Security Proofs for Identity-Based Identification and Signature Schemes

Mihir Bellare[1], Chanathip Namprempre[2], and Gregory Neven[3]

[1] Department of Computer Science & Engineering, University of California, San Diego,
9500 Gilman Drive, La Jolla, CA 92093, USA
mihir@cs.ucsd.edu
http://www-cse.ucsd.edu/users/mihir
[2] Electrical Engineering Department, Thammasat University,
Klong Luang, Patumtani 12121, Thailand
cnamprem@engr.tu.ac.th
http://www.engr.tu.ac.th/~nchanath
[3] Department of Computer Science, Katholieke Universiteit Leuven,
Celestijnenlaan 200A, 3001 Heverlee-Leuven, Belgium
Gregory.Neven@cs.kuleuven.ac.be
http://www.cs.kuleuven.ac.be/~gregory/

Abstract. This paper provides either security proofs or attacks for a large number of identity-based identification and signature schemes defined either explicitly or implicitly in existing literature. Underlying these are a framework that on the one hand helps explain how these schemes are derived, and on the other hand enables modular security analyses, thereby helping to understand, simplify and unify previous work.

1 Introduction

CURRENT STATE OF THE AREA. The late eighties and early nineties saw the proposal of many identity-based identification (IBI) and identity-based signature (IBS) schemes. These include the Fiat-Shamir IBI and IBS schemes [11], the Guillou-Quisquater IBI and IBS schemes [16], the IBS scheme in Shamir's paper [29] introducing identity-based cryptography, and others [21, 13, 6]. Now, new, pairing-based IBS schemes are being proposed [26, 17, 23, 8, 32].

Prompted by the renewed interest in identity-based cryptography that has followed identity-based encryption (IBE) [7], we decided to revisit the IBI and IBS areas. An examination of past work revealed the following.

Although there is a lot of work on proving security in the identification domain, it pertains to standard rather than identity-based schemes. (For example, security proofs have been provided for standard identification schemes related to the Fiat-Shamir and Guillou-Quisquater IBI schemes [10, 4], but not for the IBI schemes themselves.) In fact, a provable-security treatment of IBI schemes is entirely lacking: there are no security definitions, and none of the existing schemes is proven secure. Given the practical importance and usage of IBI schemes, this is an important (and somewhat surprising) gap.

C. Cachin and J. Camenisch (Eds.): EUROCRYPT 2004, LNCS 3027, pp. 268–286, 2004.

The situation for IBS is somewhat better. Cha and Cheon provide a definition of security for IBS schemes and prove their scheme secure [8]. Dodis, Katz, Xu, and Yung [9] define a class of standard signature (SS) schemes that they call trapdoor, and then present a random-oracle-using transform (let us call it tSS-2-IBS) that turns any secure trapdoor SS (tSS) scheme into a secure IBS scheme. Security proofs for several existing IBS schemes, including those of [11, 16], are obtained by observing that these are the result of applying tSS-2-IBS to underlying tSS schemes already proven secure in the literature [24, 20, 1]. However, as we will see, there are several IBS schemes not yet proven secure (one example is Shamir's IBS scheme [29]), either because they are not the result of applying tSS-2-IBS to a tSS scheme, or because, although they are, the tSS scheme in question has not yet been analyzed.

The goal of this paper is to fill the above-mentioned gaps in the IBI and IBS areas.

PRELIMINARIES. The first step, naturally, is definitions. We extend to the IBI setting the three notions of security for standard identification (SI) schemes, namely security against impersonation under passive attacks (imp-pa), active attacks (imp-aa) [10], and concurrent attacks (imp-ca) [4]. Our model allows the adversary to expose user (prover) keys, and to mount either passive, active, or concurrent attacks on the provers, winning if it succeeds in impersonating a prover of its choice. We remark that although existing security definitions for other identity-based primitives [7, 8, 9] give us some guidance as to what adversary capabilities to consider, there are some issues in the definition for IBI that need thought, mainly related to what capabilities the adversary gets in what stage of its two-stage attack. See Section 2.

The security notion for SS schemes is the standard unforgeability under chosen-message attack (uf-cma) [15]. An appropriate extension of it for IBS schemes exists [8, 9] and we refer to it also as uf-cma. These definitions are recalled in the full version of the paper [2].

CERTIFICATION-BASED IBI AND IBS. Before executing the main task of analyzing practical IBI and IBS schemes, we pause to consider the following natural design of an IBI scheme, based on any given SI scheme, via the certification paradigm. The authority picks a public and secret key pair (pk, sk) for a SI scheme, and provides these to prover I along with a certificate $cert$ consisting of the authority's signature on I, pk. The prover can now flow $pk, cert$ to the verifier and then identify itself via the SI scheme under pk. The verifier needs to know only I and the public key of the authority in order to authenticate the prover.

In [2], we prove that the above yields a secure IBI scheme. An analogous result holds in the IBS case. We believe that this is worth noting because it highlights the fact that, unlike IBE [7], IBI and IBS are trivial to achieve (and in particular do not require random-oracles), and enables us to better understand what the practical schemes are trying to do, namely to beat the trivial certification-based schemes in performance.

MAIN CONTRIBUTIONS AND APPROACH. This paper delivers security proofs for a large number of practical IBI and IBS schemes, including not only the ones mentioned above, but many more that we surface as having been, with hindsight, implicit in the literature.

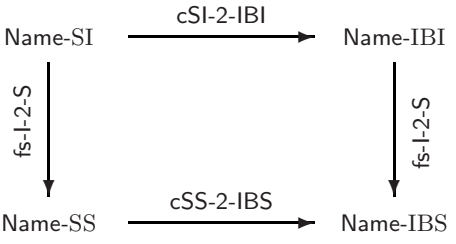

Fig. 1. Family of schemes associated to a cSI scheme Name-SI. If Name-SI is imp-atk secure then Name-IBI is also imp-atk secure, for all $\mathrm{atk} \in \{\mathrm{pa}, \mathrm{aa}, \mathrm{ca}\}$. If Name-SI is imp-pa secure then Name-IBS is uf-cma secure. Implicit in drawing the diagram this way is that fs-I-2-S(cSI-2-IBI(Name-SI)) = cSS-2-IBS(fs-I-2-S(Name-SI)).

We do this in two steps. In the first step, we provide a framework that (in most cases) reduces proving security of IBI or IBS schemes to proving security of an underlying SI scheme. In a few cases, we found that the SI schemes in question were already analyzed in the literature, but in many cases they were not. The second step, where lies the main technical work of the paper, is to provide security proofs for those SI schemes not already proven secure, and then provide direct security proofs for the few exceptional IBI or IBS schemes that escape being captured by our framework.

The framework, we believe, is of value beyond its ability to reduce proving security of IBI and IBS schemes to proving security of SI schemes. It helps understand how schemes are being derived, and in the process surfaces the implicit schemes we mentioned above. Overall, the framework contributes to simplifying and unifying our picture of the area. We now explain the framework, which is based on a set of transforms, and then summarize the results for specific schemes.

THE TRANSFORMS. We introduce (cf. Definition 2) a class of SI schemes that we call convertible. The idea is that their key-generation process be underlain by a primitive called a trapdoor samplable relation that we introduce in Definition 1. We then present a random-oracle-using transform cSI-2-IBI that transforms a convertible SI (cSI) scheme into an IBI scheme (cf. Construction 1). Theorem 1 shows that cSI-2-IBI is security-preserving, meaning that if the starting cSI scheme is imp-atk secure then so is the resulting IBI scheme (in the random oracle model), for each $\mathrm{atk} \in \{\mathrm{pa}, \mathrm{aa}, \mathrm{ca}\}$. This will be our main tool for proving security of IBI schemes.

It is useful to analogously define convertible standard signature (cSS) schemes and a transform cSS-2-IBS that turns a uf-cma secure cSS scheme into a uf-cma secure IBS scheme. These extend [9] in the sense that any tSS scheme is also a cSS scheme, and cSS-2-IBS coincides with tSS-2-IBS when the starting scheme is a tSS scheme, but the class of cSS schemes is larger than the class of tSS schemes.

Now let fs-I-2-S denote the (random-oracle using) Fiat-Shamir transform [11] which turns a SI scheme into a SS scheme. We know that if the former is imp-pa secure then the latter is uf-cma secure [1]. (Application of the transform and this last result requires

that the starting SI scheme be a three-move public-coin protocol satisfying a certain technical condition, but all this will always be true for the applications we consider.)

Putting the above together yields Corollary 1, which says that, as long as a cSI scheme X is imp-pa secure, the IBS scheme cSS-2-IBS(fs-I-2-S(X)) is uf-cma secure. This will be our main tool for proving security of IBS schemes.

We note that fs-I-2-S also transforms a given IBI scheme into an IBS scheme. Furthermore, cSS-2-IBS(fs-I-2-S(X)) = fs-I-2-S(cSI-2-IBI(X)) for any cSI scheme X. In other words, the diagram of Figure 1 "commutes."

As an aside, we remark that the analogue of the result of [1] does *not* hold for fs-I-2-S as a transform of IBI schemes to IBS schemes: Proposition 1 shows that there exists an imp-pa secure IBI scheme Y which under fs-I-2-S yields an insecure IBS scheme. This does not contradict the above since this Y is not the result of cSI-2-IBI applied to a cSI scheme, but it makes things more difficult in a few exception cases (that we will see later) in which we need to consider an IBS scheme Z = fs-I-2-S(Y) where Y is an IBI scheme that is not equal to cSI-2-IBI(X) for any cSI scheme X. See the end of Section 3 for more information.

SCHEME FAMILIES. We seek to explain any IBI scheme Y in the literature by surfacing a cSI scheme X such that cSI-2-IBI(X) = Y. We seek to explain any IBS scheme Z in the literature by surfacing a cSI scheme X such that cSS-2-IBS(fs-I-2-S(X)) = Z. We are able to do this for the schemes in [11, 16, 29, 13, 17, 8, 32, 6] and for the RSA-based IBI scheme in [21], which, by Theorem 1 and Corollary 1, reduces the task of showing that Y, Z are secure to showing that X is secure in these cases.

We remark that the above gives rise to numerous schemes that are "new" in the sense that they were not provided explicitly in the literature. For example, Shamir [29] defined an IBS scheme but no IBI scheme. (He even says providing an IBI scheme is an open question.) Denoting Shamir's IBS scheme by Sh-IBS, we surface the cSI scheme Sh-SI such that cSS-2-IBS(fs-I-2-S(Sh-SI)) = fs-I-2-S(cSI-2-IBI(Sh-SI)) = Sh-IBS. As a consequence, we surface the IBI scheme Sh-IBI = cSI-2-IBI(Sh-SI) that is related in a natural way to Sh-IBS, namely by the fact that fs-I-2-S(Sh-IBI) = Sh-IBS. In an analogous way we surface IBI schemes Hs-IBI and ChCh-IBI underlying the IBS schemes of [17] and [8, 32], respectively.

Beside explaining existing IBI or IBS schemes, we are able to derive some new ones. We found papers in the literature [19, 22, 12] not defining IBI or IBS schemes, but defining SI schemes that we can show are convertible. Our transforms then yield new IBI and IBS schemes that we analyze.

We feel that this systematic surfacing of implicit schemes helps to homogenize, unify, and simplify the area. Figure 1 summarizes the perspective that emerges. We view schemes as occurring in families. Each family has a family name Name. At the core of the family is a cSI scheme Name-SI. The other schemes are related to it via Name-IBI = cSI-2-IBI(Name-SI), Name-SS = fs-I-2-S(Name-SI), and Name-IBS = cSS-2-IBS(Name-SS). If Name-SI is secure, so are all other schemes in the family.

RESULTS FOR SPECIFIC SCHEMES. In order to complete the task of obtaining security proofs for the existing and new IBI and IBS schemes we have discussed, it remains to analyze the cSI schemes underlying the families in question. This turns out to be a large task, for although in a few cases the cSI scheme is one already analyzed in the

Name	Origin	Name-SI			Name-IBI			Name-SS	Name-IBS
		imp-pa	imp-aa	imp-ca	imp-pa	imp-aa	imp-ca	uf-cma	uf-cma
FS	IBI,IBS [11, 10]	[11]	[10]	**I**	**I**	**I**	**I**	[24]	[9]
ItR	SI, SS [19, 22]	[28]	[28]	**U**	**I**	**I**	**U**	[24]	[9]
FF	SI,SS [12]	[12]	[12]	[12]	**I**	**I**	**I**	[12]	[9]
GQ	IBI, IBS [16]	[16]	[4]	[4]	**I**	**I**	**I**	[24]	[9]
Sh	IBS [29]	**P**	**A**	**A**	**I**	**A**	**A**	**I**	**I**
Sh*	SI	**P**	**P**	**P**	**I**	**I**	**I**	**I**	**I**
OkRSA	SI, IBI, SS [21]	[21]	[21]	**I**	**I**	**I**	**I**	[24]	[9]
Gir	SI, IBI [13, 25]	**A**	**A**	**A**	**A**	**A**	**A**	**A**	**A**
SOK	IBS [26]	**P**	**A**	**A**	**I**	**A**	**A**	**I**	**I**
Hs	IBS [17]	**P**	**P**	**P**	**I**	**I**	**I**	[17]	[9]
ChCh	IBS [8, 32]	**P**	**P**	**P**	**I**	**I**	**I**	[8]	[8]
Beth	IBI [6]	**P**	**U**	**U**	**I**	**U**	**U**	**I**	**I**
OkDL	IBI [21]	**I**	**I**	**I**	**P**	**P**	**P**	**I**	**I**
BNN	SI,IBI	**I**	**I**	**I**	**P**	**P**	**P**	**I**	**I**

Fig. 2. Summary of security results. Column 1 is the family name of a family of schemes. Column 2 indicates which of the four member-schemes of the family existed in the literature. (The others we surface.) In the security columns, a known result is indicated via a reference to the paper establishing it. The marks **I**, **P**, and **A** all indicate new results obtained in this paper. An **I** indicates a proof of security obtained by implication. (If under Name-IBI it means we obtain it via Theorem 1, if under Name-IBS it means we obtain it either via Corollary 1 or via our modified fs-I-2-S transform, if elsewhere it means it follows easily from, or is an easy extension of, existing work.) A **P** indicates a new security proof, such as a from-scratch analysis of some SI or IBI scheme. An **A** indicates an attack that we have found. A **U** indicates that the security status is unknown. In all but the last two rows, the SI scheme is convertible. The first set of schemes are factoring based, the next RSA based, the next pairing based, and the last DL based. For each of the schemes above except for the last two, Name-IBS is obtained through the fs-I-2-S transform. OkDL-IBS and BNN-IBS are obtained through a modified version of the fs-I-2-S transform.

literature, we found (perhaps surprisingly) that in many cases it is not. Additionally, we need to directly analyze two IBI schemes not underlain by cSI schemes, namely the DL-based scheme in [21], and a somewhat more efficient Schnorr-based [27] variant that we introduce.

A summary of our results is in Figure 2. Section 4 and the full version of the paper [2] provide scheme descriptions and more precise result statements. Note all security proofs for SS, IBI, and IBS schemes are in the random-oracle (RO) model of [5]. Proofs are in [2]. Here, we highlight some of the important elements of these results.

CASES CAPTURED BY OUR FRAMEWORK. Section 4 begins by surfacing SI schemes underlying the first 12 (i.e. all but the last two) families of Figure 2 and shows that they

are convertible, so that the picture of Figure 1 holds in all these cases and we need only consider security of the cSI schemes. The analysis of these schemes follows.

Easy cases are FS, ItR (the iterated-root, also called 2^t-th root, family), FF, GQ, and OkRSA (an RSA-based family from [21]) where the SI schemes are already present and analyzed in the literature [10, 28, 12, 4, 21].

The Sh-SI scheme turns out to be a mirror-image of GQ-SI, and is interesting technically because we show that it is honest-verifier zero-knowledge (HVZK) even though it might not at first appear to be so. Based on this, we prove that it is imp-pa (cf. Theorem 3), but simple attacks show that imp-aa and imp-ca do not hold. A slight modification Sh*-SI of this scheme however is not only imp-pa but also proven imp-aa and imp-ca secure under the one-more-RSA assumption of [3] (cf. Theorem 4), so that its security is like that of GQ-SI [4].

An attack and a fix for Girault's IBI scheme [13] were proposed in [25], but we find attacks on the fixed scheme as well, breaking all schemes in the family.

We prove imp-pa security of the pairing-based SOK-SI, Hs-SI and ChCh-SI schemes under a computational DH assumption and imp-aa, imp-ca security under a one-more computational DH assumption (cf. Theorems 5 and 6). We remark that the SOK-IBS scheme defined via our transforms is not the one of [26], but is slightly different. This suggests the value of our framework, for it is unclear whether the IBS scheme of [26] can be proved uf-cma secure, whereas Corollary 1 implies that SOK-IBS is uf-cma secure.

Since the discrete-log function has no known trapdoor it is not an obvious starting point for IBI schemes, but some do exist. Beth's (unproven) IBI scheme [6] is based on ElGamal signatures. The proof of convertibility of the Beth-SI scheme we surface is interesting in that it exploits the existential forgeability of ElGamal signatures. Theorem 7 says that Beth-SI is imp-pa secure if the hashed-message ElGamal signature scheme is universally unforgeable under no-message attack in the random-oracle model.

EXCEPTIONS. The last two rows of Figure 2 represent cases where our framework does not apply and direct analyses are needed. The first such case is an unproven DL-based IBI scheme OkDL-IBI due to Okamoto [21], which introduces an interesting SS-based method for constructing IBI schemes and instantiates it with his own DL-based SS scheme. We were unable to surface any cSI scheme which under cSI-2-IBI maps to OkDL-IBI. (OkDL-IBI can be "dropped" in a natural way to a SI scheme OkDL-SI, but the latter does not appear to be convertible.) However, we show in [2] that OkDL-IBI is nevertheless imp-pa, imp-aa, and imp-ca secure assuming hardness of the DL problem. This direct proof is probably the most technical in the paper and uses the security of Okamoto's DL-based SS scheme under a weakened notion of non-malleability [31], which is established via an extension of the result of [1] combined with results from [21]. We also present a new IBI scheme BNN-IBI that is based on the paradigm underlying OkDL-IBI but uses Schnorr signatures [27] instead of Okamoto signatures. It is slightly more efficient than OkDL-IBI. Security results are analogous to those above. See [2] for descriptions of the schemes and our results.

Proposition 1 precludes proving security of the IBS schemes fs-I-2-S(OkDL-IBI) and fs-I-2-S(BNN-IBI) based merely on the security properties of the IBI schemes. However, we slightly modify the classical fs-I-2-S transform and obtain a transform

that yields a secure uf-cma IBS scheme when applied to an imp-pa IBI scheme. We can then apply this transform to OkDL-IBI or BNN-IBI to obtain uf-cma IBS schemes.

RELATED WORK. Independent of our work, Kurosawa and Heng [18] recently presented a transform from a certain class of "zero-knowledge" SS schemes to IBI schemes. However, the IBI scheme resulting from their transform is only shown to be secure against impersonation under *passive* attacks.

2 Security Notions for Identification Schemes

NOTATION. We let $\mathbb{N} = \{1, 2, 3, \ldots\}$ denote the set of natural numbers. If $k \in \mathbb{N}$, then 1^k is the string of k ones. The empty string is denoted ε. If x, y are strings, then $|x|$ is the length of x and $x\|y$ is the concatenation of x and y. If S is a set, then $|S|$ is its cardinality. If A is a randomized algorithm, then $A(x_1, x_2, \ldots : \mathrm{O}_1, \mathrm{O}_2, \ldots)$ means that A has inputs $x_1, x_2, \ldots$ and access to oracles $\mathrm{O}_1, \mathrm{O}_2, \ldots$, and $y \xleftarrow{\$} A(x_1, x_2, \ldots : \mathrm{O}_1, \mathrm{O}_2, \ldots)$ means that the output of A's run is assigned to y. We denote the set of all possible outputs by $[A(x_1, x_2, \ldots : \mathrm{O}_1, \mathrm{O}_2, \ldots)]$, the running time of A by $\mathbf{T}_A$, and the number of times A queried the O_i oracle by $\mathbf{Q}_A^{\mathrm{O}_i}$. We define $\mathbf{Q}_A = \sum_i \mathbf{Q}_A^{\mathrm{O}_i}$.

An interactive algorithm (modelling a party such as prover or verifier in a protocol) is a stateful algorithm that on input an incoming message M_{in} (this is ε if the party is initiating the protocol) and state information St outputs an outgoing message M_{out} and updated state St'. For an interactive algorithm A that has access to oracles $\mathrm{O}_1, \mathrm{O}_2, \ldots$, this is written as $(M_{out}, \mathrm{St}') \xleftarrow{\$} A(M_{in}, \mathrm{St} : \mathrm{O}_1, \mathrm{O}_2, \ldots)$. The initial state of A contains its inputs and optionally a random tape ρ; if no random tape is explicitly given in the initial state, A is assumed to toss its own coins.

STANDARD IDENTIFICATION SCHEMES. A *standard identification (SI) scheme* is a tuple $\mathcal{SI} = (\mathsf{Kg}, \mathsf{P}, \mathsf{V})$ where Kg is the randomized polynomial-time key generation algorithm, and P and V are polynomial-time interactive algorithms called the prover and verifier algorithms, respectively. In an initialization step, the prover runs $\mathsf{Kg}(1^k)$, where k is a security parameter, to obtain a key pair (pk, sk), and publishes the public key pk while keeping the secret key sk private. In the interactive identification protocol, the prover runs P with initial state sk, and the verifier runs V with initial state pk. The first and last messages of the protocol belong to the prover. The protocol ends when V enters either the acc or rej state. We require that for all $k \in \mathbb{N}$ and for all $(pk, sk) \in [\mathsf{Kg}(1^k)]$, the result of the interaction between P (initialized with sk) and V (initialized with pk) is acc with probability one.

SECURITY OF SI SCHEMES. An adversary A is a pair of algorithms (CV, CP) called the *cheating verifier* and the *cheating prover* [10]. We briefly recall the notions of imp-pa, imp-aa [10], and imp-ca [4]. The experiment first chooses keys (pk, sk) via $\mathsf{Kg}(1^k)$ and then runs CV on pk. For a passive attack (pa), CV gets a conversation oracle, which, upon a query, returns a transcript of the conversation between P (with initial state sk) and V (with initial state pk), each time generated under fresh coins for both parties. For an active attack (aa) or concurrent attack (ca), CV gets a prover oracle PROV. Upon a query (M, s) where M is a message and s is a session number, the PROV oracle runs the prover algorithm using M as an incoming message and returns

the prover's outgoing message while maintaining the prover's state associated with the session s across the invocations. (For each new session, PROV uses fresh random coins to start the prover, initializing it with sk.) The difference between active and concurrent attacks is that the former allows only a single prover to be active at a time. Eventually, CV halts with some output that is given to CP, and A wins if the interaction between CP and V (initialized with pk) leads the latter to accept. For $\mathrm{atk} \in \{\mathrm{pa}, \mathrm{aa}, \mathrm{ca}\}$, the *imp-atk advantage* of A in attacking $\mathcal{SI}$ is written as $\mathbf{Adv}^{\text{imp-atk}}_{\mathcal{SI},A}(k)$ and is defined to be the probability of A winning in the above experiment. We say that $\mathcal{SI}$ is an *imp*-atk-*secure SI scheme* if $\mathbf{Adv}^{\text{imp-atk}}_{\mathcal{SI},A}(\cdot)$ is negligible for every polynomial-time A.

IDENTITY-BASED IDENTIFICATION SCHEMES. An *identity-based identification (IBI) scheme* is a four-tuple $\mathcal{IBI} = (\mathsf{MKg}, \mathsf{UKg}, \overline{\mathsf{P}}, \overline{\mathsf{V}})$ of polynomial-time algorithms. The trusted, key-issuing authority runs the *master-key generation* algorithm MKg on input 1^k, where k is a security parameter, to obtain a master public and secret key pair (mpk, msk). It can then run the *user-key generation* algorithm UKg on msk and the identity $I \in \{0,1\}^*$ of a user to generate for this user a secret key usk which is then assumed to be securely communicated to the user in question. In the interactive identification protocol, the prover with identity I runs interactive algorithm $\overline{\mathsf{P}}$ with initial state usk, and the verifier runs $\overline{\mathsf{V}}$ with initial state mpk, I. The first and last messages of the protocol belong to the prover. The protocol ends when $\overline{\mathsf{V}}$ enters either the acc or rej state. In the random oracle model, $\mathsf{UKg}, \overline{\mathsf{P}}, \overline{\mathsf{V}}$ additionally have oracle access to a function H whose range may depend on mpk. We require that for all $k \in \mathbb{N}$, $I \in \{0,1\}^*$, $(mpk, msk) \in [\mathsf{MKg}(1^k)]$, functions H with appropriate domain and range, and $usk \in [\mathsf{UKg}(msk, I : \mathrm{H})]$, the interaction between P (initialized with usk) and V (initialized with mpk, I) is acc with probability one.

SECURITY OF IBI SCHEMES. The security definition for IBI schemes is similar to that of SI schemes. We highlight only the differences here. An adversary $\overline{A}$ is a pair of a cheating verifier $\overline{CV}$ and a cheating prover $\overline{CP}$. It is given a conversation oracle for passive attacks or a prover oracle for active and concurrent attacks as before except that here it can ask for transcripts or for interactions with respect to identities of its choice. For all three types of attacks, it is additionally given access to an initialization oracle and a corrupt oracle with which it can initialize and corrupt an identity, respectively. The former causes the new identity to receive a newly generated user secret key while the latter exposes the identity's user secret key to $\overline{A}$ then marks the identity as corrupted. As before, $\overline{CV}$ is run first. At its completion, it returns an uncorrupted identity J to be impersonated (along with other state information). Then, $\overline{CP}$ attempts the impersonation for J. Throughout, $\overline{A}$ is not allowed to submit queries involving corrupted identities (other than the original corrupting queries). Additionally, $\overline{CP}$ is not allowed to submit queries involving J. For $\mathrm{atk} \in \{\mathrm{pa}, \mathrm{aa}, \mathrm{ca}\}$, the *imp-atk advantage* of $\overline{A}$ in attacking $\mathcal{IBI}$ is written as $\mathbf{Adv}^{\text{imp-atk}}_{\mathcal{IBI},\overline{A}}(k)$ and is defined to be the probability of $\overline{A}$ winning in the above experiment. We say that $\mathcal{IBI}$ is an *imp*-atk-*secure IBI scheme* if $\mathbf{Adv}^{\text{imp-atk}}_{\mathcal{IBI},\overline{A}}(\cdot)$ is negligible for every polynomial-time $\overline{A}$. Details are in [2].

3 Convertible Schemes and Our Transforms

In analogy with the definition of trapdoor signature schemes [9], we define the concept of *convertible identification schemes* and show how to transform these into IBI schemes. We use a slightly more general concept than the trapdoor one-way permutations used by [9] that we will call *trapdoor samplable relations*. A relation $\mathbf{R}$ is a set of ordered pairs $(x, y) \in \mathrm{Dom}(\mathbf{R}) \times \mathrm{Ran}(\mathbf{R})$. We write the set of images of $x \in \mathrm{Dom}(\mathbf{R})$ as $\mathbf{R}(x) = \{y \mid (x, y) \in \mathbf{R}\}$ and the set of inverses of $y \in \mathrm{Ran}(\mathbf{R})$ as $\mathbf{R}^{-1}(y) = \{x \mid (x, y) \in \mathbf{R}\}$.

Definition 1. *A family of* trapdoor samplable relations F *is a triplet of polynomial-time algorithms* $(\mathsf{TDG}, \mathsf{Sample}, \mathsf{Inv})$ *such that the following properties hold: (1)* Efficient generation: *On input* 1^k*, where* $k \in \mathbb{N}$ *is the security parameter,* TDG *outputs the description* $\langle \mathbf{R} \rangle$ *of a relation* $\mathbf{R}$ *in the family together with its trapdoor information* t*; (2)* Samplability: *The output of the algorithm* Sample *on an input* $\langle \mathbf{R} \rangle$ *is uniformly distributed over* $\mathbf{R}$*; (3)* Inversion: *On input a relation description* $\langle \mathbf{R} \rangle$*, the corresponding trapdoor* t*, and an element* $y \in \mathrm{Ran}(\mathbf{R})$*, the randomized algorithm* Inv *outputs a random element of* $\mathbf{R}^{-1}(y)$*; (4)* Regularity: *Every relation* $\mathbf{R}$ *in the family is regular, meaning that the number of inverses* $|\mathbf{R}^{-1}(y)|$ *is the same for all* $y \in \mathrm{Ran}(\mathbf{R})$. ∎

Note that this definition does not ask that any computational problem relating to the family be hard. (For example, there is no "one-wayness" requirement.) We do not need any such assumption.

Definition 2. *A SI scheme* $\mathcal{SI} = (\mathsf{Kg}, \mathsf{P}, \mathsf{V})$ *is said to be* convertible *if there exists a family of trapdoor samplable relations* $F = (\mathsf{TDG}, \mathsf{Sample}, \mathsf{Inv})$ *such that for all* $k \in \mathbb{N}$ *the output of the following is distributed identically to the output of* $\mathsf{Kg}(1^k)$*:*

$(\langle \mathbf{R} \rangle, t) \xleftarrow{\$} \mathsf{TDG}(1^k)$; $(x, y) \xleftarrow{\$} \mathsf{Sample}(\langle \mathbf{R} \rangle)$;
$pk \leftarrow (\langle \mathbf{R} \rangle, y)$; $sk \leftarrow (\langle \mathbf{R} \rangle, x)$; *Return* (pk, sk) ∎

The following describes the cSI-2-IBI transform of a convertible SI (cSI) scheme into an IBI scheme. The idea is that to each identity I we can associate a value that is derivable from the master public key and I. This value plays the role of a public key for the underlying cSI scheme. This "pseudo-public-key" is $(\langle \mathbf{R} \rangle, \mathrm{H}(I))$, where H is a random oracle.

Construction 1. Let $\mathcal{SI} = (\mathsf{Kg}, \mathsf{P}, \mathsf{V})$ be a cSI scheme, and let $F = (\mathsf{TDG}, \mathsf{Sample}, \mathsf{Inv})$ be the family of trapdoor samplable relations that underlies it as per Definition 2. The cSI-2-IBI transform associates to $\mathcal{SI}$ the random-oracle model IBI scheme $\mathcal{IBI} = (\mathsf{MKg}, \mathsf{UKg}, \overline{\mathsf{P}}, \overline{\mathsf{V}})$ whose components we now describe. The master and user key generation algorithms are defined as

Algorithm $\mathsf{MKg}(1^k)$	Algorithm $\mathsf{UKg}(msk, I : \mathrm{H})$
$(\langle \mathbf{R} \rangle, t) \xleftarrow{\$} \mathsf{TDG}(1^k)$	Parse msk as $(\langle \mathbf{R} \rangle, t)$
$mpk \leftarrow \langle \mathbf{R} \rangle$; $msk \leftarrow (\langle \mathbf{R} \rangle, t)$	$x \xleftarrow{\$} \mathsf{Inv}(\langle \mathbf{R} \rangle, t, \mathrm{H}(I))$; $usk \leftarrow (\langle \mathbf{R} \rangle, x)$
Return (mpk, msk)	Return usk

where $\mathrm{H} : \{0,1\}^* \to \mathrm{Ran}(\mathbf{R})$ is a random oracle. The prover algorithm $\overline{\mathsf{P}}$ is identical to P. The verifier algorithm $\overline{\mathsf{V}}(\cdot,\cdot : \mathrm{H})$ parses its initial state as $(\langle \mathbf{R} \rangle, I)$ and runs V on initial state $(\langle \mathbf{R} \rangle, \mathrm{H}(I))$. ∎

The following theorem, proved in [2], says that cSI-2-IBI is security-preserving.

Theorem 1. *Let $\mathcal{SI}$ be a cSI scheme and let $\mathcal{IBI} = \mathsf{cSI\text{-}2\text{-}IBI}(\mathcal{SI})$ be the associated IBI scheme as per Construction 1. For any $atk \in \{pa, aa, ca\}$, if $\mathcal{SI}$ is imp-atk secure then $\mathcal{IBI}$ is imp-atk secure.*

Convertibility of a standard signature (SS) scheme $\mathcal{SS} = (\mathsf{Kg}, \mathsf{Sign}, \mathsf{Vf})$ is defined by analogy to Definition 2. (The condition is only on the key-generation algorithm.) The cSS-2-IBS transform is defined analogously to the cSI-2-IBI transform: given a convertible SS (cSS) scheme $\mathcal{SS} = (\mathsf{Kg}, \mathsf{Sign}, \mathsf{Vf})$, the transform yields an IBS scheme $\mathcal{IBS} = (\mathsf{MKg}, \mathsf{UKg}, \overline{\mathsf{Sign}}, \overline{\mathsf{Vf}})$ where the master and the user key generators are exactly as in Construction 1, and $\overline{\mathsf{Sign}}(usk, \cdot)$ and $\overline{\mathsf{Vf}}(mpk, I, \cdot, \cdot : \mathrm{H})$ are identical to $\mathsf{Sign}(usk, \cdot)$ and $\mathsf{Vf}((mpk, \mathrm{H}(I)), \cdot, \cdot)$, respectively. The proof of the following analogue of Theorem 1 is similar to the proof of Theorem 1 and is thus omitted.

Theorem 2. *Let $\mathcal{SS}$ be a cSS scheme and let $\mathcal{IBS} = \mathsf{cSS\text{-}2\text{-}IBS}(\mathcal{SS})$ be the associated IBS scheme as defined above. If $\mathcal{SS}$ is uf-cma secure then $\mathcal{IBS}$ is also uf-cma secure.*

One can check that any trapdoor SS (tSS) scheme as defined in [9] is a cSS scheme, and their tSS-2-IBS transform coincides with cSS-2-IBS in case the starting cSS scheme is trapdoor. Thus, Theorem 2 represents a (slight) extension of their result. However, the extension is important, for we will see cases of cSS schemes that are not trapdoor and where the extension is needed.

We know that, if $\mathcal{SI}$ is an imp-pa secure SI scheme, then $\mathsf{fs\text{-}I\text{-}2\text{-}S}(\mathcal{SI})$ is a uf-cma secure SS scheme [1]. It is also easy to see that the fs-I-2-S transform of a cSI scheme is a cSS scheme. Combining this with Theorem 2 yields the following, which will be our main tool to prove security of IBS schemes.

Corollary 1. *Let $\mathcal{SI}$ be a cSI scheme, and let $\mathcal{IBS} = \mathsf{cSS\text{-}2\text{-}IBS}(\mathsf{fs\text{-}I\text{-}2\text{-}S}(\mathcal{SI}))$. If $\mathcal{SI}$ is imp-pa secure then $\mathcal{IBS}$ is uf-cma secure.*

Above, it is assumed that $\mathcal{SI}$ is a three-move, public coin protocol (so that one can apply fs-I-2-S to it) and also that the commitment (first move of the prover) is drawn from a space of super-polynomial size (so that the result of [1] applies). An SI or IBI scheme having these properties is called *canonical*.

One can also apply the fs-I-2-S transform to a canonical IBI scheme to obtain an IBS scheme, and one can check that $\mathsf{cSS\text{-}2\text{-}IBS}(\mathsf{fs\text{-}I\text{-}2\text{-}S}(\mathcal{SI})) = \mathsf{fs\text{-}I\text{-}2\text{-}S}(\mathsf{cSI\text{-}2\text{-}IBI}(\mathcal{SI}))$ for any canonical cSI scheme $\mathcal{SI}$. It follows that fs-I-2-S yields a uf-cma secure IBS scheme if it is applied to a *converted* IBI scheme, meaning one that is obtained as the result of applying cSI-2-IBI to some (canonical) cSI scheme. However, one can also apply fs-I-2-S to a canonical IBI scheme that is not converted and get an IBS scheme, and there will be instances later where we would like to do this. Unfortunately, the IBS scheme so obtained need not be secure, in the sense that the analogue of the result of [1] does not hold, as stated below and proved in [2].

Proposition 1. *Assume there exists an imp-pa secure canonical IBI scheme. Then, there exists an imp-pa secure canonical IBI scheme $\mathcal{IBI}$ such that* fs-I-2-S($\mathcal{IBI}$) *is not uf-cma secure.*

We now provide a remedy for the above. We consider a modified version of the fs-I-2-S transform that hashes the identity of the signer (prover) along with the commitment and message, rather than merely hashing the commitment and message as in fs-I-2-S. We can show (by an extension of the proof of [1] that we omit) that, if this transform is applied to a canonical imp-pa secure IBI scheme, then the outcome is a uf-cma secure IBS scheme. We apply this in [2] to obtain uf-cma secure IBS schemes from the two unconverted IBI schemes we consider, namely OkDL-IBI and BNN-IBI.

4 Applying the Framework

We now apply the above transform-based framework to prove security of existing and new IBI and IBS schemes. To do this, we consider numerous SI schemes. (Some are known. Some are new.) We show that they are convertible, and then analyze their security. The implications for corresponding IBI and IBS schemes, obtained via the transforms discussed above, follow from Theorem 1 and Corollary 1. Figure 3 presents the key generation algorithms of the SI schemes we consider, and Figure 4 presents the corresponding identification protocols.

GENERATORS. The key generation algorithms shown in Figure 3 make use of parameter generation algorithms: $\mathcal{K}_{\rm fact}$ for factoring-based schemes, $\mathcal{K}_{\rm rsa}$ for RSA-based schemes, $\mathcal{K}_{\rm dlog}$ for DL-based schemes and $\mathcal{K}_{\rm pair}$ for pairing based schemes. These are randomized polynomial-time algorithms that on input 1^k produce the following outputs: $\mathcal{K}_{\rm fact}$ generates tuples (N, p, q) such that p, q are primes and $N = pq$; $\mathcal{K}_{\rm rsa}$ outputs (N, e, d) such that N is the product of two primes and $ed \equiv 1 \bmod \varphi(N)$; $\mathcal{K}_{\rm dlog}$ outputs the description of a multiplicative group $\mathbb{G}$, its prime order q and a generator g; $\mathcal{K}_{\rm pair}$ generates the description of an additive group $\mathbb{G}_1$ and a multiplicative $\mathbb{G}_2$ of the same prime order q, a generator P of $\mathbb{G}_1$ and a non-degenerate, polynomial-time computable bilinear map $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. We say that $\mathcal{K}_{\rm rsa}$ is a prime-exponent generator if e is always a prime. Security results will make various assumptions about the computational problems underlying these generators.

HASH FUNCTION RANGES. In applying cSI-2-IBI to FS-SI, we assume the hash function in Construction 1 has range the set of quadratic residues modulo N where N is the modulus in the public key. This is a convenient abstraction in the random-oracle model, but note that implementing such a hash function is difficult since the range is not decidable in polynomial-time. However, this is a standard problem in this domain and various standard changes to the scheme take care of it. The same problem arises for several other schemes below as well, and also arises in [9]. We will not mention it again, but instead assume our random-oracle hash functions have whatever ranges we need. Those usually being obvious from the scheme are not discussed explicitly.

FS AND ItR. Since FS-SI is the special case of ItR-SI in which $m = 1$, it suffices to show that the latter is convertible. This is easily seen by considering the relation $\mathbf{R} =$

FS

$(N, p, q) \xleftarrow{\$} \mathcal{K}_{\mathrm{fact}}(1^k)$
For $i = 1 \ldots t$ do
  $x_i \xleftarrow{\$} \mathbb{Z}_N^*$
  $X_i \leftarrow {x_i}^{-2} \bmod N$
$pk \leftarrow (N, (X_1, \ldots, X_t))$
$sk \leftarrow (N, (x_1, \ldots, x_t))$

ItR

$(N, p, q) \xleftarrow{\$} \mathcal{K}_{\mathrm{fact}}(1^k)$
For $i = 1 \ldots t$ do
  $x_i \xleftarrow{\$} \mathbb{Z}_N^*$
  $X_i \leftarrow {x_i}^{-2^m} \bmod N$
$pk \leftarrow (N, (X_1, \ldots, X_t))$
$sk \leftarrow (N, (x_1, \ldots, x_t))$

GQ, Sh, Sh*

$(N, e, d) \xleftarrow{\$} \mathcal{K}_{\mathrm{rsa}}(1^k)$
$x \xleftarrow{\$} \mathbb{Z}_N^*$
$X \leftarrow x^e \bmod N$
$pk \leftarrow ((N, e), X)$
$sk \leftarrow ((N, e), x)$

FF

$(N, p, q) \xleftarrow{\$} \mathcal{K}_{\mathrm{fact}}(1^k)$
Choose $\tau \geq \eta(p, q) - 1$
$g \xleftarrow{\$} \mathrm{HQR}_N$
$x_1 \xleftarrow{\$} \mathbb{Z}_{2^m}$; $x_2 \xleftarrow{\$} \mathbb{Z}_N^*$
$X \leftarrow g^{x_1} x_2^{2^{m+\tau}} \bmod N$
$pk \leftarrow ((N, \tau, g), X)$
$sk \leftarrow ((N, \tau, g), (x_1, x_2))$

Gir

$(N, e, d, f) \xleftarrow{\$} \mathcal{K}_{\mathrm{rsa}}(1^k)$
Choose $g \in \mathbb{Z}_N^*$ of order f
$h \leftarrow g^e \bmod N$; $s \xleftarrow{\$} \mathbb{Z}_f$
$X \xleftarrow{\$} \mathbb{Z}_N^*$
$S \leftarrow g^{-s} \bmod N$
$P \leftarrow X^{-d} S \bmod N$
$pk \leftarrow ((N, e, h, f), X)$
$sk \leftarrow ((N, e, h, f), (P, s))$

OkRSA

$(N, e, d) \xleftarrow{\$} \mathcal{K}_{\mathrm{rsa}}(1^k)$
$g \xleftarrow{\$} \mathbb{Z}_N^*$
$x_1 \xleftarrow{\$} \mathbb{Z}_e$; $x_2 \xleftarrow{\$} \mathbb{Z}_N^*$
$X \leftarrow g^{-x_1} x_2^{-e} \bmod N$
$pk \leftarrow ((N, e, g), X)$
$sk \leftarrow ((N, e, g), (x_1, x_2))$

SOK, Hs, ChCh

$(\mathbb{G}_1, \mathbb{G}_2, q, P, \hat{e}) \leftarrow \mathcal{K}_{\mathrm{pair}}(1^k)$
$s, u \xleftarrow{\$} \mathbb{Z}_q$; $S \leftarrow sP$
$U \leftarrow uP$; $V \leftarrow suP$
$pk \leftarrow ((\mathbb{G}_1, \mathbb{G}_2, q, P, \hat{e}, S), U)$
$sk \leftarrow ((\mathbb{G}_1, \mathbb{G}_2, q, P, \hat{e}, S), V)$

Beth

$(\mathbb{G}, q, g) \xleftarrow{\$} \mathcal{K}_{\mathrm{dlog}}(1^k)$
$r \xleftarrow{\$} \mathbb{Z}_q$; $R \leftarrow g^r$; $x, h \xleftarrow{\$} \mathbb{Z}_q$; $X \leftarrow g^x$
$s \leftarrow (h - Rx) r^{-1} \bmod q$
$pk \leftarrow ((\mathbb{G}, q, g, X), h)$
$sk \leftarrow ((\mathbb{G}, q, g, X), (R, s))$

Fig. 3. Key generation algorithms of the 12 cSI schemes that we consider. Each takes input 1^k and returns (pk, sk). The integers $m, t \geq 1$ where used are scheme parameters. See the text for notation used above.

$\{((x_1, \ldots, x_t), (X_1, \ldots, X_t)) \mid X_i \equiv x_i^{-2^m} \bmod N \text{ for } i = 1, \ldots, t\}$ with description $\langle \mathbf{R} \rangle = N$ and trapdoor (p, q). Pair sampling involves selecting random elements from $\mathbb{Z}_N^*$, raising them to the 2^m-th power, and inverting them modulo N.

We note that FS-IBI = cSI-2-IBI(FS-SI) is exactly the IBI scheme in [11] and FS-IBS = cSS-2-IBS(fs-I-2-S(FS-SI)) is exactly the IBS scheme in [11]. We know that FS-SI is imp-pa and imp-aa secure assuming factoring is hard [10], and this easily extends to imp-ca. Theorem 1 implies that FS-IBI inherits these security attributes. (Corollary 1 implies uf-cma security of FS-IBS assuming factoring is hard, but this was known [9].)

We know that ItR-SI is imp-pa and imp-aa secure assuming factoring is hard [30, 28]. Theorem 1 implies that ItR-IBI = cSI-2-IBI(ItR-SI) is imp-pa and imp-aa secure assuming factoring is hard. (Corollary 1 implies that ItR-IBS = cSS-2-IBS(fs-I-2-S(ItR-SI)) is uf-cma assuming factoring is hard, but this was known [9].) Whether ItR-SI is imp-ca secure, and hence whether ItR-IBI is imp-ca secure, remains open.

Scheme	Cmt Ch	Rsp Accept condition
FS	$y \xleftarrow{\$} \mathbb{Z}_N^*; Y \leftarrow y^2 \bmod N$	$z \leftarrow y \prod_i x_i^{c_i} \bmod N$
	$c = (c_1, \ldots, c_t) \xleftarrow{\$} \mathbb{Z}_2^t$	Accept iff $Y \equiv z^2 \prod_i X_i^{c_i} \bmod N$
ItR	$y \xleftarrow{\$} \mathbb{Z}_N^*; Y \leftarrow y^{2^m} \bmod N$	$z \leftarrow y \prod_i x_i^{c_i} \bmod N$
	$c = (c_1, \ldots, c_t) \xleftarrow{\$} \mathbb{Z}_{2^m}^t$	Accept iff $Y \equiv z^{2^m} \prod_i X_i^{c_i} \bmod N$
FF	$y_1 \xleftarrow{\$} \mathbb{Z}_{2^{m+\tau}}$ $y_2 \xleftarrow{\$} \mathbb{Z}_N^*$ $Y \leftarrow g^{y_1} y_2^{2^{m+\tau}} \bmod N$	$z_1 \leftarrow y_1 + cx_1 \bmod 2^{m+\tau}$ $\alpha \leftarrow \lfloor (y_1 + cx_1)/2^{m+\tau} \rfloor$ $z_2 \leftarrow g^{\alpha} y_2 x_2^c \bmod N$; $z \leftarrow z_1, z_2$
	$c \xleftarrow{\$} \mathbb{Z}_{2^m}$	Accept iff $g^{z_1} z_2^{2^{m+\tau}} \equiv Y X^c \bmod N$
Sh	$y \xleftarrow{\$} \mathbb{Z}_N^*; Y \leftarrow y^e \bmod N$	$z \leftarrow xy^c \bmod N$
	$c \xleftarrow{\$} \{0, \ldots, 2^{l(k)} - 1\}$	Accept iff $z^e \equiv XY^c \bmod N$
Sh*	$y \xleftarrow{\$} \mathbb{Z}_N^*; Y \leftarrow y^e \bmod N$	$z \leftarrow xy^c \bmod N$
	$c \xleftarrow{\$} \{1, \ldots, 2^{l(k)}\}$	Accept iff $z^e \equiv XY^c \bmod N$
GQ	$y \xleftarrow{\$} \mathbb{Z}_N^*; Y \leftarrow y^e \bmod N$	$z \leftarrow x^c y \bmod N$
	$c \xleftarrow{\$} \{0,1\}^{l(k)}$	Accept iff $z^e \equiv X^c Y \bmod N$
OkRSA	$y_1 \xleftarrow{\$} \mathbb{Z}_e$ $y_2 \xleftarrow{\$} \mathbb{Z}_N^*$ $Y \leftarrow g^{y_1} y_2^e \bmod N$	$z_1 \leftarrow y_1 + cx_1 \bmod e$ $\alpha \leftarrow \lfloor (y_1 + cx_1)/e \rfloor$ $z_2 \leftarrow g^{\alpha} y_2 x_2^c \bmod N$
	$c \xleftarrow{\$} \{0,1\}^{l(k)}$	Accept iff $Y \equiv g^{z_1} z_2^e X^c \bmod N$
Gir	$y \xleftarrow{\$} \mathbb{Z}_f; Y \leftarrow h^y \bmod N$ $\mathrm{Cmt} \leftarrow (P, Y)$	$z \leftarrow y + sc \bmod f$
	$c \xleftarrow{\$} \{0,1\}^{l(k)}$	Accept iff $h^z (P^e X)^c \equiv Y \bmod N$
SOK	$y \xleftarrow{\$} \mathbb{Z}_q$; $Y \leftarrow yP$	$z \leftarrow yc + V$
	$c \xleftarrow{\$} \mathbb{G}_1$	Accept iff $\hat{e}(z, P) = \hat{e}(U, S)\hat{e}(c, Y)$
Hs	$y \xleftarrow{\$} \mathbb{Z}_q; Y \leftarrow \hat{e}(P, P)^y$	$z \leftarrow yP + cV$
	$c \xleftarrow{\$} \mathbb{Z}_q$	Accept iff $\hat{e}(z, P) = Y \cdot \hat{e}(U, S)^c$
ChCh	$y \xleftarrow{\$} \mathbb{Z}_q$; $Y \leftarrow yU$	$z \leftarrow (y + c)V$
	$c \xleftarrow{\$} \mathbb{Z}_q$	Accept iff $\hat{e}(z, P) = \hat{e}(Y + cU, S)$
Beth	$y \xleftarrow{\$} \mathbb{Z}_q$; $Y \leftarrow R^{-y}$ $\mathrm{Cmt} \leftarrow (R, Y)$	$z \leftarrow y + cs \bmod q$
	$c \xleftarrow{\$} \{0,1\}^{l(k)}$	Accept iff $g^c h \equiv R^z Y X^{cR}$

Fig. 4. Identification protocols of the 12 cSI schemes that we consider. We show the first commitment message Cmt sent by the prover, the challenge Ch sent by the verifier, the response Rsp returned by the prover, and the condition under which the verifier accepts. All schemes use $\mathrm{Cmt} = Y$, $\mathrm{Ch} = c$ and $\mathrm{Rsp} = z$ unless explicitly defined otherwise. The prover is initialized with sk and the verifier with pk. The integers $m, t \geq 1$, and the challenge length $l\colon\ \mathbb{N} \to \mathbb{N}$, where used, are scheme parameters. In Sh-SI, Sh*-SI, GQ-SI, and Gir-SI, it is assumed that $2^{l(k)} < e$ for all e output by $\mathcal{K}_{\mathrm{rsa}}(1^k)$. All security results assume l is super-logarithmic. $\mathcal{K}_{\mathrm{rsa}}$ is a prime-exponent generator in Sh-SI, Sh*-SI, and GQ-SI.

FF. The FF-SI scheme was introduced by [12] as a fix to an attack they found on a scheme in [21]. In the key-generation algorithm of Figure 3, $\eta(p)$ denotes the largest integer such that $2^{\eta(p)}$ divides $p-1$ and $\eta(p,q) = \max(\eta(p), \eta(q))$. FF-SI is shown in [12] to be imp-pa, imp-aa, and imp-ca secure assuming factoring is hard. The authors defined no IBI or IBS schemes. We can show that FF-SI is convertible, and we thus obtain FF-IBI = cSI-2-IBI(FF-SI) and FF-IBS = cSS-2-IBS(fs-I-2-S(FF-SI)), and these are secure if factoring moduli generated by $\mathcal{K}_{\rm fact}$ is hard.

Let $\mathrm{HQR}_N = \{x^{2^{\eta(p,q)}} \bmod N \mid x \in \mathbb{Z}_N^*\}$ denote the set of higher quadratic residues modulo N, which is also the subset of elements of $\mathbb{Z}_N^*$ of odd order. To show convertibility of FF-SI we consider the relation $\mathbf{R} \subseteq (\mathbb{Z}_{2^m} \times \mathbb{Z}_N^*) \times \mathrm{HQR}_N$ described by (N, g, τ) and containing tuples $((x_1, x_2), X)$ such that $g^{x_1} x_2^{2^{\tau+m}} \equiv X \bmod N$. The trapdoor is the factorization of N. Regularity holds since squaring is a permutation over HQR_N and since each higher quadratic residue has exactly $2^{\eta(p)+\eta(q)}$ different $2^{\tau+m}$-th roots modulo N. Pair sampling involves choosing x_1, x_2 at random and computing $X = g^{x_1} x_2^{2^{\tau+m}}$.

GQ. The GQ-SI scheme defined via Figures 3 and 4 is the standard one considered in the literature. Convertibility is easily seen by considering the relation $\mathbf{R} = \{(x, X) \mid x^e \equiv X \bmod N\}$, relation description $\langle \mathbf{R} \rangle = (N, e)$, and trapdoor d. Pair sampling involves choosing $x \xleftarrow{\$} Z_N^*$ and computing $X \leftarrow x^e \bmod N$. We note that GQ-IBI = cSI-2-IBI(GQ-SI) is exactly the IBI scheme in [16], and GQ-IBS = cSS-2-IBS(fs-I-2-S(GQ-SI)) is exactly the IBS scheme in [16]. We know that GQ-SI is imp-pa secure assuming RSA is one-way, and imp-aa and imp-ca secure assuming hardness of the one-more-RSA problem [4]. Theorem 1 says that these results extend to GQ-IBI. (Also Corollary 1 says that GQ-IBS is uf-cma assuming RSA is one-way, but this was known [9].)

Sh AND Sh*. Shamir [29] defined an IBS scheme, but no SI or IBI schemes. He gave no security proof for his IBS scheme, and none has been provided until now.

We surface the SI scheme Sh-SI defined via Figures 3 and 4. One can check that Sh-IBS = cSS-2-IBS(fs-I-2-S(Sh-SI)) is exactly the IBS scheme in [29]. Sh-SI is interesting both historically and technically. It turns out to be a "mirror-image" of GQ-SI that closely resembles the latter. Convertibility of Sh-SI follows from the convertibility of GQ-SI since the two schemes have the same key-generation algorithm. Coming to consider security, the first question to ask is whether Sh-SI is honest-verifier zero-knowledge (HVZK). While this was obvious for GQ-SI (and in fact, if true for an SI scheme, is usually obvious), it is in fact not apparent at first glance for Sh-SI, and one might suspect that the scheme is not HVZK. However, using a trick involving gcds, we show that Sh-SI is statistical (not perfect) HVZK. We also show, in [2], that it is a proof of knowledge and thereby obtain the following:

Theorem 3. *The* Sh-SI *is imp-pa secure assuming one-wayness of the underlying RSA key generator* $\mathcal{K}_{\rm rsa}$.

Corollary 1 now implies that Sh-IBS is uf-cma secure under the same assumptions.

However, Sh-SI scheme is trivially insecure under active attacks, since the cheating verifier can learn the secret key by sending a zero challenge. But this minor weakness is

easily fixed by "removing" the zero challenge. We define via Figures 3 and 4 a modified scheme we denote Sh*-SI. This scheme turns out to have security attributes analogous to those of GQ-SI in that we can show the following:

Theorem 4. *The* Sh*-SI *scheme is imp-pa secure assuming one-wayness of the underlying RSA key generator* $\mathcal{K}_{\mathrm{rsa}}$*, and imp-aa and imp-ca secure assuming the one-more-RSA problem relative to* $\mathcal{K}_{\mathrm{rsa}}$ *is hard.*

The proof of this theorem is in [2]. We obtain the usual consequences for Sh*-IBI = cSI-2-IBI(Sh*-SI) and Sh*-IBS = cSS-2-IBS(fs-I-2-S(Sh*-SI)).

OkRSA. Okamoto [21] presented an RSA-based SI scheme and a related RSA-based IBI scheme. He proved the former imp-pa and imp-aa secure assuming factoring is hard, and the proofs extend to establish imp-ca as well. However, he did not prove the IBI scheme secure, a gap we fill.

The OkRSA-SI scheme defined via Figures 3 and 4 is the above-mentioned SI scheme. Notice that OkRSA-IBI = cSI-2-IBI(OkRSA-SI) is exactly the RSA-based IBI scheme in [21]. To show security of OkRSA-IBI and OkRSA-IBS = cSS-2-IBS (fs-I-2-S(OkRSA-SI)), it suffices to show that OkRSA-SI is convertible. For this, the relation has description $\langle \mathbf{R} \rangle = (N, e, g)$, and contains tuples $((x_1, x_2), X) \in (\mathbb{Z}_e \times \mathbb{Z}_N^*) \times \mathbb{Z}_N^*$ such that $X \equiv g^{x_1} x_2^e \bmod N$. The trapdoor is d such that $ed \equiv 1 \bmod \varphi(N)$. Pair sampling involves choosing x_1, x_2 at random and computing $X \equiv g^{x_1} x_2^e$.

Gir. In [13], Girault proposed an SI scheme that we have defined via Figures 3 and 4 and named Gir-SI. He also proposed a related IBI scheme. (These schemes are inspired by the Schnorr identification scheme [27] but use a modulus $N = pq$ where p, q are of the special form $p = 2fp' + 1$ and $q = 2fq' + 1$ such that f, p', q', p, q are all primes.) This IBI scheme did not use hash functions, which lead to an attack and later a fix [25]. The fixed IBI scheme turns out to be exactly Gir-IBI = cSI-2-IBI(Gir-SI).

Gir-SI is convertible with relation $\mathbf{R} = \{((P, s), X) \mid P^e \equiv X^{-1} h^{-s} \bmod N\}$ described by (N, e, h, f). The trapdoor is $d \equiv e^{-1} \bmod \varphi(N)$. Pair sampling involves choosing P and s at random and computing X as $P^{-e} h^{-s} \bmod N$. However, this does not help here because we found that all schemes in the family are insecure. In particular, Gir-SI is not even imp-pa secure, and neither is the fixed IBI scheme Gir-IBI. The signature scheme Gir-IBS = cSS-2-IBS(fs-I-2-S(Gir-IBI)) is not uf-cma secure either.

We attack only the Gir-IBS scheme, since the insecurity of the SI, IBI, and SS schemes then follows. In the Gir-IBS scheme, a signature of a user I on a message M under the master public key $mpk = (N, e, h, f)$ is a tuple (P, Y, z) such that $Y \equiv h^z (P^e \cdot \mathrm{H}_1(I))^{\mathrm{H}_2(P \| Y \| M)} \bmod N$. Given a valid signature (P_1, Y_1, z_1) for message M_1 and identity I, an adversary can forge I's signature for any message M_2 as follows. If first computes $d_2 \leftarrow e^{-1} \bmod f$, $g \leftarrow h^{d_2} \bmod N$, and $S \leftarrow (P^e \cdot \mathrm{H}_1(I))^{d_2} \bmod N$. Then, it chooses s_2 from $\mathbb{Z}_f$ and computes $P_2 \leftarrow P_1 S^{-1} g^{-s_2} \bmod N$. To obtain the forgery, it chooses y_2 from $\mathbb{Z}_q$, lets $Y_2 \leftarrow h^{y_2} \bmod N$, computes $z_2 \leftarrow y_2 + s_2 \mathrm{H}_2(P_2 \| Y_2 \| M_2) \bmod f$. The forgery is (P_2, Y_2, z_2).

It is natural to consider counteracting the above attack by removing f from the public key. While this might work for the SI scheme, it does not for the IBI (or IBS)

scheme. The reason is that, since f still has to be included in each user's secret key, an adversary can easily extract it by corrupting one identity.

We stress that the scheme broken here is *not* the (perhaps better-known) SI scheme by Girault based on discrete logarithms [14].

PAIRING-BASED SCHEMES. Many recent papers propose pairing-based IBS schemes [26, 8, 32, 23, 17] (the schemes independently published by [8] and [32] are actually equivalent). Barring [8], none of these papers prove their scheme secure. (Some proofs in weak models were however provided in [17, 32].) However, the scheme of [17] was proven secure in [9].

None of these papers define SI or IBI schemes. We surface SOK-SI (from [26]), ChCh-SI (from [8, 32]) and Hs-SI (from [17]), as defined by Figures 3 and 4. The ChCh-IBS = cSS-2-IBS(fs-I-2-S(ChCh-SI)) and Hs-IBS = cSS-2-IBS(fs-I-2-S(Hs-SI)) schemes are exactly the original IBS schemes, while SOK-IBS = cSS-2-IBS(fs-I-2-S(SOK-SI)) is slightly different from the scheme of [26].

We now show that all these pairing-based SI schemes are convertible. Since they all have the same key-generation algorithm, a common argument applies. The relation is $\{(V,U) \in \mathbb{G}_1 \times \mathbb{G}_1 \mid \hat{e}(V,P) = \hat{e}(U,S)\}$, described by $\langle \mathbf{R} \rangle = (\mathbb{G}_1, \mathbb{G}_2, q, P, \hat{e}, S)$. The trapdoor is s such that $S = sP$. Pair sampling involves choosing $r \xleftarrow{\$} \mathbb{Z}_q$ and computing the pair (rP, rS). The following is proved in [2].

Theorem 5. SOK-SI *and* ChCh-SI *are imp-pa secure assuming that the computational Diffie-Hellman problem in the group* $\mathbb{G}_1$ *associated to* $\mathcal{K}_{\mathrm{pair}}$ *is hard.*

Corollary 1 implies that ChCh-IBS, SOK-IBS and Hs-IBS are uf-cma secure IBS schemes, but of these only the result about SOK-IBS is new. However, we prove the following in [2]:

Theorem 6. ChCh-SI *and* Hs-SI *are imp-aa and imp-ca secure assuming that the one-more computational Diffie-Hellman problem in the group* $\mathbb{G}_1$ *associated to* $\mathcal{K}_{\mathrm{pair}}$ *is hard.*

Theorem 1 implies that the ChCh-IBI and Hs-IBI schemes are imp-aa and imp-ca secure assuming that the one-more computational Diffie-Hellman problem in the group $\mathbb{G}_1$ associated to $\mathcal{K}_{\mathrm{pair}}$ is hard. Thus, we obtain new, pairing-based IBI schemes with proofs of security.

SOK-SI and SOK-IBI are insecure under active or concurrent attacks: upon receiving a commitment Y, an adversary can choose $c' \xleftarrow{\$} \mathbb{Z}_q$, submit $c \leftarrow c'P$ as the challenge, and compute the prover's secret key from the response z as $V \leftarrow z - cY$.

Beth. The Beth-SI scheme defined via Figures 3 and 4 was surfaced from [6]. Beth-IBI = cSI-2-IBI(Beth-SI) is a more efficient version of the IBI scheme actually presented in [6]. In these schemes, the prover proves knowledge of an ElGamal signature of his identity. Beth [6] gives no security proofs, but here we obtain one for Beth-IBI.

The Beth-SI scheme is convertible with the relation $\{((R,s),h) \in (\mathbb{G} \times \mathbb{Z}_q) \times \mathbb{Z}_q \mid X^R R^s \equiv g^h\}$ described by $\langle \mathbf{R} \rangle = (\mathbb{G}, q, g, X)$. The trapdoor is x such that $g^x \equiv X$. Pair sampling involves choosing a, b at random from $\mathbb{Z}_q$ and letting $R \leftarrow X^a g^b$, $s \leftarrow a^{-1}R \bmod q$ and $h \leftarrow bs \bmod q$. In [2],we prove the following:

Theorem 7. Beth-SI *is imp-pa secure assuming that the hashed-message ElGamal signature scheme associated to* $\mathcal{K}_{\mathrm{dlog}}$ *is universally unforgeable under no-message attacks in the random oracle model.*

While the hashed-message ElGamal signature scheme has never been formally proven secure, we note that *universal* forgery under *no-message* attacks is a very weak security notion for signature schemes and that a close variant of hashed-message ElGamal was proven uf-cma secure under the discrete log assumption in [24]. Now, Theorem 1 implies that Beth-IBI inherits the above security attributes, and Corollary 1 implies that Beth-IBS $=$ cSS-2-IBS(fs-I-2-S(Beth-SI)) is uf-cma secure under the same assumptions. The imp-aa and imp-ca security of Beth-SI remains open.

Acknowledgments

We thank Marc Fischlin for pointing out that the Sh-SI scheme is zero-knowledge. The first author is supported in part by NSF grants CCR-0098123, ANR-0129617, CCR-0208842, and an IBM Faculty Partnership Development Award. The second author is supported in part by the above-mentioned grants of the first author. The third author is supported by a Research Assistantship and travel grant from the Fund for Scientific Research – Flanders (Belgium).

References

[1] M. Abdalla, J.H. An, M. Bellare, and C. Namprempre. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In L. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 418–433. Springer-Verlag, April 2002.

[2] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. http://www.cse.ucsd.edu/users/mihir/crypto-research-papers.html, February 2004.

[3] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. *J. Cryptology*, 16(3):185–215, June 2003.

[4] M. Bellare and A. Palacio. GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attack. In M. Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 162–177. Springer-Verlag, August 2002.

[5] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In ACM, editor, *Proc. of the 1st CCS*, pages 62–73. ACM Press, November 1993.

[6] T. Beth. Efficient zero-knowledged identification scheme for smart cards. In C. Gunther, editor, *EUROCRYPT 1988*, volume 330 of *LNCS*, pages 77–86. Springer-Verlag, May 1988.

[7] D. Boneh and M. Franklin. Identity-based encryption from the Weil Pairing. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer-Verlag, August 2001.

[8] J.C. Cha and J.H. Cheon. An identity-based signature from gap diffie-hellman groups. In Y. Desmedt, editor, *PKC 2003*, volume 2567 of *LNCS*, pages 18–30. Springer-Verlag, January 2003.

[9] Y. Dodis, J. Katz, S. Xu, and M. Yung. Strong key-insulated signature schemes. In Y. Desmedt, editor, *PKC 2003*, volume 2567 of *LNCS*, pages 130–144. Springer-Verlag, January 2003.

[10] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. *J. Cryptology*, 1(2):77–94, 1988.

[11] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. Odlyzko, editor, *CRYPTO 1986*, volume 263 of *LNCS*, pages 186–194. Springer-Verlag, August 1986.

[12] M. Fischlin and R. Fischlin. The representation problem based on factoring. In B. Preneel, editor, *CT-RSA 2002*, volume 2271 of *LNCS*, pages 96–113. Springer-Verlag, February 2002.

[13] M. Girault. An identity-based identification scheme based on discrete logarithms modulo a composite number. In I. Damgård, editor, *EUROCRYPT 1990*, volume 473 of *LNCS*, pages 481–486. Springer-Verlag, May 1990.

[14] M. Girault. Self-certified public keys. In D. Davies, editor, *EUROCRYPT 1991*, volume 547 of *LNCS*, pages 490–497. Springer-Verlag, April 1991.

[15] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Computing*, 17(2):281–308, April 1988.

[16] L. Guillou and J. J. Quisquater. A "paradoxical" identity-based signature scheme resulting from zero-knowledge. In S. Goldwasser, editor, *CRYPTO 1988*, volume 403 of *LNCS*, pages 216–231. Springer-Verlag, August 1989.

[17] F. Hess. Efficient identity based signature schemes based on pairings. In K. Nyberg and H. Heys, editors, *Selected Areas in Cryptography, SAC 2002*, pages 310–324. Springer-Verlag, February 2003.

[18] K. Kurosawa and S.-H. Heng. From digital signature to ID-based identification/signature. In *PKC 2004*. Springer-Verlag, 2004.

[19] K. Ohta and T. Okamoto. A modification of the Fiat-Shamir scheme. In S. Goldwasser, editor, *CRYPTO 1988*, volume 403 of *LNCS*, pages 232–243. Springer-Verlag, August 1990.

[20] K. Ohta and T. Okamoto. On concrete security treatment of signatures derived from identification. In H. Krawczyk, editor, *CRYPTO 1998*, volume 1462 of *LNCS*, pages 354–370. Springer-Verlag, August 1998.

[21] T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In E. Brickell, editor, *CRYPTO 1992*, volume 740 of *LNCS*, pages 31–53. Springer-Verlag, August 1992.

[22] H. Ong and C. Schnorr. Fast signature generation with a Fiat Shamir–like scheme. In I. Damgård, editor, *EUROCRYPT 1990*, volume 473 of *LNCS*, pages 432–440. Springer-Verlag, May 1990.

[23] K.G. Paterson. ID-based signatures from pairings on elliptic curves. Technical Report 2002/004, IACR ePrint Archive, January 2002.

[24] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *J. Cryptology*, 13(3):361–396, 2000.

[25] S. Saeednia and R. Safavi-Naini. On the security of girault's identification scheme. In H. Imai and Y. Zheng, editors, *PKC 1998*, volume 1431 of *LNCS*, pages 149–153. Springer-Verlag, February 1998.

[26] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *SCIS 2000*, Okinawa, Japan, January 2000.

[27] C. Schnorr. Efficient identification and signatures for smartcards. In G. Brassard, editor, *CRYPTO 1989*, volume 435 of *LNCS*, pages 239–252. Springer-Verlag, August 1990.

[28] C. Schnorr. Security of 2^t-root identification and signatures. In N. Koblitz, editor, *CRYPTO 1996*, volume 1109 of *LNCS*, pages 143–156. Springer-Verlag, August 1996.

[29] A. Shamir. Identity-based cryptosystems and signature schemes. In G.R. Blakely and D. Chaum, editors, *CRYPTO 1984*, volume 196 of *LNCS*, pages 47–53. Springer-Verlag, 1984.

[30] V. Shoup. On the security of a practical identification scheme. *J. Cryptology*, 12(4):247–260, 1999.

[31] J. Stern, D. Pointcheval, J. Malone-Lee, and N.P. Smart. Flaws in applying proof methodologies to signature schemes. In M. Yung, editor, *CRYPTO 2002*, volume 2442 of *LNCS*, pages 93–110. Springer-Verlag, August 2002.

[32] X. Yi. An identity-based signature scheme from the weil pairing. *IEEE Communications Letters*, 7(2):76–78, 2003.