6-2007

A more natural way to construct identity-based identification schemes

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

Jing CHEN
Tsinghua University

Duncan S. WONG
City University of Hong Kong

Xiaotie DENG
City University of Hong Kong

Dongsheng WANG
Tsinghua University

Citation

YANG, Guomin; CHEN, Jing; WONG, Duncan S.; DENG, Xiaotie; and WANG, Dongsheng. A more natural way to construct identity-based identification schemes. (2007). *Applied Cryptography and Network Security: 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8: Proceedings*. 4521, 307-322.
Available at: https://ink.library.smu.edu.sg/sis_research/7422

A More Natural Way to Construct Identity-Based Identification Schemes

Guomin Yang[1], Jing Chen[2], Duncan S. Wong[1], Xiaotie Deng[1], and Dongsheng Wang[2]

[1] Department of Computer Science
City University of Hong Kong
Hong Kong, China
{csyanggm,duncan,deng}@cs.cityu.edu.hk
[2] Department of Computer Science
Tsinghua University
Beijing, China
jingchen@cityu.edu.hk, wds@tsinghua.edu.cn

Abstract. Constructing identification schemes 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 itself to a public verifier who knows only the claimed identity of the prover and some common information. In this paper, we propose a simple and efficient framework for constructing IBI schemes. Unlike some related framework which constructs IBI schemes from some standard identification schemes, our framework is based on some more fundamental assumptions on intractable problems. Depending on the features of the underlying intractable problems presumed in our framework, we can derive IBI schemes secure against passive, active and concurrent adversaries. We show that the framework can capture a large class of schemes currently proposed, and also has the potential to cover many newly constructed schemes. As an example, based on the Katz-Wang standard signature scheme, we propose a new IBI scheme that is secure against active adversaries in a concurrent manner. It can be seen that our framework also help simplify the security proofs for new IBI schemes. Finally, and of independent interest, we define a new notion for proof systems called Witness Dualism. This notion is weaker than that of witness indistinguishable and we show that it is enough for constructing an IBI scheme secure against the most powerful type of adversaries defined.

Keywords: Identity-based cryptography, Identification schemes, Concurrent attacks.

1 Introduction

In an identity-based cryptosystem, there is an authority having a master public/secret key pair. This authority can provide a user with a user secret key which is derived from the user's identity and the master secret key. In an identity-based

J. Katz and M. Yung (Eds.): ACNS 2007, LNCS 4521, pp. 307–322, 2007.

identification (IBI) scheme, a user, playing the role of a prover, identifies itself to a verifier, who knows only the prover's identity and the master public key.

There are three notions for the security of IBI schemes: security against impersonation under passive attacks (id-imp-pa), active attacks (id-imp-aa), and concurrent attacks (id-imp-ca). In a passive attack, an adversary can obtain communication transcripts between the real prover and a verifier. In an active or concurrent attack, the adversary can directly communicate with the prover by playing the role of a cheating verifier. The difference between id-imp-aa and id-imp-ca is that in the former case, the adversary can have only one active session at a time, but in a concurrent attack, the adversary can have concurrent (or parallel) active sessions.

In this paper, we propose a simple and efficient method to construct IBI schemes. Our method is based on two notions, namely *trapdoor weak-one-more relation* and *trapdoor strong-one-more relation*. We show that the former one can be constructed from intractable problems such as trapdoor one-way permutations and the Computational Diffie-Hellman (CDH) problem; and the latter one can be constructed from the factoring problem, the RSA problem and any strongly unforgeable [1] (referred to as *non-malleability in* [17]) signature schemes. By applying a trapdoor weak-one-more relation with an honest verifier zero knowledge proof of knowledge, we get an IBI scheme secure against passive attacks. While if we apply a trapdoor strong-one-more relation with a *witness dualism* proof of knowledge, we obtain an IBI scheme secure against active and concurrent attacks. Since the notion of witness dualism is weaker than that of witness indistinguishability [9], any proof system which is witness indistinguishable can readily be used in our framework as a witness dualism proof system. Besides proposing the generic framework for constructing IBI schemes with various levels of security, we also propose a concrete scheme. The scheme is based on the Katz-Wang strongly unforgeable signature scheme. The concrete IBI scheme falls in our framework and can be shown easily to be id-imp-ca secure.

1.1 Related Work

Since Shamir introduced the identity-based cryptosystems [16], a lot of IBI schemes have been proposed. A survey can be found in [2]. In [2], the authors proposed a method to construct IBI schemes by using digital certificates: the master key generation center (or called authority) picks a public/secret key pair (pk, sk) for a standard identification (SI) scheme, and provides these to prover I along with a certificate *cert* consisting of the authority's signature on (I, pk). The prover sends pk, and *cert* to a verifier and identifies itself using the SI scheme. The verifier needs to know only I and the public key of the authority. Although simple, this method (named *certificate-based* IBI) is inefficient, and its significance is to answer a fundamental question: secure IBI schemes (in the standard model) exists if and only if one-way function exists. In [2], another framework is proposed that transforms any standard identification scheme which satisfies certain conditions (referred to as convertible SI schemes) to IBI schemes in the random oracle model [4].

Independently in [14], a transformation is proposed that converts some digital signature scheme to an IBI scheme. The authors showed that the resulting IBI scheme is id-imp-pa secure if the underlying signature scheme is existentially unforgeable against adaptive chosen message attack [10]. One aspect of this transformation is that it is not necessarily to be in the random oracle model, however, the signature scheme (the BLS short signature scheme [7]) they used to construct a concrete IBI scheme is only proven secure in the random oracle model.

In this paper, we propose a more "natural" and efficient method to construct IBI schemes. Comparing with the approach of[2] which requires a underlying provably secure convertible standard indentification (SI) scheme, our method starts directly from the definitions of some intractable problems. And more importantly, our construction explicitly explains the features a hard problem should have in order to achieve passive and active/concurrent security.

Our method is also more generic than that of [14], in the sense that constructing IBI schemes from standard signature schemes is just one of the many possible instantiations in our framework. Additionally, we can construct IBI schemes secure against active and concurrent attacks from strongly unforgeable signature schemes. In Sec. 5, we also construct a concrete IBI scheme that is secure against concurrent attacks from the Katz-Wang signature scheme [13].

2 Identity-Based Identification Schemes

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

Let $k \in \mathbb{N}$ be a security parameter. A canonical interactive proof system $(\mathbf{P}, \mathbf{V})$ has commitment length $\beta(\cdot)$ if $|\mathrm{CmtSet}| \geq 2^{\beta(k)}$, has challenge length $\ell(\cdot)$ if $|\mathrm{ChSet}| \geq 2^{\ell(k)}$, and is *non-trivial* if the function $2^{-\beta(k)}$ is negligible in k.

Definition 1 (Identity-Based Identification (IBI)). *An identity-based identification (IBI) scheme consists of four probabilistic polynomial-time (PPT) algorithms* $(\mathbf{MKGen}, \mathbf{UKGen}, \mathbf{P}, \mathbf{V})$.

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

We require that for all $k \in \mathbb{N}$, $I \in \{0,1\}^*$, $(mpk, msk) \leftarrow \mathbf{MKGen}(1^k)$, and $usk[I] \leftarrow \mathbf{UKGen}(msk, I)$, $\mathbf{V}$ (initialized with mpk, I) always outputs '*accept*' after interacting with $\mathbf{P}$ (initialized with $usk[I]$).

The security of an IBI scheme is commonly considered against three types of attacks: impersonation under passive attacks (id-imp-pa), active attacks (id-imp-aa) and concurrent attacks (id-imp-ca). The following definitions are due to [2].

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

1. $(mpk, msk) \leftarrow \mathbf{MKGen}$ *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 a user (as 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* $\mathbf{V}$ *(initialized with* $(mpk, \mathrm{I_b})$*) which is simulated by the simulator.* $\mathcal{A}$ *can continue querying* INIT*,* CORR *and* CONV*. The simulate halts when* $\mathbf{V}$ *outputs 'accept' or 'reject'.*

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

id-imp-aa and id-imp-ca security. The id-imp-aa security is defined by a similar game, but the conversation oracle, CONV, is replaced by a proving oracle, PROV. $\mathcal{A}$ can select any identity $I \in$ HU and start a conversation with PROV which is the simulation of $\mathbf{P}(usk[I])$. The difference between id-imp-aa and id-imp-ca is that in the former case, $\mathcal{A}$ can have only one active session with PROV at a time, but in the latter case, $\mathcal{A}$ can have concurrent (or parallel) active sessions.

3 A Generic IBI Scheme Secure Against Passive Attacks

In this section, we propose a generic construction of IBI schemes that can be proven secure against passive attacks (namely, id-imp-pa secure in the sense of Def. 2). In the following, we define a relation called *trapdoor weak-one-more relation*, which enables our generic construction to capture many concrete IBI schemes which include GQ-IBI [11], Sh-IBI [16] (under the RSA assumption) and Hs-IBI [12], ChCh-IBI [8] (under the CDH assumption)[1].

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

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

1. **Gen:** *On input 1^k, where $k \in \mathbb{N}$ is the security parameter,* **Gen** *generates $(\langle \mathbf{R} \rangle, t)$ where $\langle \mathbf{R} \rangle$ denotes the description of relation $\mathbf{R}$ on $W \times \Delta$ and t a trapdoor information.*
2. **Ver:** *For any $k \in \mathbb{N}$, $(\langle \mathbf{R} \rangle, t) \leftarrow \mathbf{Gen}(1^k)$, $\mathbf{Ver}(1^k, \langle \mathbf{R} \rangle, x, y) = 1$ if and only if $(x, y) \in \mathbf{R}$, otherwise, it outputs 0.*
3. **Inv:** *On input $(1^k, \langle \mathbf{R} \rangle, y, t)$, it outputs x such that $(x, y) \in \mathbf{R}$ for any $y \in \Delta$.*
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 new random target point $y \in \Delta$.*
   (b) *An inversion oracle* INV *that on any input y,*
      i. *if y is an output of* RAM*, a witness of 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 target points output by RAM and makes strictly fewer queries to INV. We say that $(\langle \mathbf{R} \rangle, t)$ is a trapdoor weak-one-more relation if the probability to win the game is negligible in k for any PPT $\mathcal{A}$.

The trapdoor weak-one-more relation family can be instantiated easily and in many different ways. In the following, we describe several methods and show that they satisfy the definition of trapdoor weak-one-more relation family.

3.1 Instantiations of Trapdoor Weak-One-More Relations

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 trapdoor weak-one-more relation from any trapdoor one-way permutation.

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

Theorem 1. *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. Now we show that it also satisfies the weak-one-more resistance. 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 $\mathcal{B}$ is to find the inverse $x^* \in \Delta$ such that $f(x^*) = y^*$. Suppose $\mathcal{A}$ makes at most $Q(k)$ queries to RAM. Initially, $\mathcal{B}$ randomly selects a number $1 \leq i \leq Q(k)$ 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 at least ϵ, $\mathcal{B}$ breaks the one-wayness of f with probability at least $\epsilon/Q(k)$. □

Computational Diffie-Hellman (CDH) Assumption Based. To be more concrete, and also make our weak-one-more relation family more explicitly linked to the techniques of some actual IBI schemes (e.g. Hs-IBI [12] and ChCh-IBI [8]), we describe another instantiation of the weak-one-more relation defined above in Def. 3.

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: *bilinear*: For any $U, V \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}_q$, $e(aU, bV) = e(U, V)^{ab}$; *non-degenerate*: $e(P, P) \neq 1$; and *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, we can construct a trapdoor weak-one-more relation as follows: on input 1^k, **Gen** outputs $(\mathbb{G}_1, \mathbb{G}_2, q, P, e, \hat{S} = sP)$ where s is randomly selected from $\mathbb{Z}_q$, the relation is defined as $\mathbf{R}^{CDH} = \{(x, y) : x, y \in \mathbb{G}_1; e(P, x) = e(\hat{S}, y)\}$ and s is the trapdoor information.

Theorem 2. *If the CDH problem is hard,* $\mathbf{R}^{CDH}$ *is a trapdoor weak-one-more relation.*

The proof is similar to that for Theorem 1 and is omitted here.

Digital Signature Schemes Secure under Known Message Attacks. Besides trapdoor one-way permutation based and some concrete CDH assumption based instantiations, we now show that the trapdoor weak-one-more relation can also be constructed from a signature scheme which is only existentially unforgeable against known message attack (euf-kma) in the sense of [10]. This also demonstrates that the trapdoor weak-one-more relation defined above can be

very useful for capturing some potentially new concrete construction methods of IBI schemes. This is also a new application for signature schemes which are proven secure under the weak notion of existential unforgeability, namely, against only known message attacks.

Let $\mathcal{SIG} = (\mathcal{KG}, \mathcal{S}, \mathcal{V})$ be a signature scheme defined on some message space $\mathcal{MS}$. Here, we assume that $|\mathcal{MS}| \geq 2^{\ell(k)}$ where $\ell(k)$ is super logarithmic in k. The security of euf-kma [10] is defined as follows: an adversary has signatures for a set (denoted by $\mathcal{M}_{known}$) of messages which are uniformly selected from $\mathcal{MS}$, the adversary's goal is to produce a signature for a message in $\mathcal{MS} \setminus \mathcal{M}_{known}$.

We can construct a trapdoor weak-one-more relation from $\mathcal{SIG}$ as follows: on input 1^k, **Gen** runs the key generation algorithm $\mathcal{KG}$ to generate a public/private key pair (pk, sk), the relation is defined as $\mathbf{R}^{SIG} = \{(x, y) : y \in \mathcal{MS}; \mathcal{V}(pk, y, x) = 1\}$ and sk is the trapdoor information.

Theorem 3. *If $\mathcal{SIG}$ is euf-kma, $\mathbf{R}^{SIG}$ is a trapdoor weak-one-more relation.*

Proof. Suppose there exists an adversary $\mathcal{A}$ which breaks the weak-one-more resistance. We build another adversary $\mathcal{F}$ which breaks $\mathcal{SIG}$ under the known message attacks. Suppose $\mathcal{A}$ makes at most $Q(k)$ queries to RAM. Initially, $\mathcal{F}$ obtains $Q(k) - 1$ message-signature pairs $\{(m_1, \sigma_1), \cdots, (m_{Q(k)-1}, \sigma_{Q(k)-1})\}$ where m_j $(1 \leq j \leq Q(k) - 1)$ is uniformly selected from $\mathcal{MS}$. Thus, $\mathcal{M}_{known} = \{m_1, \cdots, m_{Q(k)-1}\}$). $\mathcal{F}$ then uniformly selects m^* from $\mathcal{MS}$, and randomly inserts m^* into the message sequence. For simplicity, we assume any two messages in $\mathcal{M}_{known} \cup \{m^*\}$ are different. The proof then proceeds as in the proof of Theorem 1, $\mathcal{F}$ answers $\mathcal{A}$'s queries to RAM and INV by simply sending back the corresponding message/signature, $\mathcal{F}$ fails if $\mathcal{A}$ makes a query to INV on message m^*.

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

3.2 Our Generic Construction of IBI Schemes

We now start describing our method of constructing an IBI scheme. The method is based on the trapdoor weak-one-more-relation family (Def. 3) and the Honest Verifier Zero-Knowledge (HVZK) proof with special soundness defined as follows.

Definition 4. *A trapdoor weak-one-more relation $\mathbf{R}$ on $W \times \Delta$ has an HVZK proof with special soundness if there exists a non-trivial canonical proof system $(\tilde{\mathbf{P}}, \tilde{\mathbf{V}})$ such that for any $y \in \Delta$,*

1. **Completeness.** *If $\tilde{\mathbf{P}}$ knows x such that $(x, y) \in \mathbf{R}$, then $\Pr(\tilde{\mathbf{V}}$ accepts$) = 1$.*
2. **Special Soundness.** *A witness of y can be computed from any two acceptable transcripts $(\mathrm{Cmt}, \mathrm{Ch}_1, \mathrm{Rsp}_1)$ and $(\mathrm{Cmt}, \mathrm{Ch}_2, \mathrm{Rsp}_2)$ such that $\mathrm{Ch}_1 \neq \mathrm{Ch}_2$.*
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 $\tilde{\mathbf{P}}$(initialized with a witness of y) and $\tilde{\mathbf{V}}$(initialized with $\langle \mathbf{R} \rangle, y$).*

Let $\mathrm{H} : \{0,1\}^* \rightarrow \Delta$ be a hash function that is considered to be a random oracle [4] for security analysis. We construct an IBI scheme as follows.

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

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

Theorem 4. *Let* $\mathbf{R}$ *be a trapdoor weak-one-more relation which has an HVZK interactive proof with special soundness. If the challenge length* $\ell(k)$ *of the HVZK proof is super logarithmic in* k*, the IBI scheme constructed above is* id-imp-pa *secure in the random oracle model.*

Proof. Given an adversary $\mathcal{A}$ that can break the IBI scheme with advantage ϵ, we construct an adversary $\mathcal{B}$ which breaks the weak-one-more resistance of the underlying trapdoor weak-one-more relation with advantage $\epsilon' \geq (\epsilon - 2^{-\ell(k)})^2$.

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

1. H-query: On input $I \in \{0,1\}^*$, $\mathcal{B}$ checks if I is in table T. If I is not in T, $\mathcal{B}$ asks its challenge oracle RAM to get a random point $y \in \Delta$, and sets $\mathrm{H}(I) = y$ by putting (I, y) in table T. If I is already in table T, the existing value 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 is in T, I is added into HU and a symbol '1' is returned. Otherwise, $\mathcal{B}$ asks 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, $\mathcal{B}$ asks INV to generate a witness w for $\mathrm{H}(\mathrm{I})$ and returns w to $\mathcal{A}$. I is then deleted from HU and added into CU.
4. CONV(I): If $I \notin \mathrm{HU}$, $\perp$ is returned. Otherwise, $\mathcal{B}$ runs the simulation algorithm $\mathcal{SIM}$ in Def. 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. $\mathrm{H}(\mathrm{I_b})$ is returned by RAM, but the witness of $\mathrm{H}(\mathrm{I_b})$ is still not known to $\mathcal{B}$) with probability ϵ, by the Reset Lemma (Appendix A) and the special soundness, $\mathcal{B}$ can extract a witness of $\mathrm{H}(\mathrm{I_b})$ with probability at least $(\epsilon - 2^{-\ell(k)})^2$. Thus $\mathcal{B}$ breaks the weak-one-more resistance of $\mathbf{R}$ with a non-negligible probability. □

By applying the generic construction above, we can derive the id-imp-pa securiy of GQ-IBI [11], Sh-IBI [16] under the RSA assumption, and Hs-IBI [12], ChCh-IBI [8] under the CDH assumption.

4 Transforming to a Generic IBI Scheme Secure Against Active and Concurrent Attacks

To construct an IBI scheme secure against active and concurrent attacks (namely, id-imp-aa secure and id-imp-ca secure), we do not need to do so from scratch. Interestingly, as described in this section, we only need to replace the trapdoor weak-one-more relation of our generic construction described in Sec. 3 with a *trapdoor strong-one-more relation* and the HVZK proof with a *witness indistinguishable* proof, for transforming our generic construction secure against passive attacks (i.e. id-imp-pa) to a generic IBI scheme secure against active and concurrent attacks.

4.1 Trapdoor Strong-One-More Relations

Definition 5 (Trapdoor Strong-One-More Relation). *A family of trapdoor strong-one-more relations $\mathcal{R}$ is a triple of PPT algorithms* $(\mathbf{Gen}', \mathbf{Ver}', \mathbf{Inv}')$ *such that the following properties hold:*

1. **$\mathbf{Gen}'$:** *On input 1^k, where $k \in \mathbb{N}$ is the security parameter, the probabilistic polynomial-time algorithm* $\mathbf{Gen}'$ *outputs $(\langle \mathbf{R} \rangle, t)$ where $\langle \mathbf{R} \rangle$ denotes the description of a binary relation $\mathbf{R}$ on $W \times \Delta$ and t is the trapdoor information of $\mathbf{R}$.*
2. **$\mathbf{Ver}'$:** *For every $k \in \mathbb{N}$, $(\langle \mathbf{R} \rangle, t) \leftarrow \mathbf{Gen}'(1^k)$, $\mathbf{Ver}'(1^k, \langle \mathbf{R} \rangle, x, y) = 1$ if and only if $(x, y) \in \mathbf{R}$.*
3. **$\mathbf{Inv}'$:** *It is a (probabilistic or deterministic) polynomial-time algorithm such that on input $(1^k, \langle \mathbf{R} \rangle, y, t)$, it outputs an x such that $(x, y) \in \mathbf{R}$ for any $y \in \Delta$.*
4. ***Non triviality:*** *$|\Delta|$ is greater than $p(k)$ where $p(\cdot)$ is any positive polynomial.*
5. ***Strong-one-more resistance:*** *It is defined by a game. The adversary $\mathcal{A}$ is given $1^k, \langle \mathbf{R} \rangle$ as input where $(\langle \mathbf{R} \rangle, t) \leftarrow \mathbf{Gen}'(1^k)$ and access to two oracles:*
   (a) *A challenge oracle* RAM *that on any input returns a new random target point $y \in \Delta$.*
   (b) *An inversion oracle* INV *that on any input y:*
      i. *If y is from the output of* RAM, INV *returns a witness of y, and the same witness is returned if y is queried again later.*
      ii. *If y is not from the output of* RAM, *a symbol $\perp$ is returned indicating that the input is invalid.*

   The adversary wins if he can find a pair $(x', y') \in \mathbf{R}$ such that y' is one output of RAM *but (x', y') does not appear in the input/output pairs of the inversion oracle (i.e. the adversary can find one more distinct pair than the pairs given by the inversion oracle)*[2]*. A relation is a trapdoor strong-one-more relation if the probability to win the game is negligible in k for any polynomial-time adversary.*

[2] There are two cases: in the first case, y' has never been queried to the inversion oracle; in the second case, the inversion oracle has returned a witness x of y' before, but $x' \neq x$.

In the following, we describe some primitives that can be used to construct trapdoor strong-one-more relations.

Factoring Assumption Based. A Blum-Williams generator is a modulus generator that returns Blum-Williams (BW) moduli N [18,5], meaning that $N = pq$ with $p \equiv q \equiv 3 \bmod 4$. 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. We also know 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.

We construct a trapdoor strong-one-more relation as follows: on input 1^k, $\mathbf{Gen}'$ runs the Blum-Williams generator to generate (N, p, q). (p, q) is the trapdoor for relation $\mathbf{R}^{SQ} = \{(X, Y) \in \mathbb{Z}_N^* \times \mathbb{Z}_N^*[+1] : X > (N-1)/2; Y \equiv \pm X^2 \bmod N\}$. On input $Y \in \mathbb{Z}_N^*[+1]$, $\mathbf{Inv}'$ uniformly chooses an $X \in \mathbb{Z}_N^*$ over the two square roots (greater than $(N-1)/2$) of $\pm Y$ (remember either Y or $-Y$ is a square).

Theorem 5. *Assume the factoring problem is hard, $\mathbf{R}^{SQ}$ is a trapdoor strong-one-more relation.*

Proof. The proof is by contradiction. Assume there exists an adversary $\mathcal{A}$ which can break the strong-one-more resistance, then we can build an adversary $\mathcal{B}$ to factor N. Here is the simulation.

When $\mathcal{A}$ asks a challenge query, $\mathcal{B}$ uniformly selects an $x \in \mathbb{Z}_N^*$ at random such that $x > (N-1)/2$, and returns $y \xleftarrow{R} \pm x^2 \bmod N$ to $\mathcal{A}$. When $\mathcal{A}$ asks the inversion query on y, $\mathcal{B}$ returns x to $\mathcal{A}$. If $\mathcal{A}$ aborts, $\mathcal{B}$ also aborts.

Suppose $\mathcal{A}$ wins the strong-one-more resistance game, then one of the following two events must occur[3]. $\mathbf{E}_1 : \mathcal{A}$ outputs a witness x' for a challenge y that has appeared in an inversion query. Denote the witness selected by $\mathcal{B}$ in the challenge query by x, then $x' \neq \pm x$, and $\mathcal{B}$ is able to factor N. $\mathbf{E}_2 : \mathcal{A}$ outputs a witness x' for a challenge y that has not appeared in an inversion query. Denote the witness selected by $\mathcal{B}$ in the challenge query by x, if $x' = x$, $\mathcal{B}$ aborts with failure. Otherwise, $x' \neq \pm x$, and $\mathcal{B}$ is able to factor N. Since x is uniformly selected at random, $\Pr[x' \neq \pm x] = 1/2$.

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

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

$$\mathbf{Adv}_A^{rsa}(k) = \Pr[(N, e, d) \xleftarrow{R} K_{rsa}(1^k); y \xleftarrow{R} Z_N^*; x \leftarrow A(1^k, N, e, y) : x^e \equiv y \bmod N]$$

is negligible in k for all polynomial-time algorithm A.

[3] There is a chance that y and -y are returned in two challenge queries, but this only happens with a negligible probability.

We construct a trapdoor strong-one-more relation as follows: on input 1^k, **Gen′** first runs the prime-exponent RSA key generator to generate (N, e, d) such that $e > 2^{\ell(k)}$ where $\ell(k)$ is super-logarithmic in k, and then randomly picks $g \stackrel{R}{\leftarrow} \mathbb{Z}_N^*$. (N, d) is the trapdoor for relation $\mathbf{R}^{RSA} = \{((x_1, x_2), Y) \in (\mathbb{Z}_e \times \mathbb{Z}_N^*) \times \mathbb{Z}_N^* : g^{-x_1} x_2^{-e} \equiv Y \bmod N$. On input $Y \in \mathbb{Z}_N^*$, **Inv′** randomly chooses $x_1 \stackrel{R}{\leftarrow} \mathbb{Z}_e$, and then calculates $x_2 = (g^{x_1} Y)^{-d} \bmod N$.

Theorem 6. *Assume the RSA problem is hard, $\mathbf{R}^{RSA}$ is a trapdoor strong-one-more relation.*

Proof (Sketch). Assume there exists an adversary $\mathcal{A}$ which can break the strong-one-more resistance with probability ϵ, then we can build another adversary $\mathcal{B}$ which solves the RSA problem with probability at least $(1 - 1/e)\epsilon$.

Given the RSA challenge y, adversary $\mathcal{B}$ sets $g = y$ and simulates the strong-one-more resistance game as follows:

When $\mathcal{A}$ asks a challenge query, $\mathcal{B}$ randomly selects $x_1 \stackrel{R}{\leftarrow} \mathbb{Z}_e, x_2 \stackrel{R}{\leftarrow} \mathbb{Z}_N^*$, and returns $Y = g^{-x_1} x_2^{-e} \bmod N$ to $\mathcal{A}$. When $\mathcal{A}$ asks the inversion query on Y, $\mathcal{B}$ returns (x_1, x_2) to $\mathcal{A}$. If $\mathcal{A}$ aborts, $\mathcal{B}$ also aborts.

If $\mathcal{B}$ can obtain two different witnesses (x_1, x_2) and $(\hat{x}_1, \hat{x}_2)$ for the same challenge Y, since e is prime and $0 < |x_1 - \hat{x}_1| < e$, two integers a, b can be found such that $a(x_1 - \hat{x}_1) + be = 1$, then $\mathcal{B}$ outputs $g^b (x_2 \hat{x}_2^{-1})^a \bmod N$. By analyzing the probability of two similar events $\mathbf{E}_1$ and $\mathbf{E}_2$ in the proof of Theorem 5, we can see that $\mathcal{B}$ breaks the RSA problem with probability at least $(1 - 1/e)\epsilon$. □

Strongly Unforgeable Signature Based. Let $\mathcal{SIG}$ be defined as in Sec. 3.1, $\mathcal{SIG}$ is strongly unforgeable [1] under known message attack [10] (seuf-kma) if no polynomial-time adversary is feasible to produce a message-signature pair (m, σ) such that (m, σ) is not in his known list of message-signature pairs.

By using the same construction as in Sec. 3.1, we can get the following theorem.

Theorem 7. *If $\mathcal{SIG}$ is strong unforgeable under known message attack, and for any message $m \in \mathcal{MS}$[4] there are more than one valid signatures, $\mathbf{R}^{SIG}$ is a trapdoor strong-one-more relation.*

Proof (Sketch). Assume there exists an adversary $\mathcal{A}$ which can break the strong-one-more resistance, we build a forger $\mathcal{F}$ as follows.

Suppose $\mathcal{A}$ asks at most $Q(k)$ challenge queries. $\mathcal{F}$ first gets $Q(k)$ message-signature pairs (the messages are not chosen by him). Then $\mathcal{F}$ answers $\mathcal{A}$'s challenge/inversion queries by simply sending back the corresponding message/signature.

By analyzing the probability of two similar events $\mathbf{E}_1$ and $\mathbf{E}_2$ in the proof of Theorem 5, we can see that $\mathcal{F}$ has a non-negligible probability to win the strong unforgeability game. □

[4] Again, we assume $|\mathcal{MS}| \geq 2^{\ell(k)}$ where $\ell(k)$ is super logarithmic in k.

4.2 Transformation to a Generic IBI Scheme Secure Against Active and Concurrent Attacks

With reference to the generic construction of IBI schemes with id-imp-pa security described in Sec. 3.2, we use it to construct a generic IBI scheme with id-imp-aa security and id-imp-ca security, by replacing the original $\mathbf{R}$ with a trapdoor strong-one-more relation (Def. 5) and $(\tilde{\mathbf{P}}, \tilde{\mathbf{V}})$ with a non-trivial interactive proof with *witness dualism* defined below.

Definition 6 (Witness Dualism). *Let* $\mathbf{R}$ *be a trapdoor strong-one-more relation. We say that* $\mathbf{R}$ *has* Witness Dualism *if there exists a non-trivial interactive proof system* (P, V) *with special soundness such that for every* $y \in \Delta$*, and for every* $x \in W(y)$*, there exists at least one* $x' \in W(y)$ *such that* $x' \neq x$ *and for any verifier* V' *and any auxiliary input* z *for* V'*, the ensembles,* $V'_{P(y,x)}(y, z)$ *and* $V'_{P(y,x')}(y, z)$*, generated as* V'*s view of the interactive proof, are indistinguishable.*

The notion of Witness Dualism is related to *Witness Indistinguishability* [9]. For witness dualism, given a witness x of y, the notion only requires it to be indistinguishable with another witness x', rather than with all other witnesses in $W(y)$. Hence it is a weaker notion when compared with witness indistinguishability.

Theorem 8. *Let* $\mathbf{R}$ *be a trapdoor strong-one-more relation which has Witness Dualism, if the challenge length* $\ell(k)$ *of the interactive proof system is super logarithmic in* k*, then the generic IBI scheme in Sec. 3.2 (replace the HVZK proof by (P, V)) is* id-imp-aa *and* id-imp-ca *secure in the random oracle model.*

Proof. Given an adversary $\mathcal{A}$ that can break the IBI scheme, we construct an adversary $\mathcal{B}$ which breaks the strong-one-more resistance of the underlying trapdoor strong-one-more relation.

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

1. H-query: On input $I \in \{0,1\}^*$, $\mathcal{B}$ checks if I is in table T. If I is not in T, $\mathcal{B}$ asks RAM to get a random point $y \in \Delta$, then $\mathcal{B}$ sets $\mathrm{H(I)} = y$ by putting $(I, y, \perp)$ in table T[5]. If I is already in table T, the existing value is returned.
2. INIT(I): If $I \in$ HU$\cup$CU, $\perp$ is returned. Otherwise, $\mathcal{B}$ checks if I is in table T. If I is in table T, I is added into HU and a symbol '1' is returned. Otherwise, $\mathcal{B}$ asks RAM to get a random point $y \in \Delta$, then $\mathcal{B}$ sets $\mathrm{H}(I) = y$ by putting $(I, y, \perp)$ in T, I is then added into HU and a symbol '1' is returned.
3. CORR(I): If $I \notin$ HU, $\perp$ is returned. Otherwise, $\mathcal{B}$ finds the row corresponding to I in table T. If the witness is unknown, $\mathcal{B}$ asks the inversion oracle for a witness x of $\mathrm{H}(I)$, and replaces the $\perp$ symbol in that row by x. $\mathcal{B}$ returns x to $\mathcal{A}$. I is then deleted from HU and added into CU.

[5] The symbol "$\perp$" denotes the value is unknown yet.

4. PROV(I): If $I \notin$ HU, $\perp$ is returned. Otherwise, $\mathcal{B}$ finds the row corresponding to I in table T and retrieves x. If the witness is unknown, $\mathcal{B}$ asks the inversion oracle for a witness x of H(I), and replaces the $\perp$ symbol in that row by x. then $\mathcal{B}$ runs a copy of P with initial state x.

Finally, if $\mathcal{A}$ can successfully impersonate a user $\mathrm{I_b}$ that is created but not corrupted (i.e. $\mathrm{H(I_b)}$ is returned by RAM, but $\mathcal{A}$ does not ask for its witness), by the Reset Lemma (Appendix A) and the special soundness, $\mathcal{B}$ can extract a witness x_b of $\mathrm{H(I_b)}$ with probability at least $(\epsilon - 2^{-\ell(k)})^2$.

If $\mathcal{B}$ has never asked the inversion oracle for a witness of $\mathrm{H(I_b)}$, $\mathcal{B}$ successfully breaks the strong-one-more resistance. Otherwise, because of the Witness Dualism, with probability at least 1/2, the witness extracted (with the help of $\mathcal{A}$) is different from the one in table T (by following the same proof of [9], witness dualism is also preserved under concurrent composition).

Thus $\mathcal{B}$ breaks the strong-one-more resistance of the underlying trapdoor strong-one-more relation with probability at least $1/2(\epsilon - 2^{-\ell(k)})^2$. □

By applying the RSA-based trapdoor strong-one-more relation together with a witness indistinguishable interactive proof with special soundness [15], we can derive the Okamoto-RSA-IBI scheme [15,2] that is imp-ca secure.

In the next section, we construct a concrete IBI scheme that is imp-ca secure from strong unforgeable signature schemes.

5 A Concrete IBI Scheme Secure Against Concurrent Attacks

In this section, we construct an IBI scheme from the Katz-Wang signature scheme [13] which is shown to be strongly unforgeable under the DDH assumption [6] for any message space $\mathcal{MS} \subset \{0,1\}^*$. Let $\mathbb{G}$ be a cyclic group of prime order q with generator g, $H : \{0,1\}^* \to \{0,1\}^k$ and $H' : \{0,1\}^* \to \{0,1\}^k$ be hash functions which are assumed to behave as independent random oracles for security analysis. Let $k \in \mathbb{N}$ be the security parameter and $k < |q|$. We first review the signature scheme due to Katz and Wang.

The Katz-Wang Signature Scheme: To generate a public/secret key pair, $h \in \mathbb{G}$ and $x \leftarrow \mathbb{Z}_q^*$ are first chosen randomly. $y_1 = g^x$ and $y_2 = h^x$ are then computed and the public key is set to $PK = (h, y_1, y_2)$ and the secret key to x. To sign a message m, the following steps are carried out.

1. Choose random $r \leftarrow \mathbb{Z}_q$.
2. Compute $A = g^r$, $B = h^r$, and $c = H'(A, B, m)$.
3. Compute $s = cx + r \bmod q$ and set signature $\sigma = (c, s)$.

To verify the signature, $A = g^s y_1^{-c}$ and $B = h^s y_2^{-c}$ are computed and if $c = H'(A, B, m)$, the signature is valid.

The IBI Scheme: Based on the Katz-Wang signature scheme, we build an IBI scheme with id-imp-ca security. The scheme is described in Fig. 1. Next, we prove

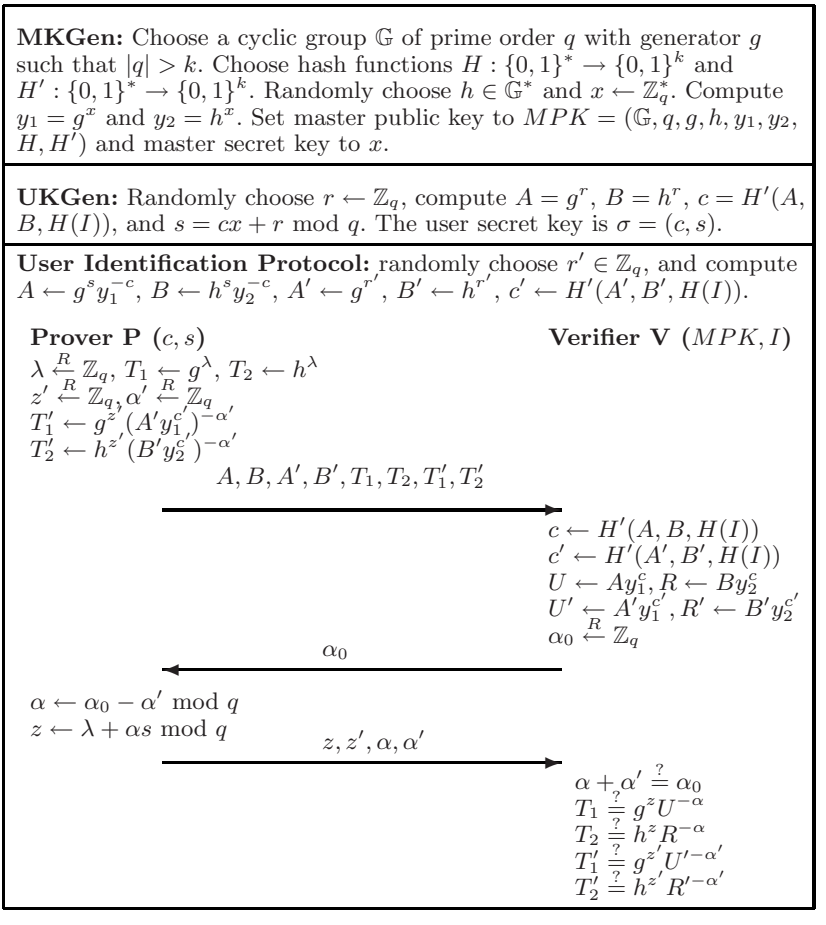

Fig. 1. The IBI scheme based on Katz-Wang signature scheme

its security by following our framework described in the previous section. It can be seen that the user identification protocol in Fig. 1 is actually a proof that the prover knows at least one of two valid signatures.

Lemma 1. *The user identification protocol in Fig. 1 has special soundness.*

Proof. Given two successful conversations where **V** outputs '*accept*':

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

such that $\alpha_0 \neq \hat{\alpha}_0$, it must be the case that at least one of the inequalities $\alpha \neq \hat{\alpha}$ and $\alpha' \neq \hat{\alpha}'$ take place. For example, if $\alpha \neq \hat{\alpha}$, (s, c) can be obtained from $s = (z - \hat{z})(\alpha - \hat{\alpha})^{-1}$ and $c = H'(A, B, H(I))$. Hence we can see that at least one of (s, c) and (s', c') can be extracted. □

Lemma 2. *The user identification protocol in Fig. 1 is witness dualism (Def. 6).*

Proof. For the two valid signatures $\sigma = (c, s)$ (with respect to r) and $\sigma' = (c', s')$ (with respect to r') of the message $H(I)$, the ensembles, $V'_{P(y,\sigma)}(y, z)$ (with illusive witness σ') and $V'_{P(y,\sigma')}(y, z)$ (with illusive witness σ), generated as V's view of the protocol, are identically distributed, where y refers to (MPK, I) and z is any auxiliary input for V'. □

Remark: In this IBI scheme, the user is required to use the same illusive witness (c', s') (with respect to r') in all the conversations, and the 'Dual Witness' of (c, s) is exactly (c', s').

By combining these two lemmas and Theorem 8, we obtain the following theorem.

Theorem 9. *The IBI scheme in Fig. 1 is secure against impersonation under concurrent attacks (id-imp-ca).*

References

1. Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the security of joint signature and encryption. In *EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 83–107. Springer, 2002.
2. Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 268–286. Springer, 2004.
3. Mihir Bellare and Adriana Palacio. GQ and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In *CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 162–177. Springer, 2002.
4. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM Conference on Computer and Communications Security (CCS)*, pages 62–73, 1993.
5. Manuel Blum. Coin flipping by telephone. In *CRYPTO 1981*, pages 11–15, 1981.
6. D. Boneh. The decision Diffie-Hellman problem. In *Proc. of the Third Algorithmic Number Theory Symposium*, pages 48–63. Springer-Verlag, 1998. LNCS 1423.
7. Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *ASIACRYPT*, pages 514–532, 2001.
8. Jae Choon Cha and Jung Hee Cheon. An identity-based signature from gap diffie-hellman groups. In *Public Key Cryptography 2003*, pages 18–30, 2003.
9. Uriel Feige and Adi Shamir. Witness indistinguishable and witness hiding protocols. In *Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing (STOC)*, 1990.
10. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attack. *SIAM J. Computing*, 17(2):281–308, April 1988.
11. Louis C. Guillou and Jean-Jacques Quisquater. A "paradoxical" indentity-based signature scheme resulting from zero-knowledge. In *CRYPTO 1988*, volume 403 of *Lecture Notes in Computer Science*, pages 216–231. Springer, 1990.
12. Florian Hess. Efficient identity based signature schemes based on pairings. In *Selected Areas in Cryptography, SAC 2002*, pages 310–324, 2002.

13. Jonathan Katz and Nan Wang. Efficiency improvements for signature schemes with tight security reductions. In *ACM CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 155–164, 2003.
14. Kaoru Kurosawa and Swee-Huay Heng. From digital signature to id-based identification/signature. In *Public Key Cryptography 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 248–261. Springer, 2004.
15. Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In *CRYPTO 1992*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer, 1993.
16. Adi Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO 1984*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1985.
17. Jacques Stern, David Pointcheval, John Malone-Lee, and Nigel P. Smart. Flaws in applying proof methodologies to signature schemes. In *CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 93–110. Springer, 2002.
18. Hugh C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Trans. Inf. Theory*, 26(6), 1980.

A Reset Lemma

Lemma 3 (Reset Lemma [3]). *Let CP be a prover in a canonical IBI scheme with challenge set* ChSet *and challenge length* $\ell(\cdot)$*. 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, and $res(St_{CP}, St_V)$ the probability that the following reset experiment returns 1:*

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

Then,

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