11-2008

A new framework for the design and analysis of identity-based identification schemes

Guomin YANG
Singapore Management University, gmyang@smu.edu.sg

Jing CHEN

Duncan S. WONG

Xiaotie DENG

Dongsheng WANG

Citation

YANG, Guomin; CHEN, Jing; WONG, Duncan S.; DENG, Xiaotie; and WANG, Dongsheng. A new framework for the design and analysis of identity-based identification schemes. (2008). *Theoretical Computer Science*. 407, (1-3), 370-388.
Available at: https://ink.library.smu.edu.sg/sis_research/7400

Theoretical Computer Science 407 (2008) 370–388

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

A new framework for the design and analysis of identity-based identification schemes

Guomin Yang[a,*], Jing Chen[b], Duncan S. Wong[a], Xiaotie Deng[a], Dongsheng Wang[c]

[a] Department of Computer Science, City University of Hong Kong, Hong Kong, China

[b] Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA

[c] Department of Computer Science, Tsinghua University, Beijing, China

ARTICLE INFO

Article history:
Received 19 March 2008
Accepted 2 July 2008
Communicated by D.-Z. Du

Keywords:
Identity-based cryptography
Identification scheme
Passive attack
Active attack
Concurrent attack

ABSTRACT

Constructing an identification scheme is one of the fundamental problems in cryptography, and is very useful in practice. An identity-based identification (IBI) scheme allows a prover to identify himself to a public verifier who knows only the claimed identity of the prover and some public information. In this paper, we propose a new framework for both the design and analysis of IBI schemes. Our approach works in an engineering way. We first identify an IBI scheme as the composition of two building blocks, and then show that, with different security properties of these building blocks, the corresponding IBI schemes can achieve security against impersonation under different levels of attacks, namely, passive attack (id-imp-pa), active attack (id-imp-aa) or concurrent attack (id-imp-ca). In particular, we show that an id-imp-pa secure IBI scheme can be built if there exists a trapdoor weak-one-more relation and an honest verifier zero-knowledge proof with special soundness, while an id-imp-aa and id-imp-ca secure IBI scheme can be built if there exists a trapdoor strong-one-more relation and a *Witness Dualism proof with Special Soundness* (WD-SS). This new framework can capture IBI construction techniques that are not captured by other known frameworks. It also helps to construct new and efficient schemes. We demonstrate this by proposing two new IBI schemes, one achieving id-imp-pa, and the other one achieving both id-imp-aa and id-imp-ca, and neither of them can be captured by existing frameworks.

1. Introduction

An identification scheme enables an entity (the prover) to identify itself to another entity (the verifier) as the owner of some secret information. In a Standard Identification (SI) scheme, the prover holds a secret key and the verifier holds the corresponding public key. In an Identity-Based Identification (IBI) scheme, there is an authority holding a master public/secret key pair. Based on the the prover's identity and the master secret key, the authority generates a user secret key for the prover. The prover then identifies himself to the verifier, who knows only the prover's identity and the authority's master public key.

An adversary's goal against an identification scheme is to impersonate the prover. However, the adversary may not start from scratch. Instead, it may have eavesdropped communication between the prover and an honest verifier, or played the role of the verifier while communicating with the prover, already for a couple of times. To capture these types

[*] Corresponding author. Tel.: +852 27888638.
E-mail addresses: csyanggm@cs.cityu.edu.hk (G. Yang), jingchen@mit.edu (J. Chen), duncan@cs.cityu.edu.hk (D.S. Wong), deng@cs.cityu.edu.hk (X. Deng), wds@tsinghua.edu.cn (D. Wang).

0304-3975/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2008.07.001

of attack, corresponding security models are normally formalized into two stages. In stage one, the adversary obtains communication transcripts between the prover and an honest verifier, or plays the role of a (possibly malicious) verifier while communicating with the prover for a number of times. In stage two, given the information collected in stage one, the adversary's goal is to impersonate the prover, that is, to make an honest verifier accept it as the prover.

Varied by the different capabilities of the adversary in the first stage, three major notions of security for IBI schemes have been defined: security against impersonation under passive attack (id-imp-pa), active attack (id-imp-aa), and concurrent attack (id-imp-ca). In a passive attack, an adversary can obtain communication transcripts between the prover and an honest verifier. In an active or concurrent attack, the adversary can directly communicate with the prover by playing the role of a (possibly malicious) verifier. The difference between id-imp-aa and id-imp-ca is that in the former attack model, the adversary can only have one active session at a time, while in the latter one, the adversary can have concurrent sessions.

Since the introduction of identity-based cryptography by Shamir in 1984 [22], many IBI schemes have been proposed. A recent survey can be found in [2]. Also in [2], Bellare, Namprempre and Neven proposed a framework that transforms any SI scheme satisfying certain security conditions (referred to as a *convertible SI* scheme) to an IBI scheme with security against impersonation under certain attack (which is determined by the actual security conditions satisfied by the underlying convertible SI) in the random oracle model [4]. Independently, in [19], Kurosawa and Heng proposed another framework. This framework transforms any digital signature scheme, which is existentially unforgeable, against adaptive chosen message attacks [14], to an IBI scheme with id-imp-pa security.

1.1. Our results

We propose a new framework to construct provably secure IBI schemes. There are three contributions in this paper.

First, we show how to construct an IBI scheme from two building blocks: a hard relation and an interactive proof system. For the hard relation, we propose two types, namely *Trapdoor Weak-one-more Relation (TWR)* and *Trapdoor Strong-one-more Relation (TSR)*. For the interactive proof system, we consider a conventional honest verifier zero-knowledge proof with special soundness (HVZK-SS) and also propose a new notion, called *Witness Dualism proof with Special Soundness (WD-SS)* and show that Witness Dualism is a weaker form of *Witness Indistinguishability* [12]. We show that "TWR + HVZK-SS" yields an id-imp-pa secure IBI scheme, and "TSR + WD-SS" yields an IBI scheme which is both id-imp-aa and id-imp-ca secure, in the random oracle model [4]. We also show that, *without random oracle*, "TWR + HVZK-SS" and "TSR + WD-SS" frameworks yield IBI schemes with security against impersonation under passive attacks and active/concurrent attacks, respectively, in a newly proposed model called *Weak Selective-ID Model*. Second, we show that each of these new building blocks can be instantiated efficiently. We will see that a TWR can be built if there exists a trapdoor one-way permutation, or a signature scheme with existential unforgeability against *known* message attacks (rather than chosen message attacks), or if the Computational Diffie–Hellman (CDH) problem is hard. On the instantiation of TSR, we show that a TSR can be built if the factorization problem or the RSA problem is hard, or if there exists a strongly unforgeable signature scheme [1] (also referred to as *non-malleable* signature [23]) against *known* message attacks. By combining these instantiations according to the results in our first contribution above, we can see that many existing IBI schemes can be proven secure. This greatly helps explain how these existing IBI schemes are derived, and enable modular security analyzes.

Third, we show that this new framework also helps construct new and efficient IBI schemes. We propose two new IBI schemes, one with id-imp-pa security and the other one with both id-imp-aa and id-imp-ca security. The first one follows the "TWR + HVZK-SS" framework with a new TWR based on the K-sCAA1 problem [20,11]. The scheme is very efficient in terms of both computational complexity and communication overhead. The second IBI scheme follows the "TSR + WD-SS" framework. The TSR is instantiated using a strongly unforgeable signature scheme due to Katz and Wang [18]. The WD-SS proof system is newly constructed for the Katz–Wang signature based TSR. This proof system also illustrates that Witness Dualism is a weaker form of Witness Indistinguishability.

Compared with existing frameworks [2,19], our approach has the following advantages. The framework of [2] starts with a Convertible Standard Identification (cSI), while ours starts directly with an intractable problem or a more standard primitive. This allows our approach to include some IBI schemes which are not covered by the one in [2]. For example, most of the IBI schemes transformed from digital signature schemes cannot be captured by the framework of [2]. Our approach is also more generic than that of [19]. In [19], the transformation is restricted to an id-imp-pa secure IBI scheme, and it requires a signature scheme which is existentially unforgeable against chosen message attacks. Under our corresponding framework, namely "TWR + HVZK-SS", we require the signature scheme to be existentially unforgeable against *known* message attacks only , rather than chosen message attacks. In addition, our approach can also construct id-imp-aa and id-imp-ca secure IBI schemes.

1.2. Paper organization

In Section 2, we define IBI schemes and review the definitions of the three security levels (id-imp-pa, id-imp-aa, id-imp-ca). In Section 3, we propose the "TWR + HVZK-SS" framework for constructing id-imp-pa secure IBI schemes in the random oracle model. In Section 4, by modifying the security requirements of the building blocks, we change the framework to "TSR + WD-SS" and show that it can be used to build id-imp-aa and id-imp-ca secure IBI schemes. In Section 5, we propose two new IBI schemes under our framework. In Section 6, we evaluate the security of our frameworks proposed in Section 3 and Section 4, but in the standard model. We show that our frameworks achieve security against impersonation, under passive attack and active/concurrent attacks, respectively, in a new model called *Weak Selective-ID Model* without random oracle. The paper is concluded in Section 7.

2. Definitions and security models

Definition 1. An identity-based identification (IBI) scheme consists of four probabilistic polynomial-time (PPT) algorithms (**MKGen**, **UKGen**, **P**, **V**).

1. **MKGen**: On input 1^k, where $k \in \mathbb{N}$ is a security parameter, it generates a master public/secret key pair (mpk, msk).
2. **UKGen**: On input msk and some identity $I \in \{0, 1\}^*$, it outputs a user secret key $usk[I]$.
3. (**P**, **V**) – **User Identification Protocol**: The prover with identity I runs algorithm **P** with initial state $usk[I]$, and the verifier runs **V** with initial state (mpk, I). The first and last messages of the protocol belong to the prover. The protocol ends when **V** outputs either 'accept' or 'reject'.

Completeness: For all $k \in \mathbb{N}, I \in \{0, 1\}^*$, $(mpk, msk) \leftarrow \mathbf{MKGen}(1^k)$, and $usk[I] \leftarrow \mathbf{UKGen}(msk, I)$, **V** (initialized with mpk, I) always outputs 'accept' at the end of the User Identification Protocol after interacting with **P** (initialized with $usk[I]$).

The security of an IBI scheme is defined as against impersonation of the prover by an adversary who does not know the secret key of the prover. There are three levels of adversarial capabilities [2]: passive attack (id-imp-pa), active attack (id-imp-aa) and concurrent attack (id-imp-ca).

Definition 2 (*id-imp-pa*). For an IBI scheme (**MKGen**, **UKGen**, **P**, **V**), consider the following game carried out by a simulator against an adversary $\mathcal{A}$.

1. $(mpk, msk) \leftarrow \mathbf{MKGen}(1^k)$ is executed and mpk is given to $\mathcal{A}$. Two sets are maintained: HU and CU. Initially, both HU and CU are empty.
2. $\mathcal{A}$ can make queries to the following oracles:
   (a) INIT(I) – create a user with identity I: If $I \in HU \cup CU$, $\perp$ is returned indicating that I has already been created. Otherwise, $usk[I] \leftarrow \mathbf{UKGen}(msk, I)$ is executed and I is added into HU. A symbol '1' is returned indicating that the creation is successful.
   (b) CORR(I) – corrupt a user with identity I: If $I \notin HU$, $\perp$ is returned, otherwise, I is deleted from HU and added into CU, and $usk[I]$ is returned.
   (c) CONV(I) – get a conversation between user I (the prover) and a verifier: If $I \notin HU$, $\perp$ is returned, otherwise, a conversation between a prover with initial state $usk[I]$ and a verifier with initial state (mpk, I) is returned.
3. $\mathcal{A}$ can adaptively query INIT, CORR and CONV, and then output an identity $\mathrm{I_b} \in HU$, which corresponds to the user that $\mathcal{A}$ wants to impersonate. After receiving $\mathrm{I_b}$, the simulator removes $\mathrm{I_b}$ from HU and adds it into CU.
4. $\mathcal{A}$ begins a run of the user identification protocol with a verifier **V** (initialized with $(mpk, \mathrm{I_b})$) which is simulated by the simulator. $\mathcal{A}$ can continue querying INIT, CORR and CONV. The simulator halts when **V** outputs 'accept' or 'reject'.

The id-imp-pa advantage of $\mathcal{A}$ on security parameter k is defined as the probability that **V** outputs 'accept'. The IBI scheme (**MKGen**, **UKGen**, **P**, **V**) is said to be id-imp-pa secure if the id-imp-pa advantage is negligible for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$. Let $k \in \mathbb{N}$ be a security parameter. A function ϵ is negligible if for every constant $c \geq 0$, there exists an integer k_c such that $\epsilon(k) < k^{-c}$ for all $k \geq k_c$.

Id-imp-aa and id-imp-ca security. The id-imp-aa security is defined using a similar game, but having the conversation oracle, CONV, above be replaced by a proving oracle, PROV. When querying this oracle, $\mathcal{A}$ provides an identity $I \in$ HU and starts a conversation with PROV(I), which is the simulation of $\mathbf{P}(usk[I])$ by the simulator. The difference between id-imp-aa and id-imp-ca is that for the former one, $\mathcal{A}$ can only have one active session with PROV(I) at a time, but in the latter one, $\mathcal{A}$ can have concurrent sessions. The corresponding advantages of $\mathcal{A}$ are defined accordingly in the same way as that for id-imp-pa security. The IBI scheme (**MKGen**, **UKGen**, **P**, **V**) is said to be id-imp-aa (resp. id-imp-ca) if the id-imp-aa (resp. id-imp-ca) advantage is negligible for any PPT adversary $\mathcal{A}$.

3. A framework for constructing IBI schemes secure against passive attack

In this section, we propose a framework for constructing IBI schemes secure against impersonation under passive attack (id-imp-pa).

In this framework, an IBI scheme is considered as a composition of two building blocks: a hard relation and a proof system. For id-imp-pa security, we introduce a new notion called *Trapdoor Weak-one-more Relation* (TWR). In the following, we define TWR and show, in the random oracle model [4], that combining TWR (as the hard relation) with an Honest Verifier Zero Knowledge proof with Special Soundness (HVZK-SS), can build an id-imp-pa secure IBI scheme.

A binary relation **R** on $W \times \Delta$ is a set of ordered pairs (x, y) such that $x \in W$ and $y \in \Delta$, where x is called a witness of y. We denote the set of witnesses of y by $W(y)$.

Definition 3 (*TWR Family*). A family of trapdoor weak-one-more relations $\mathcal{R}$ is a triple of PPT algorithms (Gen, Ver, Inv):

1. $\mathcal{R}.Gen$: On input 1^k, where $k \in \mathbb{N}$ is a security parameter, it outputs $(\langle \mathbf{R} \rangle, t)$ where $\langle \mathbf{R} \rangle$ denotes the description of relation $\mathbf{R}$ on $W \times \Delta$ and t a trapdoor information.
2. $\mathcal{R}.Ver$: For any $k \in \mathbb{N}$ and $(\langle \mathbf{R} \rangle, t) \leftarrow \mathcal{R}.Gen(1^k)$, $\mathcal{R}.Ver(\langle \mathbf{R} \rangle, x, y) = 1$ if and only if $(x, y) \in \mathbf{R}$, otherwise, it outputs 0.
3. $\mathcal{R}.Inv$: On input $(\langle \mathbf{R} \rangle, y, t)$, it outputs a random witness $x \overset{R}{\leftarrow} W(y)$.
4. **Weak-one-more resistance**: Consider the following game against an adversary $\mathcal{A}$ which is given $\langle \mathbf{R} \rangle$ but not t, and has access to two oracles:
   (a) A challenge oracle RAM that on any input returns a random point $y \in \Delta$.
   (b) An inversion oracle INV that on any input y,
      i. if y is an output of RAM, a witness chosen uniformly at random from $W(y)$ is returned, and the same witness is returned if the same value of y is queried again;
      ii. if y is not an output of RAM, $\perp$ is returned indicating that the input is invalid.

   $\mathcal{A}$ wins if $\mathcal{A}$ finds witnesses for all the points output by RAM but makes strictly fewer queries to INV. We say that $\mathbf{R}$ is a Trapdoor Weak-one-more Relation (TWR) if the probability of winning the game is negligible in k for any PPT $\mathcal{A}$.

The TWR family $\mathcal{R}$ can be instantiated in many different ways. In Section 3.2, we describe several of them which have been used though not formalized before. In Section 5.1, we propose a new instantiation for TWR. This new instantiation is based on the K-sCAA1 problem [20,11].

Next, we review the Honest Verifier Zero-Knowledge proof with Special Soundness (HVZK-SS) with respect to a binary relation $\mathbf{R}$ on $W \times \Delta$.

An interactive proof system (P, V) is said to be **canonical** if it follows a three-move structure where prover P initiates a communication with verifier V by sending a *commitment* Cmt, which is distributed uniformly over a set CmtSet; V then replies with a *challenge* Ch, which is chosen uniformly from a set ChSet; and P finishes the communication by sending a *response* Rsp to V. V outputs 'accept' or 'reject' according to the output of a deterministic function $1/0 \leftarrow \mathbf{Dec}(St_V, \mathsf{Cmt}\|\mathsf{Ch}\|\mathsf{Rsp})$ where St_V is the initial state of V. The bit-string $\mathsf{Cmt}\|\mathsf{Ch}\|\mathsf{Rsp}$ is called a *conversation* between P and V. If **Dec** outputs 1, then $(\mathsf{Cmt}, \mathsf{Ch}, \mathsf{Rsp})$ is an *acceptable* transcript.

A canonical interactive proof system (P, V) has commitment length $\beta(\cdot)$ if $|\mathsf{CmtSet}| \geq 2^{\beta(k)}$, and challenge length $\lambda(\cdot)$ if $|\mathsf{ChSet}| \geq 2^{\lambda(k)}$. (P, V) is **non-trivial** if the function $2^{-\beta(k)}$ is negligible in k.

Definition 4. An HVZK-SS for a binary relation $\mathbf{R}$ on $W \times \Delta$ is a non-trivial canonical proof system (P, V), such that for any $y \in \Delta$,

1. **Completeness**. If P knows x such that $(x, y) \in \mathbf{R}$, then $\Pr[\mathsf{V} \text{ outputs accept}] = 1$.
2. **Special Soundness**. There exists a polynomial time algorithm which on input two acceptable transcripts $(\mathsf{Cmt}, \mathsf{Ch}_1, \mathsf{Rsp}_1)$ and $(\mathsf{Cmt}, \mathsf{Ch}_2, \mathsf{Rsp}_2)$ for $\mathsf{Ch}_1 \neq \mathsf{Ch}_2$, the algorithm outputs x such that $(x, y) \in \mathbf{R}$.
3. **Honest Verifier Zero Knowledge**. There exists a polynomial time algorithm $\mathcal{SIM}$ such that on input $(\langle \mathbf{R} \rangle, y)$, its output distribution is computationally indistinguishable from the distribution of a real conversation between P (initialized with a witness of y) and V (initialized with $\langle \mathbf{R} \rangle$ and y).

3.1. Our generic construction of id-imp-pa secure IBI schemes

We now propose the framework for constructing IBI schemes based on TWR family (Definition 3) and HVZK-SS proof system (Definition 4). The resulting IBI schemes can achieve id-imp-pa security.

Let $\mathsf{H} : \{0, 1\}^* \rightarrow \Delta$ be a hash function that is modeled as a random oracle [4] for security analysis. A generic IBI scheme is constructed as follows.

1. **MKGen**: $(\langle \mathbf{R} \rangle, t) \leftarrow \mathcal{R}.Gen(1^k)$. Set $mpk = \langle \mathbf{R} \rangle$ and $msk = t$.
2. **UKGen**: on input $I \in \{0, 1\}^*$, run $x \leftarrow \mathcal{R}.Inv(\langle \mathbf{R} \rangle, \mathsf{H}(I), t)$ and set $usk[I] = x$.
3. $(\mathbf{P}, \mathbf{V})$: run $\mathbf{P}$ with the prover algorithm P of the HVZK-SS proof system with initial state $usk[I]$, and $\mathbf{V}$ with the verifier algorithm V of the HVZK-SS proof system with initial state $(\langle \mathbf{R} \rangle, \mathsf{H}(I))$.

The following theorem states that an IBI scheme constructed as above is id-imp-pa secure (Definition 2).

Theorem 1. *Let $\mathbf{R}$ be a Trapdoor Weak-one-more Relation (TWR) which has an HVZK-SS proof system. If the challenge length $\lambda(k)$ of the HVZK-SS proof system is super logarithmic in k, where $k \in \mathbb{N}$ is a security parameter, then an IBI scheme constructed as above is id-imp-pa secure in the random oracle model.*

Proof. Suppose there exists an adversary $\mathcal{A}$, who breaks the generic IBI scheme above with advantage ϵ, we construct a PPT algorithm $\mathcal{B}$ to break the weak-one-more resistance of the underlying TWR with advantage $\epsilon' \geq (\epsilon - 2^{-\lambda(k)})^2$.

$\mathcal{B}$ simulates the id-imp-pa game by setting $mpk = \langle \mathbf{R} \rangle$ and maintains two sets HU and CU, which are initialized to empty. $\mathcal{B}$ also maintains a table T, each entry of T contains an identity I and the value of $\mathsf{H}(I)$. T is also initialized to empty at the beginning of the simulation. $\mathcal{B}$ answers $\mathcal{A}$'s queries as follows:

1. H-query: On input $I \in \{0, 1\}^*$, if $I \notin \mathrm{T}$, $\mathcal{B}$ queries its challenge oracle RAM to get a random point $y \in \Delta$, then sets $\mathrm{H}(I) = y$ by putting (I, y) into table T, and returns y. If $I \in \mathrm{T}$, the existing value of $\mathrm{H}(I)$ from T is returned.
2. INIT(I): If $I \in \mathrm{HU} \cup \mathrm{CU}$, $\perp$ is returned. Otherwise, $\mathcal{B}$ checks whether I is in table T. If $I \in \mathrm{T}$, I is added into HU and a symbol '1' is returned. Otherwise, $\mathcal{B}$ queries RAM to get a random point $y \in \Delta$, and sets $\mathrm{H}(I) = y$ by putting (I, y) in table T, I is then added into HU and a symbol '1' is returned.
3. CORR(I): If $I \notin \mathrm{HU}$, $\perp$ is returned. Otherwise, $\mathcal{B}$ queries INV to obtain a witness w for $\mathrm{H}(I)$ and returns w. I is then removed from HU and added into CU.
4. CONV(I): If $I \notin \mathrm{HU}$, $\perp$ is returned. Otherwise, $\mathcal{B}$ runs the simulation algorithm $\mathcal{SIM}$ (Definition 4) to generate a simulated transcript and returns it to $\mathcal{A}$.

If $\mathcal{A}$ successfully impersonates a user $\mathrm{I_b}$, that is created but not corrupted (i.e. $\mathrm{H(I_b)}$ is returned by RAM, but the witness of $\mathrm{H(I_b)}$ is still unknown to $\mathcal{B}$) with probability ϵ, by the Reset Lemma (Appendix A) and the special soundness property of the underlying HVZK-SS proof system, $\mathcal{B}$ can extract a witness of $\mathrm{H(I_b)}$ with probability at least $(\epsilon - 2^{-\lambda(k)})^2$ through the experiment described in the Reset Lemma (Lemma 3). Note that the 'reset' takes place after the adversary sends Cmt to the simulator in Stage 4 of the id-imp-pa game (Definition 2). In this way, the value of $\mathrm{I_b}$ can be fixed and will remain unchanged at the time of reset. □

In the following, we describe several instantiations of the TWR family and show that they capture many existing IBI schemes. In Section 5.1, we propose a new TWR instantiation and use it to construct a new and efficient id-imp-pa secure IBI scheme.

3.2. *Instantiations of TWR family*

3.2.1. *Trapdoor one-way permutation based*

Let $f : \Delta \to \Delta$ be a trapdoor one-way permutation. The following theorem describes a method to construct a TWR family from any trapdoor one-way permutation family.

Theorem 2. *The binary relation* $\mathbf{R}^{TOP} = \{(x, y) : x, y \in \Delta; f(x) = y\}$ *is a trapdoor weak-one-more relation.*

Proof. It is obvious that $\mathbf{R}^{TOP}$ is efficient to generate, verify, and find witness with trapdoor information. Now we show that it also satisfies the weak-one-more resistance feature (Definition 3). Suppose there exists an adversary $\mathcal{A}$ which breaks the weak-one-more resistance, we build an adversary $\mathcal{B}$ to break the one-wayness of f.

$\mathcal{B}$ is given a random instance $y^* \in \Delta$, and $\mathcal{B}$'s goal is to find the inverse $x^* \in \Delta$ such that $f(x^*) = y^*$. Suppose $\mathcal{A}$ makes at most $Q(k)$ queries to RAM, where $k \in \mathbb{N}$ is a security parameter. Initially, $\mathcal{B}$ randomly selects a number $1 \le i \le Q(k)$, and simulates the weak-one-more resistance game as follows: to answer j-th query to RAM, if $j \neq i$, $\mathcal{B}$ randomly selects $x_j \in \Delta$ and returns $y_j = f(x_j)$ to $\mathcal{A}$; if $j = i$, y^* is returned. When $\mathcal{A}$ makes a query to INV on y_j, if $y_j \neq y^*$, x_j is returned; otherwise, $\mathcal{B}$ aborts. If $\mathcal{A}$ finds a witness $\tilde{x}$ such that $f(\tilde{x}) = y^*$, $\mathcal{B}$ outputs $\tilde{x}$ and halts. If $\mathcal{A}$ halts, $\mathcal{B}$ halts. It is easy to see that if $\mathcal{A}$ wins with probability ϵ, $\mathcal{B}$ breaks the one-wayness of f with probability at least $\epsilon/Q(k)$. □

3.2.2. *Computational Diffie–Hellman (CDH) problem based*

For a security parameter $k \in \mathbb{N}$, let q be a k-bit prime. Let $\mathbb{G}_1$ be an additive cyclic group of order q, and $\mathbb{G}_2$ be a multiplicative cyclic group of the same order. Let P be a generator of $\mathbb{G}_1$. A bilinear map is defined as $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties:

1. *bilinear*: For any $U, V \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}_q$, $e(aU, bV) = e(U, V)^{ab}$;
2. *non-degenerate*: $e(P, P) \neq 1$;
3. *computable*: there exists an efficient algorithm to compute $e(U, V)$ for any $U, V \in \mathbb{G}_1$.

The Computational Diffie–Hellman (CDH) problem in $\mathbb{G}_1$ is to compute abP from $\langle P, aP, bP\rangle$ where a, b are randomly selected from $\mathbb{Z}_q$.

Based on the CDH problem in the setting above, we construct a TWR family $\mathcal{R}^{CDH}$ as follows: on input 1^k, $\mathcal{R}^{CDH}.Gen$ generates $(\mathbb{G}_1, \mathbb{G}_2, q, P, e, \hat{S} = sP)$ where $s \in_R \mathbb{Z}_q$, and sets the TWR relation $\mathbf{R}^{CDH}$ to $\{(x, y) : x, y \in \mathbb{G}_1; e(P, x) = e(\hat{S}, y)\}$ and trapdoor information to s.

Theorem 3. *If the CDH problem in the setting above is hard,* $\mathbf{R}^{CDH}$ *is a trapdoor weak-one-more relation.*

Proof. Suppose there exists an adversary $\mathcal{A}$, who breaks the weak one-more resistance of $\mathbf{R}^{CDH}$, we build another adversary $\mathcal{B}$ to break the CDH problem above.

Similar to the proof of Theorem 2, on input $(1^k, \mathbb{G}_1, \mathbb{G}_2, q, P, e, aP, bP)$, $\mathcal{B}$ sets $\hat{S} = aP$ and randomly selects a number i, such that $1 \le i \le Q(k)$, where $Q(k)$ is the maximum number of queries to RAM made by $\mathcal{A}$. $\mathcal{B}$ then answers $\mathcal{A}$'s queries as follows.

When $\mathcal{A}$ asks the j-th challenge query (i.e. RAM), if $j \neq i$, $\mathcal{B}$ randomly selects a $t_j \in \mathbb{Z}_q$, and returns $T_j = t_jP$ to $\mathcal{A}$; if $j = i$, bP is returned. When $\mathcal{A}$ asks the inversion query (i.e. INV) on T_j, if $j \neq i$, $t_j(aP)$ is returned; if $j = i$, $\mathcal{B}$ aborts. At the end of the simulation, if $\mathcal{A}$ outputs x such that $e(P, x) = e(\hat{S}, bP)$, $\mathcal{B}$ outputs x and halts. If $\mathcal{A}$ halts, $\mathcal{B}$ halts.

In the simulation above, we can see that if $\mathcal{A}$ wins the weak one-more resistance game with probability ϵ, then $\mathcal{B}$ breaks the CDH problem with probability at least $\epsilon/Q(k)$. □

3.2.3. Digital signature based

Let $\mathcal{SIG} = (\mathcal{KG}, \mathcal{S}, \mathcal{V})$ be a signature scheme defined on some message space $\mathcal{MS}$. In [19], Kuorsawa and Heng showed how to construct an id-imp-pa secure IBI scheme from a signature scheme, which is existentially unforgeable against *chosen* message attack (euf-cma) [14]. In the following, we show that under our framework, the signature scheme only needs to be existentially unforgeable against *known* message attack (euf-kma) [14]. A signature scheme $\mathcal{SIG}$ is euf-kma, if for any sufficiently large security parameter $k \in \mathbb{N}$ and any PPT adversary, it is of negligible probability for the adversary to forge a signature for any of the messages in $\mathcal{MS} \setminus \mathcal{M}_{known}$ after getting access to signatures for a set of messages denoted by $\mathcal{M}_{known}$. The messages in $\mathcal{M}_{known}$ are chosen uniformly from $\mathcal{MS}$, rather than by the adversary.

A digital signature based TWR family $\mathcal{R}^{SIG}$ can be constructed as follows. On input 1^k, $\mathcal{R}^{SIG}.Gen$ runs $\mathcal{KG}(1^k)$ to generate a public/private key pair (pk, sk), and sets the TWR relation $\mathbf{R}^{SIG}$ to $\{(x, y) : y \in \mathcal{MS}; \mathcal{V}(pk, y, x) = 1\}$ and the trapdoor information to sk. In other words, y is a message and x is the corresponding signature.

Theorem 4. *If $\mathcal{SIG}$ is euf-kma, $\mathbf{R}^{SIG}$ proposed above is a trapdoor weak-one-more relation.*

Proof. Suppose there exists an adversary $\mathcal{A}$ who breaks the weak-one-more resistance. We build another adversary $\mathcal{F}$ which existentially forge $\mathcal{SIG}$ under known message attacks.

Suppose $\mathcal{A}$ makes at most $Q(k)$ queries to RAM, for security parameter $k \in \mathbb{N}$. First, in the game of euf-kma, $\mathcal{F}$ obtains $Q(k) - 1$ message-signature pairs $\{(m_1, \sigma_1), \ldots, (m_{Q(k)-1}, \sigma_{Q(k)-1})\}$ where m_j $(1 \le j \le Q(k) - 1)$ are uniformly distributed over $\mathcal{MS}$ and σ_j is a valid signature, that is, $\mathcal{V}(pk, \sigma_j, m_j) = 1$. In other words, $\mathcal{M}_{known} = \{m_1, \ldots, m_{Q(k)-1}\}$. $\mathcal{F}$ then chooses uniformly at random a message $m^* \in_R \mathcal{MS}$ and inserts into the message sequence $(m_1, \ldots, m_{Q(k)-1})$ at a position which is randomly chosen. Without loss of generality, we assume that any two messages in $\mathcal{M}_{known} \cup \{m^*\}$ are different. The proof then proceeds as in the proof of Theorem 2. For i-th challenge query (i.e. RAM) or inversion query (i.e. INV), $\mathcal{F}$ returns the i-th message or signature, respectively. $\mathcal{F}$ aborts if $\mathcal{A}$ makes a query to INV with message m^*. At the end of the simulation, if $\mathcal{A}$ outputs σ^* such that $\mathcal{V}(pk, \sigma^*, m^*) = 1$, $\mathcal{F}$ outputs σ^* and halts. If $\mathcal{A}$ halts, $\mathcal{F}$ halts.

If $\mathcal{A}$ wins the weak-one-more resistance game with probability ϵ, $\mathcal{F}$ breaks the euf-kma security of $\mathcal{SIG}$ with probability at least $\epsilon/Q(k)$. □

In Appendix B.1, we review some existing id-imp-pa secure IBI schemes and show that they can be captured by the "TWR + HVZK-SS" framework. In Section 5.1, we propose a new instantiation for the TWR family. This new instantiation is based on the K-sCAA1 problem [20,11]. Under the framework above, we then show that a new and efficient IBI scheme with id-imp-pa security can be built. Before that, in the next section, we modify the security requirements of the two building blocks, namely a hard relation and an interactive proof system, in such a way that our framework can be used to build id-imp-aa as well as id-imp-ca secure IBI schemes.

4. To achieve security against active and concurrent attacks

To construct an IBI scheme to be secure against active and concurrent attacks (namely, id-imp-aa and id-imp-ca), we only need to modify the security requirements of the hard relation, namely the trapdoor weak-one-more relation, and the interactive proof system, namely the HVZK-SS, in our framework described in Section 3. The new security requirements are *Trapdoor Strong-one-more Relation (TSR)* and *Witness Dualism proof with Special Soundness (WD-SS)*, respectively. Below are the definitions of them.

Definition 5 (*TSR Family*). A family of trapdoor strong-one-more relations $\mathcal{R}'$ is a triple of PPT algorithms (Gen', Ver', Inv'):

1. $\mathcal{R}'.Gen'$: On input 1^k, where $k \in \mathbb{N}$ is a security parameter, it outputs $(\langle \mathbf{R} \rangle, t)$ where $\langle \mathbf{R} \rangle$ denotes the description of relation $\mathbf{R}$ on $W \times \Delta$ and t a trapdoor information.
2. $\mathcal{R}'.Ver'$: For any $k \in \mathbb{N}$ and $(\langle \mathbf{R} \rangle, t) \leftarrow \mathcal{R}'.Gen'(1^k)$, $\mathcal{R}'.Ver'(\langle \mathbf{R} \rangle, x, y) = 1$ if and only if $(x, y) \in \mathbf{R}$.
3. $\mathcal{R}'.Inv'$: On input $(\langle \mathbf{R} \rangle, y, t)$, it outputs a random witness $x \overset{R}{\leftarrow} W(y)$.
4. **Strong-one-more resistance**: Consider the following game against an adversary $\mathcal{A}$ which is given $\langle \mathbf{R} \rangle$ but not t, and has access to two oracles:
   (a) A challenge oracle RAM that on any input returns a random point $y \in \Delta$.
   (b) An inversion oracle INV that on any input y,
      i. if y is an output of RAM, a witness chosen uniformly at random from $W(y)$ is returned, and the same witness is returned if the same value of y is queried again;
      ii. if y is not an output of RAM, $\perp$ is returned indicating that the input is invalid.

   $\mathcal{A}$ wins if $\mathcal{A}$ finds a pair $(x', y') \in \mathbf{R}$ such that y' is an output of RAM but (x', y') does not appear in the input/output pairs of INV (i.e. $\mathcal{A}$ is able to generate a distinct pair in $\mathbf{R}$ other than the pairs obtained from INV [1]). $\mathbf{R}$ is a Trapdoor Strong-one-more Relation (TSR) if the probability of winning the game is negligible in k for any PPT $\mathcal{A}$.

[1] Note that there are two possibilities. Case 1: y' has never been queried to INV; Case 2: INV has returned a witness x of y' before, but $x' \neq x$.

The TSR family $\mathcal{R}'$ can also be instantiated in many different ways. In Section 4.2, we describe several of them. In Section 5.2, we propose a new instantiation and construct a new IBI scheme based on it.

Next, we define a new notion for interactive proof systems. The new notion is called Witness Dualism proof with Special Soundness (WD-SS). We will see shortly that Witness Dualism is a weaker form of Witness Indistinguishability [12].

Definition 6 (*WD-SS*). A Witness Dualism proof system with Special Soundness (WD-SS) for a binary relation $\mathbf{R}$ on $W \times \Delta$ is a non-trivial canonical interactive proof system (P, V) such that for any $y \in \Delta$,

1. **Completeness**. If P knows x such that $(x, y) \in \mathbf{R}$, then $\Pr[\mathsf{V}$ outputs accept$] = 1$.
2. **Special Soundness**. There exists a polynomial time algorithm which on input two acceptable transcripts $(\mathsf{Cmt}, \mathsf{Ch}_1, \mathsf{Rsp}_1)$ and $(\mathsf{Cmt}, \mathsf{Ch}_2, \mathsf{Rsp}_2)$ for $\mathsf{Ch}_1 \neq \mathsf{Ch}_2$, the algorithm outputs x such that $(x, y) \in \mathbf{R}$.
3. **Witness Dualism**. For any $x \in W(y)$, there exists at least one dual witness $x' \in W(y)$ such that
   (a) $x' \neq x$, and
   (b) for any verifier V with any auxiliary input *aux* for V, the ensembles, $\mathsf{V}_{\mathsf{P}(y,x)}(y, aux)$ and $\mathsf{V}_{\mathsf{P}(y,x')}(y, aux)$, which represent V's views of the interactive proof, are indistinguishable.

Discussion. The notion of Witness Dualism is related to Witness Indistinguishability, introduced by Feige and Shamir [12]. For witness dualism, given a witness x of y, we only require it to be indistinguishable from a different witness x', rather than from *all other* witnesses in $W(y)$, the latter is required for Witness Indistinguishability. Hence, for any proof system which is witness indistinguishable, the system also has witness dualism, but may not be vice versa. In Section 5.2, we propose a concrete WD-SS which is not Witness Indistinguishable and show that Witness Dualism is a weaker form of witness indistinguishability. On the other side, witness dualism still preserves some important properties of witness indistinguishability, such as the concurrent composition property described below.

Definition 7. A polynomial composition of protocols has Witness Dualism (WD), if for all sufficiently large k, for any set of polynomial-time provers $\mathcal{P} = (P_1, P_2, \ldots, P_n)$ which follow their protocols faithfully, and any two sets of respective witnesses $\mathcal{W}^1 = (w_1^1, w_2^1, \ldots, w_n^1)$ and $\mathcal{W}^2 = (w_1^2, w_2^2, \ldots, w_n^2)$ of the set $\mathcal{Y} = (y_1, y_2, \ldots, y_n)$, where $w_i^2 = w_i^1$ or w_i^2 is a dual witness of w_i^1, it is indistinguishable to the coalition of all the other provers and verifiers whether $\mathcal{P}$ are using $\mathcal{W}^1$ or $\mathcal{W}^2$. Here n is any polynomial of k.

Theorem 5. *Witness dualism is preserved under polynomial composition of protocols.*

Proof. Consider polynomially many protocols carried out concurrently (sequentially, in parallel, or with interleaved steps). Assume by contradiction for infinitely many k, $\mathcal{P}(k)$ are subsets of provers who carry out their WD protocols faithfully and for them WD is not preserved. That is, there exists a set of verifiers $\mathcal{V}(k)$, auxiliary inputs $aux(k)$ to $\mathcal{V}(k)$, and sets of witnesses $\mathcal{W}^1(k)$ and $\mathcal{W}^2(k)$ (defined as above), such that the two ensembles $\mathcal{V}_{\mathcal{P}(\mathcal{Y}(k),\mathcal{W}^1(k))}(\mathcal{Y}(k), aux(k))$ and $\mathcal{V}_{\mathcal{P}(\mathcal{Y}(k),\mathcal{W}^2(k))}(\mathcal{Y}(k), aux(k))$ are polynomially distinguishable. By the hybrid argument [15,13], there exists i, such that if all $P \in \mathcal{P}(k)$ with index less than i use witnesses from $\mathcal{W}^1(k)$, and all $P \in \mathcal{P}(k)$ with index greater than i use witnesses from $\mathcal{W}^2$, the ensembles which differ only in the witness P_i is using are distinguishable by $\mathcal{V}(k)$. Denote the hybrid witnesses $\mathcal{W}'^1(k) = (w_1^1, \ldots, w_{i-1}^1, w_i^1, w_{i+1}^2, \ldots, w_n^2)$ and $\mathcal{W}'^2(k) = (w_1^1, \ldots, w_{i-1}^1, w_i^2, w_{i+1}^2, \ldots, w_n^2)$. Now we construct a V', which has $(aux(k), \mathcal{W}'^1(k), \mathcal{W}'^2(k))$ as part of its auxiliary input, distinguishes between faithful P_i using w_i^1 or w_i^2.

V' simulates the game against $\mathcal{V}(k)$ as follows. For each $j \neq i$, V' simulates P_j by using the j-th item in $\mathcal{W}'^1(k)$ as the witness to P_j. For the messages between P_i and $\mathcal{V}(k)$, it is relayed faithfully between P_i and $\mathcal{V}(k)$. Finally, if $\mathcal{V}(k)$ can distinguish $\mathcal{W}'^1(k) = (w_1^1, \ldots, w_{i-1}^1, w_i^1, w_{i+1}^2, \ldots, w_n^2)$ from $\mathcal{W}'^2(k) = (w_1^1, \ldots, w_{i-1}^1, w_i^2, w_{i+1}^2, \ldots, w_n^2)$, V' can distinguish between faithful P_i using w_i^1 or w_i^2. It contradicts the assumption that the original protocol has witness dualism. □

The theorem above is useful for showing the security of the framework below.

4.1. A framework to construct id-imp-aa and id-imp-ca secure IBI schemes

Starting from the framework for constructing generic IBI schemes with id-imp-pa security (Section 3.1), we transform it to a framework for constructing IBI schemes secure against active and concurrent attacks (i.e. id-imp-aa and id-imp-ca). The transformation is to replace the TWR with a trapdoor strong-one-more relation (TSR) (Definition 5), and the HVZK-SS with a Witness Dualism proof system with Special Soundness (WD-SS) (Definition 6).

The following theorem states that the resulting generic IBI scheme due to the transformation achieves both id-imp-aa and id-imp-ca security.

Theorem 6. *By replacing the TWR in the original generic construction of IBI schemes described in Section 3.1 with a TSR, and the HVZK-SS proof system with a WD-SS proof system, the resulting generic IBI construction is id-imp-aa and id-imp-ca secure in the random oracle model, provided that the challenge length $\lambda(k)$ of the WD-SS proof system is super logarithmic in k, where $k \in \mathbb{N}$ is a security parameter.*

Proof. Suppose there exists an adversary $\mathcal{A}$ who breaks an IBI scheme constructed as above with advantage ϵ, we construct a PPT algorithm $\mathcal{B}$ to break the strong-one-more resistance of the underlying TSR with advantage $\epsilon' \geq 1/2(\epsilon - 2^{-\lambda(k)})^2$.

$\mathcal{B}$ simulates the id-imp-aa (resp. id-imp-ca) game by setting $mpk = \langle \mathbf{R} \rangle$ and maintains two sets HU and CU, which are initialized to empty. $\mathcal{B}$ also maintains a table T, each entry of T contains an identity I, and the value of $\mathrm{H}(I)$ and a witness of $\mathrm{H}(I)$. T is also initialized to empty at the beginning of the simulation. $\mathcal{B}$ answers $\mathcal{A}$'s queries as follows:

1. H-query: On input $I \in \{0, 1\}^*$, if $I \notin \mathrm{T}$, $\mathcal{B}$ queries RAM to get a random point $y \in \Delta$, then sets $\mathrm{H}(I) = y$ by putting $(I, y, \perp)$ into table T, and returns y. The symbol "$\perp$" denotes that the corresponding value is unknown yet. If $I \in \mathrm{T}$, the existing value of $\mathrm{H}(I)$ is returned.
2. INIT(I): If $I \in \mathrm{HU} \cup \mathrm{CU}$, $\perp$ is returned. Otherwise, $\mathcal{B}$ checks if I is in table T. If $I \in \mathrm{T}$, I is added into HU and a symbol '1' is returned. Otherwise, $\mathcal{B}$ queries RAM to get a random point $y \in \Delta$, and sets $\mathrm{H}(I) = y$ by putting $(I, y, \perp)$ into table T, I is then added into HU and a symbol '1' is returned.
3. CORR(I): If $I \notin \mathrm{HU}$, $\perp$ is returned. Otherwise, $\mathcal{B}$ looks for the entry corresponding to I in table T. If the witness (i.e the third component of the entry) is $\perp$, $\mathcal{B}$ queries INV for a witness x of $\mathrm{H}(I)$, and replaces the $\perp$ symbol in that entry of table T by x. $\mathcal{B}$ returns x to $\mathcal{A}$. I is then removed from HU and added into CU.
4. PROV(I): If $I \notin \mathrm{HU}$, $\perp$ is returned. Otherwise, $\mathcal{B}$ looks for the entry corresponding to I in table T and retrieves the witness x of $\mathrm{H}(I)$. If the witness is unknown (i.e. the third component of the entry is $\perp$), $\mathcal{B}$ queries INV for a witness x of $\mathrm{H}(I)$, and replaces the $\perp$ symbol in that entry by x. $\mathcal{B}$ then runs a copy of $\mathbf{P}$ with initial state x.

If $\mathcal{A}$ successfully impersonates a user $\mathrm{I_b}$, that is created but not corrupted (i.e. $\mathrm{H}(\mathrm{I_b})$ is returned by RAM, but $\mathcal{A}$ has not queried for its witness), with probability ϵ, based on the Reset Lemma (Appendix A) and the special soundness of the WD-SS proof system, $\mathcal{B}$ can extract a witness x_b of $\mathrm{H}(\mathrm{I_b})$, with probability at least $(\epsilon - 2^{-\lambda(k)})^2$, through the reset experiment described in Lemma 3.

If $\mathcal{B}$ has never queried INV, for a witness of $\mathrm{H}(\mathrm{I_b})$, that is, the witness is not in table T yet, $\mathcal{B}$ successfully breaks the strong-one-more resistance. Now if $\mathcal{B}$ has queried INV for a witness of $\mathrm{H}(\mathrm{I_b})$, then the witness must be in the corresponding entry (indexed by $\mathrm{I_b}$) in table T. Due to Witness Dualism, with probability at least 1/2, the witness x_b extracted by $\mathcal{B}$ (with the help of $\mathcal{A}$) is different from the one in table T. By Theorem 5, it follows that witness dualism is preserved under concurrent composition. Hence, $\mathcal{B}$ can break the strong-one-more resistance of the underlying TSR with probability at least $1/2(\epsilon - 2^{-\lambda(k)})^2$. □

4.2. *Instantiations of TSR family*

4.2.1. *Factoring based*

A Blum-Williams generator [24,5] is a modulus generator that returns Blum-Williams (BW) moduli N, meaning that $N = pq$ with $p \equiv q \equiv 3 \pmod 4$. Let $QR_N = \{x^2 \bmod N | x \in \mathbb{Z}_N^*\}$ be the set of all quadratic residues modulo N. It is known that if N is a BW modulus, then squaring is a permutation on QR_N. Let $\mathbb{Z}_N^*[+1] = \{x \in \mathbb{Z}_N^* | Jac_N(x) = +1\}$ where $Jac_N(x)$ is the Jacobi Symbol of x with respect to N. It is known that if N is a BW modulus, -1 is a non-square modulo N with Jacobi Symbol $+1$, and for every element $x \in \mathbb{Z}_N^*[+1]$, either x or $-x$ is a square modulo N.

A TSR family $\mathcal{R}'^{SQ}$ can be constructed as follows. On input 1^k, $\mathcal{R}'^{SQ}.Gen'$ runs the Blum-Williams generator to generate (N, p, q), and sets relation

$$\mathbf{R}^{SQ} = \left\{(x, y) \in \mathbb{Z}_N^* \times \mathbb{Z}_N^*[+1] : x > (N-1)/2;\ y \equiv \pm x^2 \pmod N\right\}$$

and trapdoor information to (p, q). On input $(\langle \mathbf{R}^{SQ} \rangle, x, y)$, $\mathcal{R}'^{SQ}.Ver'$ outputs 1 if and only if $x^2 \equiv \pm y \pmod N$. For $\mathcal{R}'^{SQ}.Inv'$, given $(\langle \mathbf{R}^{SQ} \rangle, y, (p, q))$ where $y \in \mathbb{Z}_N^*[+1]$, it chooses uniformly at random an $x \in \mathbb{Z}_N^*$ over the two square roots of $\pm y$ that are greater than $(N-1)/2$ (remark: either y or $-y$ is a square).

Theorem 7. *If the factoring problem is hard,* $\mathbf{R}^{SQ}$ *described above is a trapdoor strong-one-more relation.*

Proof. Suppose there exists a PPT adversary $\mathcal{A}$ which breaks the strong-one-more resistance of $\mathbf{R}^{SQ}$, with probability ϵ. We build another PPT adversary $\mathcal{B}$ to factorize N with probability at least $\epsilon/2$.

$\mathcal{B}$ simulates the game of strong-one-more resistance as follows. When $\mathcal{A}$ queries the challenge oracle (i.e. RAM), $\mathcal{B}$ selects uniformly at random an $x \in \mathbb{Z}_N^*$, such that $x > (N-1)/2$, and returns $y \overset{R}{\leftarrow} \pm x^2 \pmod N$ to $\mathcal{A}$. When $\mathcal{A}$ queries the inversion oracle (i.e. INV) on y, $\mathcal{B}$ returns x to $\mathcal{A}$.

If $\mathcal{A}$ wins the game, that is, $\mathcal{A}$ outputs a pair $(x', y') \in \mathbf{R}^{SQ}$ such that y' is an output of RAM but (x', y') does not appear in the input/output pairs of the INV oracle, then, according to the simulation of RAM, $\mathcal{B}$ has randomly chosen a witness x when generating y'. One of the following two events must occur:

$\mathbf{E}_1$: $\mathcal{A}$ has not queried INV with y'. If $x' \neq \pm x$, $\mathcal{B}$ is able to factorize N. Otherwise, $\mathcal{B}$ aborts. Since x is uniformly selected at random, $\Pr[x' \neq \pm x] = 1/2$.

$\mathbf{E}_1$: $\mathcal{A}$ has queried INV with y'. This implies that (x, y') appears in the input/output pairs of the INV oracle. For $\mathcal{A}$ wins in this event, we must have $x' \neq \pm x$. Hence $\mathcal{B}$ is always able to factorize N in this event.

Therefore, if $\mathcal{A}$ breaks the strong-one-more resistance with probability ϵ, $\mathcal{B}$ can factorize N with probability at least $\epsilon/2$. □

4.2.2. RSA based

On input 1^k, an RSA key generator (**KG**) outputs a modulus N that is the product of two distinct odd primes p, q such that $|p| = |q| = k/2$, and exponents e, d such that $ed \equiv 1 (\text{mod } \varphi(N))$ where $\varphi(N) = (p-1)(q-1)$ is the Euler's totient function. A prime-exponent RSA key generator only outputs parameters with prime e. The RSA problem is hard if

$$\mathbf{Adv}^{rsa}_{\mathcal{A}}(k) = \Pr\left[\begin{array}{c} (N, e, d) \leftarrow \mathbf{KG}(1^k); \\ y \overset{R}{\leftarrow} Z^*_N;\ x \leftarrow \mathcal{A}(1^k, N, e, y) : \\ x^e \equiv y \ (\text{mod } N) \end{array}\right]$$

is negligible in k for any PPT algorithm $\mathcal{A}$. We construct a TSR family $\mathcal{R}'^{RSA}$ as follows.

On input 1^k, $\mathcal{R}'^{RSA}.Gen'$ runs the prime-exponent RSA key generator to generate (N, e, d) such that prime $e > 2^{\lambda(k)}$ where $\lambda(k)$ is super-logarithmic in k. It then randomly picks $g \overset{R}{\leftarrow} \mathbb{Z}^*_N$ and sets the TSR $\mathbf{R}^{RSA} = \{((x_1, x_2), y) \in (\mathbb{Z}_e \times \mathbb{Z}^*_N) \times \mathbb{Z}^*_N : g^{-x_1}x_2^{-e} \equiv y \ (\text{mod } N)\}$, the trapdoor information is set to (N, d). For $\mathcal{R}'^{RSA}.Inv'$, on input $(\langle \mathbf{R}^{RSA}\rangle, y, (N, d))$, where $y \in \mathbb{Z}^*_N$, it outputs (x_1, x_2) where $x_1 \overset{R}{\leftarrow} \mathbb{Z}_e$ and $x_2 = (g^{x_1}y)^{-d}$ (mod N).

Theorem 8. *If the RSA problem is hard, $\mathbf{R}^{RSA}$ is a trapdoor strong-one-more relation.*

Proof. Suppose there exists a PPT adversary $\mathcal{A}$ which breaks the strong-one-more resistance with probability ϵ. We construct another PPT adversary $\mathcal{B}$ which solves the RSA problem with probability at least $(1 - 1/e)\epsilon$. Below is the description of $\mathcal{B}$ which simulates the game of strong-one-more resistance for $\mathcal{A}$.

Given the RSA challenge $\hat{y}$, the adversary $\mathcal{B}$ sets $g = \hat{y}$ and simulates the game as follows. When $\mathcal{A}$ queries RAM, $\mathcal{B}$ randomly selects $x_1 \overset{R}{\leftarrow} \mathbb{Z}_e, x_2 \overset{R}{\leftarrow} \mathbb{Z}^*_N$, and returns $y = g^{-x_1}x_2^{-e}$ (mod N) to $\mathcal{A}$. When $\mathcal{A}$ queries INV on y, $\mathcal{B}$ returns (x_1, x_2) to $\mathcal{A}$ if y has been queried to RAM. Otherwise, $\mathcal{B}$ returns $\perp$.

If $\mathcal{A}$ wins the game, $\mathcal{A}$ has output a pair $((x'_1, x'_2), y') \in \mathbf{R}^{RSA}$. Suppose the witness of y' generated by $\mathcal{B}$ for simulating the corresponding RAM query of y' is (x''_1, x''_2). Similar to the proof of Theorem 7, there are two events, and one of them must occur.

$\mathbf{E}_1$: $\mathcal{A}$ has not queried INV with y'. Note that if $x''_1 = x'_1$, so is between x''_2 and x'_2. Since x''_1 is randomly chosen from $\mathbb{Z}_e$, $\Pr[x'_1 \neq x''_1] = 1 - 1/e$.

$\mathbf{E}_1$: $\mathcal{A}$ has queried INV with y'. This implies that $((x''_1, x''_2), y')$ appears in the input/output pairs of the INV oracle. For $\mathcal{A}$ wins in this event, we must have $x'_1 \neq x''_1$.

When $\mathcal{B}$ obtains two distinct witnesses (x'_1, x'_2) and (x''_1, x''_2) for the same challenge y', since e is prime and $0 < |x'_1 - x''_1| < e$, by the extended Euclidian algorithm, two integers a, b can be found such that $a(x''_1 - x'_1) + be = 1$. Therefore, $\mathcal{B}$ can solve the RSA problem instance $\hat{y}$ by computing $g^b(x'_2x''^{-1}_2)^a$ mod N.

By analyzing the combined probability of the two events $\mathbf{E}_1$ and $\mathbf{E}_2$ for the case that $x'_1 \neq x''_1$, we can see that $\mathcal{B}$ can break the RSA problem with probability at least $(1 - 1/e)\epsilon$. □

4.2.3. Strongly unforgeable digital signature based

Let $\mathcal{SIG} = (\mathcal{KG}, \mathcal{S}, \mathcal{V})$ be defined as in Section 3.2.3, but we now require that $\mathcal{SIG}$ is strongly unforgeable [1] against *known* message attacks [14] (seuf-kma). A signature scheme is said to be seuf-kma if for any PPT adversary, the probability of producing a message-signature pair (m, σ), such that this pair is not in the list of message-signature pairs the adversary has already known, is negligible.

By using the same construction as in Section 3.2.3 but requiring the underlying $\mathcal{SIG}$ to be seuf-kma, the relation $\mathbf{R}^{SIG}$ will become a TSR. We have the following theorem.

Theorem 9. *If $\mathcal{SIG}$ is seuf-kma, and for any message $m \in \mathcal{MS}$, there is more than one valid signature, $\mathbf{R}^{SIG}$ is a trapdoor strong-one-more relation.*

Proof. Suppose there exists a PPT adversary $\mathcal{A}$ which breaks the strong-one-more resistance of $\mathbf{R}^{SIG}$, we build a PPT forger $\mathcal{F}$ which breaks seuf-kma of the underling $\mathcal{SIG}$.

Suppose $\mathcal{A}$ makes at most $Q(k)$ challenge queries where $k \in \mathbb{N}$ is the security parameter. $\mathcal{F}$ first gets $Q(k)$ message-signature pairs from its own simulator. Note that the messages are not chosen by $\mathcal{F}$, but rather by its simulator. Then $\mathcal{F}$ answers $\mathcal{A}$'s challenge/inversion queries by simply sending back the corresponding message/signature. We can see that a break of the strong-one-more resistance of $\mathbf{R}^{SIG}$ by $\mathcal{A}$ with advantage ϵ directly implies an successful forgery by $\mathcal{B}$ with probability at least $\epsilon/2$. □

In Appendix B.2, we show that Okamoto–RSA–IBI scheme falls into our framework. That is, it can be decomposed into two parts: the RSA-based TSR, and a corresponding WD-SS. In Section 5.2, we propose a new id-imp-aa and id-imp-ca secure IBI scheme which is a combination of the signature based TSR and a new WD-SS. This new WD-SS also illustrates that Witness Dualism is a weaker form of Witness Indistinguishability.

5. Applying the framework – Two new IBI schemes

5.1. An IBI scheme with id-imp-pa security

By applying the "TWR + HVZK-SS" framework, in Appendix B.1, we showed the id-imp-pa security of many existing IBI schemes, such as GQ-IBI [16] and Sh-IBI [22] under the trapdoor one-way permutation assumption of RSA, and Hs-IBI [17] and ChCh-IBI [10] under the CDH problem assumption.[2] In this section, we propose a new and efficient IBI scheme with id-imp-pa security. By following the framework described in Section 3.1, we first propose a new TWR. We then propose an HVZK-SS proof system for this new TWR. This new TWR is based on the following K-sCAA1 problem [20,11].

Definition 8 (*K-sCAA1 Problem*). Let $\mathbb{G}_1, \mathbb{G}_2, q, P, e$ be the same parameters as in the CDH problem (Section 3.2.2). For any $s \overset{R}{\leftarrow} \mathbb{Z}_q$, set $Q = sP$ and choose uniformly at random $h_i \overset{R}{\leftarrow} \mathbb{Z}_q$ for $i = 0, 1, \ldots, \mathrm{K}$, where K is some polynomial in a security parameter. Given $(P, Q, h_1, \ldots, h_{\mathrm{K}}, \frac{1}{h_1+s}P, \ldots, \frac{1}{h_{\mathrm{K}}+s}P)$, compute $(h, \frac{1}{h+s}P)$ such that $h \notin \{h_1, h_2, \ldots, h_{\mathrm{K}}\}$.

The K-sCAA1 assumption [20,11] means that there is no PPT algorithm that can solve the K-sCAA1 problem with non-negligible probability. Based on the K-sCAA1 assumption, we construct a TWR family $\mathcal{R}^{K\text{–}sCAA1}$ as follows.

A K-sCAA1 Based TWR.

1. On input 1^k, $\mathcal{R}^{K\text{–}sCAA1}.Gen$ outputs $(\mathbb{G}_1, \mathbb{G}_2, q, P, e, Q = sP, s)$ where s is randomly selected from $\mathbb{Z}_q$. The relation is defined as $\mathbf{R}^{K\text{–}sCAA1} = \{(x, y) : x \in \mathbb{G}_1;\ y \in \mathbb{Z}_q;\ e(yP + Q, x) = e(P, P)\}$ and the trapdoor information as s.
2. On input $(\langle \mathbf{R}^{K\text{–}sCAA1} \rangle, x, y)$, $\mathcal{R}^{K\text{–}sCAA1}.Ver$ outputs 1 if and only if $e(yP + Q, x) = e(P, P)$.
3. On input $(\langle \mathbf{R}^{K\text{–}sCAA1} \rangle, y, s)$, $\mathcal{R}^{K\text{–}sCAA1}.Inv$ outputs x as $\frac{1}{y+s}P$.

Theorem 10. *If there exists a PPT algorithm which asks at most* $\mathrm{K} + 1$ *RAM queries, and wins the weak-one-more resistance game for the TWR* $\mathbf{R}^{K\text{–}sCAA1}$ *with probability* ϵ, *there exists another PPT algorithm that solves the K-sCAA1 problem with probability at least* $\epsilon/(\mathrm{K} + 1)$.

Proof. Suppose there exists an adversary $\mathcal{A}$ which breaks the weak-one-more resistance. We build another adversary $\mathcal{B}$ which breaks K-sCAA1.

$\mathcal{B}$ is given $(h_1, \ldots, h_{\mathrm{K}}, \frac{1}{h_1+s}P, \ldots, \frac{1}{h_{\mathrm{K}}+s}P)$ where $h_i \overset{R}{\leftarrow} \mathbb{Z}_q$ for $i = 1, \ldots, \mathrm{K}$. $\mathcal{B}$ randomly picks $h \overset{R}{\leftarrow} \mathbb{Z}_q$ and performs a random permutation on $h, h_1, \ldots, h_{\mathrm{K}}$ and gets $h'_1, \ldots, h'_{\mathrm{K}+1}$. Suppose $h'_i = h$.

Now for the m-th RAM query, $\mathcal{B}$ returns h'_m to $\mathcal{A}$. For the n-th INV query, if $\mathcal{A}$ queries the witness of h'_i, $\mathcal{B}$ fails and aborts. Otherwise, $\mathcal{B}$ returns the corresponding witness to $\mathcal{A}$. If $\mathcal{A}$ outputs x such that $e(hP + Q, x) = e(P, P)$, $\mathcal{B}$ outputs x and halts. If $\mathcal{A}$ halts, $\mathcal{B}$ halts.

If $\mathcal{A}$ wins the weak-one-more resistance game with probability ϵ, $\mathcal{B}$ breaks K-sCAA1 with probability at least $\epsilon/(\mathrm{K} + 1)$. □

Remark. From the K-sCAA1 assumption [20,11], we can see that the relation $\mathbf{R}^{K\text{–}sCAA1} = \{(x, y) : x \in \mathbb{G}_1;\ y \in \mathbb{Z}_q;\ e(yP + Q, x) = e(P, P)\}$ is non-samplable [2]. Hence, it is not a Trapdoor Samplable Relation [2] and cannot be captured by the framework of [2].

5.1.1. A HVZK-SS Proof System for $\mathbf{R}^{K\text{–}sCAA1}$

We now propose an HVZK-SS proof system for the K-sCAA1 problem based TWR $\mathbf{R}^{K\text{–}sCAA1}$. The HVZK-SS is a non-trivial canonical proof system (P, V) where P knows x such that $(x, y) \in \mathbf{R}^{K\text{–}sCAA1}$ and V has access to public information only, which includes $\langle \mathbf{R}^{K\text{–}sCAA1} \rangle$ and y. The three moves Cmt, Ch and Rsp of the proof system are as follows.

1. $\mathsf{Cmt} := r(yP + Q)$ where $r \overset{R}{\leftarrow} \mathbb{Z}_q$
2. $\mathsf{Ch} := c$ where $c \overset{R}{\leftarrow} \mathbb{Z}_q$
3. $\mathsf{Rsp} := rcP + x$

After receiving Rsp, V accepts if and only if

$$e(\mathsf{Rsp}, yP + Q) = e(P, P)e(P, \mathsf{Cmt})^c.$$

Theorem 11. *The interactive proof system* (P, V) *for the TWR* $\mathbf{R}^{K\text{–}sCAA1}$ *described above is an HVZK-SS proof system (Definition 4).*

Proof. It is obvious that (P, V) is a non-trivial canonical proof system, satisfying the Completeness requirement.

For Special Soundness, we can see that given $(\mathsf{Cmt}, c_1, \mathsf{Rsp}_1)$ and $(\mathsf{Cmt}, c_2, \mathsf{Rsp}_2)$ with $c_1 \neq c_2$, the witness x can be extracted as $(c_2 - c_1)^{-1}(c_2\mathsf{Rsp}_1 - c_1\mathsf{Rsp}_2)$.

The proof system is also Honest Verifier Zero Knowledge, as we can construct a polynomial time algorithm $\mathcal{SIM}$ which on input $(\langle \mathbf{R}^{K\text{–}sCAA1} \rangle,\ y)$, generates a conversation between P and V whose distribution is computationally indistinguishable from that of a real conversation. The construction is as follows. Randomly choose $c, z \overset{R}{\leftarrow} \mathbb{Z}_q$ and set $\mathsf{Ch} = c$, $\mathsf{Rsp} = zP$, $\mathsf{Cmt} = c^{-1}(z(yP + Q) - P)$. □

[2] The abbreviations of these IBI schemes were first used by Bellare, Namprempre and Neven in [2].

MKGen:

Generate $(\mathbb{G}_1, \mathbb{G}_2, q, P, e)$ as in the CDH problem (Sec. 3.2.2).

Choose $s \overset{R}{\leftarrow} \mathbb{Z}_q$, and compute $Q = sP$.

Let $\mathrm{H} : \{0, 1\}^* \rightarrow \mathbb{Z}_q$ be a hash function.

The master public key *mpk* is set to $(\mathbb{G}_1, \mathbb{G}_2, q, P, e, Q, \mathrm{H})$ and

the master secret key *msk* to s.

UKGen:

Given an identity $I \in \{0, 1\}^*$, set user secret key $usk[I]$ to $\frac{1}{\mathrm{H}(I)+s}P$.

User Identification Protocol:

Prover P $(usk[I] = \frac{1}{\mathrm{H}(I)+s}P)$ **Verifier V** (mpk, I)

$r \overset{R}{\leftarrow} \mathbb{Z}_q$

$\mathsf{Cmt} \leftarrow r(\mathrm{H}(I)P + Q)$

$\xrightarrow{\quad\mathsf{Cmt}\quad}$

$c \overset{R}{\leftarrow} \mathbb{Z}_q$

$\xleftarrow{\quad c\quad}$

$\mathsf{Rsp} \leftarrow rcP + usk[I]$

$\xrightarrow{\quad\mathsf{Rsp}\quad}$

$e(\mathsf{Rsp}, \mathrm{H}(I)P + Q) \overset{?}{=} e(P, P)e(P, \mathsf{Cmt})^c$

Fig. 1. A New id-imp-pa Secure IBI Scheme Based on the K-sCAA1 Assumption.

By applying the "TWR + HVZK-SS" framework (Section 3.1), a new IBI scheme is constructed from the K-sCAA1 based TWR family $\mathcal{R}^{K\text{–}sCAA1}$ and the corresponding HVZK-SS described above. According to Theorem 1, this IBI scheme is id-imp-pa secure. Fig. 1 summarizes the scheme and the following corollary is obtained directly.

Corollary 1. *The IBI scheme described in Fig. 1 is secure against impersonation under passive attacks (id-imp-pa), in the random oracle model.*

This new IBI scheme is very efficient in terms of both computational complexity and communication overhead, especially at the prover side. In practice, the value $H(I)P + Q$ can be pre-computed by user I (i.e. the prover). So the prover only needs to perform two elliptic curve scalar multiplication operations in $\mathbb{G}_1$, and one of them (in the commitment phase) can also be pre-computed. Therefore, this could be very suitable for smartcard applications. In addition, for the verifier, the value of $e(P, P)$ can also be pre-computed.

5.2. An IBI scheme with id-imp-aa and id-imp-ca security

By applying the "TSR + WD-SS" framework, in Section B.2, we showed the id-imp-aa and id-imp-ca security of the Okamoto-RSA-IBI scheme [21]. In this section, we propose a new IBI scheme which also achieves id-imp-aa and id-imp-ca security. The new scheme is constructed by applying the "TSR+WD-SS" framework. The TSR is based on the Katz–Wang signature scheme [18]. We then propose a WD-SS proof system for this TSR. As of independent interest, unlike the Okamoto-RSA-IBI scheme (Appendix B.2), this new WD-SS proof system is not witness indistinguishable. This means that our newly introduced notion of Witness Dualism is a strict superset of witness indistinguishability.

5.2.1. A TSR family based on a seuf-kma digital signature scheme

Let $\mathbb{G}$ be a cyclic group of prime order q with generator g such that $|q| > k$, where $k \in \mathbb{N}$ is a security parameter. Let $H' : \{0, 1\}^* \rightarrow \{0, 1\}^k$ be a hash function which is assumed to behave as a random oracle for security analysis. Below is the Katz–Wang signature scheme [18].

To generate a public/secret key pair, randomly choose $h \overset{R}{\leftarrow} \mathbb{G}$ and $x \overset{R}{\leftarrow} \mathbb{Z}_q$, then compute $y_1 = g^x$ and $y_2 = h^x$, and set the public key as $PK = (h, y_1, y_2)$ and the secret key as $SK = x$. To sign a message m, the following steps are carried out.

1. Randomly choose $r \overset{R}{\leftarrow} \mathbb{Z}_q$.
2. Compute $A = g^r$, $B = h^r$, and $c = H'(A, B, m)$.
3. Compute $s = cx + r \bmod q$ and return the signature $\sigma = (c, s)$.

To verify the signature σ, $A = g^s y_1^{-c}$ and $B = h^s y_2^{-c}$ are first computed, then σ is considered valid if $c = H'(A, B, m)$. The scheme has been shown to be strongly unforgeable under the DDH assumption [6]. According to Section 4.2.3, we can transform it to a TSR according to the instantiation of TSR based on strongly unforgeable (seuf-kma) digital signature. Below is the resulting TSR family $\mathcal{R}'^{KW}$.

Katz–Wang signature based TSR

1. On input 1^k, $\mathcal{R}'^{KW}.Gen'$ generates $(\mathbb{G}, q, g, H', h, y_1, y_2)$ according to the Katz–Wang signature, then defines the relation $\mathbf{R}^{KW}$ on $(\{0,1\}^k \times \mathbb{Z}_q) \times \{0,1\}^k$ as $\{((c,s),m) : c \in \{0,1\}^k; s \in \mathbb{Z}_q; m \in \{0,1\}^k; c = H'(g^s y_1^{-c}, h^x y_2^{-c}, m)\}$ and the trapdoor as x.
2. On input $(\langle \mathbf{R}^{KW} \rangle, (c,s), m)$, $\mathcal{R}'^{KW}.Ver'$ outputs 1 if and only if $c = H'(g^s y_1^{-c}, h^x y_2^{-c}, m)$.
3. For $\mathcal{R}'^{KW}.Inv'$, on input $(\langle \mathbf{R}^{KW} \rangle, m, x)$, the output (i.e. the witness) (c,s) is computed as $c = H'(g^r, h^r, m)$ and $s = cx + r \bmod q$, where $r \xleftarrow{R} \mathbb{Z}_q$.

Corollary 2. *$\mathbf{R}^{KW}$ is a trapdoor strong-one-more relation.*

Proof. This proposition follows directly from the result of Theorem 9 as both of the two conditions stated in Theorem 9 are satisfied. The first one is that the Katz–Wang digital signature scheme is seuf-kma. The second one, which is obvious, is that there are more than one valid signatures for any message $m \in \{0,1\}^*$. □

Remark. We can see that $\mathbf{R}^{KW}$ is a non-samplable relation. Hence, the IBI scheme described in Fig. 2 cannot be captured by the framework of [2].

5.2.2. A WD-SS proof system for $\mathbf{R}^{KW}$

We now propose a WD-SS proof system (P, V) for $\mathbf{R}^{WD}$, where P knows (c,s) such that $((c,s),m) \in \mathbf{R}^{WD}$ and V has access to public information only, which includes $\langle \mathbf{R}^{WD} \rangle$ and m. The three moves Cmt, Ch and Rsp of the proof system are as follows.

1. Cmt $:= (A, B, A', B', T_1, T_2, T_1', T_2')$ where $A = g^s y_1^{-c}$, $B = h^s y_2^{-c}$, $A' = g^{r'}$, $B' = h^{r'}$, $T_1 = g^{\lambda}$, $T_2 = h^{\lambda}$, $T_1' = g^{z'}(A' y_1^{c'})^{-\alpha'}$, $T_2' = h^{z'}(B' y_2^{c'})^{-\alpha'}$, here $r', \lambda, z', \alpha' \xleftarrow{R} \mathbb{Z}_q$ and $c' \leftarrow H'(A', B', m)$.
2. Ch $:= \alpha_0$ where $\alpha_0 \xleftarrow{R} \mathbb{Z}_q$.
3. Rsp $:= (\alpha', \alpha, z', z)$ where $\alpha = \alpha_0 - \alpha' \bmod q$ and $z = \lambda + \alpha s \bmod q$.

After receiving Rsp, V accepts if and only if $\alpha + \alpha' = \alpha_0$, $T_1 = g^z U^{-\alpha}$, $T_2 = h^z R^{-\alpha}$, $T_1' = g^{z'} U'^{-\alpha'}$ and $T_2' = h^{z'} R'^{-\alpha'}$ where $U = A y_1^c$, $R = B y_2^c$, $U' = A' y_1^{c'}$ and $R' = B' y_2^{c'}$.

We can see this interactive proof system actually conducts a proof that the prover P, knows at least one of two valid signatures of m.

Lemma 1. *The interactive proof system* (P, V) *above for $\mathbf{R}^{KW}$ satisfies the Special Soundness requirement of the WD-SS proof system (Definition 6).*

Proof. Given two acceptable conversations:

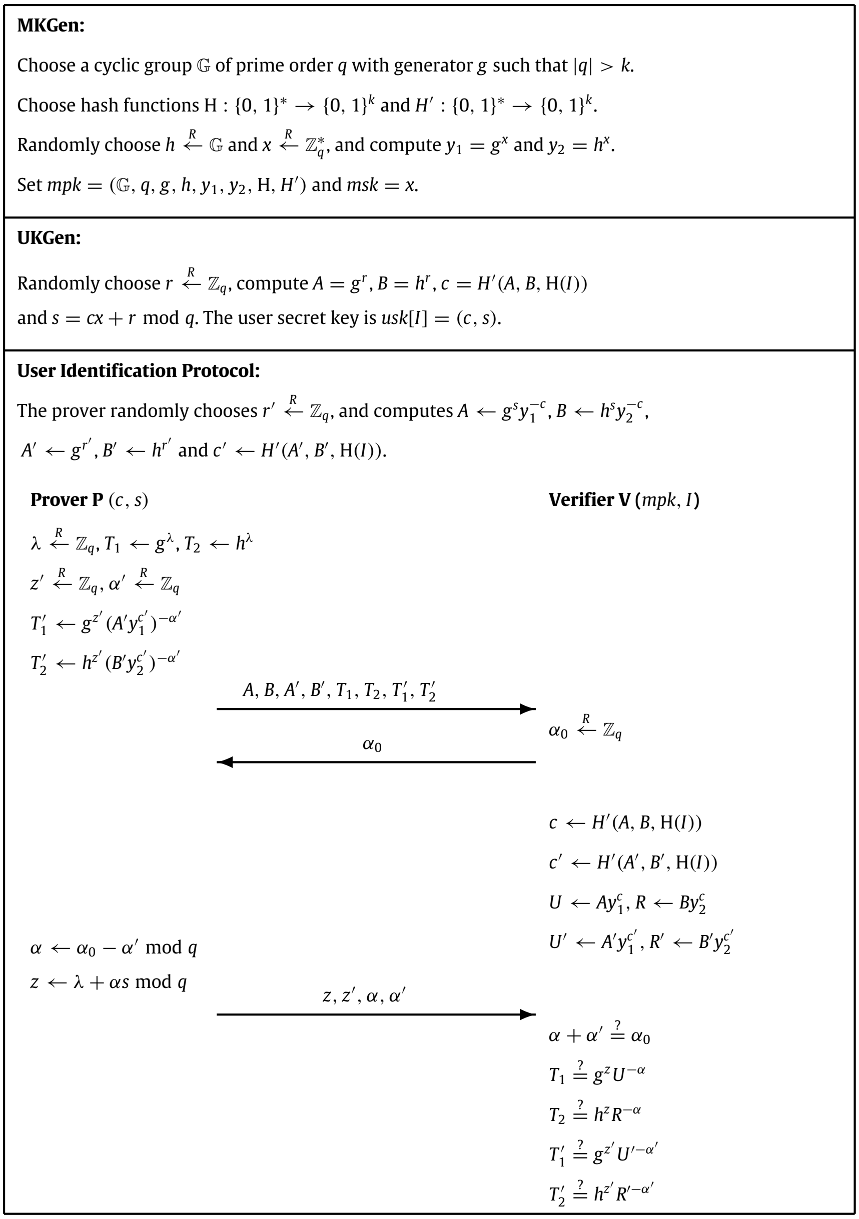
$$((A, B, A', B', T_1, T_2, T_1', T_2'),\ \alpha_0\ , (\alpha', \alpha, z', z))$$
$$((A, B, A', B', T_1, T_2, T_1', T_2'),\ \hat{\alpha}_0\ , (\hat{\alpha}', \hat{\alpha}, \hat{z}', \hat{z}))$$

where V outputs 'accept' and $\alpha_0 \neq \hat{\alpha}_0$, at least one of the inequalities $\alpha \neq \hat{\alpha}$ and $\alpha' \neq \hat{\alpha}'$ must hold. Without loss of generality, suppose $\alpha \neq \hat{\alpha}$, then (s,c) can be obtained from $s = (z - \hat{z})(\alpha - \hat{\alpha})^{-1}$ and $c = H'(A, B, m)$. Therefore, at least one of the two witnesses (s,c) and (s',c') can be extracted. □

Lemma 2. *The interactive proof system* (P, V) *above for $\mathbf{R}^{KW}$ satisfies the Witness Dualism requirement of the WD-SS proof system (Definition 6).*

Proof. For the two valid signatures $\sigma = (c,s)$ (with respect to random coins r) and $\sigma' = (c', s')$ (with respect to random coins r') of message m, the ensembles, $\mathsf{V}_{\mathsf{P}(pub,\sigma)}(pub, aux)$ where σ' is the dual witness, and $\mathsf{V}_{\mathsf{P}(pub,\sigma')}(pub, aux)$ where σ is the dual witness, generated as V's views of the interactive proof, are identically distributed, where pub refers to $(\langle \mathbf{R}^{WD} \rangle, m)$ and aux is any auxiliary input for V. □

Remark (*Important*). (A', B') are computed once for all. That is, after (A', B') are computed by the prover for the first time, they will remain unchanged for all the subsequent protocol runs. In other words, we may consider A', B' as system parameters of the prover. This is crucial for making sure that the interactive proof system satisfies witness dualism. Consider the following scenario, verifier (or distinguisher) $\mathcal{D}$ takes the transcript of one conversation between the prover and an honest verifier as part of its auxiliary input, then $\mathcal{D}$ honestly runs the identification protocol with the prover, if the prover uses different (A_1', B_1') and (A_2', B_2') in two conversations (i.e., one in the auxiliary input of $\mathcal{D}$ and the other in the conversation with $\mathcal{D}$), $\mathcal{D}$ can easily recognize the real user secret key used by the prover. In other words, after (A', B') (with respect to random coins r' and hence signature σ') are used by the prover (with user secret key σ) for the first time, there is only one dual witness of σ, which is σ'.



MKGen:

Choose a cyclic group $\mathbb{G}$ of prime order q with generator g such that $|q| > k$.

Choose hash functions $\mathrm{H} : \{0,1\}^* \to \{0,1\}^k$ and $H' : \{0,1\}^* \to \{0,1\}^k$.

Randomly choose $h \overset{R}{\leftarrow} \mathbb{G}$ and $x \overset{R}{\leftarrow} \mathbb{Z}_q^*$, and compute $y_1 = g^x$ and $y_2 = h^x$.

Set $mpk = (\mathbb{G}, q, g, h, y_1, y_2, \mathrm{H}, H')$ and $msk = x$.

UKGen:

Randomly choose $r \overset{R}{\leftarrow} \mathbb{Z}_q$, compute $A = g^r, B = h^r, c = H'(A, B, \mathrm{H}(I))$ and $s = cx + r \bmod q$. The user secret key is $usk[I] = (c, s)$.

User Identification Protocol:

The prover randomly chooses $r' \overset{R}{\leftarrow} \mathbb{Z}_q$, and computes $A \leftarrow g^s y_1^{-c}, B \leftarrow h^s y_2^{-c}$, $A' \leftarrow g^{r'}, B' \leftarrow h^{r'}$ and $c' \leftarrow H'(A', B', \mathrm{H}(I))$.

Prover P (c, s) — **Verifier V** (mpk, I)

$\lambda \overset{R}{\leftarrow} \mathbb{Z}_q, T_1 \leftarrow g^\lambda, T_2 \leftarrow h^\lambda$

$z' \overset{R}{\leftarrow} \mathbb{Z}_q, \alpha' \overset{R}{\leftarrow} \mathbb{Z}_q$

$T_1' \leftarrow g^{z'}(A'y_1^{c'})^{-\alpha'}$

$T_2' \leftarrow h^{z'}(B'y_2^{c'})^{-\alpha'}$

$\xrightarrow{A, B, A', B', T_1, T_2, T_1', T_2'}$

$\alpha_0 \overset{R}{\leftarrow} \mathbb{Z}_q$

$\xleftarrow{\alpha_0}$

$c \leftarrow H'(A, B, \mathrm{H}(I))$

$c' \leftarrow H'(A', B', \mathrm{H}(I))$

$U \leftarrow Ay_1^c, R \leftarrow By_2^c$

$U' \leftarrow A'y_1^{c'}, R' \leftarrow B'y_2^{c'}$

$\alpha \leftarrow \alpha_0 - \alpha' \bmod q$

$z \leftarrow \lambda + \alpha s \bmod q$

$\xrightarrow{z, z', \alpha, \alpha'}$

$\alpha + \alpha' \overset{?}{=} \alpha_0$

$T_1 \overset{?}{=} g^z U^{-\alpha}$

$T_2 \overset{?}{=} h^z R^{-\alpha}$

$T_1' \overset{?}{=} g^{z'} U'^{-\alpha'}$

$T_2' \overset{?}{=} h^{z'} R'^{-\alpha'}$

Fig. 2. A New id-imp-aa and id-imp-ca Secure IBI Scheme Based on Katz–Wang Signature Scheme.

Theorem 12. *The interactive proof system* (P, V) *for the TSR* $\mathbf{R}^{KW}$ *described above is a WD-SS proof system (Definition* 6*).*

This theorem follows the two lemmas above.

By applying the "TSR + WD-SS" framework (Section 4.1), we combine the seuf-kma signature based TSR family $\mathcal{R}'^{KW}$ and the WD-SS described above to construct an IBI scheme. According to Theorem 6, the resulting IBI scheme is both id-imp-aa and id-imp-ca secure. The scheme is summarized in Fig. 2 and the following corollary is obtained directly.

Corollary 3. *The IBI scheme described in Fig.* 2 *is secure against impersonation under active attacks (id-imp-aa) and concurrent attacks (id-imp-ca) in the random oracle model.*

Remark. For witness indistinguishability, it requires that the verify cannot tell which witness is used by the prover among all the valid witnesses. In our protocol, although the verifier cannot tell which of σ and σ' is used by the prover, the verifier can still exclude all other witnesses (i.e. other valid signatures of $\mathrm{H}(I)$). Therefore, different from the Okamoto-RSA-IBI (Appendix B.2), our WD-SS protocol is not witness indistinguishable. For details, please refer to the discussions following Definition 6 and Lemma 2.

6. Security without random oracle

In this section, we evaluate the security of our IBI construction frameworks *without random oracle*. We will show in the standard model that the generic constructions described in Section 3.1 and Section 4.1 achieve the security against impersonation under passive attack and active/concurrent attacks, respectively, but in a weaker security model than the fully adaptive chosen-ID model used in the games of id-imp-pa, id-imp-aa and id-imp-ca defined in Section 2. This new model is closely related to the conventional selective-ID model [8,9,7], and we call this new model as *Weak Selective-ID Model*. For a conventional selective-ID model, the adversary has to commit to an identity to be attacked *before* knowing the master public key. In a *weak* selective-ID model, the adversary can commit to a (polynomially bounded) set U of identities before knowing the master public key, and is also allowed to adaptively corrupt some of those committed identities. The adversary then chooses an (uncorrupted) identity in U to attack. The formal definition is given as follows.

Definition 9 (*wsid-imp-pa*). For an IBI scheme (**MKGen**, **UKGen**, **P**, **V**), the weak selective-ID security against impersonation under passive attack (wsid-imp-pa) is defined by the following game, which is carried out by a simulator against an adversary $\mathcal{A}$. Let $k \in \mathbb{N}$ be a security parameter.

1. Init: $\mathcal{A}$ outputs a set U of distinct identities such that $|\mathrm{U}| \leq \ell(k)$ where $\ell(\cdot)$ is a polynomial function (in the following, we simply write ℓ to represent $\ell(k)$).
2. $(mpk, msk) \leftarrow \mathbf{MKGen}(1^k)$ is executed and mpk is given to $\mathcal{A}$. Two sets are maintained: HU and CU. Initially, HU is set to U and CU is empty. For each $I \in \mathrm{HU}$, $usk[I] \leftarrow \mathbf{UKGen}(msk, I)$ is executed.
3. $\mathcal{A}$ can then make queries to the following oracles:
   (a) CORR(I) – corrupt a user with identity I: If $I \notin HU$, $\perp$ is returned, otherwise, I is deleted from HU and added into CU, and $usk[I]$ is returned.
   (b) CONV(I) – get a conversation between user I (the prover) and a verifier: If $I \notin HU$, $\perp$ is returned, otherwise, a conversation between a prover with initial state $usk[I]$ and a verifier with initial state (mpk, I) is returned.
4. $\mathcal{A}$ can adaptively query CORR and CONV, and then outputs an identity $\mathrm{I_b} \in HU$, which corresponds to the user that $\mathcal{A}$ wants to impersonate. After receiving $\mathrm{I_b}$, the simulator removes $\mathrm{I_b}$ from HU and adds it into CU.
5. $\mathcal{A}$ begins a run of the user identification protocol with a verifier **V** (initialized with $(mpk, \mathrm{I_b})$) which is simulated by the simulator. $\mathcal{A}$ can continue querying CORR and CONV. The simulator halts when **V** outputs 'accept' or 'reject'.

The wsid-imp-pa advantage of $\mathcal{A}$ on security parameter k is defined as the probability that **V** outputs 'accept'. The IBI scheme (**MKGen**, **UKGen**, **P**, **V**) is said to be wsid-imp-pa secure if the wsid-imp-pa advantage is negligible for any PPT adversary $\mathcal{A}$.

wsid-imp-aa and wsid-imp-ca security. The wsid-imp-aa and wsid-imp-ca security are defined similarly by replacing the CONV oracle with a PROV oracle as in Section 2.

Discussions. The difference between this new weak selective-ID model and the original adaptive chosen-ID model (Section 2) is that in the weak selective-ID model, the adversary has to choose the set of targeting identities before the master public/secret key pair is generated and therefore, the adversary is not allowed to adaptively choose some *new* identities to attack after the master public key is known. For other adversarial capabilities, these two models are the same, particulary, both models allow the adversary to corrupt identities adaptively. In order to remove the random oracle, we look for a replacement of H while trying to keep the rest of the frameworks unchanged. We propose to use a family of ℓ-wise independent hash functions [8]. Let $\mathcal{H}_\ell$ be a family of ℓ-wise independent hash functions from $\{0, 1\}^*$ to Δ.[3] The crucial property of $\mathcal{H}_\ell$ is the following.

Given elements $x_1, x_2, \ldots, x_n \in \{0, 1\}^*$ and $g_1, g_2, \ldots, g_n \in \Delta$ (with $n \leq \ell$), there exists an efficient algorithm to sample a random $\mathrm{H} \in \mathcal{H}_\ell$ such that $\mathrm{H}(x_i) = g_i$ for $i = 1, 2, \ldots, n$. One possible instantiation given in [8] for $\Delta = \mathbb{G}_1$ in the CDH problem (Section 3.2.2) is to let $\mathcal{H}_\ell = \{\mathrm{H}_{h_0,\ldots,h_\ell}(x)\}_{h_0,\ldots,h_\ell \in \mathbb{G}_1}$, where $\mathrm{H}_{h_0,\ldots,h_\ell}(x) = h_0 + \tilde{x}h_1 + \tilde{x}^2 h_2 + \cdots + \tilde{x}^\ell h_\ell$, here $\tilde{x} = \mathrm{G}(x)$ where $\mathrm{G} : \{0, 1\}^* \to \mathbb{Z}_{|\mathbb{G}_1|}$ is a collision resistant hash function.

We modify our construction in Section 3.1 as follows:

1. **MKGen**: $(\langle \mathbf{R} \rangle, t) \leftarrow \mathcal{R}.Gen(1^k)$, $\mathrm{H} \overset{R}{\leftarrow} \mathcal{H}_\ell$. Set $mpk = (\langle \mathbf{R} \rangle, \mathrm{H})$ and $msk = t$.
2. **UKGen**: on input $I \in \{0, 1\}^*$, run $x \leftarrow \mathcal{R}.Inv(\langle \mathbf{R} \rangle, \mathrm{H}(I), t)$ and set $usk[I] = x$.
3. (**P**, **V**): run **P** with the prover algorithm P of the HVZK-SS (WD-SS, respectively) proof system with initial state $usk[I]$, and **V** with the verifier algorithm V of the HVZK-SS (WD-SS, respectively) proof system with initial state $(\langle \mathbf{R} \rangle, \mathrm{H}(I))$.

Theorem 13 (*Theorem 1, revised*). *Let* **R** *be a Trapdoor Weak-one-more Relation (TWR) which has an HVZK-SS proof system and $\mathcal{H}_\ell$ be a family of ℓ-wise independent hash functions, for some polynomial ℓ in k, where $k \in \mathbb{N}$ is a security parameter. If the challenge length $\lambda(k)$ of the HVZK-SS proof system is super logarithmic in k, then an IBI scheme constructed as above is wsid-imp-pa secure in the standard model.*

[3] We use the notation Δ for the range of the function family as the family is always used in association with a relation on $W \times \Delta$ in this paper.

Proof. Suppose there exists an adversary $\mathcal{A}$ who breaks an IBI scheme constructed as above with advantage ϵ, we construct a PPT algorithm $\mathcal{B}$ to break the weak-one-more resistance of the underlying TWR **R** with advantage $\epsilon' \geq (\epsilon - 2^{-\lambda(k)})^2$.

The proof essentially follows the original proof of Theorem 1 except that the simulator $\mathcal{B}$ chooses a hash function in the following way. After receiving the set of identities $\mathrm{U} = \{I_1, \ldots, I_\rho\}$ (note that $\rho \leq \ell$) in the *Init* stage of the game in Definition 9, $\mathcal{B}$ queries RAM and receives ρ random points $g_1, g_2, \ldots, g_\rho \in \Delta$. $\mathcal{B}$ then randomly chooses H from $\mathcal{H}_\ell$ such that $\mathrm{H}(I_i) = g_i$ for $i = 1, 2, \ldots, \rho$. Since $\mathcal{H}_\ell$ is a family of ℓ-wise independent hash functions, the choice of H is identically distributed to that in the real game. $\mathcal{B}$ answers the CORR and CONV queries as in the proof of Theorem 1. Finally, by following the same probability analysis as that in the original proof, $\mathcal{B}$ can break the underlying trapdoor weak-one-more relation with probability at least $(\epsilon - 2^{-\lambda(k)})^2$. □

Similarly, we have the following theorem.

Theorem 14 (*Theorem 6, revised*). *Let* **R** *be a Trapdoor Strong-one-more Relation (TSR) which has a WD-SS proof system and $\mathcal{H}_\ell$ be a family of ℓ-wise independent hash functions, for some polynomial ℓ in k, where $k \in \mathbb{N}$ is a security parameter. If the challenge length $\lambda(k)$ of the WD-SS proof system is super logarithmic in k, the IBI scheme constructed as above is* wsid-imp-aa *and* wsid-imp-ca *secure in the standard model.*

Discussions. In the proof of Theorem 1, due to the idealness assumption of the random oracle, $\mathcal{B}$ can indistinguishably simulate a real game while mapping random challenge points from Δ obtained from RAM oracle to the values of $\mathrm{H}(I_i)$ corresponding to identities I_i which are to be attacked. Now in the standard model, we do not have the random oracle to do the indistinguishable mapping. Instead, we employ a family of ℓ-wise independent hash functions $\mathcal{H}_\ell$ so that for all the n pre-selected identities in U, the simulator (that is, $\mathcal{B}$) can still map the random points from Δ obtained from RAM oracle to the values of $\mathrm{H}(I_i)$, and still have the game simulated indistinguishably. However, the value of n (that is the number of to-be-attacked identities) is bounded by that of ℓ and those identities have to be pre-selected before generating the master public/secret key pair. As a result, in the standard model, we can only show that our framework is secure in the weak selective-ID model. We leave the construction of a comparable framework secure under the fully adaptive chosen-ID model an open problem.

7. Conclusion

In this paper, we proposed a new framework to the design and analysis of Identity-Based Identification (IBI) schemes. We separate an IBI scheme into two parts: a hard relation and an interactive proof system. In order to obtain IBI schemes with different security levels, we specified the security requirements of these two building blocks and defined several new notions for them. We proved that a Trapdoor Weak-one-more Relation (TWR) combining with an Honest Verifier Zero-Knowledge proof with Special Soundness (HVZK-SS) yield an IBI scheme secure against passive attack, and a Trapdoor Strong-one-more Relation (TSR) combining with a Witness Dualism proof with Special Soundness (WD-SS) yield an IBI scheme secure against active and concurrent attacks. Both of these results are proved in the random oracle model under the fully adaptive chosen-ID model (id-imp-pa, id-imp-aa and id-imp-ca) and in the standard model under the weak selective-ID model (wsid-imp-pa, wsid-imp-aa and wsid-imp-ca).

We also showed that the new notions defined in this paper can capture a large number of instantiations. This is important because it allows us to adopt a systematic way for analyzing the security of many existing IBI schemes. In addition to this, the framework also provides us an effective way for constructing new IBI schemes. We proposed two new IBI schemes, one with security against impersonation under passive attack, and the other one with security against impersonation under active and concurrent attacks. None of them is in any existing framework.

The new notions defined in this paper, namely TWR, TSR and WD-SS, are of independent interest. We believe that they can be used for other applications as well in the near future.

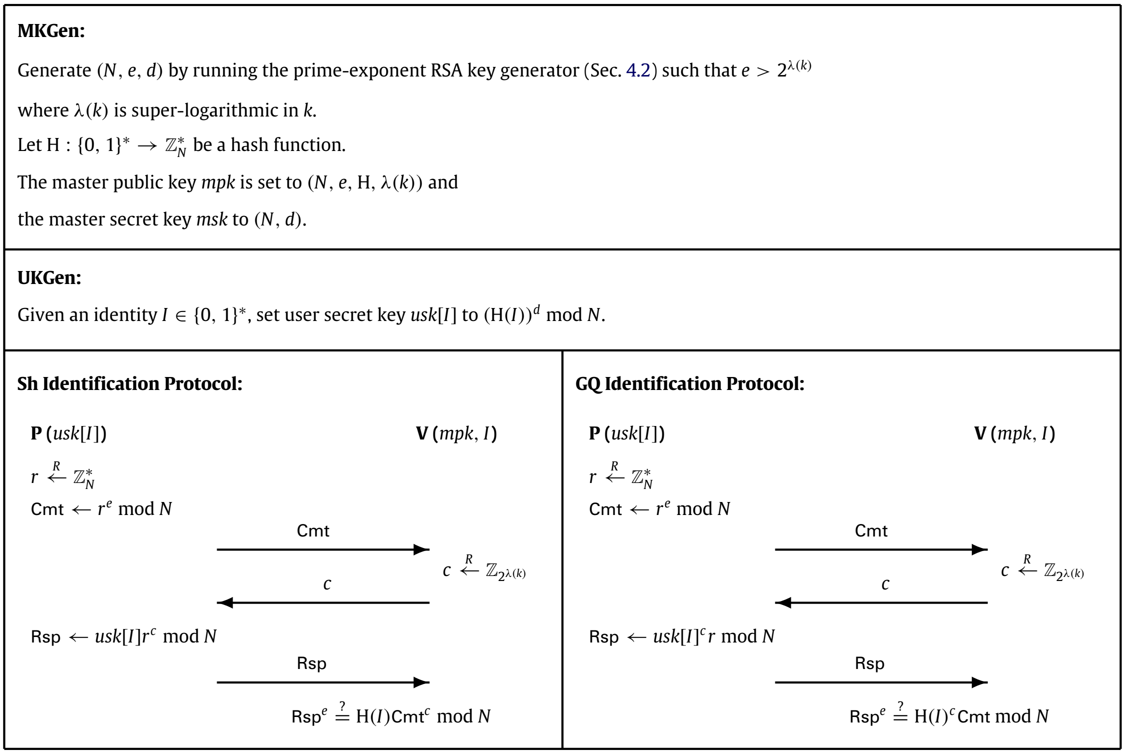
Acknowledgements

The work described in this paper was partially supported by a grant from CityU (7001975). Duncan S. Wong was supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (RGC Ref. No. CityU 122107). Jing Chen's research was conducted while at City University of Hong Kong.

Appendix A. Reset lemma

Lemma 3 (*Reset Lemma [3,2]*). *Let* **CP** *be the prover in a canonical interactive proof system with challenge set* ChSet *and challenge length $\lambda(\cdot)$. St_V and St_{CP} are the initial states of the verifier and* **CP***, respectively. Let $acc(St_{CP}, St_V)$ be the probability that the verifier accepts, i.e., the probability that the following experiment returns* 1*:*

Choose a random tape ρ for **CP***;* $(\mathsf{Cmt}, St'_{CP}) \leftarrow \mathbf{CP}(St_{CP}, \rho)$; $\mathsf{Ch} \xleftarrow{R} \mathsf{ChSet}$;
$(\mathsf{Rsp}, St''_{CP}) \leftarrow \mathbf{CP}(\mathsf{Ch}, St'_{CP})$; $d \leftarrow \mathbf{Dec}(St_V, \mathsf{Cmt}\|\mathsf{Ch}\|\mathsf{Rsp})$;
Return d



MKGen:

Generate (N, e, d) by running the prime-exponent RSA key generator (Sec. 4.2) such that $e > 2^{\lambda(k)}$

where $\lambda(k)$ is super-logarithmic in k.

Let $\mathrm{H} : \{0, 1\}^* \to \mathbb{Z}_N^*$ be a hash function.

The master public key *mpk* is set to $(N, e, \mathrm{H}, \lambda(k))$ and

the master secret key *msk* to (N, d).

UKGen:

Given an identity $I \in \{0, 1\}^*$, set user secret key $usk[I]$ to $(\mathrm{H}(I))^d \bmod N$.

Sh Identification Protocol:

P $(usk[I])$
V (mpk, I)
$r \overset{R}{\leftarrow} \mathbb{Z}_N^*$
$\mathsf{Cmt} \leftarrow r^e \bmod N$
Cmt
$c \overset{R}{\leftarrow} \mathbb{Z}_{2^{\lambda(k)}}$
c
$\mathsf{Rsp} \leftarrow usk[I]r^c \bmod N$
Rsp
$\mathsf{Rsp}^e \overset{?}{=} \mathrm{H}(I)\mathsf{Cmt}^c \bmod N$

GQ Identification Protocol:

P $(usk[I])$
V (mpk, I)
$r \overset{R}{\leftarrow} \mathbb{Z}_N^*$
$\mathsf{Cmt} \leftarrow r^e \bmod N$
Cmt
$c \overset{R}{\leftarrow} \mathbb{Z}_{2^{\lambda(k)}}$
c
$\mathsf{Rsp} \leftarrow usk[I]^c r \bmod N$
Rsp
$\mathsf{Rsp}^e \overset{?}{=} \mathrm{H}(I)^c\mathsf{Cmt} \bmod N$

Fig. 3. The Sh-IBI and GQ-IBI.

and $res(St_{CP}, St_V)$ *the probability that the following reset experiment returns* 1*:*

```
Choose a random tape $\rho$ for $\mathbf{CP}$;  $(\mathsf{Cmt}, St'_{CP}) \leftarrow \mathbf{CP}(St_{CP}, \rho)$
$\mathsf{Ch}_1 \overset{R}{\leftarrow} \mathsf{ChSet}$; $(\mathsf{Rsp}_1, St''_{CP}) \leftarrow \mathbf{CP}(\mathsf{Ch}_1, St'_{CP})$;
$d_1 \leftarrow \mathbf{Dec}(St_V, \mathsf{Cmt}\|\mathsf{Ch}_1\|\mathsf{Rsp}_1)$
$\mathsf{Ch}_2 \overset{R}{\leftarrow} \mathsf{ChSet}$; $(\mathsf{Rsp}_2, St'''_{CP}) \leftarrow \mathbf{CP}(\mathsf{Ch}_2, St'_{CP})$;
$d_2 \leftarrow \mathbf{Dec}(St_V, \mathsf{Cmt}\|\mathsf{Ch}_2\|\mathsf{Rsp}_2)$
If ($d_1 = d_2 = 1$ and $\mathsf{Ch}_1 \neq \mathsf{Ch}_2$) return 1, else return 0
```

Then,

$$res(St_{CP}, St_V) \geq (acc(St_{CP}, St_V) - 2^{-\lambda(k)})^2.$$

Appendix B. Existing IBI schemes captured by the new framework

B.1. IBI schemes with id-imp-pa security

B.1.1. Sh-IBI [22,2] and GQ-IBI [16,2]

The Sh-IBI scheme is a combination of the RSA (one candidate of Trapdoor One-way Permutation) based TWR and an HVZK-SS proof system. The GQ-IBI scheme uses the same TWR but a different HVZK-SS.

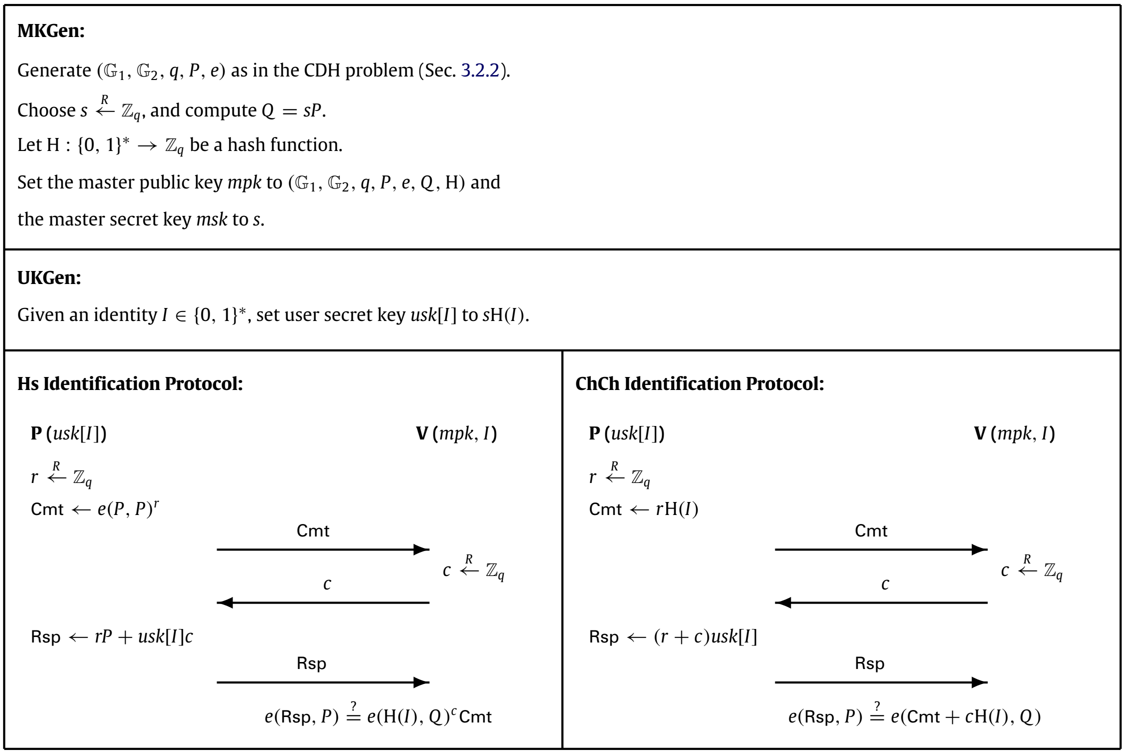
Theorem 15. *The Sh identification protocol described in Fig. 3 is an HVZK-SS proof system (Definition 4).*

Proof. It is obvious that $(\mathbf{P}, \mathbf{V})$ is a non-trivial canonical proof system satisfying the Completeness requirement.

For Special Soundness, we can see that given $(\mathsf{Cmt}, c_1, \mathsf{Rsp}_1)$ and $(\mathsf{Cmt}, c_2, \mathsf{Rsp}_2)$ with $c_1 \neq c_2$ (without loss of generality, we assume $c_1 > c_2$), we can use the Extended Euclidian Algorithm to find two integers a, b such that $a(c_1 - c_2) + be = 1$. Then $usk[I]$ can be extracted as $\mathsf{Rsp}_1((\mathsf{Rsp}_1/\mathsf{Rsp}_2)^a\mathsf{Cmt}^b)^{-c_1} \bmod N$.

The proof system is also Honest Verifier Zero Knowledge as we can construct a polynomial time algorithm $\mathcal{SIM}$ which generates a conversation between **P** and **V** as follows. Randomly choose $c \overset{R}{\leftarrow} \mathbb{Z}_{2^{\lambda(k)}}$ and use the Extended Euclidian Algorithm to compute integers a, b such that $ac + be = 1$. Randomly select $z \overset{R}{\leftarrow} \mathbb{Z}_N^*$ and set $\mathsf{Ch} = c$, $\mathsf{Rsp} = \mathrm{H}(I)^b z^c$, $\mathsf{Cmt} = z^e \mathrm{H}(I)^{-a} \bmod N$. □

Theorem 16. *The GQ identification protocol described in Fig. 3 is an HVZK-SS proof system (Definition 4).*



MKGen:

Generate $(\mathbb{G}_1, \mathbb{G}_2, q, P, e)$ as in the CDH problem (Sec. 3.2.2).

Choose $s \overset{R}{\leftarrow} \mathbb{Z}_q$, and compute $Q = sP$.

Let $\mathrm{H} : \{0, 1\}^* \rightarrow \mathbb{Z}_q$ be a hash function.

Set the master public key *mpk* to $(\mathbb{G}_1, \mathbb{G}_2, q, P, e, Q, \mathrm{H})$ and the master secret key *msk* to s.

UKGen:

Given an identity $I \in \{0, 1\}^*$, set user secret key $usk[I]$ to $s\mathrm{H}(I)$.

Hs Identification Protocol:

$\mathbf{P}\,(usk[I])$ $\mathbf{V}\,(mpk, I)$

$r \overset{R}{\leftarrow} \mathbb{Z}_q$

$\mathsf{Cmt} \leftarrow e(P, P)^r$

$\xrightarrow{\mathsf{Cmt}}$

$c \overset{R}{\leftarrow} \mathbb{Z}_q$

$\xleftarrow{c}$

$\mathsf{Rsp} \leftarrow rP + usk[I]c$

$\xrightarrow{\mathsf{Rsp}}$

$e(\mathsf{Rsp}, P) \overset{?}{=} e(\mathrm{H}(I), Q)^c \mathsf{Cmt}$

ChCh Identification Protocol:

$\mathbf{P}\,(usk[I])$ $\mathbf{V}\,(mpk, I)$

$r \overset{R}{\leftarrow} \mathbb{Z}_q$

$\mathsf{Cmt} \leftarrow r\mathrm{H}(I)$

$\xrightarrow{\mathsf{Cmt}}$

$c \overset{R}{\leftarrow} \mathbb{Z}_q$

$\xleftarrow{c}$

$\mathsf{Rsp} \leftarrow (r + c)usk[I]$

$\xrightarrow{\mathsf{Rsp}}$

$e(\mathsf{Rsp}, P) \overset{?}{=} e(\mathsf{Cmt} + c\mathrm{H}(I), Q)$

Fig. 4. The Hs-IBI and ChCh-IBI.

Proof. It is obvious that $(\mathbf{P}, \mathbf{V})$ is a non-trivial canonical proof system satisfying the Completeness requirement.

For Special Soundness, we can see that given $(\mathsf{Cmt}, c_1, \mathsf{Rsp}_1)$ and $(\mathsf{Cmt}, c_2, \mathsf{Rsp}_2)$ with $c_1 \neq c_2$ (without loss of generality, we assume $c_1 > c_2$), we can use the Extended Euclidian Algorithm to compute integers a, b such that $a(c_1 - c_2) + be = 1$. Then $usk[I]$ can be extracted as $(\mathsf{Rsp}_1/\mathsf{Rsp}_2)^a(\mathrm{H}(I))^b \bmod N$.

The proof system is also Honest Verifier Zero Knowledge as we can construct a polynomial time algorithm $\mathcal{SIM}$ which generates a conversation between **P** and **V** as follows. Randomly choose $c \overset{R}{\leftarrow} \mathbb{Z}_{2^{\lambda(k)}}$ and $z \overset{R}{\leftarrow} \mathbb{Z}_N^*$ and set $\mathsf{Ch} = c$, $\mathsf{Rsp} = z$, $\mathsf{Cmt} = z^e\mathrm{H}(I)^{-c} \bmod N$. □

Corollary 4. *The Sh-IBI and GQ-IBI are secure against impersonation under passive attack (id-imp-pa) under the RSA assumption in the random oracle model.*

B.1.2. Hs-IBI [17,2] and ChCh-IBI [10,2]

The Hs-IBI and ChCh-IBI can be decomposed into two parts: a CDH-based TWR and an HVZK-SS. These two schemes are reviewed in Fig. 4.

Theorem 17. *The Hs identification protocol is an HVZK-SS proof system (Definition 4).*

Proof. It is obvious that $(\mathbf{P}, \mathbf{V})$ is a non-trivial canonical proof system satisfying the Completeness requirement.

For Special Soundness, we can see that given $(\mathsf{Cmt}, c_1, \mathsf{Rsp}_1)$ and $(\mathsf{Cmt}, c_2, \mathsf{Rsp}_2)$ with $c_1 \neq c_2$, we can extract $usk[I]$ as $(c_1 - c_2)^{-1}(\mathsf{Rsp}_1 - \mathsf{Rsp}_2)$.

The proof system is also Honest Verifier Zero Knowledge, as we can construct a polynomial time algorithm $\mathcal{SIM}$ which generates a conversation between **P** and **V** as follows. Randomly choose $c \overset{R}{\leftarrow} \mathbb{Z}_q$ and $Z \overset{R}{\leftarrow} \mathbb{G}_1$ and set $\mathsf{Ch} = c$, $\mathsf{Rsp} = Z$, $\mathsf{Cmt} = e(Z, P)e(\mathrm{H}(I), Q)^{-c}$. □

Theorem 18. *The ChCh identification protocol is an HVZK-SS proof system (Definition 4).*

Proof. It is obvious that $(\mathbf{P}, \mathbf{V})$ is a non-trivial canonical proof system satisfying the Completeness requirement.

For Special Soundness, we can see that given $(\mathsf{Cmt}, c_1, \mathsf{Rsp}_1)$ and $(\mathsf{Cmt}, c_2, \mathsf{Rsp}_2)$ with $c_1 \neq c_2$, $usk[I]$ can be extracted as $(c_1 - c_2)^{-1}(\mathsf{Rsp}_1 - \mathsf{Rsp}_2)$.

The proof system is also Honest Verifier Zero Knowledge, as we can construct a polynomial time algorithm $\mathcal{SIM}$ which generates a conversation between **P** and **V** as follows. Randomly choose $c \overset{R}{\leftarrow} \mathbb{Z}_q$ and $z \overset{R}{\leftarrow} \mathbb{Z}_q$ and set $\mathsf{Ch} = c$, $\mathsf{Rsp} = zQ$, $\mathsf{Cmt} = zP - c\mathrm{H}(I)$. □

Corollary 5. *The Hs-IBI and ChCh-IBI are secure against impersonation under passive attack (id-imp-pa) under the CDH assumption in the random oracle model.*

MKGen:

Generate (N, e, d) by running the prime-exponent RSA key generator (Sec. 4.2) such that $e > 2^{\lambda(k)}$

where $\lambda(k)$ is super-logarithmic in k. Randomly picks $g \overset{R}{\leftarrow} \mathbb{Z}_N^*$.

Let $\mathrm{H} : \{0, 1\}^* \rightarrow \mathbb{Z}_N^*$ be a hash function.

The master public key *mpk* is set to $(N, e, g, \mathrm{H}, \lambda(k))$ and

the master secret key *msk* to (N, d).

UKGen:

Given an identity $I \in \{0, 1\}^*$, set user secret key $usk[I]$ to (x_1, x_2) where $x_1 \overset{R}{\leftarrow} \mathbb{Z}_e$ and

$x_2 = (g^{x_1}\mathrm{H}(I))^{-d} \pmod N$.

Okamoto-RSA Identification Protocol:

Prover P $(usk[I] = (x_1, x_2))$ **Verifier V** (mpk, I)

$y_1 \overset{R}{\leftarrow} \mathbb{Z}_e; y_2 \overset{R}{\leftarrow} \mathbb{Z}_N^*$

$\mathsf{Cmt} \leftarrow g^{y_1} y_2^e \bmod N$

$\xrightarrow{\mathsf{Cmt}}$

$c \overset{R}{\leftarrow} \mathbb{Z}_{2^{\lambda(k)}}$

$\xleftarrow{c}$

$z_1 \leftarrow y_1 + cx_1 \bmod e$

$z_2 \leftarrow g^{\lfloor (y_1+cx_1)/e \rfloor} y_2 x_2^c \bmod N$

$\xrightarrow{\mathsf{Rsp} = (z_1, z_2)}$

$\mathsf{Cmt} \overset{?}{=} g^{z_1} z_2^e \mathrm{H}(I)^c \bmod N$

Fig. 5. The Okamoto-RSA-IBI.

B.2. IBI schemes with id-imp-aa and id-imp-ca security

B.2.1. Okamoto-RSA-IBI

The Okamoto-RSA-IBI [21] can be decomposed into two parts: the RSA-based TSR and a WD-SS proof system. The scheme is reviewed in Fig. 5.

Theorem 19. *The Okamoto-RSA identification protocol is a WD-SS proof system (Definition 4).*

Proof. It is obvious that (**P**, **V**) is a non-trivial canonical proof system, satisfying the Completeness requirement.

For Special Soundness, we can see that given $(\mathsf{Cmt}, c, \mathsf{Rsp})$ and $(\mathsf{Cmt}, c', \mathsf{Rsp}')$ with $c \neq c'$ (without loss of generality, we assume $c > c'$), we can extract $usk[I]$ as follows: first, compute $x_1 = (c - c')^{-1}(z_1 - z_1') \bmod e$; then compute $y_1 = z_1 - cx_1 \bmod e$, and calculate

$$X = \frac{z_2/g^{\lfloor (y_1+cx_1)/e \rfloor}}{z_2'/g^{\lfloor (y_1+c'x_1)/e \rfloor}} = x_2^{c-c'} \bmod N \tag{1}$$

$$Y = (\mathrm{H}(I)g^{x_1})^{-1}) = x_2^e \bmod N \tag{2}$$

then use the Extended Euclidian Algorithm to compute integers a, b such that $a(c - c') + be = 1$, finally compute $x_2 = (X)^a(Y)^b \bmod N$.

As proved in [21], the Okamoto-RSA identification protocol is witness indistinguishable, so it is also a witness dualism proof system. □

Corollary 6. *The Okamoto-RSA-IBI is secure against impersonation under active and concurrent attacks (id-imp-aa and id-imp-ca) under the RSA assumption in the random oracle model.*

References

[1] Jee Hea An, Yevgeniy Dodis, Tal Rabin, On the security of joint signature and encryption, in: EUROCRYPT 2002, in: Lecture Notes in Computer Science, vol. 2332, Springer, 2002, pp. 83–107.

[2] Mihir Bellare, Chanathip Namprempre, Gregory Neven, Security proofs for identity-based identification and signature schemes, in: EUROCRYPT 2004, in: Lecture Notes in Computer Science, vol. 3027, Springer, 2004, pp. 268–286. Full paper available at http://eprint.iacr.org/2004/252.

[3] Mihir Bellare, Adriana Palacio, GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks, in: CRYPTO 2002, in: Lecture Notes in Computer Science, vol. 2442, Springer, 2002, pp. 162–177.

[4] Mihir Bellare, Phillip Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, in: ACM Conference on Computer and Communications Security, ACM CCS, 1993, pp. 62–73.

[5] Manuel Blum, Coin flipping by telephone, in: CRYPTO 1981, 1981, pp. 11–15.

[6] D. Boneh, The decision Diffie–Hellman problem, in: Proc. of the Third Algorithmic Number Theory Symposium, in: Lecture Notes in Computer Science, vol. 1423, Springer, 1998, pp. 48–63.

[7] Dan Boneh, Xavier Boyen, Efficient selective-id secure identity-based encryption without random oracles, in: EUROCRYPT 2004, in: Lecture Notes in Computer Science, vol. 3027, Springer, 2004, pp. 223–238.

[8] Ran Canetti, Shai Halevi, Jonathan Katz, A forward-secure public-key encryption scheme, in: EUROCRYPT 2003, in: Lecture Notes in Computer Science, vol. 2656, Springer, 2003, pp. 255–271.

[9] Ran Canetti, Shai Halevi, Jonathan Katz, Chosen-ciphertext security from identity-based encryption, in: EUROCRYPT 2004, in: Lecture Notes in Computer Science, vol. 3027, Springer, 2004, pp. 207–222.

[10] Jae Choon Cha, Jung Hee Cheon, An identity-based signature from gap Diffie–Hellman groups, in: Public Key Cryptography 2003, in: Lecture Notes in Computer Science, vol. 2567, Springer, 2002, pp. 18–30.

[11] Liqun Chen, Zhaohui Cheng, Security proof of Sakai-Kasahara's identity-based encryption scheme, in: IMA Int. Conf., 2005, pp. 442–459.

[12] Uriel Feige, Adi Shamir, Witness indistinguishable and witness hiding protocols, in: Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing, STOC, 1990.

[13] O. Goldreich, Foundations of Cryptography: Basic Tools, Cambridge University Press, 2001.

[14] S. Goldwasser, S. Micali, R. Rivest, A digital signature scheme secure against adaptive chosen-message attack, SIAM J. Comput. 17 (2) (1988) 281–308.

[15] Shafi Goldwasser, Silvio Micali, Probabilistic encryption, J. Comput. Syst. Sci. 28 (2) (1984) 270–299.

[16] Louis C. Guillou, Jean-Jacques Quisquater, A "paradoxical" indentity-based signature scheme resulting from zero-knowledge, in: CRYPTO 1988, in: Lecture Notes in Computer Science, vol. 403, Springer, 1990, pp. 216–231.

[17] Florian Hess, Efficient identity based signature schemes based on pairings, in: Selected Areas in Cryptography (SAC) 2002, in: Lecture Notes in Computer Science, vol. 2595, Springer, 2003, pp. 310–324.

[18] Jonathan Katz, Nan Wang, Efficiency improvements for signature schemes with tight security reductions. in: Proceedings of the 10th ACM conference on Computer and Communications Security, ACM CCS '03, pp. 155–164, 2003.

[19] Kaoru Kurosawa, Swee-Huay Heng, From digital signature to ID-based identification/signature, in: Public Key Cryptography 2004, in: Lecture Notes in Computer Science, vol. 2947, Springer, 2004, pp. 248–261.

[20] S. Mitsunari, R. Sakai, M. Kasahara, A new traitor tracing, IEICE Trans. Fundamentals E85-A(2) (2002).

[21] Tatsuaki Okamoto, Provably secure and practical identification schemes and corresponding signature schemes, in: CRYPTO 1992, in: Lecture Notes in Computer Science, vol. 740, Springer, 1993, pp. 31–53.

[22] Adi Shamir, Identity-based cryptosystems and signature schemes, in: CRYPTO 1984, in: Lecture Notes in Computer Science, vol. 196, Springer, 1985, pp. 47–53.

[23] Jacques Stern, David Pointcheval, John Malone-Lee, Nigel P. Smart, Flaws in applying proof methodologies to signature schemes, in: CRYPTO 2002, in: Lecture Notes in Computer Science, vol. 2442, Springer, 2002, pp. 93–110.

[24] Hugh C. Williams, A modification of the RSA public-key encryption procedure, IEEE Trans. Inform Theory 26 (6) (1980).