# An Improved Efficient Provable Secure Identity-Based Identification Scheme in the Standard Model

**Syh-Yuan Tan[1,3], Ji-Jian Chin[1,2] , Swee-Huay Heng[1] and Bok-Min Goi[3]**
[1] Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia
[2] Faculty of Engineering, Multimedia University, Cyberjaya, Selangor, Malaysia
[{e-mail: sytan,jjchin,shheng}@mmu.edu.my]
[3] Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Kuala Lumpur, Malaysia
[goibm@utar.edu.my]
*Corresponding author: Syh-Yuan Tan

*Received November 22, 2012; revised March 7, 2013; accepted April 29, 2013; published April 30, 2013*

## Abstract

In 2008, Chin et al. proposed an efficient and provable secure identity-based identification scheme in the standard model. However, we discovered a subtle flaw in the security proof which renders the proof of security useless. While no weakness has been found in the scheme itself, a scheme that is desired would be one with an accompanying proof of security. In this paper, we provide a fix to the scheme to overcome the problem without affecting the efficiency as well as a new proof of security. In particular, we show that only one extra pre-computable pairing operation should be added into the commitment phase of the identification protocol to fix the proof of security under the same hard problems.

***Keywords:*** Identity-based identification, standard model, proof of security

**http://dx.doi.org/10.3837/tiis.2013.04.018**

# 1. Introduction

Identity-based identification (IBI) schemes were proposed and rigorously defined in 2004 independently by Kurosawa and Heng [1], and Bellare et al. [2]. An identification scheme allows a prover to prove his knowledge of his secret key to a verifier in order to gain access to some resources, while the verifier learns nothing of the secret throughout the interaction. This is done by using a honest verifier zero knowledge proof of knowledge protocol. While traditional public key cryptography had to deal with the certificate management problem, Shamir [3] proposed the notion of identity-based cryptography, where a user's secret key is generated as a function related to his identity-string.

In [4], Bellare and Rogaway proposed the random oracle model, a heuristic model where random oracles exist, to prove the security of security schemes where there are no mathematical parameters available to do so. However, Canetti et al. [5] showed that there were some schemes that can be rendered insecure when the random oracles were replaced by instantiations of real-world hash functions. The majority of IBI schemes in existence to date are provable secure in the random oracle model, most of them found in the work of [2], where IBI schemes are derived from transformations from traditional identification schemes and digital signature schemes.

Kurosawa and Heng [6] proposed the first two IBI scheme in the standard model. However, their first scheme was only proven secure against passive impersonators, while their second scheme that is secure against active and concurrent impersonators is quite impractical, given that it required six pairing operations in the protocol. The authors followed up with another scheme in [7] in the standard model, however that scheme is also complex as it required a strong one-time signature in the protocol.

In the work [8], Chin et al. proposed an efficient and provable secure IBI scheme that requires only 3 pairing operations in the protocol. The only disadvantage is the large parameter size, which could be optimized by using techniques from [9] and [10]. In order to prove the security, proofs of security against passive and active/concurrent attackers were provided in the paper, but there is a very subtle flaw in the transcript and identification queries of the proofs. The flaw discredits the entire scheme because while there were no attack found in the scheme, without a proof of security, it would be hard to put confidence on it. However, fixing the complicated proof without making significant changes on the scheme itself to maintain its current complexity is not an easy task.

In this paper, we show an efficient fix to the flaw in Chin et al.'s IBI [8] where by only one extra pairing operation is added to the identification protocol. Moreover, this extra pairing operation can be pre-computed with an acceptable size increment in user private key. Our opinion is that while other IBI schemes have been proposed, a scheme provable secure in the standard model is still of research interest, especially one that is run-time efficient. The rest of the paper is partitioned as follows: In Section 2, we provide some preliminaries, such as the hard problems and assumptions. In Section 3, we first provide a review of the scheme from [8], then we explain the flaw in the proof of security. Finally, in Section 4, we propose our fixed scheme and provide the renewed proof of security. We conclude in Section 5 with some closing remarks.

# 2. Preliminaries

## 2.1. Bilinear Pairings

Let $G$ and $G_T$ be cyclic multiplicative groups of prime order $q$ where the discrete logarithm problems are intractable. We call $e: G \times G \rightarrow G_T$ an admissible bilinear map if it satisfies the properties of bilinearity, non-degeneracy and computability. Bilinearity states that $e(g^a, g^b) = e(g, g)^{ab}$ for all

generator $g \in G$ and $a, b \in Z_q^*$ while non-degenaracy defines that $e(g, g) \neq 1$. Lastly, computability terms that the computation of the bilinear map $e$ should be efficient.

## 2.2. Problems and Assumptions

The security of the IBI scheme in [8] was based on the following problems:

a) Computational Diffie-Hellman problem (CDHP):Given $g, g^a, g^b$ for some $a, b \in Z_q^*$, compute $g^{ab}$.
b) One-More computational Diffie-Hellman Problem (OMCDHP): The OMCDHP was first proposed by [11] as a game played by an adversary. The adversary is given $1^k, G, G_T, g, g^a$ as input and access to two oracles *CHALL* and *CDH*. *CHALL* on any input returns a random point $W_i$, while *CDH* on any input $h$ will return $h^a$. The adversary is required to compute the CDH solutions to all $W_0, \ldots, W_n$ the target points while using strictly less queries to the *CDH* oracle. In other words, the adverasry is required to find $W_0^a, \ldots, W_n^a$ while using the *CDH* oracle only $i < n$ times.

We assume that the CDHP and the OMCDHP are intractable, that is there are no polynomial time algorithsm for solving these problems with non-negligible probability.

## 2.3. Security Model for IBI

An IBI scheme consists of four probabilistic polynomial time algorithms **(Setup, Extract, Prove and Verify)**.

1) **Setup(S)**: **S** takes in the security parameter $1^k$. It publishes the master public key $mpk$ and keeps the master secret key $msk$ to itself.
2) **Extract(E)**: **E** takes in the public identity $ID$ and $msk$, and returns the corresponding user private key $usk$.
3) **Identification Protocol (Prover P and Verifier V)**: **P** receives $mpk, ID$, and $usk$ as input while **V** receives $ID$ and $mpk$. The two will then run an itneractive protocol where **V** will decide whether to accept or reject **P** after each iteration. The interactive protocol consists of the following steps:
   (a) Commitment: **P** sends a commitment $CMT$ to **V**.
   (b) Challenge: **V** sends a challenge $CHA$ randomly chosen from a predefined set.
   (c) Response: **P** returns a response $RSP$ where **V** will either choose to accept or reject.

The goal of an adversary on an IBI scheme is impersonation. There are three types of adversaries, namely, passive attacker, active attacker and concurrent attacker. Eavesdropping on conversations between honest parties in attempt to extract information from their transcripts is the ability of passive attacker. Active attacker on the other hand is able to interact with honest provers as a cheating verifier to extract information. Concurrent attacker the active attacker with the ability to interact with a few prover clones at once.

For IBI schemes, an adversary is required to choose a public identity of his choice as opposed to public keys from traditional identification schemes. It is also assumed that the adversary obtained some user private keys of other users and therefore the definition allows access to private keys associated with any identity besides the one being attacked. We describe the security of an IBI scheme as a two-phased game played by an impersonator *I* and a challenger *C*.

- **Setup**. *C* takes input $1^k$ and runs **Setup**. It gives the parameters to *I* and keeps the master secret key to itself.
- **Phase 1**. In this learning phase, *I* issues extract queries and identification queries adaptively to *C*. For the passive attacker, *C* responds with valid transcripts, while for the active and concurrent attackers, *C* responds by playing the role of the prover while *I* acts as the cheating verifier.
- **Phase 2**. Eventually *I* outputs a challenge identity $ID^*$ on which it wishes to impersonate. *I* now acts as the cheating prover trying to convince the verifier *C* based on the information gathered in **Phase 1** and wins the game if it is successful.

We say an IBI scheme is $(t_{IBI}, q_{IBI}, \varepsilon_{IBI})$-secure under passive (active and concurrent) attack if for any passive (active and concurrent) impersonator $I$ who runs in time $t_{IBI}$, Pr[$I$ can impersonate] $\leq \varepsilon_{IBI}$ where $I$ can make at most $q_{IBI}$ extract queries.

## 3. Chin et al.'s IBI Scheme

We now review Chin et al.'s scheme [8]. Let $G$ and $G_T$ be finite cyclic groups of large prime order $q$ and let $g$ be a generator of $G$. Use a collision-resistant hash function $H: \{0,1\}^* \rightarrow \{0,1\}^n$ to hash identity strings of arbitrary length of size $n$.

1. **Setup (S)**. Select a random secret $a \overset{\$}{\leftarrow} Z_q$, random values $g_2, u'$ and an $n$-length vector $\langle u \rangle$ which contains elements $u_1, \ldots, u_n \in G$. Set $g_1 = g^a$ and publish the public parameters as $\langle G, G_T, e, g, g_1, u', \langle u \rangle, H \rangle$. The master secret key is $g_2^a$.
2. **Extract (E)**. Parse $ID$ as an $n$-bit identity string with $d_i$, denoting the $i$-th bit of $ID$. Let $ID = \{1, \ldots, n\}$ be the set of all $i$ in which $d_i = 1$. Select $r \overset{\$}{\leftarrow} Z_q$. The user secret key can then be constructed as:

$$usk = (S, R) = (g_2^a \left( u' \prod_{i \in ID} u_i \right)^r, g^r)$$

3. **Identification protocol (Prover P and Verifier V)** will do the following:
   **a)** **P** chooses a random $z \overset{\$}{\leftarrow} Z_q$, computes $X = (u' \prod_{i \in ID} u_i)^z, Y = g_2^z$ and sends $X, Y, R$ to **V**
   **b)** **V** picks a random challenge $c \overset{\$}{\leftarrow} Z_q$ and sends it to **P**.
   **c)** **P** calculates $Z = S^{z+c}$ and sends $Z$ as a response to **V**.
   **V** accepts if

$$e(Z, g) = e(Y g_2^c, g_1) e(X \left( u' \prod_{i \in ID} u_i \right)^c, R)$$

We will briefly discuss the original security proof idea from [8] and highlight the flaw in the coming section.

### 3.1. Original Security Proofs

The original proof of security against impersonation under passive attack is done by contradicting the hardness of CDHP. In particular, Chin et al. showed that with the help of an impersonator $I$ which is equipped with passive attack ability, there exist an algorithm $M$ that can solve the CDHP. But the CDHP is intractable with technologies to date and thus such impersonator does not exist. The same technique was used for the proof of security against impersonation under active and concurrent attacks based on the OMCDHP. We now briefly describe the original proofs before pointing out the flaw.

#### 3.1.1 Security Against Passive Attack

**Theorem 1.** *The above IBI scheme is* $(t, q_I, \varepsilon)$*-secure against impersonation under passive attack in the standard model if the CDHP is* $(t, \varepsilon')$*-hard.*

*Proof.* $M$ is given a group $G$, a generator $g \in G$ and elements $g^a, g^b$. $M$ simulates the challenger for $I$ as follows in order to compute $g^{ab}$:

1. Setup. $M$ crafts master public key as $\langle G, G_T, e, g, g_1, g_2, u', \langle u \rangle, H \rangle$. $M$ defines two functions $F(ID)$

and $J(ID)$ to replace the Waters' hash function such that:

$$u' \prod_{i \in ID} u_i = g_2^{F(ID)} g^{J(ID)} \tag{1}$$

2. Extract Query. *M* computes the user private key as:

$$\left( \tilde{S}_i = g_1^{-\frac{J(ID_i)}{F(ID_i)}} \left( u' \prod_{i \in ID} u_i \right)^{r_i}, \tilde{R}_i = g_1^{-1/F(ID_i)} g^{r_i} \right)$$

As $F(ID)$ has been crafted such that its value will be equals to zero in some occasions, *M* will abort if that happens because it is unable to construct the private key (fraction with denominator zero is undefined).

3. Transcript Query. If $F(ID_j) \neq 0$, *M* runs the Extract query algorithm and produces a valid transcript for *I*. Else if $F(ID_j) = 0$, *M* chooses $r_j, c_j, z_j \overset{\$}{\leftarrow} Z_q$ and sends *I* the transcript as:

$$\left( \widetilde{X_J} = \left( u' \prod_{i \in ID} u_i \right)^{z_j}, \widetilde{Y_J} = g^{z_j} g_2^{-c_j}, \widetilde{R_J} = g^{r_j}, c_j, \widetilde{Z_J} = g_1^{z_j} \left( u' \prod_{i \in ID} u_i \right)^{(z_j + c_j) r_j} \right)$$

After some time, *I* outputs the challenge identity $ID^* \notin \{ID_i\}$ that it wishes to be challenged on and takes the role of the cheating prover to try to convince *M*. *M* obtains the transcript $(X, Y, R, c_1, z_1)$ after the first intraction with *I*. Next, *M* resets *I* to where it just sent its commitment to obtain another transcript $(X, Y, R, c_2, z_2)$. *M* can then using the reset lemma [12] to extract *S* from two conversation transcripts and outputs the solution to the CDHP as:

$$\frac{S}{R^{J(ID^*)}} = \frac{g^{ab} (u' \prod_{i \in ID^*} u_i)^r}{g^{J(ID^*) r}} = g^{ab}$$

■

### 3.1.2 Security Against Active and Concurrent Attacks

**Theorem 2.** *The above IBI scheme is* $(t, q_I, \varepsilon)$*-secure against impersonation under active and concurrent attack in the standard model if the CDHP is* $(t, \varepsilon")$*-hard.*

*Proof.* The proof of the active and concurrent attacks is similar to the one of Theorem 1. Here we only point out the differences. To begin the game, *M* is given elements $(g, g^a)$ as access to the *CHALL* and *CDH* oracles. *M* queries the *CHALL* oracle for $W_0$.

1. Setup. *M* sets $g_1 = g^a$ and queries the *CHALL* oracle for the initial challenge $W_0$, which it sets as $g_2$. The rest are simulated as the proof before.
2. Extract Query. This is similar to the proof before.
3. Identification Query. If $F(ID_j) \neq 0$, *M* will have no problem simulating an identification protocol instance for *I* by running the Extract algorithm first to obtain the private key for $ID_j$. Else if $F(ID_j) = 0$, *M* keeps a counter $m$ and does the following:
   a) *M* queries CHALL for $W_m$ and lets $\tilde{Y}_j = W_m$. *M* also selects $r_j \overset{\$}{\leftarrow} Z_q$ and computes $(\widetilde{X_J} = g^{J(ID_j)} = \left( u' \prod_{i \in ID_j} u_i \right), \widetilde{R_J} = g_1^{r_j})$. *M* sends $\widetilde{X_J}, \widetilde{Y_J}, \widetilde{R_J}$ to *I*.
   b) *I* picks a random challenge $c_j \overset{\$}{\leftarrow} Z_q$ and sends it to *M*.

c) $M$ queries the $CDH$ oracle with $[W_m\left(u'^{\prod_{i\in ID_j}u_i}\right)^{r_j}(W_0\left(u'\prod_{i\in ID_j}u_i\right))^{c_j}]$ and receives the response $[W_m\left(u'^{\prod_{i\in ID_j}u_i}\right)^{r_j}(W_0\left(u'\prod_{i\in ID_j}u_i\right))^{c_j}]^a$. $M$ increments $m$ by 1.

After some time, $I$ outputs the challenge identity $ID^* \notin \{ID_i\}$ that it wishes to be challenged on. Using the same technique as in Theorem 1, $M$ can calculates $S$ as $S = (Z_1 Z_2^{-1})^{(c_1-c_2)^{-1}}$ and outputs the solution to the CDHP as:

$$\frac{S}{R^{J(ID^*)}} = \frac{W_0^a(u'\prod_{i\in ID^*}u_i)^r}{g^{J(ID^*)r}} = W_0^a$$

■

## 3.2. Flaw in Security Proofs

We now point out the portion of the proof where the flaw appears: the response of the simulator $M$ for identification query queried by the impersonator $I$ in the simulation. In the passive attack proof, whenever $I$ issues a query on the challenge identity, which is where $M$ produces a valid transcript for $ID_j$:

$$\left(\tilde{X}_j = \left(u'\prod_{i\in ID_j}u_i\right)^{z_j}, \tilde{Y}_j = g^{z_j}g_2^{-c_j}, \tilde{R} = g^{r_j}, \tilde{Z}_j = g_1^{z_j}\left(u'\prod_{i\in ID_j}u_i\right)^{r_j(z_j+c_j)}\right)$$

Although this is a valid simulation that passes the check of completeness, the simulated transcript is not identically distributed compared to the honest valid transcript. In precise, $I$ can discern that $e(X, g_2) = e\left(\left(u'\prod_{i\in ID_j}u_i\right), Y\right)$ when $F(ID_j) \neq 0$ but $e(X, g_2) \neq e\left(\left(u'\prod_{i\in ID_j}u_i\right), Y\right)$ when $F(ID_j) = 0$ and the same occurrence happens in the active and concurrent proof. $I$ which is able to verify this distribution pattern will stop the impersonation and the game will fail. The ability of performing such DH tuple check to distinguish between valid and simulated conversations in both proofs render the scheme not provable secure, even though no attack has yet been found on the scheme itself.

# 4. Fixing the IBI Scheme

As current trend in cryptography, we would want a scheme that is provable secure especially an efficient one in the standard model. We provide the fix in the next section with the new proofs of security under the same hard problems.

## 4.1. Amending the IBI Scheme

In this section, we propose the fix for Chin et al.'s IBI scheme as follows:

1. **Setup S.** Same as original scheme.
2. **Extract E**. Same as original scheme.
3. **Identification protocol**. **Prover P** and **Verifier V** will do the following:
   a) **P** chooses a random $z \overset{\$}{\leftarrow} Z_q$, computes $X = e\left(\left(u'\prod_{i\in ID_j}u_i\right), R\right)^z, Y = g_2^z$ and sends $X, Y, R$ to **V**.
   b) **V** picks a random challenge $c \overset{\$}{\leftarrow} Z_q$ and sends it to **P**.
   c) **P** calculates $Z = S^{z+c}$ and sends $Z$ as a response to **V**.

**V** accepts if $e(Z, g) = e(Yg_2^c, g_1)\cdot X \cdot e\left(\left(u'\prod_{i\in ID_j}u_i\right)^c, R\right)$. To verify completeness:

$$
\begin{aligned}
e(Z,g) &= e(S^{z+c},g) \\
&= e\left(\left(g_2^a\left(u'\prod_{i\in ID_j}u_i\right)^r\right)^{(z+c)},g\right) \\
&= e\left(\left(g_2^{az+c}\right),g\right)e\left(\left(u'\prod_{i\in ID_j}u_i\right)^{rz}\left(u'\prod_{i\in ID_j}u_i\right)^{rc},g\right) \\
&= e(g_2^z g_2^c, g^a)e\left(\left(u'\prod_{i\in ID_j}u_i\right)^z,g^r\right)e\left(\left(u'\prod_{i\in ID_j}u_i\right)^c,g^r\right) \\
&= e(Yg_2^c,g_1)\cdot X\cdot e\left(\left(u'\prod_{i\in ID_j}u_i\right)^c,R\right)
\end{aligned}
$$

Up to here, the amendment may not be self-evident yet in fixing the flaw mentioned. Recall that the flaw of Chin et al.'s IBI scheme is discovered in the security proof but not the scheme construction itself. In fact, no problem is found in the original construction though the security proof is flawed. We now show how to take advantage of such simple amendment on the construction to overcome the problem in the original security proof. The new detailed security proofs are as follows.

### 4.1.1 Security Against Passive Attack

Most of our proof of security is similar to that of the original. The main difference will be in the way the simulator *M* simulates transcript or identification query when $F(ID_j) = 0$.

**Theorem 3.** *The above IBI scheme is* $(t, q_I, \varepsilon)$*-secure against impersonation under passive attack in the standard model if the CDHP is* $(t, \varepsilon')$*-hard where*

$$t' = t + O(\rho(2n(q_t) + \tau(q_I)), \tag{2}$$

$$\varepsilon \leq \sqrt{4q_e(n+1)\varepsilon'} + q^{-1} \tag{3}$$

*Where* $\rho$ *represents time taken to do a multiplication in* $G$*,* $\tau$ *is the time taken to do an exponentiation in* $G$ *and* $q_e$ *represents the number of extract queries made,* $q_i$ *represents the number of transcript queries made and* $q_I = q_e + q_i$*.*

*Proof.* Suppose there exists an impersonator *I* who $(t, q_I, \varepsilon)$-breaks the IBI scheme. Then we show an algorithm *M* which $(t', \varepsilon')$-breaks the CDH assumption by running *I* as a subroutine. *M* is given a group $G$, a generator $g \in G$ and elements $g^a, g^b$. *M* simulates the challenger for *I* as follows:

1. Setup. *M* sets $l = 2q_e$ and randommly chooses $k \overset{\$}{\leftarrow} Z_n$. Assume that $l(n+1) < q$ for the given values of $q_e$ and $n$. Furthermore, *M* randomly chooses $x' \overset{\$}{\leftarrow} Z_l$, a vector $\langle X \rangle$ of length $n$ with $x_i \overset{\$}{\leftarrow} Z_l$ for all $i$, a randomly selected $y' \overset{\$}{\leftarrow} Z_q$ and a vector $\langle y \rangle$ of length $n$ with $y_i \overset{\$}{\leftarrow} Z_q$ for all $i$. Define the following functions:

$$F(ID) = x' + \sum_{i\in ID} x_i - lk \tag{4}$$

$$J(ID) = y' + \sum_{i\in ID} y_i \tag{5}$$

$M$ now sets $g_1 = g^a$ and $g_2 = g^b$. $M$ also sets $u' = g_2^{x'-lk} g^{y'}$ and a vector $\langle u \rangle$ of length $n$ consisting of $n$ elements $u_i = g_2^{x_i} g^{y_i}$. $M$ passes the system parameters to $I$ as $\langle G, G_T, e, g, g_1, g_2, u', \langle u \rangle, H \rangle$. Note that with functions $F(ID)$ and $J(ID)$, we have:

$$u' \prod_{i \in ID} u_i = g_2^{F(ID)} g^{J(ID)} \tag{6}$$

2. Extract Query. When $I$ queries $M$ for the private key of $ID_i$, $I$ check if $F(ID) = 0 \; mod \; l$ and aborts if it is. This is because given the assumption $l(n+1) < q$ implies $0 \le lk \le q$ and $0 \le x' + \sum_{i \in ID} x_i \le q$. Therefore $F(ID) = 0 \; mod \; q$ implies that $F(ID) = 0 \; mod \; l$ and the simulator aborts because it is unable to construct the private key. Otherwise if $F(ID) \neq 0 \; mod \; l$, $M$ constructs the private key by randomly selecting $r_i \overset{\$}{\leftarrow} Z_q$ and computes the user private key as:

$$\left( \tilde{S}_i = g_1^{-\frac{J(ID_i)}{F(ID_i)}} \left( u' \prod_{i \in ID} u_i \right)^{r_i}, \tilde{R}_i = g_1^{-1/F(ID_i)} g^{r_i} \right)$$

3. Transcript Query. When $I$ queries $M$ for a transcript query $ID_j$, if $F(ID_j) \neq 0 \; mod \; l$ then $M$ just runs the Extract query algorithm to generate a private key to produce a valid transcript for $I$. However, if $F(ID_j) = 0 \; mod \; l$ then $M$ chooses $r_j, c_j, z_j \overset{\$}{\leftarrow} Z_q$ and sends $I$ the transcript as:

$$\widetilde{X_j} = e\left( u' \prod_{i \in ID_j} u_i, R \right)^{z_j}, \widetilde{Y_j} = g^{z_j} g_2^{-c_j}, \widetilde{R_j} = g^{r_j}, \widetilde{Z_j} = g_1^{z_j} \left( u' \prod_{i \in ID_j} u_i \right)^{r_j(z_j + c_j)}$$

$I$ can check that this is a valid transcript since:

$$\begin{aligned}
e(\widetilde{Z_j}, g) &= e\left( g_1^{z_j} (u' \prod_{i \in ID} u_i)^{(z_j + c_j) r_j}, g \right) \\
&= e(g_1^{z_j}, g) e\left( \left( u' \prod_{i \in ID} u_i \right)^{(z_j + c_j)}, g^{r_j} \right) \\
&= e(g^{z_j}, g_1) e\left( \left( u' \prod_{i \in ID} u_i \right)^{z_j} \left( u' \prod_{i \in ID} u_i \right)^{c_j}, g^{r_j} \right) \\
&= e\left( \frac{g_1^{z_j} g_2^{c_j}}{g_2^{c_j}}, g_1 \right) e\left( \left( u' \prod_{i \in ID} u_i \right)^{z_j}, g^{r_j} \right) e\left( \left( u' \prod_{i \in ID} u_i \right)^{c_j}, g^{r_j} \right) \\
&= e(\tilde{Y} g_2^{c_j}, g_1) \cdot \tilde{X} \cdot e\left( \left( u' \prod_{i \in ID} u_i \right)^{c_j}, g^{r_j} \right)
\end{aligned}$$

After some time, $I$ outputs the challenge identity $ID^* \notin \{ID_i\}$ that it wishes to be challenged on. $M$ aborts if $F(ID^*) \neq 0 \; mod \; q$. $I$ can still issue extract and identification queries, except those on $ID^*$. $I$ then takes the role of the cheating prover to try to convince $M$. $M$ obtains $(X, Y, R, c_1, z_1)$ then resets $I$ to where it just sent its commitment to obtain $(X, Y, R, c_2, z_2)$. Based on the reset lemma [12], $M$ can extract $S$ from two conversation transcripts with probability more than $(\varepsilon - q^{-1})^2$. $M$ then calculates $S$ as $S = (Z_1 Z_2^{-1})^{(c_1 - c_2)^{-1}}$ and outputs the solution to the CDHP as:

$$\frac{S}{R^{J(ID^*)}} = \frac{g^{ab}(u'\prod_{i\in ID^*} u_i)^r}{g^{J(ID^*)r}} = g^{ab}$$

The probability of *M* winning the game and solving the CDHP is now calculated. Firstly, the probability that *M* can extract 2 valid trancsripts from *I* is given by $\Pr[M\ computes\ g^{ab}|\neg abort] \geq (\varepsilon - \frac{1}{q})^2$. Upon extraction of $S$, *M* will be able to compute $g^{ab}$. We break down the probability of *M* winning the CDHP to:

$$\begin{aligned}&\Pr[M\ computes\ g^{ab}] = \Pr[M\ computes\ g^{ab} \wedge \neg abort]\\ &= \Pr[M\ computes\ g^{ab}|\neg abort]\ \Pr[\neg abort]\\ &\geq (\varepsilon - q^{-1})^2 \Pr[\neg abort]\end{aligned}$$

It remains to calculate $\Pr[\neg abort]$. Define the following events: 1) Event $A_i$ where *M* answers all queries $F(ID_i) \neq 0\ mod\ l$ and 2) Event $A^*$ where *I* outputs the challenge identity $ID^*$ where $F(ID) = 0\ mod\ q$. Calculate the probability of $A^*$ as:

$$\begin{aligned}&\Pr[A^*] = \Pr[F(ID^*) = 0\ mod\ q\ \vee F(ID^* = 0\ mod\ l\ ]\\ &= \Pr[F(ID^*) = 0\ mod\ l]\ \Pr[F(ID^*) = 0\ mod\ q\ |\ F(ID^*) = 0\ mod\ l]\\ &= \frac{1}{l}\left(\frac{1}{n+1}\right)\end{aligned}$$

Notice that:

$$\begin{aligned}&\Pr[\bigcap_{i=1}^{q_e} A_i|A^*]\\ &= 1 - \Pr[\bigcup_{i=1}^{q_e} A_i|A^*]\\ &= 1 - \sum_{i=1}^{q_e} \Pr[\neg A_i|A^*]\\ &= 1 - \frac{q_e}{l}\end{aligned}$$

since $l = 2q_e$ in the simulation. Finally the probability of *M* breaking CDHP is:

$$\begin{aligned}&\Pr[M\ computes\ g^{ab}] \geq (\varepsilon - q^{-1})^2\ \frac{1}{4q_e(n+1)}\\ &\varepsilon' \geq (\varepsilon - q^{-1})^2\ \frac{1}{4q_e(n+1)}\\ &\varepsilon \leq \sqrt{4q_e(n+1)\varepsilon'} + q^{-1}\end{aligned}$$

as desired.

■

Although the new scheme needs to compute one extra pairing where $X = e\left(\left(u'\prod_{i\in ID_j} u_i\right), R\right)^z$, *I* cannot perform the DH check as in the original proof because $\widetilde{X_j}$ is no longer a point, but an element in $G_T$. Besides, the randomness of $z_j$ will uniformly distributes $\widetilde{X_j}$, making it indistinguishable from the actual value in *I*'s view. The same reasoning is applicable to the proof of active and concurrent attacks

and thus fix the flaw completely.

### 4.1.2 Security Against Active and Concurrent Attacks

**Theorem 4**. *The above IBI scheme is* $(t, q_I, \varepsilon)$*-secure against impersonation under active and concurrent attack in the standard model if the CDHP is* $(t, \varepsilon")$*-hard where*

$$t' = t + O(\rho(2n(q_t) + \tau(q_I)), \tag{7}$$

$$\varepsilon \leq \sqrt{4q_e(n+1)\varepsilon"} + q^{-1} \tag{8}$$

*Where* $\rho$ *represents time taken to do a multiplication in* $G$, $\tau$ *is the time taken to do an exponentiation in* $G$ *and* $q_e$ *represents the number of extract queries made,* $q_i$ *represents the number of transcript queries made and* $q_I = q_e + q_i$.

*Proof*. The proof of the active and concurrent attacks is similar to the one of Theorem 1. Here we only point out the differences. To begin the game, *M* is given elements $(g, g^a)$ as access to the *CHALL* and *CDH* oracles. *M* queries the *CHALL* oracle for $W_0$.

1. Setup. *M* sets $g_1 = g^a$ and queries the *CHALL* oracle for the initial challenge $W_0$, which it sets as $g_2$. The rest are simulated as the proof before.
2. Extract Query. This is similar to the proof before.
3. Identification Query. As before if $F(ID_j) \neq 0 \ mod \ l$, *M* will have no problem simulating an identification protocol instance for *I* by running the Extract algorithm first to obtain the private key for $ID_j$. However, if $F(ID_j) = 0 \ mod \ l$, *M* keeps a counter $m$ and does the following:
   a) *M* queries CHALL for $W_m$ and lets $\tilde{Y}_j = W_m$. *M* also selects $r_j \overset{\$}{\leftarrow} Z_q$ and computes $(\tilde{X}_J = e\left(u' \prod_{i \in ID_j} u_i, \tilde{R}_J\right)^{z_j}, \tilde{Y}_J = W_m, \tilde{R}_J = g_1^{r_j})$. *M* sends sends $\tilde{X}_J, \tilde{Y}_J, \tilde{R}_J$ to *I*.
   b) *I* picks a random challenge $c_j \overset{\$}{\leftarrow} Z_q$ and sends it to *M*.
   c) *M* queries the *CDH* oracle with $[W_m W_0^{c_j}]$ and receives the response $[W_m W_0^{c_j}]^a$. *M* sends the response $\tilde{Z}_J = \left(W_m^a W_0^{ac_j}\right)\left(u' \prod_{i \in ID_j} u_i\right)^{r_j(z_j + c_j)}$ and increments *m* by 1. *I* can check that this is a valid conversation:

$$e(\tilde{Z}_j, g) = e\left(W_m^a W_0^{ac_j}\left(u' \prod_{i \in ID_j} u_i\right)^{r_j(z_j+c_j)}, g\right)$$

$$= e(W_m^a W_0^{ac_j}, g)\, e\left(\left(u' \prod_{i \in ID_j} u_i\right)^{r_j(z_j+c_j)}, g\right)$$

$$= e(W_m W_0^{c_j}, g^a)\, e\left(\left(u' \prod_{i \in ID_j} u_i\right)^{(z_j+c_j)}, g^{r_j}\right)$$

$$= e(W_m W_0^{c_j}, g^a)\, e\left(\left(u' \prod_{i \in ID_j} u_i\right)^{z_j}, g^{r_j}\right) e\left(\left(u' \prod_{i \in ID_j} u_i\right)^{c_j}, g^{r_j}\right)$$

$$= e(\tilde{Y}_j W_0^{c_j}, g_1) \cdot \tilde{X} \cdot e\left(\left(u' \prod_{i \in ID_j} u_i\right)^{c_j}, \tilde{R}\right)$$

After some time, $I$ outputs the challenge identity $ID^* \notin \{ID_i\}$ that it wishes to be challenged on. $M$ aborts if $F(ID^*) \neq 0 \ mod \ q$. $I$ can still issue extract and identification queries, except those on $ID^*$. $I$ then takes the role of the cheating prover to try to convince $M$. $M$ obtains $(X, Y, R, c_1, z_1)$ then resets $I$ to where it just sent its commitment to obtain $(X, Y, R, c_2, z_2)$. Based on the reset lemma [12], $M$ can extract $S$ from two conversation transcripts with probability more than $(\varepsilon - q^{-1})^2$. $M$ then calculates $S$ as $S = (Z_1 Z_2^{-1})^{(c_1 - c_2)^{-1}}$ and outputs the solution to the CDHP as:

$$\frac{S}{R^{J(ID^*)}} = \frac{W_0^a (u' \prod_{i \in ID^*} u_i)^r}{g^{J(ID^*)r}} = W_0^a$$

$M$ then calculates the other $m$ challenge points' solution as:

$$\frac{Z_j}{W_0^{ac_j} (u' \prod_{i \in ID_j} u_i)^{r_j(z_j + c_j)}} = \frac{W_m^a W_0^{ac_j} (u' \prod_{i \in ID_j} u_i)^{r_j(z_j + c_j)}}{W_0^{ac_j} (u' \prod_{i \in ID_j} u_i)^{r_j(z_j + c_j)}} = W_m^a$$

Calculation for the probability of $M$ winning the game and solving the OMCDHP is similar to the proof before, only the CDHP is substituted with the OMCDHP.

■

## 4.2. Efficiency Analysis

The major effect brought by the amendment to the protocol is on the verifier's verification formula and an additional pairing in commitment phase. Even though the new verification $X \cdot e((u' \prod_{i \in ID} u_i)^c, R)$ looks more complicated compared to $e(X(u' \prod_{i \in ID} u_i)^c, R)$ of the original's, the former is actually more efficient as multiplication in $G_T$ is about 7 times faster than point addition in $G$ [13].

On the other hand, we can compute the extra pairing operation incurred by the fix just once instead of every time the identification protocol is activated. This can be done by preparing an intermediate value $X' = e\left(\left(u' \prod_{i \in ID_j} u_i\right), R\right)$ during the Extract phase, so that computing $X = e\left(\left(u' \prod_{i \in ID_j} u_i\right), R\right)^z$ during each interaction can be simplified into $X = X'^z$. With such pre-computation, the amendment can be viewed as replacing the point multiplication $X = (u' \prod_{i \in ID} u_i)^z$ in $G$ from the original commitment phase by exponentiation $X = X'^z$ in $G_T$. This will speed up the identification protocol as the latter is approximately 10 times faster than the former [13]. If the underlying elliptic curve (in prime field) is using parameters of 80 bits security, we only need to increment the size of private key for $|G_T| = 1024$ bits to enjoy the this efficiency.

The only available pre-computation for the original scheme is to pre-compute the hash value for ID during **Extract** phase with an increment of $2 \times |G| = 1024$ bits in the size of private key. Given the same size growth in the private key, the amended scheme obviously outperformed the original's. The complexity comparison for the original and amended identification protocols is summarized in **Table 1**.

**Table 1.** Complexity comparison for identification protocols

| Operation | Identification Protocol | | | |
|---|---|---|---|---|
| | Original | | Amended | |
| | Without Pre-computation | With Pre-computation | Without Pre-computation | With Pre-computation |
| Addition in $Z_q$ | 1 | 1 | 1 | 1 |
| Point Addition | 2*n*+4 | *n*+3 | 2*n*+3 | *n*+2 |
| Point | 5 | 5 | 4 | 4 |

| | | | | |
|---|---|---|---|---|
| Multiplication | | | | |
| Multiplication in $G_T$ | 1 | 1 | 2 | 2 |
| Exponentiation in $G_T$ | 0 | 0 | 1 | 1 |
| Pairing | 3 | 3 | 4 | 3 |

## Conclusion

We showed the flaw in the security proof of Chin et al's IBI scheme and provided a fix for it. The main problem in the original proof is that the impersonator $I$ can perform a DH tuple check on CMT such that $e(X, g_2) = e((u' \prod_{i \in ID} u_i), Y)$, in order to distinguish whether it is in the real game or a simulated one. Our fix revolved around making the point $X$ in $G$ into an element in $G_T$ to avoid the possible check. The efficiency of the scheme is only affected by one extra pairing operation that can be precomputed at the Extract stage for each user, therefore does not incur additional cost to the protocol itself.

## Acknowledgement

The authors would like to thank the anonymous reviewers on an earlier version of this paper, as well as the Fundamental Research Grant Scheme (FRGS/1/11/TK/UTAR/03/9, FRGS/1/10/TK/MMU/03/03) and the Exploratory Research Grant Scheme (ERGS/1/2011/PK/MMU/03/1) for supporting this research.

## References

[1] K. Kurosawa, S.-H. Heng, "From digital signature to id-based identification/signature," *Public Key Cryptography*, Vol. 2947 of Lecture Notes in Computer Science, Springer, pp. 248–261, 2004.
[2] M. Bellare, C. Namprempre, G. Neven, "Security proofs for identity-based identification and signature schemes," *EUROCRYPT*, Vol. 3027 of Lecture Notes in Computer Science, Springer, pp. 268–286, 2004.
[3] A. Shamir, "Identity-based cryptosystems and signature schemes," *CRYPTO*, Vol. 196 of Lecture Notes in Computer Science, Springer, pp. 47–53, 1984.
[4] M. Bellare, P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. of ACM Conference on Computer and Communications Security, ACM*, pp. 62–73, 1993.
[5] R. Canetti, O. Goldreich, S. Halevi, "The random oracle methodology, revised" *Journal of ACM*, vol. 51, no.4, pp.557–594,2004
[6] K. Kurosawa, S.-H. Heng, "Identity-based identification without random oracles," *ICCSA*, Vol. 3481 of Lecture Notes in Computer Science, Springer, pp. 603–613, 2005.
[7] K. Kurosawa, S.-H. Heng, The power of identification schemes," *Public Key Cryptography*, Vol. 3958 of Lecture Notes in Computer Science, Springer, pp. 364–377, 2006.
[8] J.-J. Chin, S.-H. Heng, B.-M. Goi, "An efficient and provable secure identity-based identification scheme in the standard model," *EuroPKI*, Vol. 5057 of Lecture Notes in Computer Science, Springer, pp. 60–73, 2008.
[9] D. Naccache, "Secure and *practical* identity-based encryption," *IACR Cryptology ePrint Archive*, 2005 (2005) 369.
[10] S. Chatterjee, P. Sarkar, "Trading time for space: Towards an efficient ibe scheme with short(er) public parameters in the standard model," *ICISC*, Vol. 3935 of Lecture Notes in Computer Science, Springer, pp. 424–440, 2005.

[11] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme," *Public Key Cryptography*, Vol. 2567 of Lecture Notes in Computer Science, Springer, pp. 31–46, 2003.
[12] M. Bellare, A. Palacio, "GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks," *CRYPTO*, Vol. 2442 of Lecture Notes in Computer Science, Springer, pp. 162–177, 2002.
[13] S.Y. Tan, S.H. Heng, B.M. Goi "Java implementation for pairing-based cryptosystems," *ICCSA*, Vol. Part IV, Springer, pp. 188-198, 2010.

**Syh-Yuan Tan** completed his M.Sc.(I.T.) under Faculty of Science and Technology, Multimedia University (MMU) and is now teaching in the faculty. He is currently a Ph.D student under Faculty of Engineering and Science, Universiti Tunku Abdul Rahman (UTAR), researching in cryptography, particularly the area of provable security. He is also working on the security and implementation issues of bio-crypto authentication protocol.

**Shian-Shyong Tseng** received his Ph.D. degree in Computer Engineering from National Chiao Tung University (NCTU) in 1984. From Aug. 1983 to July 2009, he was on the faculty of the Department of Computer and Information Science at National Chiao Tung University. From Aug. 2009, he is with Asia University as a Chair Professor in the Department of Applied Informatics and Multimedia, and is currently a Vice President there. From 1988 to 1991, he was the Director of the Computer Center at NCTU. From 1991 to 1992 and 1996 to 1998, he acted as the Chairman of Department of Computer and Information Science at NCTU. From 1992 to 1996, he was the Director of the Computer Center at the Ministry of Education and the Chairman of Taiwan Academic Network (TANet) Management Committee. In December 1999, he founded Taiwan Network Information Center (TWNIC) and was the Chairman of the board of directors of TWNIC from 2000 to 2005, and from 2009 till now. He was the recipient of the Excellent Achievement Award for Computer Technology made by the Ministry of Transportation and Communications, Taiwan in 2010. His current research interests include data mining, expert systems, computer algorithms and Internet-based applications.

**Swee-Huay Heng** received her Doctor of Engineering degree from the Tokyo Institute of Technology, Japan. She is currently a Professor in Multimedia University, Malaysia. Her research interests include Cryptography and Information Security. She was the Programme Chair of ProvSec 2010 and CANS 2010. She has been actively involved in technical Programme Committees of several international security conferences.

**Bok-Min Goi** received his B.Eng degree from University of Malaya (UM) in 1998, and the M.Eng.Sc and Ph.D degrees from Multimedia University (MMU), Malaysia in 2002 and 2006, respectively. He is now the Deputy Dean (Academic Development & Undergraduate Programmes) and a professor in the Faculty of Engineering and Science, Universiti Tunku Abdul Rahman (UTAR), Malaysia. Prof. Goi is the Chairperson for Centre for Healthcare Science & Technology, UTAR. He was also the General Chair for ProvSec 2010 and CANS 2010, and the PC members for many crypto / security conferences. His research interests include cryptology, security protocols, information security, digital watermarking, computer networking and embedded systems design.