Inseparable Multiplex Transmission Using the Pairing on Elliptic Curves and Its Application to Watermarking

Maki Yoshida

Department of Informatics and Mathematical Science, Osaka University, Machikaneyama, Toyonaka, Osaka, 560-8531 Japan
maki-yos@ist.osaka-u.ac.jp

Abstract. Recently, various cryptographic schemes using a two-dimensional vector space over a finite field are proposed. We have proposed an inseparable multiplex transmission scheme (the IMT scheme) which also uses two-dimensional vector space. The IMT scheme is based on a new computational problem, called the vector decomposition problem (the VD problem). In this paper, the relation between the VD problem and the computational Diffie-Hellman problem on a one-dimensional vector space and the application of the IMT scheme are introduced. The application is the digital marking. The digital marking has some analogy to the digital watermarking, but the digital marking focuses on marking cryptographic data and this is new concept. The relation and the digital marking introduced in this paper is recently given by Yoshida, Mitsunari and Fujiwara.

1 Introduction

The concept of inseparable multiplex transmission is proposed in [5]. In the transmission, the two data are transformed into one multiplexed datum, and the multiplexed datum is used for carrying the contents of the original two data. The sender generates and sends multiplexed datum and the receiver extracts the contents of the original two data from the multiplexed datum. The feature of the inseparable multiplex transmission is that each original datum is inseparable from the multiplexed datum (see Section 3.1 for detail).

In [5], we propose the inseparable multiplex transmission scheme (the IMT scheme) which uses a two-dimensional vector space over a finite field and is based on the vector decomposition problem (the VD problem) on the vector space. The VD problem is the following problem: Given a basis and a vector, find the projection to the subspace spanned by each base. The idea of constructing the IMT scheme is that two data are two vectors which are linearly independent (and are generated from some basis) and the transformation is addition of two vectors. Then, if vector addition, vector subtraction and scalar multiplication are easy and the VD problem is hard, then inseparability of the original datum from the multiplexed datum is realized.
Recently, we show the relation between the VD problem on some two-dimensional vector space and the computational Diffie-Hellman problem on its one-dimensional subspace (on an additive group) in [6]. In other words, the sufficient condition under which the VD problem is at least as hard as the CDH problem and the reduction under the sufficient condition are shown. As an evidence that the sufficient condition is not very strong, we present an example of the vector space where the sufficient condition is satisfied and it is assumed that the CDH problem is hard in various cryptographic schemes in [1-4].

In [6], the digital marking is also proposed as an application of the IMT scheme. The digital marking is the technique to mark digital data such that the quality of its contents is not affected and marks are inseparable from the marked data. The target data are the cryptographic data such as ciphertexts, signatures and cryptographic keys generated in the cryptographic schemes using the pairing on elliptic curves [1–4]. Such cryptographic schemes use the two-dimensional vector space consists of the points on elliptic curves and the points are used as ciphertexts, signatures and cryptographic keys.

In this paper, these results in [6] are introduced. The results on the VD problem is shown in Section 2. Then, we overview the IMT scheme in Section 3. The digital marking is shown in Section 4.

2 The Vector Decomposition Problem

The definitions of the computational problems are shown in Section 2.1, and our recent results on the VD problem are introduced in Sections 2.2 and 2.3.

2.1 Definitions

Let $\mathbb{F}$ be a finite field, $V$ a two-dimensional $\mathbb{F}$-vector space and $0$ the zero element of $V$. For $v \in V$, let $(v)$ be $\{av | a \in \mathbb{F}\}$. First, the vector decomposition problem on $V$ is defined.

Definition 2.11 The vector decomposition (VD) problem on $V$: Given $e_1, e_2, v \in V$ such that $\{e_1, e_2\}$ is an $\mathbb{F}$-basis for $V$, find $u \in V$ such that $u \in (e_1)$ and $v - u \in (e_2)$.

A typical computational Diffie-Hellman problem is the following problem: Given $g, g^a, g^b \in G$, find $g^{ab} \in G$ where $G$ is a cyclic multiplicative group and $g$ is a generator of $G$. A one-dimensional vector space over a finite field is a cyclic additive group. The computational Diffie-Hellman problem on a one-dimensional $\mathbb{F}$-vector space $V'$ is defined similarly.

Definition 2.12 The computational Diffie-Hellman (CDH) problem on $V'$: Given $e \in V' \setminus \{0\}$ and $ae, be \in (e)$, find $u = abe \in (e)$.

We note that there is the unique solution for any instance of the above problems. For these problems, we define the Turing Machines (called function
or algorithm) from some tuple of $\Sigma^*$'s to $\Sigma^*$, where $\Sigma^*$ is the set of all possible strings over the finite alphabet $\Sigma = \{0,1\}$. In the followings, we assume that any vector in $V$ is represented by $\Sigma^*$, and that vector addition, vector subtraction and scalar multiplication are effectively defined and computed in polynomial time.

2.2 Intractability

Some of our results on the VD problem are the sufficient condition for the VD problem on $V$ to be at least as hard as the CDH problem on $V' \subset V$ and the reduction under the sufficient condition.

The sufficient condition is that on $V$ and $V'$. This condition is not very strong one. Actually, the cryptosystems proposed in [1] is based on the intractability of the CDH on $V' \subset V$ which satisfies the condition. In Section 2.3, we show $V$ and $V'$ which satisfies the condition and used in [1]. In the following theorem, we show the sufficient condition. The reduction is shown in its proof.

**Theorem 2.21** The VD problem on $V$ is at least as hard as the CDH problem on $V' \subset V$ if for any $e \in V'$ there are linear isomorphisms $\psi_e, \phi_e : V \to V$, which satisfy the following three conditions:

1. For any $v \in V$, $\psi_e(v)$ and $\phi_e(v)$ are effectively defined and can be computed in polynomial-time;
2. $\{e, \psi_e(e)\}$ is an $F$-basis for $V$;
3. There are $\alpha_1, \alpha_2, \alpha_3 \in F$ with

$$\phi_e(e) = \alpha_1 e,$$
$$\phi_e(\psi_e(e)) = \alpha_2 e + \alpha_3 \psi_e(e),$$
$$\alpha_1 \cdot \alpha_2 \cdot \alpha_3 \neq 0.$$

Elements $\alpha_1, \alpha_2, \alpha_3$ and their inverses can be computed in polynomial-time.

**Proof** For $(e, ae, be)$, the instance of the CDH problem on $V'$, $abe$ can be computed by calling the function $f_{\text{VD}}$ to solve the VD problem twice as follows:

(Step 0) The case $ae = 0$ is trivial. Suppose that $a \neq 0$. If the equation $(\alpha_3 - \alpha_1)ae = e$ holds, then we have $a = \frac{1}{\alpha_3 - \alpha_1}$ and therefore output $abe = \frac{1}{\alpha_3 - \alpha_1}be$. Otherwise, go to (Step 1).

Step 1) Let $u$ be $f_{\text{VD}}(e_1, e_2, be)$, where

$$e_1 = ae + \psi_e(\alpha_2^{-1}(\alpha_3 - \alpha_1) \cdot ae - \alpha_2^{-1}e),$$
$$e_2 = \phi_e(e_1).$$

We note that $e_1$ and $e_2$ can be computed from $e$ and $ae$ in polynomial-time, since (cond.1) and (cond.3) are satisfied.

(Step 2) Let $u_2$ be $f_{\text{VD}}(e, \psi_e(e), u_1)$. The solution is $\alpha_3^{-1}u_2$. 

Now, we show 1) the solution $\alpha_3^{-1}u_2$ of the above algorithm is always equal to $abe$, and 2) $\{e_1, e_2\}$ is a basis of $V$. To prove 1), we first show that $u_1 = \alpha_3 be_1$.

Let $\lambda = \alpha_2^{-1}(\alpha_3 - \alpha_1)a - \alpha_2^{-1}$ and $e' = \psi_e(e)$. Then, the followings are hold.

$$
e_1 = ae + \psi_e(\lambda e) = ae + \lambda e',
$$
$$
e_2 = \phi_e(e_1) = \alpha_1 ae + \lambda \phi_e(e')
= \alpha_1 ae + \lambda (\alpha_2 e + \alpha_3 e')
= (\alpha_1 a + \alpha_2 \lambda)e + \alpha_3 \lambda e'
= (\alpha_3 a - 1)e + \alpha_3 \lambda e'.
$$

Here, it holds that $\alpha_3 e_1 - e_2 = \alpha_3 ae - (\alpha_3 a - 1)e = e$, and then $be = b(\alpha_3 e_1 - e_2) = \alpha_3 be_1 - be_2$.

By applying $f_{VD}$ to $(e_1, e_2, be)$, we get $u_1 = \alpha_3 be_1$. From the definitions of $e_1 = ae + \lambda e'$ and $f_{VD}(e, e', u_1)$, $u_2 = \alpha_3 abe$. Then, the solution, $\alpha_3^{-1}u_2$, is equal to $abe$.

Finally, we show that $\{e_1, e_2\}$ is a basis of $V$, i.e. $\lambda(\alpha_3 a - \alpha_1) - \alpha\alpha_3 \lambda \neq 0$, since $\{e, e'\}$ is a basis of $V$ by (cond. 2). The condition holds if and only if

$$
\lambda \alpha_1 \neq 0 \iff \lambda \neq 0 (\alpha_1 \neq 0 \text{ by (cond. 3)})
\iff \alpha_2^{-1}((\alpha_3 - \alpha_1)a - 1) \neq 0
\iff (\alpha_3 - \alpha_1)a - 1 \neq 0
\iff (\alpha_3 - \alpha_1)a \neq 1.
$$

The last condition holds because it is the assumption to go to (Step 1). \hfill \square

2.3 Example

Another result on the VD problem is that we show an example of $V$ and $V'$ which satisfies the sufficient condition under which the VD problem on $V$ is at least as hard as the CDH problem on $V'$. The examples of $V$ and $V'$ are $E[m]$ and $E(F_p) \cap E[m]$, respectively. $E[m]$ is the two-dimensional $\mathbb{Z}/m\mathbb{Z}$-vector space. We note that the VD problem on $E[m]$ is at least as hard as the CDH problem on any one-dimensional subspace of $E[m]$. The intractability of the CDH problem on $E(F_p) \cap E[m]$ is assumed in the various cryptosystems using $E[m]$. It can be said that the sufficient condition is not very strong.

We describe the definitions of the system parameters.

$$
p: \text{ a prime with } p \equiv 2 (\text{mod } 3),
$$
$$
\mathbb{F}_p: \text{ a finite field of size } p,
$$
$$
E: y^2 = x^3 + 1, \text{ an elliptic curve over } \mathbb{F}_p,
$$
$$
m: \text{ a prime such that } 6m = p - 1,
$$
$$
E(\mathbb{F}_p): \text{ the set of the points } (x, y) \text{ on } E \text{ with } x, y \in \mathbb{F}_p,
$$
$$
E[m]: \text{ the group of } m\text{-torsion points on } E
$$
where $E[m] = \{P | mP = O\} \subset E(\mathbb{F}_p)$. 
The maps over \( E[m] \) are used to find a basis for \( E[m] \), e.g., in [1, 5]. The maps are the examples of \( \psi \) and \( \phi \) in Theorem 2.21. We describe these maps.

**Definition 2.31** [1] We define \( \psi : E[m] \to E[m] \) as the map such that \( \psi((x, y)) = (\zeta x, y) \) with \( \zeta^2 + \zeta + 1 = 0 \) and \( \zeta \in \mathbb{F}_p^2 \).

**Definition 2.32** [5] We define \( \phi : E[m] \to E[m] \) as the Frobenius map with \( p \) such that \( \phi((x, y)) = (x^p, y^p) \).

For any \( e \in V' \), \( \psi \) and \( \phi \) can be used as \( \psi_e \) and \( \phi_e \), respectively. The maps \( \psi \) and \( \phi \) do not depend on \( e \). Then, these two maps can be used for any \( e \in V \). This implies that the VD problem on \( E[m] \) is at least as hard as the CDH problem on any one-dimensional subspace of \( E[m] \).

One can prove that \( \psi \) and \( \phi \) are well-defined and linear isomorphisms. The proofs (for \( \psi \) and \( \phi \)) are shown in [1] and [5], respectively, and omitted here. For any \( e \), it can also be checked that (cond.1) and (cond.2) are satisfied.

**Theorem 2.33** If we choose a \( \mathbb{Z}/m\mathbb{Z} \)-basis \( \{e, \psi(e)\} \) for \( V \), then the followings are satisfied.

\[
\phi(e) = e, \\
\phi(\psi(e)) = -e - \psi(e).
\]

**Lemma 2.34** \( \phi(e) = e \) for any \( e \in V' \).

**Proof** For any \( e = (x, y) \in V' \), \( \phi(e) = (x^p, y^p) = (x, y) = e \). \( \square \)

**Lemma 2.35** \( \phi(\psi(e)) = -e - \psi(e) \) for any \( e \in V' \).

**Proof** For any \( e = (x, y) \in V' \), we have that

\[
\phi(\psi(e)) = \phi((\zeta x, y)) \\
= (\zeta x^p, y^p) \\
= (\zeta^2 x, y) \quad \text{(}\!\! (p \equiv 2 \pmod{3} \text{ and } \zeta^3 = 1) \\
= ((-1 - \zeta)x, y), \\
= \psi(\phi(e)) = \psi(e) \quad \text{(Lemma 2.34)} \\
= (\zeta x, y).
\]

Let \( (x', y') \) denote the coordinate of \( \phi(\psi(e)) + \psi(\phi(e)) \). Then,

\[
x' = \left( \frac{y - y}{\zeta x - (-1 - \zeta)x} \right)^2 - (-1 - \zeta)x - \zeta x \\
= x, \\
y' = -y + \left( \frac{y - y}{\zeta x - (-1 - \zeta)x} \right)((-1 - \zeta)x - x) \\
= -y.
\]

That is, \( \phi(\psi(e)) + \psi(\phi(e)) = -e \). Thus, \( \phi(\psi(e)) + \psi(\phi(e)) + e = 0 \). Since \( \psi(\phi(e)) = \psi(e) \), \( \phi(\psi(e)) = -e - \psi(e) \). \( \square \)
3 Imseparable Multiplex Transmission Scheme

In this section, we overview the IMT schemes proposed in [5, 6]. The IMT scheme has one parameter. The general transmission model and the parameter in the IMT scheme is described in Section 3.1. The tool used in the IMT scheme is defined in Section 3.2. Then, the construction of the IMT scheme is introduced in Section 3.3.

3.1 Feature

In this section, the feature of the inseparable multiplex transmission is shown. There is one parameter $f$ of the inseparable multiplex transmission where $f$ is a function. The parameter $f$ denotes what information is carried by transmitted data at each transmission. Let $F$ be a domain of $f$ and $G$ a range of $f$. Consider the following transmission between two parties, the sender and the receiver: The sender chooses two elements $a, b$ of $F$ independently, and generates the transmitted data which carries both $f(a)$ and $f(b)$; The receiver extracts both $f(a)$ and $f(b)$ from the transmitted data. At each transmission, one multiplexed datum, denoted $MD(a, b)$, is transmitted, or two non-multiplexed data, denoted $nMD(a)$ and $nMD(b)$, are transmitted. The requirements on transmitted data are as follows.

- For any $a, b \in F$, it is easy to compute $MD(a, b)$, $nMD(a)$ and $nMD(b)$.
- For any $MD(a, b)$, it is easy to compute $f(a)$ and $f(b)$.
- For any $nMD(a)$ and $nMD(b)$, it is easy to compute $f(a)$ and $f(b)$, respectively.

The feature of the inseparable multiplex transmission scheme is the following one-wayness of transmitted data, called inseparability.

- It is easy to compute $MD(a, b)$ from $nMD(a)$ and $nMD(b)$.
- It is hard to compute $nMD(a)$ or $nMD(b)$ from $MD(a, b)$.

In [5], we propose the inseparable multiplex transmission scheme using the pairing on elliptic curves where one vector in two-dimensional $\mathbb{Z}/m\mathbb{Z}$-vector space is used as the transmitted datum. The parameters of the scheme is as follows:

- $m$: a prime,
- $F: \mathbb{Z}/m\mathbb{Z}$,
- $G$: the subgroup of $\mathbb{F}_p^* = \mathbb{Z}/p\mathbb{Z}$ with size $m$
  where $p$ is a prime and $m|p - 1$,
- $g$: a generator of $G$,
- $f(x): g^x$.

In the schemes in [1-4], the two-dimensional $\mathbb{Z}/m\mathbb{Z}$-vector space is also used and one vector is used for carrying one element of $G$. On the other hand, our schemes in [5, 6] uses one vector for carrying two elements of $G$. 
3.2 Tool

The schemes in [5,6], one vector in $V$ is used as a transmitted datum and the pairing $e_m : V \times V \rightarrow G$ defined in Definition 3.21 is used for extracting two elements of $G$ from one vector of $V$. There should be an efficient algorithm to compute $e_m(v_1, v_2)$ for all $v_1, v_2 \in V$.

**Definition 3.21** For $V$ and $G$, a map $e_m : V \times V \rightarrow G$ is called a pairing if the following properties are satisfied:

- **Identity:** For any $v \in V$, $e_m(v, v) = 1$.
- **Bilinear:** For any $v_1, v_2, v_3 \in V$,

  $$e_m(v_1 + v_2, v_3) = e_m(v_1, v_3) \cdot e_m(v_2, v_3),$$
  $$e_m(v_1, v_2 + v_3) = e_m(v_1, v_2) \cdot e_m(v_1, v_3).$$

- **Non-triviality:** For any basis $(v_1, v_2)$, $e_m(v_1, v_2)$ is a generator of $G$.

We can use the Weil-pairing as $e_m$ if $V$ and $G$ are $E[m]$ and $\{x | x^m = 1\} \subseteq \mathbb{F}_q^*$, respectively, where the base field of $E$ is $\mathbb{F}_q$ and $s$ is the smallest integer which satisfies $E[m] \subseteq E(\mathbb{F}_q^*)$.

3.3 Construction

We will refer to Alice and Bob as two parties, the sender and the receiver, respectively. The scheme consists of three phases, Initialization, Encoding and Decoding.

**Initialization**

Alice and Bob agree on the following system parameters:

- $m$: a prime,
- $V$: the two-dimensional $\mathbb{Z}/m\mathbb{Z}$-vector space,
- $\phi$: an automorphism of $V$ in Theorem 2.21,
- $e_1, e_2$: the basis for $V$ with $e_2 = \phi(e_1)$,
- $G$: the cyclic multiplicative group of order $m$,
- $e_m$: a pairing defined in Definition 3.21,
- $g$: the generator for $G$ with $g = e_m(e_1, e_2)$.

**Encoding**

Suppose that Alice chooses two elements $r_1$ and $r_2$ from $\mathbb{Z}/m\mathbb{Z}$ and generates the transmitted data to carry two elements $g^{r_1}$ and $g^{r_2}$.

- When Alice generates and sends multiplexed datum denoted $MD(r_1, r_2)$, Alice computes $MD(r_1, r_2)$ based on the basis $(e_1, e_2)$, by

  $$MD(r_1, r_2) = r_1 e_1 + r_2 e_2,$$

  and sends it.
When Alice generates and sends two non-multiplexed data denoted \( nMD(r_i) \) with \( i \in \{1, 2\} \), Alice computes \( nMD(r_i) \) with \( i \in \{1, 2\} \) based on \( e_1 \), by

\[
nMD(r_i) = r_i e_1,
\]

and sends them.

- \( MD(r_1, r_2) \) can be computed from \( nMD(r_i) \) with \( i \in \{1, 2\} \) by

\[
nMD(r_1) + \phi(nMD(r_2)).
\]

**Decoding**

If the received data is the multiplexed datum \( MD(r_1, r_2) \), then Bob computes \( g^{r_1} \) and \( g^{r_2} \) by \( e_m(MD(r_1, r_2), e_2) \) and \( e_m(e_1, MD(r_1, r_2)) \), respectively. Otherwise, for \( nMD(r) \), Bob computes \( g^r \) by \( e_m(nMD(r), e_2) \).

Here, we show that \( g^{r_1} = e_m(MD(r_1, r_2), e_2) \).

\[
e_m(MD(r_1, r_2), e_2) = e_m(r_1 e_1 + r_2 e_2, e_2)
\]

\[
= e_m(e_1, e_2)^{r_1} e_m(e_2, e_2)^{r_2}
\]

\[
= e_m(e_1, e_2)^{r_1}.
\]

Similarly, it can be shown that \( g^{r_2} = e_m(e_1, MD(r_1, r_2)) \) and \( g^r = e_m(nMD(r), e_2) \).

**Remark**

Anyone who knows \( r_1 \) or \( r_2 \) can compute the non-multiplexed data \( nMD(r_i) = r_i e_1 \) with \( i \in \{1, 2\} \) since \( e_1 \) is public. But, neither \( r_1 \) nor \( r_2 \) is not trapdoor since we can use it for separating only the multiplexed datum \( MD(r_1, r_2) \).

Under the assumption that the VD problem on \( V \) is hard, it is hard to compute \( nMD(r_1) \) or \( nMD(r_2) \) from \( MD(r_1, r_2) \) \([5]\).

**4 The Digital Marking for Cryptographic Data**

Consider digital marking is the technique to mark digital data such that the quality of its contents is not affected and marks are inseparable from the marked contents. The inseparability of marks means intractability of removing marks from the marked contents without leaving traces. The digital marking can be used for watermarking for digital data. In \([6]\), target digital data are cryptographic data such as ciphertexts, signatures and cryptographic keys generated in the cryptographic schemes using the two-dimensional vector space over a finite field and the pairing on the vector space.

The quality of cryptographic data is that the functional requirements and the security are satisfied. For example, the quality of signature is that the integrity is verifiable (functional requirement) and the information to verify the integrity is unforgeable. We can realize the digital marking for cryptographic data by using the IMT scheme.

In the following, we show the digital marking for signature. The IMT scheme is used to generate the marked signature which carries both the same information.
to verify the signature and the information on mark. That is, the multiplexed datum is the marked signature. In the proposed digital marking, anyone can mark the cryptographic data and check whether the data is marked or not, and no one can remove mark from the marked data without secret information.

The correspondence between the marking and the IMT scheme is as follows: Alice is the signer who also marks the generated signature; Bob is the verifier who also detects mark in the signature; Signature is a vector (non-multiplexed datum); Mark is a random vector which is independent of the signature (non-multiplexed datum); Marked signature is the multiplexed datum generated from two non-multiplexed datum, the signature and the mark; Detecting mark and verification of signature can be done by decoding multiplexed datum. By using the trapdoor IMT scheme in [6], we realize the digital marking where only those who know the secret information can remove marks from any marked data, but the details are omitted here.

The proposed digital marking consists of three phases.

Key Generating

1. Alice and Bob do Initialization phase in the IMT scheme.
2. Alice generates the signing key $sk_A \in \mathbb{Z}/m\mathbb{Z}$ and publishes the verification key $vk_A = sk_Ae_2$.

Signing and Marking

Suppose that Alice signs on the message $M$.

1. For $M$, Alice computes the hash value $v_M \in V \setminus \{e_2\}$, and computes the signature $\text{sig}(M) = sk_A v_M$.
2. If Alice marks $\text{sig}(M)$, Alice chooses $r \in \mathbb{Z}/m\mathbb{Z}$ randomly and computes the marked signature $\text{sig}_{w(r)}(M) = sk_A v_M + re_2$.
3. Alice sends $(M, \text{sig}(M))$ or $(M, \text{sig}_{w(r)}(M))$ to Bob.

Verification and Detection

1. For the received pair $(M, \text{sig})$, Bob verifies the signature by comparing $e_m(v_M, vk_A)$ with $e_m(\text{sig}, e_2)$. If $e_m(v_M, vk_A)$ and $e_m(\text{sig}, e_2)$, then the signature $\text{sig}$ is valid. Otherwise, the signature is invalid.
2. Bob detects the existence of the mark by computing $g' = e_m(v_M, \text{sig})$. Bob decides the signature $\text{sig}$ to be marked if and only if $g' \neq 1$.

We note that Alice can remove the mark in $\text{sig}_{w(r)}(M)$ without trapdoor if Alice has $r$. Alice computes $\text{sig}(M)$ by computing $\text{sig}_{w(r)}(M) - re_2$. Then, $r$ is used as the removing information for the specific mark.

By using the same idea, we can realize the digital marking for ciphertext and cryptographic key.
5 Conclusion

Our recent results related to the IMT scheme have been shown. The results on
the VD problem is that the sufficient condition under which the VD problem is
at least as hard as the CDH problem, the reduction under the sufficient condition
and the example of vector space which satisfies the sufficient condition. In various
cryptographic schemes, the CDH problem on the example is assumed, and we
can consider that the sufficient condition is not so strong. The other result is
the digital marking which uses the IMT scheme as a tool. By using the digital
marking, we can add inseparable marks to the cryptographic data.

References

1. D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,”
Proceedings of
the Fifth Conference on
Algebraic Geometry, Number Theory,
Coding Theory and Cryptography

January 17–19, 2003
Graduate School of Mathematical Sciences
University of Tokyo