Constant-Size Hierarchical Identity-Based Signature/Signcryption without Random Oracles

Tsz Hon Yuen and Victor K. Wei

Dep. of Information Engineering, Chinese Univ. of Hong Kong, Shatin, Hong Kong
thyuen4,kwwei@ie.cuhk.edu.hk

November 16, 2005

Abstract. We propose a hierarchical identity-based signature (HIBS) scheme which is provable in the standard model. The signature size is independent to the level of the hierarchy. Combining with existing hierarchical identity-based encryption (HIBE) schemes, we obtain a hierarchical identity based signcryption (HIBSC) scheme which is provable in the standard model and whose size is independent of the level of the hierarchy.

Key words: Hierarchical identity-based signature, signcryption, bilinear pairings, random oracles

1 Introduction

Identity based cryptosystem [27] is a public key cryptosystem where the public key can be an arbitrary string such as an email address. A trusted authority (TA) uses a master secret key to issue private keys to identities that request them. For an Identity Based Encryption (IBE) scheme, Alice can securely encrypt a message to Bob using Bob's identity, such as email address, as the public key. For an Identity Based Signature (IBS) scheme, Alice can sign a message using her private key that corresponds to an unambiguous name of hers, such as email address. Then anybody can verify the authenticity of the signature from the name. An Identity Based SignCryption (IBSC) scheme is the combination of IBE and IBS with a common set of parameters and keys. With such infrastructure, it can achieve an increase in efficiency and an improvement in security.

Hierarchical IBE (HIBE) [22, 25] is a generalization of IBE that mirrors the hierarchy of organizations. An identity at level ℓ of the hierarchy tree can issue private keys to its descendant identities, but cannot decrypt messages intended for other identities. In particular, an IBE is an 1-level HIBE. Combining with Hierarchical IBS (HIBS) originated from the same idea, [17] proposed the concept of Hierarchical IBSC (HIBSC).

Many reductionist security proofs concerning identity based cryptosystems and other cryptosystems used the random oracle model [3]. Several papers proved that some popular cryptosystems previously proved secure in the random oracle are actually provably insecure when the random oracle is instantiated by any real-world hashing functions [14, 2]. Therefore identity based cryptosystems provably secure in the standard model attract a great interest. Several IBE schemes [15, 4, 24] are proposed which is secure without random oracles under a weaker "selective-ID" model [15]. Recently, Boneh and Boyen [5] and Waters [28] proposed IBE schemes which are provably secure without random oracles under the strong model of [9].

Several recent IBE schemes [4, 5, 28] achieve chosen ciphertext security without random oracles from their HIBE counterparts. They used the result of [16, 10, 8] that any chosen plaintext secure $(\ell+1)$-level HIBE scheme can be used to construct a chosen ciphertext secure ℓ-level HIBE scheme.

It is natural to ask whether other efficient hierarchical identity based cryptosystems are secure without random oracles. In this paper, we provide an affirmative answer by constructing an HIBS

and HIBSC schemes which can be provably secure in the standard model. Our approach is motivated by the above-mentioned results concerning HIBE. We construct a ℓ-level HIBS scheme from a weaker $(\ell+1)$-level HIBS scheme.

1.1 Our Contribution

We make the following contributions:

- The *first* constant-size hierarchical identity based signature (HIBS) scheme. It is existentially unforgeable providing the Diffie-Hellman Inversion (DHI) Assumption in the saID model without random oracles. The saID (sample-ID) model is a slightly weaker model related to the sID (select-ID) model of [15].
- A transformation theorem in the style of transformation theorems in [23, 16, 10, 8], that links the security of an $(\ell+1)$-level HIBS and the security of an ℓ-level HIBS. A persistent technical difficulty regarding the use of sID model in the transformation theorem was overcome by using our saID model.
- The *first* constant-size identity based signcryption (IBSC) and hierarchical identity based signcryption (HIBSC) scheme which are provably secure in the standard model.

1.2 Related Results

Most existing practical signature schemes are provably secure in the random oracle model. [21] proposed a variant of hash-and-sign RSA signature scheme, which is provably secure without random oracles, by the strong RSA assumption. A different approach is proposed in [18], and further improvements are proposed in [20]. [11] proposed a signature scheme provably secure under discrete-log type assumption in the standard model, but the signature size is long. [6] proposed a short signature scheme secure without random oracles, under the new q-SDH assumption.

Shamir [27] suggested an identity-based signature scheme. Boneh and Franklin [9] proposed the first practical identity-based encryption scheme, which is provably secure in the random oracle model. Several IBE schemes [15, 4, 24] are proposed which is secure without random oracles under a weaker "selective-ID" model [15]. Recently, Boneh and Boyen [5] and Waters [28] proposed identity based encryption scheme which is provably secure without random oracles under the model of [9]. Recently [13] proposed an identity based signature without random oracles, but their reduction is tight only if they use the "selective-ID" model.

Zheng [31] proposed that encryption and signature can be combined as "signcryption" which can be more efficient in computation than running encryption and signature separately. There are some papers (e.g. [26, 12, 29]) concerning the combination of identity-based signature and encryption to form identity based signcryption schemes. These papers are provably secure only in the random oracle model.

Hierarchical identity based cryptography was proposed in [22] and [25] proposed another hierarchical identity based encryption. HIBE without random oracles are proposed in [4, 5, 28, 7]. Hierarchical identity based signcryption is firstly proposed in [17].

Recently, Boneh et al. [8] (preliminary papers [16, 10]) suggested some methods to obtain CCA-secure encryption schemes from identity based encryption. In particular, this technique can be applied to construct CCA-secure hierarchical identity based encryption.

Classic methods of constructing fully secure signatures from combining *hierarchical authentication tree* and *one-time signatures* can be found in [23]. Various instantiations and modifications are

Type	Scheme	Security	Model	Size
ℓ-HIBS	Auth-tree	Full ACP	Standard	$O(\ell\lambda_s)$
	This paper	saID-ACP	Standard	$O(\lambda_s)$
IBS	Auth-tree	Full ACP	Standard	$O(\lambda_s)$
Standard Signature	[21, 18, 6]	ACP	Standard	$O(\lambda_s)$

Table 1. Recent results on signatures, IBS, and HIBS. Auth-tree means combining *hierarchical authentication tree* and *one-time signatures*. Full ACP means the scheme is secure against adaptive chosen identity and adaptive chosen message attack. sa-ID ACP means the scheme is secure against sample identity and adaptive chosen message attack. ℓ is the number of hierarchy level and λ_s is the security parameter.

Type	Scheme	Security	Model	Size
ℓ-HIBE	[8] + ?	Full CCA	Standard	$O(\ell\lambda_s)$
	[8] + [7]	sID-CCA	Standard	$O(\lambda_s)$
IBE	[28]	Full CCA	Standard	$O(\lambda_s)$
Standard Encryption	Cramer-Shoup/OAEP/ [8]+sID-CCA IBE	CCA	Standard	$O(\lambda_s)$

Table 2. Recent results on encryptions, IBE, and HIBE. Full CCA means the scheme is secure against adaptive chosen identity and adaptive chosen ciphertext attack. sID-CCA means the scheme is secure against selective identity and adaptive chosen ciphertext attack. ℓ is the number of hierarchy level and λ_s is the security parameter. The first row means that full CCA secure HIBE can be achieved by using [8] and an adaptive chosen identity and chosen plaintext secure HIBE. However no existing scheme achieves this with a tight security reduction.

also well-known [16, 10, 8]. We observe that some of these hierarchical authentication tree instantiations bear a striking resemblance to the multi-level authentication tree structure in HIBS. User identity can be authenticated by his parent, by signing an IBS on the user's identity. The parent's identity can be authenticated again by one level higher, and the process repeats up until the root. If in each level, the authentication of user identity is secure in the standard model, and finally the lowest level user signature is secure against adaptive chosen message attack in the standard model, then the entire HIBS scheme is Full ACP secure in the standard model. However this solution will increase the signature size by the level of hierarchy. To achieve $O(\lambda_s)$ size HIBS, we need to lower the security level to sample ID-ACP (which will be defined later). We can see that the same case applies for HIBE using sID-CCA. The recent results are summarized in table 1, 2 and 3.

1.3 Organization

In section 2, we give some background knowledges. In section 3, we give the definition for the security model for HIBS. In section 4, we show that how we obtain a secure HIBS. In section 5, we give an efficient instantiation. In section 6, we describe how our result can be applied to signcryption schemes. In section 7, we conclude our paper.

2 Preliminaries

2.1 Pairings

Our scheme uses bilinear pairings on elliptic curves. We now give a brief revision on the property of pairings and some candidate hard problems from pairings that will be used later.

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p, writing the group action multiplicatively. Let g be a generator of G.

Type	Scheme	Security	Model	Size
ℓ-HIBSC	[17]	Full CCA + ACP	Random Oracle	$O(\ell\lambda_s)$
	This paper	sID-CCA + saID-ACP	Standard	$O(\lambda_s)$
IBSC	[12], [29], etc.	Full CCA + ACP	Random Oracle	$O(\lambda_s)$
	This paper	sID-CCA + saID-ACP	Standard	$O(\lambda_s)$
Standard Signcryption	[1], [19]	CCA + ACP	Standard	$O(\lambda_s)$

Table 3. Recent results on signcryption, IBSC, and HIBSC. All notations are defined in table 1 and 2. [19] showed that only standard signcryption scheme of [1] and [19] achieves the strong *insider* security model. All existing IBSC and HIBSC schemes are provably secure in the random oracles only.

Definition 1. *A map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is called a bilinear pairing if, for all $x, y \in \mathbb{G}$ and $a, b \in Z$, we have $e(x^a, y^b) = e(x, y)^{ab}$, and $e(g, g) \neq 1$.*

Definition 2. *(ℓ-DHI problem) The ℓ-Diffie-Hellman Inversion problem is that, given g,g^{α},$g^{(\alpha^2)}$, …, $g^{(\alpha^\ell)} \in \mathbb{G}$, for unknown $\alpha \in \mathbb{Z}_p^*$, to compute $g^{1/\alpha}$.*

Definition 3. *(ℓ-DHI* problem) The ℓ-Diffie-Hellman Inversion * problem is that, given g,g^{α},$g^{(\alpha^2)}$, …, $g^{(\alpha^\ell)} \in \mathbb{G}$, for unknown $\alpha \in \mathbb{Z}_p^*$, to compute $g^{(\alpha^{\ell+1})}$.*

We say that the (t, ϵ, ℓ)-DHI* assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the ℓ-DHI* problem in $\mathbb{G}$.

Definition 4. *(ℓ-wBDHI* problem) The ℓ-weak-Bilinear-Diffie-Hellman Inversion * problem is that, given g,h,g^{α},$g^{(\alpha^2)}$, …, $g^{(\alpha^\ell)} \in \mathbb{G}$ and $T \in \mathbb{G}_T$, for unknown $\alpha \in \mathbb{Z}_p^*$, decide if $T = \hat{e}(g, h)^{(\alpha^{\ell+1})}$.*

We say that the (t, ϵ, ℓ)-wBDHI* assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the ℓ-wBDHI* problem in $\mathbb{G}$.

The ℓ-DHI problem and ℓ-DHI* problem are proven equivalent in [30].

3 Security Model: HIBS and HIBSC

We present the security models for HIBS (Hierarchical Identity-Based Signatures) and for HIBSC (Hierarchical Identity-Based Signcryption).

3.1 HIBS Security Model

In identity based cryptography, the security model for IBE was proposed in [9]. Besides the decryption oracle, the adversary is also allowed to query the key extraction oracle adaptively to extract the secret key for any identity except the challenge identity. [15] proposed a weaker "selective-identity" model, where the adversary selects the challenge identity in advance, before the public parameter is generated. In this paper, we will introduce its counterpart for signature scheme, namely a "sample-identity" model.

An ℓ-level HIBS scheme handling identities of length n consists of four algorithms: (Setup, Der, Sign, Verify). The algorithms are specified as follows:

– Setup: On input a security parameter 1^{λ_s}, the TA generates $\langle \mathsf{msk}, \mathsf{param} \rangle$ where msk is the randomly generated master secret key, and param is the corresponding public parameter.

- Der: On input an identity vector $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_i)$, where all $\mathsf{id}_j \in \{0,1\}^n$ and $i < \ell$, its associated secret key SK_{ID}, and a string r, it returns the corresponding private key $SK_{\mathsf{ID}.r}$ (corresponds to param).
- Sign: On input the private key of the signer ID, SK_{ID} and a message M, it outputs a signature σ corresponding to param.
- Verify: On input the signer identity vector ID, a message M and ciphertext σ, it outputs $\top$ if σ is a valid signature of M corresponding to $\mathsf{ID}, \mathsf{param}$. Otherwise, it outputs $\perp$.

We make the correctness constraint that if $\sigma \leftarrow \mathsf{Sign}(SK_{\mathsf{ID}}, M)$, then $\top \leftarrow \mathsf{Verify}(\mathsf{ID}, M, \sigma)$.

Sample-ID Existential Unforgeability We define the existential unforgeability against sample identity and adaptive chosen message attack for HIBS, as in the following game. We define the following oracles:

- $\mathcal{KEO}$: The Key Extraction Oracle with input ID will output the corresponding secret key SK_{ID}.
- $\mathcal{SO}$: The Signing Oracle with input signer ID and message M will output a signature σ such that $\mathsf{Verify}(\mathsf{ID}, M, \sigma) = \top$.

Game EU-saID(ℓ) for HIBS schemes:

1. (*Init. Phase*) Simulator $\mathcal{S}$ generates polynomially many identity vectors $(\mathsf{ID}_1, \cdots, \mathsf{ID}_n)$ and denotes the set as $\tilde{\mathsf{ID}}$. $\mathcal{S}$ generates param and give $(\tilde{\mathsf{ID}}, \mathsf{param})$ to Adversary $\mathcal{A}$.
2. (*Probe Phase*) $\mathcal{A}$ queries $\mathcal{KEO}(\mathsf{ID})$ and $\mathcal{SO}(\mathsf{ID}, M)$, in arbitrary interleave.
3. (*End Game*) $\mathcal{A}$ delivers a signature $(\mathsf{ID}_{ga}, \sigma_{ga}, M_{ga})$, where $\mathsf{ID}_{ga} \in \tilde{\mathsf{ID}}$. ID_{ga} or its prefix have never been input to a $\mathcal{KEO}$ query or a $\mathcal{SO}$ query.

$\mathcal{A}$ *wins* if he completes the Game with $\top = \mathsf{Verify}(\mathsf{ID}_{ga}, M_{ga}, \sigma_{ga})$. Its *advantage* is its probability of winning.

Definition 5. *The ℓ-level HIBS scheme is* (t, ϵ, ℓ)-EU-saID *secure if no algorithm that runs in time t has an advantage ϵ.*

In this paper, we will consider a HIBS scheme using with a strong one-time signature scheme (OTS) in the later section. Let $\mathsf{IdGen}(1^{\lambda_s}, \ell) \xrightarrow{Sa} (Ra)^\ell$ be a fair random sampling function, where Ra is the range of the identities. We will drop the 1^{λ_s} for convenience. For a OTS scheme, it has $(\mathcal{G}, \mathcal{SIG}, \mathcal{V})$ protocol for key generation, signing and verification respectively, where the keys are in Ra. We will define the combined security model here.

Game EU-saID-ACP-wOTS(ℓ) for HIBS schemes with OTS (one-time signature):

1. (*Init. Phase*) $\mathcal{S}$ invokes $\mathsf{IdGen}(\ell)$ to generate polynomially many $\mathbf{I}_1, \cdots, \mathbf{I}_{n_1} \in (Ra)^\ell$ and denotes the set as $\tilde{\mathbf{I}}$. It invokes $\mathsf{IdGen}(1)$ to generate polynomially many $I_1, \cdots, I_{n_2} \in Ra$ and denotes the set as $\tilde{I}$. $\mathcal{S}$ generates param and give $(\tilde{\mathbf{I}}, \tilde{I}, \mathsf{param})$ to $\mathcal{A}$.
2. (*Probe Phase*) $\mathcal{A}$ queries $\mathcal{KEO}(\mathbf{I})$, $\mathcal{SO}(\mathbf{I}, M)$, for $\mathbf{I} \in (Ra)^\ell$, in arbitrary interleave.
3. (*End Game*) $\mathcal{A}$ delivers a signature $(\mathbf{I}_{ga}, I_{ga}, \sigma_{ga}, OTS, M_{ga})$, where $\mathbf{I}_{ga} \in \tilde{\mathbf{I}}, I_{ga} \in \tilde{I}$. $\mathbf{I}_{ga}$ or its prefix have never been input to a $\mathcal{KEO}$ query.

$\mathcal{A}$ *wins* if he completes the Game with (σ_{ga}, OTS) passes $(\mathsf{Verify}, \mathcal{V})$ respectively with respect to $\mathbf{I}_{ga}, I_{ga}, M_{ga}$. Its *advantage* is its probability of winning.

Definition 6. *The ℓ-level HIBS-with-OTS scheme is* (t, ϵ, ℓ)-EU-saID-ACP-wOTS *if no algorithm that runs in time t has an advantage ϵ.*

3.2 Hierarchical Identity-Based Signcryption (HIBSC)

Chow et al. [17] defined a security model for HIBSC without *insider security*. We modify it by adding insider security.

Summarizing [17]'s security model for HIBSC without insider security: The syntax, oracles, the correctness, and security notions including unforgeability and indistinguishability from [17] are adopted without alteration. In particular, the unforgeability game is summarized as follows:

The **Unforgeability Game**

1. (*Setup Phase*) $\mathcal{S}$ sets up system parameters and key pairs.
2. (*Probe Phase*) $\mathcal{A}$ queries Key Extraction Oracle $\mathcal{KEO}$, Signcryption oracle $\mathcal{SCO}$, and Unsigncryption Oracle $\mathcal{UO}$ in arbitrary interleave.
3. (*End Game*) $\mathcal{A}$ delivers a signcryption ciphertext C^* and recipient ID_B^*.

$\mathcal{A}$ *wins* if the following holds: $(M^*, \mathsf{ID}_A^*, \sigma^*) \leftarrow \mathsf{Unsigncrypt}(C^*, SK_{\mathsf{ID}_B^*})$, ID_A^* is never been queried to the $\mathcal{KEO}$ and no $\mathcal{SCO}$ request has resulted in a ciphertext C_i, whose unsigncryption under some SK_{ID_B} is identical to the triple $(M^*, \mathsf{ID}_A^*, \sigma^*)$. $\mathcal{A}$'s *advantage* is the probability that he wins.The HIBSC is *EU-ACP-secure* if no PPT attacker has a non-negligible advantage in the Unforgeability Game.

The **Indistinguishability Game**

1. (*Setup Phase*) $\mathcal{S}$ sets up system parameters and key pairs.
2. (*Probe 1 Phase*) $\mathcal{A}$ queries $\mathcal{KEO}$, $\mathcal{SCO}$, and $\mathcal{UO}$ in arbitrary interleave.
3. (*Gauntlet Phase*) $\mathcal{A}$ gives two messages M_0^*, M_1^*, sender ID_A^* and recipient ID_B^* to $\mathcal{S}$. $\mathcal{S}$ randomly picks a bit b and returns $C^* = \mathsf{Signcrypt}(M^*, SK_{\mathsf{ID}_A^*}, \mathsf{ID}_B^*)$ to $\mathcal{A}$.
4. (*Probe 2 Phase*) $\mathcal{A}$ queries $\mathcal{KEO}$, $\mathcal{SCO}$, and $\mathcal{UO}$ in arbitrary interleave.
5. (*End Game*) $\mathcal{A}$ delivers a guess $\hat{b}$.

$\mathcal{A}$ *wins* if the following holds: $\hat{b} = b$ and ID_B^* is never been queried to the $\mathcal{KEO}$. $\mathcal{A}$'s *advantage* is its probability that he wins over half. The HIBSC is *IND-CCA-secure* if no PPT attacker has a non-negligible advantage in the Indistinguishability Game.

Adding insider security: We say an attacker $\mathcal{A}$ wins the **IS Game** if it plays the Unforgeability Game and delivers a signcryption ciphertext, recipient) pair, (C^*, ID_B^*), satisfying the following condition: Denote $(M^*, \mathsf{ID}_A^*, \sigma^*) \leftarrow \mathsf{Unsigncrypt}(C^*, SK_{\mathsf{ID}_B^*})$. Then ID_A^* has never been queried to $\mathcal{KEO}$ and no $\mathcal{SCO}$ request has resulted in a ciphertext C_i, whose unsigncryption under $SK_{\mathsf{ID}_B^*}$ is identical to the triple $(M^*, \mathsf{ID}_A^*, \sigma^*)$. $\mathcal{A}$'s *advantage* is his winning probability. An HIBSC is *EU-IS-secure* if no PPT attacker has a non-negligible advantage in the IS Game.

Definition 7. *An HIBSC scheme is* secure *if it is EU-ACP-secure, IND-CCA-secure. It is* insider-secure *provided it is also EU-IS-secure.*

4 Generic Hierarchical Identity-Based Signature

Boneh et al. [8] showed that an adaptive CCA-secure ℓ-level hierarchical identity based encryption (HIBE) scheme Π can be constructed from a CPA-secure ℓ-level HIBE scheme Π' and a strong one-time signature scheme Sig. The intuition behind their construction is that Π' uses the key extraction oracle to simulate the decryption oracle of Π. If Π wants to query the challenge identity, he must have to forge a signature of Sig. We notice that similar technique can be applied for simulating the

signing oracle of hierarchical identity based signature (HIBS). In particular, we obtain an adaptive CMA secure IBS from a 2-level HIBS scheme.

Unlike its HIBE counterpart in [8], we cannot show how to construct a selective ID, ACP secure ℓ-level HIBS from a weaker selective ID secure $(\ell+1)$-level HIBS. The reason is that $\mathcal{A}'$ does not know in advance the $(\ell+1)$-level identity vk^* returned by $\mathcal{A}$ at the end of the game. Then $\mathcal{A}'$ cannot give the whole challenge identity at the beginning of the selective identity game. Therefore we define the sample ID model in the previous section and will use it here. Detailed constructions and proofs are given below.

4.1 Hierarchical IBS Construction

For arbitrary $\ell \geq 1$, let $\Pi' = (\mathsf{Setup'}, \mathsf{Der'}, \mathsf{Sign'}, \mathsf{Vfy'})$ be an $(\ell+1)$-level HIBS scheme handling identities of length n, and let $\mathsf{Sig} = (\mathcal{G}, \mathcal{SIG}, \mathcal{V})$ be a one-time signature scheme, in which the verification key has length n. We construct an ℓ-level HIBS scheme Π handling identities of length n. Π is constructed as follows:

Setup: $\mathsf{Setup}(1^\lambda, \ell, n)$ returns param from Π', expect the public parameters used in level $\ell+1$.

Der: $\mathsf{Der}(SK_v, (v, r))$ runs as follows: Run $\mathsf{Der'}(SK_v, v.r)$ and output the result as $SK_{v.r}$.

Sign: $\mathsf{Sign}(SK_v, m)$ first run $\mathcal{G}$ to obtain (vk, sk). Then run $\mathsf{Extract'}(SK_v, v.vk)$ to generate the key $SK^* = SK'_{v.vk}$. The algorithm then computes $C \leftarrow \mathsf{Sign'}(SK^*, m)$ and $\sigma \leftarrow \mathcal{SIG}(sk, C)$. The final ciphertext is $\langle vk, C, \sigma \rangle$.

Verify: $\mathsf{Vfy}(v, m, \langle vk, C, \sigma \rangle)$ runs as follows: first check whether $\mathcal{V}(vk, C, \sigma) = 1$. If not, output $\perp$. Then output $\top/\perp \leftarrow \mathsf{Vfy'}(v.vk, m, C)$.

Remark: We regard a signature scheme as a 0-level HIBS scheme. Then we drop $\mathsf{Extract}$ for a standard signature scheme. The master secret key of TA in HIBS will be the secret key in a standard signature scheme.

4.2 Security Analysis

It can be verified easily that the scheme achieve correctness. The security of the scheme is analyzed as follows:

Theorem 1. *If Π' is EU-saID secure and Sig is a strong one-time signature, then Π is EU-saID-ACP-wOTS secure.*

Proof. Given any PPT adversary $\mathcal{A}$ attacking the unforgeability of Π in a EU-saID-ACP-wOTS game. We define an adversary $\mathcal{A}'$ attacking the unforgeability of Π' in a EU-saID game. $\mathcal{A}'$ is defined as follows:

1. $\mathcal{A}'(1^\lambda, \ell+1)$ runs $\mathcal{A}(1^\lambda, \ell)$. When $\mathcal{A}'$ is given $(\tilde{\mathsf{ID}}, \mathsf{param})$, he divides $\mathsf{ID}_j = (\mathbf{I}_j, I_j)$ for all $\mathsf{ID}_j \in \tilde{\mathsf{ID}}$, where $|\mathbf{I}_j| = \ell$ and $|I_j| = 1$. Denote the set of $\mathbf{I}_j$s be $\tilde{\mathbf{I}}$ and the set of I_js be $\tilde{I}$. He gives $(\tilde{\mathbf{I}}, \tilde{I}, \mathsf{param})$ to $\mathcal{A}$, excluding the parameter used in the $(\ell+1)$-level HIBS.

2. Oracle queries by $\mathcal{A}$ is handled as follows:
   (a) When $\mathcal{A}$ queries $\mathcal{KEO}(v)$, $\mathcal{A}'$ requests the secret key SK'_v from its own $\mathcal{KEO}'$ and returns this secret key to $\mathcal{A}$.
   (b) When $\mathcal{A}$ queries $\mathcal{SO}(v, M)$, $\mathcal{A}'$ first runs $\mathcal{G}$ to obtain (vk, sk). $\mathcal{A}'$ requests the signature C for signer $v.vk$ and message M from its own $\mathcal{SO}'$. It then computes one-time signature σ for C using sk. $\mathcal{A}'$ returns the signature (vk, C, σ) to $\mathcal{A}$.
3. Finally, $\mathcal{A}$ outputs a ciphertext $\langle vk^*, C^*, \sigma^* \rangle$ for message m^* and sender identity $\mathbf{I}^* \in \tilde{\mathbf{I}}$, such that $\mathcal{V}(vk^*, C^*, \sigma^*) = 1$ and $vk^* \in \tilde{I}$. Then $\mathcal{A}'$ returns the ciphertext C^* for message m^* and sender $\mathbf{I}^*.vk^*$ as the solution.

Let Forge denotes the event that $\mathcal{A}$ outputs a ciphertext $\langle vk^*, C^*, \sigma^* \rangle$ with sender identity $\mathbf{I}^*$, where $\mathsf{Vfy}(vk^*, C^*, \sigma^*) = 1$; and $\mathcal{A}$ has queried $\mathcal{SO}$ with sender $\mathbf{I}^*$ and gets vk^* as part of the output ciphertext. If Forge occurs, then $\mathcal{A}'$ cannot return C^* as the solution.

Note that $\Pr[\mathsf{Forge}]$ is negligible. If $\mathcal{A}$ happens to receive a valid ciphertext $\langle vk^*, C, \sigma \rangle$ with sender identity $\mathbf{I}^*$ from the $\mathcal{SO}$ before, we must have $(C, \sigma) \neq (C^*, \sigma^*)$. By the security of strong one-time signature scheme, $\Pr[\mathsf{Forge}]$ is negligible.

Therefore for non-negligible probability, $\mathcal{A}'$ can return C^* as the solution. □

Remarks: Our security proof holds for an adaptive chosen ID, ACP secure ℓ-level HIBS from an adaptive chosen ID, weaker ACP attack secure $(\ell + 1)$-level HIBS. The proof is similar and hence omitted.

5 Efficient Instantiation of HIBS

We construct an efficient ℓ-level HIBS scheme which is provably secure without random oracles, based on the ℓ-DHI* assumption. The key system comes from [7].

Let $\mathbb{G}$ be a bilinear group of prime order p. Given a pairing: $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$.

Setup: To generate system parameters, the algorithm selects a random generator $g, g_2, g_3, h_1, \ldots, h_\ell \in \mathbb{G}$, picks a random $\alpha \in \mathbb{Z}_p$, and sets $g_1 = g^\alpha$. The system parameters $\mathsf{param} = (g, g_1, g_2, g_3, h_1, \ldots, h_\ell)$ and the master key is g_2^α.

Der: To generate a private key for $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_k)$. where $k \leq \ell$, the algorithm picks a random $r \in \mathbb{Z}_p$ and computes:

$$SK_{\mathsf{ID}} = \left(g_2^\alpha \cdot (h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)^r, \quad g^r, \quad h_{k+1}^r, \ldots, h_\ell^r \right) = (a_0, a_1, b_{k+1}, \ldots, b_\ell)$$

The private key for ID can also be generated by its parent $\mathsf{ID}_{|k-1} = (\mathsf{id}_1, \ldots, \mathsf{id}_{k-1})$. Details refer to [7].

Sign: For a user with identity ID and private key SK_{ID}, he signs a message M as follows. He picks a random $t \in \mathbb{Z}_p$, and computes:

$$C_1 = \hat{e}(g_1, g_2)^t \qquad h = H(C_1, \mathsf{ID}, M, \mathsf{param}) \qquad C_2 = {a_0}^{h+t} \qquad C_3 = {a_1}^{h+t}$$

The signature σ is (C_1, C_2, C_3).

Verify: The verifier receives a signature $\sigma = (C_1, C_2, C_3)$ for message M and signer ID, he computes $h = H(C_1, \mathsf{ID}, M, \mathsf{param})$. The verifier checks if:

$$\hat{e}(g, C_2) \stackrel{?}{=} C_1 \cdot \hat{e}(g_1, g_2)^h \cdot \hat{e}(C_3, h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)$$

The verifier outputs $\top$ if it is true. Otherwise, he outputs $\perp$.

5.1 Security Analysis

The correctness of the scheme is shown as follows:

$$\begin{aligned}\hat{e}(g, C_2) &= \hat{e}(g, g_2^{\alpha} \cdot (h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)^r)^{h+t} \\ &= \hat{e}(g^{\alpha}, g_2)^{h+t} \cdot \hat{e}(g^r, h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)^{h+t} \\ &= C_1 \cdot \hat{e}(g_1, g_2)^h \cdot \hat{e}(C_3, h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)\end{aligned}$$

Then we show that our HIBS scheme achieves existential unforgeability.

Theorem 2. *Our ℓ-level HIBS scheme is (t, ϵ, ℓ)-EU-saID secure assuming the $((t + O(\tau \ell q)), \epsilon/n_1, \ell)$-DHI* assumption holds, where n_1 are the number of sample identities given in the game, q is the total number of query to $\mathcal{KEO}$ and $\mathcal{SO}$, τ is the maximum time for an exponentiation in $\mathbb{G}$.*

Proof. Suppose a dealer gives the ℓ-DHI* tuple $(g, y_1, \ldots, y_\ell)$ to a simulator, where $y_i = g^{(\alpha^i)}$. The sample identity games begins with a simulator randomly picks ID_1, $\cdots$, $\mathsf{ID}_{n_1} \in (\mathbb{Z}_p)^\ell$ and denotes the set as $\tilde{\mathsf{ID}}$. The simulator picks a $\mathsf{ID}^* \in \tilde{\mathsf{ID}}$. Denote $\mathsf{ID}^* = (\mathsf{id}_1^*, \ldots, \mathsf{id}_\ell^*)$.

The simulator picks a random $\gamma \in \mathbb{Z}_p$ and assigns $g_1 = y_1, g_2 = y_\ell \cdot g^\gamma$. The simulator picks random $\gamma_1, \ldots \gamma_\ell \in \mathbb{Z}_p$ and sets $h_i = g^{\gamma_i} / y_{\ell - i + 1}$ for $1 \le i \le \ell$. It also picks a random $\delta \in \mathbb{Z}_p$ and sets $g_3 = g^\delta \cdot \prod_{i=1}^{\ell} y_{\ell-i+1}^{\mathsf{id}_i^*}$. The simulator gives the adversary $\mathcal{A}$ the public parameters $\mathsf{param} = (g, g_1, g_2, g_3, h_1, \ldots, h_\ell)$ and $\tilde{\mathsf{ID}}$. The corresponding (unknown) master secret key is $g_2^\alpha = g^{\alpha(\alpha^\ell + \gamma)} = y_{\ell+1} y_1^\gamma$.

Key Extraction Oracle: Simulate as in [7]. For input identity $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_u)$, if ID is ID^* or a prefix of it, the simulator declares failure and exits. Otherwise there exists a $k \le u$ such that $\mathsf{id}_k \neq \mathsf{id}_k^*$. We set k be the smallest such index. To answer the query, the simulator derives a secret key for the identity $(\mathsf{id}_1, \ldots, \mathsf{id}_k)$ from which it then constructs a private key for $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_k, \ldots, \mathsf{id}_u)$.

To generate the secret key for the identity $(\mathsf{id}_1, \ldots, \mathsf{id}_k)$, the simulator chooses a random $\tilde{r} \in \mathbb{Z}_p$. Denote $r = \frac{\alpha^k}{(\mathsf{id}_k - \mathsf{id}_k^*)} + \tilde{r}$ and compute:

$$a_0 = y_1^\gamma \cdot Z \cdot y_{\ell-k+1}^{\tilde{r}(\mathsf{id}_k^* - \mathsf{id}_k)} \quad \text{where} \quad Z = \left(g^{\delta + \sum_{i=1}^{k} \mathsf{id}_i \gamma_i} \cdot \prod_{i=k+1}^{\ell} y_{\ell-i+1}^{\mathsf{id}_i^*} \right)^r$$

$$a_1 = g^r = y_k^{1/(\mathsf{id}_k - \mathsf{id}_k^*)} g^{\tilde{r}}$$

Refer to [7] for the well-formedness of the secret key. The remaining $h_{k+1}^r, \ldots, h_\ell^r$ can be computed by the simulator since they do not involve a $y_{\ell+1}$ term.

Signing Oracle: For the signer ID , if ID is ID^* or a prefix of it, the simulator declares failure and exits. Otherwise, the simulator extracts the secret key d_{ID} as in the key extraction oracle, and then computes the signature.

Finally, the adversary $\mathcal{A}$ returns a signature σ^* for message M^* and signer $\hat{ID} \in \tilde{\mathsf{ID}}$, where $\hat{ID}$ or its prefix is never been queried to $\mathcal{KEO}$ or $\mathcal{SO}$. For probability $1/n_1$, $\hat{ID} = \mathsf{ID}^*$. Otherwise the simulator declares failure and exits. We can rewind and extract the secret keys from $\sigma_0^* = (C_1, C_2, C_3)$ and $\sigma_1^* = (C_1, C_2', C_3')$ with the hash value h and h' respectively:

$$a_0 = (C_2'/C_2)^{1/(h'-h)} \qquad a_1 = (C_3'/C_3)^{1/(h'-h)}$$

Therefore we can set $a_1 = g^{\bar{r}}$ for some $\bar{r} \in \mathbb{Z}_p$. Then:

$$\begin{aligned} a_0 &= g_2^{\alpha}(g_3 \prod_{i=1}^{k} h_i^{\mathsf{id}_i^*})^{\bar{r}} \\ &= g_2^{\alpha}(g^{\delta} \prod_{j=1}^{\ell} y_{\ell-j+1}^{\mathsf{id}_j^*} \prod_{i=1}^{k} (\frac{g^{\gamma_i}}{y_{\ell-i+1}})^{\mathsf{id}_i^*})^{\bar{r}} \\ &= g_2^{\alpha}(g^{\delta} \prod_{i=1}^{k} g^{\gamma_i \mathsf{id}_i^*})^{\bar{r}} \\ &= g_2^{\alpha}(g^{\delta+\sum_{i=1}^{k}(\gamma_i \mathsf{id}_i^*)})^{\bar{r}} \end{aligned}$$

Therefore the simulator returns $y_{\ell+1} = g_2^{\alpha}/y_1^{\gamma} = a_0/(a_1^{\delta+\sum_{i=1}^{k}(\gamma_i \mathsf{id}_i^*)} y_1^{\gamma})$ as the solution. □

5.2 ACP HIBS

By the result of Theorem 1, we can show that we obtain ACP-secure HIBS scheme in the standard model. We use the signature scheme in [6] to replace the strong one-time signature scheme in section 4.

We have the following instantiation for $(\ell-1)$-level HIBS scheme using the signature scheme in [6] and the ℓ-level HIBS in the above section.

Setup: To generate system parameters, the algorithm selects a random generator $g, g_2, g_3, h_1, \ldots, h_\ell \in \mathbb{G}$, picks a random $\alpha \in \mathbb{Z}_p$, and sets $g_1 = g^{\alpha}$. The system parameters $\mathsf{param} = (g, g_1, g_2, g_3, h_1, \ldots, h_\ell)$ and the master key is g_2^{α}.

Der: To generate a private key for $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_k)$. where $k \leq \ell$, the algorithm picks a random $r \in \mathbb{Z}_p$ and computes:

$$SK_{\mathsf{ID}} = \left(g_2^{\alpha} \cdot (h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)^r, \quad g^r, \quad h_{k+1}^r, \ldots, h_\ell^r\right) = (a_0, a_1, b_{k+1}, \ldots, b_\ell)$$

The private key for ID can also be generated by its parent $\mathsf{ID}_{|k-1} = (\mathsf{id}_1, \ldots, \mathsf{id}_{k-1})$. Details refer to [7].

Sign: For a user with identity $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_k)$ and private key $SK_{\mathsf{ID}} = (a_0, a_1, b_{k+1}, \ldots, b_\ell)$, he signs a message M as follows. He randomly picks $x, y \in \mathbb{Z}_p^*$. Denote $\mathsf{id}_{k+1} = H_0(g^x, g^y, \mathsf{param}) \in \mathbb{Z}_p^*$ and $\mathsf{ID}' = (\mathsf{id}_1, \ldots, \mathsf{id}_{k+1})$. He picks a random $r_0, r_1, t \in \mathbb{Z}_p$, and computes:

$$a_0' = a_0 \cdot b_{k+1}^{\mathsf{id}_{k+1}} \cdot (h_1^{\mathsf{id}_1} \cdots h_{k+1}^{\mathsf{id}_{k+1}} \cdot g_3)^{r_0} \qquad a_1' = a_1 \cdot g^{r_0}$$
$$C_1 = \hat{e}(g_1, g_2)^t \qquad h = H(C_1, \mathsf{ID}, M, \mathsf{param}) \qquad C_2 = {a_0'}^{h+t} \qquad C_3 = {a_1'}^{h+t}$$
$$h' = H_1(C_1, C_2, C_3) \in \mathbb{Z}_p^* \qquad \sigma = g^{1/(x+h'+yr_1)}$$

The signature σ is $(g^x, g^y, C_1, C_2, C_3, r_1, \sigma)$.

Verify: The verifier receives a signature $(g^x, g^y, C_1, C_2, C_3, r_1, \sigma)$ for message M and signer $\mathsf{ID} = (\mathsf{id}_1, \ldots, \mathsf{id}_k)$, he computes $\mathsf{id}_{k+1} = H_0(g^x, g^y, \mathsf{param})$, sets $\mathsf{ID}' = (\mathsf{id}_1, \ldots, \mathsf{id}_{k+1})$, computes $h = H(C_1, \mathsf{ID}', M, \mathsf{param})$ and $h' = H_1(C_1, C_2, C_3)$. The verifier checks if:

$$\hat{e}(g, C_2) \stackrel{?}{=} C_1 \cdot \hat{e}(g_1, g_2)^h \cdot \hat{e}(C_3, h_1^{\mathsf{id}_1} \cdots h_{k+1}^{\mathsf{id}_{k+1}} \cdot g_3)$$
$$\hat{e}(g, g) \stackrel{?}{=} \hat{e}(\sigma, g^x \cdot g^{h'} \cdot (g^y)^{r_1})$$

The verifier outputs $\top$ if it is true. Otherwise, he outputs $\perp$.

By theorem 1, 2 and the security of the signature scheme in [6] (which is provably secure under the q-SDH assumption), we can see that the above HIBS scheme is EU-saID-ACP secure under the q-SDH and ℓ-DHI* assumptions.

6 Efficient HIBSC without Random Oracles

Motivated by [1]'s generic composition of SC from E and S, we present a generic composition of HIBSC from HIBE and HIBS. Its security is argued below. Then we present a concrete instantiation by composing a HIBSC from [7]'s HIBE and our HIBS in Section 5. The security of this specific HIBSC is reduced to a combination of the securities of respective components. The result is a provable HIBSC with size $O(\lambda_s)$ bits which is independent of the levels in the HIBSC. Its security is provable without random oracles, albeit in a weaker model concerning assumptions on the attacker's ability to maneuver identities in the oracles.

6.1 Generic composition from HIBE and HIBS

The generic composition of signcryption from a CCA-secure encryption and an ACP-secure signature is proposed by [1]. They showed the security of the outcome without insider attacks. The also give the guidelines of *whenever signing include receiver identity in message* and *whenver encrypting include sender identity in plaintext*, and argued the result would be secure against insider attacks. Motivated by their result, we present a generic composition of HIBSC from HIBE and HIBS.

In [1], a secure signcryption can be compositioned from a secure signature Sig and a secure encryption Enc via the *sign-then-encrypt* paradigm as follows:

$$\sigma = \mathsf{Enc}_R(\mathsf{Sig}_S(m, \mathsf{ID}_R), \mathsf{ID}_S)$$

where S is the sender and R is the recipient. We observe that such composition can be applied to HIBE and HIBS by treating Enc as the HIBE encryption algorithm and Sig as the HIBS signing algorithm. If [1]'s security theorem for multi-user signcryption is valid, and the hierarchical

key derivation system does not cause any problems, then we are likely to have security for the compositioned HIBSC.

Remarks: In [1], their security is actually for generalized CCA (gCCA), which is a slight relaxation of CCA security. For simplicity, we only mention the CCA security here.

6.2 Concrete Instantiation

We give a concrete instantiation of HIBSC from our proposed HIBS and the constant size HIBE from [7]. As a result, we obtain a constant size HIBSC secure in the standard model. The instantiation is given below:

Setup, **Der:** same as section 5.

Signcrypt: For a user with identity ID_A and private key SK_{ID_A}, he signcrypts a message M to recipient $I_B = (I_1, \ldots, I_k)$ as follows. He picks a random $t \in \mathbb{Z}_p$, and computes:

$$C_1 = \hat{e}(g_1, g_2)^t \qquad h = H(C_1, \mathsf{ID}_A, I_B, M, \mathsf{param}) \qquad C_2 = {a_0}^{h+t} \qquad C_3 = {a_1}^{h+t}$$
$$C_4 = C_1 \oplus \langle M, \mathsf{ID}_A, C_2, C_3 \rangle \qquad C_5 = g^t \qquad C_6 = (h_1^{I_1} \cdots h_k^{I_k} \cdot g_3)^t$$

The ciphertext σ is (C_4, C_5, C_6).

Unsigncrypt: The recipient I_B with private key $SK_{I_B} = (a_0, a_1, b_k, \ldots, b_\ell)$ receives a ciphertext σ is $(C_2, C_3, C_4, C_5, C_6)$, he computes:

$$C_1 = \hat{e}(C_5, a_0)/\hat{e}(a_1, C_6) \qquad \langle M, \mathsf{ID}_A, C_2, C_3 \rangle = C_4 \oplus C_1 \qquad h = H(C_1, \mathsf{ID}_A, M, \mathsf{param})$$

Denote $\mathsf{ID}_A = (\mathsf{id}_1, \ldots, \mathsf{id}_k)$. The recipient checks if:

$$\hat{e}(g, C_2) \stackrel{?}{=} C_1 \cdot \hat{e}(g_1, g_2)^h \cdot \hat{e}(C_3, h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)$$

The recipient outputs M if it is true. Otherwise, he outputs $\perp$.

Security Analysis We can prove our HIBSC scheme in the standard model. In particular, it can also imply a secure identity based signcryption scheme in the standard model.

Theorem 3. *Our HIBSC scheme is insider-secure assuming the wBDHI* assumption, DHI* assumption and SDH assumption holds in the saID model for HIBS and the sID model for HIBE.*

Proof. (Sketch) For the Indistinguishability Game, suppose a simulator $\mathcal{S}$ is given the decisional ℓ-wBDHI* tuple $(g, h, y_1, \ldots, y_\ell, T)$ where $y_i = g^{(\alpha^i)}$. $\mathcal{A}$ gives the challenge identity id^* to $\mathcal{S}$. $\mathcal{S}$ setups the game as in the proof in [7]. He simulates the key extraction oracle as in Theorem 2. All signcryption or unsigncryption query for users, which are not equal to the challenge ID or its prefix, can be computed by extracting the private key of the sender/recipient. Other settings and $\mathcal{A}$'s answer are handled as in [7].

For the Unforgeability Game, suppose a simulator $\mathcal{S}$ is given the ℓ-DHI* tuple $(g, y_1, \ldots, y_\ell)$ where $y_i = g^{(\alpha^i)}$. $\mathcal{S}$ setups the game as in the proof in [7]. He simulates the key extraction oracle as in Theorem 2. All signcryption or unsigncryption query for users which are not equal to the challenge ID or its prefix can be computed by extracting the private key of the sender/recipient. Other settings and $\mathcal{A}$'s answer are handled as in Theorem 2..

By using one-time signature scheme, our HIBSC instantiation can be converted to sID-CCA and saID-ACP secure HIBSC in the standard model, by using Theorem 1 and the theorem in [16, 10, 8].

7 Conclusions

We presented the first constant-size HIBS (resp. HIBSC) provable without random oracles. The sID model and the saID models were used in the reductionist security proofs. It is an open problem to avoid these models.

References

1. Jee Hea An, Yevgeniy Dodis, and Tal Rabin. On the Security of Joint Signature and Encryption. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 83–107. Springer, 2002.
2. Mihir Bellare, Alexandra Boldyreva, and Adriana Palacio. An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 171–188. Springer, 2004.
3. Mihir Bellare and Phillip Rogaway. Random Oracles Are Practical: A Paradigm For Designing Efficient Protocols. In *ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.
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, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 2004.
5. Dan Boneh and Xavier Boyen. Secure Identity Based Encryption Without Random Oracles. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 443–459. Springer, 2004.
6. Dan Boneh and Xavier Boyen. Short Signatures Without Random Oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 2004.
7. 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, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 440–456. Springer, 2005.
8. Dan Boneh, Ran Canatti, Shai Halevi, and Jonathan Katz. Chosen-Ciphertext Security from Identity-Based Encryption. http://crypto.stanford.edu/~dabo/abstracts/ccaibejour.html, 2005.
9. Dan Boneh and Matt Franklin. Identity-Based Encryption from the Weil Pairing. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.
10. Dan Boneh and Jonathan Katz. Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption. In Alfred Menezes, editor, *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*, volume 3376 of *Lecture Notes in Computer Science*, pages 87–103. Springer, 2005.
11. Dan Boneh, Ilya Mironov, and Victor Shoup. A Secure Signature Scheme from Bilinear Maps. In Marc Joye, editor, *Topics in Cryptology - CT-RSA 2003, The Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings*, volume 2612 of *Lecture Notes in Computer Science*, pages 98–110. Springer, 2003.
12. Xavier Boyen. Multipurpose Identity-Based Signcryption (A Swiss Army Knife for Identity-Based Cryptography). In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 383–399. Springer, 2003.
13. Xavier Boyen and Brent Waters. Compact Group Signatures Without Random Oracles. Cryptology ePrint Archive, Report 2005/381, 2005.

14. Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. In *STOC*, pages 209–218, 1998.
15. Ran Canetti, Shai Halevi, and Jonathan Katz. A Forward-Secure Public-Key Encryption Scheme. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 255–271. Springer, 2003.
16. Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-Ciphertext Security from Identity-Based Encryption. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 207–222. Springer, 2004.
17. Sherman S.M. Chow, Tsz Hon Yuen, Lucas C.K. Hui, and S.M. Yiu. Signcryption in Hierarchical Identity Based Cryptosystem. In *20th IFIP International Information Security Conference, Chiba, Japan, May 30 - June 1, 2005*, pages 443–457, 2005.
18. Ronald Cramer and Victor Shoup. Signature Schemes Based on the Strong RSA Assumption. In *6th ACM Conference on Computer and Communications Security, November 1-4, 1999, Singapore*, pages 46–51, 1999.
19. Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, and Shabsi Walfish. Versatile padding schemes for joint signature and encryption. In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick Drew McDaniel, editors, *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washingtion, DC, USA, October 25-29, 2004*, pages 344–353. ACM, 2004.
20. Marc Fischlin. The Cramer-Shoup Strong-RSA Signature Scheme Revisited. In Yvo Desmedt, editor, *Public Key Cryptography - PKC 2003, 6th International Workshop on Theory and Practice in Public Key Cryptography, Miami, FL, USA, January 6-8, 2003, Proceedings*, volume 2567 of *Lecture Notes in Computer Science*, pages 116–129. Springer, 2003.
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, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 123–139. Springer, 1999.
22. Craig Gentry and Alice Silverberg. Hierarchical ID-Based Cryptography. In Yuliang Zheng, editor, *Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer, 2002.
23. Oded Goldreich. *Foundations of Cryptography. Volume II, Basic Applications*. Cambridge University Press, 2004.
24. Swee-Huay Heng and Kaoru Kurosawa. k-Resilient Identity-Based Encryption in the Standard Model. In Tatsuaki Okamoto, editor, *Topics in Cryptology - CT-RSA 2004, The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings*, volume 2964 of *Lecture Notes in Computer Science*, pages 67–80. Springer, 2004.
25. Jeremy Horwitz and Ben Lynn. Toward Hierarchical Identity-Based Encryption. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 466–481. Springer, 2002.
26. John Malone-Lee. Identity-based signcryption. Cryptology ePrint Archive, Report 2002/098, 2002.
27. Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.
28. Brent Waters. Efficient Identity-Based Encryption Without Random Oracles. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer, 2005.
29. Tsz Hon Yuen and Victor K. Wei. Fast and Proven Secure Blind Identity-Based Signcryption from Pairings. In Alfred Menezes, editor, *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*, volume 3376 of *Lecture Notes in Computer Science*, pages 305–322. Springer, 2005.
30. Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Application. In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 277–290. Springer, 2004.
31. Yuliang Zheng. Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption). In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual*

International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings, volume 1294 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 1997.