IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 11, 2020, accepted February 24, 2020, date of publication March 27, 2020, date of current version April 13, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2983750

An Identity Based-Identification Scheme With Tight Security Against Active and Concurrent Adversaries

JASON CHIA, (Student Member, IEEE), AND JI-JIAN CHIN
Faculty of Engineering, Multimedia University, Cyberjaya 63100, Malaysia

Corresponding author: Jason Chia (chia_jason96@live.com)

This work was supported in part by the Ministry of Education of Malaysia through the Fundamental Research Grant Scheme under Grant FRGS/1/2019/ICT04/MMU/02/5, and in part by the Multimedia University's Research Management Fund.

ABSTRACT Identification schemes are used by machines to securely authenticate the identity of other machines or their users over computer networks. As conventional public key schemes require a trusted third party (TTP) or a public file to ensure the corresponding public key matches with the identity, identity-based cryptosystems emerged as a form of certificate-free system. The entity's identity is the public key itself, therefore eliminating the need for a TTP. The identity-based identification (IBI) scheme introduced by Kurosawa and Heng using their transform in 2004 remains as the only IBI derived from the Boneh-Lynn-Shacham (BLS) short signature scheme which has the advantage of shorter keys. We show tight security reduction against active and concurrent attackers (*imp-aa/ca*) on our scheme that is obtained from the same transform. As the transform will only produce schemes that are only secure against passive attackers (*imp-pa*), security against *imp-aa/ca* scheme relies on a strong One-More interactive assumption and therefore resulted in weak security. While the OR-proof method allows schemes secure against *imp-pa* to be secure against *imp-aa/ca*, the resulting security against *imp-aa/ca* will suffer from loose bounds in addition to the user secret keys being doubled in size. Our work avoids both OR-proof and strong interactive assumptions by showing an ad-hoc proof for our construction which utilizes the weaker well-studied co-computational Diffie-Hellman assumption and yet still has tight security against *imp-aa/ca*. We demonstrate the tight security of our scheme which allows usage of even shorter key sizes.

INDEX TERMS Access control, access protocols, computer security, cryptographic protocols, identity-based identification, identity management systems, tight security.

I. INTRODUCTION

An identification scheme or Standard identification (SI) scheme is a set of algorithms that allows one entity (the prover) to assert it's own identity to another entity (the verifier) by acquisition of corroborative evidences through an interactive protocol [1]. The applications of SI schemes includes facilitating access control to critical resources (e.g., Accessing remote extra-terrestrial rovers, automated teller machine cash withdrawals) when different levels of security clearance is linked to different user accounts. SI schemes can also be used for border controls to grant entry for eligible passport holders as well as access to private health records on hospital networks. An identity-based cryptosystem functions similarly to public key cryptosystems with the exception that the public key is a publicly known value such as a tuple consisting information which uniquely identifies a person (e.g., Name, Social Security Number). Shamir [2] first proposed the concept of an identity-based scheme for encryption and signatures, which then further developed into the basis of an identification scheme by Fiat and Shamir [3]. Figure 1 depicts a typical setup for an identity-based identification (IBI) scheme.

The associate editor coordinating the review of this manuscript and approving it for publication was Fan Zhang.

A. RELATED WORKS

Since Fiat and Shamir's [3] fundamental paper in 1986, the development on IBI continued with various schemes [4]–[6]. While there is a decent number of IBI schemes, no rigorous formalization exist until Kurosawa and Heng [7]

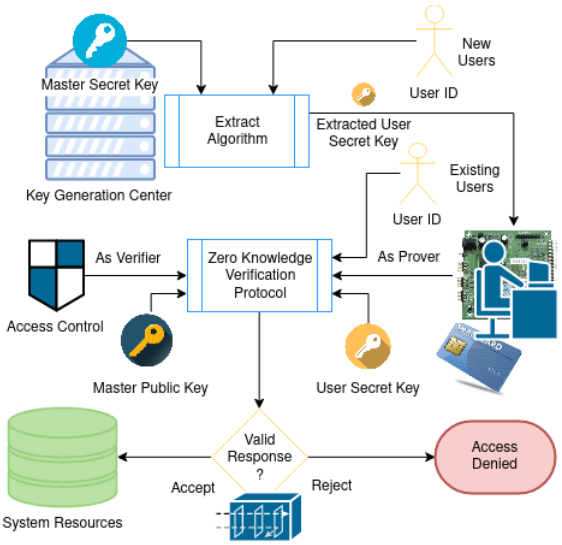

FIGURE 1. System architecture of an IBI scheme. The figure shows 2 of the 3 algorithms used in IBI deployments. User secret keys (usk) are extracted by a trusted authority (Key Generation Center) from a user identity (User ID) and the master secret key. The usk is then stored securely by the user. A user (e.g., a person, machine or an electronic chip) who wishes to authenticate their identity will undergo a zero knowledge verification protocol with a verifier holding the master public key. The verifier acts as an access control mechanism and the result of the protocol can then be used to decide on granting or denying access to system resources. The system is compromised if the master secret key is leaked as it allows forgery of new unauthorized user secret keys.

first proposed one in 2004. They introduced a transform known as the Kurosawa-Heng transform which turns a signature scheme that is existentially unforgeable under chosen message attacks (*euf-cma*) into an IBI that is secure under passive impersonation (*imp-pa*). In their extended paper, they also proved the security against active/concurrent impersonation (*imp-aa/ca*).

In the same year, Bellare *et al.* [8] independently argued that most of the schemes [3], [5], [6] are only shown to be provably secure in the standard identification domain and proceeded to complete the security proofs in the identity-based domain for all three types of attacks (i.e., *imp-pa,imp-aa,imp-ca*). In addition, they also showed their framework of SI, Standard Signature (SS), IBI and Identity based Signature (IBS) transformations if the SI and SS schemes satisfy certain security properties. Direct proofs were shown for Okamoto-IBI and their own proposed IBI scheme (i.e., BNN-IBI).

Yang *et al.* [9] introduced an improved framework in 2008 for IBI construction and proposed two new IBI schemes which are showed to be secure under *imp-pa* and *imp-aa* respectively. Their framework generalized the One-More relations to two families: trapdoor weak/strong one more relationships (TWR,TSR). These assumptions are then used to prove security for passive and active/concurrent attacks. Their work also included frameworks for the standard model, using a variant selective-ID (Weak selective-ID) to show the security of schemes transformed using their framework. In a conventional selective-ID model, the attacker must first commit to a single target identity before entering phase 1 of the security game. Meanwhile, for weak selective-ID, the attacker can commit a set of identities.

The security of Beth-IBI under *imp-aa/ca* was attempted by Crescenzo [10] but was shown to be totally broken by Chin *et al.* [11], allowing the master key to be retrieved by an attacker with just two extracts and hash queries. In 2011, Tan *et al.* [12] showed a variant of the Schnorr signature based IBI with tight security reduction. A security reduction is considered tight if the probability of breaking the IBI scheme is nearly the same as that of breaking the underlying hard mathematical assumption. Generally speaking, a scheme without tight reduction would require larger key sizes to have the same level of security.

A technique known as OR-proof is known to enhance a *imp-pa* secure SI scheme into one that is *imp-ca* secure. In 2012, Fujioka *et al.* [13] demonstrated that the technique is also useful for IBI schemes. Particularly, the technique converted *imp-pa* secure IBI schemes that satisfy special zero-knowledge, special soundness and special challenge for *dual-identity* (DI) and *master-identity* (MI) transforms into a *imp-ca* secure IBI. The popular technique and its variant are used by [14]–[16].

In 2015, Chin *et al.* [17] showed an upgrade to the Schnorr-IBI variant [12] by extending the number of secret key components to 2. In contrast to the OR-proof technique, their scheme (Twin-Schnorr) employs the AND-proof technique which the impersonator must prove the knowledge of corresponding private keys to both public keys rather than just one of it. Twin-Schnorr is based on Schnorr SS and is proved with strong security for active and concurrent attacks with high efficiency and is pairing free. They also subsequently answered the question on the security of Beth-IBI under *imp-aa/ca* in [18], aptly named Twin-Beth.

Subsequently, Chin et. al. also presented new reset secure IBI schemes [19]. A reset attacker is a special class of attacker which can reset the prover to any state it desires in addition to being a *imp-ca*. Their work succeeded previous works on IBI schemes against reset attacks [20], [21]. However, as pointed out by [12], reset attacks can be easily prevented by having the prover erase the commit value before sending out the response message.

Aside from conventional IBI schemes that are based on the intractability of problems in number theory, there exist schemes that are catered for post-quantum cryptography. The earliest of this was an identification protocol in 1993 by Stern [22] that is based coding theory. Works by Cayrel *et al.* [23]–[25] and El Yousfi Alaoui *et al.* [26] builds on the Stern authentication protocol. Cayrel's most recent work in 2010 consist of a 5-pass variant of Stern's protocol and requires 16 iterations of it to be run to achieve 128-bit security [27]. Yang *et al.* [15] code-based IBI scheme is similar to Cayrel's, but uses the OR-proof method and thus is provably secure for *imp-ca* security. In 2016, Song and Zhao [16] introduced use of Preetha, Vasant and

TABLE 1. Security bounds of existing IBI schemes.

Scheme	Security Bound for *imp-aa/ca*
GQ [7]	$\epsilon \leq \sqrt{e(1+q_E)Adv_{q,M}^{om-rsa}} + \frac{1}{q}$
BLS [7]	$\epsilon \leq \sqrt{e(1+q_E)Adv_{q,M}^{om-cdh}} + \frac{1}{q}$
OKDL [8]	$\epsilon \leq \sqrt{Adv_{G,M}^{dlog}} + \sqrt{Adv_{\mathcal{OKCL},F}^{ss-cma}} + \frac{3}{q^{1/2}}$
BNN [8]	$\epsilon \leq \sqrt{Adv_{G,M}^{om-dlog}} + \sqrt{Adv_{Schnorr,F}^{ss-cma}} + \frac{2}{q}$
BB [14]	$\epsilon \leq \sqrt{2 \cdot Adv_{Boneh-Boyen,F}^{euf-cma}} + \frac{1}{q}$
Yang [9]	$\epsilon \leq \sqrt{2 \cdot Adv_{\mathcal{KW},F}^{seuf-cma}} + \frac{1}{q}$
Tight-Schnorr [12]	$\epsilon \leq Adv_{G,M}^{ddh} + 2\frac{(q_E+1)}{q}$
Fujioka (OR-proof) [13]	$\epsilon \leq \sqrt{2 \cdot Adv_{IBI,I'}^{imp-pa}} + \frac{1}{q}$
Twin-Schnorr [17]	$\epsilon \leq \sqrt{Adv_{G,M}^{dlog} + \frac{1}{q}} + \frac{1}{q}$
Twin-Beth [18]	$\epsilon \leq \sqrt{Adv_{G,M}^{dlog}} + \sqrt{Adv_{Elgamal,F}^{ss-cma}} + \frac{3}{q^{1/2}}$

$\epsilon : Adv_{IBI,I}^{imp-aa/ca}$, $Adv_{IBI,I'}^{imp-aa/ca}$:underlying IBI security bounds, q: challenge $C_{HA} \in \{0, 1, ..q-1\}$ which is of super logarithmic challenge length $\lambda(k)$, q_E: maximum extraction queries for *I*, *k*: security parameter, *dlog*: discrete logarithm assumption, *ddh*: decisional Diffie-Hellman assumption, *rsa*: RSA factoring hard problem assumption, om-*: One-More assumptions, *ss-cma*: semi-strong unforgeability under chosen message attacks, *e*: natural logarithm, *M*: algorithm which breaks the hard assumption, *F*: forger with breaks the signature scheme. *G*: The group in which the hard assumption is considered intractable.

Rangan (PVR) signatures to the Stern identification protocol which allows their scheme to be resistant against the Bleichenbacher attack known to affect [23]–[25]. Their scheme has shorter parameter sizes and is also provably secure due to the OR-proof method.

We conclude this section with Table 1 which shows a comparison of security bounds relative to the underlying hard assumption on relevant existing IBI schemes.

B. PROBLEMS WITH EXISTING SCHEMES

The IBI schemes derived by Kurosawa and Heng [7] using their transform only has security against *imp-pa*. To show security against *imp-aa/ca*, they use One-More interactive assumptions which result in loose bounds as well as weaker security due to the assumptions being naturally stronger.

In the work by Bellare et. al., Beth-IBI [4] is only shown to be secure under *imp-pa* with the security under *impaa/ca* left unanswered. Yang's framework [9] provided better generalizations of IBI transforms, but still suffers from the use of interactive assumptions.

Tight-Schnorr [12] was able to avoid the use of the One-More assumptions in its proof, but its security is affected by the number of extract queries. This means that if an attacker manages to get their hands on an extract oracle (KGC breach), it can effectively break the scheme when the impersonator has extracted enough user keys even if the master secret key is secure.

As for the OR-proof approach, despite the upgrade in security model, the *imp-ca* IBI's security is based on the underlying security of the *imp-pa* IBI scheme. This has caused the security bounds for *imp-ca* to be relatively loose. One major limitation with the OR-proof technique is that more exchanges are required by the protocols using this method since the prover will need extra commit and response messages to prove their identity. Another problem is the user secret keys with *dual-identity* or *master-identity* will be almost doubled in size. Schemes such as [15], [16] that uses OR-proof technique has weaker security bounds against *imp-ca* and has larger user key sizes.

Even with tighter security for Twin-Schnorr and Twin-Beth, the schemes still require public key components to be doubled, which introduces additional storage and transmission overhead to an access control system.

Finally, we do not consider coding-based IBI schemes due to multiple problems such as large public keys (5-30 Megabits), large transmission bandwidth (30-40 Kilobits) and non-standard protocols (multiple 3-pass or 5-pass rounds needed to be run for one identification attempt).

Essentially, it is difficult to achieve tight *imp-aa/ca* security on IBI schemes **without** sacrificing security guarantees. Prior to the OR-proof method, schemes employ an inefficient method of using interactive assumptions [7], [9] to prove *imp-aa/ca* security. Schemes that are proved with OR-proof [13] have loose bounds that rely on *imp-pa* security and requires user secret key sizes to be doubled. While achieving tighter security, the AND-proof method [17], [18] requires doubling of public key components.

C. OUR CONTRIBUTION

While existing IBI schemes are secure against active and concurrent adversaries, their security is not tight. Security of cryptosystems are related to hard problems, and schemes are proved secure by reducing the probability of breaking a scheme to the probability of solving a hard problem, most of which are thought to be improbable within reasonable time. If the probability of breaking the scheme approaches closely to the probability of solving the hard problem, the reduction is considered tight. Tight security reduction not only gives stronger security guarantees, but also allows secure use of smaller sized parameters [28].

In this work, **we perform tight security reduction against active and concurrent attackers (*imp-aa/ca*) on our scheme that is obtained from the *Kurosawa-Heng transform***. The transform will only result in schemes that are only secure against *passive attackers* (*imp-pa*). To show security against *imp-aa/ca*, the existing scheme relies on a strong interactive assumption and thus resulted in weak security. While the OR-proof method [13] allows schemes that are *imp-pa* secure to also be *imp-aa/ca* secure, the resulting security against *imp-aa/ca* will suffer from loose bounds in addition to the user secret key size doubled and having more exchanges in their protocol. In order to avoid OR-proof or strong interactive assumptions [7], [9], we show an ad-hoc proof for our construction which uses a weak assumption and yet still has tight security against *imp-aa/ca*.

We perform the transform using a variant of the BLS-signature scheme by Ng *et al.* [29]. **The new BLS-IBI scheme runs on Type-3 pairings and its stronger security against *imp-aa/ca* is derived from the weaker static co-CDH assumption**. In comparison, the existing BLS-IBI scheme runs on Type-1 pairings that are deemed broken [30], [31] and have weaker security as it relies on a strong interactive assumption. In addition, our tight reduction allows use of smaller group and key sizes.

On the 128-bit security level based on NIST recommendations [32], **our scheme has the advantage of shorter key sizes with at least a reduction by 255 bits and reduced bandwidth requirements by 6143 bits/session in comparison to existing IBI schemes**. Our scheme also surpasses the original BLS-IBI by a factor of $\frac{e(1+q_E)}{2}$ on their security bound and is first to use the Multi-Instance Reset-Lemma [33] to further tighten our security bound against concurrent attackers. The presented scheme is suitable for remote authentication on memory limited and bandwidth starved systems such as Wireless Sensor Networks (WSN) node authentication, satellite management access control or even naval submarine identification under the depths. As the scheme can function without the KGC during verification, it is particularly well suited for ad-hoc networks created during disasters relief operations where the TTP infrastructure may not be readily available, not to mention the scarcity of bandwidth in those situations.

TABLE 2. Default notations.

Notation	Meaning
$\{0,1\}^*$	Bit string of arbitrary length
$\{0,1\}^n$	Bit string of length n
$r \xleftarrow{\$} S$	Uniformly sample r from finite set S
$a \leftarrow (f_1, f_2)$	Parse the tuple (f_1, f_2) as a
k	Security parameter, usually denoted by 1^k and is of value 128, 192 and 256
p, q	A large prime number ($\approx 2^{-k}$)
$\mathbb{Z}_q$	Integers modulo q or Scalars or order q
$\mathbb{G}$	DLOG/ECC group
B	Elliptic curve base point
a, b, c (lowercase)	Integers, scalars on ECC
A, P, Q (uppercase)	Group elements, points on ECC
$s \xleftarrow{\$} \mathbb{Z}_q$	Uniformly sample an integer or scalar s
$S \xleftarrow{\$} \mathbb{G}$	Uniformly sample a DLOG group element/point S
$(m)pk$	(Master) public key
$(m)sk$	(Master) secret key
usk	User secret key
ϵ	Hard assumption (i.e., DLOG, RSA factoring, CDH)

DLOG - Discrete Logarithm, RSA - Rivest-Shamir-Adleman (A public key cryptographic scheme), CDH - Computational Diffie-Hellman

D. ORGANIZATION

We first provide a definition of identity-based identification and the security notions used in this work in section II. The tight BLS signature scheme along with our construction of the IBI scheme and its security proof is then examined under section III. Section IV discusses on the designed IBI scheme in terms of key lengths, security tightness, operational speed and provides comparison against existing IBI schemes before finally concluding on section V.

II. PRELIMINARIES

1) NOTATION

Table 2 shows the default notation and their meaning throughout this work. While finite field arithmetic over integers $\mathbb{F}_q$ uses multiplicative groups (i.e., $\mathbb{Z}_q^*$), $\mathbb{Z}_q$ is somtimes used for the sake of simplicity. Additive notation is used as the scheme is instantiated using elliptic curve cryptography (ECC).

2) CO-COMPUTATIONAL DIFFIE-HELLMAN ASSUMPTION

The co-computational Diffie-Hellman assumption or co-CDH in $\mathbb{G}_1 \times \mathbb{G}_2$ is defined by definition 1.

Definition 1: The Co-Computational Diffie-Hellman assumption (Co-CDH). Given $(B_1, B_2, xB_1, xB_2) \in \mathbb{G}1 \times \mathbb{G}_2$ and $P \in \mathbb{G}_1$, compute $xP \in \mathbb{G}_1$. The advantage of an

adversary A running in time t is:

$$Adv^{Co-CDH}_{\mathbb{G}_1\times\mathbb{G}_2} := Pr[A(B_1, B_2, P, xB_1, xB_2) = xP] \quad (1)$$

A $(t, Adv^{Co-CDH}_{\mathbb{G}_1\times\mathbb{G}_2})$-breaks the assumption if the probability in equation 1 is non negligible.

3) BILINEAR PAIRING

A bilinear pairing is a function e that maps $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are groups of prime order based on the curve E over the finite field $\mathbb{F}_q$. This is *Type-3* pairing and its security is determined by the hardness of the co-CDH assumption [34]. The following are properties of e:

1) **Bilinearity**:
   $\forall B_1 \in \mathbb{G}_1, B_2 \in \mathbb{G}_2 : e(aB_1, bB_2) = e(B_1, B_2)^{ab}$.
2) **Non-degeneracy**:
   $e(B_1, B_2) \neq 1$.
3) **Computability**:
   There exists an efficient way to compute $e(B_1, B_2)$.

4) PSEUDO-RANDOM BIT GENERATOR

A pseudo-random bit generator (PRBG) is an efficient function that outputs a bit upon being invoked such that no distinguishing algorithm D is able to tell apart its output sequence J_1 with that of a truly random bit sequence J_2. The advantage of D telling apart the two sequence $Adv^{PRBG}_{D,PRBG}$ is only negligibly more than 1/2 and is given as follows:

$$\Pr_{j\xleftarrow{\$}J_1}[D(j) = 1] - \Pr_{j\xleftarrow{\$}J_2}[D(j) = 1] - 1/2 \leq \epsilon$$

5) RANDOM ORACLE

A random oracle is a theoretical blackbox which responds to queries in a truly random manner. For the security analysis of this work, the hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ is considered to be a random oracle.

6) MULTI-INSTANCE RESET LEMMA

The Multi-Instance Reset Lemma [33] is a generalization of many parallel instances of the Reset Lemma [6].

Definition 2: The Multi-Instance Reset Lemma is a "generalization of many parallel instances of the Reset Lemma" [33].

Lemma 1: Multi-Instance Reset Lemma. For an integer $N \geq 1$, a non-empty set $Q \neq \emptyset$ and an algorithm $\mathcal{H}$ which returns a tuple (b,σ) on input (a, q) where b is a bit and σ is the side output. The probability that $\mathcal{H}$ accepts is defined by:

$$acc := Pr[b = 1 | a \xleftarrow{\$} \mathcal{I}; q \xleftarrow{\$} Q; (b, \sigma) \xleftarrow{\$} \mathcal{H}(a, q)]$$

where $\mathcal{I}$ is a random input generator. The multi-instance reset algorithm $\mathcal{R}_{\mathcal{H}}$ takes input $a_1, \ldots, a_N$ and runs algorithm 1.
Let

$$res := Pr[i^* \geq 1 | a_1, \ldots, a_N \xleftarrow{R} \mathcal{I}; (i^*, \sigma, \sigma') \xleftarrow{R} \mathcal{R}_{\mathcal{H}}]$$

Algorithm 1 Multi-Instance Reset Algorithm

procedure MI-reset $\mathcal{R}_{\mathcal{H}}(a_1, \ldots, a_N)$
  for $i \in [N]$ **do**
    initialize random coins ρ_i
    $q_i \xleftarrow{\$} Q$
    $(b_i, \sigma_i) \xleftarrow{\$} \mathcal{H}(a_i, q_i, \rho_i)$
  end for
  if $b_1 = \ldots = b_N$ **then**
    return $\perp$
  end if
  Fix $i^* \in [N]$ such that $b_{i^*} = 1$
  for $j \in [N]$ **do**
    $q'_j \xleftarrow{\$} Q$
    $(b'_j, \sigma'_j) \xleftarrow{\$} \mathcal{H}(a_i, q'_i, \rho_{i^*})$
  end for
  if $\exists j^* \in [N] : (q_{i^*} \neq q'_{j^*} and b'_{j^*} = 1)$ **then**
    return $(i^*, \sigma_{i^*}, \sigma'_{j^*})$
  else
    return $\perp$
  end if
end procedure

Then

$$res \geq (1 - (1 - acc + \frac{1}{|Q|})^N)^2 \quad (2)$$

A. IDENTITY-BASED IDENTIFICATION (IBI)

Based on the similarities in SS schemes and IBI schemes, Kurosawa and Heng [7] formalized the notion of an IBI scheme and proposed a transformation to convert a SS scheme to an IBI scheme. The transformation is hereby referred to as the **Kurosawa-Heng transform**.

Definition 3: An identity-based identification (IBI) scheme is a 4-tuple scheme specified by 4 Probabilistic Polynomial Time (PPT) algorithms $\mathcal{IBI} = (\mathcal{S}, \mathcal{E}, \mathcal{P}, \mathcal{V})$: Namely, the setup algorithm $\mathcal{S}$, extract algorithm $\mathcal{E}$ and an identification protocol. $\mathcal{P}$ and $\mathcal{V}$ are interactive algorithms that are run by the prover and the verifier respectively and they form the identification protocol $(\mathcal{P},\mathcal{V})$.

- **Setup** $\mathcal{S}$: This algorithm is run by the key generation center (KGC) to generate the parameters of the scheme. The KGC inputs 1^k to $\mathcal{S}$ and obtains `params` (mpk) and the `master-key` (msk). mpk is known to the public while msk is kept secret.
- **Extract** $\mathcal{E}$: This algorithm is run by the KGC to compute a private key corresponding to some public identity string `ID`. It requires the msk, mpk and `ID`, returning the user private key usk.
- **Identification Protocol** $(\mathcal{P},\mathcal{V})$: Prover $\mathcal{P}$ with (mpk, `ID`, usk) and Verifier $\mathcal{V}$ with (mpk, `ID`) runs an interactive protocol in which the $\mathcal{P}$ attempts to convince $\mathcal{V}$ that $\mathcal{P}$ indeed possesses usk, thereby authenticating the identity

Identification Protocol

Input: $\mathcal{P}$ has inputs (mpk, ID, usk), $\mathcal{V}$ has inputs (mpk, ID).

Protocol:

1. $\mathcal{P}$ samples nonce and sends commit C_{MT} to $\mathcal{V}$
2. $\mathcal{V}$ samples and sends challenge C_{HA} to $\mathcal{P}$
3. $\mathcal{P}$ computes and sends response R_{SP} to $\mathcal{V}$
4. $\mathcal{V}$ verifies the transcript (C_{MT}, C_{HA}, R_{SP}) and outputs 1 on `accept` or 0 on `reject`.

FIGURE 2. Identification protocol.

of $\mathcal{P}$. This protocol outputs `accept` (1) for any legitimate $\mathcal{P}$ and `reject` (0) otherwise.

Figure 2 shows an identification protocol which is referred to as the three-move protocol (canonical).

1) SECURITY MODEL FOR IBI

An impersonating adversary to an IBI scheme breaks the security if it is able to fool the verifier into accepting it's proof of identity with non-negligible probability. The adversaries can be further categorized into 3 different types with increasing capabilities:

- *Passive Attacker* (*imp-pa*): A passive attacker can eavesdrop on the conversation between provers and verifiers before attempting to impersonate.
- *Active Attacker* (*imp-aa*): In addition to eavesdropping like a passive attacker, an active attacker can actively participate in the conversation with honest verifiers to learn more information before the impersonation attempt.
- *Concurrent Attacker* (*imp-ca*): A concurrent attacker has multiple instances of active attackers running in parallel.

A game between an impersonator I and a challenger C can be used to model the security of an IBI scheme. The goal of the impersonator is to impersonate an honest user in the system. C runs $\mathcal{S}$ and obtains mpk, msk. mpk is passed to I. Here we describe the security model of an IBI scheme with the experiment $Exp^{imp-atk}_{IBI,I}$ which consist of the following phases sequentially:

- *Phase 1*. I is allowed to issue extract and identification queries. For identification queries, should I be a passive attacker, then C replies with valid transcripts of the identification protocol. Otherwise, C (Or its clones) will then assume the role of a verifier while I will be the prover.
- *Phase 2*. I outputs an identity that it wishes to be challenged on, while still being able to issue extract and identification queries. C plays the role of the verifier and I as the prover. The output of C, $\mathtt{dec} \in \{\mathtt{accept}, \mathtt{reject}\}$ from the identification protocol is the output of the experiment. I wins if `dec = accept`.

Lemma 2: The security of an IBI scheme is based on the advantage of the adversary I in winning the game for all types of attacks (i.e., $atk \in$ *pa,aa,ca*). $Adv^{imp-atk}_{IBI,I}(k) = Pr[Exp^{imp-atk}_{IBI,I} = \mathtt{accept}]$ where k is the security parameter.

Definition 4: An IBI is $(t, q_E, q_I, Adv^{imp-atk}_{IBI,I}(k))$-secure against *imp-atk* if the advantage for any I that runs with polynomial time t, $Adv^{imp-atk}_{IBI,I}(.)$ is negligible, where q_E and q_I are the number of queries made to the *Extract* and *Identification* oracle respectively.

B. STANDARD SIGNATURE (SS)

Definition 5: A standard signature scheme (SS) consist of 3 PPT algorithms (Key Generation, Sign and Verify) which are described as follows:

- **Key Generation**: On input 1^k, generates pk, sk. Only sk is kept secret.
- **Sign**: On input sk and message m, outputs a signature of m, denoted as σ.
- **Verify**: On input pk, m, σ, decide if σ is a valid signature of m based on pk. Returns `accept` (1) for a valid σ and `reject` (0) otherwise.

1) SECURITY NOTIONS FOR SS

Briefly, the security notion of SS considers the attacker goal of forgery. Existential unforgeability (euf) whereby no attacker can forge signatures on new messages and the stronger strong existential unforgeability (seuf) where no attacker can forge different signatures on previously queried messages. In terms of the attacker capability, the strongest being the adaptive chosen message attack (cma), where the attacker has access to the sign oracle and is able to issue queries adaptively.

2) REQUIREMENT FOR SS

For a SS scheme to be transformed into IBI, the Kurosawa-Heng transform requires that it possesses what is known as a Δ-challenge semi zero knowledge protocol (Δ semi-ZKP). Given public key pk, message m and σ which is a signature on m, $(\mathcal{P}, \mathcal{V})$ receives (pk, m) as input, while $\mathcal{P}$ receives an additional secret input σ. A transcript between $\mathcal{P}$ and $\mathcal{V}$ is denoted as $T = (C_{MT}, C_{HA}, R_{SP})$ and we say that the transcript is acceptable if $\mathcal{V}$ accepts it.

Definition 6: Defined by Kurosawa and Heng, "A standard signature scheme is said to have a Δ-challenge semi zero-knowledge protocol if there exists a 3-move (canonical) protocol $(\mathcal{P}, \mathcal{V})$ as follows:

Completeness. If $\mathcal{P}$ knows signature σ, then $Pr[\mathcal{V}$ accepts$] = 1$.

Soundness. There are Δ possible challenges C_{HA} and σ can be easily computed from 2 valid transcripts $(C_{MT}, C_{HA_1}, R_{SP_1})$ and $(C_{MT}, C_{HA_2}, R_{SP_2})$ such that $C_{HA_1} \neq C_{HA_2}$.

Simulatability. There is a simulator S which can output valid transcripts indistinguishable from one between an honest prover and verifier." [7].

III. CONSTRUCTION

Our IBI scheme is constructed from the Kurosawa-Heng transform, which requires a standard signature (SS) scheme. We chose the BLS variant by Ng *et al.* [29] due to its security tightness and the fact that it is *seuf-cma*. We first briefly recall the tight variant for the BLS signature scheme in Type-3 pairing and then followed with the canonical protocol design and finally introduces the constructed IBI.

A. TIGHT BLS SIGNATURE

The tight variant for BLS signature in Type-3 pairing [29] is defined by algorithm 2 (Keygen), algorithm 3 (Sign) and algorithm 4 (Verify). For correctness, it is trivial to see that the equality in the **Verify** algorithm holds as shown in equation 3. Figure 3 shows the Tight BLS signature scheme has a Δ-challenge zero knowledge protocol which is required by the Kurosawa-Heng transform.

$$\begin{aligned} e(H(m) - rP_2, Q) &= e(H(m) - rP_2, aB_2) \\ &= e(a(H(m) - rP_2), B_2) \\ &= e(\delta, B_2) \end{aligned} \tag{3}$$

Algorithm 2 Tight BLS Signatures: Key Generation

procedure TBLS-Keygen(1^k)
  $B_1 \xleftarrow{\$} \mathbb{G}_1$; $B_2 \xleftarrow{\$} \mathbb{G}_2$; $a, b \xleftarrow{\$} \mathbb{Z}_p$
  $P_1 \leftarrow aB_1$; $P_2 \leftarrow bB_1$; $Q \leftarrow aB_2$
  Select $H : \{0,1\}^* \rightarrow \mathbb{G}_1$
  Select $PRBG : \{0,1\}^* \times Z_q \times Z_q \rightarrow 0, 1$
  Select $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
  $pk \leftarrow (B_1, B_2, P_1, P_2, Q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, H, PRBG)$
  $sk \leftarrow (a, b)$
return (pk, sk)
end procedure

Algorithm 3 Tight BLS Signatures: Signature Generation

procedure TBLS-Sign(pk, m, sk)
  $r \xleftarrow{\$} PRBG(m, a, b)$; $\delta \leftarrow a(H(m) - rP_2)$
  $\sigma \leftarrow (\delta, r)$
return σ
end procedure

Algorithm 4 Tight BLS Signatures: Signature Verification

procedure Verify(pk, m, σ)
  if $e(H(m) - rP_2, Q) = e(\delta, B_2)$ **then**
return 1 ▷ `accept`
  else
return 0 ▷ `reject`
  end if
end procedure

Notice that the public key component B_1 and secret key component b are not used throughout the scheme. They are only used by the security proof of the scheme. Practically, there are one $\mathbb{G}_1$ and two $\mathbb{G}_2$ elements for *mpk* and one $\mathbb{G}_1$ element + 1 bit for *usk*.

Δ-challenge semi zero-knowledge protocol for Tight BLS Signatures

Input: $\mathcal{P}$ has inputs (pk, m, σ), $\mathcal{V}$ has inputs (pk, m).

Protocol:

1. $\mathcal{P}$ samples $t \xleftarrow{\$} Z_q$, computes and sends commit $C_{MT} \leftarrow (t(H(m) - rP_2), r)$ to $\mathcal{V}$
2. $\mathcal{V}$ samples $c \xleftarrow{\$} Z_q$, sends challenge $C_{HA} \leftarrow c$ to $\mathcal{P}$
3. $\mathcal{P}$ computes and sends response $R_{SP} \leftarrow (t + c)\delta$ to $\mathcal{V}$
4. $\mathcal{V}$ extracts $C \leftarrow t(H(m) - rP_2)$ from the commit and decide $e(C + c(H(m) - rP_2), Q) \stackrel{?}{=} e(R_{SP}, B_2)$. $\mathcal{V}$ outputs 1 or `accepts` if the equality holds and 0 or `reject` otherwise.

FIGURE 3. Δ-challenge semi ZKP for Tight BLS signatures.

Theorem 1: The protocol shown in figure 3 for the proposed SS scheme by [29] satisfies definition 6, where the prime order $q = \Delta$.

Proof: The protocol shown in figure 3 satisfy *completeness*, *soundness* and *simulability*.

Completeness. Any $\mathcal{P}$ which has a valid σ is certainly able to obtain an `accept` from $\mathcal{V}$. Correctness follows the same form as shown under equation 3.

Soundness. Consider 2 acceptable conversation between $(\mathcal{P}, \mathcal{V})$:
$(C_{MT}, C_{HA_1}, R_{SP_1}), (C_{MT}, C_{HA_2}, R_{SP_2})$, where $C_{HA_1} \neq C_{HA_2}$. Then δ (and thus, σ) can be computed as follows:

$$\begin{aligned} \frac{R_{SP_1} - R_{SP_2}}{(C_{HA_1} - C_{HA_2})} &= \frac{(t + c_1)\delta - (t + c_2)\delta}{c_1 - c_2} \\ &= \frac{(c_1 - c_2)\delta}{c_1 - c_2} \\ &= \delta \end{aligned} \tag{4}$$

Simulatability. Zero knowledge-ness is shown by having a simulator S output the tuple (C_{MT}, C_{HA}, R_{SP}) such that it is an acceptable conversation. S randomly chooses $t, c \in Z_q$ and samples $r \xleftarrow{\$} \{0, 1\}$. Finally, S can output the valid transcript $((tB_2 - c(H(m) - rP_2), r), c, tQ)$.

■

B. A VARIANT OF BLS-IBI

We now construct the IBI scheme using the SS scheme discussed under section III-A. Following the Kurosawa-Heng transform, **Key Generation** is now **Setup** for the IBI, **Sign** is then **Extract** and the Δ-challenge semi zero-knowledge protocol is the **Identification Protocol**. Likewise, the *pk* is now the `params` (*mpk*) and *sk* is the `master-key` (*msk*).

Tight BLS-IBI identification protocol

Input: $\mathcal{P}$ has inputs $(mpk, \texttt{ID}, \sigma)$, $\mathcal{V}$ has inputs $(mpk, \texttt{ID})$.

Protocol:

1. $\mathcal{P}$ samples $t \xleftarrow{\$} Z_q$, computes and sends commit $C_{MT} \leftarrow (t(H(\texttt{ID}) - rP_2), r)$ to $\mathcal{V}$
2. $\mathcal{V}$ samples $c \xleftarrow{\$} Z_q$ and sends challenge $C_{HA} \leftarrow c$ to $\mathcal{P}$
3. $\mathcal{P}$ computes and sends response $R_{SP} \leftarrow (t + c)\delta$ to $\mathcal{V}$
4. $\mathcal{V}$ extracts $C \leftarrow t(H(\texttt{ID}) - rP_2)$ from the commit and decide $e(C + c(H(\texttt{ID}) - rP_2), Q) \stackrel{?}{=} e(R_{SP}, B_2)$. $\mathcal{V}$ outputs 1 or `accepts` if the equality holds and 0 or `reject` otherwise.

FIGURE 4. Identification protocol for Tight BLS-IBI.

Generated signatures σ will be used as the user secret key usk. The new IBI $= (\mathcal{S}, \mathcal{E}, \mathcal{P}, \mathcal{V})$ is described by algorithm 5 and 6 and figure 4 shows the identification protocol.

Algorithm 5 Tight BLS-IBI: Setup $\mathcal{S}$

procedure Setup(1^k)
  $(pk, sk) \leftarrow$ TBLS-KEYGEN(1^k)
  $(mpk, msk) \leftarrow (pk, sk)$
return (mpk, msk)
end procedure

Algorithm 6 Tight BLS-IBI: Extract $\mathcal{E}$

procedure Extract(mpk, ID, msk)
  $\sigma \leftarrow$ TBLS-SIGN(mpk, ID, msk)
  $usk \leftarrow \sigma$
return usk
end procedure

1) SECURITY AGAINST PASSIVE ATTACKS

Lemma 3: The Δ-challenge semi zero knowledge protocol that satisfies completeness, soundness and simulatability implies that the transformed IBI scheme satisfies *imp-pa* security vis-a-vis the Kurosawa-Heng transformation.

2) SECURITY AGAINST ACTIVE ATTACKS

Theorem 2: The transformed IBI scheme under section III-B is $(t, q_E, q_I, Adv^{imp-atk}_{IBI,I}(k))$-secure against *imp-aa/ca* per equation 5.

$$Adv^{imp-atk}_{IBI,I}(k) \leq 1 - (1 - \sqrt{2 \cdot \epsilon})^{(\frac{1}{N})} + \frac{1}{q} \tag{5}$$

where $\epsilon = Adv^{co-CDH}_{G_1 \times G_2}$, time t bounded by a polynomial and $N \geq 1$ is the number of parallel reset instances described later in the proof.

Proof: A proof by contradiction by reducing an impersonator I which supposedly $(t, q_E, q_I, Adv^{imp-atk}_{IBI,I}(k))$-breaks the scheme, to a simulator S which can be used to break the co-CDH assumption. Therefore, no such I may exist as their existence meant that there also exist an algorithm S which can use I (or their parallel instances) in the following manner:

S receives the co-CDH instance $(\mathbb{G}_1, \mathbb{G}_2, B_1, B_2, aB_1, aB_2) \in \mathbb{G}_1 \times \mathbb{G}_2$ and $U \in \mathbb{G}_1$. S must then output $aU \in \mathbb{G}_1$. S does not know the secret value a. For the `params` mpk components, S sets them as follows $\mathbb{G}_1 = \mathbb{G}_1, \mathbb{G}_2 = \mathbb{G}_2, B_1 = B_1, B_2 = B_2, P_1 = aB_1$, $P_2 = U, Q = aB_2$. S selects $PRBG$, e and passes $mpk \leftarrow (B_1, B_2, P_1, P_2, Q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, H, PRBG, e)$ to I. For the hash queries H, S programs it and responds to queries from I in *Phase 1* of the game as described:

- **Hash Queries** H: S maintains a list of healthy users HU and a list of tuples $(\texttt{ID}_i, s_i, r_i)$. On input $(\texttt{ID}_i)$:
  1) If $\texttt{ID}_i$ is in any of the entry in the list, return $H(\texttt{ID}_i) = s_iB_1 + r_iB_2$.
  2) Else, samples $s_i, s_1, s_2 \xleftarrow{\$} \mathbb{Z}_q$ and $r \leftarrow PRBG(\texttt{ID}_i, s_1, s_2)$. S stores the tuple $(\texttt{ID}_i, s_i, r_i)$ onto the list and returns $H(\texttt{ID}_i) = s_iB_1 + r_iP_2$.
  3) $HU \leftarrow HU \cup \{\texttt{ID}_i\}$
- **Extract Queries**: S maintains a list of corrupted users CU. On input $(\texttt{ID}_i)$:
  1) If $\texttt{ID}_i \notin CU \cup HU$, run Hash query on $\texttt{ID}_i$.
  2) $CU \leftarrow CU \cup \{\texttt{ID}_i\}$, $HU \leftarrow HU \setminus \{\texttt{ID}_i\}$
  3) Return $usk_i \leftarrow (\delta_i = s_iP_1, r_i)$.
- **Identification Queries**: S plays the role of an honest prover $\mathcal{P}$ interacting with I as the cheating verifier $\mathcal{CV}$. On input $\texttt{ID}_i$ from $\mathcal{CV}$:
  1) If $\texttt{ID}_i \notin HU \cup CU$, run Hash query on $\texttt{ID}_i$.
  2) S obtains usk_i as it knows s_i and r_i from the tuple list.
  3) $\mathcal{P}$ samples $t \xleftarrow{\$} \mathbb{Z}_q$, computes $C_{MT} \leftarrow (ts_iB_1, r_i)$, and sends C_{MT} to $\mathcal{CV}$.
  4) $\mathcal{P}$ receives C_{HA}, computes and sends $R_{SP} \leftarrow (t + C_{HA})\delta_i = (t + C_{HA})s_iP_1$.
  5) The conversation is (C_{MT}, C_{HA}, R_{SP}), which $\mathcal{CV}$ actively participated in.

(C_{MT}, C_{HA}, R_{SP}) is an acceptable conversation because for $\mathcal{CV}$, the equality $e(C + C_{HA}(s_iB_1 + r_iP_2 - r_iP_2), Q) = e(R_{SP}, B_2)$ holds as shown in the following equations. $C = ts_iB_1$ can be easily extracted from C_{MT}.

$$\begin{aligned}
&e(C + C_{HA}(H(\texttt{ID}) - r_iP_2), Q) \\
&\quad = e(C + C_{HA}(s_iB_1 + r_iP_2 - r_iP_2), aB_2) \\
&\quad = e(ts_iB_1 + C_{HA}(s_iB_1), B_2)^a \\
&\quad = e((t + C_{HA})s_iaB_1, B_2) \\
&\quad = e((t + C_{HA})\delta_i, B_2) \\
&\quad = e(R_{SP}, B_2)
\end{aligned}$$

TABLE 3. Comparison with original BLS-IBI.

Scheme	Assumptions	Security Bounds	#mpk comp.	#usk comp.
BLS-IBI [7]	One-More CDH	$\sqrt{e(1+q_E)Adv_{q,M}^{om-cdh}} + \frac{1}{q}$	$2\mathbb{G}_1$	$\mathbb{G}_1$
OR-proof [13]	BLS-IBI(*imp-pa*)	$\sqrt{2 \cdot (2eq_E Adv_{G,M}^{GDH} + \frac{1}{q})} + \frac{1}{q}$	$2\mathbb{G}_1$	$2\mathbb{G}_1$
Tight-BLS-IBI	co-CDH	$1 - (1 - \sqrt{2 \cdot Adv_{\mathbb{G}_1 \times \mathbb{G}_2}^{co-CDH}})^{(\frac{1}{N})} + \frac{1}{q}$	$\mathbb{G}_1 + 2\mathbb{G}_2$	$\mathbb{G}_1 + 1$bit

Once I is ready for impersonation, S moves the game onto *Phase 2*, where I then outputs an identity which it wishes to be challenged on, $\texttt{ID}^* \notin CU$. If $\texttt{ID}^* \notin HU$, then S runs the Extract query to obtain $usk = (\delta, r)$ and s from the tuple of $\texttt{ID}^*$. S then plays as the challenger. When the interaction produces a conversation $(C_{MT}, C_{HA_1}, R_{SP_1})$, S resets I back to after it has sent the C_{MT} message, and continues from there. By the end, 2 conversation $(C_{MT}, C_{HA_1}, R_{SP_1})$ and $(C_{MT}, C_{HA_2}, R_{SP_2})$ will be obtained. From C_{MT}, S gets the random bit r^* and check if it equals to r from usk. There are 2 cases to be analyzed from this point, provided the challenges $C_{HA_1} \neq C_{HA_2}$:

Case 1: I impersonates successfully with $ID^* \notin CU$. If $r = r^*$, then the attack on co-CDH has failed and S aborts. Else, S proceeds to solve the co-CDH problem by extracting δ^* using the soundness property from equation 4.

Case 2: I impersonates successfully with $ID^* \in CU$, but $\delta^* \neq \delta$. If $r = r^*$, the attack on co-CDH has failed and S aborts. Else, S proceeds to solve the co-CDH problem with the δ^* extracted from the soundness property.

In both cases, S aborts only if $r = r^*$. Else, co-CDH can be solved as follows:

$$\begin{aligned}
\frac{\delta^* - \delta}{r - r^*} &= \frac{a(H(\texttt{ID}*) - r^*P_2) - sP_1}{r - r^*} \\
&= \frac{a(sB_1 + rP_2 - r^*P_2) - saB_1}{r - r^*} \\
&= \frac{a(sB_1 + (r - r^*)P_2 - sB_1)}{r - r^*} \\
&= \frac{a(r - r^*)P_2}{r - r^*} \\
&= aP_2 \\
&= aU
\end{aligned}$$

S is able to solve co-CDH using I. Let event A be the event that S solves co-CDH by reset and event B be the event that S does not abort while running the above simulation. The probability of S solving co-CDH is then $Pr[A] \times Pr[B]$ where $Pr[A]$ is based off a generalization to the Reset Lemma by Bellare and Palacio [6], known as the Multi-Instance Reset Lemma by Kiltz *et al.* [33] following the inequality defined under equation 2. As S is able to answer all extract and identification queries without risk of aborting, event B only occurs during *Phase 2* when $r = r^*$, which occurs with probability 1/2. The bound for S to solve co-CDH is then:

$$\epsilon \geq (1 - (1 - Pr[I \text{ impersonates}] + \frac{1}{q})^N)^2 \times \frac{1}{2}$$

where $\epsilon = Adv_{G_1 \times G_2}^{co-CDH}$. □ ■

When N = 1, or a strictly single-instance active attacker, the bounds reduce to a form similar to the schemes studied under table 1.

$$Adv_{G_1 \times G_2}^{co-CDH} \geq (Pr[I \text{ impersonates}] - \frac{1}{q})^2 \times \frac{1}{2}$$

which results in:

$$Adv_{IBI,I}^{imp-atk}(k) \leq \sqrt{2 \cdot Adv_{G_1 \times G_2}^{co-CDH}} + \frac{1}{q} \tag{6}$$

Notice that for $N > 1$, the tightness increases by $\log_2 N$ bits. Since the proof bases on the premise that no adversary running in polynomial time can break co-CDH, therefore the security guarantee of the IBI scheme improves as the probability of breaking co-CDH increases if S runs parallel instances of I during impersonation attempts. This setting is possible as with consideration for concurrent attacker which runs multiple instances of the active attacker concurrently. This is also the strongest security setting as the concurrent attacker is the strongest type of attacker.

IV. ANALYSIS AND DISCUSSION

Throughout the comparison here, the key lengths derived shall be based on 128-bit security level recommended by National Institute of Standards and Technology (NIST) [32], where we try to equate the advantage of the impersonator $Adv_{IBI,I}^{imp-atk}$. We refer to our BLS-IBI scheme as "Tight-BLS-IBI" or simply "our scheme/variant" throughout the discussion. Since this is the first IBI scheme which employs Multi-Instance Reset Lemma for security against concurrent attackers, where N indicates the number of active attackers used concurrently. We by default use a conservative N=1 for easier comparison with existing schemes, and will explicitly state otherwise when making other form of comparisons.

A. KEY SIZE AND BANDWIDTH COMPARISONS

1) COMPARISON WITH THE ORIGINAL BLS-IBI

Comparing to the original BLS IBI [7], our scheme is able to achieve a much tighter security bound independent of the number of extract queries made by the impersonator as we managed to answer the extract queries without risk of aborting. Table 3 shows comparison between the new BLS IBI scheme to the original.

TABLE 4. Comparison with other pairing-based IBI.

Scheme	BB-IBI [14]	Tight-BLS-IBI
Assumption	BB signature under euf-cma	co-CDH
Random Oracle	No	Yes
Security Bounds	$\sqrt{2 \cdot Adv^{euf-cma}_{Boneh-Boyen,F}} + \frac{1}{q}$	$1 - (1 - \sqrt{2 \cdot Adv^{co-CDH}_{\mathbb{G}_1 \times \mathbb{G}_2}})^{(\frac{1}{N})} + \frac{1}{q}$
#bilinear pairing op.	7	2
mpk components	$2\mathbb{G}_1 + 2\mathbb{G}_2$	$\mathbb{G}_1 + 2\mathbb{G}_2$
usk components	$\mathbb{G}_1 + \mathbb{G}_2 + 2\mathbb{Z}^*_q$	$\mathbb{G}_1 + 1$bit

We see that while our scheme has a tighter security bound, we also use a much weaker assumption that is co-CDH relative to the One-More CDH assumption used in the original. This is because co-CDH is non-interactive, which improves the security guarantees provided by our scheme. However for the sake of comparison we shall roughly assume they have the same strength (i.e., $Adv^{om-CDH}_{q,M} \gtrapprox Adv^{co-CDH}_{\mathbb{G}_1 \times \mathbb{G}_2}$). We see that the 2 schemes then equates in security level when the hardness of the One-More CDH increases by approximately a factor of $\frac{e(1+q_E)}{2}$. For security level of the original BLS-IBI to match our new scheme, the original would have to increase its key sizes by **at least 11** bits for **every 1000** extract queries. Albeit having more public key *mpk* components, our scheme is able to achieve great savings in key lengths especially for the user keys as we avoided the use of One-More interactive assumptions to prove the security for *imp-aa/ca*, resulting in tight reduction. If we apply the OR-proof reduction [13] by the dual identity (DI) transformation to the original BLS-IBI, thus eliminating the use of One-More interactive assumptions for security under *imp-aa/ca*. We see that the resulting scheme still has a much weaker bound relative to our scheme due to the reduction from security bounds of the underlying *imp-pa* secure IBI, and that the usk component now has one additional $\mathbb{G}_1$ element compared to our variant.

We note that this improvement arises from the fact that the Kurosawa-Heng transform in 2004 only applies to security against *passive impersonators*, relying on a relatively loose proof system using the One-More CDH assumption for proof of security against active and concurrent attackers. While our scheme uses the transform, we introduced a new way of proving the security against active and concurrent attackers to provide significantly better security guarantees with smaller key sizes.

As remarked by Galbraith *et al.* [35], Type-3 pairings generally offer better performance even with high security parameters. Not only does our scheme enjoy better security bounds, it is also more secure in the sense that Type-1 pairings which are used by the original BLS-IBI is considered to be broken as recent advances in discrete logarithm algorithms [30], [31] meant that Type-1 construction using field characteristics of 2 or 3 is insecure.

2) COMPARISON WITH OTHER IBI SCHEMES

While the bounds on Yang's IBI [9] and BB-IBI [14] may have the same form as ours, they are based off the hardness on the strong existential unforgeability of the Katz-Wang signature scheme [36] and the existential unforgeability of the Boneh-Boyen signature scheme [37] respectively which are much stronger than the co-CDH assumption, thus having weaker security. The same argument applies to OKDL-IBI and BNN-IBI [8] which in addition to stronger assumptions, have looser bounds compared to ours scheme. Referring to Table 4 for comparison wtih BB-IBI, despite our scheme requiring the random oracle, it is much more efficient than BB-IBI requiring only **2** bilinear pairing operations instead of 7 in the identification protocols. Our user keys is also shorter by **767** bits.

As our scheme uses Type-3 pairing based operations during identification, it lacks operational efficiency in comparison to other non-pairing based IBI schemes [8], [12], [17], [18]. However, we note a few key points in which our scheme performs much better. Table 5 compares our scheme in terms of key sizes and bandwidth required during the identification protocol with references to schemes that also have tight bounds.

All 3 schemes have roughly the same public key sizes, our scheme has an obvious advantage in terms of the user key sizes and bandwidth efficiency. In terms of user key size on the 128-bit level, our user key size is 257 bits while the shortest of the other 2 is 512 bits, resulting our keys to be **at least** shorter by **255** bits. For the identification protocol, our scheme also performs better as it requires only 769 bits to be transferred throughout the 3 moves, lowering the required bandwith by **6143** bits/session against the shorter of the other 2 on 6912 bits/session (Twin-Schnorr). Table 6 shows the key size and total bandwidth reduction advantages of our scheme with different security levels in comparison with other schemes. In general, we see as the security level increases over time, our scheme stands to gain larger key size and bandwidth reductions in the long run thanks to tight reductions and the short keys of the BLS signature scheme.

When dealing with concurrent attackers, our scheme has an edge in terms of our security bounds as we are the first and only scheme to take advantage of the parallel instances

TABLE 5. Comparison with stronger IBI schemes.

Scheme	Tight-Schnorr [12]	Twin-Schnorr [17]	Tight-BLS-IBI
Assumption	Decisional-DH	Discrete Log	co-CDH
Security Bounds	$Adv^{DDH}_{q,M} + \frac{2(q_E+1)}{q}$	$\sqrt{Adv^{DLOG}_{q,M} + \frac{1}{q}} + \frac{1}{q}$	$1-(1-\sqrt{2 \cdot Adv^{co-CDH}_{\mathbb{G}_1 \times \mathbb{G}_2}})^{(\frac{1}{N})} + \frac{1}{q}$
mpk components	$4\mathbb{G}$	$3\mathbb{G}$	$\mathbb{G}_1 + 2\mathbb{G}_2$
usk components	$2\mathbb{Z}_q$	$3\mathbb{Z}_q$	$\mathbb{G}_1 + 1$bit
Prot. bandwidth	$3\mathbb{G} + 2\mathbb{Z}_q$	$2\mathbb{G} + 3\mathbb{Z}_q$	$2\mathbb{G}_1 + \mathbb{Z}^*_q + 1$bit

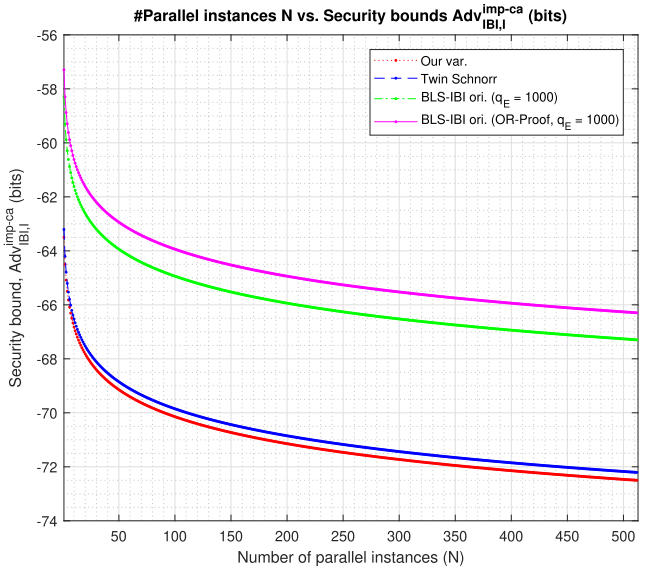

FIGURE 5. Comparison between Reset-Lemma based schemes upgraded with Multi-Instance Reset Lemma with security level k=128 for hard-assumptions.

of active attackers to tighten our bounds. Referring to equation 5, for some reasonable number of instances $N > 1$, our bounds improves by $\log_2 N$ bits. This seems counter-intuitive, but actually the scheme does not gain additional security but rather tighten its security to that of its hard-assumption, which translates to an apparent gain in security bounds. Obviously, any scheme proved with the Reset Lemma [6] can also be upgraded with the Multi-Instance Reset Lemma [33] under concurrent security. Our result on figure 5 indicate that most IBI schemes are more secure against concurrent attackers with up to roughly 8-bit gain. For schemes that are affected by the number of hash queries q_E, the amount must be shared among the number of instances. This is because the possibility for the simulator to abort in phase 1 increases, which meant that advantage brought by Multi-Instance Reset Lemma that is only applicable in phase 2 could be offset by it. In this regard, schemes like Twin-Schnorr or our scheme can benefit directly from Multi-Instance Reset Lemma compared to the original BLS-IBI and the OR-proof version of it.

While Tight-Schnorr has a remarkably tight bound due to the absence the Reset Lemma and therefore the square root, its bounds are affected by the number of extract queries up to a factor of $2q_E$ while our variant is free from it.

B. OPERATIONAL SPEED COMPARISONS

To evaluate our scheme in terms of its speed, we implemented the scheme in C/C++ using the Pairing-Based Cryptography (PBC) library developed by Ben Lynn [38]. Type-D curves with an embedding degree of 6 is used because they allow our scheme to achieve higher discrete logarithm (DLOG) equivalent security in addition to being able to perform Type-3 pairings. The curves were discovered by Miyaji *et al.* [39] and the PBC library generates the curve parameters using Scott and Barreto's Complex Multiplication algorithm [40]. A discriminant D is specified to obtain curve parameters of corresponding base field F_q of size q bits. Table 7 shows the discriminants that is used in our implementation and their DLOG equivalent security. The DLOG equivalent is essentially $6q$ due to the embedding degree of 6 [41]. For Schnorr-based IBI schemes, we used the original SchnorrSuite developed by the authors of [12], [17], which uses Java Big Integer for their operations. As their implementation only allows fixed groups sizes, we are limited to DLOG group sizes of 1024, 2048, 3072 and 7680.

Our test machine uses the Intel(R) Core(TM) i7-8750H CPU with 6 cores running at 2.20GHz under 64-bit Linux OS. Bandwidth is not taken into consideration here as the commit, challenges and responses are not sent over to any computers but rather written to and read from memory. Setup algorithms were ran 30 times (n=30) and the results averaged, while the extract and identification algorithms were ran 100 times (n=100).

In total, we evaluated the run-times for 4 schemes (Tight-BLS-IBI, Tight-Schnorr, Twin-Schnorr and BLS-IBI original) on each of the setup, extract and identify algorithms. Figure 6 and 7 shows the setup and extract algorithm run-times respectively for the 4 schemes for comparison. While the setup and extract run-times is not really important compared to the identification run-times, it gives us insight into the expected non-pairing performance of each scheme. The new Tight-BLS-IBI has a shorter setup time as the security level increases compared to both Schnorr schemes possibly thanks to shorter and less key generations. Likewise, the setup time for our variant is longer compared to the original BLS-IBI due to more points on the curve being sampled. Another factor that affects the speed is that Tight-BLS-IBI performs an extra point multiplication in $\mathbb{G}_2$ compared to the original BLS-IBI scheme during setup.

TABLE 6. *usk* and total bandwidth size reduction for different security levels, k = minimum security level.

IBI schemes	Key size reductions (bits)			Bandwidth reductions (bits)		
	k=128	k=192	k=256	k=128	k=192	k=256
Tight-Schnorr [17]	255	385	511	6,143	15,359	30,719
Twin-Schnorr [12]	511	767	1,023	8,959	22,655	45,567
BB-IBI [14]	767	1,151	1,535	1,535	2,303	3,071

TABLE 7. Type-D curve base field sizes and their DLOG security equivalent, generated using the Complex Multiplication algorithm with the PBC library.

Discriminant D	Base field size q (bits)	DLOG group size equivalent (bits)
1835683	192	1152
249563	252	1512
481843	359	2154
238859	407	2442
311387	522	3132
594739	677	4062
972483	1357	8142

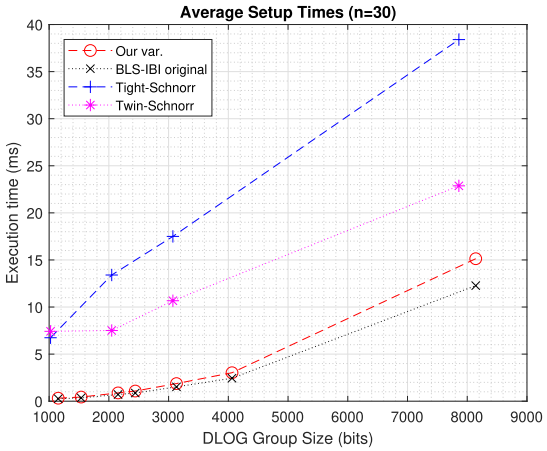

FIGURE 6. Setup algorithm run-times.

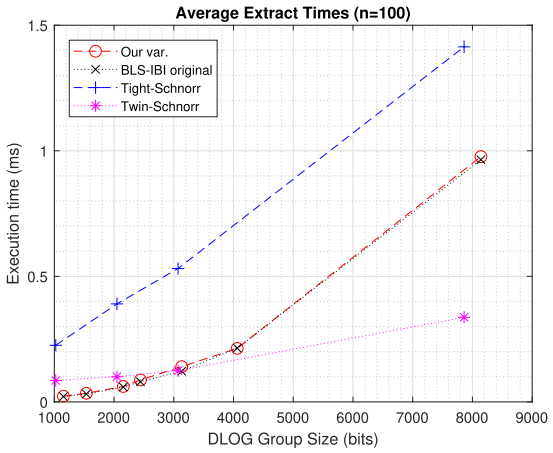

FIGURE 7. Extract algorithm run-times.

Figure 8 shows the most important comparison for run-time tests as the identification algorithm will be constantly used throughout the deployment of an IBI scheme. At the 3072-bit DLOG security level (3132 for BLS schemes on Type-D curves), the identification protocol run-time for Tight-BLS-IBI is around 5.5 times longer than that of Twin-Schnorr. This is caused by the expensive pairing operation involved in the BLS-based identification algorithm. However, in comparison to the original BLS-IBI, the difference is minute with a 0.3% increase in run-time for Tight-BLS-IBI given the additional security guarantees and the reduced key sizes. The negligible increase in run-time despite having more operations for Tight-BLS-IBI is due to the use of Type-3 pairings, which are more efficient than Type-1 pairings [42] used by the original BLS-IBI scheme.

C. IDENTIFICATION RUNTIME OPTIMIZATIONS

As the identification protocol is the core process of the IBI scheme, we provide suggestions on improving its run-time performance by considering optimizations on different aspects of the protocol.

1) PROVER OPTIMIZATIONS

Referring to figure 3, time spent computing the first component of the commit message $t(H(m) - rP_2)$ can be sped up. This is because $H(m) - rP_2$ is constant throughout all identification sessions for the same *usk* and thus can be precomputed and stored in memory. This will save 1 subtraction, multiplication and hash-to-group operation in $\mathbb{G}_1$. While an additional value is being stored, there is no need to sacrifice storage space because P_2 no longer needs to be stored, keeping storage requirements the same. This brings the total operations required for the prover to only 1 addition in $\mathbb{Z}_p$ and 2 multiplication in $\mathbb{G}_1$.

2) VERIFIER OPTIMIZATIONS

The verifier may also optimize its runtime by computing 1 of the 2 pairing operation $e(C + c(H(m) - rP_2), Q)$ before receiving the response from the prover. This is because the left-hand side of the verification equation shown in figure 3 does not require the response message. As such, a verifier with multi-core computing capabilities can easily parallelize this operation with the first thread computing the left-hand side while the second thread waits for the response.

3) PAIRING OPTIMIZATIONS

While this is beyond the scope of this work, it is interesting to look at other pairing operations that our IBI scheme could use to further optimize our slower runtime against the pairing-free schemes. Type-F pairings operating on curves

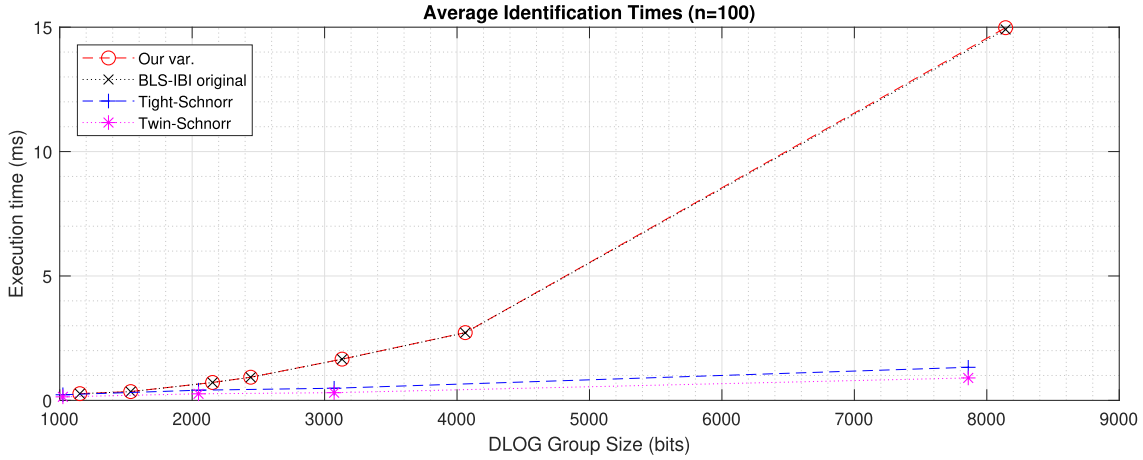

FIGURE 8. Identification algorithm run-times.

with the form $y^2 = x^3 + b$, or more commonly known as Barreto-Naehrig (BN) curves [43] can be used instead of the Type-D pairings used in this work. BN-curves has embedding degree of 12 which not only allows higher security level for a base field size of merely 160 bits, but has undergone much optimizations lately [44], [45]. Pairing optimizations include reducing the Miller-loop steps, representing integers differently and using low level techniques such as Single-Instruction-Multiple-Data (SIMD) floating-point arithmetic. The downside of using Type-F pairings is that the DLOG security level is now fixed at 1920 bits, compared to Type-D pairings which allows flexibility up to 8142 bits as shown in table 7.

D. USE CASES FOR TIGHT-BLS-IBI

Pertaining to the suitability of our scheme in actual deployments, we find that it is well suited to facilitate access control in large networks particularly those that has a scarcity of bandwidth. One possible class of networks are the Sensor Networks used by the currently trending Internet of Things (IoT). Wireless Sensor Networks (WSN) is a key enabler to allow massive data collection across different domains to fuel the big data analytics and such networks requires security to ensure that attackers cannot easily spoof themselves up as a legitimate sensor to insert adversarial data onto the network. Several works [46]–[49] have listed security challenges for WSNs and we envision our IBI scheme to be part of the solution to such networks. For example, the verifier protocol can be installed on gateways, whereby sensor nodes must authenticate themselves before pushing data up to the cloud. Since the prover has no need to perform pairing operation, and only requires at most 2 multiplication in $\mathbb{G}_1$ and 1 addition in $\mathbb{Z}_q$, the operational cost is minimal for the nodes. As our scheme utilizes low bandwidth for identification, this is very well suited for the WSNs with thousands to millions of sensors compared to other IBI schemes. The small *usk* sizes also saves non-volatile memory on the sensor nodes. The Key Generation Centers (KGC) can be the manufacturer of the sensors, inserting *usk* onto the sensors as they are manufactured. Different vendors may use multiple sets of *mpk* for different companies to disallow other sensors of the same build to authenticate. The sensors in the network may also use their own unique IDs to authenticate themselves the WSN, which stores the *mpk* of the groups of sensors that is allowed to push their data. The ID-based nature of this application also means that there is no need for a Trusted Third Party (TTP) to validate the public keys of the sensors attempting to authenticate as they could simply use their unique IDs assigned to them by the system designer or the manufacturer.

Aside from WSNs, IBI schemes offers very strong authentication compared to conventional password-based authentication methods. Several works [50]–[52] have pointed out weaknesses in password-based mechanisms, and we believe IBI schemes are better alternatives to password-based authentication because of 2 main reasons. The first being that verifiers no longer need to store user credentials, removing all possibilities of mis-implementation when securing their databases because all the verifier needs is just the publicly known *mpk*. User credentials are stored by the user themselves and if they are lost (e.g., accidental deletion), the KGC could always re-issue a new one. Another reason to use IBI schemes is that the authentication mechanism is no longer vulnerable due to weak passwords chosen by users who have trouble remembering the longer (and thus stronger) passwords. The pervasive nature of mobile computing also meant that users now have a device to store their user keys (*usk*). Our scheme has short keys that can be easily stored on user devices without too much of a burden to their storage requirement. Lastly, authentication using our scheme only takes less than 20 milliseconds which is very fast compared to the speed of typing in a password.

Recent works by Teh *et al.* [53] and Cheah *et al.* [54] focus on prototypes to facilitate access control using mobile smart devices with identity-based identification schemes. In the case of [53], the mobile smart devices are the provers seeking to unlock an electromagnetic lock controlled by the verifier. The runtime for their prototype ranges from

0.8 millisecond (512-bit DLOG security) to 21.7 milliseconds (1536-bit DLOG security). The IBI scheme used in their implementation is the original BLS-IBI scheme by Kurosawa and Heng [7]. In this regard, as our runtime for all 3 algorithms are similar to the original BLS-IBI, we foresee that our scheme is also a suitable candidate with better security bounds and shorter keys for prototyping in real world applications. Since our scheme uses Type-3 pairing, it is much more secure compared to the original with broken Type-1 pairing [30], [31].

E. FUTURE WORKS

The method we used to prove the security of imp-aa/ca is ad-hoc and we believe there exist better techniques which could lead to even tighter schemes without additional overheads. Another research direction one could take is to perform such security reductions on pairing-free IBI schemes (e.g. Schnorr-based) that will have faster identification runtime.

V. CONCLUSION

This paper proposed an IBI scheme that is based on a variant of the BLS signature scheme, and demonstrated its tight security using the co-computational Diffie-Hellman assumption on Type-3 pairing. The scheme is a leap forward in security compared to the original Kurosawa and Heng's BLS-IBI scheme with tighter security against active and concurrent attackers and with weaker assumptions. Being the first IBI scheme to use the Multi-Instance Reset Lemma, we show that the presented scheme has improved security guarantees for concurrent attackers comparing to the existing IBI schemes. While the new scheme has slightly longer run-time, it is shown to be superior in the area of bandwidth efficiency and user key sizes against more recent and sophisticated schemes, rendering it useful in scenarios where storage and bandwidth efficiency is a major concern.

ACKNOWLEDGMENT

The authors would like to first thank the anonymous reviewers for their helpful suggestions to improve the quality of this article. They would also like to thank Dr. S.-C. Yip for pointing out some of the grammatical errors on an earlier version of the manuscript. This work was supported in part by the Ministry of Education of Malaysia through the Fundamental Research Grant Scheme under Grant FRGS/1/2019/ICT04/MMU/02/5, and in part by the Multimedia University's Research Management Fund.

REFERENCES

[1] A. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, 5th ed. Boca Raton, FL, USA: CRC Press, Oct. 1996.
[2] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. New York, NY, USA: Springer-Verlag, 1985, pp. 47–53. [Online]. Available: http://dl.acm.org/citation.cfm?id=19478.19483
[3] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in Cryptology*, A. M. Odlyzko, Ed. Berlin, Germany: Springer, 1987, pp. 186–194.
[4] T. Beth, "Efficient zero-knowledge identification scheme for smart cards," in *Advances in Cryptology*. Berlin, Germany: Springer, 1988, pp. 77–84.
[5] M. Girault, "An identity-based identification scheme based on discrete logarithms modulo a composite number," in *Advances in Cryptology*, I. B. Damgård, Ed. Berlin, Germany: Springer, 1991, pp. 481–486.
[6] M. Bellare and A. Palacio, "GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks," in *Advances in Cryptology*, M. Yung, Ed. Berlin, Germany: Springer, 2002, pp. 162–177.
[7] K. Kurosawa and S.-H. Heng, "From digital signature to ID-based identification/signature," in *Public Key Cryptography*, F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany: Springer, 2004, pp. 248–261.
[8] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," in *Advances in Cryptology*, C. Cachin and J. L. Camenisch, Eds. Berlin, Germany: Springer, 2004, pp. 268–286.
[9] G. Yang, J. Chen, D. S. Wong, X. Deng, and D. Wang, "A new framework for the design and analysis of identity-based identification schemes," *Theor. Comput. Sci.*, vol. 407, nos. 1–3, pp. 370–388, Nov. 2008.
[10] G. D. Crescenzo, "On the security of Beth's identification schemes against active and concurrent adversaries," in *Mathematical Methods in Computer Science*. Berlin, Germany: Springer, Dec. 2008, pp. 1–17.
[11] J.-J. Chin, S.-Y. Tan, S.-H. Heng, and R. C.-W. Phan, "On the security of a modified beth identity-based identification scheme," *Inf. Process. Lett.*, vol. 113, nos. 14–16, pp. 580–583, Jul. 2013.
[12] S.-Y. Tan, S.-H. Heng, R. C. W. Phan, and B.-M. Goi, "A variant of Schnorr identity-based identification scheme with tight reduction," in *Future Generation Information Technology*, T.-H. Kim, H. Adeli, D. Slezak, F. E. Sandnes, X. Song, K.-I. Chung, and K. P. Arnett, Eds. Berlin, Germany: Springer, 2011, pp. 361–370.
[13] A. Fujioka, T. Saito, and K. Xagawa, "Security enhancements by OR-proof in identity-based identification," in *Proc. 10th Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS)*, Singapore, Jun. 2012, pp. 135–152.
[14] K. Kurosawa and S.-H. Heng, "Identity-based identification without random oracles," in *Computational Science and Its Applications*, O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan, Eds. Berlin, Germany: Springer, 2005, pp. 603–613.
[15] G. Yang, C. H. Tan, Y. Mu, W. Susilo, and D. S. Wong, "Identity based identification from algebraic coding theory," *Theor. Comput. Sci.*, vol. 520, pp. 51–61, Feb. 2014.
[16] B. Song and Y. Zhao, "Provably secure identity-based identification and signature schemes with parallel-PVR," in *Proc. 18th Int. Conf. Inf. Commun. Secur. (ICICS)*, Lecture Notes in Computer Science, vol. 9977, K. Lam, C. Chi, and S. Qing, Eds. Singapore: Springer, Nov./Dec. 2016, pp. 227–238, doi: 10.1007/978-3-319-50011-9_18.
[17] J.-J. Chin, S.-Y. Tan, S.-H. Heng, and R. C.-W. Phan, "Twin-Schnorr: A security upgrade for the Schnorr identity-based identification scheme," *Sci. World J.*, vol. 2015, Jan. 2015, Art. no. 237514.
[18] J.-J. Chin, S.-Y. Tan, S.-H. Heng, and R. C.-W. Phan, "Twin-Beth: Security under active and concurrent attacks for the Beth identity-based identification scheme," *Cryptogr. Commun.*, vol. 8, no. 4, pp. 579–591, Oct. 2016.
[19] J.-J. Chin, H. Anada, and S.-Y. Tan, "Reset-secure identity-based identification schemes without pairings," in *Provable Security*, M.-H. Au and A. Miyaji, Eds. Cham, Switzerland: Springer, 2015, pp. 227–246.
[20] M. Bellare, M. Fischlin, S. Goldwasser, and S. Micali, "Identification protocols secure against reset attacks," in *Advances in Cryptology*, B. Pfitzmann, Ed. Berlin, Germany: Springer, 2001, pp. 495–511.
[21] P. Thorncharoensri, W. Susilo, and Y. Mu, "Identity-based identification scheme secure against concurrent-reset attacks without random oracles," in *Information Security Applications*, H. Y. Youm and M. Yung, Eds. Berlin, Germany: Springer, 2009, pp. 94–108.
[22] J. Stern, "A new identification scheme based on syndrome decoding," in *Advances in Cryptology*, D. R. Stinson, Ed. Berlin, Germany: Springer, 1994, pp. 13–21.
[23] P. Cayrel, P. Gaborit, and E. Prouff, "Secure implementation of the stern authentication and signature schemes for low-resource devices," in *Smart Card Research and Advanced Applications* (Lecture Notes in Computer Science), vol. 5189, G. Grimaud and F. Standaert, Eds. London, U.K.: Springer, Sep. 2008, pp. 191–205, doi: 10.1007/978-3-540-85893-5_14.
[24] P. Cayrel, P. Gaborit, and M. Girault, "Identity-based identification and signature schemes using error correcting codes," in *Identity-Based Cryptography* (Cryptology and Information Security Series), vol. 2, M. Joye and G. Neven, Eds. Amsterdam, The Netherlands: IOS Press, 2009, pp. 119–134, doi: 10.3233/978-1-58603-947-9-119.

[25] P. Cayrel, P. Gaborit, D. Galindo, and M. Girault, "Improved identity-based identification using correcting codes," *CoRR*, vol. abs/0903.0069, pp. 1–9, Feb. 2009. [Online]. Available: http://arxiv.org/abs/0903.0069

[26] S. M. El Yousfi Alaoui, P.-L. Cayrel, and M. Mohammed, "Improved identity-based identification and signature schemes using quasi-dyadic Goppa codes," in *Information Security and Assurance*, T.-H. Kim, H. Adeli, R. J. Robles, and M. Balitanas, Eds. Berlin, Germany: Springer, 2011, pp. 146–155.

[27] P. Cayrel and P. Véron, "Improved code-based identification scheme," *CoRR*, vol. abs/1001.3017, pp. 1–5, Jan. 2010. [Online]. Available: http://arxiv.org/abs/1001.3017

[28] N. Fleischhacker, T. Jager, and D. Schröder, "On tight security proofs for Schnorr signatures," Cryptol. ePrint Arch., Int. Assoc. Cryptol. Res., Lyon, France, Tech. Rep. 2013/418, 2013. [Online]. Available: https://eprint.iacr.org/2013/418

[29] T.-S. Ng, S.-Y. Tan, and J.-J. Chin, "A variant of BLS signature scheme with tight security reduction," in *Mobile Networks and Management*, J. Hu, I. Khalil, Z. Tari, and S. Wen, Eds. Cham, Switzerland: Springer, 2018, pp. 150–163.

[30] G. Adj, A. Menezes, T. Oliveira, and F. Rodríguez-Henríquez, "Computing discrete logarithms in F_{36*137} and F_{36*163} using magma," Cryptology ePrint Archive, Tech. Rep. 2014/057, 2014. [Online]. Available: https://eprint.iacr.org/2014/057

[31] R. Granger, T. Kleinjung, and J. Zumbrägel, "Breaking '128-bit secure' supersingular binary curves," in *Advances in Cryptology*, J. A. Garay and R. Gennaro, Eds. Berlin, Germany: Springer, 2014, pp. 126–145.

[32] B. Elaine, *Recommendation for Key Management, Part 1: General*. Washington, DC, USA: U.S. Department of Commerce, 2016.

[33] E. Kiltz, D. Masny, and J. Pan, "Optimal security proofs for signatures from identification schemes," in *Advances in Cryptology*, M. Robshaw and J. Katz, Eds. Berlin, Germany: Springer, 2016, pp. 33–61.

[34] M.-S. Lacharité, "Security of BLS and BGLS signatures in a multi-user setting," *Cryptogr. Commun.*, vol. 10, no. 1, pp. 41–58, Jan. 2018, doi: 10.1007/s12095-017-0253-6.

[35] S. Galbraith, K. Paterson, and N. Smart, "Pairings for cryptographers," Cryptol. ePrint Arch., Int. Assoc. Cryptol. Res., Lyon, France, Tech. Rep. 2006/165, 2006. [Online]. Available: https://eprint.iacr.org/2006/165

[36] J. Katz and N. Wang, "Efficiency improvements for signature schemes with tight security reductions," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, Oct. 2003, pp. 155–164.

[37] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Advances in Cryptology*, C. Cachin and J. L. Camenisch, Eds. Berlin, Germany: Springer, 2004, pp. 56–73.

[38] B. Lynn. (2007). *PBC Library—Pairing-Based Cryptography—About*. [Online]. Available: https://crypto.stanford.edu/pbc/

[39] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E84-A, no. 5, pp. 1234–1243, May 2001.

[40] M. Scott and P. S. L. M. Barreto, "Generating more MNT elliptic curves," *Des., Codes Cryptogr.*, vol. 38, no. 2, pp. 209–217, Feb. 2006.

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

[42] S. Chatterjee, D. Hankerson, and A. Menezes, "On the efficiency and security of pairing-based protocols in the type 1 and type 4 settings," Cryptol. ePrint Arch., Int. Assoc. Cryptol. Res., Lyon, France, Tech. Rep. 2010/388, 2010. [Online]. Available: https://eprint.iacr.org/2010/388

[43] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science), vol. 3897, B. Preneel and S. Tavares, Eds. Berlin, Germany: Springer-Verlag, 2006, pp. 319–331. [Online]. Available: http://cryptojedi.org/papers/#pfcpo

[44] C. Costello, T. Lange, and M. Naehrig, "Faster pairing computations on curves with high-degree twists," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 6056, P. Q. Nguyen and D. Pointcheval, Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 224–242. [Online]. Available: http://cryptojedi.org/papers/#edate

[45] M. Naehrig, R. Niederhagen, and P. Schwabe, "New software speed records for cryptographic pairings," in *Progress in Cryptology* (Lecture Notes in Computer Science), vol. 6212, M. Abdalla and P. S. Barreto, Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 109–123. [Online]. Available: http://cryptojedi.org/papers/#dclxvi

[46] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," in *Proc. Int. Conf. Mach. Intell. Res. Adv. (ICMIRA)*, Dec. 2013, pp. 58–62.

[47] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," *IEEE Access*, vol. 5, pp. 1872–1899, 2017.

[48] S. Boubiche, D. E. Boubiche, A. Bilami, and H. Toral-Cruz, "Big data challenges and data aggregation strategies in wireless sensor networks," *IEEE Access*, vol. 6, pp. 20558–20571, 2018.

[49] G. Cerullo, G. Mazzeo, G. Papale, B. Ragucci, and L. Sgaglione, "Iot and sensor networks security," in *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks* (Intelligent Data-Centric Systems), M. Ficco and F. Palmieri, Eds. New York, NY, USA: Academic, 2018, ch. 4, pp. 77–101.

[50] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2019–2020, Dec. 2003.

[51] D. Florencio and C. Herley, "A large-scale study of Web password habits," in *Proc. 16th Int. Conf. World Wide Web (WWW)*, 2007, pp. 657–666.

[52] J. Bonneau, C. Herley, P. C. V. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 553–567.

[53] T.-Y. Teh, Y.-S. Lee, Z.-Y. Cheah, and J.-J. Chin, "IBI-mobile authentication: A prototype to facilitate access control using identity-based identification on mobile smart devices," *Wireless Pers. Commun.*, vol. 94, no. 1, pp. 127–144, May 2017, doi: 10.1007/s11277-016-3320-y.

[54] Z.-Y. Cheah, Y.-S. Lee, T.-Y. The, and J.-J. Chin, "Simulation of a pairing-based identity-based identification scheme in IOS," in *Proc. IEEE Int. Conf. Signal Image Process. Appl. (ICSIPA)*, Oct. 2015, pp. 298–303.

JASON CHIA (Student Member, IEEE) is currently pursuing the bachelor's degree in electronics engineering majoring in computers with the Faculty of Engineering, Multimedia University.

He was a Research Intern with the NUS-Singtel CyberSecurity Lab, National University of Singapore. He has been working part-time as a Software Developer for security applications. He is involved with a security project under a government-linked agency. He did his final year project under the guidance of Dr. J.-J. Chin from the Faculty of Engineering, Multimedia University. Their work focuses on public key cryptographic schemes. He was a recipient of the Multimedia University's President Scholarship Award and is on the dean's list for the Faculty of Engineering, from 2016 to 2020. He has served as the Vice Chairperson for the Faculty of Engineering's Engineering Society. He was the President of the IET Student Chapter in the Faculty. He was also the Champion of KPMG Malaysia's cyber-tech challenge, in 2019.

JI-JIAN CHIN received the B.Sc. degree *(magna cum laude)* in computer science and computational mathematics from Campbell University, the M.Eng.Sc. degree from the Faculty of Engineering, Multimedia University, specializing in the research area of cryptography, and the Ph.D. degree from the Faculty of Information Science and Technology, Multimedia University.

He is currently serving as a Senior Lecturer with the Faculty of Engineering, Multimedia University. In his research, he has spent close to a decade in researching theoretical public key cryptography, specializing in entity and message authentication schemes, such as identification and digital signature schemes, with particular interest in designing schemes that do not require certificates. Eager to bridge the gap between theoretical cryptography and practical computer security, he currently focuses his research interests on development and implementation projects, such as searchable symmetric encryption and access-control prototypes using mobile devices. He received the Best Thesis Award in I.T. for his thesis.