# An Efficient and Provably Secure Certificateless Identification Scheme

Ji-Jian Chin[1], Raphael C.-W. Phan[1], Rouzbeh Behnia [2] and Swee-Huay Heng[2]
[1]*Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Selangor, Malaysia*
[2]*Faculty of Information Science & Technology, Multimedia University, 75450 Melaka, Malaysia.*
{*jjchin, raphael, rouzbeh.behnia, shheng*}*@mmu.edu.my*

Keywords: Certificateless, identity based, identification, provable security, without escrow

Abstract: Identity-based identification, first formalized independently by Bellare et al. and Kurosawa and Heng in 2004, still had the inherent key escrow problem, as the TA generating the user secret keys had full access to every user's secret key. In 2003, Al-Riyami and Paterson introduced the notion of certificateless cryptography, and subsequently many certificateless encryption, signature and other schemes were introduced in literature. However, to this date there are still no certificateless identification schemes in existence. Therefore, in this paper, we formalize the notion of certificateless identification schemes and construct the first concrete certificateless identification scheme.

## 1 INTRODUCTION

In public key cryptography, users had to bind their public keys to their entities using a certificate obtained from a Certificate Authority. This led to the certificate management problem. In 1984, (Shamir, 1984) proposed the notion of identity-based cryptography to deal away with the certificate management problem. The idea was to use an identity string to generate the user's public/private key pairs, and with implicit certification, deal away with certificates. However, there was still the inherent problem of key escrow, as the Trusted Authority (TA) who created the public/private key pairs had access to every user's private keys.

(Al-Riyami and Paterson, 2003) proposed the notion of certificateless cryptography. In certificateless cryptography, a trusted third party called the Key Generation Center (KGC) would only generate a partial private key for each user, who will then complete the public/private key pair with a secret value of its own selection. (Al-Riyami and Paterson, 2003) also proposed the first certificateless encryption scheme and certificateless signature scheme in the same paper. Since then, many certificateless schemes have appeared in literature. However, to the best of our knowledge, there has not been any certificateless identification schemes in existence to date.

An identification scheme allows a prover to verify himself to a verifier in order to gain access to some resources. Traditional identification schemes required the use of certificates which led to certificate management issues as mentioned above. To remove the need for certificates, identity-based identification schemes were first proposed and rigorously defined by (Bellare et al., 2004) and (Kurosawa and Heng, 2004) independently in 2004. Since then, while there has been advancement in the area of identity-based identification schemes, certificateless identification schemes have yet to be explored.

### 1.1 Motivations

Our motivations from exploring certificateless identification stem from the fact that while there are many certificateless encryption and signature schemes in literature, there is no certificateless identification primitive existing as yet. In our opinion, identification is an important primitive because it allows for access control in the distribution of resources, while at the same time serves as a base primitive for signature schemes to be built by using the Fiat-Shamir transform (Fiat and Shamir, 1986). A similar transformation relationship may be definable with regards to certificateless signatures and certificateless identification, but that remains a topic of further study due to the complexity of definition for adversarial capabilities, specifically with regards to the public key replacement power of an adversary and its effects on the signature and identification oracles in question.

The main motivation remains that while research in certificateless signatures has thrived, certificateless identification remains untouched. Without the notion

of certificateless identification schemes, identification schemes currently suffer from the high cost of certifying public keys with regards to traditional public key identification schemes, or key escrow in the area of identity-based identification schemes where the TA learns every user's private keys. This represents a serious shortcoming in the advancement of research and development for identification schemes.

Certificateless identification schemes can be implemented in areas that require access control facilitation for users, where it is desirable that the KGC does not have full access to users' private keys. This may range anywhere from using smart cards to open doors to using mobile devices to authenticate a user to a service provider. Although these are achievable using traditional public key identification or identity-based identification, the added security is desirable so that the scheme is protected against insider attacks, such as the case of a staff of the service provider who wishes to impersonate a user.

## 1.2 Related Work

We mention the related sections of certificateless cryptography as well as identity-based identification schemes, since certificateless identification schemes are actually an expansion of identity-based identification schemes into the area of certificateless cryptography to remove key escrow from the identification primitive, as well as the need for certificates.

(Al-Riyami and Paterson, 2003) first proposed the notion of certificateless encryption and signatures in their seminal work. Subsequently much work has been done in proposing and refining the adversarial model in the area of encryption and signatures. We highlight only some of the latest (due to page constraints) certificateless signature schemes, models and cryptanalysis as related work. For further information on certificateless encryption schemes, one can refer to a comprehensive survey done by Dent in (Dent, 2008).

With the discovery of a Type-1 attack on the initial certificateless signature scheme by (Al-Riyami and Paterson, 2003) along with a corresponding fix by (Huang et al., 2005), thus began a long line of work of proposing certificateless signature schemes such as work by (He et al., 2012; Tso et al., 2011; Tso et al., 2012; Zhang and Mao, 2012), refining the security models of certificateless signatures such as proposals by (Huang et al., 2012; Hu et al., 2007; Huang et al., 2007) as well as cryptanalysis of the proposed schemes (Zhang et al., 2010; Fan et al., 2009; Chen et al., 2013; Wu et al., 2013; Tian and Huang, 2012). One can see the area of study is still quite open to debate with regards with how much power an adversary towards a certificateless signature scheme should be allowed. However, it is our opinion that the adversaries defined by (Huang et al., 2012) is sufficiently suited and comprehensive enough to encapsulate the definition of adversaries for certificateless identification schemes.

In the area of identity-based identification, the initial rigorous definitions were first proposed independently by (Kurosawa and Heng, 2004) and (Bellare et al., 2004). Subsequently, (Kurosawa and Heng, 2005) also proposed the first identity-based identification scheme in the standard model. (Yang et al., 2007) proposed a generic framework to construct identity-based identification schemes from one-more trapdoor functions. Subsequent advancements include the proposal of hierarchical identity-based identification schemes by (Chin et al., 2009) as well as reset-secure identity-based identification schemes by (Thorncharoensri et al., 2009). However, all these schemes still face the issue of key escrow since the TA who generates the keys has access to every user's private key.

Expanding on the idea of identity-based identification without key escrow, we propose the notion of certificateless identification in this work.

## 1.3 Contributions

We present two main contributions in this paper. The first contribution is the rigorous definition of the security definitions for certificateless identification schemes. We base our definitions of certificateless identification schemes on the key generation algorithms from certificateless signature schemes, while expanding the definition to cover user public key input on the identification protocol algorithms of an identity-based identification scheme. Our definition on the adversarial capabilities and strengths are analogous to the definitions given by (Huang et al., 2012), but adapted to the identification setting where the adversary's main goal is impersonation instead of forgery. This is non-trivial since simulating a conversation of an identification protocol is largely different from simulating a signing oracle, therefore, certificateless signatures and certificateless identification do have major differences in terms of the security games their respective adversaries play.

We then proceed to construct the first certificateless identification scheme, complete with security analysis against all four adversaries which we will define in Section 2. Our scheme is fast and efficient based on the efficiency analysis provided in Section 6, as well as protected against public key replacement at-

tacks from Type 1 adversaries. This will be explained further in the security definitions.

Lastly, our scheme also uses only one component for the user's full private key. This is different than the conventional two component full private keys generated by key generation algorithms from the works cited above, where one component is generated by the KGC while the other is generated by the user. Our approach translates to a smaller storage requirement for users, especially if the scheme is implemented on smart cards or other mobile devices with smaller storage capacities.

### 1.4 Layout

The rest of the paper is divided as follows: we begin with some preliminaries in Section 2 and proceed to provide the security definitions in Section 3. We continue on with the construction of the first concrete certificateless identification scheme in Section 4. We provide the security analysis in Section 5 and an efficiency analysis in Section 6. Finally we conclude in Section 7.

## 2 PRELIMINARIES

In this section, we review the main components required for building our certificateless identification scheme.

### 2.1 Bilinear Pairings

Let $G_1$ and $G_2$ be two cyclic multiplicative groups of prime order $q$ where the discrete logarithm problems are intractable. Then $e : G_1 \times G_1 \to G_2$ is an admissible bilinear map if it satisfies the properties of:

1. Bilinearity: $e(g^a, g^b) = e(g,g)^{ab}$ for all $g \in G_1$ and $a, b \in \mathbb{Z}_q^*$
2. Non-degeneracy: There exists $g \in G_1$ such that $e(g,g) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e$.

### 2.2 Problems and Assumptions

We build the security of our certificateless identification scheme based on the following intractable mathematical problems:

1. **Computational Diffie-Hellman problem (CDHP)**: Given $g, g^a, g^b$ for some $a, b \in \mathbb{Z}_q^*$, compute $g^{ab}$.
2. **One-More Computational Diffie-Hellman problem (OMCDHP)**: This is an interactive variant of the CDHP first proposed by (Boldyreva, 2003). This problem is modeled by a game played by an adversary who is given $\langle 1^k, G_1, G_2, g, g^a \rangle$ 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 the target points $W_0, \ldots, W_n$ while using strictly less queries to the *CDH* oracle. In other words, the adversary is required to find $W_0^a, \ldots, W_n^a$ while using the *CDH* oracle only $i \leq n$ times.

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

### 2.3 The Knowledge of Exponent Assumption (Damgård, 1991)

We use the knowledge of exponent assumption, first proposed in (Damgård, 1991) and further elaborated in (Bellare and Palacio, 2004) in our proof of security for our certificateless identification scheme to defend against public key replacement attacks. Let $k = \log |\langle g \rangle|$ be the security parameter of a prime order group where $g$ is a generator. For any probabilistic polynomial time algorithm $A$ that takes as input $g$ and $g^a$, where $a$ is chosen from $[0, |\langle g \rangle| - 1]$ uniformly at random, and which produces as output a pair of the form $(x, y), x \in \langle g \rangle$, there exists a probabilistic polynomial time extractor $E$, which takes in the same input and outputs the pair $(x, y)$ along with an exponent $r$ such that for sufficiently large $k$,

$$\Pr[y = x^a \text{and} g^r \neq x] \leq \frac{1}{Q^k}$$

for any polynomial $Q$.

## 3 Certificateless Identification (CLI) Schemes

A CLI scheme consists of six polynomial time algorithms:

- **Setup** is run by the KGC. It takes in the security parameter $1^k$ as input and returns the system parameters params and the master secret key MSK.
- **Set-User-Key** is run by the user before registering himself to the KGC. It takes in the security

parameter $1^k$ and the user's identity ID as input, generates the secret value for a user $\mathsf{SV}_{\mathsf{ID}}$ along with the corresponding user's public key $\mathsf{UPK}_{\mathsf{ID}}$.

- **Partial-Private-Key-Extract** is run by the KGC upon the user's request for a partial private key. It takes in params, MSK, the user's public key $\mathsf{UPK}_{\mathsf{ID}}$ and the user's identity ID, returns the partial private key $\mathsf{PPK}_{\mathsf{ID}}$ for the user. Note that the user's public key is bound to his partial private key, allowing us to elevate the trust level to level 3 according to the hierarchy described in (Girault, 1991).
- **Set-Private-Key** takes in the user's partial private key $\mathsf{PPK}_{\mathsf{ID}}$, public key $\mathsf{UPK}_{\mathsf{ID}}$ and secret value $\mathsf{SV}_{\mathsf{ID}}$ and sets the user private key as $\mathsf{USK}_{\mathsf{ID}}$.
- **Identification-Protocol** is the interactive protocol run by the 2 algorithms **Prover** and **Verifier**. They perform the three-step canonical honest verifier zero knowledge proof of knowledge protocol with the following steps:
  1. **Prover** sends the COMMITMENT to the **Verifier**.
  2. **Verifier** sends the CHALLENGE to the **Prover**.
  3. **Prover** sends the RESPONSE to the **Verifier**, which the **Verifier** will choose to either accept or reject.

**Setup** and **Partial-Private-Key-Extract** are performed by the Key Generation Center (KGC) whilst **Set-User-Key** and **Set-Private-Key** are done by the user.

We consider four types of adversaries for the certificateless identification scheme: 1) **IMP-PA-1**: the Type-1 passive impersonator, 2) **IMP-AA/CA-1**: the Type-1 active and concurrent impersonator, 3) **IMP-PA-2**: the Type-2 passive impersonator, 4) **IMP-AA/CA-2**: the Type-2 active and concurrent impersonator.

The capability between passive and active impersonator differs in that the passive impersonator can only eavesdrop on conversations between honest parties, while the active impersonator can act as a cheating verifier to gain knowledge from honest provers through interacting with them. The concurrent impersonator is a special case of an active impersonator who can run several instances of the protocol at the same time.

Type-1 impersonators model malicious third party impersonators against the CLI scheme who do not have access to the master secret key, but is able to request and replace public keys with values of his own selection. On the other hand, the Type-2 impersonator models the malicious KGC who can generate partial private keys of users.

Based on certificateless signature schemes according to the definitions by (Huang et al., 2007) and subsequently extended in the full version of their paper in (Huang et al., 2012), adversarial classifications can be further broken down into the Normal-Type, Strong-Type and Super-Type adversary for Type 1 and Type 2 categories, differing in their strengths.

- Normal-Type adversaries cannot use a prover to converse with a verifier once its public key is replaced.
- Strong-Type adversaries can continue using a prover which public key has been replaced, provided they supply the secret value corresponding to the replaced public key for the conversation.
- Super-Type adversaries can replace a prover's public key and still use it to correspond with a verifier without the new secret value.

Our concrete scheme manages to achieve the level of security against Super-Type-1 and Super-Type-2 adversaries for impersonation under passive attacks, and security against Strong-Type-1 and Strong-Type-2 adversaries for impersonation under active and concurrent attacks, according to the above definitions.

We describe the security model of CLI schemes against Type-1 and Type-2 impersonators as the following games, and highlight the differences in capabilities when making identification queries within the game for both passive and active and concurrent impersonators.

**Game I**. The game is played between a challenger $C$ and the Type-1 Impersonator $I_1$ for the CLI scheme $\Pi$ as follows:

- **Setup**: $C$ runs **Setup** and passes the system parameters params to $I_1$. It keeps the master secret key MSK to itself.
- **Phase 1**: In this training phase, $I_1$ will be allowed to make the following queries adaptively to $C$.
  - **ExtrFullSK**(ID).On request for the full private key USK on user ID, $C$ will run **Set-User-Key**, **Partial-Private-Key-Extract** and **Set-Private-Key** algorithms to generate the complete user's private key and passes it to $I_1$.
  - **ExtrPartSK**(ID). On request for the partial private key PPK on user ID, $C$ will run **Partial-Private-Key-Extract** and returns the user's partial private key to $I_1$.
  - **RequestPK**(ID). On request for the public key UPK on user ID, $C$ will run **Set-User-Key** to generate the user's public key and passes it to $I_1$.
  - **ReplacePK**(ID,$\mathsf{UPK}_{\mathsf{ID}}$). $I_1$ is able to replace the user ID's public key $\mathsf{UPK}_{\mathsf{ID}}$ with the public key

UPK'$_{\mathsf{ID}}$ chosen by him. Note that the corresponding secret value is not required for public key replacement queries.

– **Identification**(ID). For passive $I_1$, $C$ will generate a valid transcript on a conversation between user ID and itself as the verifier and returns the transcript to $I_1$. For active and concurrent $I_1$, $C$ will play the role of the prover to interact with $I_1$ as the cheating verifier. Further breakdown of identification query responses by $C$ will depend on which level of Type-1 adversary it is dealing with.
  1. Normal-Type-1 adversaries cannot make identification queries if their public keys have been replaced.
  2. Strong-Type-1 adversaries require an additional input of the user secret value $SV$ if the public key has been replaced. If $SV = \perp$ then the public key must be the original one. Otherwise $C$ will use $SV$ to correspond to the replaced public key in the conversation.
  3. Super-Type-1 adversaries can make identification queries without user secret values even for those who have replaced public keys. $SV$ is not required to generate valid responses.

- **Phase 2**. $I_1$ will eventually output $ID^*$ on which it wants to be challenged on. $I_1$ will now play the role of the cheating prover while $C$ assumes the role of the verifier. $I_1$ wins the game if it manages to convince $C$ to accept.

We say an CLI scheme $\Pi$ is $(t, q_I, \varepsilon)$ -secure under passive or active and concurrent attacks if for any passive or active and concurrent Type-1 impersonator $I_1$ who runs in time $t$, $\Pr[I_1 \text{can impersonate}] < \varepsilon$, where $I_1$ can make at most $q_I$ extract queries on partial or full private keys.

**Game II**. The game is played between a challenger $C$ and the Type-2 Impersonator $I_2$ for the CLI scheme $\Pi$ as follows:

- **Setup**: $C$ runs **Setup** and passes both the system parameters params and the master secret key MSK to $I_2$.
- **Phase 1**: In this training phase, $I_2$ will be allowed to make the following queries adaptively to $C$.
  – **ExtrFullSK**(ID). On request for the full private key USK on user ID, $C$ will run **Set-User-Key**, **Partial-Private-Key-Extract**, **Set-Private-Key** algorithms to generate the complete user's private key and passes it to $I_2$.
  – **RequestPK**(ID). On request for the public key UPK on user ID, $C$ will run **Set-User-Key** to generate the user's public key and passes it to $I_2$.
  – **ReplacePK**(ID,UPK'). $I_2$ is able to replace the user ID's public key UPK with the public key UPK' chosen by him. Once again, the corresponding secret value is not required for public key replacement queries. The only exception is the target ID, $ID^*$, otherwise it will be trivial to win the game.
  – **Identification**(ID). For passive $I_2$, $C$ will generate a valid transcript on between user ID and itself as the verifier and returns the transcript to $I_2$. For active and concurrent $I_2$, $C$ will play the role of the prover to interact with $I_2$ as the cheating verifier. Further breakdown of identification query responses by $C$ will depend on which level of Type-2 adversary it is dealing with.
    1. Normal-Type-2 adversaries cannot make identification queries if their public keys have been replaced.
    2. Strong-Type-2 adversaries require an additional input of the user secret value $SV$ if the public key has been replaced. If $SV = \perp$ then the public key must be the original one. Otherwise $C$ will use $SV$ to correspond to the replaced public key in the conversation. If the identification query is on the challenge identity and $SV \neq \perp$, the **Identification** oracle will just generate a valid response for $I_2$ on the challenge identity using the original public key, since $I_2$ is not allowed to replace the public key for the challenge identity, therefore $SV$ should be discarded.
    3. Super-Type-2 adversaries can make identification queries without user secret values even for those who have replaced public keys. $SV$ is not required to generate valid responses. It will not be possible to query the challenge identity with a replaced public key since $I_2$ is not allowed to run **ReplacePK** on the challenge identity.
- **Phase 2**. $I_2$ will eventually output $ID^*$ on which it wants to be challenged on. $I_2$ will now play the role of the cheating prover while $C$ assumes the role of the verifier. $I_2$ wins the game if it manages to convince $C$ to accept.

Note that $I_2$ does not need to perform **ExtrPartSK** queries as it already has knowledge of the master secret key and can generate partial private keys itself. $I_2$ is also not allowed to replace the public key of the challenge identity, but is able to do so for any other user.

We say an CLI scheme is $(t, q_I, \varepsilon)$ -secure under passive or active and concurrent attacks if for any passive or active and concurrent Type-2 impersonator $I_2$

who runs in time $t$, Pr[$I_2$can impersonate] $< \varepsilon$, where $I_2$ can make at most $q_I$ extract queries on full private keys.

# 4 Construction

Define $(G_1, G_2)$ to be multiplicative cyclic groups of prime $q$ and let $e$ be an admissible bilinear map. Our construction is a certificateless identification scheme given by the following algorithms.

1. **Setup**$(1^k)$: run by the KGC, taking in the security parameter $1^k$. It chooses $s \xleftarrow{\$} \mathbb{Z}_q$, a generator $g \xleftarrow{\$} G_1$ and sets $g_1 = g^s$. Setup also chooses $H : \{0,1\}^* \to G_1$. Setup publishes the system parameters $\mathsf{params} = \langle e, G_1, G_2, q, g, g_1, H \rangle$ and keeps the master secret key $\mathsf{MSK} = s$ secret.
2. **Set User Key**$(1^k)$: run by the user, taking in the security parameter $1^k$. It chooses and sets the user secret value as $\mathsf{SV}_{ID} = x_{ID} \xleftarrow{\$} \mathbb{Z}_q$, calculates $X_{1,ID} = g^{x_{ID}}, X_{2,ID} = g_1^{x_{ID}}$ and sets the user public keys as $\mathsf{UPK}_{ID} = \langle X_{1,ID}, X_{2,ID} \rangle$.
3. **Partial Private Key Extract**(params,MSK,ID,$\mathsf{UPK}_{ID}$): run by the KGC whenever a user registers with the system, taking in $\mathsf{params}, \mathsf{MSK} = s$, $\mathsf{UPK}_{ID}$ and ID, as input. It calculates $Q_{ID} = H(\mathsf{ID}, X_{1,ID}, X_{2,ID})$ and sets $D_{ID} = Q_{ID}^s$. It outputs the partial private key $\mathsf{PPK}_{ID} = D_{ID}$.
4. **Set Private Key**$(\mathsf{params}, ID, \mathsf{SV}_{ID}, \mathsf{UPK}_{ID}, \mathsf{PPK}_{ID})$: run by the user, taking in $\mathsf{SV}_{ID} = x_{ID}, \mathsf{UPK}_{ID} = \langle X_{1,ID}, X_{2,ID} \rangle$ and partial private key $\mathsf{PPK}_{ID} = D_{ID}$ as input. User first checks whether $e(g, D_{ID}) = e(g_1, Q_{ID})$ where $Q_{ID} = H(ID, X_{1,ID}, X_{2,ID})$. It then sets the user secret key as $S_{ID} = (D_{ID} Q_{ID})^x = Q_{ID}^{sx+x}$. It outputs the user private key $\mathsf{USK} = S_{ID}$ which is kept secret by the user.
5. **Identification Protocol** is run by the **Prover** and **Verifier** as such:
   (a) **prover** chooses $r \xleftarrow{\$} \mathbb{Z}_q$ and sets $U = Q_{ID}^r = H(ID, X_{1,ID}, X_{2,ID})^r$ and sends $U$ to **verifier**.
   (b) **verifier** chooses a random challenge $c \xleftarrow{\$} \mathbb{Z}_q$ and sends it to **prover**.
   (c) **prover** sends its response as $V = S_{ID}^{r+c}$ to **verifier**.

   **verifier** accepts if and only if $e(g_1, X_{1,ID}) = e(X_{2,ID}, g)$ and $e(g, V_{ID}) = e(X_{2,ID} X_{1,ID}, U Q_{ID}^c)$.

To check for completeness:

$$\begin{aligned} e(g_1, X_{1,ID}) &= e(g^s, g^x) && (1)\\ &= e(g^{sx}, g) && (2)\\ &= e(X_{2,ID}, g) && (3) \end{aligned}$$

and

$$\begin{aligned} e(g, V) &= e(g, S_{ID}^{r+c}) && (4)\\ &= e(g, Q_{ID}^{(s+x)(r+c)}) && (5)\\ &= e(g^{(s+x)}, Q_{ID}^r Q_{ID}^c) && (6)\\ &= e(X_{2,ID} X_{1,ID}, U Q_{ID}^c) && (7) \end{aligned}$$

# 5 SECURITY ANALYSIS

We provide security analysis of our scheme against both Type-1 and Type-2 adversaries in this section. However, due to page constraints, we had to remove our proofs for Theorems 1,2,3 and 4 from this paper. This will be included in the full version.

## 5.1 Type-1 Impersonation under Passive Attack

**Theorem 1.** *The certificateless identification scheme is $(t, q_I, \varepsilon)$-secure against impersonation under passive attacks against Super-Type-1 Impersonators in the random oracle if the Computational Diffie-Hellman Problem is $(t, \varepsilon)$-hard where*

$$\varepsilon \leq \sqrt{\varepsilon' e(q_I + 1)} + \frac{1}{q} \quad (8)$$

## 5.2 Type-1 Impersonation under Active and Concurrent Attack

**Theorem 2.** *The certificateless identification scheme is $(t, q_I, \varepsilon)$-secure against impersonation under active and concurrent attacks against Strong-Type-1 Impersonators in the random oracle if the One-More Computational Diffie-Hellman Problem is $(t, q_H, \varepsilon'')$-hard.*

$$\varepsilon \leq \sqrt{\varepsilon'' e(q_I + 1)} + \frac{1}{q} \quad (9)$$

## 5.3 Type-2 Impersonation under Passive Attack

**Theorem 3.** *The certificateless identification scheme is $(t, q_I, \varepsilon)$-secure against impersonation under passive attacks against Super-Type-2 Impersonators in the random oracle if the Computational Diffie-Hellman Problem is $(t, \varepsilon)$-hard where*

$$\varepsilon \leq \sqrt{\varepsilon' e(q_I + 1)} + \frac{1}{q} \quad (10)$$

### 5.4 Type-2 Impersonation under Active and Concurrent Attack

**Theorem 4.** *The certificateless identification scheme is $(t, q_I, \varepsilon)$-secure against impersonation under active and concurrent attacks against* Strong-Type-2 *Impersonators in the random oracle if the One-More Computational Diffie-Hellman Problem is $(t, q_H, \varepsilon'')$-hard.*

$$\varepsilon \leq \sqrt{\varepsilon'' e(q_I + 1)} + \frac{1}{q} \tag{11}$$

## 6 EFFICIENCY ANALYSIS

We omit addition operations in $\mathbb{Z}_q^*$ because it is negligible compared to other group operations in $G_1$. By letting M:Multiplication, E:Exponentiation, P:Pairing, our scheme requires the following group operational costs:

Table 1: Operation costs for our CLI scheme.

| **Algorithm** | M | E | P |
|---|---|---|---|
| **Setup** | 0 | 1 | 0 |
| **Partial-Private-Key-Extract** | 0 | 1 | 0 |
| **Set-User-Key** | 0 | 1 | 0 |
| **Set-Private-Key** | 1 | 1 | 0 |
| **Prover** | 0 | 2 | 0 |
| **Verifier** | 2 | 1 | 4 |

Our scheme is very efficient as our **Prover** and **Verifer** algorithms require only one group multiplication and three group exponentiations in $G_1$ and two pairing operations to $G_2$ per round of interaction.

## 7 Conclusion

We proposed the first security model for certificateless identification and provided the first concrete proof for a certificateless identification scheme. The scheme is provable secure against both Type-1 and Type-2 impersonators, both passive and active and concurrent alike using the CDH assumption and the OMCDH assumption respectively. It is secure against Super-Type-1 and Super-Type-2 adversaries with regard to passive adversaries while secure against Strong-Type-1 and Strong-Type-2 adversaries with regard to active and concurrent security.

## ACKNOWLEDGEMENTS

We wish to thank the Malaysian Ministry of Higher Education for their financial support for this research through the Fundamental Research Grant Scheme and Exploratory Research Grant Scheme.

## REFERENCES

Al-Riyami, S. S. and Paterson, K. G. (2003). Certificateless Public Key Cryptography. In Laih, C.-S., editor, *ASIACRYPT*, volume 2894 of *Lecture Notes in Computer Science*, pages 452–473. Springer.

Bellare, M., Namprempre, C., and Neven, G. (2004). Security Proofs for Identity-Based Identification and Signature Schemes. In Cachin, C. and Camenisch, J., editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 268–286. Springer.

Bellare, M. and Palacio, A. (2004). The Knowledge-of-Exponent Assumptions and 3-round Zero-Knowledge Protocols. In Franklin, M. K., editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 273–289. Springer.

Boldyreva, A. (2003). Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In Desmedt, Y., editor, *Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 31–46. Springer.

Chen, Y.-C., Tso, R., and Horng, G. (2013). Cryptanalysis of a Provably Secure Certificateless Short Signature Scheme. In *Advances in Intelligent Systems and Applications-Volume 2*, pages 61–68. Springer.

Chin, J.-J., Heng, S.-H., and Goi, B.-M. (2009). Hierarchical Identity-Based Identification Schemes. In Slezak, D., Kim, T.-H., Fang, W.-C., and Arnett, K. P., editors, *FGIT-SecTech*, volume 58 of *Communications in Computer and Information Science*, pages 93–99. Springer.

Damgård, I. (1991). Towards Practical Public Key Systems Secure Against Chosen Ciphertext Attacks. In Feigenbaum, J., editor, *CRYPTO*, volume 576 of *Lecture Notes in Computer Science*, pages 445–456. Springer.

Dent, A. W. (2008). A Survey of Certificateless Encryption Schemes and Security Models. *Int. J. Inf. Sec.*, 7(5):349–377.

Fan, C., Hsu, R.-H., and Ho, P.-H. (2009). Cryptanalysis on Du-Wen Certificateless Short Signature Scheme. *Proceedings of JWIS09. Available at http://jwis2009. nsysu. edu. tw/location/paper/Cryptanalysis*.

Fiat, A. and Shamir, A. (1986). How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In Odlyzko, A. M., editor, *CRYPTO*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer.

Girault, M. (1991). Self-Certified Public Keys. In Davies, D. W., editor, *EUROCRYPT*, volume 547 of *Lecture Notes in Computer Science*, pages 490–497. Springer.

He, D., Chen, J., and Zhang, R. (2012). An Efficient and Provably-Secure Certificateless Signature Scheme without Bilinear Pairings. *International Journal of Communication Systems*, 25(11):1432–1442.

Hu, B. C., Wong, D. S., Zhang, Z., and Deng, X. (2007). Certificateless Signature: A New Security Model and an improved Generic Construction. *Des. Codes Cryptography*, 42(2):109–126.

Huang, X., Mu, Y., Susilo, W., Wong, D. S., and Wu, W. (2007). Certificateless Signatures Revisited. In Pieprzyk, J., Ghodosi, H., and Dawson, E., editors, *ACISP*, volume 4586 of *Lecture Notes in Computer Science*, pages 308–322. Springer.

Huang, X., Mu, Y., Susilo, W., Wong, D. S., and Wu, W. (2012). Certificateless Signatures: New Schemes and Security Models. *Comput. J.*, 55(4):457–474.

Huang, X., Susilo, W., Mu, Y., and Zhang, F. (2005). On the Security of Certificateless Signature Schemes from Asiacrypt 2003. In Desmedt, Y., Wang, H., Mu, Y., and Li, Y., editors, *CANS*, volume 3810 of *Lecture Notes in Computer Science*, pages 13–25. Springer.

Kurosawa, K. and Heng, S.-H. (2004). From Digital Signature to ID-based Identification/Signature. In Bao, F., Deng, R. H., and Zhou, J., editors, *Public Key Cryptography*, volume 2947 of *Lecture Notes in Computer Science*, pages 248–261. Springer.

Kurosawa, K. and Heng, S.-H. (2005). Identity-Based Identification Without Random Oracles. In Gervasi, O., Gavrilova, M. L., Kumar, V., Laganà, A., Lee, H. P., Mun, Y., Taniar, D., and Tan, C. J. K., editors, *ICCSA (2)*, volume 3481 of *Lecture Notes in Computer Science*, pages 603–613. Springer.

Shamir, A. (1984). Identity-Based Cryptosystems and Signature Schemes. In Blakley, G. R. and Chaum, D., editors, *CRYPTO*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer.

Thorncharoensri, P., Susilo, W., and Mu, Y. (2009). Identity-based Identification Scheme Secure against Concurrent-Reset Attacks without Random Oracles. In Youm, H. Y. and Yung, M., editors, *WISA*, volume 5932 of *Lecture Notes in Computer Science*, pages 94–108. Springer.

Tian, M. and Huang, L. (2012). Cryptanalysis of a Certificateless Signature Scheme without Pairings. *International Journal of Communication Systems*, pages n/a–n/a.

Tso, R., Huang, X., and Susilo, W. (2012). Strongly Secure Certificateless Short Signatures. *Journal of Systems and Software*, 85(6):1409–1417.

Tso, R., Yi, X., and Huang, X. (2011). Efficient and Short Certificateless Signatures Secure Against Realistic Adversaries. *The Journal of Supercomputing*, 55(2):173–191.

Wu, C., Lin, W., Huang, H., and Chen, Z. (2013). Cryptanalysis of Some Certificateless Signature Schemes in the Standard Model. *International Journal of Applied Mathematics and Statistics*, 36(6):16–25.

Yang, G., Chen, J., Wong, D. S., Deng, X., and Wang, D. (2007). A More Natural Way to Construct Identity-Based Identification schemes. In Katz, J. and Yung, M., editors, *ACNS*, volume 4521 of *Lecture Notes in Computer Science*, pages 307–322. Springer.

Zhang, F., Li, S., Miao, S., Mu, Y., Susilo, W., and Huang, X. (2010). Cryptanalysis on Two Certificateless Signature Schemes. *International Journal of Computers Communications & Control*, 5(4):586–591.

Zhang, J. and Mao, J. (2012). An Efficient RSA-Based Certificateless Signature Scheme. *Journal of Systems and Software*, 85(3):638–642.