Article

A Pairing-Free Identity-Based Identification Scheme with Tight Security Using Modified-Schnorr Signatures

Jason Chia ^{1,*}, Ji-Jian Chin ² and Sook-Chin Yip ¹

¹ Faculty of Engineering, Multimedia University, Cyberjaya 63100, Malaysia; scyip@mmu.edu.my

² Faculty of Computing and Informatics, Multimedia University, Cyberjaya 63100, Malaysia; jjchin@mmu.edu.my

* Correspondence: 1161300548@student.mmu.edu.my

Abstract: The security of cryptographic schemes is proven secure by reducing an attacker which breaks the scheme to an algorithm that could be used to solve the underlying hard assumption (e.g., Discrete Logarithm, Decisional Diffie–Hellman). The reduction is considered tight if it results in approximately similar probability bounds to that of solving the underlying hard assumption. Tight security is desirable as it improves security guarantees and allows the use of shorter parameters without the risk of compromising security. In this work, we propose an identity-based identification (IBI) scheme with tight security based on a variant of the Schnorr signature scheme known as TNC signatures. The proposed IBI scheme enjoys shorter parameters and key sizes as compared to existing IBI schemes without increasing the number of operations required for its identification protocol. Our scheme is suitable to be used for lightweight authentication in resource-constrained Wireless Sensor Networks (WSNs) as it utilizes the lowest amount of bandwidth when compared to other state-of-the-art symmetric key lightweight authentication schemes. Although it is costlier than its symmetric key counterparts in terms of operational costs due to its asymmetric key nature, it enjoys other benefits such as decentralized authentication and scalable key management. As a proof of concept to substantiate our claims, we perform an implementation of our scheme to demonstrate its speed and memory usage when it runs on both high and low-end devices.

Keywords: access control; identity-based identification; tight security; provable security

Citation: Chia, J.; Chin, J.-J.; Yip, S.-C. A Pairing-Free Identity-Based Identification Scheme with Tight Security Using Modified-Schnorr Signatures. *Symmetry* **2021**, *13*, 1330. <https://doi.org/10.3390/sym13081330>

Academic Editors: José Carlos R. Alcántud and Kuo-Hui Yeh

Received: 23 June 2021

Accepted: 19 July 2021

Published: 23 July 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Identification or authentication is the act of ensuring the identity of an entity that one is interacting with, is in fact what the entity claims it to be. An identity-based identification (IBI) scheme is an identification scheme with the public key as a publicly identifiable string (i.e., johnsmith@example.com) instead of a random-looking one (i.e., An RSA key). The IBI scheme allows a user to prove the possession of a secret key corresponding to their public identity with a verifier by acquiring corroborative evidence through an interactive protocol [1].

When the public key is publicly identifiable, the scheme enjoys several advantages compared to its random-looking counterparts. This is due to the fact that the keys are no longer needed to be verified or authenticated, as they represent the entity in plain-text. Besides, the storage and transmission bandwidth requirements are also significantly reduced because identity strings are small in comparison (e.g., well known www.google.com of size 14 bytes versus a 2048-bit RSA key of size 256 bytes).

Figure 1 shows the system architecture of an access control system using IBI schemes. Essentially, the key generation center (KGC) acts as the trusted authority which issues user keys corresponding to their public identities. The system then employs authentication servers to verify valid users attempting to access critical resources. Much like the conventional public key infrastructure, the system assumes the existence of a secure trusted

third party [2]. The identity-based access system is able to provide a strong authentication mechanism while keeping operating overhead requirements low.

Figure 1. Overview of an identity-based access control system.

1.1. Motivation

As Internet-of-Things (IoT) devices begin to proliferate the digital landscape in the coming years [3], new challenges such as device authentication using minimal resources (i.e., storage, bandwidth requirements) emerged. Identity-based cryptography is proposed as a primitive to tackle such challenges [4,5].

For example, IoT devices (i.e., sensors in a Wireless Sensor Network (WSN)) can use their MAC address as their public key. In the case where the sensors connect to a gateway before they can push data up to the cloud, the gateway would simply check if the connecting device's MAC address has permission based on the access control policy before running the identity-based cryptographic protocol to perform authentication.

In contrast to conventional public key cryptography, a certificate is first required to validate the authenticity of the MAC address before performing authentication. The key difference is that in identity-based cryptography, the authentication will fail when the identity is not authentic **or** the entity does not have the secret key. In other words, the result of the protocol is mathematically bounded to the identity and its proof of identity (i.e., the secret), which makes it very useful for authentication as it figuratively kills two birds with one stone.

An alternative to address the challenge is to utilize symmetric key cryptography. Recent advances in this field such as an instantiation using only Hash and XOR primitives [6] are very efficient in terms of computation and bandwidth requirements. However, a consistent database of keys and device identities must be maintained and synchronized across the authenticators. It becomes an obstacle in scaling up for Wide Area Network because it is not practical to have a centralized authenticator. In this regard, the properties of identity-based cryptography are desirable as there is no need to consistently update any database even if there are multiple authenticators.

Despite the strengths of identity-based cryptography, the main disadvantage is key revocation. While some may argue that the use of a revocation list or something akin to an Online Certificate Status Protocol (OCSP) service may be put in place to overcome this problem, it brings back the synchronization issues across a vast array of authenticators when dealing with IoT networks. Recent progress in hierarchical identity-based cryptography [7,8] shows that the problem may be alleviated by partitioning the entire network into smaller subnets controlled by a local authority.

Another issue with identity-based cryptography is key escrow. The KGC inherently knows all the user's secrets as it is responsible for generating them, unlike in the conventional public key setting where users could generate their own key-pair and have the public key infrastructure certify their public keys [9].

There are other scenarios in which authentication is not required at the network layer but on the application or other layers. The above scenarios only serve as examples in which identity-based cryptography can pragmatically support the authentication requirements of the expanding networks of IoT devices, which motivates our work in such schemes.

1.2. Related Works

Identity-based cryptosystems were first proposed by Shamir [10], followed by various improvements and enhancements as discussed in [11–14]. The works by Kurosawa and Heng [15], Bellare et al. [16] and Yang et al. [17] added frameworks and transform methods, allowing direct conversion of existentially unforgeable digital signature schemes to an IBI scheme that is secure against *passive* attackers. Despite the advances, proving security against *active* and *concurrent* attackers are proved to be difficult. In 2008, Crescenzo [18] attempted to show security against *active* and *concurrent* attackers for the Beth-IBI scheme. Despite the fact, Chin et al. has pointed out that the scheme suffers from a complete break [19], allowing extraction of the master key from only two hash and corrupt queries in 2013.

In 2011, Tan et al. [20] and Chin et al. [21] in IBI focused on tightening security proofs for schemes. The notion of provable security is to link an adversary which is first thought to be able to break the cryptographic scheme to an adversary that could be used to solve an underlying hard assumption (i.e., factoring large numbers, Computational Diffie–Hellman problem) that are thought to be impractical within a reasonable amount of time. The link is a reduction from one problem to another, while a tight reduction means that the probability of breaking the scheme is close to the probability of solving the hard problem.

There are several advantages to having a security scheme with tight security proofs, most notably, being able to securely use smaller size parameters [22]. In such a case, the storage and bandwidth overheads are reduced while the cryptographic scheme is in place. Meanwhile, some transformation frameworks such as the Kurosawa–Heng transform [15] can convert signature schemes into IBI schemes but the resulting proof is not tight. In 2011, Tan et al. [20] showed a tight security proof on an IBI scheme which uses Schnorr signatures. It is achieved by foregoing usage of both the Reset-Lemma [14] and the stronger interactive one-more assumptions [17], resulting in a tighter bound.

In 2012, Fujioka et al. [23] introduced the use of the OR-proof method in proving security against *active* and *concurrent* attackers. Prior to their proposal, IBI schemes relied on strong interactive assumptions for their security proof which results in weaker security guarantees. The OR-proof allows direct conversion of *passive* security to *active* security without the use of the interactive assumptions and was used by [24,25]. However, the security on active/concurrent secure schemes become reliant on the security of the passive scheme. In other words, the bounds are still loose when compared to a direct reduction to a hard assumption. OR-proofing will also lead to an increase in bandwidth requirements as commit, challenge and response messages are practically doubled.

In 2020, Chia and Chin [26] revisited the use of Boneh–Lynn–Shacham signatures [27] in an IBI scheme. Their proposal runs on Type-3 pairings and has tight security against *active* and *concurrent* attackers. Although their proposed scheme enjoys advantages in terms of key sizes and system parameters, it is nevertheless pairing-based and has a longer identification runtime as compared to pairing-free IBI schemes.

Aside from the three common types of attackers (i.e., *passive*, *active* and *concurrent*), there is a stronger fourth type known as the *reset* attacker. This attacker has the ability to reset a legitimate user up to any state that it desires in the identification protocol, which can easily break IBI schemes that are proven under the Reset Lemma [14]. Chin et al. continued the work of Bellare et al. [28] and Pairat et al. [29] by showing two instances of reset-secure

IBI scheme with existing Schnorr-based IBI scheme [30] in 2015. However, as pointed out by Tan et al. [20], reset attacks can be thwarted through proper implementation by forcing erasure of the committed message before the final response is sent.

One of the main issues with previous schemes such as [15–17] is mainly the use of the interactive One-More assumptions, which is a strong assumption that ultimately results in weak security. While schemes like [21,26] do not rely on One-More assumptions, they require the Reset Lemma [14] in their security proof which effectively halved the security bound due to the square root. These generally meant keys are to be doubled in length (e.g., 128-bit security $\sqrt{2^{-k}} = 2^{-k/2}$, $2^{-128} = 2^{-256/2}$ requires a 256-bit key) to compensate for the looseness in their reduction techniques.

1.3. Our Contribution

In this work, we propose an IBI scheme that is based on a new signature scheme known as TNC signatures designed by Tan et al. [31]. We prove that our construction satisfies *passive* security by showing that the identification protocol is an honest verifier semi zero-knowledge protocol as required by the Kurosawa–Heng transform [15].

We then present a non-trivial proof of security against both *active/concurrent* attackers under the D-square-DH assumption, which is believed to be as hard as the decisional Diffie–Hellman assumption [32]. We manage to avoid the use of One-More assumptions as well as the Reset Lemma, and the resulting scheme enjoys a lesser number of public key components as well as a tighter bound compared to previous pairing-free schemes. Additionally, we present a C/C++ run-time evaluation of our scheme in the form of a library built using the NaCL library (libsodium) [33].

We finally give an analysis of the effectiveness of our scheme in terms of key sizes and computational savings, and subsequently provide suggestions on use-cases for the newly designed scheme both in the context Internet-of-Things (IoT) security and as a suitable alternative for lightweight authentication schemes.

2. Preliminaries

In this work, $\{0, 1\}^k$ is a bit-string of length k , while $\{0, 1\}^*$ is a bit-string of arbitrary length. $r \xleftarrow{\$} \mathbb{S}$ denotes uniformly sampling an element r from a set $\mathbb{S}$. $s \leftarrow (a, b)$ means assigning tuple (a, b) as s while $(a, b) \leftarrow s$ means parsing s to a tuple with elements a and b . q by default implies a prime number and k the security parameter. $\mathcal{P}$ and $\mathcal{V}$ shall represent the prover and the verifier, respectively. $\mathbb{Z}_q$ and $\mathbb{G}$ represent the integers modulo q and a group where the discrete logarithm problem is hard, respectively. *IMP-ATK* is short for an impersonation attack model where $ATK \in \{\text{passive(PA)}, \text{active(AA)}, \text{concurrent(CA)}\}$. $Adv_{IBI, I}^{IMP-ATK}$ is the security of an IBI scheme under *IMP-ATK* against an impersonator I . Finally, C_{MT} , C_{HA} and R_{SP} are, respectively, the commit, challenge and response messages. We denote $\mathcal{A}(x_1, \dots, x_n : o_1, \dots, o_m)$ as algorithm $\mathcal{A}$ running with n inputs $x_1, \dots, x_n$ and has access to m oracles $o_1, \dots, o_m$.

2.1. Identity-Based Identification (IBI)

Definition 1. An IBI scheme consists of four probabilistic polynomial-time algorithms, $\mathcal{IBI} = (\text{MKGen}, \text{UKGen}, \text{PROVE}, \text{VERIFY})$. The specification and functionality of the 4 algorithms are described as follows:

- $\text{MKGen}(1^k)$: Takes in a security parameter 1^k , outputs a master secret-key (msk) and a corresponding master public-key (mpk). msk is to be securely kept while mpk may be freely distributed to the provers and verifiers.
- $\text{UKGen}(\text{msk}, \text{ID})$: Takes in msk and a publicly verifiable identity string (ID), outputs a user key (uk) corresponding to ID . The uk contains a secret and public part, which are used by users to identify themselves with their public identity ID during the identification protocol.
- $\text{PROVE}(st, mi)$: This interactive algorithm is run by a prover $\mathcal{P}$ with inputs state information (st) and an incoming message string (mi) from a verifier $\mathcal{V}$. It produces updated state infor-

mation (st') for its next invocation and an outgoing message string (mo) to be sent to $\mathcal{V}$. st initially consists of mpk , ID and uk .

- **VERIFY(st, mi):** This interactive algorithm is run by a verifier $\mathcal{V}$ with inputs state information (st) and an incoming message string (mi) from a prover $\mathcal{P}$. It produces updated state information (st') for its next invocation and an outgoing message string (mo) to be sent to $\mathcal{P}$. st initially consists of mpk and ID . At some point, mo is the decision of the interaction that is either **accept** for legitimate provers and **reject** otherwise.

We use the notation similarly to Bellare's [16]:

$$(\mathcal{T}, d) \leftarrow \mathcal{P}(p_1, \dots, p_n : OP_1, \dots, OP_n) \leftrightarrow \mathcal{V}(v_1, \dots, v_m : OV_1, \dots, OV_m)$$

to denote an interaction between prover $\mathcal{P}$ and verifier $\mathcal{V}$ using a Sigma protocol. The interaction between $\mathcal{P}$ and $\mathcal{V}$ ends when $\mathcal{V}$ outputs accept or reject obtained from the VERIFY interactive algorithm. The results of the interaction are a transcript $\mathcal{T}$ which can be parsed as a tuple $(C_{MT}, C_{HA}, R_{SP}) \leftarrow \mathcal{T}$ and a decision coin d , where $d = 1$ when $\mathcal{V}$ accepts $\mathcal{P}$'s claim of identity ID , and 0 otherwise. We say $\mathcal{T}$ is an acceptable transcript on ID if $d = 1$. A sigma protocol may satisfy the honest-verifier semi zero-knowledge as defined under Definition 2.

Definition 2. A Sigma protocol is honest-verifier semi zero-knowledge if it satisfies Completeness, Special Soundness and Honest-Verifier Zero-Knowledge.

Completeness. For any legitimate prover $\mathcal{P}$ and honest verifier $\mathcal{V}$,

$$\Pr[(\mathcal{T}, d) \leftarrow \mathcal{P}(\cdot) \leftrightarrow \mathcal{V}(\cdot) : d = 1] = 1$$

Special Soundness. For any two acceptable transcripts $\mathcal{T}_1, \mathcal{T}_2$ with $C_{MT_1} = C_{MT_2}$ and $C_{HA_1} \neq C_{HA_2}$, the user secret key (usk) can be computed efficiently.

Honest-Verifier Zero-Knowledge. There exists a simulator $\mathcal{S}$ with no knowledge of any secrets (i.e., msk, uk) but could generate transcripts with itself such that

$$\Pr[(\mathcal{T}, d) \leftarrow \mathcal{S}(\cdot) \leftrightarrow \mathcal{S}(\cdot) : d = 1] = 1$$

The last property implicates that the transcript leaks no additional knowledge due to the fact that it could entirely be simulated without a priori on any secrets.

2.2. Security Model for IBI

An IBI scheme is considered broken if an adversary (i.e., impersonator) successfully tricks $\mathcal{V}$ in accepting the transcript produced from the identification protocol with non-negligible probability. The goal of an attacker is impersonation *IMP* and there are traditionally 3 types of attacks which are *passive*(PA), *active*(AA) and *concurrent*(CA) attacks. We adopt the security requirements of an IBI scheme based on the works of Bellare et al. [16] as a game between adversary $\mathcal{A}$ and challenger $\mathcal{C}$ shown in Figure 2, where $\mathcal{A}$ wins if the result of the game is 1 and lose otherwise. There are two phases in the game. In the first phase, $\mathcal{A}$ gets to accumulate information and prepare for impersonation on an identity string that it desires (ID^*). Meanwhile, in the second phase, it has to impersonate ID^* successfully. It is obvious that ID^* cannot have its user key corrupted by $\mathcal{A}$ or the game would be pointless, since $\mathcal{A}$ would always win in phase 2, Therefore, $\mathcal{C}$ will check for corruption of ID^* after phase 1. Intuitively, an IBI scheme that is secure against *active/concurrent* attacks is also secure against *passive* attacks as *passive* attacks are inherently weaker.

<p style="text-align: center;">Security game between $\mathcal{A}$ and $\mathcal{C}$ for $IMP\text{-}ATK$, $Exp_{IBI,I}^{IMP\text{-}ATK}$</p> <p>Input: $\mathcal{C}$ receives security parameter k.</p> <p>Game:</p> <pre> 1: $(msk, mpk) \xleftarrow{\\$} \text{MKGen}(1^k)$; 2: $LU \leftarrow \emptyset$; $CU \leftarrow \emptyset$; $RU \leftarrow \emptyset$ $\triangleright$ Initialize Legal, Corrupted and Running Users 3: if $ATK == PA$ then $ORAC \leftarrow TRANS$ else $ORAC \leftarrow IDENT$ 4: $(ID^*, st) \leftarrow \mathcal{A}(1^k, mpk : CORR, ORAC)$ $\triangleright$ Run $\mathcal{A}$ (phase 1) 5: if $ID^* \in CU$ then return 0 $\triangleright$ Fail if corrupted ID^* 6: $(\mathcal{T}, d) \leftarrow \mathcal{A}(st : CORR, ORAC) \leftrightarrow \mathcal{C}(mpk, ID^*)$ $\triangleright \mathcal{A}$ prove ID^* (phase 2) 7: return d </pre>	
<p><u>Oracles.</u></p> <p>Oracle for Corruption: $CORR(ID \in \{0, 1\}^*)$</p> <pre> 1: if $ID == ID^*$ then return $\perp$ $\triangleright ID^*$ is target ID in phase 2 2: if $ID \in CU$ then 3: return $\perp$ $\triangleright ID$ is already corrupted. 4: else 5: if $ID \notin LU$ then $LU[ID] \leftarrow \text{UKGen}(msk, ID)$ 6: $CU \leftarrow CU \cup \{ID\}$ $\triangleright ID$ is now corrupted 7: return $uk_{ID} \leftarrow LU[ID]$ 8: end if </pre> <p>Oracle for Transcript: $TRANS(ID \in \{0, 1\}^*)$</p> <pre> 1: if $ID \notin LU$ then $LU[ID] \leftarrow \text{UKGen}(msk, ID)$ 2: $uk_{ID} \leftarrow LU[ID]$ 3: return $\mathcal{T} \leftarrow \mathcal{P}(mpk, ID, uk_{ID}) \leftrightarrow \mathcal{V}(mpk, ID)$ </pre> <p>Interactive Oracle for Identification: $IDENT(ID \in \{0, 1\}^*, i, mi)$</p> <pre> 1: if $ID \notin LU$ then $LU[ID] \leftarrow \text{UKGen}(msk, ID)$ 2: $uk_{ID} \leftarrow LU[ID]$ 3: if $ID \notin RU$ then 4: if $ATK == AA$ then $RU \leftarrow \{(ID, i)\}$ 5: if $ATK == CA$ then $RU \leftarrow RU \cup \{(ID, i)\}$ 6: $St[ID, i] \leftarrow (mpk, ID, uk_{ID})$ 7: end if 8: $(St[ID, i], mo) \leftarrow \text{PROVE}(St[ID, i], mi)$ 9: return mo </pre>	

Figure 2. A Security Game between $\mathcal{A}$ and $\mathcal{C}$.

Lemma 1. The security of an IBI scheme is defined by the advantage of the adversary in the security game as described in Figure 2 for all types of attacks. The advantage of an impersonator I is defined in Equation (1).

$$Adv_{IBI,I}^{IMP\text{-}ATK}(k) = \Pr[Exp_{IBI,I}^{IMP\text{-}ATK} = 1], \quad (1)$$

where k is the security parameter.

Definition 3. An IBI is said to be $t, q_C, Adv_{IBI,I}^{IMP-ATK}(k)$ -secure against IMP-ATK when the advantage for all polynomial-time I , $Adv_{IBI,I}^{IMP-ATK}(\cdot)$ is negligible. q_C is the number of queries made to the corruption oracle.

2.3. Complexity Assumptions

Definition 4. The Decisional Square Diffie–Hellman assumption (D-Square-DH). Given (g, g^a, g^c) , decide if $g^c \stackrel{?}{=} g^{a^2}$ by returning 1 if yes and 0 otherwise. The advantage of an adversary A running in time t is:

$$Adv_{\mathbb{G}}^{DSDH} := |Pr[a \xleftarrow{\$} \mathbb{Z}_q : A(g, g^a, g^{a^2}) = 1] - Pr[a, c \xleftarrow{\$} \mathbb{Z}_q : A(g, g^a, g^c) = 1]| \quad (2)$$

$A(t, Adv_{\mathbb{G}}^{DSDH})$ -breaks the assumption if the above probability is non-negligible. The D-Square-DH assumption states that no adversary running under polynomial-time t can break D-Square-DH. The D-Square-DH assumption was studied by Bao et al. [32].

3. Construction of the Scheme

In this work, we propose a construction of an IBI scheme by using the TNC digital signature scheme by Tan et al. [31,34] (i.e., Tan–Ng–Chin signature).

3.1. TNC Digital Signature

The TNC signature scheme is a digital signature scheme that reduces to the D-square-DH assumption with tight security [31,34]. We recap the 3 main algorithms in the TNC signature scheme in the algorithms shown in Figure 3.

<u>TNC.KeyGen(1^k)</u>	<u>TNC.Sign(pk, m, sk)</u>
1. $g \xleftarrow{\$} \mathbb{G}$	1. $r \xleftarrow{\$} \mathbb{Z}_q$;
2. $a \xleftarrow{\$} \mathbb{Z}_q$	2. $U \leftarrow g^r$
3. $y_1 \leftarrow g^a$	3. $V \leftarrow y_1^r$
4. $y_2 \leftarrow g^{a^2}$	4. $x \leftarrow H(m, U, V)$
5. select $H : \{0, 1\}^* \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q$	5. $s \leftarrow r + xa$
6. $pk \leftarrow (g, y_1, y_2, \mathbb{G}, H)$	6. return $\sigma \leftarrow (s, x)$
7. $sk \leftarrow a$	
8. return (pk, sk)	
<u>TNC.Verify(pk, m, σ)</u>	
1. $U' \leftarrow g^s \cdot y_1^{-x}$	
2. $V' \leftarrow y_1^s \cdot y_2^{-x}$	
3. $x' = H(m, U', V')$	
4. if $x = x'$	
5. return 1	
6. else	
7. return 0	

Figure 3. The 3 algorithms of the TNC signature scheme.

A valid signature can always be verified correctly because Equation (3) holds for the right s, x values. Notice that this will fail for all s, x when $y_2 = g^c \neq g^{aa}$, except for a specific case of $x = \frac{a(s-r)}{c}$ which has a negligible probability of occurring at $1/q$:

$$\begin{aligned}
x' &= H(M, U', V') \\
&= H(M, g^s \cdot y_1^{-x}, y_1^s \cdot y_2^{-x}) \\
&= H(M, g^s \cdot g^{-ax}, g^{as} \cdot g^{-aax}) \\
&= H(M, g^{s-ax}, g^{a(s-ax)}) \\
&= H(M, g^r, g^{ar}) \\
&= H(M, U, V) \\
&= x
\end{aligned} \tag{3}$$

We show that TNC digital signature has a Sigma protocol that satisfies honest verifier semi zero-knowledge, which can result in IBI schemes that are secure against IMP-PA attacks via the Kurosawa–Heng transform. Our proposed protocol is shown in Figure 4.

Theorem 1. *The identification protocol shown in Figure 4 is an honest verifier zero-knowledge protocol with the challenges sampled from the finite field of prime order q .*

Proof. We show that the protocol satisfies *Completeness*, *Special Soundness* and *Honest-Verifier Zero-Knowledge*.

Completeness is proved by showing that a $\mathcal{P}$ with valid σ is able to prove itself to $\mathcal{V}$ successfully. To see why, Equation (4) which is the verifying equation in step 4 of the protocol holds when $\mathcal{P}$ indeed possess a valid σ . In fact, the key equation is equivalent to Equation (3) because if $\mathcal{V}$ could not compute x correctly (i.e., $H(M, U, V) \neq H(M, U', V')$), Equation (4) will not hold.

$$\begin{aligned}
T(U' \cdot y_1^x)^c &= g^t(g^s \cdot y_1^{-x} \cdot y_1^x)^c \\
&= g^t(g^s)^c \\
&= g^{t+cs} \\
&= g^e
\end{aligned} \tag{4}$$

Special Soundness is proved with the help of two acceptable conversations 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 the secret part of uk , s can be computed following Equation (5).

$$\begin{aligned}
\frac{(R_{SP_1} - R_{SP_2})}{(C_{HA_1} - C_{HA_2})} &= \frac{(t + c_1s - t - c_2s)}{(c_1 - c_2)} \\
&= \frac{s(c_1 - c_2)}{(c_1 - c_2)} \\
&= s
\end{aligned} \tag{5}$$

Honest-Verifier Zero-Knowledge is proved by showing a simulator S that is capable of simulating a valid conversation (C_{MT}, C_{HA}, R_{SP}) . S first samples $e, c, r \xleftarrow{\$} \mathbb{Z}_q$, then sets $U' = g^r$, $V' = y_1^r$ and computes $x' = H(ID, U', V')$ as well as $T = g^e / (U' \cdot y_1^{x'})^c$. Finally, it outputs an acceptable transcript: $((U', V', T), c, e)$. $\square$

3.2. TNC Identity-Based Identification (TNC-IBI)

We now apply the Kurosawa–Heng transform by converting KeyGen and Sign to MKGen and UKGen as shown in Figure 4. The message m is turned into the publicly verifiable string ID . The public key pk is the system parameters mpk or $params$ while sk denotes the master secret key msk . The signature on ID is thus the user key uk , and s is the secret part whilst x is the public part. The protocol shown in Figure 4 is the identification protocol.

Figure 4. The 2 algorithms and the identification protocol of the TNC-IBI scheme. Note that the verifier is able to compute the public part of the user key $H(ID, U, V) = x = x' = H(ID, U', V')$ with the ID of the prover and U', V' obtained from C_{MT} .

3.3. Security against Passive Attackers

Lemma 2. The IBI scheme with an honest-verifier zero-knowledge protocol that satisfies completeness, soundness and honest-verifier zero-knowledge implies that it satisfies IMP-PA security based on the Kurosawa–Heng transform [15].

3.4. Security against Active and Concurrent Attackers

We stress that the Kurosawa–Heng transform is **insufficient** to show security against IMP-AA/CA attacks. We show an ad hoc proof satisfying our security model defined under Section 2.2.

Theorem 2. The IBI scheme presented in Section 3.2 is $(t, q_C, \text{Adv}_{\text{IBI}, I}^{\text{IMP-ATK}})$ -secure against IMP-AA/CA in the random oracle model, as computed in Equation (6).

$$\text{Adv}_{\text{IBI}, I}^{\text{IMP-ATK}} \leq \text{Adv}_{\mathbb{G}}^{\text{DSDH}} - \frac{q_C + 1}{q}, \quad (6)$$

where time t is bounded by polynomial and q_C is the number of corrupt queries.

Proof. By proof of contradiction, an adversary which breaks D-Square-DH within polynomial-time does not exist. We show that an adversary that breaks the IBI scheme as shown in

Section 3.2 could be reduced to one that solves D-square-DH. We construct a simulator S which runs the impersonator I and subsequently show S can use I within the context of an IBI scheme to solve D-square-DH. Thus, any polynomial-time I to our scheme could not exist based on the hardness of the D-square-DH assumption. S first receives the D-square-DH problem (g, g^a, g^c) and must output 1 if $g^c = g^{a^2}$ and 0 otherwise. S sets $y_1 = g^a, y_2 = g^c$ and $mpk \leftarrow (g, y_1, y_2)$ with H modeled as a random oracle that takes 3 inputs $H : \{0, 1\}^* \times \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{Z}_q$. S also initializes sets $LU \leftarrow \emptyset; CU \leftarrow \emptyset; RU \leftarrow \emptyset$ for bookkeeping. Note that S does not know the secret a . In phase 1, S runs I with the inputs $1^k, mpk$ and the oracles as defined by the security game under Figure 2. S then answers oracle queries from I as described in Figure 5.

Initialization for Legal User: INIT(ID $\in \{0, 1\}^*$)

```

1: if ID  $\notin LU$  then
2:    $s, e \xleftarrow{\$} \mathbb{Z}_q$ 
3:    $U \leftarrow g^s \cdot y_1^{-e}; V \leftarrow y_1^s \cdot y_2^{-e}$ 
4:    $x \leftarrow H(\text{ID}, U, V)$ 
5:    $LU[\text{ID}] \leftarrow (s, x)$ 
6: end if
7: return  $uk_{\text{ID}} \leftarrow LU[\text{ID}]$ 

```

Oracle for Corruption: CORR(ID $\in \{0, 1\}^*$)

```

1: if ID == ID* then return  $\perp$                                  $\triangleright$  ID* is target ID in phase 2
2: if ID  $\in CU$  then return  $\perp$                                  $\triangleright$  ID is already corrupted
3:  $CU \leftarrow CU \cup \{\text{ID}\}$                                  $\triangleright$  ID is now corrupted
4: return  $uk_{\text{ID}} \leftarrow \text{INIT}(\text{ID})$ 

```

Interactive Oracle for Identification: IDENT(ID $\in \{0, 1\}^*, i, mi$)

```

1: if ID  $\notin LU$  then  $LU[\text{ID}] \leftarrow \text{UKGen}(msk, \text{ID})$ 
2:  $uk_{\text{ID}} \leftarrow LU[\text{ID}]$ 
3: if ID  $\notin RU$  then
4:   if ATK == AA then  $RU \leftarrow \{(\text{ID}, i)\}$ 
5:   if ATK == CA then  $RU \leftarrow RU \cup \{(\text{ID}, i)\}$ 
6:    $St[\text{ID}, i] \leftarrow (mpk, \text{ID}, uk_{\text{ID}})$ 
7: end if
8:  $(St[\text{ID}, i], mo) \leftarrow \text{PROVE}(St[\text{ID}, i], mi)$ 
9: return  $mo$ 

```

Figure 5. Oracles for Active/Concurrent Impersonation. $\{0, 1\}^*$ denotes a bitstring of arbitrary length.

Once phase 1 is over, I is ready. It will present itself ready to impersonate on ID^* where $\text{ID}^* \notin CU$. S and I play the role as the verifier $\mathcal{V}$ and prover $\mathcal{P}$, respectively. Finally, S receives the transcript (U^*, V^*, T, c, e) . S is able to solve the D-square-DH problem because Equation (7) holds when $g^c = g^{a^2}$. Those who doubt this may refer back to Equation (3) to see why.

$$H(\text{ID}^*, U^*, V^*) \stackrel{?}{=} x \quad (7)$$

Consider the case that the D-square-DH tuple was indeed $g^c = g^{a^2}$, then S answers all queries correctly with no chance to abort. Although one may argue that S could abort if a hash collision occurs during the corrupt queries, this problem is eliminated as the corrupt

query is programmed such that the same ID will always have the same uk . Because we assume I breaks the IBI scheme, the transcript is always valid for the case of $y_2 = g^c = g^{a^2}$ and thus S outputs 1 correctly to the D-square-DH problem.

For the case that the D-square-DH tuple is such that $g^c \neq g^{a^2}$, the transcript would *generally* be invalid and S would answer 0 correctly to the D-square-DH problem. There is, however, a negligible probability of $1/q$ causing Equation (7) to be valid when $x = \frac{a(s-r)}{c}$. This could happen on every invocation to the corrupt query or during verification of transcript in Phase 2, which means there are $q_C + 1$ chances of outputting 1 wrongly to the D-square-DH problem. Therefore, there is a probability of $\frac{q_C+1}{q}$ for S to fail at solving D-square-DH. The total probability that S solves D-square-DH successfully is bounded by Equation (8).

$$\begin{aligned} Pr[S \text{ wins}] &= Pr[I \text{ impersonates}] \\ &\quad - Pr[S \text{ abort if } g^c = g^{aa}] \\ &\quad - Pr[S \text{ not abort if } g^c \neq g^{aa}] \\ Adv_{\mathbb{G}}^{DSDH} &\geq Adv_{IBI,I}^{IMP-ATK} - 0 - \frac{(q_C + 1)}{q} \end{aligned} \quad (8)$$

□

3.5. On the Strong Unforgeability of the Underlying Signature Scheme

The TNC signature scheme is under a stronger security notion known as strong unforgeability [31]. In the strong unforgeability model, the forger is allowed to use a message m^* that was previously queried to the forgery oracle as a challenge but cannot submit a signature previously obtained from a forgery oracle [35]. This security notion guarantees that the signatures are non-malleable and any valid signatures must originate from an honest party. Counter-intuitively, this increased security on the signature scheme does not provably increase the security of this IBI scheme based on the following rationale:

1. Suppose the impersonator obtains (ID, uk_{ID}) from a corrupt query on ID. It then manages to perform forgery on ID to obtain (ID, uk'_{ID}) where $uk_{ID} \neq uk'_{ID}$ such that uk'_{ID} can be used to produce an acceptable transcript on ID with an honest verifier.
2. While the impersonator has broken the strong unforgeability of the signature scheme, it cannot be used to break the IBI scheme. This is because once an ID is queried to the corrupt oracle, it can no longer be used as the challenge ID*.

This realization highlights the contextual difference in the importance of malleability in digital signatures and user keys in IBI schemes. Digital signatures can be made public and should therefore be non-malleable while user keys in IBI are kept secret. Even when an attacker gained illegal access to the user keys, there is no motive to alter it to a different key that still works. If the key is valid, it will help the prover (impersonator or not) convince the honest verifier irrespective of how someone got it.

4. Discussion and Analysis

In this section, we compare our work with existing pairing-free IBI schemes. Note that we do not consider pairing-based IBI schemes in our comparison analysis such as the new IBI scheme from [26] to maintain fairness since pairing operations are more complex and have higher operational costs compared to pairing-free schemes. Our calculations are computed based on the 256-bit security as recommended by NIST [36]. We use 256 bits for integers $|\mathbb{Z}_q|$ and elliptic curve points and 3072 bits for discrete logarithm group sizes $|\mathbb{G}|$.

4.1. Security, Storage and Bandwidth Efficiency

Table 1 shows the comparison of TNC-IBI (this work) with other existing pairing-free IBI schemes. Comparatively, TNC-IBI has the tightest security when bounded against a hard problem for a limited number of corrupt queries. While Schnorr-IBI [15] may appear

to have a tight bound, it is reliant on the security of Schnorr signatures which is a stronger assumption compared to the weaker hard problem assumptions.

In comparison with the Tight Schnorr–IBI, their bounds can be reduced by $\frac{q_C+1}{q}$ to get the same bounds to that of TNC–IBI if their corrupt queries were programmed such that the same ID will return the same uk to avoid the collision and thus the abort. However, TNC–IBI has the advantage of a smaller mpk size (one $\mathbb{G}$ element). In other words, the proposed scheme has a mpk that could be smaller by up to 3072 bits for finite-field arithmetic over integers implementation and 256 bits for finite-field arithmetic over elliptic curves (i.e., Curve25519) implementation.

In the latest work proposed by [21], the Twin–Schnorr IBI scheme is constructed based on a very weak assumption, whereby the bounds of TNC–IBI are shown to be tighter for a small number of hash queries q_C . The main advantage of TNC–IBI against Twin–Schnorr is the smaller requirement for user key storage, saving one $\mathbb{Z}_q$ component. Our scheme can save up to 256 bits (i.e., one $\mathbb{Z}_q$ element) in uk storage for both finite-field arithmetic over integers $\mathbb{Z}_q$ and elliptic curve-based implementation.

Table 1. Comparison with other pairing-free IBI schemes.

Scheme	Security Bounds	#mpk	#uk	#Prot. BW
Schnorr–IBI (2004) [15]	$Adv_{Schnorr,F}^{ss-cma} + \frac{1}{q}$	$2\mathbb{G}$	$2\mathbb{Z}_q$	$2\mathbb{G} + 2\mathbb{Z}_q$
Schnorr–IBI-B (2004) [16]	$\sqrt{Adv_{q,M}^{DLOG}} + \sqrt{Adv_{OKCL}^{ss-cma}} + \frac{3}{\sqrt{q}}$	$2\mathbb{G}$	$2\mathbb{Z}_q$	$3\mathbb{G} + 2\mathbb{Z}_q$
Tight–Schnorr (2011) [20]	$Adv_{q,M}^{DDH} + \frac{2(q_C+1)}{q}$	$4\mathbb{G}$	$2\mathbb{Z}_q$	$3\mathbb{G} + 2\mathbb{Z}_q$
Twin–Schnorr (2015) [21]	$\sqrt{Adv_{q,M}^{DLOG}} + \frac{1}{q} + \frac{1}{q}$	$3\mathbb{G}$	$3\mathbb{Z}_q$	$2\mathbb{G} + 3\mathbb{Z}_q$
TNC–IBI (This work)	$Adv_{q,M}^{DSDH} + \frac{(q_C+1)}{q}$	$3\mathbb{G}$	$2\mathbb{Z}_q$	$3\mathbb{G} + 2\mathbb{Z}_q$

Prot. BW—Protocol bandwidth measured per session; $Adv_{Schnorr}^{ss-cma}$ —chosen message attack security of Schnorr signature scheme (see [37]); Adv_{OKCL}^{ss-cma} —chosen message attack security of Okamoto signature scheme (see [38]); $Adv_{q,M}^{DLOG}$ —security of discrete logarithm in prime order group of size q ; $Adv_{q,M}^{DDH}$ —security of decisional Diffie–Hellman in prime order group of size q .

4.2. With Storage Variant

To further lower TNC–IBI bandwidth, the commit messages can be shortened from (U', V', T) to just T itself. This requires that the verifier maintains a database with tuples (ID, U', V') . Effectively, the total bandwidth size per session is reduced to $\mathbb{G} + 2\mathbb{Z}_q$, totaling up to 3584 bits on finite-field arithmetic over integers and 768 bits on finite-field arithmetic over elliptic curves implementations. This idea mimics the symmetrical lightweight authentication schemes [6], which maintains a symmetric key database containing the authentication containing the authentication information of the sensors on the verifiers.

4.3. Identification Runtime Efficiency

Table 2 shows the number of operations required to perform identification for the pairing-free IBI schemes. If the precomputation for parts of the commit message C_{MT} is factored in, our proposed scheme has the same or a lesser amount of operations in comparison to Tight–Schnorr and Twin–Schnorr. Particularly, our scheme outperforms Twin–Schnorr by 2 exponentiation and 2 multiplication in $\mathbb{G}$, 1 multiplication and 1 addition in $\mathbb{Z}_q$. This is because the values U' and V' in the protocol under Figure 4 can be precomputed and stored without introducing additional storage overhead to the prover $\mathcal{P}$ as the mpk values y_1 and y_2 are no longer needed to be stored. Similar optimizations can also be made for Twin–Schnorr to gain storage efficiency for 1 $\mathbb{Z}_q$ element.

Table 2. #Op. needed during identification.

Scheme	Exp. $\mathbb{G}$	Mult. $\mathbb{G}$	Mult. $\mathbb{Z}_q$	Add. $\mathbb{Z}_q$
Schnorr–IBI (2004)	4 + (2)	2 + (1)	1	1
Schnorr–IBI-B (2004)	4 + (1)	2 + (0)	1	1
Tight–Schnorr (2011)	4 + (4)	2 + (2)	1	1
Twin–Schnorr (2015)	6 + (3)	4 + (2)	2	2
TNC–IBI (This work)	4 + (4)	2 + (2)	1	1

Op. Operations; Exp. Exponentiation; Mult. Multiplication; Add. Addition. The operation counts in brackets () can be omitted for comparison as their output can be precomputed and stored.

The above improvement only benefits the PROVE algorithm. For optimization on the VERIFY algorithm, we notice that during step 4. of the identification protocol, the right-hand side equation of the final check equation can be independent of the R_{SP} message sent by $\mathcal{P}$ in the last pass, and therefore can utilize Out-of-Order execution. VERIFY can first compute the right-hand side while waiting for PROVE to finish computing the R_{SP} , effectively speeding up the final step as it only needs to perform one exponentiation in $\mathbb{G}$ and an equality check.

4.4. Use-Cases for TNC–IBI

Like other identity-based schemes, TNC–IBI has the advantage of a publicly identifiable public key. Signatures on public keys are not needed. TNC–IBI is particularly suitable for environments where there is difficulty in establishing a trusted public key infrastructure (i.e., disaster-struck regions, memory-constrained environments). Therefore, our proposed scheme is more suitable for networks with scarce bandwidth and computing resources. With the advent of Wireless Sensor Networks (WSNs) along with the rise of the Internet of Things (IoT), various works [39–42] raised concerns for security challenges in WSNs. We foresee that our proposed scheme will be part of the solution to the problems raised.

For example, the gateway nodes for WSNs can run the verification algorithm against a sensor that pushes data to the cloud. The vendors or manufacturers of the sensor nodes can thus be the respective key generation center for each sensor, using devices with a Physical Unclonable Function (PUF) to store the user key. To ensure only authorized sensor nodes are sending data through the gateway, the sensors may be infrequently requested to run the identification protocol to ensure that communication with the sensor nodes is not hijacked. As TNC–IBI has the shortest key sizes and the least number of operations required during identification, it is, therefore one of the most suitable asymmetric authentication candidates for WSNs as compared to other schemes for asymmetric lightweight authentication.

Most lightweight authentication schemes catered for WSNs are designed based on symmetric key cryptography [6,43,44] (i.e., the gateway and the sensor nodes share a secret). We argue that even though that asymmetric key cryptography is generally more computationally costly than symmetric cryptography, TNC–IBI is still an attractive alternative due to the following reasons:

- Low bandwidth requirements. Referring to Table 3, TNC–IBI has low bandwidth requirements compared to other symmetric-based alternatives mainly due to the use of Curve25519. While TNC–IBI only authenticates the prover as opposed to mutual authentication, it is sufficient for the use-case of WSNs. It is because the cost-benefit trade-off of impersonating as sensor node (i.e., low cost, but gains access to the edge network, pushing malicious data/code to cloud) far outweighs that of impersonating as a gateway (i.e., high cost, gains access to sensor data).
- Decentralized authentication. Symmetric schemes require a database that stores the symmetric keys and auxiliary information pertaining to the authentication of sensor nodes. Suppose if a network spans across a vast area, multiple gateways would be required which mimics the structure of a cellular network (i.e., LoRaWAN [45] and Narrowband IoT [46]). In this scenario, symmetric schemes would need to relay authentication messages between gateways to a central authenticator or keep a copy

of the database on the gateways. The former option means a high latency during authentication while the latter requires synchronization between the database on the gateways, in which both introduce complexity to the network. TNC-IBI allows for authentication to be decentralized because the gateway would only need to store the master public key without any necessity for updating.

- Scalable key management on authenticators. TNC-IBI has constant storage requirements on the authenticator across any number of sensors deployed in the network even if multiple authenticators are required. For the symmetric based schemes, storage requirements increase linearly with the number of sensors added into the network. While schemes like [6] have a “without-storage” mode which trade-offs some storage for computational and bandwidth requirements, a symmetric key database must still be maintained and its size increases linearly with the number of sensors added into the network.

When a sensor node reaches its end-of-life, the revocation of keys becomes a challenge as the gateways would need to share a synchronized blacklist of MAC addresses. We point out that recent works in hierarchical based IBI schemes [7] can effectively partition each gateway into its local jurisdiction. While converting TNC-IBI to such a hierarchical form may be non-trivial, we believe it is possible.

Table 3. Lightweight authentication scheme comparison.

Scheme: Author, Year	Bandwidth Req. (Bits)
Chen et al., 2018 [44]	2080
Lara et al., 2020 [43]	3072
Braeken, 2020 [6]	
w/ storage	896
w/o storage	1426
(This work)	1280
w/ storage	768
w/o storage	1280

We note that TNC-IBI can sacrifice storage requirements for lower bandwidth too as described in Section 4.2. For a WSN with only a single authenticator (i.e., centralized verifier), TNC-IBI has the shortest bandwidth requirements even among state-of-the-art lightweight authentication schemes. Therefore, for environments where bandwidth is scarce relative to computational power, TNC-IBI is the optimal choice.

Wearable devices also present another use-case for lightweight authentication schemes. A survey by Kumar et al. [47] highlighted the lightweight requirements for wearable devices due to the limited resources available. Here, our proposed scheme is compared with some presented candidate schemes in terms of computing and communication overhead. Table 4 shows the comparison between our proposed scheme and some schemes considered for wearable device security. Since these schemes are designed for mutual authentication, TNC-IBI has to execute identification runs for both the wearable device and the gateway (i.e., smartphone of the user). In such a case, our proposed scheme is still a lightweight protocol for authenticating the various wearable devices owned and worn on a user, while keeping out malicious attackers who attempt to gain access to the user’s home and office network or even their smartphones.

Our proposed scheme can also be used in another scenario known as Zero Interaction Authentication (ZIA) that is introduced by Corner and Noble [48]. ZIA, which utilizes a device known as the token (i.e., IBM Linux wristwatch) to constantly prove the presence of a person to allow access to a resource in a high-security environment. In this scenario, there is an obvious need for an identification protocol that fits nicely to the lightweight storage and protocol bandwidth requirements constrained by the capabilities of the token. These requirements go neatly along with the features of TNC-IBI.

In 2014, Muñoz and Maña proposed a combination of hardware and software approaches for certification [49] for use in cloud computing security monitoring [50–52]. Their proposal allows binding of the hardware certification approaches that are used to certify the bare-metal and the operating system to a software certification approach that is suitable for higher level, dynamic, and highly distributed environments. Instead of using a CA to secure the assert statements during certification, TNC–IBI can be used in-place which eliminates the need for client use-case verification.

Table 4. Wearable authentication device comparison.

Scheme: Author, Year	Comm. (Bits)	Msgs.
Sun 2008 [53]	4512	3
Liu 2016 [54]		
(device pairing)	2528	3
(challenge-response)	1504	4
Liu 2016 [55]	2720	7
(This work)	1280	3

Auth. Authentication; Comm. Communication requirement; Msgs. Number of messages required for authentication.

4.5. Run-Time Evaluation

We performed run-time evaluations on the algorithms MKGen, UKGen, PROVE and VERIFY using finite-field arithmetic over Curve25519, an elliptic curve structure designed by Bernstein et al. [56]. The library `libsodium`, a fork of `NaCl` (Also known as Networking and Cryptography library or its fork, `libsodium`. `NaCl` is a library designed by Bernstein et al. [33] which consist of their original implementation of Curve25519) is used as it comes with `Ristretto`, allowing construction of prime-order elliptic curves using a method known as `decaf` [57].

Table 5 depicts the runtime for the 4 algorithms and their memory usage, which is averaged over 10,000 runs. Memory usage is measured using a popular Linux tool for checking memory leaks known as `Valgrind` [58].

Table 5. Runtime and memory use of TNC–IBI on two different machines.

Algorithm	Runtime (ms)		Heap Usage (Bytes)	
	A	B	A	B
MKGen	0.6870	6.794	83,393	30,609
UKGen	0.5630	6.239	88,138	35,202
PROVE	0.1097	1.380	83,267	30,483
VERIFY	0.2447	4.439	78,546	25,914

A: Intel(R) Core(TM) i7-8750H CPU 2.20 GHz, 6 cores. 64-bit Linux OS. B: RaspberryPi 3B+ ARMv7 Cortex A-53 600 MHz, 4 cores. arm71 Linux OS.

It is observed that the memory use of all 4 algorithms is below 100 kilobytes on the 64-bit Intel machine, and below 40 kilobytes on the ARM CPU machine. The implementation is tested on the Raspberry Pi 3 due to its popularity as both the gateway and node device used by various IoT projects. As mentioned by Petrov et al. [59], there are many examples of use-cases of the credit card-sized computer in IoT. Although a runtime of 4.44 milliseconds for the VERIFY algorithm on machine B may seem huge, service providers can always invest in better hardware to run the verification algorithm as there are generally more provers than verifiers. Aside from that, the optimization for verifiers discussed in Section 4.3 is also relevant in allowing even lower runtimes. The Raspberry Pi computer is a very lightweight device, which is more suitable for function as a prover than a verifier.

5. Future Directions

Due to its suitability as a candidate for lightweight authentication, an extensive analysis of the IBI scheme as a security pattern will reveal better system design principles in the context of security and dependability [60,61].

6. Conclusions

In this work, an IBI scheme based on a later variant of the Schnorr-signature which is secure against passive, active and concurrent attackers is proposed. In addition to having shorter parameters and key sizes, the proposed IBI scheme has tighter security as compared to the latest pairing-free IBI schemes while maintaining similar runtime efficiency in terms of operation count. The scheme is compared with state-of-the-art lightweight authentication schemes in the context of Wireless Sensor Networks. It has a clear advantage in key management and distribution and low bandwidth requirements with the trade-off of higher operational costs due to its asymmetric cryptography setting. A test implementation shows that the newly designed scheme is lightweight and can be easily run on low-end devices. Therefore, it is a natural choice to be used as an asymmetric authentication mechanism for resource-limited systems.

Author Contributions: Conceptualization, J.C. and J.-J.C.; Data curation, J.C.; Formal analysis, J.C. and J.-J.C.; Funding acquisition, J.-J.C.; Investigation, J.C.; Methodology, J.C.; Project administration, J.-J.C.; Resources, J.-J.C.; Software, J.C.; Supervision, J.-J.C. and S.-C.Y.; Validation, J.-J.C. and S.-C.Y.; Visualization, J.C.; Writing—original draft, J.C.; Writing—review & editing, J.C., J.-J.C. and S.-C.Y. All authors have read and agreed to the draft version of the manuscript.

Funding: This work is supported by the Fundamental Research Grant Scheme under the Ministry of Higher Education of Malaysia (FRGS/1/2019/ICT04/MMU/02/5) and in part by Multimedia University's Research Management Fund.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Menezes, A.; Oorschot, P.C.V.; Vanstone, S.A. *Handbook of Applied Cryptography*, 5th ed.; CRC Press: Boca Raton, FL, USA, 1996; pp. 385–424.
2. Canetti, R. Universally Composable Signatures, Certification and Authentication. Cryptology ePrint Archive, Report 2003/239. 2003. Available online: <https://eprint.iacr.org/2003/239> (accessed on 21 February 2021).
3. Cisco. *The Internet of Things Reference Model*; Technical Report; Cisco: San Jose, CA, USA, 2014.
4. Emura, K.; Takayasu, A.; Watanabe, Y. Efficient Identity-Based Encryption with Hierarchical Key-Insulation from HIBE. Cryptology ePrint Archive, Report 2020/1087. 2020. Available online: <https://eprint.iacr.org/2020/1087> (accessed on 21 February 2021).
5. Andersen, M.P.; Kumar, S.; AbdelBaky, M.; Fierro, G.; Kolb, J.; Kim, H.S.; Culler, D.E.; Popa, R.A. WAVE: A Decentralized Authorization Framework with Transitive Delegation. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; USENIX Association: Santa Clara, CA, USA, 2019; pp. 1375–1392.
6. Braeken, A. Highly Efficient Symmetric Key Based Authentication and Key Agreement Protocol Using Keccak. *Sensors* **2020**, *20*, 2160. [CrossRef]
7. Vangujar, A.; Chin, J.; Tan, S.; Ng, T. A Hierarchical Identity-Based Identification Scheme Without Pairing. *Malays. J. Math. Sci.* **2019**, *13*, 93–109.
8. Langrehr, R.; Pan, J. Hierarchical Identity-Based Encryption with Tight Multi-Challenge Security. Cryptology ePrint Archive, Report 2020/146. 2020. Available online: <https://eprint.iacr.org/2020/146> (accessed on 3 March 2021).
9. Bai, Q.H. Comparative research on two kinds of certification systems of the public key infrastructure (PKI) and the identity based encryption (IBE). In Proceedings of the CSQRWC 2012, New Taipei, Taiwan, 23–27 July 2012; pp. 147–150. [CrossRef]
10. Shamir, A. Identity-based Cryptosystems and Signature Schemes. In Proceedings of the CRYPTO 84 on Advances in Cryptology, Santa Barbara, CA, USA, 19–22 August 1984; Springer Inc.: New York, NY, USA, 1985; pp. 47–53.
11. Fiat, A.; Shamir, A. How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Advances in Cryptology—CRYPTO '86*; Odlyzko, A.M., Ed.; Springer: Berlin/Heidelberg, Germany, 1987; pp. 186–194.

12. Beth, T. Efficient Zero-Knowledge Identification Scheme for Smart Cards. In *Advances in Cryptology—EUROCRYPT'88*; Springer: Berlin/Heidelberg, Germany, 1988; pp. 77–84.
13. Girault, M. An identity-based identification scheme based on discrete logarithms modulo a composite number. In *Advances in Cryptology—EUROCRYPT'90*; Damgård, I.B., Ed.; Springer: Berlin/Heidelberg, Germany, 1991; pp. 481–486.
14. Bellare, M.; Palacio, A. GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. In *Advances in Cryptology—CRYPTO'2002*; Yung, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2002; pp. 162–177.
15. Kurosawa, K.; Heng, S.H. From Digital Signature to ID-based Identification/Signature. In *Public Key Cryptography—PKC 2004*; Bao, F., Deng, R., Zhou, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 248–261.
16. Bellare, M.; Namprempre, C.; Neven, G. Security Proofs for Identity-Based Identification and Signature Schemes. In *Advances in Cryptology—EUROCRYPT'2004*; Cachin, C., Camenisch, J.L., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 268–286. [\[CrossRef\]](#)
17. Yang, G.; Chen, J.; Wong, D.S.; Deng, X.; Wang, D. A new framework for the design and analysis of identity-based identification schemes. *Theor. Comput. Sci.* **2008**, *407*, 370–388. [\[CrossRef\]](#)
18. Crescenzo, G.D. On the Security of Beth's Identification Schemes against Active and Concurrent Adversaries. In *Mathematical Methods in Computer Science*; MMICS 2008; Lecture Notes in Computer Science, vol 5393; Springer: Berlin/Heidelberg, Germany, 2008; pp. 1–17. [\[CrossRef\]](#)
19. Chin, J.J.; Tan, S.Y.; Heng, S.H.; Phan, R.C.W. On the security of a modified Beth identity-based identification scheme. *Inf. Process. Lett.* **2013**, *113*, 580–583. [\[CrossRef\]](#)
20. Tan, S.Y.; Heng, S.H.; Phan, R.C.W.; Goi, B.M. A Variant of Schnorr Identity-Based Identification Scheme with Tight Reduction. In *Future Generation Information Technology*; Kim, T.H., Adeli, H., Slezak, D., Sandnes, F.E., Song, X., Chung, K.I., Arnett, K.P., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 361–370. [\[CrossRef\]](#)
21. Chin, J.J.; Tan, S.Y.; Heng, S.H.; Phan, R. Twin-Schnorr: A Security Upgrade for the Schnorr Identity-Based Identification Scheme. *TheScientificWorldJournal* **2015**, *2015*, 237514. [\[CrossRef\]](#) [\[PubMed\]](#)
22. Fleischhacker, N.; Jager, T.; Schröder, D. On Tight Security Proofs for Schnorr Signatures. In *Advances in Cryptology—ASIACRYPT 2014*; Sarkar, P., Iwata, T., Eds.; Lecture Notes in Computer Science, vol 8873; Springer: Berlin/Heidelberg, Germany, 2013. [\[CrossRef\]](#)
23. Fujioka, A.; Saito, T.; Xagawa, K. Security Enhancements by OR-Proof in Identity-Based Identification. In *Proceedings of the Applied Cryptography and Network Security—10th International Conference, ACNS 2012, Singapore, 26–29 June 2012*; pp. 135–152. [\[CrossRef\]](#)
24. Yang, G.; Tan, C.H.; Mu, Y.; Susilo, W.; Wong, D.S. Identity based identification from algebraic coding theory. *Theor. Comput. Sci.* **2014**, *520*, 51–61. [\[CrossRef\]](#)
25. Song, B.; Zhao, Y. Provably Secure Identity-Based Identification and Signature Schemes with Parallel-PVR. In *Proceedings of the Information and Communications Security—18th International Conference, ICICS 2016, Singapore, 29 November–2 December 2016*; Lecture Notes in Computer Science; Lam, K., Chi, C., Qing, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9977, pp. 227–238. [\[CrossRef\]](#)
26. Chia, J.; Chin, J. An Identity Based-Identification Scheme with Tight Security against Active and Concurrent Adversaries. *IEEE Access* **2020**. [\[CrossRef\]](#)
27. Boneh, D.; Lynn, B.; Shacham, H. Short Signatures from the Weil Pairing. *J. Cryptol.* **2004**, *17*, 297–319. [\[CrossRef\]](#)
28. Bellare, M.; Fischlin, M.; Goldwasser, S.; Micali, S. Identification Protocols Secure against Reset Attacks. In *Advances in Cryptology—EUROCRYPT'2001*; Pfitzmann, B., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; pp. 495–511.
29. Thorncharoensri, P.; Susilo, W.; Mu, Y. Identity-Based Identification Scheme Secure against Concurrent-Reset Attacks without Random Oracles. In *Information Security Applications*; Youm, H.Y., Yung, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 94–108.
30. Chin, J.J.; Anada, H.; Tan, S.Y. Reset-Secure Identity-Based Identification Schemes Without Pairings. In *Provable Security*; Au, M.H., Miyaji, A., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 227–246.
31. Ng, T.; Tan, S.; Chin, J. A variant of Schnorr signature scheme with tight security reduction. In *Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 18–20 October 2017*; pp. 411–415. [\[CrossRef\]](#)
32. Bao, F.; Deng, R.H.; Zhu, H. Variations of Diffie-Hellman Problem. In *Information and Communications Security*; Qing, S., Gollmann, D., Zhou, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2003; pp. 301–312.
33. Bernstein, D.J.; Lange, T.; Schwabe, P. The Security Impact of a New Cryptographic Library. In *Progress in Cryptology—LATINCRYPT'2012*; Hevia, A., Neven, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 159–176.
34. *Malaysian Digital Signature Algorithm Proposal: TNC Signature Scheme*; MySEAL AKBA, National Trusted Cryptographic Algorithm List; Cybersecurity Malaysia: Selangor, Malaysia, 2017.
35. Boneh, D.; Shen, E.; Waters, B. Strongly Unforgeable Signatures Based on Computational Diffie-Hellman. In *Public Key Cryptography—PKC 2006*; Yung, M., Dodis, Y., Kiayias, A., Malkin, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 229–240.

36. Elaine, B. *Recommendation for Key Management, Part 1: General*; U.S. Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
37. Schnorr, C. Efficient signature generation by smart cards. *J. Cryptol.* **1990**, *4*, 161–174. [\[CrossRef\]](#)
38. Okamoto, T. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In *Advances in Cryptology—CRYPTO'92, Proceedings of the 12th Annual International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 1992*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1992; Volume 740, pp. 31–53. [\[CrossRef\]](#)
39. Sharma, S. Issues and Challenges in Wireless Sensor Networks. In Proceedings of the 2013 International Conference on Machine Intelligence and Research Advancement (ICMIRA), Katra, India, 21–23 December 2013. [\[CrossRef\]](#)
40. Kobo, H.I.; Abu-Mahfouz, A.M.; Hancke, G.P. A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements. *IEEE Access* **2017**, *5*, 1872–1899. [\[CrossRef\]](#)
41. Boubiche, S.; Boubiche, D.E.; Bilami, A.; Toral-Cruz, H. Big Data Challenges and Data Aggregation Strategies in Wireless Sensor Networks. *IEEE Access* **2018**, *6*, 20558–20571. [\[CrossRef\]](#)
42. Cerullo, G.; Mazzeo, G.; Papale, G.; Ragucci, B.; Sgaglione, L. Chapter 4—IoT and Sensor Networks Security. In *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*; Intelligent Data-Centric Systems; Ficco, M., Palmieri, F., Eds.; Academic Press: Cambridge, MA, USA, 2018; pp. 77–101. [\[CrossRef\]](#)
43. Lara, E.; Aguilar, L.; Sanchez, M.A.; García, J.A. Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices in Industrial Internet of Things. *Sensors* **2020**, *20*, 501. [\[CrossRef\]](#)
44. Chen, C.M.; Xiang, B.; Wu, T.Y.; Wang, F. An Anonymous Mutual Authenticated Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks. *Appl. Sci.* **2018**, *8*, 1074. [\[CrossRef\]](#)
45. Basford, P.J.; Bulot, F.M.J.; Apetroaie-Cristea, M.; Cox, S.J.; Ossont, S.J. LoRaWAN for Smart City IoT Deployments: A Long Term Evaluation. *Sensors* **2020**, *20*, 648. [\[CrossRef\]](#)
46. Nair, K.K.; Abu-Mahfouz, A.M.; Lefophane, S. Analysis of the Narrow Band Internet of Things (NB-IoT) Technology. In Proceedings of the 2019 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 6–8 March 2019; pp. 1–6. [\[CrossRef\]](#)
47. Das, A.K.; Zeadally, S.; Wazid, M. Lightweight authentication protocols for wearable devices. *Comput. Electr. Eng.* **2017**, *63*, 196–208. [\[CrossRef\]](#)
48. Corner, M.; Noble, B. Protecting File Systems with Transient Authentication. *Wirel. Netw.* **2005**, *11*. [\[CrossRef\]](#)
49. Munoz, A.; Mana, A. Software and hardware certification techniques in a combined certification model. In Proceedings of the 2014 11th International Conference on Security and Cryptography (SECRYPT), Vienna, Austria, 28–30 August 2014; pp. 1–6.
50. Muñoz, A.; Maña, A.; González, J. Dynamic Security Properties Monitoring Architecture for Cloud Computing. *Secur. Eng. Cloud Comput.* **2013**, 1–18. [\[CrossRef\]](#)
51. Muñoz, A.; Gonzalez, J.; Maña, A. A Performance-Oriented Monitoring System for Security Properties in Cloud Computing Applications. *Comput. J.* **2012**, *55*, 979–994. [\[CrossRef\]](#)
52. Waller, A.; Sandy, I.; Power, E.; Aivaloglou, E.; Skianis, C.; Muñoz, A.; Maña, A. Policy Based Management for Security in Cloud Computing. In *FTRA International Conference on Secure and Trust Computing, Data Management, and Application*; STA Workshops; Springer: Berlin/Heidelberg, Germany, 2011.
53. Sun, D.Z.; Huai, J.P.; Sun, J.Z.; Zhang, J.; Feng, Z. A New Design of Wearable Token System for Mobile Device Security. *IEEE Trans. Consum. Electron.* **2008**, *54*, 1784–1789. [\[CrossRef\]](#)
54. Liu, S.; Hu, S.; Weng, J.; Zhu, S.; Chen, Z. A novel asymmetric three-party based authentication scheme in wearable devices environment. *J. Netw. Comput. Appl.* **2016**, *60*, 144–154. [\[CrossRef\]](#)
55. Liu, W.; Liu, H.; Wan, Y.; Kong, H.; Ning, H. The Yoking-Proof-Based Authentication Protocol for Cloud-Assisted Wearable Devices. *Pers. Ubiquitous Comput.* **2016**, *20*, 469–479. [\[CrossRef\]](#)
56. Bernstein, D.J. Curve25519: New Diffie-Hellman Speed Records. In *Public Key Cryptography—PKC'2006*; Yung, M., Dodis, Y., Kiayias, A., Malkin, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 207–228.
57. Hamburg, M. Decaf: Eliminating Cofactors through Point Compression. Cryptology ePrint Archive, Report 2015/673. 2015. Available online: <https://eprint.iacr.org/2015/673> (accessed on 12 April 2021).
58. Nethercote, N.; Seward, J. How to Shadow Every Byte of Memory Used by a Program. In Proceedings of the 3rd International Conference on Virtual Execution Environments, San Diego, CA, USA, 13–15 June 2007; Association for Computing Machinery: New York, NY, USA, 2007; pp. 65–74. [\[CrossRef\]](#)
59. Petrov, N.; Dobrilovic, D.; Kavalić, M.; Stanisavljev, S. Examples of Raspberry Pi usage in Internet of Things. In Proceedings of the International Conference on Applied Internet and Information Technologies, Fuzhou, China, 23–25 December 2016; pp. 112–119. [\[CrossRef\]](#)
60. Sánchez-Cid, F.; Maña, A.; Spanoudakis, G.; Kloukinas, C.; Serrano, D.; Muñoz, A. Representation of Security and Dependability Solutions. In *Security and Dependability for Ambient Intelligence*; Kokolakis, S., Gómez, A.M., Spanoudakis, G., Eds.; Springer: Boston, MA, USA, 2009; pp. 69–95. [\[CrossRef\]](#)
61. Serrano, D.; Ruiz, J.; Muñoz, A.; Maña, A.; Armenteros, A.; Gallego-Nicasio, B. Development of Applications Based on Security Patterns. In Proceedings of the 2009 Second International Conference on Dependability, Athens, Greece, 18–23 June 2009. [\[CrossRef\]](#)