Identity-Based Signatures

Eike KILTZ [a] Gregory NEVEN [b]
[a] *CWI Amsterdam, The Netherlands*
[b] *IBM Zürich Research Laboratory, Switzerland, and Katholieke Universiteit Leuven, Belgium*

Abstract. This chapter gives an overview of the literature on identity-based signature (IBS) schemes, from Shamir's seminal scheme to the current state-of-the-art. Rather than presenting all schemes separately, we present three generic transformations that together cover the majority of known IBS schemes as special cases. The first transformation follows a certification approach based on standard signatures; the second is a transformation in the random oracle model from "convertible" identification schemes; and the third is based on hierarchical identity-based encryption. We also discuss a number of direct schemes that escape being covered by any of the generic transformations. Finally, we show how the principles of the first transformation can be extended to a hierarchical setting and to IBS schemes with special properties.

Keywords. Identity-based signatures; electronic signatures; identification schemes

1. Introduction

Digital signatures are among the most basic primitives in cryptography, providing authenticity, integrity, and non-repudiation in an asymmetric setting. In their most basic form, each user in the system generates his own key pair consisting of a public key and a corresponding secret key, and the user is assumed to be uniquely identified by his public key. In the real world however, users are generally not identified by randomly generated keys, but by more meaningful identities like their names or email addresses. To map public keys to real-world identities, a so-called public-key infrastructure (PKI) needs to be set up, for example involving a hierarchy of trusted certification authorities (CAs) that can certify public keys as belonging to a certain user.

In the identity-based setting, as proposed by Shamir in 1984 [32], the public key of a user simply *is* his identity, simplifying the PKI requirements. The corresponding secret key is issued by a trusted key generation center (KGC), who derives it from a master secret that only the KGC knows, and who is assumed to have an out-of-band way to verify the identity of the user. This eliminates some of the costs associated to PKIs and certificates, and opens the way to more efficient schemes.

From a security point of view, the major drawback of identity-based cryptography is the inherent key escrow property: the KGC can derive the secret keys of

all users in the system, and must therefore be trusted not to abuse this power. This is unlike a traditional PKI, where the CA only issues certificates on user-generated public keys, but does not know the corresponding secret keys. While most people find it a discomforting thought that a malafide KGC can sign any message on their behalf, one should be aware that the same type of fraud is possible in the public-key setting as well. Namely, since the certificate is usually sent along with the signature, a cheating CA can always generate a fake certificate for a public key of which it knows the corresponding secret key, and thereby create valid signatures. The victim could try to prove his innocence by showing his real certificate to a judge, but nothing prevents the CA from claiming that the user registered two different public keys. The escrow property is therefore not so much an issue for signatures as it is for encryption, where a malafide KGC can actually decrypt ciphertexts intended for any of its users. So even though there is no legitimate use for escrow of signing keys, as already mentioned in the introduction chapter, a limited form of key escrow is inherently present in *both* PKI-based and ID-based signature schemes.

Identity-based signatures (IBS) also seem to be much "easier" to achieve than identity-based encryption (IBE), of which only few instantiations are known. In contrast, many practical instantiations of IBS schemes have been known for decades, including the scheme in Shamir's seminal paper from 1984 [32]. In this chapter, we give an overview of the state-of-the-art in IBS schemes. We present three generic transformations to build IBS schemes from standard signature schemes, from a special class of identification schemes, and from hierarchical identity-based encryption schemes, respectively. With each transformation, we discuss some of its most interesting concrete instantiations, and compare the efficiency and security properties of all these schemes. Finally, we show how the first transformation can also be applied to obtain identity-based variants of signature schemes with special properties, including blind, threshold, and verifiably encrypted signatures.

2. Definition of Identity-Based Signatures

We first introduce some notation. If $x_1, \ldots, x_n$ are bit strings, then we denote by $x_1 \| \ldots \| x_n$ a string encoding of $x_1, \ldots, x_n$ from which the constituent objects are uniquely recoverable. If x is a string, then $|x|$ denotes its length, and if S is a set, then $|S|$ is its cardinality. If A is a randomized algorithm, then $y \xleftarrow{\$} \mathsf{A}(x_1, x_2, \ldots)$ means that A has inputs $x_1, x_2, \ldots$ and that y is assigned the output of A when run on a fresh random tape.

We measure the resources of an adversary, such as its running time and its number of oracle queries, asymptotically in terms of an underlying security parameter k. A function $\nu(k)$ is said to be negligible (in k) if for all $c \in \mathbb{N}$ there exists $k_c \in \mathbb{N}$ such that $\nu(k) < k^{-c}$ for all $k > k_c$.

An *identity-based signature (IBS) scheme* is a tuple of algorithms $\mathcal{IBS} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Sign}, \mathsf{Vf})$ with running time polynomial in the security parameter k. The first three may be randomized but the last is not. The trusted key distribution center runs the setup algorithm Setup on input 1^k to obtain a master public

and secret key pair (mpk, msk). (Here, 1^k is the unary notation of the security parameter k.) To generate the secret signing key usk for the user with identity $id \in \{0,1\}^*$, it runs the key derivation algorithm KeyDer on input msk and id. The signing key is assumed to be securely communicated to the user in question. On input usk and a message M, the signing algorithm Sign returns a signature σ of M. On input mpk, id, M, and a signature σ, the verification algorithm Vf returns 1 if σ is valid for id and M, and returns 0 otherwise. Correctness requires that $\mathsf{Vf}(mpk, id, M, \mathsf{Sign}(usk, M)) = 1$ with probability one for all $k \in \mathbb{N}$ and $id, M \in \{0,1\}^*$ whenever the keys mpk, M, usk are generated as indicated above.

For security we consider the notion of existential unforgeability under chosen-message and chosen-identity attack (uf-cma) [22]. Security is defined through an experiment with a forger F and parameterized with the security parameter k. The experiment begins with the generation of a fresh master key pair $(mpk, msk) \xleftarrow{\$} \mathsf{Setup}(1^k)$. The forger F is run on input the master public key mpk, and has access to the following oracles:

- $\mathsf{KeyDer}(\cdot)$: On input identity $id \in \{0,1\}^*$, this oracle returns a secret signing key $usk \xleftarrow{\$} \mathsf{KeyDer}(msk, id)$.
- $\mathsf{Sign}(\cdot,\cdot)$: On input identity $id \in \{0,1\}^*$ and message $M \in \{0,1\}^*$, this oracle returns a signature $\sigma \xleftarrow{\$} \mathsf{Sign}(usk, M)$ where $usk \xleftarrow{\$} \mathsf{KeyDer}(msk, id)$.

At the end of its execution, the forger outputs identity id^*, message M^* and a forged signature σ^*. The forger is said to win the game if $\mathsf{Vf}(mpk, id^*, M^*, \sigma^*) = 1$ and F never queried $\mathsf{KeyDer}(id^*)$ or $\mathsf{Sign}(id^*, M^*)$. The advantage $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{IBS},\mathsf{F}}(k)$ is defined as the probability that F wins the game, and $\mathcal{IBS}$ is said to be uf-cma secure if $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{IBS},\mathsf{F}}(k)$ is negligible in k for all polynomial-time forgers F.

3. The Certification Approach

Unlike identity-based encryption, there is a very natural way to build identity-based signatures from more basic cryptographic tools by using certificates, as already pointed out in Chapter 1. This may sound paradoxical since one of the primary purposes of identity-based cryptography is to avoid certificates, but certification here refers to a technique, not to a PKI. The idea is simply that the a user's secret key includes a secret key of a standard signature scheme and a certificate for the corresponding public key, i.e., a standard signature from the authority that links the user's identity to that public key. To accomplish IBS, the user signs messages using the secret signing key, and appends to the signature his public key and certificate.

This straightforward construction has long been folklore in the research community, and was explicitly mentioned in [22,17,3]. The construction is important however as a benchmark, relative to which the efficiency of direct IBS schemes must be measured. Moreover, from a foundational point of view, the certificate-based construction shows that IBS schemes can be built in the standard model from one-way functions [31]. This is in stark contrast with identity-based encryption, for which the answer to such fundamental questions is still unknown.

3.1. Standard Signature Schemes

Before giving more details about the construction, we recall the syntax and security definitions of standard signature (SS) schemes [23]. It is defined as a tuple of polynomial-time algorithms $\mathcal{SS} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vf})$. The randomized key generation algorithm KeyGen on input 1^k generates a key pair (pk, sk). The signer creates a signature on a message M via $\sigma \xleftarrow{\$} \mathsf{Sign}(sk, M)$, and the verifier can check the validity of a signature by testing whether $\mathsf{Vf}(pk, M, \sigma) = 1$. Correctness requires that $\mathsf{Vf}(pk, M, \mathsf{Sign}(sk, M)) = 1$ with probability one for all $M \in \{0,1\}^*$.

Security is defined through the notion of existential unforgeability under chosen-message attack (uf-cma), described by the following game with a forger F. The forger is run with a fresh public key pk as input, and is given access to a signing oracle for the corresponding secret key sk. It is said to win the game if it can output a pair (M^*, σ^*) such that $\mathsf{Vf}(pk, M^*, \sigma^*) = 1$ and it never queried M^* from the signing oracle. The advantage $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{SS},\mathsf{F}}(k)$ is defined as the probability that F wins this game, and $\mathcal{SS}$ is said to be uf-cma secure if this is a negligible function in k for all polynomial-time forgers F.

3.2. The SS-2-IBS *Transformation*

Given a standard signature scheme $\mathcal{SS} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vf})$, one can build a certificate-based IBS scheme $\mathcal{Cert\text{-}IBS} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Sign}', \mathsf{Vf}') = \text{SS-2-IBS}(\mathcal{SS})$ as follows. One can easily prove that if $\mathcal{SS}$ is uf-cma secure, then $\mathcal{Cert\text{-}IBS}$ is uf-cma secure as well.

Scheme 1 The certificate-based IBS scheme $\mathcal{Cert\text{-}IBS}$

Algorithm $\mathsf{Setup}(1^k)$**:**
$(mpk, msk) \xleftarrow{\$} \mathsf{KeyGen}(1^k)$
return (mpk, msk)

Algorithm $\mathsf{KeyDer}(msk, id)$**:**
$(pk, sk) \xleftarrow{\$} \mathsf{KeyGen}(1^k)$; $cert \xleftarrow{\$} \mathsf{Sign}(msk, pk \| id)$
return $usk \leftarrow (sk, pk, cert)$

Algorithm $\mathsf{Sign}'(usk, M)$**:**
Parse usk as $(sk, pk, cert)$; $\sigma \xleftarrow{\$} \mathsf{Sign}(sk, M)$
return $\sigma' \leftarrow (\sigma, pk, cert)$

Algorithm $\mathsf{Vf}'(mpk, id, M, \sigma')$**:**
Parse σ' as $(\sigma, pk, cert)$
If $\mathsf{Vf}(pk, M, \sigma) = 1$ and $\mathsf{Vf}(mpk, pk \| id, cert) = 1$ then $d \leftarrow 0$ else $d \leftarrow 1$
return d

Since there are numerous constructions of uf-cma secure SS schemes without random oracles [21,14,5], we obtain from the above IBS schemes without random oracles. Given that the existence of uf-cma secure SS schemes is equivalent to the existence of one-way functions [31], an easy corollary says that uf-cma secure IBS schemes exist if and only if one-way functions exist.

When instantiated with an efficient SS scheme, the SS-2-IBS transformation yields fairly efficient IBS schemes. Signing costs the same as for the underlying SS scheme, and verification comes at twice the cost of the SS scheme. The size of the signature increases due to inclusion of the certificate. The sole goal of the direct IBS schemes presented in this chapter is therefore to reduce costs below that of even the best instantiations of the SS-2-IBS transform.

3.3. Instantiations

The main advantage of the certificate-based approach from is its generality. The efficiency and security properties depend highly on the underlying SS scheme being used. For example, to obtain IBS schemes with security in the standard model, one can use any of the standard-model SS schemes of [21,14,5]. To save on signature size, one can instantiate the scheme with short BLS signatures [10]. The IBS schemes thus obtained are not the most efficient, but they may be an interesting alternative in case for example fast SS implementations are readily available.

4. Constructions from Identification Schemes

A second generic transformation yielding more efficient IBS schemes was proposed by Bellare, Namprempre, and Neven [3]. The transform works for a particular class of three-move identification schemes called *convertible* identification schemes. Instances of such schemes can be found based on various cryptographic assumptions such as RSA, factoring, and pairings. The transformation itself bears a lot in common with the Fiat-Shamir transform [19] that turns a three-move identification scheme into a standard (i.e., not identity-based) signature scheme. Bellare et al. proved the security of the transformation in the random oracle model, and gave an extensive overview of instantiations that either appeared in the literature as identification schemes, or that appeared as IBS schemes directly but that in retrospect can be seen as being derived from a convertible identification scheme.

4.1. Canonical Convertible Identification Schemes

We first recall the definition of standard identification (SI) schemes, and then define a particular class of schemes to which the transform applies. A SI scheme is a tuple of polynomial-time algorithms $\mathcal{SI} = (\mathsf{KeyGen}, \mathsf{P}, \mathsf{V})$. The key generation algorithm KeyGen, on input the security parameter 1^k, outputs a fresh key pair (pk, sk). The prover and verifier algorithms P and V are interactive algorithms that together form the identification protocol. The prover P is run with the secret key sk as initial input, and interacts with the verifier V that gets the public key pk as initial input. At the end of the interaction, V outputs 0 or 1 indicating whether the prover was successfully identified. Correctness requires that V outputs 1 for all honest provers.

For security, we focus on the relatively weak notion of resistance against impersonation under passive attacks (imp-pa), since this notion suffices for our purposes of building IBS schemes. The adversary A, also called an impersonator,

gets as input a fresh public key pk, and has access to a transcript oracle that on each invocation returns the transcript of an interaction between the $\mathsf{P}(sk)$ and $\mathsf{V}(pk)$ algorithms. (It is easy to see that the protocol has to be randomized for the scheme to be secure, so the generated transcripts will be different at each invocation.) The impersonator A can then interact with an instance of $\mathsf{V}(pk)$, and wins the game if the latter outputs 1. The advantage $\mathbf{Adv}^{\text{imp-pa}}_{\mathcal{SI},\mathsf{A}}(k)$ is the probability that A wins, and $\mathcal{SI}$ is said to be imp-pa secure if the advantage is negligible for all polynomial-time adversaries A.

Before defining convertibility of SI schemes, we need to introduce the concept of trapdoor-samplable relations.

Definition 4.1 A family of *trapdoor-samplable relations* $\mathcal{F}$ is a triplet of polynomial-time algorithms $(\mathsf{TDG}, \mathsf{Smp}, \mathsf{Inv})$ such that the following properties hold:

- *Efficient generation:* On input 1^k, TDG outputs the description of a relation $R \subseteq \text{Dom} \times \text{Rng}$ together with its trapdoor information t;
- *Samplability:* The algorithm Smp, on input the description of a relation R, returns a uniformly random couple from R;
- *Inversion:* On input the description of a relation R, the corresponding trapdoor t, and an element $y \in \text{Rng}$, the randomized algorithm Inv outputs a random element of $R^{-1}(y)$;
- *Regularity:* For every relation R in the family, there is an integer d such that $|R^{-1}(y)| = d$ for all $y \in \text{Rng}$.

A SI scheme $\mathcal{SI} = (\mathsf{KeyGen}, \mathsf{P}, \mathsf{V})$ is said to be *convertible* (or a cSI scheme) if its key-generation process is underlain by a family of trapdoor-samplable relations. More specifically, there must exist a family $\mathcal{F} = (\mathsf{TDG}, \mathsf{Smp}, \mathsf{Inv})$ such that the keys generated by KeyGen are of the form $pk = (R, y)$ and $sk = (R, x)$ distributed according to

$$(R, t) \xleftarrow{\$} \mathsf{TDG}(1^k) \;\; ; \;\; (x, y) \xleftarrow{\$} \mathsf{Smp}(R) \; .$$

A cSI scheme $\mathcal{SI} = (\mathsf{KeyGen}, \mathsf{P}, \mathsf{V})$ is said to be *canonical* if it follows a three-move structure where the prover initiates the communication with a "commitment" cmt distributed uniformly over a set $\text{CmtSet}(R)$ possibly depending on the relation embedded in the public and secret keys; the verifier sends back a "challenge" ch chosen uniformly from a set $\text{ChSet}(R)$; the prover replies with a "response" rsp; and the verifier's decision to accept or reject is a deterministic function $\text{dec}(pk, cmt \,\|\, ch \,\|\, rsp) \in \{0, 1\}$ of the public key and the communication transcript. We require that $1/|\text{CmtSet}(R)|$ is negligible.

4.2. The cSI-2-IBS *Transformation*

A canonical cSI scheme directly yields a SS scheme through the well-known Fiat-Shamir transform [19]; the resulting SS scheme is uf-cma secure in the random oracle model if the underlying SI scheme is imp-pa secure [1]. To obtain an IBS scheme from a canonical cSI scheme $\mathcal{SI} = (\mathsf{KeyGen}, \mathsf{P}, \mathsf{V})$, consider the scheme $\mathcal{IBS} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Sign}, \mathsf{Vf}) = \text{cSI-2-IBS}(\mathcal{SI})$ as given below, where

$\mathrm{H} : \{0,1\}^* \to \mathrm{Rng}$ and $\mathrm{G} : \{0,1\}^* \to \mathrm{ChSet}(R)$ are hash functions, modeled as random oracles, whose range depends on the relation R. Bellare et al. [3] showed that if $\mathcal{SI}$ is imp-pa secure, then cSI-2-IBS($\mathcal{SI}$) is uf-cma secure in the random oracle model.

Scheme 2 The scheme $\mathcal{IBS} = \text{cSI-2-IBS}(\mathcal{SI})$.

Algorithm $\mathsf{Setup}(1^k)$**:**
$(R,t) \xleftarrow{\$} \mathsf{TDG}(1^k)$; $mpk \leftarrow R$; $msk \leftarrow (R,t)$
return (mpk, msk)

Algorithm $\mathsf{KeyDer}(msk, id)$**:**
$(R,t) \leftarrow msk$; $x \xleftarrow{\$} \mathsf{Inv}(R,t,\mathrm{H}(id))$
return $usk \leftarrow (R,x)$

Algorithm $\mathsf{Sign}(usk, M)$**:**
$(R,x) \leftarrow usk$; $cmt \xleftarrow{\$} \mathsf{P}(usk)$; $ch \leftarrow \mathrm{G}(cmt \| M)$; $rsp \leftarrow \mathsf{P}(ch)$
return $\sigma \leftarrow (cmt, rsp)$

Algorithm $\mathsf{Vf}(mpk, id, M, \sigma)$**:**
$R \leftarrow mpk$; $(cmt, rsp) \leftarrow \sigma$; $pk \leftarrow (R, \mathrm{H}(id))$; $ch \leftarrow \mathrm{G}(cmt \| M)$
return $\mathrm{dec}(pk, cmt \| ch \| rsp)$

4.3. Instantiations

As many as twelve different suitable cSI schemes were surfaced in [3] based on factoring, RSA, pairings, and discrete logarithms. These give rise to twelve different IBS schemes through the cSI-2-IBS transform. As an example, we highlight here the original IBS scheme proposed by Shamir in 1984 [32].

Let $\mathsf{K}_{\mathrm{rsa}}$ be an *RSA key generator* that on input 1^k outputs a modulus N that is the product of two distinct odd primes, and exponents e, d such that $ed = 1 \bmod (p-1)(q-1)$ and such that $e > 2^{l(k)}$ for some function $l(\cdot)$. We say that the RSA function associated to $\mathsf{K}_{\mathrm{rsa}}$ is one-way if

$$\mathbf{Adv}^{\mathrm{rsa}}_{\mathsf{K}_{\mathrm{rsa}},\mathsf{A}}(k) \;=\; \Pr\left[x^e = y \bmod N \;:\; \begin{array}{c} (N,e,d) \xleftarrow{\$} \mathsf{K}_{\mathrm{rsa}}(1^k)\ ;\ y \xleftarrow{\$} \mathbb{Z}_N^*\ ; \\ x \leftarrow \mathsf{A}(1^k, N, e, y) \end{array} \right]$$

is negligible in k for all polynomial-time algorithms A. First consider the identification scheme $\mathcal{Sh}$-$\mathcal{SI}$ given in Scheme 3.

To see why this SI scheme is convertible, observe the family of trapdoor-samplable relations described by pairs (N,e) and corresponding trapdoor d such that $R = \{(x,y) \in {\mathbb{Z}_N^*}^2 \;:\; y = x^e \bmod N\}$. It is also canonical with $\mathrm{CmtSet}(N,e) = \mathbb{Z}_N^*$ and $\mathrm{ChSet}(N,e) = \{0,1\}^{l(k)}$. Applying the cSI-2-IBS transformation yields the $\mathcal{Sh}$-$\mathcal{IBS}$ scheme given in Scheme 4, which is exactly the scheme from [32].

The $\mathcal{Sh}$-$\mathcal{SI}$ scheme was shown [3] to be imp-pa secure if the RSA function associated to $\mathsf{K}_{\mathrm{rsa}}$ is one-way. The $\mathcal{Sh}$-$\mathcal{IBS}$ scheme is therefore uf-cma secure under the same assumption.

Scheme 3 The SI scheme underlying Shamir's IBS scheme.

Algorithm $\mathsf{KeyGen}(1^k)$**:**
$(N, e, d) \xleftarrow{\$} \mathsf{K}_{\mathrm{rsa}}(1^k)$; $x \xleftarrow{\$} \mathbb{Z}_N^*$; $y \leftarrow x^e \bmod N$
$pk \leftarrow (N, e, y)$; $sk \leftarrow (N, e, x)$
return (pk, sk)

Algorithm $\mathsf{P}(sk)$**:**
Parse sk as (N, e, x)
$t \xleftarrow{\$} \mathbb{Z}_N^*$; $T \leftarrow t^e \bmod N$ — T →
— c ←
$s \leftarrow xt^c \bmod N$ — s →

Algorithm $\mathsf{V}(pk)$**:**
Parse pk as (N, e, y)
$c \xleftarrow{\$} \{0,1\}^{l(k)}$
If $s^e = yT^c \bmod N$
then $d \leftarrow 1$ else $d \leftarrow 0$
return d

Scheme 4 Shamir's IBS scheme $\mathcal{SH}$-$\mathcal{IBS}$.

Algorithm $\mathsf{Setup}(1^k)$**:**
$(N, e, d) \xleftarrow{\$} \mathsf{K}_{\mathrm{rsa}}(1^k)$; $mpk \leftarrow (N, e)$; $msk \leftarrow (N, e, d)$
return (mpk, msk)

Algorithm $\mathsf{KeyDer}(msk, id)$**:**
Parse msk as (N, e, d) ; $x \leftarrow \mathrm{H}(id)^d \bmod N$
return $usk \leftarrow (N, e, x)$

Algorithm $\mathsf{Sign}(usk, id, M)$**:**
$(N, e, x) \leftarrow usk$; $t \xleftarrow{\$} \mathbb{Z}_N^*$; $T \leftarrow t^e \bmod N$; $c \leftarrow \mathrm{G}(T \| M)$; $s \leftarrow xt^c \bmod N$
return $\sigma \leftarrow (T, s)$

Algorithm $\mathsf{Vf}(mpk, id, M, \sigma)$**:**
$(N, e) \leftarrow mpk$; $(T, s) \leftarrow \sigma$
If $s^e = \mathrm{H}(id)T^{\mathrm{G}(T\|M)} \bmod N$ then $d \leftarrow 1$ else $d \leftarrow 0$
return d

Other instantiations of the cSI-2-IBS transform sketched in [3] include the RSA-based Guillou-Quisquater ($\mathcal{GQ}$-$\mathcal{IBS}$) scheme [25], the factoring-based iterated-root ($\mathcal{ItR}$-$\mathcal{IBS}$) scheme [19,18,29], and the pairing-based Cha-Cheon ($\mathcal{ChCh}$-$\mathcal{IBS}$) scheme [11,34]. We refer to [3] for a more complete overview. The $\mathcal{BNN}$-$\mathcal{IBS}$ [3] and $\mathcal{BBMQ}$-$\mathcal{IBS}$ [2] schemes bear some similarity to schemes derived via the cSI-2-IBS transform, but fail to be captured by it. They were proved secure in the random oracle model under the discrete logarithm assumption and the q-strong Diffie-Hellman assumption, respectively.

5. Constructions from Hierarchical Identity-Based Encryption

As noted by Naor [7, Section 6] and formalized in [15], the key derivation of an identity-based encryption (IBE) scheme immediately gives rise to a standard

signature scheme. Similarly, Gentry and Silverberg [22] observed that any two-level hierarchical identity-based encryption (HIBE) scheme (which is a natural extension of an IBE allowing for hierarchical key delegation) can be transformed into an IBS scheme. We revisit their transformation in this section.

5.1. Hierarchical Identity-Based Encryption.

A hierarchical identity $\vec{id}$ of depth d is a tuple $\vec{id} = (id_1, \ldots, id_d)$, where $id_i \in \{0,1\}^*$. We say that $\vec{id}$ of depth d is an ancestor of $\vec{id}'$ of depth d' if $\vec{id}$ is a proper prefix of $\vec{id}'$, i.e., if $d \leq d'$ and $id_i = id'_i$, for all $1 \leq i \leq d$. If $\vec{id}$ has depth 0 then it is the empty string ϵ. Note that ϵ is a ancestor of any hierarchical identity.

A *hierarchical identity-based encryption* (HIBE) scheme of depth D is a tuple of polynomial-time algorithms $\mathcal{HIBE} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Enc}, \mathsf{Dec})$. The first three may be randomized but the last is not. The trusted key distribution center runs the setup algorithm Setup on input 1^k to obtain a master public and secret key pair (mpk, msk). As a convention, the user secret key of $\vec{id} = \epsilon$ is the master secret key msk. When a user with hierarchical identity $\vec{id}$ wants to generate the secret key for a descendant $\vec{id}'$, it runs the key derivation algorithm KeyDer on input its own user secret key $usk_{\vec{id}}$ and the identity $\vec{id}'$. The resulting user secret key is assumed to be securely communicated to the user in question. On input $mpk, \vec{id}, M$, the encryption algorithm Enc returns a ciphertext C of M for hierarchical identity $\vec{id}$. On input $usk_{\vec{id}}$ and a ciphertext C, the decryption algorithm Dec returns a message M, or $\perp$ when the ciphertext is invalid. Correctness requires that $\mathsf{Dec}(usk_{\vec{id}}, \mathsf{Enc}(mpk, \vec{id}, M)) = M$ with probability one for all $k \in \mathbb{N}$ and $\vec{id}, M$ whenever the keys $mpk, M, usk_{\vec{id}}$ are generated as indicated above. As a special case, an IBE scheme is a HIBE of depth $D = 1$.

The common security notion of HIBE schemes is indistinguishability against chosen-plaintext attacks [22] (ind-id-cpa). Here we only require the HIBE to be one-way against chosen-plaintext attacks (ow-id-cpa), a slightly weaker notion that only requires it to be hard to decrypt encryptions of random messages (as opposed to adversarially-chosen ones).

5.2. The HIBE-2-IBS *Transformation*

The idea of this transformation is to use the user secret key of $\vec{id} = (id, M)$ as the identity-based signature of M under identity id. Given the user secret key usk_{id} of id, the hierarchical key derivation algorithm can be used for signing. Verification is done by checking whether the encryption of a random message under identity (id, M) decrypts correctly when using the signature as decryption key. More formally, given $\mathcal{HIBE} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Enc}, \mathsf{Dec})$ of depth $D = 2$ with message space $MsgSp$, we build $\mathcal{IBS} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Sign}, \mathsf{Vf}) = \text{HIBE-2-IBS}(\mathcal{HIBE})$ as given in Scheme 5.

One can prove that if $\mathcal{HIBE}$ is ow-id-cpa secure, then HIBE-2-IBS($\mathcal{HIBE}$) is uf-cma secure. In contrast to the cSI-2-IBS transformation from Section 4, this transformation does not rely on the random oracle model, so when instantiated with a HIBE scheme that is ow-id-cpa secure in the standard model, one obtains an IBS scheme that is uf-cma secure in the standard model as well.

Scheme 5 The scheme $\mathcal{IBS}$ = HIBE-2-IBS($\mathcal{HIBE}$).

Algorithm $\mathsf{Sign}(usk_{id}, M)$**:**
$\vec{id} \leftarrow (id, M)$; $\sigma \xleftarrow{\$} \mathsf{KeyDer}(usk_{id}, \vec{id})$
return σ

Algorithm $\mathsf{Vf}(mpk, id, M, \sigma)$**:**
$\vec{id} \leftarrow (id, M)$; $M' \xleftarrow{\$} MsgSp$; $C \xleftarrow{\$} \mathsf{Enc}(mpk, \vec{id}, M')$
If $\mathsf{Dec}(usk_{\vec{id}} = \sigma, C) = M'$ then $d \leftarrow 1$ else $d \leftarrow 0$
return d

The verification algorithm above works generically for any HIBE scheme, but for most concrete instantiations a more efficient deterministic test exists. Also, while the generic transformation yields uf-cma security of the IBS scheme under the same assumption as the HIBE scheme, the IBS scheme can usually be proved secure under a weaker assumption via a direct proof.

5.3. Instantiations

The first practical HIBE construction was the $\mathcal{GS}$-$\mathcal{HIBE}$ due to Gentry and Silverberg [22], which through the HIBE-2-IBS transformation leads to the $\mathcal{GS}$-$\mathcal{IBS}$ scheme that was also mentioned in [22]. Its security is based on the CDH assumption in groups equipped with bilinear maps in the random oracle model. We briefly describe the scheme here.

For simplicity we restrict our attention to symmetric pairings $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ generated by a polynomial-time *pairing generator* K_{pair}. On input 1^k this algorithm outputs $pars = (\mathbb{G}, \mathbb{G}_T, \hat{e}, p, g)$ where $\mathbb{G}, \mathbb{G}_T$ are descriptions of an additive group $\mathbb{G}$ and a multiplicative group $\mathbb{G}_T$ of the same prime order p, P is a generator of $\mathbb{G}$, and $\hat{e}$ is the description of a non-degenerate computable bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. The computational Diffie-Hellman (CDH) problem in $\mathbb{G}$ associated to K_{pair} is said to be hard if

$$\mathbf{Adv}^{\text{cdh}}_{\mathsf{K}_{\text{pair}},\mathsf{A}}(k) \;=\; \Pr[\mathsf{A}(pars, aP, bP) = abP \;:\; pars \xleftarrow{\$} \mathsf{K}_{\text{pair}}(1^k) \;;\; a, b \xleftarrow{\$} \mathbb{Z}_p]$$

is negligible in k for any polynomial-time algorithm A. The assumption that CDH is hard is a weaker assumption than the Bilinear CDH assumption used by Boneh and Franklin [8] which states that, given (aP, bP, cP), computing $\hat{e}(P, P)^{abc}$ is hard.

The Setup and KeyDer algorithms of the $\mathcal{GS}$-$\mathcal{HIBE}$ scheme are as follows. The master secret key msk is a random exponent $x \xleftarrow{\$} \mathbb{Z}_p$, the master public key mpk contains a pairing description $pars$ generated by $\mathsf{K}_{\text{pair}}(1^k)$ and the element $X \leftarrow xP$. The user secret key of an identity id_1 at the first level is $usk_{id_1} \leftarrow x \cdot \mathrm{H}(id_1)$, where $\mathrm{H} : \{0,1\}^* \to \mathbb{G}$ is a public hash function, modeled as a random oracle. The user secret key of an second-level identity $\vec{id} = (id_1, id_2)$ is a pair (R, S) where $R \leftarrow rP$ for a random $r \xleftarrow{\$} \mathbb{Z}_p$ and $S \leftarrow usk_{id_1} + r \cdot \mathrm{H}(id_1, id_2)$. Applying the HIBE-2-IBS transform and using a more efficient verification test yields the $\mathcal{GS}$-$\mathcal{IBS}$ scheme given in Scheme 6.

Scheme 6 The $\mathcal{GS}$-$\mathcal{IBS}$ scheme.

Algorithm $\mathsf{Setup}(1^k)$**:**
$pars \xleftarrow{\$} \mathsf{K}_{\mathrm{pair}}(1^k)$; $x \xleftarrow{\$} \mathbb{Z}_p$; $X \leftarrow xP$; $mpk \leftarrow (pars, X)$; $msk \leftarrow (pars, x)$
return (mpk, msk)

Algorithm $\mathsf{KeyDer}(msk, id)$**:**
$(pars, x) \leftarrow msk$
return $usk_{id} \leftarrow x \cdot \mathrm{H}(id)$

Algorithm $\mathsf{Sign}(usk_{id}, M)$**:**
$r \xleftarrow{\$} \mathbb{Z}_p$; $R \leftarrow rP$; $S \leftarrow usk_{id} + r \cdot \mathrm{H}(id, M)$
return $\sigma \leftarrow (R, S)$

Algorithm $\mathsf{Vf}(mpk, id, M, \sigma)$**:**
Parse mpk as $(pars, X)$ and σ as (R, S)
If $\hat{e}(g, S) = \hat{e}(\mathrm{H}(id), X) \cdot \hat{e}(R, \mathrm{H}(id, M))$ then $d \leftarrow 1$ else $d \leftarrow 0$
return d

The $\mathcal{GS}$-$\mathcal{HIBE}$ scheme is ow-id-cpa secure in the random oracle model if the Bilinear CDH problem in $pars = (\mathbb{G}, \mathbb{G}_{\mathrm{T}}, \hat{e}, p, g)$ associated to $\mathsf{K}_{\mathrm{pair}}$ is hard. With a direct proof the $\mathcal{GS}$-$\mathcal{IBS}$ scheme can be proved to be uf-cma secure under the weaker CDH assumption.

Another IBS scheme $\mathcal{BB}$-$\mathcal{IBS}$ with the same security properties can be obtained by transforming the random-oracle variant of the HIBE proposed by Boneh and Boyen [4]. Waters [33] proposed a HIBE scheme that is ow-id-cpa secure under the Bilinear CDH assumption in the standard model. The HIBE-2-IBS transformation yields the $\mathcal{Waters}$-$\mathcal{IBS}$ scheme that was directly proposed in [30]. The HIBE scheme due to Boneh, Boyen and Goh [6] can be combined with Waters' techniques to obtain a HIBE scheme [12,27] that is ow-id-cpa secure under some variant of the Bilinear CDH assumption in the standard model. Again, applying the HIBE-2-IBS transform and using a more efficient verification test yields the $\mathcal{BBG}$-$\mathcal{IBS}$ scheme given in Scheme 7.

Here we assume that identities and messages are bit-stings from $\{0,1\}^n$. For arbitrary identities and messages one can use a collision-resistant hash function with image $\{0,1\}^n$, where $n = 2k$ (due to the birthday paradox). The $\mathcal{BBG}$-$\mathcal{IBS}$ scheme has a particularly short signature sizes of only two elements of $\mathbb{G}$, matching the signature size of the (random-oracle) $\mathcal{GS}$-$\mathcal{IBS}$ scheme. Using a direct proof its uf-cma security can proved under the mCDH assumption which states that given (aP, bP, b^2P), computing abP is hard. The drawback of the $\mathcal{BBG}$-$\mathcal{IBS}$ scheme are its relatively large public parameters and (user) secret keys.

6. Efficiency and Security Comparison

Table 1 gives an overview of the efficiency and security properties of the IBS schemes covered in this chapter. For each scheme it displays the transform through which the IBS scheme was obtained (if any), the signature size, the dominating

Scheme 7 The *BBG-IBS* scheme.

Algorithm $\mathsf{Setup}(1^k)$**:**
$pars \xleftarrow{\$} \mathsf{K}_{\mathrm{pair}}(1^k)$; $X \xleftarrow{\$} \mathbb{G}$; $Y \leftarrow \hat{e}(X, P)$
$\mathbf{U} = (U_0, \ldots, U_n) \xleftarrow{\$} \mathbb{G}^{n+1}$; $\mathbf{V} = (V_1, \ldots, V_n) \xleftarrow{\$} \mathbb{G}^n$
$mpk \leftarrow (pars, Y, \mathbf{U}, \mathbf{V})$; $msk \leftarrow (pars, X, \mathbf{U}, \mathbf{V})$
return (mpk, msk)

Algorithm $\mathsf{KeyDer}(msk, id)$**:**
Parse msk as $(pars, X, \mathbf{U}, \mathbf{V})$; $r \xleftarrow{\$} \mathbb{Z}_p$
$R_1 \leftarrow rP$; $R_2 \leftarrow X + r \cdot (U_0 + \sum_{i=1}^{n} id_i \cdot U_i)$
For $i = 1, \ldots, n$ do $W_i \leftarrow rV_i$
$usk \leftarrow (pars, \mathbf{U}, \mathbf{V}, R_1, R_2, W_1, \ldots, W_n)$
return usk

Algorithm $\mathsf{Sign}(usk, id, M)$**:**
Parse usk as $(pars, \mathbf{U}, \mathbf{V}, R_1, R_2, W_1, \ldots, W_n)$
$s \xleftarrow{\$} \mathbb{Z}_p$; $S_1 \leftarrow R_1 + sP$; $S_2 \leftarrow R_2 + s \cdot (U_0 + \sum_{i=1}^{n} id_i \cdot U_i) + \sum_{i=1}^{n} M_i \cdot (W_i + sV_i)$
return $\sigma \leftarrow (S_1, S_2) \in \mathbb{G}^2$

Algorithm $\mathsf{Vf}(mpk, id, M, \sigma)$**:**
Parse mpk as $(pars, Y, \mathbf{U}, \mathbf{V})$ and σ as (S_1, S_2)
If $\hat{e}(S_2, P) = Y \cdot \hat{e}(S_1\ ,\ U_0 + \sum_{i=1}^{n} id_i \cdot U_i + M_i \cdot V_i)$ then $d \leftarrow 1$ else $d \leftarrow 0$
return d

computational overhead of signing and verification, the security assumption under which the IBS scheme has been proved secure, and whether this proof is in the random-oracle model (ROM) or the standard model (SM).

For the certificate-based scheme *Cert-IBS* all properties are denoted in terms of the underlying standard signature scheme. The numbers for the RSA- and factoring-based schemes *Sh-IBS*, *GQ-IBS*, and *ItR-IBS* are stated in terms of elements (el.), multiplications (mult.), exponentiations (exp.), and multi-exponentiations (mexp.) in the group $\mathbb{Z}_N^*$ where N is the product of two large primes. For the pairing-based schemes *ChCh-IBS*, *GS-IBS*, *Waters-IBS*, *BBG-IBS*, and *BBMQ-IBS*, we consider symmetric pairings $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathrm{T}}$ over groups of prime order p. Signature sizes and computational overhead are given in terms of elements (el.) of $\mathbb{G}$ or $\mathbb{Z}_p$; exponentiations (exp.) in $\mathbb{G}$ or $\mathbb{G}_{\mathrm{T}}$; and pairing evaluations (pairings). (Note that we follow the popular convention to refer to multiplication in the additive group $\mathbb{G}$ as exponentiations.) Computing a sum $U_0 + \sum_{i=1}^{n} id_i \cdot U_i$ takes $n+1$ multiplications (i.e., additions in the group) in $\mathbb{G}$, which for $n = 2k = \log_2 |\mathbb{G}|$ takes about half the time of an exponentiation in G using the "square-and-multiply" method. For the discrete-logarithm based *BNN-IBS* scheme, we consider multiplicative groups $\mathbb{G}$ of prime order p. Values are in terms of elements (el.) of $\mathbb{G}$ and $\mathbb{Z}_p$, exponentiations (exp.) and multi-exponentiations (mexp.) in $\mathbb{G}$.

Table 1. Efficiency and security comparison of all treated IBS schemes.

Scheme	Transform	Sig. size	Signing time	Verif. time	Sec. assumption	ROM/SM
Cert-IBS	SS-2-IBS	2 sig. of $\mathcal{SS}$ 1 pk of $\mathcal{SS}$	1 Sign of $\mathcal{SS}$	2 Vf of $\mathcal{SS}$	$\mathcal{SS}$ is uf-cma	SM
Sh-IBS	cSI-2-IBS	2 el. of $\mathbb{Z}_N^*$	2 exp. in $\mathbb{Z}_N^*$	1 mexp in $\mathbb{Z}_N^*$	RSA	ROM
GQ-IBS	cSI-2-IBS	2 el. of $\mathbb{Z}_N^*$	2 exp. in $\mathbb{Z}_N^*$	1 mexp in $\mathbb{Z}_N^*$	RSA	ROM
ItR-IBS	cSI-2-IBS	2 el. of $\mathbb{Z}_N^*$	$O(k)$ mult. in $\mathbb{Z}_N^*$	$O(k)$ mult. in $\mathbb{Z}_N^*$	factoring	ROM
ChCh-IBS	cSI-2-IBS	2 el. of $\mathbb{G}$	2 exp. in $\mathbb{G}$	2 pairings	CDH in $\mathbb{G}$	ROM
BNN-IBS	direct	3 el. of $\mathbb{G}$ 1 el. of $\mathbb{Z}_p$	1 exp. in $\mathbb{G}$	1 mexp in $\mathbb{G}$ 1 exp. in $\mathbb{G}$	discrete log	ROM
BBMQ-IBS	direct	1 el. of $\mathbb{G}$ 1 el. of $\mathbb{Z}_p$	2 exp. in $\mathbb{G}$	1 pairing 1 exp. in $\mathbb{G}_T$	ℓ-SDH in $\mathbb{G}$	ROM
GS-IBS	HIBE-2-IBS	2 el. of $\mathbb{G}$	2 exp. in $\mathbb{G}$	3 pairings	CDH in $\mathbb{G}$	ROM
Waters-IBS	HIBE-2-IBS	3 el. of $\mathbb{G}$	1.5 exp. in $\mathbb{G}$	3 pairings 0.5 exp. in $\mathbb{G}$	CDH in $\mathbb{G}$	SM
BBG-IBS	HIBE-2-IBS	2 el. of $\mathbb{G}$	2 exp. in $\mathbb{G}$	2 pairings 0.5 exp. in $\mathbb{G}$	mCDH in $\mathbb{G}$	SM

7. Extensions

7.1. Hierarchical Identity-Based Signatures

Similar to the concept of hierarchical identity-based encryption (HIBE) one can also consider the concept of hierarchical identity-based signatures (HIBS) [22]. Here hierarchical identities are tuples of identities $\vec{id} = (id_1, \ldots, id_d)$, and user secret keys for hierarchical identity $\vec{id}'$ can be derived by the owner of the user secret key from some ancestor $\vec{id}$ of $\vec{id}'$. In analogy with the certification approach for IBS schemes, Kiltz et al. [26] showed how to construct HIBS schemes from SS schemes using certificate chains. Also, analogously to the HIBE-2-IBS transform, more efficient d-level HIBS schemes can be constructed from $(d+1)$-level HIBE schemes.

7.2. Identity-Based Signatures with Special Properties

In order to satisfy the needs of some specific scenarios such as electronic commerce, cash, voting, or auctions, the original concept of a digital signature has been extended and modified in multiple ways, giving rise to many kinds of digital signatures with "special properties", including blind signatures [13], threshold signatures [16], and aggregated signatures [9]. Originally, these extensions were introduced for the (certificate-based) public-key setting, but nothing prohibits extending them to the identity-based setting.

7.2.1. The Certification Approach

The easiest way to construct IBS schemes with special properties is to again follow the certification approach from Section 3. A signature then consists of two parts: a standard signature with special properties on the message using a standard secret key, and a certificate that links the corresponding public key to the identity of the user. The latter can be implemented using a standard signature scheme. As shown by Galindo et al. [20], this construction works for many types of identity-based signatures with special properties such as proxy signatures, blind signatures, verifiably encrypted signatures, undeniable signatures, forward-secure signatures, strong key insulated signatures, online/offline signatures, threshold signatures, and aggregate signatures. However, the same approach does not seem to work in settings when additional public keys have to be used in the protocol, different from that of the signer. This includes ring, designated verifier, confirmer, nominative, and chameleon signatures. For these kinds of signatures, therefore, it makes more sense to consider specific constructions in the identity-based framework.

7.2.2. Verifiably Encrypted Signatures

As an example of IBS schemes with special properties, let us consider ID-based verifiably encrypted signatures. Verifiably encrypted signature (VES) schemes can be seen as a special extension of the standard signature primitive. VES schemes enable the signer to create a signature that is encrypted using an adjudicator's public key (the VES signature), but in such a way that public verification of the

signature remains possible. The adjudicator is a trusted third party, who can reveal the plaintext signature when needed. VES schemes provide an efficient way to enable fairness in many practical applications such as contract signing. Compared to a standard signature a VES scheme has three additional algorithms: VES signing/verification (with respect to an adjudicator's public key), and adjudication. Here the adjudication algorithm inputs an adjudicator's secret key and transforms a VES into a standard signature.

Identity-based verifiably encrypted signature (IB-VES) schemes were introduced in [24] where also a concrete instantiation based on bilinear maps was proposed. For the generic certificate-based construction, VES signing and verification can be lifted to the identity-based case using certificates following the techniques from Section 3. IB-VES signing replaces σ with its VES counterpart by running the VES signing algorithm on sk, M, and the adjudicator's public key. IB-VES verification checks the certificate and the VES using the standard VES verification algorithm.

An efficient VES scheme in the random oracle model based on pairings was given in [9], one in the standard model in [28]. It was further noted in [28] that VES schemes can be constructed on general assumptions such as trapdoor one-way permutations. Therefore the generic construction yields an IB-VES scheme based on any trapdoor one-way function [28], and a more efficient one using [9].

References

[1] Michel Abdalla, Jee Hea An, Mihir Bellare, and Chanathip Namprempre. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In Lars R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 418–433. Springer Verlag, 2002.

[2] Paulo S. L. M. Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In Bimal K. Roy, editor, *Advances in Cryptology – ASIACRYPT 2005*, volume 3788 of *Lecture Notes in Computer Science*, pages 515–532. Springer Verlag, 2005.

[3] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 268–286. Springer Verlag, 2004. Full version available from Cryptology ePrint Archive, Report 2004/252.

[4] Dan Boneh and Xavier Boyen. Efficient selective-ID secure identity based encryption without random oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer Verlag, 2004.

[5] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73. Springer Verlag, 2004.

[6] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 440–456. Springer Verlag, 2005.

[7] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer Verlag, 2001.

[8] Dan Boneh and Matthew K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[9] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer Verlag, 2003.

[10] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer Verlag, 2001.

[11] Jae Choon Cha and Jung Hee Cheon. An identity-based signature from gap Diffie-Hellman groups. In Yvo Desmedt, editor, *PKC 2003: 6th International Workshop on Theory and Practice in Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 18–30. Springer Verlag, 2003.

[12] Sanjit Chatterjee and Palash Sarkar. New constructions of constant size ciphertext HIBE without random oracle. In Min Surp Rhee and Byoungcheon Lee, editors, *ICISC 06: 9th International Conference on Information Security and Cryptology*, volume 4296 of *Lecture Notes in Computer Science*, pages 310–327. Springer Verlag, 2006.

[13] David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology – CRYPTO'82*, pages 199–203. Plenum Press, 1983.

[14] Ronald Cramer and Victor Shoup. Signature schemes based on the strong RSA assumption. In *ACM CCS 99: 6th Conference on Computer and Communications Security*, pages 46–51. ACM Press, 1999.

[15] Yang Cui, Eiichiro Fujisaki, Goichiro Hanaoka, Hideki Imai, and Rui Zhang. Formal security treatments for signatures from identity-based encryption. In *Provable Security*, volume 4786 of *Lecture Notes in Computer Science*, pages 218–227. Springer, 2007.

[16] Yvo Desmedt. Society and group oriented cryptography: A new concept. In Carl Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 120–127. Springer Verlag, 1988.

[17] Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung. Strong key-insulated signature schemes. In Yvo Desmedt, editor, *PKC 2003: 6th International Workshop on Theory and Practice in Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 130–144. Springer Verlag, 2003.

[18] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.

[19] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *Advances in Cryptology – CRYPTO'86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer Verlag, 1987.

[20] David Galindo, Javier Herranz, and Eike Kiltz. On the generic construction of identity-based signatures with additional properties. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 178–193. Springer Verlag, 2006.

[21] Rosario Gennaro, Shai Halevi, and Tal Rabin. Secure hash-and-sign signatures without the random oracle. In Jacques Stern, editor, *Advances in Cryptology – EUROCRYPT'99*, volume 1592 of *Lecture Notes in Computer Science*, pages 123–139. Springer Verlag, 1999.

[22] Craig Gentry and Alice Silverberg. Hierarchical ID-based cryptography. In Yuliang Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer Verlag, 2002.

[23] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, April 1988.

[24] C. Gu and Y. Zhu. An id-based verifiable encrypted signature scheme based on Hess's scheme. In *CISC'05*, pages 42–52, 2005.

[25] Louis C. Guillou and Jean-Jacques Quisquater. A "paradoxical" indentity-based signature scheme resulting from zero-knowledge. In Shafi Goldwasser, editor, *Advances in Cryptol-*

ogy – CRYPTO'88, volume 403 of *Lecture Notes in Computer Science*, pages 216–231. Springer Verlag, 1990.

[26] Eike Kiltz, Anton Mityagin, Saurabh Panjwani, and Barath Raghavan. Append-only signatures. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *ICALP 2005: 32nd International Colloquium on Automata, Languages and Programming*, volume 3580 of *Lecture Notes in Computer Science*, pages 434–445. Springer Verlag, 2005.

[27] Eike Kiltz and Yevgeniy Vahlis. CCA2 Secure IBE: Standard model efficiency through authenticated symmetric encryption. In *CT-RSA*, volume 4964 of *Lecture Notes in Computer Science*, pages 221–239. Springer, 2008.

[28] Steve Lu, Rafail Ostrovsky, Amit Sahai, Hovav Shacham, and Brent Waters. Sequential aggregate signatures and multisignatures without random oracles. In Serge Vaudenay, editor, *Advances in Cryptology – EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 465–485. Springer Verlag, 2006.

[29] H. Ong and Claus-Peter Schnorr. Fast signature generation with a Fiat-Shamir-like scheme. In Ivan Damgård, editor, *Advances in Cryptology – EUROCRYPT'90*, volume 473 of *Lecture Notes in Computer Science*, pages 432–440. Springer Verlag, 1990.

[30] Kenneth G. Paterson and Jacob C. N. Schuldt. Efficient identity-based signatures secure in the standard model. In *ACISP*, volume 4058 of *LNCS*, pages 207–222. Springer, 2006.

[31] John Rompel. One-way functions are necessary and sufficient for secure signatures. In *22nd Annual ACM Symposium on Theory of Computing*, pages 387–394. ACM Press, 1990.

[32] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer Verlag, 1985.

[33] Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer Verlag, 2005.

[34] Xun Yi. An identity-based signature scheme from the Weil pairing. *IEEE Communications Letters*, 7(2):76–78, February 2003.