The Power of Identification Schemes

Kaoru Kurosawa[1] and Swee-Huay Heng[2]

[1] Department of Computer and Information Sciences,
Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
kurosawa@mx.ibaraki.ac.jp

[2] Faculty of Information Science and Technology,
Multimedia University,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
shheng@mmu.edu.my

Abstract. In this paper, we show that identification schemes (ID-schemes) are very powerful in some areas of cryptography. We first prove an equivalence between non-interactive trapdoor commitment schemes and a natural class of identification schemes. We next propose a more efficient on-line/off-line signature transformation than Shamir-Tauman. As an application, we present a variant of Boneh-Boyen (BB) signature scheme which is not only on-line/off-line but also has a smaller public key size than the original BB scheme. Finally, we present the first identity-based ID-scheme which is secure against concurrent man-in-the-middle attack without random oracles by using our variant of BB signature scheme.

Keywords: Identification scheme, signature scheme, trapdoor commitment scheme, on-line/off-line, identity-based

1 Introduction

1.1 Background

A commitment scheme consists of two phases: in the commit phase, a sender commits to a message, while in the decommit phase, the sender reveals the committed message. A trapdoor commitment scheme admits a trapdoor whose knowledge allows to open a commitment in any possible way. Gennaro generalized trapdoor commitment schemes to multi-trapdoor commitment schemes [12]. A multi-trapdoor commitment scheme is a family of secure trapdoor commitment schemes such that it admits a master trapdoor whose knowledge allows to open any commitment in the family in any possible way. He also showed a compiler which transforms any proof of knowledge (identification scheme) into one which is secure against the concurrent man-in-the-middle attack, where the compiler needs a multi-trapdoor commitment scheme and a strong one-time signature scheme in addition. We can thus have the following relationship:

ID-scheme + multi-trapdoor commitment + strong one-time signature
$\rightarrow$ ID-scheme secure against concurrent man-in-the-middle attack.

On the other hand, the notion of on-line/off-line signature schemes was introduced by Even et al. [9]. The on-line phase of this kind of signatures can be made very fast due to the pre-computation of the off-line phase. Shamir and Tauman showed how to transform a non-adaptively secure signature scheme to an adaptively secure on-line/off-line signature scheme by using trapdoor commitment schemes [25]. That is,

$$\text{Non-adaptive signature} + \text{trapdoor commitment} \rightarrow \text{Adaptive on-line/off-line signature} \quad (1)$$

This result is important because there exist only a few adaptively secure signature schemes in the standard model: Cramer-Shoup scheme [8] and Gennaro-Halevi-Rabin scheme [13] under the strong RSA assumption, and Boneh-Boyen scheme [1] under the strong Diffie-Hellman assumption.

Meanwhile, the idea of identity (ID)-based cryptography was formulated by Shamir [24] in 1984. An ID-based scheme is an asymmetric system wherein the public key is effectively replaced by a user's publicly available identity information or any arbitrary string which derived from the user's identity. It enables any pair of users to communicate securely without exchanging public or private keys and without keeping any key directories. Many ID-based schemes appeared in the literature since then, for example ID-based encryption schemes [4, 2, 3], ID-based signature schemes [21, 16, 7], etc.

The notion of ID-based identifications was formalized in Kurosawa and Heng [18] and Bellare et al. [6] independently. All the ID-based ID-schemes presented in the above two papers are provably secure in the random oracle model only. Provably secure ID-based ID-schemes in the standard model were first appeared in [19], but they are not secure against concurrent man-in-the-middle attack. In this paper, we propose the first ID-based ID-scheme which is provably secure against concurrent man-in-the-middle attack in the standard model.

1.2 Our Contributions

In this paper, we show that identification schemes (ID-schemes) are very powerful in some areas of cryptography.

We first prove an equivalence between non-interactive trapdoor commitment schemes and a natural class of identification schemes. This class includes Schnorr scheme [23], GQ scheme[15], Fiat-Shamir scheme [11] and the 2^{ℓ}-th root scheme [26].

Next, we show a more efficient transformation from a non-adaptively secure signature to an adaptively secure on-line/off-line signature than equation (1) by *directly* employing the canonical ID-scheme as a tool. The proposed transformation requires lesser memory in the off-line phase than Shamir-Tauman transformation [25] which is indicated by equation (1)).

Additionally, we present an on-line/off-line variant of Boneh-Boyen signature scheme (BB scheme) [1] as an example of the above transformation. The proposed scheme is not only on-line/off-line, but also the public key size is smaller than that of the original BB scheme. Although a similar scheme can be obtained by applying Shamir-Tauman transformation, our scheme, however, requires lesser memory in the off-line phase.

Finally, we present the first ID-based ID-scheme which is provably secure against concurrent man-in-the-middle attack in the standard model, deriving from our proposed variant of BB signature scheme.

All our results hold without relying on the random oracle heuristic. In the random oracle model, it is well-known that a canonical identification scheme can be transformed to a signature scheme by using the Fiat and Shamir technique [11]. Many signature schemes are obtained by this transformation [10, 15, 23, 20].

1.3 Organization

The rest of this paper is organized as follows. In Section 2, we briefly review some preliminaries. In Section 3, we prove the equivalence between identification scheme and trapdoor commitment scheme. In Section 4, we present a general transformation from any non-adaptively secure signature to the adaptively secure on-line/off-line signature by employing a canonical ID-scheme as a tool. In Section 5, we exhibit a concrete example by applying the above transformation to Boneh-Boyen signature scheme. In Section 6, we propose the first ID-based ID-scheme which is secure against concurrent man-in-the-middle attack in the standard model. Finally, we conclude this paper in Section 7.

2 Preliminaries

Throughout this paper, ℓ denotes the security parameter and a PPT algorithm denotes a probabilistic polynomial time algorithm.

2.1 Identification Scheme

In an identification scheme (ID-scheme), a prover P proves to a verifier V that she knows a *witness* s_I related to a public *instance* p_I. A canonical ID-scheme can be formalized by $\mathcal{ID} = (\mathsf{G}_{ID}, \mathsf{Commit}, \mathsf{Response}, \mathsf{Check})$, where G_{ID} is a PPT algorithm which generates (p_I, s_I). Commit , $\mathsf{Response}$ and Check are algorithms which specify the protocol (P, V) as follows.

Step 1. P chooses r at random from a certain domain $\textsc{Cmt}$ and computes $x = \mathsf{Commit}(r)$. P then sends x to V.

Step 2. V chooses a challenge c at random from a certain set $\textsc{Cha}$ and sends it to P.

Step 3. P computes a response $y = \mathsf{Response}(s_I, r, c)$ and sends y to V. Let $\textsc{Res}$ denote the set of possible y for p_I.

Step 4. V checks if

$$x = \mathsf{Check}(p_I, c, y). \tag{2}$$

V accepts P if and only if equation (2) holds.

The above protocol (P, V) is often called a Σ-protocol. We say that (x, c, y) is a valid transcript for p_I if it satisfies equation (2).

Definition 1. *We say that $\mathcal{ID}$ is a Σ-ID-scheme if the following holds:*

Completeness. $\Pr($*equation (2) holds*$) = 1$.

Special Soundness. *It is hard to compute two valid transcripts (x, c, y) and (x, c', y') such that $c \neq c'$ on input p_I.*

y-Uniformity. *For any fixed (s_I, c), $y = \mathsf{Response}(s_I, r, c)$ is uniformly distributed over* $\textsc{Res}$ *if r is uniformly distributed over* $\textsc{Cmt}$.

It is easy to see that y-uniformity implies that the protocol (P, V) is honest-verifier zero-knowledge. All the important identification schemes in cryptographic applications are Σ-ID-schemes.

2.2 Trapdoor Commitment Scheme

A trapdoor commitment scheme is defined by $\mathcal{TC} = (\mathsf{G}_{TC}, \mathsf{Tcom}, \mathsf{Topen})$. G_{TC} is a PPT algorithm which generates (pk, tk), where pk is the public key and tk is the trapdoor.

Tcom is the algorithm that computes a commitment on m as $x = \mathsf{Tcom}(pk, m, r)$, where r is a random number. To open the commitment x, the sender reveals m, r and the receiver recomputes x.

Topen is the algorithm that opens a commitment in any possible way with the trapdoor tk. For given m, r and $m' \neq m$, it outputs $r' = \mathsf{Topen}(tk, m, r, m')$ such that $x = \mathsf{Tcom}(pk, m, r) = \mathsf{Tcom}(pk, m', r')$.

This implies that the receiver has no information on m given x. We require that the sender cannot find a collision such as follows.

Definition 2. *We say that a trapdoor commitment scheme $\mathcal{TC}$ is secure if it is hard to compute (m, r) and (m', r') such that $\mathsf{Tcom}(m, r) = \mathsf{Tcom}(m', r')$ on input pk where $m \neq m'$.*

An example of trapdoor commitment scheme under the discrete logarithm assumption [22] is shown in Appendix A.

2.3 Signature Scheme

A signature scheme is denoted by $\Omega = (\mathsf{G}_{sign}, \mathsf{Sign}, \mathsf{Verify})$. G_{sign} is a PPT algorithm which generates (vk, sk), where vk is a verification key and sk is the secret key. Sign is a PPT algorithm which generates a signature σ on input a message m and the secret key sk. Verify is a polynomial time algorithm which checks the validity of (m, σ) by using vk, say $\mathsf{Verify}(vk, m, \sigma) = accept$ or $reject$.

Adaptive Security. The standard security notion of signature schemes is existential unforgeability against adaptive chosen message attack [14]. It is defined using the following game between a challenger and an adversary A:

1. The challenger runs G_{sign} to obtain (vk, sk). A is given vk.
2. A queries some message m_i to the challenger for $i = 1, \ldots, t$ adaptively. The challenger responds to each query with a signature $\sigma_i = \mathsf{Sign}(sk, m_i)$.
3. Eventually, A outputs a forgery (m^*, σ^*). A wins the game if $m^* \notin \{m_1, \ldots, m_t\}$ and $\mathsf{Verify}(vk, m^*, \sigma^*) = accept$.

We say that Ω is adaptively secure if $\Pr(A \text{ wins})$ is negligible for any PPT adversary A as shown above.

Non-Adaptive Security. A much weaker security notion is existential unforgeability against weak non-adaptive chosen message attack. It is defined using the following game between a challenger and an adversary A:

1. On input the security parameter 1^ℓ, the adversary A submits messages $m_1, \ldots, m_t$ (non-adaptively) to the challenger.
2. The challenger generates (vk, sk) randomly and computes the signatures $\sigma_1, \ldots, \sigma_t$. He then sends $vk, \sigma_1, \ldots, \sigma_t$ to A.
3. A outputs a forgery (m^*, σ^*). A wins the game if $m^* \notin \{m_1, \ldots, m_t\}$ and $\mathsf{Verify}(vk, m^*, \sigma^*) = accept$.

We say that Ω is non-adaptively secure if $\Pr(A \text{ wins})$ is negligible for any PPT adversary A as shown above.

There is another notion called one-time signature, informally this means that the adversary A is given the verification key vk and the signature σ on a message m of her choice (chosen after seeing vk), then it is infeasible for A to compute the signature of a different message, say (m^*, σ^*) such that $m^* \neq m$.

A *strong* one-time signature scheme means that it is infeasible for A to also generate (m^*, σ^*) such that $(m^*, \sigma^*) \neq (m, \sigma)$.

3 Equivalence between $\mathcal{ID}$ and $\mathcal{TC}$

We say that a Σ-ID-scheme is *reversible* if there exists a polynomial time algorithm $\mathsf{Reverse}$ which computes r such that

$$x = \mathsf{Commit}(r) = \mathsf{Check}(p_I, c, y)$$

from p_I, s_I, c and y. All the important identification schemes in cryptographic applications are *reversible* Σ-ID-schemes.

For example, we have a look at the famous Schnorr ID-scheme [23]. Suppose that the Schnorr ID-scheme is defined as $\mathcal{ID} = (\mathsf{G}_{ID}, \mathsf{Commit}, \mathsf{Response}, \mathsf{Check})$. Let G be a group of prime order q and g be the generator of G. G_{ID} is a PPT algorithm which generates $(p_I, s_I) = (g^s, s)$ where s is randomly chosen from Z_q. Commit , $\mathsf{Response}$ and Check are algorithms which specify the protocol (P, V) as follows.

Step 1. P chooses r at random from Z_q and computes $x = \mathsf{Commit}(r) = g^r$. P then sends x to V.

Step 2. V chooses a challenge c at random from Z_q and sends it to P.
Step 3. P computes a response

$$y = \mathsf{Response}(s, r, c) = r + cs \bmod q \tag{3}$$

and sends y to V.
Step 4. V checks if

$$x = \mathsf{Check}(g^s, c, y).$$

More precisely, V checks whether $x = g^r = g^y/(g^s)^c$. V accepts P if and only if the above equation holds.

Thus, it is not difficult to see that the Schnorr ID-scheme is a Σ-ID-scheme since it satisfies all the conditions in Definition 1. It is also a reversible Σ-ID-scheme since there exists a polynomial time algorithm $\mathsf{Reverse}$ which computes r such that

$$x = \mathsf{Commit}(r) = \mathsf{Check}(g^s, c, y),$$

given g^s, s, c and y. That is, r can be computed from equation (3) via

$$r = y - cs \bmod q.$$

Next, we prove that non-interactive trapdoor commitment schemes are equivalent to *reversible* Σ-ID-schemes.

Theorem 1. *If there exists a reversible Σ-ID-scheme, then there exists a trapdoor commitment scheme.*

Proof. We first prove that a reversible Σ-ID-scheme implies a trapdoor commitment scheme. Suppose that there exists a reversible Σ-ID-scheme. We then construct a trapdoor commitment scheme $\mathcal{TC} = (\mathsf{G}_{TC}, \mathsf{Tcom}, \mathsf{Topen})$ as follows. Let H be a collision-resistant hash function. Let $\mathsf{G}_{TC} = \mathsf{G}_{ID}$. That is, the key pair of $\mathcal{TC}$ is given by $(pk, tk) = (p_I, s_I)$, where $(p_I, s_I) \leftarrow \mathsf{G}_{ID}(1^\ell)$.

(Commitment) For a message m, let $x = \mathsf{Tcom}(pk, m, y) = \mathsf{Check}(p_I, H(m), y)$, where y is chosen at random. That is, we consider an execution of $\mathcal{ID}$ on input p_I such that x is a commit, $H(m)$ is a challenge and y is a response.

(Trapdoor) Suppose that m, y and $m' \neq m$ are given. Then we compute y' such that $x = \mathsf{Check}(p_I, H(m), y) = \mathsf{Check}(p_I, H(m'), y')$ as follows. By using $\mathsf{Reverse}$, compute r such that $x = \mathsf{Commit}(r)$ from $p_I, s_I, H(m)$ and y. Then let $y' = \mathsf{Response}(s_I, r, H(m'))$.

(Security) The above $\mathcal{TC}$ is secure from the special soundness of $\mathcal{ID}$. □

Theorem 2. *If there exists a trapdoor commitment scheme, then there exists a reversible Σ-ID-scheme.*

Proof. We prove that a trapdoor commitment scheme implies a reversible Σ-ID-scheme. Suppose that there exists a trapdoor commitment scheme $\mathcal{TC} = (\mathsf{G}_{TC}, \mathsf{Tcom}, \mathsf{Topen})$. We then construct a reversible Σ-ID-scheme as follows. Let H be a collision-resistant hash function.

Let $\mathsf{G}_{ID} = \mathsf{G}_{TC}$. That is, let $(p_I, s_I) = (pk, tk)$. Let $x = \mathsf{Commit}(R) = \mathsf{Tcom}(p_I, m, r)$, where $R = (m, r)$ is randomly chosen.

From $R = (m, r)$ and a given challenge c, compute y such that

$$\mathsf{Tcom}(p_I, c, y) = \mathsf{Tcom}(p_I, m, r)$$

by using the trapdoor key tk. Let $\mathsf{Response}(tk, R, c) = y$.

Define $\mathsf{Check}(p_I, c, y) = \mathsf{Tcom}(p_I, c, y)$.

We show that the above scheme is a reversible Σ-ID-scheme. It is easy to see that Pr(equation (2) holds) = 1. The special soundness holds from the security of $\mathcal{TC}$. The y-uniformity is clearly satisfied. Finally, we need to show $\mathsf{Reverse}$ which computes $R = (m, r)$ such that

$$x = \mathsf{Commit}(T) = \mathsf{Check}(p_I, c, y)$$

from tk, c and y. From our definition of Commit and Check, the above equation is written as

$$\mathsf{Tcom}(p_I, m, r) = \mathsf{Tcom}(p_I, c, y).$$

Next, $\mathsf{Reverse}$ chooses r at random and computes r which satisfies the above equation by using tk. This completes the proof. □

4 New On-line/Off-line Signature Scheme

The notion of on-line/off-line signature schemes was introduced by Even et al. [9]. In these schemes, the on-line phase of the signing algorithm is made very fast due to the pre-computation in the off-line phase. Shamir and Tauman showed how to transform a non-adaptively secure signature scheme to an on-line/off-line signature scheme which is adaptively secure by using trapdoor commitment schemes [25].

In this section, we show a more efficient transformation which requires lesser memory than Shamir-Tauman transformation by *directly* using Σ-ID-schemes instead of using our equivalence of Section 3 (see Table 1).

4.1 Proposed Transformation

Let $\Omega = (\mathsf{G}_{sign}, \mathsf{Sign}, \mathsf{Verify})$ be a non-adaptively secure signature scheme.
Let $\mathcal{ID} = (\mathsf{G}_{ID}, \mathsf{Commit}, \mathsf{Response}, \mathsf{Check})$ be a Σ-ID-scheme, where $\textsc{Cha}$ is the set of challenges and $\textsc{Res}$ is the set of responses. Let $H : \{0,1\}^* \to \textsc{Cha}$ be a collision-resistant hash function.

Then our on-line/off-line signature scheme is constructed as follows.

Key generation. Run G_{sign} to generate (vk, sk), and run G_{ID} to generate (p_I, s_I). The verification key is $vk' = (vk, p_I)$ and the secret key is $sk' = (sk, s_I)$.

Signing. The signing algorithm operates as follows.

1. Off-line phase: Choose $r \in \textsc{Cmt}$ randomly and compute $x = \mathsf{Commit}(r)$. For x, compute $\sigma = \mathsf{Sign}(sk, x)$ and store (r, σ).
2. On-line phase: Given a message $m \in \{0,1\}^*$, the on-line phase proceeds as follows. Retrieve (r, σ) from the memory. Compute $y = \mathsf{Response}(s_I, r, H(m))$. Let $\sigma' = (\sigma, y)$ be a signature of m.

Note that $(x, H(m), y)$ is a valid transcript of $\mathcal{ID}$.

Verification. For m and $\sigma' = (\sigma, y)$, first compute $x = \mathsf{Check}(p_I, H(m), y)$. Next accept (m, σ') if and only if (x, σ) is a valid message-signature pair under vk, that is, $\mathsf{Verify}(vk, x, \sigma) = accept$.

Note that the on-line phase is efficient because it computes only $y = \mathsf{Response}(s_I, r, H(m))$.

Theorem 3. *The above signature scheme Ω' is adaptively secure if Ω is non-adaptively secure and $\mathcal{ID}$ is a Σ-ID-scheme.*

Proof. Suppose that there exists a PPT adversary A for Ω' such that $\Pr(A \text{ wins})$ is non-negligible in the adaptive chosen message attack. Then we show that Ω is not non-adaptively secure or $\mathcal{ID}$ is not a Σ-ID-scheme.

The challenger gives $vk' = (vk, p_I)$ to A as the verification key. Assume that A queries messages m_i to the challenger and the challenger returns signature $\sigma' = (\sigma_i, y_i)$ for $i = 1, \ldots, t$. Eventually, A outputs a forgery m^* and $z = (\sigma^*, y^*)$. Let $x^* = \mathsf{Check}(p_I, H(m^*), y^*)$ and $x_i = \mathsf{Check}(p_I, H(m_i), y_i)$ for $i = 1, \ldots, t$.

We then distinguish two types of forgeries, Type-1 in which $x^* = x_j$ for some j, and Type-2 in which $x^* \neq x_i$ for any i. Type-1 forgery or type-2 forgery occurs with non-negligible probability.

(Type-1 forgery) In this case, we show a PPT algorithm M which breaks the special soundness of $\mathcal{ID}$. On input p_I, M behaves as follows.

1. M runs G_{sign} to obtain (vk, sk). M then acts as a challenger and sends $vk' = (vk, p_I)$ to A.
2. M simulates the challenger of A as follows. Suppose that A asks for a signature on m_i. Then M chooses $y_i \in \textsc{Res}$ randomly and computes $x_i = \mathsf{Check}(p_I, H(m_i), y_i)$. M next computes $\sigma_i = \mathsf{Sign}(sk, x_i)$ by using sk and returns a signature $\sigma'_i = (\sigma_i, y_i)$ to A.
3. Eventually, A returns a valid forgery m^* and $z = (\sigma^*, y^*)$ such that $m^* \neq m_j$ and $x^* = x_j$ for some j.

M then outputs two valid transcripts $(x^*(= x_j), H(m^*), y^*)$ and $(x_j, H(m_j), y_j)$ for p_I. Note that $H(m^*) \neq H(m_j)$ with overwhelming probability because $m^* \neq m_j$ and H is collision-resistant. This means that M breaks the special soundness of $\mathcal{ID}$.

(Type-2 forgery) In this case, we show a PPT adversary B that breaks Ω by non-adaptive chosen message attack. On input 1^ℓ, B behaves as follows.

1. M runs G_{ID} to obtain (p_I, s_I). For $i = 1, \ldots, t$, B chooses $r_i \in \textsc{Cmt}$ randomly and computes $x_i = \mathsf{Commit}(r_i)$. B sends $x_1, \ldots, x_t$ as messages to its challenger.
2. The challenger runs G_{sign} to obtain (vk, sk). It computes $\sigma_i = \mathsf{Sign}(sk, x_i)$ for $i = 1, \ldots, t$. It then returns $vk, \sigma_1, \ldots, \sigma_t$ to B.
3. B runs A on input $vk' = (vk, p_I)$.
4. M simulates the challenger of A as follows. Suppose that A asks for a signature on m_i. Then B computes $y_i = \mathsf{Response}(s_I, r_i, H(m_i))$ by using s_I and returns a signature $\sigma'_i = (\sigma_i, y_i)$ to A.
5. Eventually, A returns a valid forgery m^* and $z = (\sigma^*, y^*)$ such that $x^* \neq x_i$ for any i because it is a type-2 forgery.

B then outputs a forgery (x^*, σ^*). Now B wins because $x^* \neq x_i$ for any i and σ^* is a valid signature on x^*.

This completes the proof. □

4.2 Comparison

Shamir-Tauman [25] showed a transformation using trapdoor commitment schemes $\mathcal{TC} = (\mathsf{G}_{TC}, \mathsf{Tcom}, \mathsf{Topen})$ as follows.

Let $\Omega = (\mathsf{G}_{sign}, \mathsf{Sign}, \mathsf{Verify})$ be a non-adaptively secure signature scheme. A secret key of the on-line/off-line signature scheme is (sk, tk), where sk is a secret key of Ω and tk is a trapdoor key of $\mathcal{TC}$. The public key is (vk, pk), where vk is a verification key of Ω and pk is a public key of $\mathcal{TC}$.

1. Off-line phase: Choose a random message m' and a random number r'. Compute $hash = \mathsf{Tcom}(pk, m', r')$ and $\sigma = \mathsf{Sign}(sk, hash)$. Then store (m', r', σ).
2. On-line phase: Given a message m, the on-line phase proceeds as follows. Retrieve (m', r', σ) from the memory. By using tk, find r such that $\mathsf{Tcom}(pk, m, r) = \mathsf{Tcom}(pk, m', r')$. Let $\sigma' = (\sigma, r)$ be a signature of m.

Now in Shamir-Tauman scheme, the off-line phase must store (m', r', σ). On the other hand, our off-line phase stores only (r, σ). Hence our memory size is smaller if $|r| = |r'|$.

Table 1. On-line/Off-line Signature Transformation

	Tool	Memory
Shamir-Tauman [25]	trapdoor commitment	(m', r', σ)
Proposed	Σ-ID-scheme	(r, σ)

5 Application to BB Signature Scheme

Boneh and Boyen showed a signature scheme under the strong Diffie-Hellman assumption in the standard model [1].

In this section, we show an on-line/off-line variant of BB signature scheme as an application of our transformation. The proposed scheme is not only on-line/off-line, but also the public key size is smaller than that of BB scheme while the other parameters are of the same size. A similar scheme can be obtained by using Shamir-Tauman transformation. Our scheme, however, requires lesser memory in the off-line phase as shown in Table 1.

5.1 BB Signature Scheme

Let (G_1, G_2) be bilinear groups such that $|G_1| = |G_2| = p$, where p is a prime. Let $e : G_1 \times G_2 \to G_T$ be a pairing, where $|G_T| = p$. Let g_1 be a generator of G_1 and g_2 be a generator of G_2. Let $H : \{0,1\}^* \to Z_p^*$ be a collision-resistant hash function.

The basic BB scheme is non-adaptively secure under the strong DH assumption. A verification key is $v(= g_2^{\alpha})$, where $\alpha \in Z_q$ is the secret key. For a message $m \in \{0,1\}^*$, a signature is given by $\sigma = g_1^{\frac{1}{\alpha + H(m)}}$. Given (m, σ), verify that

$$e(\sigma, v \cdot g_2^{H(m)}) = e(g_1, g_2).$$

The full BB scheme is adaptively secure under the same assumption. A verification key is $u(= g_2^{\alpha})$ and $v(= g_2^{\beta})$, where $\alpha, \beta \in Z_q$ are the secret key. For a message $m \in \{0,1\}^*$, a signature is given by $(\sigma = g_1^{\frac{1}{\alpha + H(m) + \beta r}}, r)$, where $r \in Z_q$ is randomly chosen by the signer. Given (m, σ, r), verify that

$$e(\sigma, u \cdot g_2^{H(m)} \cdot v^r) = e(g_1, g_2).$$

5.2 Proposed On-line/Off-line Signature Scheme

We now apply our transformation of Section 4.1 to the basic BB scheme Ω and Schnorr identification scheme. Let $H : \{0,1\}^* \to Z_p^*$ and $\widetilde{H} : G_1 \to Z_p^*$ be two collision-resistant hash functions.

Key generation. Choose $\alpha \in Z_p$ randomly and compute $v = g_2^{\alpha}$. Let $\widetilde{g_1}$ be a generator of G_1. Choose $s \in Z_p$ randomly and compute $w = \widetilde{g_1}^{-s}$. Let (v, w) be a verification key and (α, s) be the secret key. Note that (v, α) is a key-pair of the basic BB scheme and (w, s) is a key-pair of Schnorr identification scheme.

Signing.

1. Off-line phase: Choose $r \in Z_p$ randomly and compute $x = \widetilde{g_1}^{r}$. For x, compute $\sigma = g_1^{\frac{1}{\alpha + \widetilde{H}(x)}}$ and store (r, σ). (Note that σ is a signature on x in the basic BB scheme.)
2. On-line phase: Given a message $m \in \{0,1\}^*$, the on-line phase proceeds as follows. Retrieve (r, σ) from the memory. Compute $y = r + sH(m) \bmod p$. Let $\sigma' = (\sigma, y)$ be a signature of m.

Verification. Given (m, σ, y), first compute $x = \widetilde{g_1}^y w^{H(m)}$. Next by using x, verify that

$$e(\sigma, v \cdot g_2^{\widetilde{H}(x)}) = e(g_1, g_2). \tag{4}$$

Theorem 4. *The above on-line/off-line signature scheme is adaptively secure under strong DH assumption in the standard model.*

Proof. The basic BB scheme is non-adaptively secure under strong DH assumption [1] and Schnorr scheme is a Σ-ID-scheme under the discrete logarithm assumption. Therefore, from Theorem 3, the above signature scheme is adaptively secure under strong DH assumption. □

Note that the on-line phase computes only $y = r + sH(m) \bmod p$. Hence it is very efficient. Moreover, our scheme has a smaller verification key as shown below. In [5], it is suggested to use an elliptic curve over $GF(3^\ell)$ for G_1 and one over $GF(3^{6\ell})$ for G_2. Hence in our scheme, the verification key size is approximately a half of the full BB signature scheme as shown in the following table.

Table 2. BB Scheme and Our Variant

	verification key	secret key	signature
Full BB scheme [1]	$u, v \in G_2$	$\alpha, \beta \in Z_p$	$\sigma \in G_1, r \in Z_p$
Our scheme	$v \in G_2,\ w \in G_1$	$\alpha, s \in Z_p$	$\sigma \in G_1, y \in Z_p$

6 ID-Based ID-Scheme without Random Oracles

The main differences of ID-based identification schemes from the usual identification schemes are that: (1) The adversary can choose a target identity ID of her choice to impersonate as opposed to a random public key; (2) The adversary can possess private keys of some users which she has chosen. The formal model of ID-based identification scheme was formalized in [18, 6].

In this section, we show the first ID-based ID-scheme which is provably secure against man-in-the-middle attack in the standard model by using our variant of BB signature scheme in Section 5.2. By applying Gennaro's technique [12] to the BB on-line/off-line *signature scheme*, we manage to transform it to an ID-based *ID-scheme* secure against concurrent man-in-the-middle attack under the strong DH assumption.

Gennaro [12]: Σ-ID-scheme → Very secure ID-scheme
Proposed: BB signature scheme → Very secure ID-based ID-scheme

6.1 Another Tool

We adopt the strong DH-based multi-trapdoor commitment scheme introduced by Gennaro into our construction since our BB on-line/off-line signature scheme is also based on the strong DH assumption.

The master key generation algorithm selects a random $\mu \in Z_p$ which will be the master trapdoor. The master public key will be the pair (g, g') where $g' = g^\mu$ in G. Each commitment in the family will be identified by a specific public key which is simply an element $n \in Z_p$. The specific trapdoor of this scheme is the value f_n in G such that $f_n^{\mu+n} = g$. To commit a message $m \in Z_p$ with public key n, the sender runs Pedersen's commitment [22] with bases g, h_n, where $h_n = g^n \cdot g'$. That is, it selects a random $\gamma \in Z_p$ and computes $\mathsf{com} = g^m h_n^\gamma$. The commitment to m is the value com. To open a commitment, the sender reveals m and $F = g^\gamma$. The receiver accepts the opening if $(g, F, g^n \cdot g', \mathsf{com} \cdot g^{-m})$ is a DH-tuple.

We also use a strong one-time signature scheme $\Omega = (\mathsf{G}_{sign}, \mathsf{Sign}, \mathsf{Verify})$.

6.2 Proposed ID-Based ID-Scheme

Let $\mathcal{IBI} = (\mathcal{S}, \mathcal{E}, \mathcal{P}, \mathcal{V})$ be four PPT algorithms known as setup, extract, and the identification protocol $(\mathcal{P}, \mathcal{V})$. Basically, our proposed scheme employs the key generation algorithm of BB on-line/off-line signature scheme as the setup algorithm and its signing algorithm as the extract algorithm.

Let (G_1, G_2) be bilinear groups where $|G_1| = |G_2| = p$ for some prime p. As usual, g_1 is a generator of G_1 and g_2 is a generator of G_2. Our proposed construction is as follows.

Setup. Choose $\alpha \in Z_p$ randomly and compute $v = g_2^\alpha$. Let $\widetilde{g_1}$ be a generator of G_1. Choose $s \in Z_p$ randomly and compute $w = \widetilde{g_1}^{-s}$. Choose two collision-resistant hash functions $H : \{0,1\}^* \to Z_p^*$ and $\widetilde{H} : G_1 \to Z_p^*$.

We also need the following extra common reference string: $g_1' = g_1^\mu$ for a random $\mu \in Z_p$ and a collision-resistant hash function H' with output in Z_p. The system parameters params is $(g_1, g_1', \widetilde{g_1}, g_2, v, w, H, \widetilde{H}, H')$ and the $\mathsf{master\text{-}key}$ is (α, s).

Extract. Given a $\mathsf{master\text{-}key}$ (α, s) and an identity $\mathsf{ID} \in \{0,1\}^*$, pick a random $r \in Z_p^*$ and compute $x = \widetilde{g_1}^r$. For x, compute $\sigma = g_1^{\frac{1}{\alpha + \widetilde{H}(x)}} \in G_1$. Next, compute $y = r + sH(\mathsf{ID}) \bmod p$. The user private key is (σ, y).

Protocol $(\mathcal{P}, \mathcal{V})$**.**

1. $\mathcal{P}$ first computes $(vk, sk) \leftarrow \mathsf{G}_{sign}(1^\ell)$ (run the key generation of the strong one-time signature scheme) and computes $n = H(vk)$, where n is a specific public key of the multi-trapdoor commitment scheme.

   It next chooses $R \in G_1$ randomly and computes $X = e(R, v \cdot g_2^{\widetilde{H}(x)})$. It also does the following: sets $h_n = g_1^n g_1'$; chooses $\gamma \in Z_p$ randomly and computes the commitment $\mathsf{com} = g_1^{H'(X)} h_n^\gamma$. It finally sends (y, com, vk) to $\mathcal{V}$.
2. $\mathcal{V}$ chooses $c \in Z_p$ randomly and sends c to $\mathcal{P}$.
3. $\mathcal{P}$ computes $S = R + c\sigma$ and $\mathsf{sig} = \mathsf{Sign}(sk, \mathsf{ID}, v, w, \mathsf{com}, c, X, \gamma, S)$. It then sends $(X, \gamma, S, \mathsf{sig})$ to $\mathcal{V}$.

4. $\mathcal{V}$ first computes $x = \widetilde{g_1}^y w^{H(\mathsf{ID})}$. $\mathcal{V}$ accepts if and only if $\mathsf{com} = g_1^{H'(X)} h_n^{\gamma}$, $\mathsf{Verify}(vk, \mathsf{ID}, v, w, \mathsf{com}, c, X, \gamma, S) = \mathit{accept}$ and $e(S, v \cdot g_2^{\widetilde{H}(x)}) = X \cdot e(g_1, g_2)^c$.

Note that (v, w) is a verification key, (α, s) is a secret key and (σ, y) is a signature on a message ID of our variant of BB signature scheme. In the basic Σ-ID-scheme, the prover reveals y at step 1, and then proves that it knows σ satisfying equation (4), where (X, c, S) is a valid transcript of the Σ-ID-scheme.

W can prove the following theorem even if the prover reveals y at step 1.

Theorem 5. *The above scheme is an ID-based ID-scheme which is secure against concurrent man-in-the-middle attack under the strong DH assumption.*

The above theorem can be proven similarly to Theorem 2 of the full version of [12] by adapting the proof for the identity-based setting.

7 Conclusion

We proved an equivalence between non-interactive trapdoor commitment schemes and a natural class of identification schemes. We also showed an efficient transformation from any non-adaptively secure signature to an adaptively secure on-line/off-line signature by using a canonical ID-scheme as a tool. For instance, we applied the above transformation to Boneh-Boyen signature scheme and we managed to obtain an on-line/off-line signature scheme with smaller public key size than that of the original Boneh-Boyen scheme. Finally, we presented the first ID-based ID-scheme which is provably secure against concurrent man-in-the-middle attack in the standard model.

References

1. D. Boneh and X. Boyen. Short signatures without random oracles. *Advances in Cryptology — EUROCRYPT '04*, LNCS 3027, pp. 56–73, Springer-Verlag, 2004.
2. D. Boneh and X. Boyen. Efficient selective-ID secure identity-based encryption without random oracles. *Advances in Cryptology — EUROCRYPT '04*, LNCS 3027, pp. 223–238, Springer-Verlag, 2004.
3. D. Boneh and X. Boyen. Secure identity based encryption without random oracles. *Advances in Cryptology–CRYPTO '04*, LNCS 3152, pp.443–459, Springer-Verlag, 2004.
4. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *Advances in Cryptology — CRYPTO '01*, LNCS 2139, pp. 213–229, Springer-Verlag, 2001.
5. D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing. *Advances in Cryptology — ASIACRYPT '01, LNCS 2248,* pp. 514–532, Springer-Verlag, 2001.
6. M. Bellare, C. Namprempre and G. Nevan. Security proofs for identity-based identification and signature schemes. *Advances in Cryptology — EUROCRYPT '04*, LNCS 3027, pp. 268–286, Springer-Verlag, 2004.

7. J. C. Cha and J. H. Cheon. An identity-based signature from gap Diffie-Hellman groups. *Public Key Cryptography — PKC '03*, LNCS 2567, pp. 18–30, Springer-Verlag, 2003.
8. R. Cramer and V. Shoup. Signature schemes based on the strong RSA assumption. *ACM Transactions on Information and System Security — ACM TIDSEC '00*, vol. 3, no. 3, 2000. Extended abstract in *Proc. 6th ACM CCS*, 1999.
9. S. Even, O. Goldreich and S. Micali. On-line/Off-line digital signatures. *Journal of Cryptology*, vol. 9, no. 1, pp. 35–67, Springer-Verlag, 1996.
10. U. Feige, A. Fiat and A. Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology*, vol. 1, pp. 77–94, Springer-Verlag, 1988.
11. A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. *Advances in Cryptology — CRYPTO '86*, LNCS 263, pp. 186–194, Springer-Verlag, 1987.
12. R. Gennaro. Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-the-middle attacks. *Advances in Cryptology — CRYPTO '04*, LNCS 3152, pp. 220–236, Springer-Verlag, 2004. Full version is available from IACR ePrint archive Report 2003/114 at `http://eprint.iacr.org/2003/214`.
13. R. Gennaro, S. Halevi and T. Rabin. Secure hash-and-sign signatures without the random oracle. *Advances in Cryptology — EUROCRYPT '99*, LNCS 1592, pp. 123–139, Springer-Verlag, 1999.
14. S. Goldwasser, S. Micali and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal of Computing*, vol. 17, no. 2, pp. 281–308, 1988.
15. L. Guillou and J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory. *Advances in Cryptology — EUROCRYPT '88*, LNCS 330, pp. 123–128, Springer-Verlag, 1989.
16. F. Hess. Efficient identity based signature schemes based on pairings. *Selected Areas in Cryptography — SAC '02*, LNCS 2595, pp. 310–324, Springer-Verlag, 2002.
17. E. van Heyst and T. P. Pedersen. How to make efficient fail-stop signatures. *Advances in Cryptology — EUROCRYPT '92*, LNCS 658, pp. 366–377, Springer-Verlag, 1992.
18. K. Kurosawa and S.-H. Heng. From digital signature to ID-based identification/signature. *Public Key Cryptography — PKC '04*, LNCS 2947, pp. 248–261, Springer-Verlag, 2004.
19. K. Kurosawa and S.-H. Heng. Identity-based identification without random oracles. *Information Security and Hiding — ISH '05 (in conjuction with ICCSA '05)*, LNCS 3481, pp. 603–613, Springer-Verlag, 2005.
20. T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. *Advances in Cryptology — CRYPTO '92*, LNCS 740, pp. 31–53, Springer-Verlag, 1993.
21. K. G. Paterson. ID-based signatures from pairings on elliptic curves. *Electronic Letters*, vol. 38, no. 18, pp. 1025–1026, 2002.
22. T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. *Advances in Cryptology — CRYPTO '91*, LNCS 576, pp. 129–140, Springer-Verlag, 1992.
23. C. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, vol. 4, pp. 161–174, Springer-Verlag, 1991.
24. A. Shamir. Identity-based cryptosystems and signature schemes. *Advances in Cryptology — CRYPTO '84*, LNCS 0196, pp. 47–53, Springer-Verlag, 1985.

25. A. Shamir and Y. Tauman. Improved online/offline signature schemes. *Advances in Cryptology — CRYPTO '01*, LNCS 2139, pp. 355–367, Springer-Verlag, 2001.
26. V. Shoup. On the security of a practical identification scheme. *Journal of Cryptology*, vol. 12, no. 4, pp. 247–260, Springer-Verlag, 1999.

A DLOG-Based Trapdoor Commitment

The public key consists of a group G of prime order p and its two generators g_1 and $g_2 = g_1^t$, where t is the trapdoor key. Let $\mathsf{Tcom}(m, r) = g_1^m g_2^r$. From m, r and $m' \neq m$, it is easy to compute r' such that $\mathsf{Tcom}(m, r) = \mathsf{Tcom}(m', r')$ by using t. Just solve

$$m + tr = m' + tr' \bmod p. \tag{5}$$

On the other hand, if one can find such a collision pair, then he can compute the discrete logarithm t of g_2 on base g_1 by solving equation (5) on t.