University of Plymouth

PEARL **https://pearl.plymouth.ac.uk**

Faculty of Science and Engineering | School of Engineering, Computing and Mathematics

2023-12-14

Malaysian Journal of Mathematical Sciences 17(S): 19–31 (2023)
https://doi.org/10.47836/mjms.17.S.02

Malaysian Journal of Mathematical Sciences

Journal homepage: https://mjms.upm.edu.my

A Pairing-free Provable Secure and Efficient Identity-based Identification Scheme with Anonymity

Kannan, R.[1], Chin, J. J.[2], Goh, V. T.*[1], and Yip, S. C.[1]

[1]*Faculty of Engineering, Multimedia University, Malaysia*
[2]*Faculty of Science and Engineering, University of Plymouth, United Kingdom*

E-mail: vtgoh@mmu.edu.my
**Corresponding author*

Received: 21 June 2022
Accepted: 4 October 2023

Abstract

In this paper, we propose a Blind Identity-Based Identification (Blind IBI) scheme based on the Guillou-Quisquater (GQ) scheme. Our proposed scheme combines the benefits of traditional Identity-Based Identification (IBI) schemes that can authenticate a user's identity without relying on a trusted third party with the Blind Signature (BS) scheme that provides anonymity. As a result, the proposed scheme assures absolute user privacy during the authentication process. It does not rely on a third party, yet the verifier can still be assured of the user's identity without the user actually revealing it. In our work, we show that the proposed scheme is provably secure under the random oracle model, with the assumption that the one-more-RSA-inversion problem is difficult. Furthermore, we demonstrate that the proposed scheme is secure against passive, active, and concurrent impersonation attacks. In conclusion, the proposed scheme is able to achieve the desired blindness property without compromising the security of the GQ-IBI scheme it is based upon.

Keywords: blind GQ-IBI; blind IBI; blind signature; IBI; random oracle model; one-more-RSA inversion problem.

1 Introduction

The current world of the internet uses digital signatures that require certificates issued by trusted third parties for the purposes of verification. This method can be financially costly because it involves the services of a third party. As such, the Identity-based Identification (IBI) schemes were proposed. This class of schemes neither requires third-party certificates nor requires that both parties be online during the verification process. This makes IBI schemes cheaper relative to digital signature schemes.

IBI schemes have been used in various technologies such as facial recognition and smartcards since their introduction. Recently published research works like [13, 2] focus on creating IBI schemes or adapting existing IBI schemes to be used for a wide variety real world applications. With the increasing concern about privacy vulnerabilities, there is a need for the current solutions to be adjusted for an increase in privacy without compromising security. Blind IBI schemes are IBI schemes that have the blindness property thus providing a level of anonymity. In IBI schemes, user identity is public, but in Blind IBI schemes there is an option of obfuscating the user identity for verification. We introduce the first Blind IBI scheme that is provably secure in the random oracle model.

The RSA scheme which was introduced in 1977 is still widely used in the world today with many stable libraries and optimized for old and modern processors. Due to this, we have chosen to base our proposed scheme on RSA. Although RSA has some vulnerabilities shown by [1] and while quantum computing can break RSA, it is still not widely available, thus making the risk low for applications based on the RSA scheme. Even with the risk of quantum computing, our RSA-based scheme is suitable to be deployed in low-risk and low-security areas where speed and efficiency are paramount.

1.1 Definitions

The Guillou-Quisquater (GQ) identification scheme which is based on RSA, is one of the most efficient and best known identification scheme derived from Fiat-Shamir . This work proposes the first Blind Guillou-Quisquater IBI (Blind GQ-IBI) scheme that has the properties of both blind signature and IBI schemes. Our Blind GQ-IBI scheme is provably secure in the Random Oracle Model.

A Blind Signature (BS) scheme is a type of digital signature scheme where the message is blinded, preventing the signer from knowing the content of the message being signed. Similar to a digital signature system, a probabilistic algorithm (Gen) is used to produce parameters p, q, e, d, and N. These parameters satisfy the equations $N = p \times q$, $\phi(N) = (p-1)(q-1)$, and $e \times d = 1 \mod \phi(N)$. Only the signer knows the secret key (d, N) while the user knows the public key (e, N). The message M is blinded using $r^e \mod N$ where r is a random variable which is non-negative, less than, and relatively prime to N. The blinded message is signed by the signer using the d and then returned to the sender. The sender can unblind the signed blinded message to receive the signed message due to knowing r.

remove "the"

The idea of ID-Based cryptography was introduced in 1985 by [12] as a means of eliminating public key certificates by using a public key bound to the user's identity (string) like name, email address, or telephone number. Using that as the foundation, the Identity-based Identification (IBI) scheme was introduced in 2004 by [9] and can be summarized into four probabilistic

polynomial-time (PPT) algorithms that are Setup, Extract, Proving and Verifying algorithms. The setup algorithm uses a private key generator (PKG) algorithm with the input of 1^k where k is the security parameter to generate the global parameters $(params)$ which are known publicly and the master secret key (msk) which is known only to the PKG. Then the Extract algorithm with the inputs of msk and the public identity ID of the user is used to generate a private key d that is given to each user. Proving and Verifying are interactive algorithms where a user can use the Proving algorithm to prove to another who uses the verifying algorithm to prove his or her identity.

Identity-Based Blind Signature (ID-Based Blind Signature or IBBS) schemes have properties that are a combination of blind signature schemes and ID-based signature schemes. In an IBBS scheme, the identity of the user being issued the private key is not known to the issuer. An IBBS scheme like an IBI scheme consists of 4 PPT algorithms. There are 3 phases, setup phase, extract phase, and identification phase. In the setup phase, a private key generator (PKG) algorithm with the input of 1^k is used to generate the $params$ which are known publicly and the msk which is known only to the PKG. In the Extract phase, the identity string of the user is blinded using a random variable and sent to the issuer who signs it and sends it back. The user then unblinds the blinded private key as he or she only knows the random variable. In the identification phase like in IBI schemes, the Prover proves his or her identity to the verifier without revealing the private key.

Blind IBI schemes simillar to IBBS have properties that are a combination of BS schemes and IBI schemes. In Blind IBI schemes, the Issuer assigns the private key to users where the user's identity is not known to the Issuer. Blind IBI schemes fill a niche where multiple users can get their user private keys anonymously without the issuer knowing their identity and allow users the option to verify their identity anonymously or through their public identity. Relative to IBI schemes, Blind IBI schemes provide additional capabilities and a higher level of privacy.

1.2 Related works

Blind Signatures (BS) were introduced by Chaum [4] in 1984 as the method for realizing untraceable payment systems that offer improved privacy, control, and auditability. The basic idea of BS can be explained in the form of conducting a secret ballot. In a secret ballot, special envelopes that are carbon lined are used so that a trustee can sign the envelope (verify it being valid) without knowing the vote signed by the elector. The signer in a BS system does not know about what he has signed but only that what he has signed is valid.

Moldovyan [11] examines the first implementation of Blind Digital Signatures using Russian digital signature standards. He has also proposed protocols that conform with the signature verification equations based on the Russian digital signature standards GOST R 34.10-94 and GOST R 34.10-2001 for the implementation of Blind Digital Signatures. Moldovyan's [11] work is an indication of BS schemes being practical and can be used with little effort. Schemes related to BS like Blind-IBI, and IBBS will be just as easily available for implementation once adapted to the current standards.

Coron [6] proposes a proof for Full Domain Hash (FDH) scheme with a tighter security reduction. FDH scheme is a RSA-based signature scheme that is provably secure in the random oracle model (ROM) assuming that inverting RSA is hard. The proposed FDH scheme is more efficient due to the smaller RSA moduli used for the same level of security. The method used by him can also be applied to the Rabin signature scheme, the Paillier signature scheme and the Gennaro-Halevi-Rabin signature scheme. Our Blind GQ-IBI scheme is a modified version of the FDH-RSA

scheme proposed by him.

The concept of IBI schemes was first formalized in Kurosawa and Heng [9]. A transformation technique has been proposed where any digital signature satisfying certain conditions can be transformed to an IBI scheme with a tight security bond. Based on the proposed transformation the first IBI scheme based on the hardness of gap Diffie-Hellman problem is introduced. Kurosawa and Heng's [9] work acts as the basis through which secure IBI schemes can be derived from any signature scheme satisfying the conditions like deriving Blind IBI scheme from a BS scheme.

Kurosawa and Heng [10] is the first to propose IBI schemes that are provably secure in the standard model. The proposed scheme is based on the Boneh-Boyen signature scheme which is secure in the standard model. The proposed scheme in their paper is secure against impersonation under active and concurrent attacks if Boneh-Boyen signature scheme is existentially unforgeable under adaptive chosen message attack.

An IBI scheme that is provably secure against impersonation under passive attack based on the Computational Diffie-Hellman assumption and secure under active and concurrent attacks based on the One-More Computational Diffie-Hellman assumption was introduced by Chin et al. [5]. The proposed IBI scheme is based on the Waters signature scheme. Kurosawa and Heng's [10], and Chin et al.'s [5] work can be used for making the IBI schemes derived from [9] provably secure in the standard model and against impersonation under passive attack.

Security Proofs for many IBI and Identity-Based Signature schemes have been provided in [3]. This is done through a common framework that unifies and explains the area. The method proposed by them allows easy implementation of any one-way function like IBI and Identity-Based Signature schemes without random oracles. We use the one-more-RSA-inversion proof introduced by [3] to show the security of the Blind GQ-IBI scheme in this work.

There have been many papers proposing IBBS schemes using bilinear pairing. The computational cost of bilinear pairings is approximately 20 times higher than that of scalar multiplication over elliptic curve group. Due to this, He et al. [7] proposed the first IBBS scheme without bilinear pairings using the elliptic curve that is provably secure in the random oracle model. The advantages of the IBBS schemes without bilinear pairings include faster running time and smaller size of signature without compromising the security of the scheme. Blind IBI schemes and IBBS schemes have similar properties making the two kinds of schemes ideal for comparison and conversion between them while maintaining their privacy and security.

The contribution of this paper is the development of the first Blind GQ-IBI scheme that is provably secure under the random oracle model. The paper is organized as follows. In Section 2, the proposed solution is explained. In Section 3, the results obtained from this work and the discussion is presented. The conclusions are presented in Section 4.

2 Methodology

2.1 Blind IBI

A Blind IBI scheme is composed of 3 entities which are the Trusted Authority (TA), User, and Identifier. Blind IBI schemes use 4 algorithms which are the Setup, Extract, Prover and Verifier.

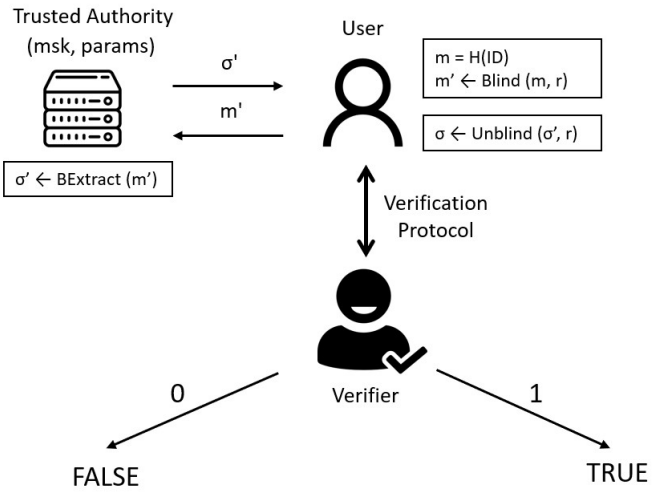

Figure 1: Blind Identity-Based Identification Scheme.

The TA runs the Setup algorithm. The Setup algorithm takes a security parameter as input to generate the $params$ and msk. The $params$ is published while the msk is kept secret. The Extract algorithm is run by the TA and User given the inputs of user identity (ID), msk, and $params$ to generate a user private key d_{ID} which is then sent to the signer.

The Extract algorithm, also known as the Issue algorithm, consists of 3 sub-algorithms that are run by the User and the TA. The User uses a Blind algorithm that takes a random string (r) and a hash of ID (m) to generate a blinded message $(\tilde{m})$. $\tilde{m}$ is sent to the TA who generates a blinded user private key $\tilde{\sigma}$ using the BExtract algorithm and sends it back to the User. The User uses the Unblind algorithm with the input of r and $\tilde{\sigma}$ to produce the unblinded user private key σ.

The Prover and Verifier algorithm interact together through an identification protocol to verify the identity of the user. The identification protocol is derived from the Sigma protocol consisting of commitment, challenge, and response. Here the User is the Prover, and the Verifier is the entity to whom the User wants to prove their identity. The Prover first sends a commitment (CMT) to the Verifier who replies with a random challenge (CHL). The Prover then sends a response (RSP) based on the user private key σ and the challenge to the Verifier, who then accepts or rejects the Prover's identity. With the inputs of CMT, CHL, RSP, m, and $params$, the Verifier algorithm outputs 1 if User identity is verified or 0 otherwise.

2.2 Blind GQ-IBI

Blind GQ-IBI consists of 4 algorithms: Setup, Extract, Prover and Verifier. In the setup phase, a key generation center $(Keygen)$ uses an algorithm K_{rsa} with the input 1^k to generate p, q, N, e and d. N is the product of two distinct large odd prime numbers (p and q). e and d are random positive numbers less than N such that $e \times d = 1 \mod \phi(N)$, where $\phi(N) = (p-1) \times (q-1)$ is Euler's totient function. 'k' is the security parameter used by the $Keygen$. The $params$, consisting of N and e is known to the public and the msk, consisting of d is known only to the $Keygen$.

Algorithm 1 Blind GQ-IBI

procedure KeyGen(1^k)
  $(N, e, d) \leftarrow \mathsf{K}_{\mathsf{rsa}}(1^k)$
  $e \times d = 1 \mod \phi(N)$
  $params \leftarrow (N, e)$
  $msk \leftarrow (d)$
  return $(params, msk)$
end procedure
procedure Extract(m, msk)
  User:
  $m = message = H(ID)$
  $r \leftarrow Z_N^*$
  $\tilde{m} = mr^e \mod N$
  Issuer:
  $\tilde{\sigma} = \tilde{m}^d \mod N$
  User:
  $\tilde{\sigma} = \tilde{m}^d \mod N$
  $\tilde{\sigma} = (mr^e)^d \mod N$
  $\tilde{\sigma} = m^d r^{e*d} \mod N$
  $\tilde{\sigma} = m^d r \mod N$
  $\sigma = \tilde{\sigma} \times r^{-1} = m^d \mod N$
  return σ and $\tilde{\sigma}$
end procedure

In the extract phase, there are 2 parties which are the user and the issuer. The user uses their public identity (ID), which can be any string, such as their email address, passport number, etc., to generate a user private key (usk), also known as the user secret key. m is the hash of the user ID, r is a random number used to blind the hash of the user ID, $\tilde{m}$ is the blinded m, σ is the usk, and $\tilde{\sigma}$ is the blinded usk.

The user hides his or her identity using a random number r which only he or she knows. The blinded user ID, $\tilde{m}$ is sent to the issuer. The issuer does not know to whom he or she is signing the $\tilde{m}$ for. The issuer returns $\tilde{\sigma}$ to the user. The user is able to extract σ from $\tilde{\sigma}$ as he or she only knows r.

Change verifier to Verifier

The identification protocol consists of the Prover and Verifier. The prover knows the public key (pk) and the secret key (sk) while the verifier only knows the public key. In the conventional version as shown in Figure 2, the pk consists of N, m and e, and sk consists of σ. If $V(e, \sigma, CMT, CHL, RSP)$ returns 1 then it is true, and 0 then it is false.

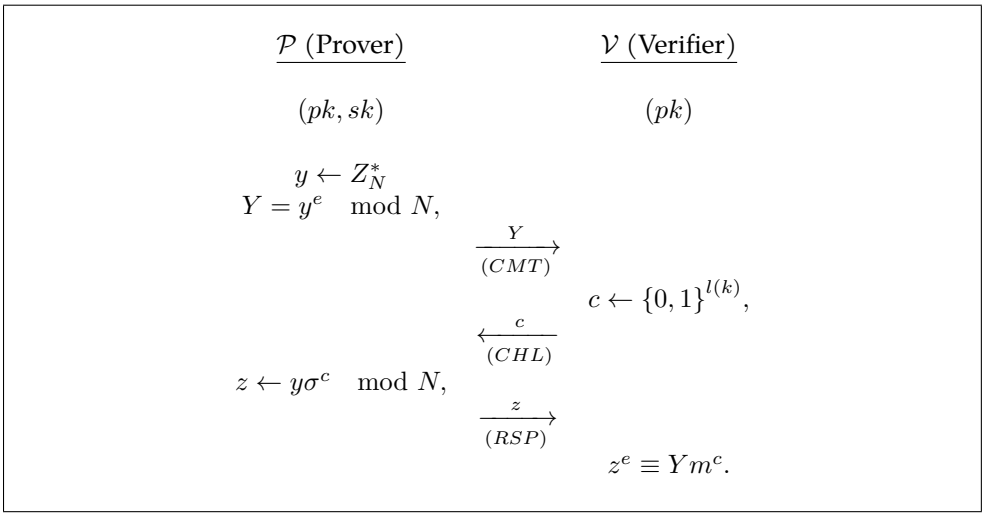

Figure 2: The Conventional Identification protocol Version.

The completeness of the conventional identification protocol is shown in Equation 1.

$$z^e \equiv (y\sigma^c)^e \equiv y^e\sigma^{ce} \equiv y^e(m^d)^{ce} \equiv y^e m^c \equiv Ym^c. \tag{1}$$

In the Blind Identification protocol version as shown in Figure 3 is the same as the conventional version, except that the pk consists of N, $\tilde{m}$ and e, and sk consists of $\tilde{\sigma}$. Therefore, $V(e, \tilde{\sigma}, CMT, CHL, RSP)$ returns 1 if true and 0 if false.

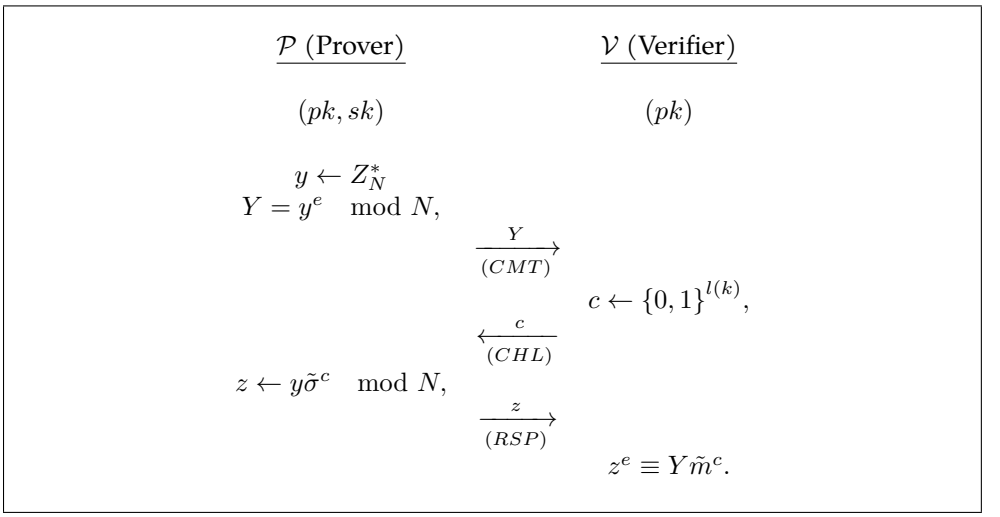

Figure 3: The Blind Identification protocol Version.

In Equation 2, the completeness of the blind identification protocol is shown.

$$z^e \equiv (y\tilde{\sigma}^c)^e \equiv y^e\tilde{\sigma}^{ce} \equiv y^e(\tilde{m}^d)^{ce} \equiv y^e\tilde{m}^c \equiv Y\tilde{m}^c. \tag{2}$$

3 Results and Findings

In this section, a will represent the secret key d, and b will represent the public key e. In addition, e is now used as the base of the natural logarithm for this section. The security definition of the IBI scheme from [8] applies similarly to the Blind IBI scheme, as shown below

Definition 3.1. *A Blind Identity-based Identification scheme is* (t,q_I,ϵ)*- secure under passive* (*active and concurrent*) *attack if for any passive* (*active and concurrent*) *impersonator* I *who runs in time* t*,*

$$Pr[I \text{ impersonates}] < \epsilon,$$

where I *can make at most* q_I *extraction queries and* ϵ *represents the advantage of the impersonator.*

3.1 Impersonation through passive attacks (imp-pa)

The security proof of an IBI scheme in [8] can be applied to a Blind IBI scheme if the latter satisfies the same requirements as the former. A Blind IBI scheme is secure under impersonation through passive attacks if it satisfies the 3 properties of completeness, soundness, and zero knowledge.

The identification protocol in our scheme is a 3-move canonical protocol, as shown in Figures 2 and 3, where if the P knows σ or $\tilde{\sigma}$ then the V always accepts. Therefore, the identification protocols of our Blind GQ-IBI scheme satisfy completeness. The identification protocol is designed in such a way that the V does not need to know σ or $\tilde{\sigma}$ to verify the identity of the P. Therefore, this satisfies the zero knowledge condition.

We can prove that our Blind GQ-IBI scheme satisfies soundness using the soundness extractor as follows. Suppose that (y, c_1, z_1) and (y, c_2, z_2) are two transcripts that are successful. Then,

$$z_1^b = ym^{c_1} \mod N \text{ and } z_2^b = ym^{c_2} \mod N.$$

From the above equation,

$$(z_1/z_2)^b = m^{c_1-c_2} \mod N.$$

Since b is a prime and $-b < c_1 - c_2 < b$ making the $gcd(b, c_1 - c_2) = 1$. We can obtain the value of integers S and T using the extended Euclidean algorithm as shown below.

$$bS + (c_1 - c_2)T = 1.$$

It follows that,

$$\begin{aligned} m &= m^{bS+(c_1-c_2)T} \mod N \\ &= (m^S)^b(m^{c_1-c_2})^T \mod N \\ &= (m^S)^b(z_1/z_2)^{bT} \mod N \\ &= (m^S(z_1/z_2)^T)^b \mod N. \end{aligned}$$

Since $\sigma = m^a$, it is clear that we can obtain $\sigma = m^S(z_1/z_2)^T \mod N$ as a signature on m. From this, we can solve for the value of a. This clarifies that even with the same commitment, the challenge and response will differ between transcripts. This proves the soundness condition.

Similar to the GQ-IBI scheme in [8], our Blind GQ-IBI scheme achieves security against impersonation through passive attacks, as stated in the following theorem. A Blind GQ-IBI scheme is (t, q_i, q_h, ϵ)-secure under passive attacks if the 3 conditions are satisfied, where the impersonator I can make at most q_H random oracle queries.

Theorem 3.1. *Suppose RSA is (t', ϵ')-secure. A Blind GQ-IBI Scheme is (t, q_I, q_H, ϵ)-secure under passive attacks, where,*

$$t = (t'/2) - (q_H + q_I + 1).poly(k),$$
$$\epsilon = \sqrt{e.q_I.\epsilon'} + (1/b).$$

3.2 Impersonation through active and concurrent attacks (imp-aa,ca)

We use a modified version of the security proof proposed in [8] to prove that our scheme is secure against impersonation through active and concurrent attacks. The one-more-RSA-inversion problem, which is regularly applied in [3, 8], is used in our scheme to address the challenge of proving security against active and concurrent attackers.

Theorem 3.2. *Suppose the one-more-RSA-inversion problem is (t',ϵ')-hard. Then Blind GQ-IBI scheme is (t,q_I, q_H, ϵ)-secure under active and concurrent attacks, where,*

$$t' = O(t), \qquad \epsilon \leq \sqrt{e(1 + q_I)\epsilon'} + (1/b).$$

Proof. Let I be an impersonator who (t, q_I, q_H, ϵ)-breaks the scheme. An algorithm is presented where M using (t', ϵ')- breaks the one-more-RSA-inversion problem by using I. □

An algorithm M is constructed and it uses I with advantage $(1/e(1+q_I))(\epsilon - 1/b)^2$. Algorithm M sets the system parameters $params = (N, b, H)$ based on the inputs (N, b). H is a random oracle used by M such that a random element $W_0 \in Z_N^*$ is obtained through queries of it's challenge oracle. Let $j := 0$.

In **Phase 1**, the following is how algorithms M and I interact with each other where I collects the information necessary to try impersonating an identity.

Random Oracle Queries Algorithm: M contains a list of tuples $(ID_i, Q_i, f_i, coin_i)$ which is used when I queries H. This list is empty at the start. M responds as follows when I queries $H(ID_i)$:

1. $Q_i = H(ID_i)$ is returned when ID_i is already on the list.
2. If it is not on the list a random coin is generated, $coin_i \in (0, 1)$ such that $Pr[coin_i = 0] = \delta$. δ is defined later.
3. If $coin_i = 0$, then $Q_i = f_i^b \mod N$ is generated. Otherwise $Q_i = W_0 f_i^b \mod N$ is generated. $f_i \in Z_N^*$.
4. The tuple $(ID_i, Q_i, f_i, coin_i)$ is added. The response $H(ID_i) = Q_i$ is sent to I.

Extraction Queries: An extraction query ID_i is sent to M by I. M responds as follows:

1. The random oracle H is used to obtain $Q_i = H(ID_i)$ which corresponds to the tuple $(ID_i, Q_i, f_i, coin_i)$. The One-more-RSA attack fails if $coin_i = 1$.
2. Else, it should be $coin_i = 0$ thus making $Q_i = f_i^b \mod N$. In Blind GQ-IBI, Q_i will be blinded into $\tilde{Q}_i$ using a random variable r known only to the user such that $\tilde{Q}_i = Q_i \times r^b$. $\tilde{Q}_i$ is sent to an Issuer who responds by generating a private key $\tilde{d}_i$ which is blinded. $\tilde{d}_i = (Q_i \times r^b)^a = Q_i^a$. The user is able to deblind $\tilde{d}_i$ as he or she only knows r. Therefore, the private key $d_i = \tilde{d}_i \times r^{-1} = Q_i^a \times r \times r^{-1} = Q_i^a = f_i^{a \times b} \mod N = f_i \mod N$.

Identification Queries: Now I acts as a cheating Verifier while M acts as the Prover whose identity is ID_i. The interaction between them is as follows:

1. The random oracle H is used to produce $Q_i = H(ID_i)$ and $(ID_i, Q_i, f_i, coin_i)$ as the corresponding tuple.
2. If $coin_i = 0$ then an extraction query is run by M to obtain the private key d_i which will be known only to M.
3. If $coin_i = 1$ then $j := j + 1$. M issues a commitment to I to which I sends a challenge $c_j \in (0, 1, ..., b-1)$. M responds to the challenge $V_j = (W_j(W_0 f_i^b)^{c_j})^a = W_j^a (W_0^a f_i)^{c_j} \mod N$.

In **Phase 2**, I after collecting enough information decides that Phase 1 is over. An identity ID is selected by I to impersonate which will be challenged by M. First M runs the random oracle model to obtain $Q = H(ID)$ and the tuple $(ID, Q, f, coin)$:

1. If $coin = 0$ then the one-more-RSA attack has failed. The algorithm will report failure and terminate.
2. Otherwise, $coin = 1$ making $Q = W_0 f^b \mod N$.

Let *Good* be the event that M has not failed until now. If the current value of $j = n$. Then,

- M has made $n + 1$ queries to its challenge oracle and has obtained $W_0, \ldots, W_n$.
- M has made n queries $V_j = [W_j(W_0 f_i^b)^{c_j}]^a \mod N$ for $j = 1, \ldots, n$.

Now M, runs I as a cheating prover whose identity is ID, making $Q = H(ID) = W_0 f^b \mod N$. I sends a commitment y to M who selects a challenge $c \in 0, 1, \ldots, b-1$ to return to I who responds with z. After this, I is instructed to be reset such that the same commitment y is sent to M. M selects and sends another challenge $c' \in 0, 1, \ldots, b-1$ to which I responds with z'.

If both transcripts are accepted and $c \neq c'$, then I can extract the inverse of W_0 which w_0. Since,

$$z^b = y(W_0 f^b)^c \mod N,$$
$$(z')^b = y(W_0 f^b)^{c'} \mod N,$$

thus,

$$(z/z')^b = (W_0 f^b)^{c-c'} \mod N.$$

Since b is a prime and $-b < c - c' < b$ making the $gcd(b, c - c') = 1$. We can obtain the value of integers S and T using the extended Euclidean algorithm as shown below.

$$bS + (c - c')T = 1.$$

It follows that,

$$\begin{aligned} W_0 f^b &= (W_0 f^b)^{bS+(c-c')T} \mod N \\ &= (W_0 f^b)^{bS} (W_0 f^b)^{(c-c')T} \mod N \\ &= (W_0 f^b)^{bS} (z/z')^{bT} \mod N \\ &= [(W_0 f^b)^S (z/z')^T]^b \mod N. \end{aligned}$$

This shows that $(W_0 f^b)^S (z/z')^T / f = W_0^S f^{bS-1} (z/z')^T (\mod N)$. Using the Reset Lemma, we can see that

$$Pr[M \text{ can compute } w_0 \mid Good\,] \geq (\epsilon - 1/b)^2.$$

Once w_0 is obtained, M can compute, $w_j = V_j (w_0 f_i)^{-c_j} \mod N$ for $j = 1, \ldots, n$. To prove that this computation yields the desired RSA-inverse we show that $w_j^b = W_j \mod N$. Since V_j is the inverse of $W_j (W_0 f_i^b)^{c_j}$ and w_0 is the inverse of W_0,

$$\begin{aligned} w_j^b &= [V_j (w_0 f_i)^{-c_j}]^b \mod N \\ &= V_j^b w_0^{-bc_j} f_i^{-bc_j} \mod N \\ &= W_j W_0^{c_j} f_j^{bc_j} W_0^{-c_j} f_i^{-bc_j} \mod N \\ &= W_j \mod N. \end{aligned}$$

Hence M wins the one-more-RSA-inversion problem. Therefore,

$$\begin{aligned} Pr[Mwins] &= Pr[M \text{ computes } w_0 \wedge Good] \\ &= Pr[M \text{ computes } w_0 \mid Good] \\ &\geq (\epsilon - 1/b)^2 Pr[Good]. \end{aligned}$$

$Pr[Good]$ remains to be calculated to complete the proof. If I makes a total of q_I extraction queries, then the probability that M answers to all the extraction queries is δ^{q_I} and the probability that M does not abort when checking the validity of the challenge public identity ID submitted by I, is $1 - \delta$. Therefore, the probability that M does not abort during the simulation is $\delta^{q_I}(1 - \delta)$. This value is maximized at $\delta_{opt} = 1 - 1/(q_I + 1)$. Using δ_{opt}, the probability that M does not abort is at least $1/e(1 + q_I)$. This is because the value $(1 - 1/(q_I + 1))^{q_I}$ approaches $1/e$ for large q_I. This shows that M's advantage ϵ' is at least $(1/e(1 + q_I))(\epsilon - 1/b)^2$ as required.

4 Conclusion

Our work proposes the first Blind GQ-IBI scheme provably secure in the random oracle model. Our scheme is secure against impersonation through passive, active, and concurrent attacks. For future work, a discrete logarithmic-based version of this work could be explored for schemes based on Elliptic Curve Cryptography. Our Blind GQ-IBI scheme can be further developed to be secure in the standard model. Our scheme is well suited for real world applications like within building

security systems where employees can use their smartphone to enter the building and its restricted areas.

Acknowledgement The researchers sincerely appreciate and express gratitude for financial support from the Ministry of Higher Education, Malaysia, under the Fundamental Research Grant Scheme with grant number FRGS/1/2023/ICT07/MMU/03/1 and Multimedia University for its Research Management Fund.

Conflicts of Interest The authors declare no conflict of interest.

References

[1] S. Abubakar, M. Ariffin & M. Asbullah (2019). Successful cryptanalytic attacks upon rsa moduli $N = pq$. *Malaysian Journal of Mathematical Sciences*, *13*(S), 141–189.

[2] M. B. Algehawi & A. Samsudin (2015). Certificateless public key encryption (CL-PKE) scheme using extended chebyshev polynomial over the finite field Z_p. *Malaysian Journal of Mathematical Sciences*, *9*(S), 53–69.

[3] M. Bellare, C. Namprempre & G. Neven (2004). Security proofs for identity-based identification and signature schemes. In C. Cachin & J. L. Camenisch (Eds.), *Advances in Cryptology - EUROCRYPT 2004*, pp. 268–286. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24676-3_17.

[4] D. Chaum (1983). Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest & A. T. Sherman (Eds.), *Advances in Cryptology*, pp. 199–203. Springer US, Boston, MA. https://doi.org/10.1007/978-1-4757-0602-4_18.

[5] J. J. Chin, S. H. Heng & B. M. Goi (2008). An efficient and provable secure identity-based identification scheme in the standard model. In S. F. Mjølsnes, S. Mauw & S. K. Katsikas (Eds.), *Public Key Infrastructure*, pp. 60–73. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-69485-4_5.

[6] J. S. Coron (2000). On the exact security of full domain hash. In M. Bellare (Ed.), *Advances in Cryptology – CRYPTO 2000*, pp. 229–235. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44598-6_14.

[7] D. He, J. Chen & R. Zhang (2011). An efficient identity-based blind signature scheme without bilinear pairings. *Computers & Electrical Engineering*, *37*(4), 444–450. https://doi.org/10.1016/j.compeleceng.2011.05.009.

[8] H. S. Huay (2004). *Design and Analysis of Some Cryptographic Primitives*. PhD thesis, Tokyo Institute of Technology, Tokyo, Japan.

[9] K. Kurosawa & S. H. Heng (2004). From digital signature to ID-based identification/signature. In F. Bao, R. Deng & J. Zhou (Eds.), *Public Key Cryptography – PKC 2004*, pp. 248–261. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24632-9_18.

[10] K. Kurosawa & S. H. Heng (2005). Identity-based identification without random oracles. In O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar & C. J. K. Tan

(Eds.), *Computational Science and Its Applications – ICCSA 2005*, pp. 603–613. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/11424826_64.

[11] N. A. Moldovyan (2011). Blind signature protocols from digital signature standards. *International Journal of Network Security*, *13*(1), 22–30.

[12] A. Shamir (1985). Identity-based cryptosystems and signature schemes. In G. R. Blakley & D. Chaum (Eds.), *Advances in Cryptology*, pp. 47–53. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39568-7_5.

[13] T. Y. Teh, Y. S. Lee, Z. Y. Cheah & J. J. Chin (May 2017). IBI-mobile authentication: A prototype to facilitate access control using identity-based identification on mobile smart devices. *Wireless Personal Communications*, *94*(1), 127–144. https://doi.org/10.1007/s11277-016-3320-y.