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

Tsz Hon Yuen and Victor K. Wei

Dept. of Information Engineering, The Chinese Univ. of Hong Kong, Hong Kong
{thyuen4,kwwei}@ie.cuhk.edu.hk

March 2, 2006

Abstract. We construct the first constant-size hierarchical identity-based signature (HIBS) without random oracles - the signature size is $O(\lambda_s)$ bits, where λ_s is the security parameter, and it is independent of the number of levels in the hierarchy.

We observe that an efficient hierarchical identity-based signcryption (HIBSC) scheme without random oracles can be compositioned from our HIBS and Boneh, Boyen, and Goh's HIBE (hierarchical identity-based encryption)[9]. We further optimize it to a constant-factor efficiency improvement. This is the first constant-size HIBSC without random oracles.

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

1 Introduction

Identity based cryptosystem [34] 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 an unambiguous name of him, 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 Alice's identity. Then anybody can verify the authenticity of the signature from the identity. 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 identity based cryptosystem [27, 30] is a generalization of identity based cryptosystem 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 sign or decrypt messages for other identities. [27] proposed the idea of Hierarchical IBS (HIBS) and Hierarchical IBE (HIBE). In particular, an IBS (resp. IBE) is an 1-level HIBS (resp. HIBE). Combining HIBS and HIBE, [22] proposed the concept of Hierarchical IBSC (HIBSC).

Many reductionist security proofs concerning identity based cryptosystems and other cryptosystems used the random oracle model [5]. 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 [18, 2]. Therefore identity based cryptosystems provably secure in the standard model attract a great interest. [3] showed that a certificate-based IBS is secure without random oracles. However these scheme

Several IBE schemes [19, 6, 29] are secure without random oracles under a weaker "selective-ID" model [19]. Recently, [7] and [36] proposed IBE schemes which are provably secure without random oracles under the stronger model of [11].

Most existing practical signature schemes are provably secure in the random oracle model. [26] 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 was proposed in [23], and further improvement was proposed in [25]. [14] proposed a signature scheme provably secure under discrete-log type assumption in the standard model, but the signature size is long. [8] proposed a short signature scheme secure without random oracles, under the new q-SDH assumption. [37] proposed some short signatures without random oracles. The signatures originate from the signature schemes in [8, 39, 17, 13]. They showed how these signatures can be constructed from new assumptions without random oracles.

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 without random oracles.

1.1 Our Contribution

We make the following contributions:

- The *first* constant-size hierarchical identity based signature (HIBS) scheme. It is existentially unforgeable without random oracles under a new interactive intractability assumption.
- Our HIBS scheme is existentially unforgeable providing the Diffie-Hellman Inversion (DHI) Assumption holds in the gauntlet-ID model without random oracles. We introduce the gauntlet-ID model, which is a slightly weaker model related to the select-ID model of [19].
- The *first* constant-size identity based signcryption (IBSC) and hierarchical identity based signcryption (HIBSC) scheme which are provably secure without random oracles.

1.2 Related Results

Shamir [34] suggested an identity-based signature scheme. Many different IBS schemes were proposed (e.g. [21, 3]). Boneh and Franklin [11] proposed the first practical identity-based encryption scheme, which is provably secure in the random oracle model. Several IBE schemes [19, 6, 29] are secure without random oracles under a weaker "selective-ID" model [19]. [7] and [36] proposed IBE schemes which are provably secure without random oracles under the model of [11]. Recently [16] proposed an identity based signature without random oracles, but their reduction is tight only if they use the "selective-ID" model.

Zheng [41] 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. [32, 15, 38]) 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 (HIBS and HIBE) was proposed in [27] and [30] proposed another HIBE. Recently, Boneh et al. [10] (preliminary papers [20, 12]) suggested some methods to construct CCA secure ℓ-level HIBE scheme from a CPA $(\ell + 1)$-level HIBE scheme. Several HIBE without random oracles are proposed in [6, 7, 36, 9] using this result. Hierarchical identity based signcryption is firstly proposed in [22].

Type	Scheme	Security	ROM	Size
ℓ-HIBS	Cert-chain	Full ACP	No	$O(\ell\lambda_s)$
	This paper	Full ACP/gID-ACP	No	$O(\lambda_s)$
IBS	Cert-chain	Full ACP	No	$O(\lambda_s)$
Standard Signature	[26, 23, 8]	ACP	No	$O(\lambda_s)$

Table 1. Recent results on signatures, IBS, and HIBS. Cert-chain 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. gID-ACP means the scheme is secure against gauntlet identity and adaptive chosen message attack. Our scheme is provably secure in Full ACP or gID-ACP model by using different intractability assumptions. ℓ is the number of hierarchy level and λ_s is the security parameter. ROM means if the reductionist security proof is in the random oracle model.

Our Intuition. Classic methods of constructing fully secure signatures from combining *hierarchical authentication tree* and *one-time signatures* can be found in [28]. [3] suggested that IBS without random oracles can be constructed by certificate chaining, but it is less efficient. Various instantiations and modifications for IBE are also well-known [20, 12, 10]. We observe that some of these certificate chaining instantiations bear a striking resemblance to the multi-level certificate chaining structure in HIBS. User identity can be certified by his parent, by signing an IBS on the user's identity. The parent's identity can be certified again by one level higher, and the process repeats up until the root. If in each level, the certification 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 either use an *interactive intractability assumption*, or lower the security level to gauntlet ID-ACP (which we will define below). We can see that the same case applies for HIBE using sID-CCA. The recent results are summarized in table 1, 2 and 3.

Interactive intractability assumptions: An interactive intractability problem instance means that an attacker can adaptively query an external oracle and can get distinct valid tuples from the oracle which satisfy a relation $\mathcal{R}$. Finally he needs to return a new valid tuple which satisfies $\mathcal{R}$. [31] proposed a LRSW assumption with an external oracle. In proving the security of a signature scheme, the simulator simply forwards all signing oracle queries to this external oracle and returns its output to the adversary. Signature schemes like [17] use this type of assumption. The problem of interactive intractability assumptions is that we need to assume that the tuples return by the oracle should not help the attacker to solve the intractability problem. Therefore we need to be extremely careful when formulating interactive intractability assumptions.

Gauntlet ID-ACP unforgeability: Gauntlet ID-ACP unforgeability means that in the unforgeability game, the adversary finally returns a signature of a user who has never been queried to the key extraction oracle or the signing oracle. It is related to the select-ID model of [19], which further requires the adversary to select the user he attacks at the beginning of the unforgeability game.

Type	Scheme	Security	ROM	Size
ℓ-HIBE	[10] + ?	Full CCA	No	$O(\ell\lambda_s)$
	[10] + [9]	sID-CCA	No	$O(\lambda_s)$
IBE	[36]	Full CCA	No	$O(\lambda_s)$
Standard Encryption	Cramer-Shoup/OAEP/ [10]+sID-CCA IBE	CCA	No	$O(\lambda_s)$

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. ROM means if the reductionist security proof is in the random oracle model. The first row means that full CCA secure HIBE can be achieved by using [10] and an adaptive chosen identity and chosen plaintext secure HIBE. However no existing scheme achieves this with a tight security reduction.

Type	Scheme	Security	ROM	Size
ℓ-HIBSC	[22]	Full CCA + ACP	Yes	$O(\ell\lambda_s)$
	This paper	sID-CCA + Full ACP	No	$O(\lambda_s)$
IBSC	[15], [38], etc.	Full CCA + ACP	Yes	$O(\lambda_s)$
	This paper	sID-CCA + Full ACP	No	$O(\lambda_s)$
Standard Signcryption	[1], [24]	CCA + ACP	No	$O(\lambda_s)$

Table 3. Recent results on signcryption, IBSC, and HIBSC. All notations are defined in table 1 and 2. ROM means if the reductionist security proof is in the random oracle model. [24] showed that only standard signcryption scheme of [1] and [24] achieves the strong *insider* security model. All existing IBSC and HIBSC schemes are provably secure in the random oracles only.

We observe that by using either approach, we can achieve a constant size HIBS secure without random oracles.

1.3 Organization

In section 2, we give some background knowledges. In section 3, we give the definition for the security model for HIBS and HIBSC. In section 4, we show an efficient instantiation of HIBS and an ordinary signature from the HIBS. In section 5, we describe how our result can be applied to signcryption schemes. In section 6, we conclude our paper.

2 Preliminaries

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.

2.1 Pairings

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.

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 $e(g, g) \neq 1$.*

2.2 Intractability Assumptions

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

We say that the ℓ-DHI* assumption holds if no PPT algorithm can solve a random instance of the ℓ-DHI* problem with non-negligible probability.

Definition 4. *(decisional ℓ-wBDHI* problem)[9] The decisional ℓ-weak-Bilinear-Diffie-Hellman Inversion * problem is that, given g, h, g^{α}, $g^{\alpha^2}, \ldots, g^{\alpha^\ell} \in \mathbb{G}$ 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 decisional ℓ-wBDHI* assumption holds if no PPT algorithm can solve a random instance of the decisional ℓ-wBDHI* problem with non-negligible probability over half.

The ℓ-DHI problem and ℓ-DHI* problem are proven equivalent in [40].

We introduce a new intractability assumption called the OrcYW assumption.

Definition 5. *The* OrcYW Problem *is that given*

1. *$\ell \geq 1$, $\{g^{x^i} : 0 \leq i \leq \ell\}$, γ, δ, g_4, g_5, γ_1, $\cdots$, γ_ℓ, an identity $I = \{I_1, \cdots, I_\ell\}$, full-domain collision-resistant hash function $\mathcal{H}$,*
2. *an oracle $O_{\mathcal{H}}$ which upon input a message m and an identity $I' = \{I_1, \cdots, I_k\}$ for $k \leq \ell$, outputs a tuple (D_1, D_2, Z_1, Z_2) satisfying: For some random t, r, which differ for each query to $O_{\mathcal{H}}$,*

$$D_1 = g^t, \quad D_2 = Q^t, \quad Z_1 = a_0^h g_4^t, \quad Z_2 = a_1^h g_5^t$$

where

$$Q = g_3 \textstyle\prod_{i=1}^k h_i^{I_i}, \quad h_i = g^{\gamma_i} g^{-x^{\ell-i+1}}, \text{ for } 1 \leq i \leq \ell \quad g_2 = g^{x^\ell+\gamma}, \quad g_3 = g^{\delta+\sum_{i=1}^{\ell} x^{\ell-i+1} I_i},$$
$$a_0 = g_2^x Q^r, \quad a_1 = g^r, \quad h = \mathcal{H}(D_1, D_2, I', m, \mathsf{param}),$$
$$\mathsf{param} = (g, g^x, g_2, g_3, g_4, g_5, h_1, \cdots, h_\ell)$$

to output $(\tilde{m}, \tilde{D}_1, \tilde{D}_2, \tilde{Z}_1, \tilde{Z}_2)$ satisfying

$$\hat{e}(g, \tilde{Z}_1) \cdot \hat{e}(g_5, \tilde{D}_2) = \hat{e}(g_1, g_2)^{\tilde{h}} \cdot \hat{e}(\tilde{D}_1, g_4) \cdot \hat{e}(\tilde{Z}_2, Q)$$
$$\wedge \;\; \hat{e}(\tilde{D}_1, Q) = \hat{e}(g, \tilde{D}_2) \;\; \wedge \;\; \tilde{m} \textit{ was not queried to } O_{\mathcal{H}}$$
$$\wedge \;\; Q = g_3 \textstyle\prod_{i=1}^{\ell} h_i^{I_i}$$

where $\tilde{h} = \mathcal{H}(\tilde{D}_1, \tilde{D}_2, I, \tilde{m}, \mathsf{param})$.

We say that the *OrcYW Assumption* holds if no PPT algorithm can solve a random instance of the OrcYW Problem with non-negligible probability.

The intractability of the OrcYW Assumption will be discussed in section 5.

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 [11]. 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. [19] 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 a variant for signature scheme, namely a "gauntlet-identity" model.

An ℓ-level HIBS scheme 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 ID, 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 signature σ, it outputs $\top$ if σ is a valid signature of M corresponding to $\mathsf{ID}, \mathsf{param}$. Otherwise, it outputs $\perp$.

The security of a HIBS consists of two requirements, namely *Correctness* and *Existential Unforgeability.* They are defined as follows:

Correctness. We require that $\top \leftarrow \mathsf{Verify}(\mathsf{ID}, M, \mathsf{Sign}(SK_{\mathsf{ID}}, M))$ for any message M, any private key SK_{ID} and its corresponding identity ID.

Existential Unforgeability. We define the existential unforgeability against adaptive identity and adaptive chosen plaintext attack for HIBS (ACP-UF). We require that the user identity should be queried through an oracle as in [3]. We assume the simulator maintains an honest user list HU and a corrupt user list CU. We define the following oracles:

- $\mathcal{IO}(\mathsf{ID})$: The Initialization Oracle with input ID outputs $\perp$ if $\mathsf{ID} \in HU \cup CU$. Otherwise it puts ID in HU and returns 1.
- $\mathcal{KEO}(\mathsf{ID})$: The Key Extraction Oracle with input ID outputs $\perp$ if $\mathsf{ID} \notin HU$. Otherwise it outputs the corresponding secret key SK_{ID}, removes ID from HU and adds ID to CU.
- $\mathcal{SO}(\mathsf{ID}, M)$: The Signing Oracle with input signer ID and message M outputs $\perp$ if $\mathsf{ID} \notin HU$. Otherwise it will output a signature σ such that $\mathsf{Verify}(\mathsf{ID}, M, \sigma) = \top$.

The Game is defined as follows:

1. (*Init. Phase*) Simulator $\mathcal{S}$ generates system parameter param and gives it to Adversary $\mathcal{A}$.
2. (*Probe Phase*) $\mathcal{A}$ queries $\mathcal{IO}(\mathsf{ID})$, $\mathcal{KEO}(\mathsf{ID})$ and $\mathcal{SO}(\mathsf{ID}, M)$, in arbitrary interleaf.
3. (*End Game*) $\mathcal{A}$ delivers a signature σ_{ga} for signer identity ID_{ga} and message M_{ga}. ID_{ga} or its prefix have never been input to a $\mathcal{KEO}$ and σ_{ga} should not be the output of $\mathcal{SO}(\mathsf{ID}_{ga}, M_{ga})$.

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

Definition 6. *The HIBS scheme is* ACP-UF *secure if no PPT adversary $\mathcal{A}$ has non-negligible advantage in the ACP-UF game.*

We say that a HIBS is *secure* if it satisfies *Correctness* and *Existential Unforgeability.*

Gauntlet-ID Existential Unforgeability. We define the existential unforgeability against gauntlet identity and adaptive chosen plaintext attack for HIBS (gID-ACP-UF) as follows. The game is similar to the ACP-UF game, except in the end game phase, ID_{ga} or its prefix have never been input to a $\mathcal{SO}$ query. The HIBS scheme is *gID-ACP-UF* secure if no PPT adversary $\mathcal{A}$ has non-negligible advantage in the gID-ACP-UF game.

Remark: [21] and many IBS schemes have the $\mathcal{SO}$ query of the gauntlet ID to be handled by the random oracle. They also disallow the query of gauntlet ID to the $\mathcal{KEO}$, which is similar to our gID model.

Selective-ID Existential Unforgeability. We define the existential unforgeability against selective identity and adaptive chosen plaintext attack for HIBS (sID-ACP-UF) as follows. The game is similar to the gID-ACP-UF game, except before the Init. phase, $\mathcal{A}$ gives ID_{ga} to $\mathcal{S}$ in advance. The HIBS scheme is *sID-ACP-UF* secure if no PPT adversary $\mathcal{A}$ has non-negligible advantage in the sID-ACP-UF game.

3.2 Hierarchical Identity-Based Signcryption (HIBSC)

An ℓ-level HIBSC scheme consists of four algorithms: (Setup, Der, Signcrypt, Unsigncrypt). The algorithms are specified as follows:

- Setup: On input a security parameter 1^{λ_s}, the TA generates $\langle \mathsf{msk}_A, \mathsf{msk}_B, \mathsf{param}\rangle$ where msk_A (resp. msk_B) is the randomly generated master secret key for signcryptor (resp. unsigncryptor), and param is the corresponding public parameter.
- Der: On input an identity vector ID, its associated secret key SK_{ID}, and a string r, it returns the corresponding private key $SK_{\mathsf{ID}.r}$ (corresponds to param).
- Signcrypt: On input the private key of the signer ID_A, SK_{ID_A}, the recipient identity ID_B and a message M, it outputs a ciphertext σ corresponding to param.
- Unsigncrypt: On input the private key of the recipient ID_B, SK_{ID_B}, and a signature σ, it decrypts to a message M, sender identity ID_A and a signature s. It outputs M and ID_A if s is valid corresponding to $M, \mathsf{ID}_A, \mathsf{ID}_B, \mathsf{param}$ and signer = encryptor. Otherwise, it outputs $\perp$.

The security of a HIBSC consists of three requirements, namely *Correctness*, *Indistinguishability* and *Existential Unforgeability.* They are defined as follows:

Correctness. We require that $M \leftarrow \mathsf{Unsigncrypt}(SK_{\mathsf{ID}_B}, \mathsf{Signcrypt}(SK_{\mathsf{ID}_A}, \mathsf{ID}_B, M))$ for any message M, any private key SK_{ID} and its corresponding identity ID.

Indistinguishability. We define the indistinguishability against selective identity and adaptive chosen ciphertext attack for HIBS (sID-IND-CCA), as in the following game. We define the following oracles:

- $\mathcal{KEO}_{A/B}(\mathsf{ID})$: The Key Extraction Oracle with input ID will output the secret key SK_{ID} corresponding to msk_A or msk_B.
- $\mathcal{SCO}(\mathsf{ID}_A, \mathsf{ID}_B, M)$: The Signcryption Oracle with input signer identity ID_A, recipient identity ID_B and message M will output a ciphertext σ such that $\mathsf{Unsigncrypt}(SK_{\mathsf{ID}_B}, \sigma) = M$.

- $\mathcal{UO}(\mathsf{ID}_B, \sigma)$: The Unsigncryption Oracle with input recipient identity ID_B and ciphertext M will output a message M and the sender identity ID_A for a valid ciphertext σ or will output $\perp$ otherwise.

The Game is defined as follows:

1. (*Setup Phase*) Adversary $\mathcal{A}$ gives recipient ID_B^* to Simulator $\mathcal{S}$. Then $\mathcal{S}$ generates system parameter param and gives $(\mathsf{param}, \mathsf{msk}_A)$ to Adversary $\mathcal{A}$.
2. (*Probe 1 Phase*) $\mathcal{A}$ queries $\mathcal{KEO}_B$, $\mathcal{SCO}$, and $\mathcal{UO}$ in arbitrary interleaf.
3. (*Gauntlet Phase*) $\mathcal{A}$ gives two messages M_0^*, M_1^* and sender ID_A^* to $\mathcal{S}$. $\mathcal{S}$ randomly picks a bit b and returns $\sigma^* = \mathsf{Signcrypt}(SK_{\mathsf{ID}_A^*}, \mathsf{ID}_B^*, M_b^*)$ to $\mathcal{A}$.
4. (*Probe 2 Phase*) $\mathcal{A}$ queries $\mathcal{KEO}_B$, $\mathcal{SCO}$, and $\mathcal{UO}$ in arbitrary interleaf.
5. (*End Game*) $\mathcal{A}$ delivers a guess $\hat{b}$.

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

Existential Unforgeability. We define the existential unforgeability against adaptive chosen identity and adaptive chosen plaintext attack for HIBSC (ACP-UF), as in the following game.

1. (*Setup Phase*) $\mathcal{S}$ sets up system parameters and gives $(\mathsf{param}, \mathsf{msk}_B)$ to Adversary $\mathcal{A}$.
2. (*Probe Phase*) $\mathcal{A}$ queries $\mathcal{KEO}_A$, $\mathcal{SCO}$, and $\mathcal{UO}$ in arbitrary interleaf.
3. (*End Game*) $\mathcal{A}$ delivers a ciphertext σ^* and a recipient identity ID_B^*.

$\mathcal{A}$ *wins* if the following holds: $(M^*, \mathsf{ID}_A^*) \leftarrow \mathsf{Unsigncrypt}(\sigma^*, SK_{\mathsf{ID}_B^*})$, ID_A^* or its prefix has never been queried to the $\mathcal{KEO}_A$ and no $\mathcal{SO}$ 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 the probability that he wins. The HIBSC is *ACP-UF* secure if no PPT attacker has a non-negligible advantage in the Unforgeability Game.

We say that a HIBSC is *secure* if it satisfies *Correctness*, *Indistinguishability* and *Existential Unforgeability.*

4 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 [9].

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

Setup: To generate system parameters, the algorithm selects a random generator g, g_2, g_3, g_4, g_5, h_1, …, $h_\ell \in \mathbb{G}$, picks a random $\alpha \in \mathbb{Z}_p$, and sets $g_1 = g^\alpha$. It chooses an collision-resistant hash function $\mathcal{H}$. Note $\mathcal{H}$ is not a random oracle. Anyone, including the attacker, can compute $\mathcal{H}$ in private. The system parameters $\mathsf{param} = (g, g_1, g_2, g_3, g_4, g_5, h_1, \ldots, h_\ell, \mathcal{H})$ 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:

$$SK_{\mathsf{ID}} = \left(g_2^\alpha Q_{\mathsf{ID}}^r, \quad g^r, \quad h_{k+1}^r, \ldots, h_\ell^r\right) = (a_0, a_1, b_{k+1}, \ldots, b_\ell)$$

where $Q_{\mathsf{ID}} = h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3$. 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 [9].

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

$$D_1 = g^t, \quad D_2 = Q_{\mathsf{ID}}{}^t, \quad h = H(D_1, D_2, \mathsf{ID}, M, \mathsf{param})$$
$$\bar{a}_0 = a_0 Q_{\mathsf{ID}}{}^{\bar{r}}, \quad \bar{a}_1 = a_1 g^{\bar{r}}, \quad Z_1 = \bar{a}_0^h g_4^t, \quad Z_2 = \bar{a}_1^h g_5^t$$

The signature σ is (D_1, D_2, Z_1, Z_2).

Verify: The verifier receives a signature $\sigma = (D_1, D_2, Z_1, Z_2)$ for message M and signer ID, he computes $h = H(D_1, D_2, \mathsf{ID}, M, \mathsf{param})$. The verifier checks if both of the following relations hold:

$$\hat{e}(g, Z_1) \cdot \hat{e}(g_5, D_2) \stackrel{?}{=} \hat{e}(g_1, g_2)^h \cdot \hat{e}(D_1, g_4) \cdot \hat{e}(Z_2, Q_{\mathsf{ID}}) \quad (1)$$

$$\hat{e}(D_1, Q_{\mathsf{ID}}) \stackrel{?}{=} \hat{e}(g, D_2) \quad (2)$$

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

Remark: We can view Q_{ID} as the output of a hash function with input ID. In many HIBE schemes like [7, 36, 9], they specify $Q_{\mathsf{ID}} = h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3$.

4.1 Security Analysis

We will prove the security of the HIBS scheme using the new OrcYW assumption and other assumptions.

Theorem 1. *Assume $\mathcal{H}$ is a full-domain collision-resistant hash function. The hierarchical identity-based signature scheme* $\mathsf{HIBS}_{\mathsf{BBG}}(\ell)$ *is* correct *and* ACP-UF *secure provided the* OrcYW Assumption *holds.*

Proof Sketch: The correctness of the scheme is shown as follows:

$$\begin{aligned}\hat{e}(g, Z_1) \cdot \hat{e}(g_5, D_2) &= \hat{e}(g, g_2^\alpha \cdot (h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)^{r+\bar{r}})^h \cdot \hat{e}(g, g_4)^t \cdot \hat{e}(g_5, h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)^t \\ &= \hat{e}(g^\alpha, g_2)^h \cdot \hat{e}(g^{r+\bar{r}}, h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)^h \cdot \hat{e}(D_1, g_4) \cdot \hat{e}(g_5^t, h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3) \\ &= \hat{e}(g_1, g_2)^h \cdot \hat{e}(D_1, g_4) \cdot \hat{e}(Z_2, h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)\end{aligned}$$

Next, we prove ACP-UF.

Setup : Simulator $\mathcal{S}$ received a OrcYW Problem instance: $\{g^{x^i} : 0 \leq i \leq \ell\}$,$\gamma$, δ, g_4, g_5, γ_1, $\cdots$, γ_ℓ, a special identity chain $\mathbf{I}^* = \{I_1^*, \ldots, I_\ell^*\}$, a full-domain collision-resistant hash function $\mathcal{H}$ and an oracle O_{YW}.

$\mathcal{S}$ computes $g_1 = g^x$, $g_2 = g^{x^\ell + \gamma}$, $g_3 = g^{\delta + \sum_{j=1}^{\ell} x^{\ell-j+1} I_j^*}$ and $h_j = g^{\gamma_j} g^{-x^{\ell-j+1}}$, for $1 \leq j \leq \ell$. $\mathcal{S}$ randomly selects n identity chains $\mathbf{I}_1, \ldots, \mathbf{I}_n$, including $\mathbf{I}^*$ in it. $\mathcal{S}$ gives the public parameters $\mathsf{param} = (g, g_1, g_2, g_3, g_4, g_5, h_1, \ldots, h_\ell)$ and n identity chains to $\mathcal{A}$.

Simulating $\mathcal{KEO}$: Simulate as in [9]. For input identity $\mathsf{ID} = (\mathsf{id}_1, \dots, \mathsf{id}_u)$, if ID is $\mathbf{I}^*$ or a prefix of it, the simulator declares failure and exits. Otherwise there exists a $k \leq u$ such that $\mathsf{id}_k \neq I_k^*$. We set k be the smallest such index. To answer the query, the simulator derives a secret key for the identity $(\mathsf{id}_1, \dots, \mathsf{id}_k)$ from which it then constructs a private key for $\mathsf{ID} = (\mathsf{id}_1, \dots, \mathsf{id}_k, \dots, \mathsf{id}_u)$.

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

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

$$a_1 = g^r = g^{x^k/(\mathsf{id}_k - I_k^*)} g^{\tilde{r}}$$

Refer to [9] for the well-formedness of the secret key. The remaining $h_{k+1}^r, \dots, h_\ell^r$ can be computed by the simulator since they do not involve a $g^{x^{\ell+1}}$ term.

Simulating $\mathcal{SO}$: For query with $(\mathsf{ID}_\tau, m_\tau)$, if ID_τ is $\mathbf{I}^*$ or its prefix, $\mathcal{S}$ queries $O_{YW}(m_\tau, \mathsf{ID}_\tau)$ and forwards the answer to $\mathcal{A}$.

Otherwise, $\mathcal{S}$ computes the secret key of ID_τ as in $\mathcal{KEO}$, and then computes the signature using the secret key.

Simulation Deviation : It can be shown that the statistical distance among the Real World and the Ideal World is negligible.

Extraction : $\mathcal{A}$ outputs $(D_1^*, D_2^*, Z_1^*, Z_2^*)$ for signer $I^* \in \{\mathbf{I}_1, \dots, \mathbf{I}_n\}$ and message m^*. If $I^* \neq \mathbf{I}^*$, $\mathcal{S}$ declares failure and exits. Otherwise, as (I^*, m^*) has never been queried to $\mathcal{SO}$, $\mathcal{S}$ can use the signature to answer the problem instance.

Theorem 2. *Assume $\mathcal{H}$ is a full-domain collision-resistant hash function. The hierarchical identity-based signature scheme* $\mathsf{HIBS_{BBG}}(\ell)$ *is* correct *and* gID-ACP-UF *secure provided the* ℓ-DHI* Assumption *holds.*

Proof Sketch: Suppose a simulator $\mathcal{S}$ is given the ℓ-DHI* tuple $(g, g^x, \dots, g^{x^\ell})$. The gID-ACP-UF games begins with a simulator randomly picks $\mathcal{S}$ randomly selects n identity chains $\tilde{\mathsf{ID}} = \{\mathbf{I}_1, \dots, \mathbf{I}_n\}$. Denote $\mathbf{I}^* = \{I_1^*, \dots, I_\ell^*\}$ be an identity in $\tilde{\mathsf{ID}}$.

The simulator picks a random $\gamma \in \mathbb{Z}_p$ and assigns $g_1 = g^x, g_2 = g^{x^\ell} \cdot g^\gamma$. The simulator picks random $\gamma_1, \dots \gamma_\ell \in \mathbb{Z}_p$ and sets $h_j = g^{\gamma_j} g^{-x^{\ell-j+1}}$, for $1 \leq j \leq \ell$. It also picks a random $\delta \in \mathbb{Z}_p$ and computes $g_3 = g^{\delta + \sum_{j=1}^{\ell} x^{\ell-j+1} I_j^*}$. The simulator picks random $\omega_1, \omega_2 \in \mathbb{Z}_p$ and sets $g_4 = g^{\omega_1}, g_5 = g^{\omega_2}$. The simulator gives the adversary $\mathcal{A}$ the public parameters $\mathsf{param} = (g, g_1, g_2, g_3, g_4, g_5, h_1, \dots, h_\ell)$ and $\tilde{\mathsf{ID}}$. The corresponding (unknown) master secret key is $g_2^x = g^{x(x^\ell + \gamma)}$.

Simulating $\mathcal{KEO}$: Simulate as in [9]. For input identity $\mathsf{ID} = (\mathsf{id}_1, \dots, \mathsf{id}_u)$, if ID is $\mathbf{I}^*$ or a prefix of it, the simulator declares failure and exits. Otherwise there exists a $k \leq u$ such that $\mathsf{id}_k \neq I_k^*$. 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 $r = \frac{x^k}{(\mathsf{id}_k - I_k^*)} + \tilde{r}$ and compute:

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

$$a_1 = g^r = g^{x^k/(\mathsf{id}_k - I_k^*)} g^{\tilde{r}}$$

Refer to [9] 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 $g^{x^{\ell+1}}$ term.

Simulating $\mathcal{SO}$: For query with $(\mathsf{ID}_\tau, m_\tau)$, if ID_τ is $\mathbf{I}^*$ or its prefix, the simulator declares failure and exits. Otherwise, $\mathcal{S}$ computes the secret key of ID_τ as in $\mathcal{KEO}$, and then computes the signature using the secret key.

Simulation Deviation : It can be shown that the statistical distance among the Real World and the Ideal World is negligible.

Extraction : 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 $1/n_1$, $\hat{ID} = \mathbf{I}^*$. Otherwise $\mathcal{S}$ declares failure and exits. We denote $\sigma^* = (D_1^*, D_2^*, Z_1^*, Z_2^*)$. Then we compute $h = H(D_1^*, D_2^*, \mathbf{I}^*, M^*, \mathsf{param})$ and we have:

$$D_1^* = g^t \qquad Z_1^* = a_0^h g_4^t = a_0^h g^{\omega_1 t} \qquad Z_2^* = a_1^h g_5^t = a_1^h g^{\omega_2 t}$$

Then we can compute $a_0 = (Z_1^*/D_1^{*\omega_1})^{1/h}$ and $a_1 = (Z_2^*/D_1^{*\omega_2})^{1/h}$. Therefore for $\mathbf{I}^*$, we can set $a_1 = g^{\bar{r}}$ for some $\bar{r} \in \mathbb{Z}_p$. Then:

$$\begin{aligned} a_0 &= g_2^{\alpha} (g_3 \prod_{i=1}^{\ell} h_i^{I_i^*})^{\bar{r}} \\ &= g_2^{\alpha} (g^{\delta + \sum_{i=1}^{\ell} (\gamma_i I_i^*)})^{\bar{r}} \end{aligned}$$

Therefore the simulator returns $g^{x^{\ell+1}} = g_2^{\alpha}/g^{x\gamma} = a_0/(a_1^{\delta + \sum_{i=1}^{\ell}(\gamma_i I_i^*)} g^{x\gamma})$ as the solution.

4.2 Ordinary Signature from HIBS

For a secure HIBS scheme with $\ell = 1$, we obtain a secure IBS scheme. We further show that we have a secure (ordinary) signature scheme from a secure IBS scheme. The construction is as follows:

(Ordinary) signature scheme:

- **Setup:** The user secret key sk is the master key of IBS. The user public key pk is param of IBS.

- **Sign:** The signer picks random β and generates the secret key sk_β for its child β as in IBS. The signer uses sk_β to sign the message M as in IBS. The signature is the IBS signature plus β.
- **Verify:** The verifier checks the validity of the IBS signature with respect to identity β and pk.

We give our instantiation as follows:

(Ordinary) signature scheme $\mathsf{Sig}_{\mathsf{IBS.BBG}}$:

- **Setup:** To generate system parameters, the algorithm selects a random generator g, g_2, g_3, g_4, g_5, $h_1 \in \mathbb{G}$, picks a random $\alpha \in \mathbb{Z}_p$, and sets $g_1 = g^\alpha$. It chooses an collision-resistant hash function $\mathcal{H}$. The public keys are $pk = (g, g_1, g_2, g_3, g_4, g_5, h_1, \mathcal{H})$ and the secret key is g_2^α.
- **Sign:** The signer picks random $t, \beta, \bar{r} \in \mathbb{Z}_p$, and computes:

$$D_1 = g^t, \quad D_2 = \left(g_3 h_1^\beta\right)^t, \quad h = H(D_1, D_2, \beta, M, pk)$$
$$\bar{a}_0 = g_2^\alpha \left(g_3 h_1^\beta\right)^{\bar{r}}, \quad \bar{a}_1 = g^{\bar{r}}, \quad Z_1 = \bar{a}_0^h g_4^t, \quad Z_2 = \bar{a}_1^h g_5^t$$

The signature σ is $(D_1, D_2, Z_1, Z_2, \beta)$.
- **Verify:** The verifier receives a signature $\sigma = (D_1, D_2, Z_1, Z_2, \beta)$ for message M, he computes $h = H(D_1, D_2, \beta, M, pk)$. The verifier checks if both of the following relations hold:

$$\hat{e}(g, Z_1) \cdot \hat{e}(g_5, D_2) \stackrel{?}{=} \hat{e}(g_1, g_2)^h \cdot \hat{e}(D_1, g_4) \cdot \hat{e}(Z_2, g_3 h_1^\beta) \tag{3}$$
$$\hat{e}(D_1, g_3 h_1^\beta) \stackrel{?}{=} \hat{e}(g, D_2) \tag{4}$$

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

5 Plausibility arguments for the intractability of the OrcYW Assumption

Assuming knowledge of $\omega_1 = \log_g g_4$ *and* $\omega_2 = \log_g g_5$, then an OrcYW Problem solver can solve the DHI* Problem. But $\mathcal{S}$ can also solve the DHI* Problem from one OrcYW query outcome, using this knowledge. Let $\tilde{t} = \log_g \tilde{D}_1$, $\tilde{t}' = \log_Q \tilde{D}_2$. Then Relation (2) implies $\tilde{t} = \tilde{t}'$. Let A, B be such that $\tilde{Z}_1 = g_2^{x\tilde{h}} A g_4^{\tilde{t}}$, $\tilde{Z}_2 = B g_5^{\tilde{t}}$. Let $\tilde{r} = (\tilde{h})^{-1} \log_Q A$, $\tilde{r}' = (\tilde{h})^{-1} \log_g B$. Then Relation (1) implies $\tilde{r} = \tilde{r}'$. Finally, $\mathcal{S}$ computes $\bar{A} = g_2^x Q^{\tilde{r}} = (\tilde{Z}_1 g_4^{-\tilde{t}})^{1/\tilde{h}} = (\tilde{Z}_1 (\tilde{D}_1)^{-\omega_1})^{1/\tilde{h}}$, $\bar{B}$ $= g^{\tilde{r}} = (\tilde{Z}_2 g_5^{-\tilde{t}})^{1/\tilde{h}} = (\tilde{Z}_2 (\tilde{D}_1)^{-\omega_2})^{1/\tilde{h}}$, $g_2^x = \bar{A}\bar{B}^{-\delta - \sum_{i=1}^{\ell} \gamma_i I_i}$. Then $\mathcal{S}$ computes $g^{x^{\ell+1}} = g_2^x g^{-x\gamma}$.

Therefore, the OrcYW Assumption is in the category of *one-more* assumptions, akin to the *one-more RSA Assumption* and the *one-more DL Assumption* [4]. It is more akin to the latter than the former. The state-of-the-art attack on the parallel one-more DL assumption is Schnorr's ROS attack [33] and Wagner's generalized birthday (GB) attack [35]. Below, we examine the plausibility of our OrcYW Assumption against attackers motivated by ROS attackers and GB attackers.

Assume m_1, $\cdots$, m_q are queried to O_{YW} and the outputs are $(D_{1,\tau}, D_{2,\tau}, Z_{1,\tau}, Z_{2,\tau})$, $1 \le \tau \le q$. An attack motivated by Schnorr's ROS [33] attack would attempt to construct γ_1, $\cdots$, γ_q satisfying

$$\tilde{D}_1 = \prod_\tau D_{1,\tau}^{\gamma_\tau} = g^{\sum \gamma_\tau t_\tau},$$

$$\begin{aligned}
\tilde{D}_2 &= \prod_\tau D_{2,\tau}^{\gamma_\tau} = Q^{\sum \gamma_\tau t_\tau}, \\
\tilde{h} &= \sum_\tau \gamma_\tau h_\tau, \\
\tilde{Z}_1 &= \prod_\tau Z_{1,\tau}^{\gamma_\tau} = g_2^{x \sum \gamma_\tau h_\tau} Q^{\sum \gamma_\tau r_\tau h_\tau} g_4^{\sum \gamma_\tau t_\tau}, \\
\tilde{Z}_2 &= \prod_\tau Z_{2,\tau}^{\gamma_\tau} = g^{\sum \gamma_\tau r_\tau h_\tau} g_5^{\sum \gamma_\tau t_\tau},
\end{aligned}$$

The crucial relation is the one about a linear dependence of the hash outputs. Schnorr's blind signature [33] also suffers from similar attack, and he relates the security of the blind signature scheme to the ROS problem.

6 Efficient HIBSC without Random Oracles

Motivated by [1]'s generic composition of SignCryption from Encrypt and Sign, 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 [9]'s HIBE and our HIBS in Section 4. 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 show the security of the outcome without insider attacks. They also give the guidelines of *whenever signing include receiver identity in message* and *whenever 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 composed of 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 composed 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, the constant size HIBE from [9] and the transformation technique in [10].

Boneh et al. [10] 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 gauntlet identity, he must have to forge a signature of Sig. Boneh et al. further suggest that a secure encapsulation scheme and a secure message authentication code can be used together in order to replace the strong one-time signature scheme.

As a result, we obtain a constant size HIBSC secure without random oracles. We use [10]'s instantiation of encapsulation scheme. The instantiation is given below:

Setup, **Der:** same as section 4. In addition, let $(\mathsf{Mac}, \mathsf{Vfy})$ be a message authentication code. We assume all signers get the secret keys from master key A $g_2^{\alpha_A}$ and all recipients get the secret keys from master key B $g_2^{\alpha_B}$. Therefore we have $g_{1A} = g^{\alpha_A}$ and $g_{1B} = g^{\alpha_B}$. All other public parameters remain the same as section 4.

Signcrypt: For a user with identity $\mathsf{ID}_A = (\mathsf{id}_1, \ldots, \mathsf{id}_k)$ and private key SK_{ID_A}, he signcrypts a message M to recipient $I_B = (I_1, \ldots, I_j)$ as follows. He picks random $t, \chi \in \mathbb{Z}_p$, and computes:

$$\begin{gathered}
C_1 = g^t, \quad C_2 = (h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3)^t, \quad I_{j+1} = \mathcal{H}_3(\chi), \quad k_1 = \mathcal{H}_4(\chi), \\
h = \mathcal{H}(C_1, C_2, \mathsf{ID}_A, I_B, \mathsf{id}', M, \mathsf{param}), \quad C_3 = {a_0}^h g_4^t, \quad C_4 = {a_1}^h g_5^t, \\
C_5 = \mathcal{H}_2(\hat{e}(g_{1B}, g_2)^t) \oplus \langle M, \mathsf{ID}_A, C_2, C_3, C_4, \chi \rangle, \quad C_6 = (h_1^{I_1} \cdots h_j^{I_j} h_{j+1}^{I_{j+1}} \cdot g_3)^t, \\
C_7 = \mathsf{tag} = \mathsf{Mac}_{k_1}(\mathsf{ID}_A, I_B, I_{j+1}, C_1, \cdots, C_6)
\end{gathered}$$

The ciphertext σ is $(C_1, C_5, C_6, C_7, I_{j+1})$. Generically,

$$C_5 = \mathsf{SKE.Enc}(\mathsf{key} = \hat{e}(g_1, g_2)^t, \mathsf{ptxt} = \langle M, \mathsf{ID}_A, C_2, C_3, C_4 \rangle)$$

We have adopted Boneh et al.'s [10] tag design above.

Unsigncrypt: The recipient I_B with private key $SK_{I_B} = (a_0, a_1, b_{j+1}, \ldots, b_\ell)$ receives a ciphertext σ $(C_1, C_5, C_6, C_7, I_{j+1})$, he computes:

$$\begin{aligned}
W = \hat{e}(C_1, a_0 b_{j+1}^{I_{j+1}}) / \hat{e}(a_1, C_6) \quad \langle M, \mathsf{ID}_A, C_2, C_3, C_4, \chi \rangle = C_5 \oplus \mathcal{H}_2(W) \\
h = \mathcal{H}(C_1, C_2, \mathsf{ID}_A, I_B, I_{j+1}, M, \mathsf{param})
\end{aligned}$$

Denote $\mathsf{ID}_A = (\mathsf{id}_1, \ldots, \mathsf{id}_k)$. The recipient computes $k_1 = \mathcal{H}_4(\chi)$ and checks if:

$$\begin{aligned}
\hat{e}(g, C_3) \cdot \hat{e}(g_5, C_2) &\overset{?}{=} \hat{e}(g_{1A}, g_2)^h \cdot \hat{e}(C_1, g_4) \cdot \hat{e}(C_4, h_1^{\mathsf{id}_1} \cdots h_k^{\mathsf{id}_k} \cdot g_3) \\
1 &\overset{?}{=} \mathsf{Vfy}_{k_1}(\mathsf{ID}_A, I_B, I_{j+1}, C_1, \cdots, C_6, C_7) \\
I_{j+1} &\overset{?}{=} \mathcal{H}_3(\chi)
\end{aligned}$$

The recipient outputs M if they are all true. Otherwise, he outputs $\perp$.

Security Analysis Our HIBSC scheme is secure without random oracles. In particular, it can also imply a secure identity based signcryption scheme without random oracles.

Proposition 1. *Our HIBSC scheme is correct, sID-IND-CCA secure and ACP-UF secure assuming the decisional wBDHI* assumption, the OrcYW assumption holds and Schnorr's ROS Problem is hard.*

The correctness is straightforward.

For indistinguishability, combining the sID-IND-CPA proofs in [9], the transformation theorem in [10] and also the composition theorem of signature and encryption in [1], it implies that our HIBSC is sID-IND-CCA secure.

For existential unforgeability, the HIBSC scheme is ACP-UF secure by Theorem 2 and the composition theorem of signature and encryption in [1].

7 Conclusions

We presented the first constant-size HIBS and HIBSC provable without random oracles. In the reductionist security proofs, we either use an interactive intractability assumption, or use the gID models. We also need the sID model for HIBSC security proof. It is an open problem to avoid these models and assumptions.

Acknowledgements to Jin Li and Kenny Paterson for pointing out an aspect of random oracles, and to Hong Kong Earmarked Grants 4232-03E and 4328-02E for sponsorship.

References

1. J. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption. In *Proc. CRYPTO 2002*, pages 83–107. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2332.
2. M. Bellare, A. Boldyreva, and A. Palacio. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. In *EUROCRYPT 2004*, pages 171–188. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3027.
3. M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. In *Proc. EUROCRYPT 2004*, pages 268–286. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3027.
4. M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The one-more-RSA-inversion problem and the security of Chaum's blind signature scheme. *J. of Cryptology*, pages 185–215, 2003.
5. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. 1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.
6. D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In *Proc. EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238. Springer-Verlag, 2004.
7. D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In *Proc. CRYPTO 2004*, volume 3152 of *LNCS*, pages 443–459. Springer-Verlag, 2004.
8. D. Boneh and X. Boyen. Short signatures without random oracles. In *Proc. EUROCRYPT 2004*, pages 56–73. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3027.
9. D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456. Springer, 2005.
10. D. Boneh, R. Canatti, S. Halevi, and J. Katz. Chosen-Ciphertext Security from Identity-Based Encryption. http://crypto.stanford.edu/~dabo/abstracts/ccaibejour.html, 2005.
11. D. Boneh and M. Franklin. Identity-based encryption from the Weil paring. In *Proc. CRYPTO 2001*, pages 213–229. Springer-Verlag, 2001. Lecture Notes in Computer Science No. 2139.
12. D. Boneh and J. Katz. Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In *CT-RSA 2005*, volume 3376 of *LNCS*, pages 87–103. Springer-Verlag, 2005.

13. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 514–532. Springer-Verlag, 2001.
14. D. Boneh, I. Mironov, and V. Shoup. A Secure Signature Scheme from Bilinear Maps. In *CT-RSA 2003, Proceedings*, volume 2612 of *Lecture Notes in Computer Science*, pages 98–110. Springer, 2003.
15. X. Boyen. Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. In *Proc. CRYPTO 2003*, pages 382–398. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2729.
16. X. Boyen and B. Waters. Compact group signatures without random oracles. Cryptology ePrint Archive, Report 2005/381, 2005. http://eprint.iacr.org/.
17. J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *Proc. CRYPTO 2004*. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3152.
18. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *Proc. 13th ACM Symp. on Theory of Computing*, pages 209–128. ACM Press, 1998.
19. R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. In *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 255–271. Springer-Verlag, 2003.
20. R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 207–222. Springer-Verlag, 2004.
21. J. Cha and J. Cheon. An identity-based signature from gap diffie-hellman groups. In *Practice and Theory in Public Key Cryptography – PKC'2003*, pages 18–30. Springer-Verlag, 2003. Lecture Notes in Computer Science No. 2567.
22. S. S. Chow, T. H. Yuen, L. C. Hui, and S. Yiu. Signcryption in hierarchical identity based cryptosystem. In *SEC 2005*, pages 443–457, 2005.
23. R. Cramer and V. 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.
24. Y. Dodis, M. J. Freedman, S. Jarecki, and S. Walfish. Versatile padding schemes for joint signature and encryption. In *ACM Conference on Computer and Communications Security 2004*, pages 344–353. ACM Press, 2004.
25. M. Fischlin. The Cramer-Shoup strong-RSA signature scheme revisited. In *PKC*, pages 116–129, 2003.
26. R. Gennaro, S. Halevi, and T. Rabin. Secure hash-and-sign signatures without the random oracle. In *Proc. EUROCRYPT 99*, volume 1592 of *LNCS*, pages 123–139. Springer-Verlag, 1999.
27. C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. In *Proc. ASIACRYPT 2002*, pages 548–566. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2501.
28. O. Goldreich. *Foundations of Cryptography*, volume 1 and 2. Cambridge Univesity Press, 2001 and 2005.
29. S.-H. Heng and K. Kurosawa. k-resilient identity-based encryption in the standard model. In *CT-RSA 2004*, pages 67–80. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 2964.
30. J. Horwitz and B. Lynn. Toward Hierarchical Identity-Based Encryption. In *EUROCRYPT 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 466–481. Springer, 2002.
31. A. Lysyanskaya, R. Rivest, A. Sahai, and S. Wolf. Pseudonym systems. In *Selected Areas in Cryptography (SAC) 1999*, volume 1758 of *LNCS*, pages 184–199. Springer-Verlag, 1999.
32. J. Malone-Lee. Identity-based signcryption. Cryptology ePrint Archive, Report 2002/098, 2002. http://eprint.iacr.org/.
33. C. P. Schnorr. Security of blind discrete log signatures against interactive attacks. In *ICICS 2001*, volume 2229, pages 1–12. Springer–Verlag, 2001. LNCS.
34. A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. CRYPTO 84*, pages 47–53. Springer-Verlag, 1984. Lecture Notes in Computer Science No. 196.
35. D. Wagner. A generalized birthday problem. In *Proc. CRYPTO 2002*, pages 288–303. Springer-Verlag, 2002. Lecture Notes in Computer Science No. 2442.
36. B. Waters. Chosen-ciphertext security from identity-based encryption. In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer-Verlag, 2005.
37. V. K. Wei and T. H. Yuen. More short signatures without random oracles. To appear in IJNS. Cryptology ePrint Archive, Report 2005/463, 2005. http://eprint.iacr.org/.
38. T. H. Yuen and V. K. Wei. Fast and proven secure blind identity-based signcryption from pairings. In *Proc. CT-RSA 2005*, volume 3376 of *LNCS*, pages 305–322. Springer-Verlag, 2005.
39. F. Zhang, X. Chen, W. Susilo, and Y. Mu. A new short signature scheme without random oracles from bilinear pairings. Cryptology ePrint Archive, Report 2005/386, 2005. http://eprint.iacr.org/.
40. F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In *PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 277–290. Springer, 2004.

41. Y. Zheng. Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost (encryption). In *Proc. CRYPTO 97*, pages 165–179. Springer-Verlag, 1997. Lecture Notes in Computer Science No. 1294.