PAPER *Special Section on Cryptography and Information Security*

Candidate One-Way Functions on Non-Supersingular Elliptic Curves*

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

SUMMARY This paper proposes new candidate one-way functions constructed with a certain type of endomorphisms on non-supersingular elliptic curves. We can show that the one-wayness of our proposed functions is equivalent to some special cases of the co-Diffie-Hellman assumption. Also a digital signature scheme is explicitly described using our proposed functions.

key words: *one-way function, pairing-based cryptosystem, distortion map, the Weil and the Tate pairings, 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 two formers are based on the intractability of a computational number-theoretic problem, factoring integer problem and the latter is of another problem, discrete logarithm problem. Discrete logarithm problem can be defined on any efficiently computable cyclic group and recently, as the underlying group of problem, group of rational points on elliptic curve has been receiving much attention.

In this paper we propose other number-theoretic candidates for one-way function, whose one-wayness is related to the discrete logarithm problem on elliptic curve but which are not exponentiation functions themselves, and present several pieces of evidence of their one-wayness. The candidates are constructed with a certain type of endomorphisms on *non-supersingular elliptic curve*. We also show that their one-wayness is equivalent to some special cases of the *co-Diffie-Hellman assumption* [8], [9].

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 distortion map ψ (see [29]) is easy[**]. In their proof, they constructed a non-degenerate bilinear map $\hat{e}$ from $\mathbb{G} \times \mathbb{G}$ to $\overline{\mathbb{F}}_q^{\times}$ by combining the Weil pairing e with the distortion map ψ as follows:

$$\hat{e}(P_1, P_2) = e(\psi(P_1), P_2).$$

Joux and Nguyen's result on the DDH problem and the ideas of the Sakai-Ohgishi-Kasahara [23] and the Joux [16] papers have led us to a new field in cryptography, *pairing-based cryptosystems*, in the construction of which the bilinear map is used as a 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 distortion map has been used, which maps points in $\mathbb{G}$ to points in other cyclic group, and combination of the Weil pairing and the distortion map achieves the property of non-degeneracy. However it is known that there exists no distortion map on non-supersingular elliptic curves[***] and then the underlying elliptic curves for pairing-based cryptosystems have been often restricted to be supersingular.

Boneh, Lynn and Shacham [9], in addition to the basic pairing-based cryptosystem constructed with supersingular curve, also presented another modified cryptosystem with non-supersingular curves. Boneh, Gentry, Lynn and Shacham [8] presented cryptosystems that directly use the Weil or the Tate pairing in stead of the above type of bilinear map and can be constructed with non-supersingular curves. Their cryptosystems are based on an extension of

Manuscript received March 23, 2005.
Manuscript revised June 23, 2005.
Final manuscript received August 29, 2005.

[†] The author is with Tokyo Denki University, Tokyo, 101-8457 Japan.

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

[*] A preliminary version was presented at ISEC2003 [22].

a) E-mail: taiichi@c.dendai.ac.jp

DOI: 10.1093/ietfec/e89–a.1.144

[**] 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.

[***] The non-existence of distortion map on non-supersingular elliptic curve was shown implicitly in [30] and explicitly in [24], and recently rediscovered in [29].

the Diffie-Hellman problem, the *co-Diffie-Hellman problem*, which is defined with a pair of groups of the same order. A precise classificaiton of the co-Diffie-Hellman problems on non-supersingular curves was presented in [28]. We will see that the one-wayness of our candidates is equivalent to special cases of the co-Diffie-Hellman assumption.

Miyaji, Nakabayashi and Takano [20], 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. Using their results as building block, we will construct our candidate one-way functions.

2. Background

In this paper, we follow the notation and definition in *Silverman's book* [25] 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 $E[l] \simeq \langle P \rangle \times \langle Q \rangle$:

$$(\mathrm{proj}_1, \mathrm{proj}_2) : r_1 P + r_2 Q \mapsto (r_1 P, r_2 Q),$$

where we define proj_1 and proj_2 as

$$\mathrm{proj}_1(R) = [(1-q)^{-1} \bmod l] \circ (\phi - [q \bmod l])R,$$
$$\mathrm{proj}_2(R) = [(q-1)^{-1} \bmod l] \circ (\phi - 1)R.$$

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 [29] 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 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 [29].

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 $\langle Q \rangle$.

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], [29] and the verifiable random function in [10][†]. 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 Sect. 3.4).

3. Candidate One-Way Functions

This section proposes two type of endomorphisms as candidates of one-way functions, discusses several pieces of evidence of their conjectured one-wayness and presents other properties.

To be brief, our proposed functions are two type of endomorphism $(\phi - [q \bmod l])$ and $(\phi - 1)$, whose domain is restricted to non-eigenspace $\langle R \rangle$. We can show the following theorems:

Theorem 1: *The DDH assumption in* $\langle P \rangle$ *(resp.* $\langle Q \rangle$*) implies the one-wayness of* $f_i = (\phi - [q \bmod l])$ *(resp.* $f_i' = (\phi - 1)$*). There is no inverse endomorphism of* f_i *and* f_i'*.*

Also we will see that the one-wayness of our proposed functions is equivalent to special class of co-Diffie-Hellman assumption.

Hereafter we follow *Goldreich's book* [14] and *Goldwasser and Bellare's note* [15] for one-way functions.

As well as almost popular candidate one-way functions, 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 a function f_i and an element x in the 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 that any efficient algorithm, when given an index of i

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

and $f_i(x)$, cannot retrieve x, except with negligible probability. Formally:

Definition 1: (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:
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 $F(i, x) = f_i(x)$.

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

$$\Pr[x = A(i, y); i \leftarrow I(1^n), x \leftarrow D(i), y = F(i, x)] \leq \mu_A(n)$$

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

3.1 A Candidate of Collection of One-Way Functions $\mathcal{F}$

We suggest a candidate of 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 an 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 $\mathrm{proj}_1 R \neq O$ and $\mathrm{proj}_2 R \neq O$.
- 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], [20] and the methods of group selection in [4].

Domain sampling algorithm D: The domain sampling algorithm D takes an index i as input and outputs a 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 an index i and a point $R' \in \langle R \rangle$ as input and returns $f_i(R') (= F(i, R'))$ and f_i, which maps $\langle R \rangle$ to $\langle P \rangle$, is constructed as follows:

$$f_i(R') = F(i, R') = (\phi - [q \bmod l])R'$$

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

$$\Pr\left[A(i, P') = R' \; ; \; \begin{array}{c} i \leftarrow I(1^n), \\ R' \overset{R}{\leftarrow} \langle R \rangle, P' = f_i(R') \end{array}\right] \leq \mu_A(n)$$

where $i = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, R)}$ and the probability is taken over the coin-tosses of A, I and the choices of R'.

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 $\mathrm{Tr} = \sum_{i=0}^{k-1} \phi^i$.

We give a proof of **Theorem 1** in the case of f_i.
[proof of Theorem 1 (case f_i)] Firstly, we show that there is no inverse endomorphism of f_i. Since any endomorphism commutes with ϕ because of the non-supersingularity of E, $\mathrm{End}_{\overline{\mathbb{F}}_q}(E) = \mathrm{End}_{\mathbb{F}_q}(E)$ holds [24], [29], [30]. That is, any endomorphism on E is defined over $\mathbb{F}_q$. On the other hand, $\langle P \rangle$ consists entirely of $\mathbb{F}_q$-rational points but any point in $\langle R \rangle$ is not $\mathbb{F}_q$-rational except for O. Thus we see that there is no endomorphism of E that maps the image of f_i, $\langle P \rangle$, onto the range of f_i, $\langle R \rangle$. Secondly, we show the DDH assumption in $\langle P \rangle$ implies the one-wayness of f_i. If we have an efficient algorithm inverting f_i on non-negligible fraction of the image $\langle P \rangle$, we can construct another efficient algorithm inverting f_i on overwhelming probability because of the random self-reducibility of the inverting prolem. This inverting algorithm f_i^{-1} is almost an isomorphism from $\langle P \rangle$ to $\langle R \rangle$ and has the same function as the distortion map ψ. That is, by combining the Weil pairing e with the inverting algorithm f_i^{-1} as follows:

$$\hat{e}'(P_1, P_2) = e(f_i^{-1}(P_1), P_2),$$

we obtain an efficiently computable non-degenerate bilinear map $\hat{e}'$ from $\langle P \rangle \times \langle P \rangle$ to $\overline{\mathbb{F}}_q^{\times}$. It is easy to see that $\log_{P_1} P_2 = \log_{P_3} P_4$ holds iff $\hat{e}'(P_1, P_4) = \hat{e}'(P_2, P_3)$ holds. Thus we can break the DDH assumption in $\langle P \rangle$. This completes the proof of Theorem 1 (case f_i).

Verheul [29] showed there is no distortion map that sends $\langle P \rangle$ to other group. Then the construction of non-degenerate bilinear map by combining pairing with distortion map cannot be applied to this case. Thus the DDH assumption in $\langle P \rangle$ still remains valid.

Next we discuss relation between the one-wayness of $\mathcal{F}$ and special case of co-DH assumption.

- *The skewed-DH assumption is equivalent to the one-wayness of 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

$$\text{given } P, Q, P', \text{ to find } Q' \in \langle Q \rangle \text{ such that } \log_P P' = \log_Q Q'.$$

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 for detail).

As we have seen, the one-wayness of f_i is strongly related to the hardness of 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 [21], [26].
- *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. f_i is conjectured to map the Gap-DH group to the DDH group.
- *Efficiency*
  Boneh and Franklin [7] and Verheul [29] discussed the one-wayness of bilinear maps based on the Weil or the Tate pairings, which the bilinear maps 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*
  $R' (\in E[l])$ 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 of a 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 an index i and a point $R' \in \langle R \rangle$ as input and returns $f_i'(R') (= F'(i, R'))$ and f_i', which maps $\langle R \rangle$ to $\langle Q \rangle$, is constructed as follows:

$$f_i'(R') = F'(i, R') = (\phi - 1)R',$$

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

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.

We give a proof of **Theorem 1** in the case of f_i'.
[proof of Theorem 1 (f_i' case)] Firstly, we show that there is no inverse endomorphism of f_i'. Since any endomorphism α commutes with $(\phi - [q \bmod l])$ because of non-supersingularity, $\langle Q \rangle$ 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). Thus there is no endomorphism of E that maps the image of f_i', $\langle Q \rangle$, onto the range of f_i', $\langle R \rangle$. Secondly, we show that the DDH assumption in $\langle Q \rangle$ implies the one-wayness of f_i'. If we have an efficient algorithm inverting f_i' on non-negligible fraction of the image $\langle Q \rangle$, we can construct another efficient algorithm inverting f_i' on overwhelming probability. This inverting algorithm $(f_i')^{-1}$ is almost an isomorphism from $\langle Q \rangle$ to $\langle R \rangle$. Combining the Weil pairing e with the inverting algorithm $(f_i')^{-1}$ as follows:

$$\hat{e}''(Q_1, Q_2) = e((f_i')^{-1}(Q_1), Q_2),$$

we obtain an efficiently computable non-degenerate bilinear map $\hat{e}''$ from $\langle Q \rangle \times \langle Q \rangle$ to $\overline{\mathbb{F}}_q^{\times}$. It is easy to see that $\log_{Q_1} Q_2 = \log_{Q_3} Q_4$ holds iff $\hat{e}''(Q_1, Q_4) = \hat{e}''(Q_2, Q_3)$ holds. Thus we can break the DDH assumption in $\langle Q \rangle$. This completes the proof of Theorem 1 (case f_i').

Since there is no endomorphism that sends $\langle Q \rangle$ to other group, the construction of non-degenerate bilinear map by combining pairing with distortion map cannot be applied to this case. Thus the DDH assumption in $\langle Q \rangle$ still remains valid.

Next we discuss relation between the one-wayness of $\mathcal{F}'$ and special case of co-DH assumption.

- *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

  $$\text{given } P, Q, Q', \text{ to find } P' \in \langle P \rangle \text{ such that } \log_P P' = \log_Q Q'.$$

  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 has efficiently recognizable since $Q'(\in E[l])$ is in $\langle Q \rangle$ if and only if $(\phi - [q \bmod l])Q' = O$.

3.3 Applications

The proposed one-way functions f_i and f'_i are efficiently computable isomorphisms. Then the relation $R_i = \{(f_i(y), y) | y \in \langle R \rangle\}$ and $R'_i = \{(f'_i(y), y) | y \in \langle R \rangle\}$ are commutative random self-reducible [21], [26]. The commutative random self-reducible problems have many cryptographic applications: identification, digital signature, divertible zero-knowledge interactive proof, blind signature, multi signature and so on.

Here we show a digital signature scheme using our candidate f_i.

[Key generation] Run the index generation algorithm $I(1^n)$ and obtain an index $i = (E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, R)$. Run the domain sampling algorithm $D(i)$ and obtain $S \in \langle R \rangle$. Run the function-evaluation algorithm $F(i, S)$ and obtain $V = f_i(S) \in \langle P \rangle$. Publicize (i, V, h) as verification key and keep S secret as signing key where h denotes a hash function from $\{0, 1\}^*$ to Z/lZ.

[Signing] Here we let m be a message to be signed. Run the domain sampling algorithm $D(i)$ and obtain $T \in \langle R \rangle$. Run the function-evaluation algorithm $F(i, T)$ and obtain $U = f_i(T) \in \langle P \rangle$. Compute a hash value $e = h(m, U)$ and $\sigma = T + eS$. Output (e, σ) as a signature on m.

[Verification] Assume we have an alleged signature (e, σ) on m. Confirm that σ is in $\langle R \rangle$ (i.e., confirm that $e(\sigma, R) = 1$ holds using the Weil pairing e). Verify whether the following equation holds:

$$e = h(m, f_i(\sigma) - eV).$$

We can prove the existential unforgeability against adaptively chosen message attack under the random oracle model, which is reducible to the one-wayness of f_i.

In the similar fashion, we can construct identification scheme, divertible zero-knowledge interactive proof, blind signature and multi signature based on our one-way functions.

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

Verification Given a public key V, a message m and a signature S, compute a 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 the Tate pairing.

The co-GDH signature is proved 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

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

would not be directly proved because there exist no endomorphisms that induces 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:

- Skewed-DH problem for $\mathcal{F}$: $(\langle P \rangle, \langle Q \rangle)$.
- Variant problem for $\mathcal{F}'$: $(\langle Q \rangle, \langle P \rangle)$.
- 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 assumption and the variant, respectively. Then it is concluded that the co-GDH signature should adopt the variant of the skewed-DH assumption (i.e., the 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:

- Challenge for the one-wayness of $\mathcal{F}$: $(\langle P \rangle, \langle R \rangle), f_i(P_2) = P_1$.

- Challenge for the one-wayness of $\mathcal{F}'$:
  $(\langle Q\rangle, \langle R\rangle), f_i'(P_2) = P_1$.

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 candidates of collection 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 open questions that have appeared 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-eigenspace $\langle R\rangle$
- 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," 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. SCN2002, 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, LNCS 2139, pp.213–229, Springer-Verlag, 2001.

[8] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," Proc. Eurocrypt 2003, LNCS 2656, pp.416–432, Springer-Verlag, 2003.

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

[10] Y. Dodis, "Efficient construction of (distributed) verifiable random functions," Proc. PKC2003, LNCS 2567, pp.1–17, Springer-Verlag, 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. ANTS-V, LNCS 2369, pp.324–337, Springer-Verlag, 2002.

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

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

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

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

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

[19] A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," IEEE Trans. Inf. Theory, vol.39, no.5, pp.1639–1646, 1993.

[20] 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

[21] T. Okamoto and K. Ohta, "Divertible zero-knowledge interactive proofs and commutative random self-reducibility," Proc. Eurocrypt '89, LNCS434, pp.134–149, Springer-Verlag, 1990.

[22] T. Saito, F. Hoshino, S. Uchiyama, and T. Kobayashi, "Candidate one-way functions on non-supersingular elliptic curves," IEICE Technical Report, ISEC2003-65, Sept. 2003.

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

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

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

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

[27] T. Saito, F. Hoshino, S. Uchiyama, and T. Kobayashi, "Non-supersingular elliptic curves for pairing-based cryptosystems," IEICE Trans. Fundamentals, vol.E87-A, no.5, pp.1203–1205, May 2004.

[28] T. Saito and S. Uchiyama, "The co-Diffie-Hellman problem over elliptic curves," Reports of the Faculty of Science and Engineering, Saga University, Mathematics, vol.33, no.1, pp.1–8, 2004.

[29] 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.

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

Appendix: 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 $\phi(P) - P = O$; Q is a point of order l such that $\phi(Q) - [q \bmod l]Q = O$; $P' = [r]P$ for randomly chosen $r \in \mathbb{Z}/l\mathbb{Z}$.

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

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

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

$$\Pr\left[\begin{array}{ll} A'(i') & = Q' \text{ and } \log_P P' = \log_Q Q' \\ & ;\ i' \leftarrow I'(1^n) \end{array}\right] \le \mu_{A'}(n)$$

where $i' = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P, Q, P')}$ and the probability is taken over the coin-tosses of A' and I'.

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

$$\left\{ i' \;;\; \begin{array}{ll} i & \leftarrow I(1^n), \\ R' & \overset{R}{\leftarrow} \langle R \rangle, P' = \mathrm{proj}_1(R') \end{array} \right\},$$

where

$$i = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, R)} \text{ and}$$
$$i' = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, \mathrm{proj}_1(R), \mathrm{proj}_2(R), P')},$$

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',

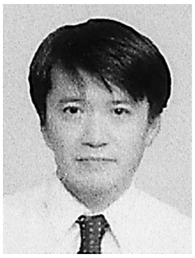
$$\left\{ (i, P') \;;\; i' \leftarrow I'(1^n) \right\},$$

where

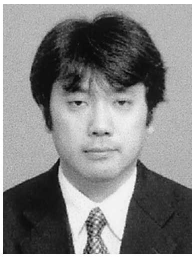
$$i' = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P, Q, P')} \quad \text{and}$$
$$i = \overline{(E, \mathbb{F}_q, l, \mathbb{F}_{q^k}, P + Q)}.$$

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 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 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'. Then we return $Q' = R' - P'$ as the answer of the DH-like problem.
  If $P' = [r]P$ and A succeeds, $R' = [r](P + Q)$ holds. Then we have $Q' = [r]Q$.

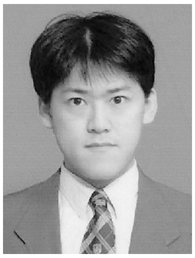


Taiichi Saito received his B.S. and M.S. degrees from Waseda University, Tokyo, Japan, and D.E. degree from Chuo University, Tokyo, Japan, in 1989, 1991 and 2001, respectively. He has been an associate professor at Tokyo Denki University since 2004. His research work focuses on algebraic algorithm and provable security in cryptography.



Fumitaka Hoshino received his B.Eng. and M.Eng. degrees from Tokyo University, Tokyo, Japan, in 1996 and 1998, respectively. He is a research engineer of NTT Information Sharing Platform Laboratories. His research interests are Information Security.

Shigenori Uchiyama received his B.S., M.S. and Ph.D. degrees from Kyushu University, Fukuoka, Japan, in 1991, 1993 and 1996, respectively. In 2000–2001, he was a visiting scholar of the Computer Science Department at the University of Southern California. Since joining NTT Laboratories in 1996, he has been engaged in research on cryptography and information security. He is currently a research scientist of NTT Information Sharing Platform Laboratories. Dr. Uchiyama is a member of the Mathematical Society of Japan.



Tetsutaro Kobayashi received his B.Eng. and M.Eng. degrees from Tokyo Institute of Technology, Tokyo, Japan, in 1993 and 1995, respectively. He is a Researcher in the NTT Information Sharing Platform Laboratories. He is presently engaged in research on Information Security. His interests lie in elliptic curve cryptosystems. He was awarded the SCIS'00 paper prize.