We have proposed candidate collections of one-way functions. Their one-wayness is equivalent to the skew-DH assumption and the variant, which are special cases of the co-DH assumption. We would like to mention that if the one-wayness of proj_1 is breakable, we can construct identity-based cryptosystems and signature schemes based on the DH problem on non-supersingular curves by embedding identities or conventional hash values into the range $\langle P\rangle$ and sending them to the domain $\langle R\rangle$.

We conclude by summarizing the open questions raised in this paper:

- the DDH, DH, DL problems in the eigenspaces $\langle P\rangle$ and $\langle Q\rangle$
- the DH, DL problems in the non-eigenspaces $\langle R\rangle$
- the one-wayness of f_i and f_i' (equivalently, the skewed-DH assumption and the variant)
- reducibility between these problems

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," *Journal of Cryptology*, 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. of Crypto 2002*, LNCS 2442, Springer-Verlag, pp.354–368, 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. of SCN'2002*, LNCS 2576, Springer-Verlag, pp. 257–267, 2003.

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

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

[8] D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," *Proc. of Eurocrypt 2003*, LNCS 2656, Springer-Verlag, pp. 416–432, 2003.

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

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

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

[12] G. Frey and H. G. Rück, "A Remark Concerning m-divisibility and The Discrete Logarithm in The Divisor Class Group of Curves," *Math. Comp.*, vol.62, no.206, pp.865–874, 1994.

[13] S. D. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate pairing," *Proc. of ANTS-V*, LNCS 2369, Springer-Verlag, pp. 324–337, 2002.

[14] O. Goldreich, "Foundations of Cryptography: Basic Tools", Cambridge University Press, 2001.

[15] S. Goldwasser and M. Bellare, "Lecture Notes on Cryptography", `http://www-cse.ucsd.edu/users/mihir/`, 1999.

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

[17] A. Joux, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems," *Proc. of ANTS 2002*, LNCS2369, Springer-Verlag, pp.20–32, 2002.

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

[19] 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, 2000, `http://search.ieice.or.jp/index-e.html`.

[20] A. Menezes, T. Okamoto and S. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," *IEEE Transaction on Information Theory*, vol.IT-39, no.5, pp.1639–1646, 1993.

[21] 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, 2001, `http://search.ieice.or.jp/index-e.html`.

[22] T. Okamoto and K. Ohta, "Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility," *Proc. of Eurocrypt '89*, LNCS434, SpringerVerlag, pp.134–149, 1990

[23] 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, 2001, `http://search.ieice.or.jp/index-e.html`.

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

[25] R. Schoof, "Nonsingular plane cubic curves over finite fields," *J. Combin. Theory*, Ser. A 46, pp.183–211, 1987.

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

[27] M. Tompa and H. Woll, " Random self-reducibility and zero knowledge interactive proofs of possession of information," *Proc. of FOCS '87*, pp.472–482, 1987.

[28] E. R. Verheul, "Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems," *Proc. of Eurocrypt 2001*, LNCS 2045, Springer-Verlag, pp.195–210, 2001.

[29] W. C. Waterhouse, "Abelian varieties over finite fields," *Ann. Sci. École Norm. Sup.*, Ser. 2(4), pp.521–560, 1969.

Appendix

1. The skewed-DH assumption is equivalent to the one-wayness of $\mathcal{F}$

Here assume for simplicity that $f_i = \mathrm{proj}_1$.

We define the *skewed-DH problem* and *the skewed-DH assumption*.

Let I' be a problem instance generation algorithm that takes 1^n (n: security parameter) as input and outputs an instance of problem, $i' = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P, Q, P')}$, where the parameters $E, \mathbb{F}_q, l$ and $\mathbb{F}_{q^k}$ are the same as of I; P is a point of order l such that $\phi(P) - P = \mathcal{O}$; Q is a point of order l such that $\phi(Q) - [q \bmod l]Q = \mathcal{O}$; $P' = [r]P$ for randomly chosen $r \in \mathbb{Z}/l\mathbb{Z}$.

The *skewed-DH problem* with respect to I' is

> for given $(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P, Q, P')$, to find $Q' \in \langle Q \rangle$ such that $\log_P P' = \log_Q Q'$.

We say the *skewed-DH assumption* with respect to I' holds if the skewed-DH problem with respect to I' is intractable. Formally, the skewed-DH assumption with respect to I' is that for any probabilistic polynomial-time algorithm, A', there exists a negligible function $\mu_{A'}$ such that

$$\Pr\left[\begin{array}{l} A'(i') = Q' \text{ and } \log_P P' = \log_Q Q' \\ \ ;\ i' = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P, Q, P')} \leftarrow I'(1^n) \end{array}\right] \leqq \mu_{A'}(n)$$

where the probability is taken over the coin-tosses of A' and I'.

Assume that the distribution ensemble of the output of problem instance generation algorithm I' is identical to the following distribution ensemble constructed with index generation algorithm I of $\mathcal{F}$,

$$\left\{\begin{array}{r} i' = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, \mathrm{proj}_1(R), \mathrm{proj}_2(R), P')} \\ ;\ i = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, R)} \leftarrow I(1^n), \\ R' \xleftarrow{R} \langle R \rangle, P' = \mathrm{proj}_1(R') \end{array}\right\},$$

or that the distribution ensemble of the challenge $(i, P') = (\overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, R)}, \mathrm{proj}_1(R'))$ given to the adversaries against the one-wayness of $\mathcal{F} = (I, D, F)$ is identical to the following distribution ensemble constructed with a problem instance generation algorithm I',

$$\left\{\begin{array}{r} (i, P') = (\overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P + Q)}, P') \\ ;\ i' = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P, Q, P')} \leftarrow I'(1^n) \end{array}\right\}.$$

Then we see the skewed-DH assumption with respect to I' is equivalent to the one-wayness of $\mathcal{F} = (I, D, F)$ as follows:

- Assume that there exists an efficient algorithm A' for the skewed-DH problem. We can construct an efficient algorithm that breaks the one-wayness as follows: On input $i = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, R)}$ and $P' = \mathrm{proj}_1(R')$, we run A' with input $i' = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, \mathrm{proj}_1(R), \mathrm{proj}_2(R), P')}$ and obtain $Q' = A(i')$. Then we return $R' = P' + Q'$ as the preimage of P'.

  We see that $R = P + Q$ and $P' = [r]P$ for randomly distributed $r \in \mathbb{Z}/l\mathbb{Z}$. If A' succeeds, $Q' = [r]Q$ holds and then $R' = [r](P + Q)$ holds.
- Assume that there exists an efficient algorithm A that breaks the one-wayness. We can construct an efficient algorithm for the skewed-DH problem as follows: On input $i' = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P, Q, P')}$, we run A with input P' and $i = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P + Q)}$ and obtain R'. We then return $Q' = R' - P'$ as the answer of the DH-like problem.

  If $P' = [r]P$ and A succeeds, $R' = [r](P + Q)$ holds. This yields $Q' = [r]Q$.

2. A method of group selection

Here we summarize the method of group selection presented in [19], [23], which can be used for computing the Weil or Tate pairing. More precisely, the method generates a point $S(\neq \mathcal{O}) \in E[l]$ such that $(\phi - [q \bmod l])S = \mathcal{O}$.

First we study the group structure of the l-part of $E(\mathbb{F}_{q^k})$. In the previous sections, we used a $\mathbb{Z}/l\mathbb{Z}$-linear representation of the q^{th}-power Frobenius endomorphism ϕ on $E[l]$, whereas here we consider a representation ϕ_l of ϕ on the l-adic Tate module $T_l(E)$. Recall $T_l(E)$ is isomorphic to $\{(R_1, R_2, \ldots) \in \oplus_{i=1}^{\infty} E[l^i]\ ;\ [l]R_{j+1} = R_j$ for any $j\}$. We saw in the previous sections that under the assumption $l \nmid (q-1)$, the eigenequation of $\mathbb{Z}/l\mathbb{Z}$-linear representation of ϕ has two distinct roots. The eigenequation of ϕ_l has two distinct l-adic integer roots λ_1, λ_2 such that $\lambda_1 = 1 + cl^d$ and $\lambda_2 = (q \bmod l) + c'l^e$ for some rational integers d, e and some c, c' in $\mathbf{Z}_l^{\times}$. Thus $T_l(E)$ can be decomposed into $T_l(E) = T_{\lambda_1} \oplus T_{\lambda_2}$ where eigenspaces T_{λ_1} and T_{λ_2} correspond to λ_1 and λ_2, respectively. Let $(T_{\lambda_j})_i$ be the i-th component of the eigenspace T_{λ_j}, $(T_{\lambda_j})_i = \{R \in E[l^i]; \phi R = \lambda_j R\}$. It is easy to see that $(T_{\lambda_1})_i$ and $(T_{\lambda_2})_i$ are cyclic groups of order l^i. Note that since $\lambda_1 = 1 + cl^d$ and $c \in \mathbf{Z}_l^{\times}$, the l-part of $E(\mathbb{F}_q)$ is $(T_{\lambda_1})_d$. Using these notations, it is easy to see that for any k', $(T_{\lambda_1})_{d+1} \subset E(\mathbb{F}_q^{k'}) \Leftrightarrow l|k'$. On the other hand, since k is the minimum integer such that $q^k \equiv 1 \pmod{l}$, it follows that $k|(l-1)$. Then for such k, we have $(T_{\lambda_1})_{d+i} \cap E(\mathbb{F}_{q^k}) = (T_{\lambda_1})_d$ for any i.

Consequently, if f is the integer such that $l^f || \#E(\mathbb{F}_{q^k})$, we can determine the group structure of the l-part of $E(\mathbb{F}_q)$ as follows:

$$\text{the } l\text{-part of } E(\mathbb{F}_{q^k}) = (T_{\lambda_1})_d \oplus (T_{\lambda_2})_{f-d}.$$

Now we describe an algorithm for picking up the point $S(\neq \mathcal{O})$ in $E[l]$ such that $(\phi - [q \bmod l])S = \mathcal{O}$ in the case of $l \nmid (q-1)$.

Let m be the cardinality of $E(\mathbb{F}_{q^k})$,

Algorithm

[Step 1]

Choose any point $P \in E(\mathbb{F}_{q^k})$, and compute $P' = [m/l^f]P$.

[Step 2]

Compute $P'' = \phi(P') - P'$. If $P'' = \mathcal{O}$ goto **Step 1**.

[Step 3]

Find the minimum integer j such that $[l^j]P'' = \mathcal{O}$, and output $S = [l^{j-1}]P''$.

If we choose point P in $E(\mathbb{F}_{q^k})$ randomly and uniformly, point $P' = [m/l^e]P$ is uniformly distributed on the l-part of $E(\mathbb{F}_{q^k})$.

Because $(\phi - 1)$ annihilates only the $(T_{\lambda_1})_d$ part of the decomposition, point P'' is uniformly distributed on $(T_{\lambda_2})_{f-d}$. Thus the probability that $P'' = \mathcal{O}$ is less than $1/l^{f-d}$.