ID-based Cryptography from Composite Degree Residuosity

Man Ho Au and Victor K. Wei

Department of Information Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong
{mhau3,kwwei}@ie.cuhk.edu.hk

Abstract. We present identity-based identification (resp. encryption, signature, blind signature, ring signature) from composite degree residuosity (CDR). Constructions of identifications and signatures motivated by several existing CDR-based bandwidth-efficient encryption schemes are presented. Their securities are proven equivalent to famous hard problems, in the random oracle model. Motivated by Cocks[12], we construct an identity-based encryption from CDR. Its security is proven equivalent to a new problem, the JSR (Jacobi Symbol of Roots of two quadratic polynomials) Problem. We prove JSR is at least as hard as QRP (Quadratic Residuosity Problem). Furthermore, we present the first two-way equivalence reduction of the security of Cocks' IBE, to the JSR Problem.

1 Introduction

Identity-based cryptography: In 1984, Shamir [37] proposed the idea of identity-based cryptography in which the identity of each user is used as his public key string. Shamir's motivation is to avoid the need for certificates to link users to their public keys. Since the problem was posed identity-based signature (IBS) and identity-based identification (IBI) schemes have been proposed [14, 37, 20, 31]. However, Good identity-based encryption (IBE) schemes are far rarer[5].

Due to its wide applications, research on identity-based cryptography has been a very active area. Many new identity-based signature schemes (resp. blind signature, ring signature) based on pairings have been proposed[22, 35, 9, 38](resp. [39, 40], [39, 27, 21]).

Composite Degree Residuosity (CDR): Goldwasser-Micali, Benaloh, Naccache-Stern, and Okamoto-Uchiyama have worked on trapdoor based on CDR [19, 29, 30]. In 1999, Pailier[33] brought re-envigored interests to this trapdoor mechanism. Since then, it has found widespread applications in verifiable encryption [7], double trapdoor decryption [6], ..., etc. Several variants of Paillier's cryptosystem have been proposed recently [8, 16].

In this paper, we introduce identity-based cryptography from the trapdoor mechanism of CDR. There have been identity-based identifications and signatures from essentially all major trapdoor or one-way mechanisms, including Fact-

goring, RSA, DL (Discret Log), and pairings[4]. We initiate CDR-trapdoored studies here. Specifically, we make the following contributions:

Our contributions:

- We present the first identity-based identification and the first identity-based signature schemes from composite degree residuosity. Our four constructions are motivated by bandwidth-efficient CDR-based encryption schemes, namely Paillier[33], Catalano, et al.[8], Galindo, et al.[16], and Kurosawa, et al.[26].
- we present a thorough hierarchy of attacker security models for IBI and IBS, including passive attacker, enhanced passive attacker, two-stage active attacker, two-stage concurrent attacker, and parallel one-more attacker.
- We prove the securities of our IBI's (resp. IBS's) are equivalent to well-known hard problems, e.g. RSA[n, n], RSA[n, e], and Factoring, in the random oracle model (ROM).
- We present the first identity-based encryption from CDR, motivated by Cocks[12]. Its security is proven equivalent to a new problem: The JSR (Jacobi Symbol of Roots of two quadratic polynomials) Problem. We prove JSR is at least as hard as QRP (Quadratic Residuosity Problem).
- We present the first two-way equivalence reduction of the security of Cocks' IBE [12], to JSR. Previously, only one-way reduction from security of Cocks' IBE to QRP was known, and only proven by informal arguments.
- We present the first identity-based blind signature and the first identity-based ring signature schemes from CDR.

The rest of the paper is **organized** as follows: In Section 2, we review background results. Section 3 provides security models and formal definitions of security notions. In Section 4, we presents the constructions and security analyses of our IBI's. In Section 5, we presents our IBE and its security analyses. In Section 6, we presents identity-based signatures, blind signatures, ring signatures. We conclude in Section 7.

2 Preliminaries

2.1 Related Results

Bellare et al.[4] formalized security models and definitions of security notions for IBI and IBS schemes. They also systematically studied the formal security of a dozen or more IBI schemes in the literature. Others, such as [9, 23], studies formal security of IBS schemes. [23] presented a general transfrom from signature schemes to IBI schemes using zero-knowledge techniques.

The concept of blind signatures was introduced by Chaum [11], which provides anonymity of users in application such as e-cash or credential systems. It allows users to obtain a signature of a message in a way that the signer learns nothing about the message and the resulting signature.

The concept of ring signature was introduced by Rivest et al. [36]. A ring signature scheme is a group signature scheme without group manager. The formation of a group is spontaneous such that diversion group members can be totally unaware of being conscripted to the group. It allows members of a group to anonymously sign messages on behalf of the group.

2.2 Notations

We review background results needed subsequently. If N is an RSA modulus, i.e., $N = pq$ where p, q are different odd primes, then we denote by RSA[n,e] the RSA problem with exponent e. If N is a positive integer, then $\mathbb{QR}_N$ stands for the set of quadratic residues modulo N. If $p = 2p' + 1$ where p and p' are both prime, then p is a safe prime. Denote by $\mathcal{SP}(\ell)$ the sets of safe prime numbers of length ℓ. Also denote by $\lambda(N)$ the Carmichael's function taken on N.

Definition 1. (The Quadratic Residuosity Problem, QRP) *Given N a product of two large primes, and $Q \in Z_N$, determine whether $Q \in \mathbb{QR}_N$ with probability non-negligibly over random guessing.*

2.3 Some Previous Schemes

We review some CDR-based encryptions, and Cocks' IBE.

Paillier's Encryption Scheme [33]: Let $N = pq$ be an RSA modulus and g an element having order αN with $\alpha \geq 1$ in the multiplicative group $\mathbb{Z}^*_{N^2}$. To encrypt a message $m \in \mathbb{Z}^*_{N^2}$, Paillier proposed the following mechanism.

$$\varepsilon_g = g^{m_1} {m_2}^N \bmod N^2$$

where $m = m_1 + m_2 N$ and he proved that:

- ε_g is a bijection between $\mathbb{Z}_N \times \mathbb{Z}^*_N$ and $\mathbb{Z}^*_{N^2}$.
- ε_g is a one-way trapdoor permutation equivalent to RSA[n,n]
- the above is OW-CPA if and only if RSA[n,n] is hard.

Since ε_g is a bijection, for any $w \in \mathbb{Z}^*_{N^2}$, there exists unique (x, y) such that $x \in \mathbb{Z}_N$ and $y \in \mathbb{Z}^*_N$ and $w = \varepsilon_g(x, y)$. Paillier called x the class of w relative to g(denoted by $[w]_g$). Informally, Paillier call computing $[w]_g$ given w and g the computational composite residuosity class problem. If $w \in < g >$, computing $[w]_g$ is called partial discrete logarithm problem (PDL). Paillier assume both of them are hard. We denote inverting ε_g the Paillier problem and it is equivalent to RSA[n,n].

Catalano et al.'s Encryption Scheme [8]: Catalano et al.'s proposed an encryption scheme by modifying Paillier's scheme. Let N be an RSA modulus. Let $e \in \mathbb{Z}_N$ such that $\gcd(e, \lambda(N^2)) = 1$ and

$$\begin{aligned} \varepsilon_e : \mathbb{Z}_N \times \mathbb{Z}^*_N &\to \mathbb{Z}^*_{N^2} \\ (m, r) &\mapsto (1 + mN) r^e \bmod N^2 \end{aligned}$$

To encrypt a message $m \in \mathbb{Z}_N$, randomly generate $r \in \mathbb{Z}_N^*$, compute ciphertext $c = \varepsilon_e(m, r)$. Catalano et al. proved that ε_e is one-way if computational small e-root problem (CSE) in $\mathbb{Z}_{N^2}^*$ is hard. Informally, the CSE problem is to compute $x \in_R [0, ..., N-1]$, given $y = x^e \bmod N^2$.

Galindo et al.'s Encryption Scheme [16]: Galindo et al. obtained an encryption scheme as secure as factoring from a modification of Catalano et al.'s scheme. Let $N = pq$ be an RSA modulus such that $p \equiv q \equiv 3 \bmod 4$. Let $e \in \mathbb{Z}_N$ such that $\gcd(e, \lambda(N)) = 1$ and

$$\begin{aligned} \mathcal{F}_e : \mathbb{Z}_N \times \mathbb{QR}_N &\rightarrow \mathbb{QR}_{N^2} \\ (m, r) &\mapsto r^{2e} + mN \bmod N^2 \end{aligned}$$

To encrypt a message $m \in \mathbb{Z}_N$, randomly generate $r \in \mathbb{QR}_N$ and compute ciphertext $c = \mathcal{F}_e(m, r)$. The encryption scheme is one-way if factorization of $N = pq$ is hard. Note that here p, q are restricted to $p \equiv q \equiv 3 \bmod 4$.

Kurosawa et al.'s Encryption Scheme [26]: Kurosawa et al. proposed an one-way secure encryption scheme based on [24, 25]. The public key is $N = pq$, α such that $(\frac{\alpha}{p}) = (\frac{\alpha}{q}) = -1$ and a prime e. The private key is p and q. To encrypt a message $m \in \mathbb{Z}_N$, randomly generate $r \in \mathbb{Z}_N^*$ such that $(\frac{r}{N}) = 1$ and $\alpha/r > r \bmod N$, compute

$$c = (r + \alpha/r)^e + mN \bmod N^2$$

The encryption scheme is one-way if factorization is hard.

Cocks ID-based Encryption Scheme [12] Cocks proposed an IBE based on quadratic residuosity problem (QRP). The user secret key is the square root of a value $Q \in \mathbb{QR}_N$ related to his identity. To encrypt a message $m \in \{-1, 1\}$, randomly generate t such that the Jacobi symbol $(\frac{t}{N}) = m$ and compute ciphertext $c = t + Q/t \bmod N$. The user holding the square root of Q decrypt by computing $m = (\frac{c+2\sqrt{Q}}{N})$.

3 Security Models

We present our security model, and define security notions.

3.1 ID-based Identification

An identity-based Identification (IBI) scheme is a four-tuple (MKg, UKg, IBP, IBV) specified as follow.

- $(msk, mpk) \leftarrow \mathsf{MKg}(1^{\lambda_s})$ is a PPT algorithm which, on input a security parameter $\lambda_s \in \mathbb{N}$, outputs a master private/public key pair (msk, mpk).

- $(usk) \leftarrow \mathsf{UKg}(\mathrm{ID}, mpk, msk)$ is a PPT algorithm which , on input ID and (mpk, msk), generates user secret key usk with overwhelming probability.
- IBP is a PPT algorithm which on input ID, mpk and usk, conduct a 3-move interactive protocol with querier.
- IBV is a PPT algorithm which on input ID and mpk, conduct a 3-move interactive protocol with IBP. At the end of the protocol IBV output either Accept or Reject.
- The 3-move interactive protocol between IBP and IBV, **Identification Protocol**, is as follows:
  - IBP sends a commitment t to IBV.
  - IBV sends a challenge c randomly chosen from some set.
  - IBP provides a response s.
  - $\mathsf{Accept}/\mathsf{Reject} \leftarrow \mathsf{IBV}(\mathrm{ID}, mpk, t, c, s)$.

An IBI should satisfy three properties, namely, completeness, soundness and zero-knowledgeness.

(*Completeness.*) If all parties act as they should, the end result should be IBV outputting Accept with overwhelming probability. Formally, for all security parameter λ_s and $\forall \mathrm{ID} \in \{0,1\}^*, (mpk, msk) \in [\mathsf{MKg}(1^{\lambda_s})]$, and $usk \in [\mathsf{UKg}(\mathrm{ID}, mpk, msk)]$, IBV(initialized with mpk, ID) output Accept after interacting with IBP (initialized with ID, usk, mpk) with overwhelming probability.

(*Soundness.*) If verifier output Accept after interacting with the prover following the 3-move protocol, then prover knows the secret. Formally, usk is computed efficiently from any two acceptable conversation (t, c, s) and $(t, \hat{c}, \hat{s})$,where t,c,s is the commitment, challenge, response respectively, such that $c \neq \hat{c}$ with overwhelming probability. Formal definitions shortly.

(*Zero-knowledgeness.*) (IBP, IBV) should be zero-knowledge for honest verifier. That is, there exists a PPT simulator $\mathcal{S}$ such that it output acceptable conversation exhibiting the same probability distribution as the actual conversation.

Remark: There are subtle differences between the identity-based prover, denoted IBP, and the ordinary prover of a three-move identification, typically denoted P. Discussions later.

Oracles: To model various attack scenarios, we provide the adversary with the following oracles.

- *Initialization Oracle*: $(\{\mathrm{ID}\}) \leftarrow \mathcal{IO}(\perp, mpk)$. Upon inputs the empty string, $\perp$, and mpk, outputs (sets up) an user identity $\{\mathrm{ID}\}$.
- *Key Extraction oracle*: $(usk) \leftarrow \mathcal{KEO}(\mathrm{ID}, mpk)$. Upon input $\mathrm{ID} \in \{\mathrm{ID}\}$ and mpk, returns the corresponding secret key of ID. (Sometimes known as Corruption Oracle)
- *Conversation Oracle*: $(t, c, s) \leftarrow \mathcal{CO}(\mathrm{ID}, mpk)$. Upon input ID and mpk, returns a valid 3-move conversation w.r.t. ID and mpk.
- *Identity-based Prover Oracle*: $\mathcal{IBPO}_{\mathrm{ID}}$. Upon valid request, conduct the 3-move interactive protocol with querier as follow.
  - Sends a commitment t to querier.
  - Receives a challenge c from querier.
  - Provides a response s such that $\mathsf{Accept} \leftarrow \mathsf{IBV}(\mathrm{ID}, mpk, t, c, s)$

Security notions The goal of an adversary is impersonation. We consider 5 different attack scenarios, namely, passive attack(pa1-ib-imp), enhanced passive attack(pa2-ib-imp), active attack(aa-ib-imp), concurrent attack(ca-ib-imp) and parallel-one-more attack(p1m-ib-imp).

[**Game IB-IMP**]

1. Setup Phase: Dealer $\mathcal{D}$ runs $\mathsf{MKg}(1^{\lambda_s})$ to obtain (mpk, msk).
2. Probe-1 Phase: Adversary $\mathcal{A}$ makes q_I (resp. q_K, q_C, q_P) queries to $\mathcal{IO}$ (resp. $\mathcal{KEO}$, $\mathcal{CO}$, $\mathcal{IBPO}$).
3. (Throw down the) Gauntlet Phase: At some point $\mathcal{A}$ decided Probe-1 phase is over and select a gauntlet ID, ID_G, to impersonate. ID_G must not have been submitted to $\mathcal{KEO}$ before and must be returned from $\mathcal{IO}$. Then $\mathcal{A}$ ensures IBV has ID_G and mpk, sends q_G commitments to IBV and receives q_G challenges from IBV.
4. Probe-2 Phase: $\mathcal{A}$ makes makes $\hat{q}_I$ (resp. $\hat{q}_K$, $\hat{q}_C$, $\hat{q}_P$) queries to $\mathcal{IO}$ (resp. $\mathcal{KEO}$, $\mathcal{CO}$, $\mathcal{IBPO}$). But $\mathcal{A}$ cannot query $\mathcal{KEO}$ or $\mathcal{IBPO}$ w.r.t. ID_G.
5. Answer Phase: $\mathcal{A}$ sends q_G responses to IBV. IBV outputs Accept or $\mathsf{Rejecton}$ each conversation.

Queries can be arbitrarily interleaved, even across Probe-1 and Probe-2 Phases, unless otherwise stated explicitly (such as in the Subgames below).

1. **Subgame pa1-ib-imp** (*Passive attacker*) $q_K = \hat{q}_K = q_P = \hat{q}_P = 0$
2. **Subgame pa2-ib-imp** (*Enhanced passive attacker*) No queries to $\mathcal{IBPO}$ w.r.t. ID_G in Probe-1 or Probe-2.
3. **Subgame 2s-aa-ib-imp** (*Two-stage active attacker*) One query must end before another can start, $q_G = 1$, and $\hat{q}_P = 0$.
4. **Subgame 2s-ca-ib-imp** (*Two-stage concurrent attacker*) $\hat{q}_P = 0$.
5. **Subgame p1m-ib-imp** (*Parallel one-more attacker*) None of the above restrictions.

Let $N_{G,i}$ be the number of acc's outputted by $\mathsf{IBV}_{\mathrm{ID}_G}$ in Probe-i, $i = 1, 2$. Let $q_{P,G}$ (resp. $\hat{q}_{P,G}$) be the number of queries to $\mathcal{IBPO}_{\mathrm{ID}_G}$ in Probe-1 (resp. Probe-2). For Subgames pa1- (resp. pa2-, p1m-)ib-imp, the *advantage* of the Adversary is the probability that $N_{G,1} + N_{G,2} > q_{P,G} + \hat{q}_{P,G}$. For Subgames 2s-aa- (resp. 2s-ca-)ib-imp, the *advantage* of the Adversary is the probability that $N_{G,2} > 0$. We use the "oracle clone" concept and the two-stage attacker model from [2]. Consult there for further details.

Definition 2. *An IBI scheme (MKg, UKg, IBP, IBV) is* pa1-ib-imp (resp. pa2-ib-imp, 2s-aa-ib-imp, 2s-ca-ib-imp, p1m-ib-imp) secure *if no PPT adversary has non-negligible advantage in Subgame pa1-ib-imp (resp. pa2-ib-imp, 2s-aa-ib-imp, 2s-ca-ib-imp, p1m-ib-imp).*

In contrast to counterpart security notions in non-IB identification schemes, we allow queries to the key extraction oracle, and these queries are typically simulated by backpatching the random oracle in our proofs. Our security models

differ from the IBI security models in Bellare, et al. [4] most distinctly in the way the gauntlet prover oracle, $\mathcal{IBPO}_{\mathrm{ID}_G}$, is simulated. The difference is most contrasted in "one-key" IBI's such as Guillou-Guisquater IBI [4] (and Paillier1-IBI and CGHGN1-IBI here). We simulate this 3-move oracle, $\mathcal{IBPO}_{\mathrm{ID}_G}$, by a 3-move prover oracle while [4] simulated it with a 2-move RSA-Inversion Oracle just like [2], p.172, l.-13, did in simulating its non-IB prover oracle. For "2-key" IBI's or other "witness-indistinguishable" IBI's such as Fiat-Shamir IBI, Okamoto-RSA IBI in [4] and HMMV-IBI, KT-IBI here, the difference between our security models and those in [4] is less pronounced.

Zero-knowledge: We review an old ZK and define a new ZK.

Definition 3. *The identity-based prover, IBP, is* Honest Verifier Zero-Knowledge (HVZK) *if an arbitrary PPT identity-based verifier IBV, following the interactive Identification Protocol honestly, cannot gain any knowledge of usk.*

Definition 4. *The identity-based prover, IBP, is* Extraction Resisten Zero Knowledge (ERZK) *if there does not exist an PPT algorithm which, when equipped with identity-based prover oracle w.r.t. ID, $\mathcal{IBPO}_{ID}$, can compute usk = UKg(ID, mpk, msk) from mpk and ID with non-negligible probability.*

Comparing ERZK with HVZK: Either model has its relative strength. The former considers $\mathcal{IBPO}$ and dishonest verifiers but needs to extract the entire secret usk. The latter is concerned about not leaking any part of the knowledge, usk. The ERZK (for "one-key" ibp) is strictly weaker than computational statistical ZK because it is about a a PPT disnonest verifier extracting all of usk, not just a part of it. However, IBP's where there exists $usk' \neq usk$ such that knowing usk' also enables a PPT algorithm to simulate $\mathcal{IBPO}_{\mathrm{ID}}$, does not have ERZK. This technicality simplifies our presentation.

3.2 ID-based Encryption

An identity-based encryption (IBE) scheme is a four-tuple (MKg, UKg, encrypt, decrypt), specified as follow.

- MKg, UKg defined before.
- $c \leftarrow \mathsf{encrypt}(\mathrm{ID}, mpk, m)$ is a PPT algorithm which, on input ID, mpk and message m, produces ciphertext c.
- $m \leftarrow \mathsf{decrypt}(\mathrm{ID}, mpk, usk, c)$ is a PPT algorithm which on input ciphertext c, ID, mpk, usk, output message m or fail.

Oracles: To model the attack scenario, we provide the adversary with the following oracles.

- $\mathcal{IO}$, $\mathcal{KEO}$ defined before.
- *Decryption Oracle*: $(m) \leftarrow \mathcal{DO}(c, \mathrm{ID})$. On input ciphertext c and $\mathrm{ID} \in \{\mathrm{ID}\}$, output the corresponding message m, or output fail if no message corresponding to the queried ciphertext exists.

Security notions We are interested in the completeness and the semantic security.

(**Completeness.**) A legitimate ciphertext should be decryptable by the intended user. Formally, for all security parameter λ_s and $\forall \mathrm{ID} \in \{0,1\}^*$, $(mpk, msk) \in [\mathsf{MKg}(1^{\lambda_s})]$, and $usk \in [\mathsf{UKg}(\mathrm{ID}, mpk, msk)]$,$m \leftarrow \mathsf{decrypt}(\mathrm{ID}, mpk, usk, c)$ if $c \leftarrow \mathsf{encrypt}(\mathrm{ID}, mpk, m)$ with overwhelming probability.

Semantic security: Attackers should not gain information or knowledge of the message from the ciphertext. We definie the semantic security via the following game(s).

[**Game IB-Semantic-Security**]

1. Setup Phase: Dealer $\mathcal{D}$ runs $\mathsf{MKg}(1^{\lambda_s})$ to obtain (mpk, msk).
2. Probe-1 Phase: Adversary $\mathcal{A}$ queries the oracles.
3. Gauntlet Phase: $\mathcal{A}$ sends its choice of gauntlet ID, ID_G, and message $m_1 \in \{0,1\}^\ell$. ID_G must not have been submitted to $\mathcal{KEO}$ before. $\mathcal{D}$ randomly generates message $m_0 \in \{0,1\}^\ell$, flips fair coin $b \in \{0,1\}$, computes $c_G =$encrypt(ID,mpk, m_b), and sends c_G to $\mathcal{A}$.
4. Probe-2 Phase: $\mathcal{A}$ queries oracles, except querying ID_G to $\mathcal{KEO}$ and querying (c_G, ID_G) to $\mathcal{DO}$.
5. Delivery Phase: $\mathcal{A}$ outputs an estiamte b' of b, and an estimate m' of m_0.

Queries can be arbitrarily interleaves even across Probe-1 and Probe-2 Phases, unless explicitely stated otherwise such as in the Subgames below:

1. **(sub-)Game IB-OW-CPA:** No $\mathcal{DO}$ queries in any Phase, and $b = 0$. The Adversary's *advantage* is the probability $m' = m_0$, minus the probability of guessing correcting by random m'. The latter probability equals $2^{-\ell}$.
2. **(sub-)Game IB-IND-CPA:** No $\mathcal{DO}$ queries in any Phase, $m_0 \neq m_1$ is required, and m_0 is uniformly randomly generated among all messages not equal to m_1. The Adversary's *advantage* is the probability, minus 1/2, that $b' = b$.
3. **(sub-)Game IB-IND-CCA:** That $m_0 \neq m_1$ is required, and m_0 is uniformly randomly generated among all messages not equal to m_1. The Adversary's *advantage* is the probability, minus 1/2, that $b' = b$.

Definition 5. *An IBE scheme (MKg, UKg, encrypt, decrypt) is* IB-OW-CPA *(resp.* IB-IND-CPA, IB-IND-CCA*) secure if no PPT adversary has a non-negligible advantage in Game* IB-OW-CPA *(resp.* IB-IND-CPA, IB-IND-CCA*).*

In contrast to similar security notions for (non-IB) encryptions, we allow queries to $\mathcal{KEO}$, and typically simulate these queries by backpatching the random oracle in our proofs.

3.3 ID-based Signature

An identity-based signature (IBS) scheme is a four-tuple (MKg, UKg, IBSS, IBSV) specified as follow.

– MKg, UKg are defined before.
– $(\sigma) \leftarrow \mathsf{IBSS}(\mathrm{ID}, mpk, usk, m)$ is a PPT algorithm which, on input ID, mpk, usk and message m, generate a signature σ.
– $\mathsf{Accept/Reject} \leftarrow \mathsf{IBSV}(\mathrm{ID}, mpk, m, \sigma)$ is a PPT algorithm which, on input ID, signature σ, message m, output Accept or Reject.

An IBS should satisfy two properties, namely, completeness and soundness.

(**Completeness.**) A legitimate signature should be accepted. Formally, for all security parameter λ_s and $\forall \mathrm{ID} \in \{0,1\}^*, (mpk, msk) \in [\mathsf{MKg}(1^{\lambda_s})]$, and $usk \in [\mathsf{UKg}(\mathrm{ID}, mpk, msk)]$, $\mathsf{Accept} \leftarrow \mathsf{IBSV}(\mathrm{ID}, mpk, m, \sigma)$ with overwhelming probability if $\sigma \leftarrow \mathsf{IBSS}(\mathrm{ID}, mpk, usk, m)$.

(**Soundness.**) An invalid signature should be rejected. Formally, for all security parameter λ_s and $\forall \mathrm{ID} \in \{0,1\}^*, (mpk, msk) \in [\mathsf{MKg}(1^{\lambda_s})]$, and $usk \in [\mathsf{UKg}(\mathrm{ID}, mpk, msk)]$, $\mathsf{Reject} \leftarrow \mathsf{IBSV}(\mathrm{ID}, mpk, m, \sigma)$ with overwhelming probability if $\sigma \nleftarrow \mathsf{IBSS}(\mathrm{ID}, mpk, usk, m)$.

Oracles: To model the attack scenario, we provide the adversary with the following oracles.

– $\mathcal{IO}$, $\mathcal{KEO}$ defined before.
– *Signing Oracle*: $\sigma \leftarrow \mathcal{SO}(\mathrm{ID}, mpk, m)$. Upon inputs $\mathrm{ID} \in \{\mathrm{ID}\}$, mpk and message m, output a signature σ such that $\mathsf{Accept} \leftarrow \mathsf{IBSV}(\mathrm{ID}, mpk, m, \sigma)$.

Security notions The accepted security notion for IBS is existential unforgeability against adaptive chosen ID and message attack (uf-cma).

[**Game IB-UF-CMA**]
1. Setup Phase: Dealer $\mathcal{D}$ runs $\mathsf{MKg}(1^{\lambda_s})$ to obtain (mpk, msk).
2. Probe Phase: Adversary $\mathcal{A}$ can issue queries to the oracles. At some point, $\mathcal{A}$ chooses a gauntlet ID, ID_G, to forge a signature with on any message of its choice. $\mathcal{A}$ cannot submit ID_G to $\mathcal{KEO}$ and it must be returned from $\mathcal{IO}$.
3. Delivery Phase: At the end, $\mathcal{A}$ submit a signature σ for message m of ID_G. m and ID_G pair must not be submitted to $\mathcal{SO}$ before. $\mathcal{D}$ outputs either Accept (if $\mathsf{Accept} \leftarrow \mathsf{IBSV}(\mathrm{ID}, mpk, m, \sigma)$) or Reject (otherwise).

The advantage of adversary is defined as the probability that Dealer output Accept.

Definition 6. *An IBS scheme (MKg, UKg, IBSS, IBSV) is* uf-cma-secure *if no PPT adversary has non-negligible advantage in Game IB-UF-CMA.*

3.4 Blind ID-based Signature

An blind identity-based signature (BIBS) scheme is a five-tuple (MKg, UKg, IBP, Warden, IBSV) specified as follow.

– MKg, UKg, IBP, IBSV are defined before.

– $(\sigma) \leftarrow \mathsf{Warden}(\mathrm{ID}, mpk, m)$ is a PPT algorithm which, on input ID, mpk, and message m, interact with IBP and generate a signature σ as follow.
  - IBP sends a commitment t to Warden.
  - Warden sends a challenge c to IBP.
  - IBP provides a response s.
  - Warden output σ such that $\mathsf{Accept} \leftarrow \mathsf{IBSV}(\mathrm{ID}, mpk, m, \sigma)$.

An BIBS should satisfy three properties, namely, blindness, completeness and soundness.

(**Blindness.**) The signature outputted by Warden cannot be linked to any of the conversation between Warden and IBP. Formally, let the adversary keeps the transcript $\mathcal{T}$ of the interaction between IBP and Warden. Then given a valid σ, we say that BIBS is blind if:

$$Prob\{\sigma \ by \ \mathsf{Warden}\} = Prob\{\sigma \ by \ \mathsf{Warden}|\mathcal{T}\}$$

(**Completeness.**) A legitimate signature should be accepted. Formally, for all security parameter λ_s and $\forall \mathrm{ID} \in \{0,1\}^*, (mpk, msk) \in [\mathsf{MKg}(1^{\lambda_s})]$, and $usk \in [\mathsf{UKg}(\mathrm{ID}, mpk, msk)]$, $\mathsf{Accept} \leftarrow \mathsf{IBSV}(\mathrm{ID}, mpk, m, \sigma)$ with overwhelming probability if $\sigma \leftarrow \mathsf{Warden}(\mathrm{ID}, mpk, m)$ (interacted with IBP(initialized with ID, usk, mpk).

(**Soundness.**) An invalid signature should be rejected. Formally, for all security parameter λ_s and $\forall \mathrm{ID} \in \{0,1\}^*, (mpk, msk) \in [\mathsf{MKg}(1^{\lambda_s})]$, and $usk \in [\mathsf{UKg}(\mathrm{ID}, mpk, msk)]$, $\mathsf{Reject} \leftarrow \mathsf{IBSV}(\mathrm{ID}, mpk, m, \sigma)$ with overwhelming probability if $\sigma \nleftarrow \mathsf{Warden}(\mathrm{ID}, mpk, m)$ (interacted with IBP(initialized with ID, usk, mpk).

Oracles: To model the attack scenario, we provide the adversary with oracles $\mathcal{IO}$, $\mathcal{KEO}$ and $\mathcal{IBPO}$ which are as specified before.

Security notions: Accepted security notion for BIBS scheme is security against parallel one-more existential forgery attack. Consider the following game (**Game IB-UF-P1M**).

1. Setup Phase: Dealer $\mathcal{D}$ runs $\mathsf{MKg}(1^{\lambda_s})$ to obtain (mpk, msk).
2. Probe Phase: Adversary $\mathcal{A}$ can issue queries to the oracles. In particular, $\mathcal{A}$ can issue queries to $\mathcal{IBPO}$ for q_b times. Queries to oracles can be made concurrently and in an interleaving manner.
3. Delivery Phase: $\mathcal{A}$ produces $q_b + 1$ triples of $(\mathrm{ID}_i, m_i, \sigma_i)$ for $i = 1, ...q_b + 1$ such that ID_i has never been submitted to $\mathcal{KEO}$. $\mathcal{A}$ wins the game if all the signatures are valid and all $\mathrm{ID}_i \in \{\mathrm{ID}\}$.

The advantage of adversary is defined as the probability that it wins **Game IB-UF-P1M**.

Definition 7. *A BIBS scheme (MKg, UKg, IBP, Warden, IBSV) is* one-more-unforgeable(uf-p1m-secure) *if no PPT adversary can win* ***Game IB-UF-P1M*** *with non-negligible advantage.*

4 ID-based Identifications from CDR

We present several IBI's which are derived from four bandwidth-efficient CDR-based encryption schemes, namely Paillier[33], Catalano et al.[8], Galindo, et al.[16], and Kurosawa et al.[26]. Then we prove the equivalence of their securities to well-known hard problems. A general method of constructing IBI's from other bandwidth-efficient encryption schemes is presented in Appendix B.

Paillier1-IBI and Paillier2-IBI schemes

MKg On input 1^{λ_s}, generate two primes p,q from $\mathcal{SP}(\lambda_s)$, compute $N = pq$. Chooses cryptographic hash function $H_1 : \{0,1\}^* \to \mathbb{Z}^*_{N^2}$ and compute $g = 1 + N$. The master secret key is (p, q).

UKg For an identity ID, the secret key is a pair $(x, y) \in (\mathbb{Z}_N, \mathbb{Z}^*_N)$ such that $g^x y^N = H_1(\mathrm{ID})$.

Identification Protocol

1. IBP chooses $r_1 \in_R \mathbb{Z}_N$,$r_2 \in_R \mathbb{Z}^*_N$, computes $t = \theta({g^{r_1}}{r_2}^N \bmod N^2)$ and sends t to IBV.
2. IBV chooses $c \in \mathbb{Z}_N$, and sends c to IBP.
3. IBP computes $s_1 = r_1 - cx \bmod N$, $s_2 = r_2 y^{-c} \bmod N$ and sends s_1, s_2 to IBV.
4. IBV verifies whether $t = \theta(H_1(\mathrm{ID})^c {g^{s_1}}{s_2}^N \bmod N^2)$

In Paillier1-IBI, θ is the identity mapping. In Paillier2-IBI, θ is a collision-free secure hashing of suitable range and domain ($\theta : \mathbb{Z}^*_{N^2} \to \mathbb{Z}^*_{N^2}$).

CGHGN1-IBI and CGHGN2-IBI schemes

MKg On input 1^{λ_s}, generate two primes p,q from $\mathcal{SP}(\lambda_s)$, compute $N = pq$. Choose a sufficiently large prime e satisfying $gcd(e, \lambda(N^2)) = 1$. Chooses cryptographic hash function $H_1 : \{0,1\}^* \to \mathbb{Z}^*_{N^2}$ and compute $g = 1 + N$. The master secret key is (p, q).

UKg For an identity ID, the secret key is a pair $(x, y) \in (\mathbb{Z}_N, \mathbb{Z}^*_N)$ such that $g^x y^e = H_1(\mathrm{ID})$.

Identification Protocol

1. IBP chooses $r_1 \in_R \mathbb{Z}_N$,$r_2 \in_R \mathbb{Z}^*_N$, computes $t = \theta(g^{r_1} {r_2}^e \bmod N^2)$ and sends t to IBV.
2. IBV chooses $c \in \mathbb{Z}_e$, and sends c to IBP.
3. IBP computes $s_1 = r_1 - cx \bmod N$, $s_2 = r_2 y^{-c} \bmod N^2$ and sends s_1, s_2 to IBV.
4. IBV verifies whether $t = \theta(H_1(\mathrm{ID})^c g^{s_1} {s_2}^e \bmod N^2)$

In CGHGN1-IBI, θ is the identity mapping. In CGHGN2-IBI, θ is a collision-free secure hashing of suitable range and domain ($\theta : \mathbb{Z}^*_{N^2} \to \mathbb{Z}^*_{N^2}$).

How large is e sufficiently large? The prime exponent e has to be sufficiently large to guard against the impersonation described in Appendix A. We have in mind e is 80 to 160 bits.

GMMV-IBI scheme

MKg On input 1^{λ_s}, generate two primes p,q from $\mathcal{SP}(\lambda_s)$, compute $N = pq$. Choose random prime exponent e (of length λ_e) such that $gcd(e, \lambda(N)) = 1$. Chooses cryptographic hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}^*_{N^2}$. The master secret key is (p, q, d) such that $de = 1 \bmod \lambda(N)$. Also publish some small integer K and ℓ.

UKg For an identity ID, the secret key is $(x_k, y_k) \in (\mathbb{Z}^*_N, \mathbb{Z}_N)$ such that $x_k^{2e} + y_k N = H_1(\text{ID}||k) = Q_k \bmod N^2$ for $k = 1, \cdots, K$.

Identification Protocol

Repeat the following for $\tau = 1, \cdots, \ell$:

1. IBP chooses $r_{1,\tau} \in_R \mathbb{Z}^*_N$,$r_{2,\tau} \in_R \mathbb{Z}_N$, computes $t_\tau = {r_{1,\tau}}^{2e} + r_{2,\tau} N \bmod N^2$ and sends t_τ to IBV.
2. IBV sends a binary vector $(c_{1,\tau}, \cdots, c_{K,\tau})$ to IBP.
3. IBP sends to IBV $s_{1,\tau} = r_{1,\tau} \prod (x_k)^{-c_{k,\tau}} \bmod N^2$ and $s_{2,\tau} = r_{2,\tau} r_{1,\tau}^{-2e} - \sum c_{k,\tau} y_k x_k^{-2e} \bmod N$.
4. V verifies whether $t_\tau = s_{1,\tau}^{2e} (1+N)^{s_{2,\tau}} \prod (Q_k)^{c_{k,\tau}} \bmod N^2$.

We have in mind $k\ell \approx 80$ to 160.

Given a random ID and a random "tail" k, the probability of Q_k being a quadratic residue (QR) and therefore the probability of successfully producing x_k is only about 1/4. There are at least two techniques to increase that probability towards 1. The first technique follows [12]. The hashing is iterated (up to a certain limit), $H_1(H_1(\cdots(ID)\cdots))$, until it yields the first value, $\bar{Q}$, whose Jacobi symbol $(\frac{\bar{Q}}{N}) = 1$. Then user is told which one of $\bar{Q}$ and $-\bar{Q}$ is a quadratic residue in mod N. The IBI can be altered by having the sender tell, in the first move, which one of $\bar{Q}$ and $-\bar{Q}$ is QR. Or, two, the IBI can be conducted in parallelism of two, for $\bar{Q}$ and for $-\bar{Q}$, respectively. Note that testing for $(\frac{\bar{Q}}{N}) = 1$ without knowledge of the factoring of N is efficient [12]. This technique require $N = pq$ such that $p \equiv q \equiv 3 \bmod 4$ and is satisfied when N is safe-prime modulus.

The second technique alters UKg by decrypting multiple Q's with multiple tails. If a sufficient number of tails are decrypted, at least one of $H(\text{ID}||tail)$ is likely to be a quadratic residue mod N, and produces the user secret key successfully.

KT-IBI scheme

MKg On input 1^{λ_s}, generate two primes p,q from $\mathcal{SP}(\lambda_s)$, compute $N = pq$. Choose random $\alpha \in_R \mathbb{Z}_N$ such that $(\frac{\alpha}{p}) = (\frac{\alpha}{q}) = -1$.Chooses cryptographic hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}^*_{N^2}$. The master secret key is (p, q). Also publish some small integer K and ℓ .

UKg For an identity ID, the secret key is $(x_k, y_k) \in (\mathbb{Z}^*_N, \mathbb{Z}_N)$ such that $Q_k = H_1(\text{ID}) = (x_k + \alpha/x_k) + y_k N \bmod N^2$ for $k = 1, \cdots, K$. Denote $A_k = (x_k + \alpha/x_k) \bmod N^2$ and $B_k = (x_k - \alpha/x_k) \bmod N^2$.

Identification Protocol

Repeat the following for $\tau = 1, \cdots, \ell$:

1. IBP chooses $r_{1,\tau} \in_R \mathbb{Z}^*_N$,$r_{2,\tau} \in_R \mathbb{Z}_N$, computes $t_\tau = {r_{1,\tau}}^2 + r_{2,\tau} N \bmod N^2$ and sends t_τ to IBV.
2. IBV sends a binary vector $(c_{1,\tau}, \cdots, c_{K,\tau})$ to IBP.

3. IBP sends to IBV $s_{1,\tau} = r_{1,\tau} \prod (B_k)^{-c_{k,\tau}} \bmod N^2$ and $s_{2,\tau} = r_{2,\tau} r_{1,\tau}^{-2} - \sum c_{k,\tau} 2 y_k A_k B_k^{-2} \bmod N$.
4. IBV verifies whether $t_\tau = s_{1,\tau}^2 (1+N)^{s_{2,\tau}} \prod ({Q_k}^2 - 4\alpha)^{c_{k,\tau}} \bmod N^2$.

Security Analyses We prove the equivalence of the securities of our IBI schemes to well-known hard problems in the random oracle model. Proofs are in the Appendices.

Theorem 1. *Paillier1-IBI, Paillier2-IBI,CGHGN1-IBI, CGHGN2-IBI, GMMV-IBI, KT-IBI are HVZK.*

Theorem 2. *Paillier1-IBI is pa1-ib-imp (resp. pa2-ib-imp) secure, if and only if RSA[n,n] is hard, in the random oracle model (ROM). Paillier2-IBI is pa1-ib-imp (resp. pa2-ib-imp, 2s-aa-ib-imp, 2s-ca-ib-imp) secure, if and only if RSA[n,n] is hard, in ROM.*

Theorem 3. *CGHGN1-IBI is pa1-ib-imp (resp. pa2-ib-imp) secure, if and only if RSA[n,e] is hard, in ROM. CGHGN2-IBI is pa1-ib-imp (resp. pa2-ib-imp, 2s-aa-ib-imp, 2s-ca-ib-imp) secure, if and only if RSA[n,e] is hard, in ROM.*

Theorem 4. *GMMV-IBI is pa1-ib-imp (resp. pa2-ib-imp, 2s-aa-ib-imp, 2s-ca-ib-imp) secure, if and only if and only if factoring is hard, in ROM.*

Theorem 5. *KT-IBI is pa1-ib-imp (resp. pa2-ib-imp, 2s-aa-ib-imp, 2s-ca-ib-imp) secure, if and only if and only if factoring is hard, in ROM.*

Theorem 6. *Paillier1-IBI (resp. CGHGN1-IBI) is 2s-ca-ib-imp and 2s-aa-ib-imp secure if and only if its identity-based prover has ERZK, in ROM.*

These Theorems are proved in Appendices C, D, E, F, G, K.

We have not been able to prove Paillier1-IBI or CGHGN1-IBI has ERZK. There are may methods in the literature to convert an arbitrary HKZK scheme to one which is statistical ZK[1, 32, 17]. These methods can be used to convert Paillier1-IBI and CGHGN1-IBI to statistical ZK and therefore ERZK. Then a similar theorem to Theorem 6 can be proved to establish the 2s-ca-ib-imp security of the converted scheme. However, many known methods of conversion increases the number of moves beyond 3 moves, or decresse the length/entropy of the challenge, or both. It is an open problem to prove the 3-move Paillier1-IBI or CGHGN1-IBI has ERZK.

5 ID-based encryption from CDR

Motivated by Cocks [12], we construct an IBE scheme from CDR, called CDR-IBE. Its security is proven equivalence to a new hard problem. Furthermore, we prove the equivalence of the security of Cock's original IBE [12] to this new problem.

[**CDR-IBE scheme**]

MKg Same as Paillier1-IBI, but with the additionally requirement $p = q = 3 \bmod 4$.

UKg For an identity ID, compute $Q = H_1^\star(\text{ID})$, where hashing H_1 is applied repeatedly until the first result Q whose Jacobi symbol is $(\frac{Q}{N}) = +1$. The secret key is $(flag, x, y)$ where (Case 1) $flag = 1$, $g^x y^{2N} = Q$, if $Q \in \mathbb{QR}_N$; or (Case 2) $flag = -1$, $g^x y^{2N} = -Q$, if $-q \in \mathbb{QR}_N$.

encrypt message $m \in \{-1, +1\}$: Choose $t, t' \in Z_n$ with $(\frac{t}{N}) = (\frac{t'}{N}) = m$. Randomly generate r, r'. Send $c = g^r(t + Q/t)$ and $c' = g^{r'}(t' - Q/t')$.

decrypt If $flag = 1$, then compute message$=(\frac{c+2y^N \bmod N}{N})$. Else, compute message$=(\frac{c'+2y^N \bmod N}{N})$.

Note that the Jacobi symbol can be computed without knowing the factoring of N[12].

Security analyses of CDR-IBE and of Cocks' IBE[12]: We prove the equivalence of the security of CDR-IBE (resp. Cock's IBE[12]) to a new hard problem, the JSR Problem. We also prove JSR is at least as hard as QRP. We also present a conversion of CDR-IBE to an IB-IND-CCA secure IBE scheme.

Definition 8. (Jacobi Symbol of Roots of 2 Quadratic Polynomials (JSR) Problem) *Let $N = pq$ where primes $p \equiv q \equiv 3 \bmod 4$, $p = 2p' + 1$, $q = 2q' + 1$ and p', q' are also primes. $(\frac{\pi}{N}) = 1$, and $\sigma^2 - 4\pi, (\sigma')^2 + 4\pi \in \mathbb{QR}_N$. Let $f(X) = X^2 - \sigma X + \pi$, $f'(X) = X^2 - \sigma' X - \pi$, t is any root of $f(X)$ and t' is any root of $f'(X)$. The* JSR Problem *is to compute, based on the above assumptions:*

$$JSR(N, \pi, \sigma, \sigma') = \begin{cases} (\frac{t}{N}), & \text{if } \pi \in \mathbb{QR}_N \\ (\frac{t'}{N}), & \text{if } -\pi \in \mathbb{QR}_N \end{cases}$$

Note either polynomial has four roots in Z_N. If $\pi \in \mathbb{QR}_N$ then the four roots of $f(X)$ have identical Jacobi symbols while exactly two of the roots of $f'(X)$ have positive Jacobi symbols. If $-\pi \in \mathbb{QR}_N$ then the four roots of $f'(X)$ have identical Jacobi symbols while two of the roots of $f(X)$ have positive Jacobi symbols. In JSR, roots from different polynomials may have different Jacobi symbols. Also $(\frac{-1}{p}) = (\frac{-1}{q}) = -1$, $(\frac{-1}{N}) = 1$, $(\frac{\pi}{N}) = (\frac{-\pi}{N})$.

Lemma 7 *The JSR Problem is at least as hard as QRP.*

Proof Sketch: Set $\sigma = t + \pi/t$, $\sigma' = t' - \pi/t'$ where $(\frac{t}{N}) = 1$ and $(\frac{t'}{N}) = -1$, and the solution of JSR also solves QRP. □

Theorem 8. *CDR-IBE is IB-OW-CPA secure if and only if the JSR Problem is hard, in ROM.*

Proof Sketch: W.l.o.g, $\pi \in \mathbb{QR}_N$, and $\sigma = t + \pi/t$, $\sigma' = t' - \pi/t'$. Easily, breaking IB-OW-CPA is equivalent to computing JSR with the additional assumption that $(\frac{t}{N}) = (\frac{t'}{N})$ which reflects a valid ciphertext. Note $f(X)$ has four roots with identical Jacobi symbols, while $f'(X)$ has four roots, exactly two of which have posibive Jacobi symbols. It is witness indistinguishable to decryptor

whether $(\frac{t'}{N})$ is +1 or -1. Therefore the additional assumption can be dropped and the theorem is proved. □.

Using the same security model and the same proof technique, we can easily obtain that

Corollary 9 *Cocks' IBE[12] is IB-OW-CPA if and only if JSR is hard, in ROM.*

It remains an open problem to prove JSR equivalent to QRP.

There are well-known methods to convert an OW-CPA encryption to an IND-CCA encryption[3, 13, 33]. They can be used to convert CDR-IBE to an IB-IND-CCA-secure IBE with multi-bit messages. We demonstrate by using OAEP[3]. Let $\mathbf{m}$ be a multi-bit message, G and H be secure hashing functions. Randomly generate $\mathbf{r}$. Let $\mathbf{s} = (\mathbf{m}||0^\ell) \oplus G(\mathbf{r})$, $\mathbf{t} = H(s) \oplus \mathbf{r}$, ctxt be the bit-by-bit CDR-IBE encryption of $(\mathbf{s}||\mathbf{t})$. Then the scheme is IB-IND-CCA secure in ROM, provided the padding length ℓ is sufficiently large.

The particular conversion in Cocks [12] can also be used. But it comes without a formal proof of security.

We make the observation that CDR-IBE (resp. Cocks' IBE) can be used as an *oblivious transfer (OT)*[15]. In a *1-2 OT*, Alice sends Bob two messages, Bob receives at most one, and Alice does not know which one. In a *chosen 1-2 OT*[28], Bob gets to choose which one he receives. CDR-IBE (resp. Cock's IBE) can be used as a chosen 1-2 OT as follows: Alice and Bob both know N, and Bob may know its factoring. Bob generates π, $(\frac{\pi}{N}) = 1$, and sends it to Alice. Alice verifies $(\frac{\pi}{N}) = 1$, then encrypts multi-bit message m_0 to the case $\pi \in \mathbb{QR}_N$ bit-by-bit, and she encrypts multi-bit message m_1 to the case $-\pi \in \mathbb{QR}_N$ bit-by-bit, using CDR-IBE (resp. Cocks' IBE). This is indeed a chosen 1-2 OT: Alice is assured Bob can only decrypt one message, but she does not know which one. But its bandwidth efficiency is poor.

6 ID-Based Signature, Blind Signature, Ring Signature

We can further transform our proposed IBI into IBS schemes following the Fiat-Shamir paradigm. The resulting schemes are shown below.

Paillier1-IBS and Paillier2-IBS schemes

MKg Same as Paillier1-IBI, except picking one more cryptographic hash function, $H_2 : \mathbb{Z}_{N^2} \times \mathbb{Z}^*_{N^2} \to \mathbb{Z}_N$.

UKg Same as Paillier1-IBI.

IBSS On input message m, randomly pick $r_1 \in_R \mathbb{Z}_N$,$r_2 \in_R \mathbb{Z}^*_N$ and computes:

1. $t = \theta(g^{r_1} {r_2}^N \bmod N^2)$
2. $c = H_2(m, t)$
3. $s_1 = r_1 - cx \bmod N$
4. $s_2 = r_2 y^{-c} \bmod N$

Return the signature $(t, s_1, s_2) \in (\mathbb{Z}^*_{N^2}, \mathbb{Z}_N, \mathbb{Z}^*_N)$

IBSV Check whether $t = \theta(H_1(\mathrm{ID})^{H_2(m,t)} g^{s_1} {s_2}^N \bmod N^2)$

CGHGN1-IBS and CGHGN2-IBS schemes

MKg Same as CGHGN1-IBI, except picking one more cryptographic hash function, $H_2 : \mathbb{Z}_{N^2} \times \mathbb{Z}^*_{N^2} \rightarrow \mathbb{Z}_e$.

UKg Same as CGHGN1-IBI.

IBSS On input message m, randomly pick $r_1 \in_R \mathbb{Z}_N$,$r_2 \in_R \mathbb{Z}^*_N$ and computes:

1. $t = \theta(g^{r_1} {r_2}^e \bmod N^2)$
2. $c = H_2(m, t)$
3. $s_1 = r_1 - cx \bmod N$
4. $s_2 = r_2 y^{-c} \bmod N^2$

Return the signature $(t, s_1, s_2) \in (\mathbb{Z}^*_{N^2}, \mathbb{Z}_N, \mathbb{Z}^*_{N^2})$

IBSV Check whether $t = \theta(H_1(\mathrm{ID})^{H_2(m,t)} g^{s_1} {s_2}^N \bmod N^2)$

GMMV-IBS scheme

MKg Same as GMMV-IBI, except picking one more cryptographic hash function, $H_2 : \{0,1\}^* \rightarrow \{0,1\}^{K\ell}$.

UKg Same as GMMV-IBI.

IBSS On input message m, Randomly pick $r_{1,\tau} \in_R \mathbb{Z}_N$,$r_{2,\tau} \in_R \mathbb{Z}^*_N$ for $\tau = 1, \cdots, \ell$ and computes:

1. $t_\tau = r_{1,\tau}^{2e} + r_{2,\tau} N \bmod N^2$
2. $[c_{1,1}, \cdots, c_{K,1}, \cdots, c_{1,\ell}, \cdots, c_{K,\ell}] = H_2(m, t_1, \cdots, t_\ell)$
3. $s_{1,\tau} = r_{1,\tau} \prod (x_k)^{-c_{k,\tau}} \bmod N^2$ and $s_{2,\tau} = r_{2,\tau} r_{1,\tau}^{-2e} - \sum c_{k,\tau} y_k x_k^{-2e} \bmod N$.

Return the signature $(t_1, \cdots, t_\ell, s_{1,1}, \cdots s_{1,\ell}, s_{2,1} \cdots, s_{2,\ell})$

IBSV Compute $[c_{1,1}, \cdots, c_{K,1}, \cdots, c_{1,\ell}, \cdots, c_{K,\ell}] = H_2(m, t_1, \cdots, t_\ell)$. Check whether $t_\tau = s_{1,\tau}^{2e} (1+N)^{s_{2,\tau}} \prod (Q_k)^{c_{\tau,k}} \bmod N^2$ for $\tau = 1, \cdots, \ell$.

KT-IBS scheme

MKg Same as KT-IBI, except picking one more cryptographic hash function, $H_2 : \{0,1\}^* \rightarrow \{0,1\}^{K\ell}$.

UKg Same as KT-IBI.

IBSS On input message m, Randomly pick $r_{1,\tau} \in_R \mathbb{Z}_N$,$r_{2,\tau} \in_R \mathbb{Z}^*_N$ for $\tau = 1, \cdots, \ell$ and computes:

1. $t_\tau = r_{1,\tau}^{2e} + r_{2,\tau} N \bmod N^2$
2. $[c_{1,1}, \cdots, c_{K,1}, \cdots, c_{1,\ell}, \cdots, c_{K,\ell}] = H_2(m, t_1, \cdots, t_\ell)$
3. $s_{1,\tau} = r_{1,\tau} \prod (B_k)^{-c_{k,\tau}} \bmod N^2$ and $s_{2,\tau} = r_{2,\tau} r_{1,\tau}^{-2} - \sum c_{k,\tau} 2 y_k A_k B_k^{-2} \bmod N$.

Return the signature $(t_1, \cdots, t_\ell, s_{1,1}, \cdots s_{1,\ell}, s_{2,1} \cdots, s_{2,\ell})$

IBSV Compute $[c_{1,1}, \cdots, c_{K,1}, \cdots, c_{1,\ell}, \cdots, c_{K,\ell}] = H_2(m, t_1, \cdots, t_\ell)$. Check whether $t_\tau = s_{1,\tau}^2 (1+N)^{s_{2,\tau}} \prod ({Q_k}^2 - 4\alpha)^{c_{k,\tau}} \bmod N^2$ for $\tau = 1, \cdots, \ell$.

Security Analyses of IBI's: We prove the security of our signature schemes. It is well-know that passive secure and HVZK identification schemes produces uf-cam-secure signatures via the Fiat-Shamir paradigm. We have the following theorem. Proof omitted.

Theorem 10. *Paillier1-IBS (resp. Paillier2-IBS, CGHGN1-IBS, CGHGN2-IBS, GMMV-IBS, KT-IBS) is uf-cma-secure if and only if RSA[n,n] (resp. RSA[n,n], RSA[n,e], RSA[n,e], Factoring, Factoring) is hard, in ROM.*

ID-based blind signature (BIBS) We extend our Paillier1-IBS and CGHGN1-IBS to Blind IBS (BIBS) as follows.

Paillier1-BIBS and CGHGN1-BIBS schemes
In Paillier1-BIBS, $M = N$ while in CGHGN1-BIBS, $M = e$.
MKg Same as corresponding IBS.
UKg Same as corresponding IBS.
IBP Same as corresponding IBI.
IBSV Same as corresponding IBS.
Warden

1. Warden send a request to IBP and receive commitment t.
2. Warden chooses $r_3 \in_R \mathbb{Z}_N$,$r_4 \in_R \mathbb{Z}_N^*$, $\delta \in_R \mathbb{Z}_M$ and computes $t' = H_1(\mathrm{ID})^{\delta} t g^{r_3} {r_4}^M \mod N^2$. Warden then computes $c' = H_2(m, t')$ and $c = c' - \delta + rM$ for some integer c, r such that $0 \leq c < M$. Sends c to IBP.
3. IBP returns s_1, s_2 to Warden.
4. Warden computes $s_1' = s_1 + r_3 \mod N$, $s_2' = H_1(\mathrm{ID})^r s_2 r_4 \mod N$ (for CGHGN1-BIBS, Warden computes s_2' in $\mathbb{Z}_{N^2}^*$instead of $\mathbb{Z}_N^*$). Warden outputs (m, t', s_1', s_2') as the signature of message m.

Theorem 11. *Our blind identity-based signatures, Paillier1-BIBS and CGHGN1-BIBS, have blindness.*

ID-based ring signature, and its blind version: We also present the first identity-based ring signature (IBRS) and blind identity-based ring signature (BIBRS), from paillier1-IBI, in Appendix H.

7 Conclusion

We have presented 4 different IBI schemes from CDR and extend them to IBS. We also extend some of them to BIBS and IBRS. We also construct an encryption scheme from CDR motivated by Cocks. We provide rigorous definition of security models and proven our constructions under them. In particular, we provide a thorough hierarchy of attacker models for IBI. Our schemes are possibly more efficient than other pairing-based identity-based signature schemes as pairing operations is expensive. It is also possible to extend our scheme using composite degree greater than 2 as in [34].

Acknowledgements. Helpful discussions between the first author and P. K. Tsang are acknowledged.

References

1. M. Bellare, S. Micali, and R. Ostrovsky. The (true) complexity of statistical zero-knowledge. In *Proc. STOC'90*, pages 494–502, 1990.

2. M. Bellare and A. Palacio. GQ and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In *Proc. CRYPTO 2002*, pages 162–177. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2442.
3. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. 1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.
4. Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes. In *Proc. EUROCRYPT 2004*, pages 268–286. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3027.
5. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *Proc. CRYPTO 2001*, pages 213–229. Springer-Verlag, 2001. Lecture Notes in Computer Science No. 2139.
6. E. Bresson, D. Catalano, and D. Pointcheval. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. In *Proc. ASIACRYPT 2003*, pages 37–54. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2894.
7. J. Camenisch and V. Shoup. Practical verifiable encryption and decryption of discrete logarithms. In *Proc. CRYPTO 2003*, pages 126–144. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2729.
8. D. Catalano, P. Gennaro, N.Howgrave-Graham, and P. Nguyen. Paillier's cryptosystem revisited. *ACM Communication and Computer Security -CCS'01, ACM pp.206-214, ACM*, 2001.
9. J. C. Cha and J. H. Cheon. An identity-based signature from gap diffie-hellman groups. In *PKC 2003*, pages 18–30. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2567.
10. Tony K. Chan, Karyin Fung, Joseph K. Liu, and Victor K. Wei. Blind spontaneous anonymous group signatures for ad hoc groups. *To be appeared in ESAS*, 2004.
11. D. Chaum. Blind signatures for untraceable payments. In *Proc. CRYPTO 82*, pages 199–203. Plenum Press, 1982.
12. C. Cocks. An identity based encryption scheme based on quadratic residues. In *Cryptography and coding*, pages 360–363. Springer-Verlag, 2001. Lecture Notes in Computer Science No. 2260.
13. R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Proc. CRYPTO 98*, pages 13–25. Springer-Verlag, 1998. Lecture Notes in Computer Science No. 1462.
14. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Proc. CRYPTO 86*, pages 196–194. Springer-Verlag, 1986. Lecture Notes in Computer Science No. 263.
15. M. J. Fischer, S. Micali, and C. Rackoff. A secure protocol for the oblivious transfer. In *Journal of Cryptology*, volume 9(3), pages 191–195, March 1996.
16. D. Galindo, S. Mollevi, P. Morillo, and J. Villar. A practical public key cryptosystem from paillier and rabin schemes. In *PKC'03*, pages 279–291. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2567.
17. O. Goldreich, A. Sahai, and S. Vadhan. Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In *Proc. 30th ACM Symposium on Theory of Computing*, pages 399–408. ACM Press, 1998.
18. Oded Goldreich. Zero-knowledge twenty years after their invention. *http://www.wisdom.weizmann.ac.il/ oded/papers.html*, 2002.

19. S. Goldwasser and S. Micali. Probabilistic encryption. In *Journal of Computer and System Sciences*, volume 28(2), pages 270–299, April 1984.
20. L. Guillou and J. J. Quisquater. A paradoxical identity-based signature scheme resulting from zero-knowledge. In *Proc. CRYPTO 88*, pages 216–231. Springer-Verlag, 1988. Lecture Notes in Computer Science No. 403.
21. Javier Herranz and German Saez. A provably secure id-based ring signature scheme. *eprint*, 2003(261), 2003.
22. F. Hess. Efficient identity based signature schemes based on pairings. In *SAC 2002*, pages 310–324. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2595.
23. K. Kurosawa and Swee-Huay Heng. From digital signature to id-based identification/signature. In *PKC'04*, pages 248–261. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 2947.
24. K. Kurosawa, T. Itoh, and M. Takeuchi. Public key cryptosystem using reciprocal number with the same intractability as factoring a large number. In *Cryptologia*, volume XII, pages 225–233, 1988.
25. K. Kurosawa, W. Ogata, T. Matsuo, and S. Makishima. Ind-cca public key schemes equivalent to factoring n=pq. In *PKC'01*, pages 36–47. Springer-Verlag, 2001. Lecture Notes in Computer Science No. 1992.
26. K. Kurosawa and T. Takagi. Some rsa-based encryption schemes with tight security reduction. In *Proc. ASIACRYPT 2003*, pages 19–36. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2894.
27. Chih-Yin Lin and Tzong-Chen Wu. An identity-based ring signature scheme from bilinear pairings. *eprint*, 2003(117), 2003.
28. Y. Mu, J. Zhang, and V. Varadharajan. m out of n oblivious transfer. In *Proc. ACISP 2002*, pages 395–405. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2384.
29. D. Naccache and J. Stern. A new public-key cryptosystem based on higher residues. In *Proc. 5th ACM Conference on Computer and Communications Security*, pages 59–66. ACM Press, 1998.
30. T. Okamato and S. Uchiyama. A new public-key cryptosystem as secure as factoring. In *Proc. EUROCRYPT 98*, pages 308–318. Springer-Verlag, 1998. Lecture Notes in Computer Science No. 1403.
31. T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In *Proc. CRYPTO 92*, pages 231–253. Springer-Verlag, 1992. Lecture Notes in Computer Science No. 740.
32. T. Okamoto. On relationships between statistical zero-knowledge proofs. In *Proc. STOC'96*, pages 649–658, 1996.
33. P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Proc. EUROCRYPT 99*, pages 223–238. Springer-Verlag, 1999. Lecture Notes in Computer Science No. 1592.
34. P. Paillier and D. Pointcheval. Efficient public-key cryptosystems provably secure against active adversaries. In *Proc. ASIACRYPT 99*, pages 165–179. Springer-Verlag, 1999. Lecture Notes in Computer Science No. 1716.
35. K. G. Paterson. Id-based signatures from pairings on elliptic curves. *eprint*, 2002(004), 2002.
36. R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In *Proc. ASIACRYPT 2001*, pages 552–565. Springer-Verlag, 2001. Lecture Notes in Computer Science No. 2248.

37. A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. CRYPTO 84*, pages 47–53. Springer-Verlag, 1984. Lecture Notes in Computer Science No. 196.
38. X. Yi. An identity-based signature scheme from the weil pairing. *IEEE Communications Letters*, 7(2):76–78, 2003.
39. F. Zhang and K. Kim. ID-Based blind signature and ring signature from pairings. In *Proc. ASIACRYPT 2002*, pages 533–547. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2501.
40. F. Zhang, R. Safavi-Naini, and W. Susilo. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings. In *Proc. INDOCRYPT 2003*, pages 191–204. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2904.

A Small exponent cryptanalysis of CGHGN1 and 2

The value of e should be chosen sufficiently large such that the following impersonation probability is sufficiently small: For $Q = H_1(\mathrm{ID})$, adversary obtains from Conversation Oracle (t, c, s_1, s_2), then impersonate with $(t, \hat{c}, s_1, \hat{s_2})$ where $\hat{s_2} = Q^{(c-\hat{c})/e} s_2 \bmod N^2$ for any challenge $\hat{c}$ such that $e \mid (c - \hat{c})$. It is safe to use e of length 80 bits. In our setting, we set challenge to be within $\mathbb{Z}_e$ so that such cryptanalysis is not possible.

B Transformation from Encryption to ID-based Identification

We outline a transform to build IBI from encryption schemes satisfying certain conditions.

B.1 Requirement for Encryption

We call an encryption scheme Π satisfy the following requirements a convertible encryption scheme.

- Π is OW-CPA secure and without known CCA attacks.
- Π is bandwidth-efficient, in the sense that the combined length of plaintext m and randomness used in encryption r roughly equals the length of the ciphertext c.
- The relation ((m,r),c) is in $\mathcal{NP}$.
- There exists cryptographic hash function H such that its range is in the ciphertext space with non-negligible probability.
- Decryption of the ciphertext c recovers both message m and randomness r.

Roughly speaking, a suitable encryption scheme Π=(Kg, Encrypt, Decrypt) can be transformed into an IBI, (MKg, UKg, IBP, IBV), as follow.

MKg $\mathsf{MKg}(1^{\lambda_s}) = \mathsf{Kg}(1^{\lambda_s})$ On input security parameter 1^{λ_s}, run Kg and obtain (pk, sk). The master public key $mpk = pk$ and master secrete key $msk = sk$.

UKg $\mathsf{UKg}(\mathrm{ID}, mpk, msk) = usk = \mathsf{Decrypt}(H(\mathrm{ID}))$. On input ID, randomly generate *tail* and compute Q=H(ID||*tail*) such that Q is decryptable. Run $\mathsf{Decrypt}(\mathrm{Q},sk)$ and obtain (m,r). The user secret key is (m,r) and *tail* is also given to the user. If the output of H is always decryptable, then *tail* is not needed.

Identification Protocol Since the relation (usk, H(Q||*tail*))is $\mathcal{NP}$, by theorem 5 in [18], a protocol of zero-knowledge proof exists. In the implementation, since *tail* is unknown to the verifier, prover has to send the tail to verifier in advance.

Remarks: [18] provides an efficient systematic implementation of the zero-knowledge proof. However, it is impractical. To yield a practical IBI, simple designs in the paradigm of a 3-move Σ protocol should be handcrafted.

C Proof of Theorem 1

Simulator $\mathcal{S}$ can generate transcript of Paillier1-IBI for any ID such that $H_1(\mathrm{ID}) = Q$ as follow:

1. Randomly generate $c, s_1 \in_R \mathbb{Z}_N$ and $s_2 \in_R \mathbb{Z}_N^*$.
2. Compute $t = Q^c g^{s_1} {s_2}^N \bmod N^2$
3. the simulated transcript is (t, c, s_1, s_2).

It is easy to verify that the generated transcript is indistinguishable from actual transcript. Similarly, $\mathcal{S}$ can generate transcript of Paillier2-IBI, CGHGN1-IBI, CGHGN2-IBI, GMMV-IBI and KT-IBI. Thus, Paillier1-IBI, Paillier2-IBI ,CGHGN1-IBI, CGHGN2-IBI, GMMV-IBI and KT-IBI are HVZK (wrt secret key). □.

D Proof of Theorem 2

It is obvious that if an adversary can solve RSA[n,n] problem, it can extract the private key for all ID and can thus break Paillier1-IBI and Paillier2-IBI. We prove the pa1-ib-imp security of Paillier1-IBI first.

Setup Dealer $\mathcal{D}$ gives (N, u) to simulator $\mathcal{S}$ and ask $\mathcal{S}$ to compute y such that $y^N = u \bmod N$. Set $mpk = N$.

Oracle Simulation

1. ($\mathcal{IO}$) Randomly generate a set of ID $\in \{0,1\}^*$. Return {ID}.
2. (H_1 **Oracle**) Assume $\mathcal{I}$ makes q_{H_1} queries to the oracle. Let ID_i be the i^{th} query to the H_1 oracle. $\mathcal{S}$ chooses $r \in [1, ..., q_{H_1}]$ and set $H_1(\mathrm{ID}_r) = u$. For other H_1 query for ID_i, $\mathcal{S}$ randomly generate x_i, y_i and set $H_1(\mathrm{ID}_i) = g^{x_i} y_i^N$.
3. ($\mathcal{KEO}$)When $\mathcal{I}$ query $\mathcal{KEO}$ for ID_i, $\mathcal{S}$ return (x_i, y_i). If $\mathcal{I}$ query $\mathcal{KEO}$ for ID_r, $\mathcal{S}$ output failure and abort.
4. ($\mathcal{CO}$) Suppose $H_1(\mathrm{ID}) = Q$, $\mathcal{S}$ random generate c, s_1, s_2, compute $t = Q^c g^{s_1} s_2^N \bmod N^2$. Then return (t, c, s_1, s_2).

Witness Extraction Eventually, impersonator $\mathcal{I}$ output the gauntlet ID and act as cheating prover. If the gauntlet ID is not ID_r, output failure and abort. Do rewind simulation once and obtain two valid transcripts with same commitment from $\mathcal{I}$, namely, (t, c, s_1, s_2), $(t, \hat{c}, \hat{s_1}, \hat{s_2})$. Assume $t = g^a b^N \bmod N^2$.

$$\begin{aligned} g^a b^N &= g^{cx+s_1}(y^c s_2)^N \bmod N^2 \\ g^a b^N &= g^{\hat{c}x+\hat{s_1}}(y^{\hat{c}} \hat{s_2})^N \bmod N^2 \\ x &= (\hat{s_1} - s_1)/(c - \hat{c}) \bmod N \end{aligned}$$

The last equation come from the fact that $[t]_g$ is unique modulo N. $\mathcal{S}$ can compute y as follow.

$$\begin{aligned} t &= u^c (s_2)^N \bmod N \\ t &= u^{\hat{c}} (\hat{s_2})^N \bmod N \\ u^{c-\hat{c}} &= (\hat{s_2}/s_2)^N \bmod N \end{aligned}$$

Denote by s $\hat{s_2}/s_2 \bmod N$. $\mathcal{S}$ then compute (d, k_1, k_2) such that $d = \gcd(N, c - \hat{c})$ and $k_1 N + k_2(c - \hat{c}) = d$. If $d \neq 1$, then $\mathcal{S}$ successfully factorize N (since $0 < c, \hat{c} < N$). Hence, $k_1 N + k_2(c - \hat{c}) = 1$. $u = u^{k_1 N} u^{k_2(c-\hat{c})} = (u^{(k_1)}(s)^{k_2})^N \bmod N$. Thus, $y = u^{k_1} s^{k_2} \bmod N$.

We proceed to prove the pa2-ib-imp security of Paillier1-IBI. The proof is similar except the simulation of the prover oracle which is outlined as follow.

Oracle Simulation $\mathcal{IBPO}$: Suppose $H_1(\mathrm{ID}_i) = Q_i$, since the secret key for ID_i is known, $\mathcal{S}$ can stimulate perfectly. The only ID $\mathcal{S}$ cannot stimulate is ID_r, but query to $\mathcal{IBPO}$ for ID_r is not allowed in the pa2-ib-imp Subgame.

We proceed to prove the 2s-ca-ib-imp security of Paillier2-IBI, which implies the 2s-aa-ib-imp security, pa2-ib-imp security and pa1-ib-imp security.

Setup Dealer $\mathcal{D}$ gives (N, u) to simulator $\mathcal{S}$ and ask $\mathcal{S}$ to compute y such that $y^N = u \bmod N$. Set $mpk = N$.

Oracle Simulation

1. ($\mathcal{IO}$) Randomly generate a set of ID $\in \{0,1\}^*$. Return $\{\mathrm{ID}\}$.
2. (H_1 **Oracle**) Assume $\mathcal{I}$ makes q_{H_1} queries to the oracle. Let ID_i be the i^{th} query to the H_1 oracle. $\mathcal{S}$ chooses $r \in [1, ..., q_{H_1}]$ and set $H_1(\mathrm{ID}_r) = u$. For other H_1 query for ID_i, $\mathcal{S}$ randomly generate x_i, y_i and set $H_1(\mathrm{ID}_i) = g^{x_i} y_i^N$.
3. ($\mathcal{KEO}$)When $\mathcal{I}$ query $\mathcal{KEO}$ for ID_i, $\mathcal{S}$ return (x_i, y_i). If $\mathcal{I}$ query $\mathcal{KEO}$ for ID_r, $\mathcal{S}$ output failure and abort.
4. ($\mathcal{IBPO}$) $\mathcal{S}$ simulate $\mathcal{IBPO}$ by backpatching the θ oracle as follow. $\mathcal{S}$ randomly generate t such that t is different from all the previous output of the θ oracle and send t as commitment. When challenge c come, $\mathcal{S}$ randomly generate random generate s_1, s_2 and compute $h = Q^c g^{s_1} s_2^N \bmod N^2$. Backpatch $\theta(h) = t$.

Witness Extraction This is similar to the proof in Paillier1-IBI. By doing rewind simulation once, $\mathcal{S}$ obtain two transcripts (t, c, s_1, s_2) and $(t, \hat{c}, \hat{s_1}, \hat{s_2})$. By

lunchtime argument, $\mathcal{I}$ must have query θ oracle such that there exists h with $t = \theta(h)$. $\mathcal{S}$ can compute y as follow.

$$h = u^c(s_2)^N \bmod N$$
$$h = u^{\hat{c}}(\hat{s_2})^N \bmod N$$
$$u^{c-\hat{c}} = (\hat{s_2}/s_2)^N \bmod N$$

Denote by s $\hat{s_2}/s_2 \bmod N$. $\mathcal{S}$ then compute (d, k_1, k_2) such that $d = \gcd(N, c-\hat{c})$ and $k_1N + k_2(c - \hat{c}) = d$. If $d \neq 1$, then $\mathcal{S}$ successfully factorize N (since $0 < c, \hat{c} < N$). Hence, $k_1N+k_2(c-\hat{c}) = 1$. $u = u^{k_1N}u^{k_2(c-\hat{c})} = (u^{(k_1)}(s)^{k_2})^N \bmod N$. Thus, $y = u^{k_1}s^{k_2} \bmod N$. □.

E Proof Sketch of Theorem 3

It is obvious that if an adversary can solve RSA[n,e] problem, it can extract the private key for all ID and can thus break CGHGN1-IBI and CGHGN2-IBI. We first prove the pa1-ib-imp security of CGHGN1-IBI.

Setup Dealer $\mathcal{D}$ gives (N, e, u) to simulator $\mathcal{S}$ and ask $\mathcal{S}$ to compute the RSA[n,e] problem on u. Set $mpk = (N, e)$.

Oracle Simulation

1. ($\mathcal{IO}$) Randomly generate a set of ID $\in \{0,1\}^*$. Return {ID}.
2. (H_1 **Oracle**) Assume $\mathcal{I}$ makes q_{H_1} queries to the oracle. Let ID_i be the i^{th} query to the H_1 oracle. $\mathcal{S}$ chooses $r \in [1, ..., q_{H_1}]$ and set $H_1(\mathrm{ID}_r) = u$. For other H_1 query for ID_i, $\mathcal{S}$ randomly generate x_i, y_i and set $H_1(\mathrm{ID}_i) = g^{x_i}y_i^e \bmod N^2$.
3. ($\mathcal{KEO}$)When $\mathcal{I}$ query $\mathcal{KEO}$ for ID_i, $\mathcal{S}$ return (x_i, y_i). If $\mathcal{I}$ query $\mathcal{KEO}$ for ID_r, $\mathcal{S}$ output failure and abort.
4. ($\mathcal{CO}$) Suppose $H_1(\mathrm{ID}) = Q$, $\mathcal{S}$ random generate c, s_1, s_2, compute $t = Q^c g^{s_1} s_2^e \bmod N^2$. Then return (t, c, s_1, s_2).

Witness Extraction Eventually, impersonator $\mathcal{I}$ output the gauntlet ID and act as cheating prover. If the gauntlet ID is not ID_r, output failure and abort. Do rewind simulation once and obtain two valid transcripts with same commitment from $\mathcal{I}$, namely, (t, c, s_1, s_2) and $(t, \hat{c}, \hat{s_1}, \hat{s_2})$.

$$t = u^c(s_2)^e \bmod N$$
$$t = u^{\hat{c}}(\hat{s_2})^e \bmod N$$
$$u^{c-\hat{c}} = (\hat{s_2}/s_2)^e \bmod N$$

Denote by s $\hat{s_2}/s_2 \bmod N$. $\mathcal{S}$ then compute (d, k_1, k_2) such that $d = \gcd(e, c-\hat{c})$ and $k_1e+k_2(c-\hat{c}) = d$. Since $0 < c, \hat{c} < e$, $d = 1$. Hence, $k_1e+k_2(c-\hat{c}) = 1$. $u = u^{k_1e}u^{k_2(c-\hat{c})} = (u^{(k_1)}(s)^{k_2})^e \bmod N$. Thus, $y = u^{k_1}s^{k_2} \bmod N$. $\mathcal{S}$ successfully compute $y \in [0, ..., N-1]$ such that $y^e = u \bmod N$ and win the game.

We proceed to prove the pa2-ib-imp security of CGHGN1-IBI. The proof is similar except the simulation of the prover oracle which is outlined as follow.

Oracle Simulation $\mathcal{IBPO}$: Suppose $H_1(\mathrm{ID}_i) = Q_i$, since the secret key for ID_i is known, $\mathcal{S}$ can stimulate perfectly. The only ID $\mathcal{S}$ cannot stimulate is ID_r, but query to $\mathcal{IBPO}$ for ID_r is not allowed in the pa2 Subgame.

We proceed to prove the 2s-ca-ib-imp security of CGHGN2-IBI, which implies the 2s-aa-ib-imp security, pa2-ib-imp security and pa1-ib-imp security.

Setup Dealer $\mathcal{D}$ gives (N, u) to simulator $\mathcal{S}$ and ask $\mathcal{S}$ to compute y such that $y^e = u \bmod N$. Set $mpk = (N, e)$.

Oracle Simulation

1. ($\mathcal{IO}$) Randomly generate a set of ID $\in \{0,1\}^*$. Return {ID}.
2. (H_1 **Oracle**) Assume $\mathcal{I}$ makes q_{H_1} queries to the oracle. Let ID_i be the i^{th} query to the H_1 oracle. $\mathcal{S}$ chooses $r \in [1, ..., q_{H_1}]$ and set $H_1(\mathrm{ID}_r) = u$. For other H_1 query for ID_i, $\mathcal{S}$ randomly generate x_i, y_i and set $H_1(\mathrm{ID}_i) = g^{x_i} y_i^e$.
3. ($\mathcal{KEO}$)When $\mathcal{I}$ query $\mathcal{KEO}$ for ID_i, $\mathcal{S}$ return (x_i, y_i). If $\mathcal{I}$ query $\mathcal{KEO}$ for ID_r, $\mathcal{S}$ output failure and abort.
4. ($\mathcal{IBPO}$) $\mathcal{S}$ simulate $\mathcal{IBPO}$ by backpatching the θ oracle as follow. $\mathcal{S}$ randomly generate t such that t is different from all the previous output of the θ oracle and send t as commitment. When challenge c come, $\mathcal{S}$ randomly generate random generate s_1, s_2 and compute $h = Q^c g^{s_1} s_2^e \bmod N^2$. Backpatch $\theta(h) = t$.

Witness Extraction This is similar to CGHGN1-IBI and is thus omitted.□.

F Proof Sketch of Theorem 4

It is obvious that if an adversary can solve factorization problem, it can extract the private key for all ID and can thus break the system. We proves the 2s-ca-ib-imp security of GMMV-IBI which implies the 2s-aa-ib-imp, pa2-ib-imp and pa1-ib-imp security.

Setup The proof is by witness indistinguishability. Dealer $\mathcal{D}$ gives (N) to simulator $\mathcal{S}$. $\mathcal{S}$ generate a large prime e, two small number K, ℓ. Set $mpk = (N, e, K, \ell)$.

Oracle Simulation

1. ($\mathcal{IO}$) Randomly generate a set of ID $\in \{0,1\}^*$. Return {ID}.
2. (H_1 **Oracle**) For query for ID, $\mathcal{S}$ randomly generate x_i, y_i (for $i = 1, \cdots, K$) and set $H_1(\mathrm{ID}||i) = {x_i}^{2e} + y_i N \bmod N^2$.
3. ($\mathcal{KEO}$) When $\mathcal{I}$ query $\mathcal{KEO}$ for ID, $\mathcal{S}$ return (x_i, y_i) (for $i = 1, \cdots, K$).
4. ($\mathcal{IBPO}$) $\mathcal{S}$ knows all the secret keys and can thus simulate perfectly.

Witness Extraction Eventually, impersonator $\mathcal{I}$ output the gauntlet ID and act as cheating prover. Do rewind simulation once (for any rounds, say, round j). For visual comfort , we drop the subscript j here. Two valid transcripts with same commitment from $\mathcal{I}$, namely, $(t, \boldsymbol{c}, s_1, s_2)$, $(t, \hat{\boldsymbol{c}}, \hat{s_1}, \hat{s_2})$ are obtained.

Here, $\boldsymbol{c}$ and $\hat{\boldsymbol{c}}$ are binary vectors.

$$t = s_1^{2e} \prod_{c[i]=1} x_i^{2e} \bmod N$$
$$t = \hat{s_1}^{2e} \prod_{\hat{c}[i]=1} x_i^{2e} \bmod N$$
$$(\hat{s_1}/s_1)^2 = (\prod_{c[i]=1} x_i / \prod_{\hat{c}[i]=1} x_i)^2 \bmod N$$

Since $\mathcal{I}$ cannot distinguish which square root $\mathcal{S}$ is using, with probability 1/2, $\hat{s_1}/s_1 \neq \pm(\prod_{c[i]=1} x_i/\prod_{\hat{c}[i]=1} x_i) \bmod N$. $\mathcal{S}$ compute the gcd of their difference and successfully factorize N. □.

G Proof Sketch of Theorem 5

It is obvious that if an adversary can solve factorization problem, it can extract the private key for all ID and can thus break the system. We proves the 2s-ca-ib-imp security of KT-IBI which implies the 2s-aa-ib-imp, pa2-ib-imp and pa1-ib-imp security.

Setup The proof is by witness indistinguishability. Dealer $\mathcal{D}$ gives (N) to simulator $\mathcal{S}$. $\mathcal{S}$ generate α and two small number K, ℓ. Set $mpk = (N, \alpha, K, \ell)$.

Oracle Simulation

1. ($\mathcal{IO}$) Randomly generate a set of ID $\in \{0,1\}^*$. Return {ID}.
2. (H_1 **Oracle**) For query for ID, $\mathcal{S}$ randomly generate x_i, y_i (for $i = 1, \cdots, K$) and set $H_1(\text{ID}||i) = (x_i + \alpha/x_i) + y_i N = Q_i \bmod N^2$.
3. ($\mathcal{KEO}$)When $\mathcal{I}$ query $\mathcal{KEO}$ for ID, $\mathcal{S}$ return (x_i, y_i) (for $i = 1, \cdots, K$).
4. ($\mathcal{IBPO}$) $\mathcal{S}$ knows all the secret keys and can thus simulate perfectly.

Witness Extraction Eventually, impersonator $\mathcal{I}$ output the gauntlet ID and act as cheating prover. Do rewind simulation once (for any rounds, say, round j). For visual comfort , we drop the subscript j here. Two valid transcripts with same commitment from $\mathcal{I}$, namely, $(t, \boldsymbol{c}, s)$, $(t, \hat{\boldsymbol{c}}, \hat{s})$ are obtained. Here, $\boldsymbol{c}$ and $\hat{\boldsymbol{c}}$ are binary vectors.

$$t = s^2 \prod_{c[i]=1} ({Q_i}^2 - 4\alpha) \bmod N$$
$$t = \hat{s_1}^2 \prod_{\hat{c}[i]=1} ({Q_i}^2 - 4\alpha) \bmod N$$
$$(\hat{s_1}/s_1)^2 = (\prod_{c[i]=1} (x_i - \alpha/x_i) / \prod_{\hat{c}[i]=1} (x_i - \alpha/x_i))^2 \bmod N$$

Since $\mathcal{I}$ cannot distinguish which square root $\mathcal{S}$ is using, with probability 1/2, $\hat{s_1}/s_1 \neq \pm(\prod_{c[i]=1}(x_i - \alpha/x_i)/\prod_{\hat{c}[i]=1}(x_i - \alpha/x_i) \bmod N$. $\mathcal{S}$ compute the gcd of their difference and successfully factorize N. □.

H ID-based ring signature and its blind version

We construct IBRS (identity-based ring signature) from Paillier1-IBI and its blind identity-based ring signature (BIBRS) version. For details of the security model, see [10]. (For completeness, the primitive and security model of IBRS is shown in appendix J.)

Paillier1-IBRS scheme

MKg Same as the Paillier1-IBI, except picking another cryptographic hash function $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_N$

UKg Same as the Paillier1-IBI.

RingSign Let $L = \{ID_1, ID_2, ..., ID_k\}$ be the set of the k identities. For some message $m \in \{0,1\}^*$, a signer π uses his private key (x_π, y_π) to generate a (1,k)-ring signature with respect to L as follows. Randomly pick $r_1 \in_R \mathbb{Z}_N$,$r_2 \in_R \mathbb{Z}_N^*$ and computes:

1. $t = g^{r_1} {r_2}^N \bmod N^2$
2. $c_{\pi+1} = H_2(L, m, t)$
3. For $i = \pi+1, ..., k, 1, ..., \pi-1$, pick $s_i \in_R \mathbb{Z}_N$, $s'_i \in_R \mathbb{Z}_N^*$ and compute $c_{i+1} = H_2(L, m, H_1(\mathrm{ID}_i)^{c_i} g^{s_i} {s'_i}^N \bmod N^2)$
4. s_π, α such that $s_\pi + \alpha N = r_1 - x_\pi c_\pi$, for some integer α and $0 \leq s_\pi < N$.
5. $s'_\pi = g^\alpha r_2 y^{-c} \bmod N$
6. The ring signature on m is $(L, c_1, s_1, s'_1, s_2, s'_2, ..., s_k, s'_k)$.

RingVerify A public verifier checks a signature on m $(L, c_1, s_1, s'_1, s_2, s'_2, ..., s_k, s'_k)$ of a set of identities as follow.

1. For $i = 1, ..., k-1$, compute $c_{i+1} = H_2(L, m, H_1(ID_i)^{c_i} g^{s_i} {s'_i}^N)$
2. Check whether $c_1 = H_2(L, m, H_1(ID_k)^{c_k} g^{s_k} {s'_k}^N) \bmod N^2$.
3. If yes, accept, otherwise, reject.

Remarks: Paillier ring signature can be used as a Zero-Knowledge proof-of-membership identification scheme.

I Proof of Theorem 11

(Paillier1-BIBS, CGHGN1-BIBS) In Paillier1-BIBS, $M = N$ while in CGHGN1-BIBS, $M = e$. Let $\mathcal{S}$ be IBP and obtain usk from UKg(ID, mpk, msk). Suppose $\mathcal{S}$ gets $\sigma_j = (t_j, s_{1,j}, s_{2,j})$ and message m_j where $t_j = H_1(\mathrm{ID})^{H_2(t_j, m_j)} g^{s_{1,j}} s_{2,j}^M \bmod N^2$ for $j \in [0, ..., k]$. Let $(t_i, c_i, s_{1,i}, s_{2,i})$ for $i = 0, ..., k$ be the data exchanged during the blind signature generation protocol.

It is sufficient to show that there exist blinding factors that maps each of the $(t_i, c_i, s_{1,i}, s_{2,i})$ to (σ_j, m_j). Since we have

$$
\begin{aligned}
t_i &= H_1(\mathrm{ID})^{c_i} g^{s_{1,i}} s_{2,i}^M \bmod N^2 \\
t_i H_1(\mathrm{ID})^\delta &= H_1(\mathrm{ID})^{c_i + \delta} g^{s_{1,i}} s_{2,i}^M \bmod N^2 \\
t_i H_1(\mathrm{ID})^\delta g^{r_3} {r_4}^M &= H_1(\mathrm{ID})^{c_i + \delta} g^{s_{1,i} + r_3} (s_{2,i} r_4)^M \bmod N^2
\end{aligned}
$$

There always exists δ, r_3, r_4 such that $c_i+\delta = H_2(t_j, m_j)$, $s_{1,i}+r_3 = s_{1,j} \bmod N$ and $s_{2,i}r_4 = s_{2,j} \bmod N$ ($\bmod N^2$ for CGHGN1-BIBS here). Then, $t_j = t_i H_1(\mathrm{ID})^{\delta} g^{r_3} {r_4}^M \bmod N^2$. As every data exchange during the signature generation protocol can lead to (σ_j, m_j), even an infinitely powerful $\mathcal{S}$ cannot tell which data exchange actually produce the signature with probability $> 1/k$. □.

J ID-based Ring Signature

An identity-based ring signature (IBRS) scheme is a four-tuple (MKg, UKg, RingSign, RingVerify) specified as follow.

- MKg, UKg are defined before.
- $(\sigma) \leftarrow \mathsf{RingSign}(\mathcal{L}, mpk, usk, m)$ is a PPT algorithm which, on input a list of ID $\mathcal{L}$, mpk, one usk corresponding to one of the ID in $\mathcal{L}$ and message m, generate a signature σ.
- $\mathsf{Accept/Reject} \leftarrow \mathsf{RingVerify}(\mathcal{L}, mpk, m, \sigma)$ is a PPT algorithm which, on input a list of ID $\mathcal{L}$, signature σ, message m, output Accept or Reject.

An IRBS should satisfy three properties, namely, completeness, soundness and signer ambiguity.(**Completeness.**) A legitimate signature should be accepted. Formally, for all security parameter λ_s and $\forall \mathrm{ID} \in \{0,1\}^*, (mpk, msk) \in [\mathsf{MKg}(1^{\lambda_s})]$, and $usk \in [\mathsf{UKg}(\mathrm{ID}, mpk, msk)]$, $\mathsf{Accept} \leftarrow \mathsf{RingVerify}(\{\mathrm{ID}\}, mpk, m, \sigma)$ with overwhelming probability if $\sigma \leftarrow \mathsf{RingSign}(\{\mathrm{ID}\}, mpk, usk, m)$.

(**Soundness.**) An invalid signature should be rejected. Formally, for all security parameter λ_s and $\forall \mathrm{ID} \in \{0,1\}^*, (mpk, msk) \in [\mathsf{MKg}(1^{\lambda_s})]$, and $usk \in [\mathsf{UKg}(\mathrm{ID}, mpk, msk)]$, $\mathsf{Reject} \leftarrow \mathsf{RingVerify}(\{\mathrm{ID}\}, mpk, m, \sigma)$ with overwhelming probability if $\sigma \nleftarrow \mathsf{RingSign}(\{\mathrm{ID}\}, mpk, usk, m)$.

(**Signer-ambiguity**) We gives a formal definition of signer-ambiguity. An IBRS scheme is unconditionally signer-ambiguous if any adversary(with infinite computing power) cannot tell the identity of the actual signer with probability greater than $1/r$, where r is the cardinality of the ring.

Oracles: To model the attack scenario, we provide the adversary with the following oracles.

- $\mathcal{IO}$, $\mathcal{KEO}$ defined before.
- *Ring Signing Oracle*: $\sigma \leftarrow \mathcal{RSO}(\mathcal{L}, mpk, usk, m)$. Upon inputs a list of ID$\mathcal{L}$, mpk and message m, output a signature σ such that $\mathsf{Accept} \leftarrow \mathsf{RingVerify}(\mathcal{L}, mpk, m, \sigma)$.

Security notions Security of IBRS scheme against existential forgery under adaptive chosen ID and message attack(ring-uf-cma) is defined in the following game(**Game RING-UF-CMA**).

1. Setup Phase: Dealer $\mathcal{D}$ runs $\mathsf{MKg}(1^{\lambda_s})$ to obtain (mpk, msk). mpk is then given to adversary $\mathcal{A}$.
2. Probe Phase: $\mathcal{A}$ can issue queries to oracles adaptively.

3. Delivery Phase: At the end, $\mathcal{A}$ submit a signature on m for the an ID list $\mathcal{L}$. m and $\mathcal{L}$ pair must not be submitted to $\mathcal{RSO}$ before and none of the ID in $\mathcal{L}$ has been submitted to $\mathcal{KEO}$. $\mathcal{D}$ outputs either Acceptor Reject

The advantage of adversary is defined as the probability that $\mathcal{D}$ outputs Accept.

Definition 9. *An IBRS scheme (MKg, UKg, RingSign, RingVerify) is* ring-uf-cma-secure *if no PPT adversary has non-negligible advantage in Game RING-UF-CMA.*

K Proof Sketch of Theorem 6

One direction of the proof is easy: If ERZK does not hold, then there exists a PPT algorithm which can compute usk from given mpk and ID with queries to $\mathcal{IBPO}_{\mathrm{ID}}$. To prove the opposite direction, assume there is a PPT algorithm $\mathcal{A}$ which can impersonate ID_G in Probe-2 Phase after completing all $\mathcal{IBPO}$ queries in Probe-1 Phase. Simulator $\mathcal{S}$ simulates $\mathcal{A}$. It also simulates, in ROM with backpatching if necessary, all of $\mathcal{A}$'s queries to $\mathcal{IO}$, $\mathcal{CO}$, $\mathcal{KEO}$. It also simulates all non-ID_G queries to $\mathcal{IBPO}$ by backpatching usk. It simulates $\mathcal{IBPO}_{\mathrm{ID}_G}$ queries by consulting the real-world $\mathcal{IBPO}_{\mathrm{ID}_G}$ oracle. Then $\mathcal{S}$ rewinds $\mathcal{A}$ to the challenge in Probe-2, to extract usk. □.