Black-Box Constructions of Signature Schemes in the Bounded Leakage Setting

Qiong Huang, Jianye Huang

College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China.

Abstract

To simplify the certificate management procedures, Shamir introduced the concept of *identity-based* cryptography (IBC). However, the key escrow problem is inherent in IBC. To get rid of it, Al-Riyami and Paterson introduced in 2003 the notion of *certificateless* cryptography (CLC). However, if a cryptosystem is not perfectly implemented, adversaries would be able to obtain part of the system's secret state via *side-channel attacks*, and thus may break the system. This is not considered in the security model of traditional cryptographic primitives. *Leakage-resilient cryptography* was then proposed to prevent adversaries from doing so. There are fruitful works on leakage-resilient encryption schemes, while there are not many on signature schemes in the leakage setting.

In this work, we review the folklore generic constructions of identity-based signature and certificateless signature, and show that if the underlying primitives are leakage-resilient, so are the resulting identity-based signature scheme and certificateless signature scheme. The leakage rate follows the minimum one of the underlying primitives. We also show some instantiations of these generic constructions.

Key words: identity-based signature, certificateless signature, black-box construction, bounded leakage model, leakage-resilient cryptography

1. Introduction

Digital signature is the analogy of message authentication code (MAC) in the public key setting that ensures the integrity of transmitted messages over public channels. In traditional public key infrastructure (PKI), to associate a user's identity with its public key, a digital certificate issued by a Certificate Authority (CA) is needed. If Alice wants to send an important message m to Bob and does not want anyone to modify m, she first registers her public key to a CA and obtains a digital certificate $Cert_A$ from the CA. Alice then signs m using her secret signing key, and sends m and the signature σ along with her certificate to Bob. To check the integrity of the message, Bob first verifies $Cert_A$ and then verifies σ under the public key of Alice given in the certificate. If both verifications pass, Bob believes that m was not modified by anyone else.

Email addresses: qhuang@scau.edu.cn (Qiong Huang), hjnubys@stu.scau.edu.cn (Jianye Huang)

Although PKI ensures the binding of a user's identity and its public key and is well used in practice, it suffers from the certificate management problem. Certificate creation, storage, revocation and etc, require high computation and storage costs.Therefore, we need a more convenient way to deal with the identity-public key binding problem.

To simplify the certificate management procedure, Shamir [1] introduced the notion of *identity-based cryptography* (IBC) in 1984, in which a user can use any (personal) information as its public key, such as its name, telephone number, email address, IP address and etc. A third party called Key Generation Center (KGC)[1], is then responsible for generating secret keys for all users in the system. IBC reduces the computational and storage effort by simplifying the key distribution, which makes it advantageous over the traditional PKI. On the other hand, however, IBC inherently suffers from the key escrow problem, i.e. the KGC knows all users' private keys, and therefore a trusted KGC is necessary. Moreover, a secure channel is required for key issuance between the KGC and a user.

To get rid of the key escrow problem, Al-Riyami and Paterson introduced the notion of *certificateless cryptography* in 2003 [2]. In a certificateless signature (CLS) scheme, a KGC is responsible for issuing a partial secret key psk to a user according to its identity ID. Besides, the user itself chooses a public key upk along with some secret information usk. Only if the user knows both psk and usk can it sign a message. Verification of a signature requires the knowledge of both the signer's identity ID and its public key upk. Thus, the KGC in a certificateless cryptosystem could not sign a message on behalf of a user, and the key escrow problem does not exist any more.

(*Leakage-Resilient Cryptography*). Traditional cryptography (including IBC and CLC) focuses on that the input/output of a cryptosystem does not affect the system's security. However, recent works have shown that if a cryptosystem is not implemented well, an adversary is capable of obtaining (part of) the system secret state (even the secret key) via *side channel attacks*, which is not captured in the security model. For example, Halderman *et al.* showed in their seminal paper [3] the *cold boot attack* on encryption keys that are stored in the memory even when it loses power. Other side-channel attacks include running-time attack [4], electromagnetic radiation analysis [5], power consumption analysis [6], fault detection [7] and etc. To address side-channel attacks, Dziembowski *et al.* [8] introduced *leakage-resilient cryptography*, which aims to constructing cryptographic schemes that remain secure even if the adversary is able to obtain part of the secret state of the scheme. Dziembowski *et al.* [8] constructed stream ciphers under the assumption *only computation leaks information* in the influential work [9] of Micali and Reyzin.

How to formalize the *leakage* is one of the major research topics of leakage-resilient cryptography. Inspired by [9, 10], the security challenger additionally provides the adversary a leakage oracle $O_L(\cdot)$, which takes as input a polynomial-time computable *leakage function* $f(\cdot)$ chosen by the adversary and outputs the value of the function on input the system's secret key, e.g. $f(sk)$. It is required that all leakage functions should be efficiently computable since we only consider probabilistic polynomial-time adversaries. If we additionally consider the leakage on the randomness used in the computation, e.g. the random number used in the generation of a signature, we call this stronger notion *fully leakage resilience* (FLR) [11]. To prevent the adversary from winning the security game trivially, we usually restrict

[1] KGC is also known as the *Public Key Generator* (PKG) in many other works.

the amount of leakage to the adversary. In the *bounded leakage-resilient* (BLR) model, the amount of leakage should satisfy $\sum_{i=1}^{q} \|f_i(X)\| \leq \lambda$ for some bound λ after q leakage queries in order to ensure certain entropy of the secret state. Otherwise, secure cryptographic schemes are never achievable if the system internal state keeps unchanged over time. If we do not limit the total length of leakage the adversary obtains over time, we then resort to the *continuous leakage-resilient* (CLR) model [12], in which the system's secret state is updated periodically while the public information keeps unchanged. The adversary is allowed to get a limited amount of leakage in each period.

There have been many works on leakage-resilient encryption schemes, but not many on the construction of signature schemes in the leakage setting. In this paper we focus on the (black-box) construction of leakage-resilient signature schemes in the bounded leakage model.

1.1. Related Work

(*Leakage-Resilient Signature*). Katz and Vaikuntanathan proposed signature schemes which are existentially unforgeable under chosen-message attacks in the bounded leakage model based on standard assumptions [11] in Asiacrypt 2009. There are also some leakage-resilient signature schemes secure in other leakage models, for example, continuous leakage model [12], hard-to-invert leakage model [13], auxiliary input model [14] and etc. Furthermore, full leakage model was considered for digital signature [15, 14], in which the adversary is capable of obtain leakage of both the secret key and the randomness used in the signing procedure. Wang *et al.* [16, 17] proposed a leakage-resilient and strongly unforgeable signature scheme following the framework of [18], which however, requires adding elements to the signature key pair. Recently, [19, 20] further proved the leakage resilience of Huang *et al.*'s strongly unforgeable signature schemes [21], which removes the need of changing the key pair of the underlying signature scheme.

(*Identity-Based Signature*). Shamir proposed the first identity-based signature (IBS) scheme based on integer factorization problem in [1]. Since then, a lot of IBS schemes have been proposed, e.g. [22, 23, 24, 25, 26]. To name a few, a provably secure IBS scheme was proposed by Hess in [23], which is existentially unforgeable under adaptively chosen message and fixed ID attacks. In 2003, Choon *et al.* [24] proposed an IBS scheme based Gap Diffie-Hellman groups. They formalized the definition of security of IBS, named existential unforgeability under adaptive chosen-message and ID attacks. An IBS scheme supporting batch verification was later proposed by Cheon *et al.* in [25], which is a variant of the scheme given in [24]. Chen *et al.* [26] proposed an IBS scheme without the need of a trusted KGC, eliminating the inherent key escrow problem. In the leakage setting, Li *et al.* [27] proposed a traceable IBS scheme and proved its security under the hardness of DDH problem. Wu *et al.* [28] proposed another leakage-resilient IBS scheme based on Galindo and Vivek's leakage-resilient signature scheme [29] under the continuous leakage model, and proved that their IBS scheme is secure against leakage attacks under the generic group model.

(*Certificateless Signature*). Al-Riyami *et al.* [2] proposed the first CLS scheme in 2003. Later, many different security models and schemes [30, 31, 32, 33] as well as applications [34, 35, 36, 37, 38] of CLS have been proposed. However, lots of the existing certificateless schemes are proven secure in the random oracle model. Liu *et al.* [39] proposed the first CLS scheme without random oracles. However, [40, 41] demonstrated that Liu *et al.*'s CLS scheme cannot resist the *KGC attacks* [42] where the KGC becomes malicious and generates its master key in a special way so that even if the KGC does not know a user's secret key, it still can sign a message (or decrypt a ciphertext) on behalf of the user. Xia *et al.* pointed out that the CLS schemes in the standard model [39, 43] are insecure under the *key replacement attacks*. However, to the best of our knowledge, there is no work on certificateless signature in the leakage setting in the literature.

1.2. Our Contributions

In this work we study the black-box construction of leakage-resilient identity-based signature scheme and certificateless signature scheme. That is, we construct IBS and CLS from some basic cryptographic primitives and treat them as black boxes. We do not care about the internal implementation of these primitives. We show that the folklore generic constructions of IBS and CLS are leakage-resilient if the underlying building blocks are leakage-resilient. More precisely, we make the following contributions in the paper.

1. It is known that identity-based signature scheme could be constructed from a standard signature scheme in a black-box manner [44, 45]. If the signature scheme is existentially unforgeable under chosen-message attacks, the resulting IBS is then existentially unforgeable under chosen-message and chosen-identity attacks. However, it is only known to hold in the traditional security model. In this work we formally prove that the aforementioned claim also holds in the leakage setting. Namely, if the signature scheme is leakage-resilient, so is the resulting IBS scheme.

2. Naor [46] observed that a standard signature scheme could be obtained via a simple transform from an IBE scheme. The user secret key in IBE could serve as a signature on the identity. This transform could be extended to convert a 2-level Hierarchical IBE (HIBE) scheme to an IBS scheme. We formally prove that if the underlying 2-level HIBE is one-way secure in the leakage setting, the resulting IBS is also leakage-resilient.

3. Hu *et al.* [47] showed that a secure CLS scheme can be constructed from an IBS scheme and a standard signature scheme. We prove that the same method could also be used to construct a leakage-resilient CLS scheme. That is, if the underlying signature scheme and the IBS scheme are both leakage-resilient, so is the resulting CLS scheme.

Among all our proofs, the major difficulty lies in the simulation of the leakage oracle. Fortunately, by the hard-coding technique [16, 17, 19, 20] the problem can be solved. The leakage rate of the resulting scheme follows the minimum one of the underlying building blocks.

1.3. Paper Organization

In the next section we present some related definitions and adversarial models of signature schemes. In Sect. 3, we describe two generic constructions of IBS and prove their security in the leakage setting. In Sect. 4, we describe the generic construction of CLS and prove its leakage resilience. In Sect. 5, we discuss about the instantiations of these generic construction of leakage-resilient signature schemes. Finally, we conclude the paper in Sect. 6.

2. Definitions and Security Models

2.1. Digital Signature

Definition 1 (Digital Signature)

A digital signature scheme is specified by a triple of probabilistic polynomial-time (PPT) algorithms $(\mathsf{Kg}, \mathsf{Sig}, \mathsf{Ver})$, called key generation algorithm, signing algorithm and verification algorithm, respectively.

- **Key Generation Algorithm.** On input 1^k, the algorithm generates a signing/verification key pair (vk, sk), i.e. $(vk, sk) \leftarrow \mathsf{Kg}(1^k)$.
- **Signing Algorithm.** On input a signing key sk and a message m, the algorithm returns a signature σ, i.e. $\sigma \leftarrow \mathsf{Sig}(sk, m)$.
- **Verification Algorithm.** On input a verification key vk and a message/signature pair (m, σ), the algorithm returns 1 for acceptance or 0 for rejection, i.e. $1/0 \leftarrow \mathsf{Ver}(vk, m, \sigma)$.

Security Model. The *de facto* security notion of digital signature is *existential unforgeability under adaptive chosen-message attack*. Let $\Sigma = (\mathsf{Kg}, \mathsf{Sig}, \mathsf{Ver})$ be a signature scheme. Then consider the following experiment, in which C is a challenger and $\mathcal{A}$ is an adversary who tries to forge a valid message/signature pair.

EUF-CMA Experiment $\mathsf{EUF\text{-}CMA}_{\mathcal{A},\Sigma}(1^k)$:

1. C runs $(vk, sk) \leftarrow \mathsf{Kg}(1^k)$ and gives the verification key vk to $\mathcal{A}$. C keeps the signing key sk as a secret and maintains a query list Q_s which is initially empty.
2. $\mathcal{A}$ accesses to a signing oracle $\mathcal{SO}(\cdot)$ adaptively for polynomially many times. Given a message m, the signing oracle returns a signature σ obtained by running Sig algorithm. Set $Q_s = Q_s \cup \{m\}$.
3. Finally, $\mathcal{A}$ outputs $(\hat{m}, \hat{\sigma})$. $\mathcal{A}$ wins if and only if (a) $\mathsf{Ver}(\hat{m}, \hat{\sigma}) = 1$ and (b) $\hat{m} \notin Q_s$. The advantage of $\mathcal{A}$ in the experiment is defined to be its winning probability.

Definition 2 (EUF-CMA Security)

A signature scheme Σ is *existentially unforgeable under adaptive chosen-message attack* (EUF-CMA secure) if no PPT adversary $\mathcal{A}$ has a non-negligible advantage in the experiment $\mathsf{EUF\text{-}CMA}_{\mathcal{A},\Sigma}(1^k)$, i.e.

$$\Pr\left[\mathsf{Ver}(\hat{m}, \hat{\sigma}) = 1 \wedge \hat{m} \notin Q_s : (\hat{m}, \hat{\sigma}) \leftarrow \mathcal{A}^{\mathcal{SO}(\cdot)}(vk)\right] \leq \mathrm{negl}(k),$$

where negl $(\cdot)$ is a negligible function in k.

Leakage-Resilient Unforgeability. To model an adversary against a signature scheme, which is allowed to launch side channel attacks, we additionally allow $\mathcal{A}$ to access to a leakage oracle $\mathcal{LO}(\cdot)$. Given the ith adversarially chosen leakage function $f_i(\cdot)$, $\mathcal{LO}(f_i)$ returns $\Lambda_i := f_i(sk)$ where $|\Lambda_i| = \lambda_i$. W.l.o.g., we suppose that the adversary makes at most q_L leakage queries. We have following definition.

Definition 3 (Leakage-Resilient Unforgeability)

A signature scheme Σ is *λ-leakage-resilient and existentially unforgeable under adaptive chosen-message attacks* (λ-LR-EUF-CMA secure) if the probability that any PPT adversary $\mathcal{A}$ succeeds in outputting a valid signature on a new message in the modified experiment is negligible, i.e.

$$\Pr\left[\mathsf{Ver}(vk, \hat{m}, \hat{\sigma}) = 1 \wedge \hat{m} \notin Q_s \wedge \sum_{i=1}^{q_L} \lambda_i \leq \lambda : (\hat{m}, \hat{\sigma}) \leftarrow \mathcal{A}^{SO(\cdot), \mathcal{LO}(\cdot)}(vk)\right] \leq \mathrm{negl}(k).$$

2.2. ID-based Signature

Identity-based signature (IBS) scheme differs from a standard signature scheme mainly in that the signer's public key in IBS could be any identity string and that its secret key is generated by a third party. Below is the formal definition of IBS.

Definition 4 (IBS)

An identity-based signature scheme $\Sigma = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Sig}, \mathsf{Ver})$ is specified by a tuple of four PPT algorithms, called setup algorithm, key extraction algorithm, signing algorithm and verification algorithm, respectively.

- **Setup Algorithm.** On input 1^k, KGC runs Setup to generate a master public/secret key pair (mpk, msk), i.e. $(mpk, msk) \leftarrow \mathsf{Setup}(1^k)$.
- **Extraction Algorithm.** On input master key msk along with an identify ID, KGC runs $\mathsf{Extract}$ to generate the corresponding signing key sk_{ID}, i.e. $sk_{ID} \leftarrow \mathsf{Extract}(msk, ID)$.
- **Signing Algorithm.** On input a user signing key sk_{ID}, and a message m, the algorithm returns a signature σ, i.e. $\sigma \leftarrow \mathsf{Sig}(sk_{ID}, m)$.
- **Verification Algorithm.** On input a tuple (ID, m, σ), the verification algorithm returns 1 for acceptance or 0 for rejection, i.e. $0/1 \leftarrow \mathsf{Ver}(ID, m, \sigma)$.

Note that we assume the master public key mpk is implicitly used in last three algorithms described above and therefore is omitted for simplicity.

Security Model. The *de factor* security notion of IBS is existential unforgeability under adaptive chosen-message and chosen-ID attack, which is a generalization of that of standard signature. Let $\Sigma = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Sig}, \mathsf{Ver})$ be an IBS scheme. Then consider the following experiment, in which C is the challenger and $\mathcal{A}$ is a PPT adversary.

EUF-CMIA Experiment of IBS $\mathsf{CMA\text{-}IDA}_{\mathcal{A},\Sigma}(1^k)$:

1. C runs $(mpk, msk) \leftarrow \mathsf{Setup}(1^k)$ and gives mpk to $\mathcal{A}$. It sets two initially empty list, Q_e and Q_s, and initializes the system state $\mathcal{S} = \{(KGC, msk)\}$.

2. $\mathcal{A}$ accesses to following oracles:

   CreateUser Oracle $CO(\cdot)$**.** On input an identity ID, if ID has already been created, nothing is to be taken. Otherwise, generate $sk_{ID} \leftarrow \mathsf{Extract}(msk, ID)$ and update $\mathcal{S} = \mathcal{S} \cup \{(ID, sk_{ID})\}$.

   Extraction Oracle $\mathcal{E}O(\cdot)$**.** Given an identity ID, check the list $\mathcal{S}$ and return the corresponding sk_{ID}. Set $Q_e = Q_e \cup \{ID\}$.

   Signing Oracle $\mathcal{S}O(\cdot)$**.** Given a tuple (ID, m), retrieve the corresponding sk_{ID} from $\mathcal{S}$ and return $\sigma \leftarrow \mathsf{Sig}(sk_{ID}, m)$. Set $Q_s = Q_s \cup \{(ID, m)\}$.

3. Finally, $\mathcal{A}$ outputs $(\hat{ID}, \hat{m}, \hat{\sigma})$. $\mathcal{A}$ wins if and only if (a) $\mathsf{Ver}(\hat{ID}, \hat{m}, \hat{\sigma}) = 1$, (b) $\hat{ID} \notin Q_e$ and (c) $(\hat{ID}, \hat{m}) \notin Q_s$. The advantage of $\mathcal{A}$ in the experiment is defined to be its winning probability.

Note that compared with the security models considered in [23, 25, 24], we additionally add an auxiliary oracle named *CreateUser Oracle* $CO(\cdot)$. W.l.o.g., we suppose that each ID used in other oracle queries has already been created by $CO(ID)$. Let Forge be the event that (a) $\mathsf{Ver}(\hat{ID}, \hat{m}, \hat{\sigma}) = 1$, (b) $\hat{ID} \notin Q_e$ and (c) $(\hat{ID}, \hat{m}) \notin Q_s$. Then, we have following definition.

Definition 5 (EUF-CMIA Security)

An IBS scheme Σ is *existentially unforgeable under adaptive chosen-message and chosen-ID attack* (EUF-CMIA secure) if no PPT $\mathcal{A}$ has a non-negligible advantage in the experiment $\mathsf{CMA\text{-}IDA}_{\mathcal{A},\Sigma}(1^k)$, i.e.

$$\Pr\left[\mathsf{Forge} : (\hat{ID}, \hat{m}, \hat{\sigma}) \leftarrow \mathcal{A}^{CO(\cdot), \mathcal{E}O(\cdot), \mathcal{S}O(\cdot)}(mpk)\right] \le \mathrm{negl}(k),$$

where negl $(\cdot)$ is a negligible function in k.

Leakage-Resilient Unforgeability. Similar to Def. 3, we additionally allow the adversary $\mathcal{A}$ to access to a leakage oracle $\mathcal{L}O(\cdot)$ to obtain a bounded leakage of the mater secret key and the signing keys used in the signing query phase in an IBS scheme. Let Forge be the event that (a) $\mathsf{Ver}(\hat{ID}, \hat{m}, \hat{\sigma}) = 1$, (b) $\hat{ID} \notin Q_e$, (c) $(\hat{ID}, \hat{m}) \notin Q_s$ and (d) $\sum_{i=1}^{q} \lambda_i \le \lambda$. Then, we have following definition.

Definition 6 (Leakage-Resilient Identity-Based Signature, LR-IBS)

An IBS scheme Σ is λ-leakage-resilient and existentially unforgeable under adaptive chosen-message and chosen-ID attack (λ-LR-EUF-CMIA secure) if no PPT $\mathcal{A}$ has a non-negligible advantage in the modified experiment, i.e.

$$\Pr\left[\mathsf{Forge} : (\hat{ID}, \hat{m}, \hat{\sigma}) \leftarrow \mathcal{A}^{CO(\cdot), \mathcal{E}O(\cdot), \mathcal{S}O(\cdot), \mathcal{L}O(\cdot)}(mpk)\right] \le \mathrm{negl}(k),$$

where negl $(\cdot)$ is a negligible function in k.

2.3. Certificateless Signature

In this part we give a brief introduction to certificateless signature. We follow the definition and security model of certificateless signature scheme given in [47].

Definition 7 (CLS)

A certificateless signature scheme $\Sigma = (\mathsf{MKg}, \mathsf{PKg}, \mathsf{UKg}, \mathsf{CL\text{-}Sig}, \mathsf{CL\text{-}Ver})$ is specified by a tuple of five PPT algorithms, called master key generation algorithm, user partial key generation algorithm, user key generation algorithm, signing algorithm and verification algorithm, respectively.

- **Master Key Generation.** On input 1^k, the algorithm generates a master public/secret key pair (mpk, msk), i.e. $(mpk, msk) \leftarrow \mathsf{MKg}(1^k)$.
- **User Partial Key Generation.** On input msk and a user identity ID, the algorithm generates a user partial key, i.e. $psk \leftarrow \mathsf{PKg}(msk, ID)$.
- **User Key Generation.** On input mpk and identify ID, the algorithm generates a user signing/verification key pair (upk, usk), i.e. $(upk, usk) \leftarrow \mathsf{UKg}(mpk, ID)$.
- **Signing Algorithm.** On input a tuple (psk, usk, m), the algorithm generates the corresponding signature, i.e. $\sigma \leftarrow \mathsf{CL\text{-}Sig}(psk, usk, m)$.
- **Verification Algorithm.** On input mpk, user identity ID, user public key uvk, message m and signature σ, the algorithm returns 1 for acceptance or 0 for rejection, i.e. $0/1 \leftarrow \mathsf{CL\text{-}Ver}(mpk, ID, upk, m, \sigma)$.

Security Model. There are two types of adversaries in CLS, $\mathcal{A}_{\mathrm{I}}$ and $\mathcal{A}_{\mathrm{II}}$. Adversary $\mathcal{A}_{\mathrm{I}}$ models a malicious user, which may compromise the target user's usk or replace uvk but does not get access to the user's partial key psk nor msk of KGC. Adversary $\mathcal{A}_{\mathrm{II}}$ models a *malicious-but-passive* KGC, which knows msk and is able to derive partial keys of any user.

There are five oracles according to the security model in [47]. Denote the system state by $\mathcal{S} = \{\mathcal{S}_0, \mathcal{S}_1\}$. Let $Q_{rpk}, Q_{rsk}, Q_{rk}, Q_s$ be initially empty query lists. The oracles work as below.

$\mathsf{CreateUser}$. On input ID, if ID has already been created, nothing is to be taken. Otherwise, generate $psk \leftarrow \mathsf{PKg}(msk, ID)$ and $(upk, usk) \leftarrow \mathsf{UKg}(mpk, ID)$. Update system state $\mathcal{S}_1 = \mathcal{S}_1 \cup \{(ID, psk, upk, usk)\}$. In both case, uvk is returned.

$\mathsf{RevealPartialKey}$. Given an identity ID, check the list $\mathcal{S}_1$ and return the corresponding psk. Set $Q_{rpk} = Q_{rpk} \cup \{ID\}$.

$\mathsf{RevealSecretKey}$. Given an identity ID, check the list $\mathcal{S}_1$ and return the corresponding usk. Set $Q_{rsk} = Q_{rsk} \cup \{ID\}$.

$\mathsf{ReplaceKey}$. Given an identity ID and a user signing/verification key pair (upk, usk), update the original user key pair of ID in $\mathcal{S}_1$ with (upk, usk). Set $Q_{rk} = Q_{rk} \cup \{ID\}$.

Signing. Given (ID, m), retrieve (psk, upk, usk) where $(ID, psk, upk, usk) \in \mathcal{S}_1$. Return the signature by running $\sigma \leftarrow \text{CL-Sig}(psk, usk, m)$. Set $Q_s = Q_s \cup \{(ID, m)\}$.

Let $\Sigma = (\mathsf{MKg}, \mathsf{PKg}, \mathsf{UKg}, \text{CL-Sig}, \text{CL-Ver})$ be a CLS scheme and denote the set of oracles described above by O. Consider the following experiments.

Type-I Security Experiment $\mathsf{UA}_{\mathcal{A}_\mathrm{I},\Sigma}(1^k)$:

1. Challenger C initializes the system as follows.
   (a) Run $(mpk, msk) \leftarrow \mathsf{MKg}(1^k)$ and give mpk to $\mathcal{A}_\mathrm{I}$ along with oracles O.
   (b) Set $\mathcal{S}_0 = \{(KGC, msk)\}$ and $\mathcal{S}_1 = \phi$.
2. $\mathcal{A}_\mathrm{I}$ makes queries to oracles O adaptively for polynomially many times.
3. Finally, $\mathcal{A}_\mathrm{I}$ outputs $(\hat{ID}, \hat{m}, \hat{\sigma})$. $\mathcal{A}_\mathrm{I}$ wins if and only if (a) $\text{CL-Ver}(mpk, \hat{ID}, upk_{\hat{ID}}, \hat{m}, \hat{\sigma}) = 1$, (b) $\hat{ID} \notin Q_{rpk}$ and (c) $(\hat{ID}, \hat{m}) \notin Q_s$. The advantage of $\mathcal{A}_\mathrm{I}$ in the experiment is defined to be its winning probability.

Type-II Security Experiment $\mathsf{KGCA}_{\mathcal{A}_\mathrm{II},\Sigma}(1^k)$:

1. Challenger C initializes the system as follows.
   (a) C invokes the adversary $\mathcal{A}_\mathrm{II}$ on input 1^k, which then submits a master key pair (mpk, msk).
   (b) Set $\mathcal{S}_0 = \{(KGC, msk)\}$ and $\mathcal{S}_1 = \phi$.
2. $\mathcal{A}_\mathrm{II}$ makes queries to oracles O (except the RevealPartialKey oracle) adaptively for polynomially many times.
3. Finally, $\mathcal{A}_\mathrm{II}$ outputs a tuple $(\hat{ID}, \hat{m}, \hat{\sigma})$. $\mathcal{A}_\mathrm{II}$ wins if and only if (a) $\text{CL-Ver}(mpk, \hat{ID}, upk_{\hat{ID}}, \hat{m}, \hat{\sigma}) = 1$, (b) $\hat{ID} \notin Q_{rsk}$, and (c) $\hat{ID} \notin Q_{rk}$ and $(\hat{ID}, \hat{m}) \notin Q_s$. The advantage of $\mathcal{A}_\mathrm{II}$ in the experiment is defined to be its winning probability.

Definition 8 (Secure Certificateless Signature)
A certificateless signature scheme Σ is existentially unforgeability under adaptive chosen-message and chosen-ID attack (CL-EUF-CMIA secure) if no PPT $\mathcal{A}_\mathrm{I}$ nor $\mathcal{A}_\mathrm{II}$ has a non-negligible advantage in experiment $\mathsf{UA}_{\mathcal{A}_\mathrm{I},\Sigma}$ and $\mathsf{KGCA}_{\mathcal{A}_\mathrm{II},\Sigma}$, respectively.

Leakage-Resilient Unforgeability. Similar to Def. 3, we modify the experiments by additionally providing $\mathcal{A}_\mathrm{I}$, $\mathcal{A}_\mathrm{II}$ a leakage oracle $\mathcal{LO}(\cdot)$ which outputs at most λ bits of the system's secret state. That is, given an adversarially chosen leakage function $f(\cdot)$, $\mathcal{LO}(f)$ returns $\Lambda := f(\mathcal{S})$. We have the following definition.

Definition 9 (Leakage-Resilient Certificateless Signature, LR-CLS)

A certificateless signature scheme Σ is λ-leakage-resilient and existentially unforgeable under adaptive chosen-message and chosen-ID attack (λ-LR-CL-EUF-CMIA secure) if there is no probabilistic polynomial-time adversary $\mathcal{A}_{\mathrm{I}}$ nor $\mathcal{A}_{\mathrm{II}}$ has a non-negligible advantage in the modified experiments.

2.4. Hierarchical Identity-based Encryption

An identity hierarchy $\overrightarrow{id}^{(k)}$ of depth k is a tuple of k strings $\overrightarrow{id}^{(k)} = (id_1, \cdots, id_k)$, where $id_i \in \{0,1\}^*$ for all $i \in [k]$. We say that $\overrightarrow{id}^{(k)}$ is a descendant of $\overrightarrow{id}^{(k-1)}$ if $\overrightarrow{id}^{(k-1)}$ is a prefix of $\overrightarrow{id}^{(k)}$. Specifically, $\overrightarrow{id}^{(0)}$ is defined as the empty string ϵ, which is an ancestor of any identity hierarchy. The formal definition of *hierarchical identity-based encryption* (HIBE) scheme is described as below.

Definition 10 (Hierarchical IBE, HIBE)

A hierarchical identity-based signature (HIBE) scheme $\mathcal{HIBE} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Enc}, \mathsf{Dec})$ is specified by a tuple of four PPT algorithms, called setup algorithm, key derivation algorithm, encryption algorithm and decryption algorithm, respectively.

- **Setup Algorithm.** On input 1^k, the KGC runs Setup to generate a master public/secret key pair (mpk, msk), i.e. $(mpk, msk) \leftarrow \mathsf{Setup}(1^k)$.

- **Extraction Algorithm.** On input the secret key $sk_{\overrightarrow{id}^{(k)}}$ of a k-level identity $\overrightarrow{id}^{(k)}$ and a descendant identity id_{k+1}, the algorithm generates the corresponding private key $sk_{\overrightarrow{id}^{(k+1)}}$, i.e. $sk_{\overrightarrow{id}^{(k+1)}} \leftarrow \mathsf{KeyDer}(sk_{\overrightarrow{id}^{(k)}}, \overrightarrow{id}^{(k)}, id_{k+1})$. Here we assume $\overrightarrow{id}^{(0)} = \epsilon$ (which is an empty string) and $sk_\epsilon = msk$.

- **Encryption Algorithm.** On input the master public key mpk, an identity hierarchy $\overrightarrow{id}$ and a message m, the algorithm returns a ciphertext $c \leftarrow \mathsf{Enc}(mpk, \overrightarrow{id}, m)$.

- **Decryption Algorithm.** On input a ciphertext c and the secret key $sk_{\overrightarrow{id}}$, the algorithm Dec returns a message $m \leftarrow \mathsf{Dec}(sk_{\overrightarrow{id}}, c)$ or $\perp$ if the decryption fails.

Security Models. The standard security notion of HIBE schemes is indistinguishability under chosen-identity and chosen-plaintext attack (IND-ID-CPA). However, a weaker security notion of HIBE called one-wayness under chosen-identity and chosen-plaintext attack (OW-ID-CPA) [48] suffices for our purpose. Let us consider the following experiment for an ℓ-level HIBE.

HIBE One-wayness Experiment. $\mathsf{ID\text{-}OWE}_{\mathcal{A},\Sigma}(1^k)$:

1. The challenger C runs $(mpk, msk) \leftarrow \mathsf{Setup}(1^k)$ and gives $sk_{\overrightarrow{id}^{(0)}} := msk$ to $\mathcal{A}$. Let $\mathcal{S} := \{(KGC, msk)\}$.
2. $\mathcal{A}$ adaptively accesses to oracle $\mathcal{KO}(\cdot)$. Namely, it submits an identity hierarchy $\overrightarrow{id}^{(i)} = (id_1, \cdots, id_i)$ $(0 \leq i < \ell)$ and an identity id_{i+1}, and is returned $sk_{\overrightarrow{id}^{(i+1)}} \leftarrow \mathsf{KeyDer}(sk_{\overrightarrow{id}^{(i)}}, \overrightarrow{id}^{(i)}, id_{i+1})$.
3. $\mathcal{A}$ submits a challenge identity hierarchy $\overrightarrow{id}^{(*)}$, with the restriction that any query $(\overrightarrow{id}^{(i)}, id_{i+1})$ issued to $\mathcal{KO}(\cdot)$ should not be a prefix of $\overrightarrow{id}^{(*)}$. The challenger C randomly selects a message $m \leftarrow \mathcal{M}$, computes $c \leftarrow \mathsf{Enc}(mpk, \overrightarrow{id}^{(*)}, m)$ and returns c to the adversary. For any $\overrightarrow{id'}$ that is a prefix of $\overrightarrow{id}^{*}$, set $\mathcal{S} = \mathcal{S} \cup \{(\overrightarrow{id'}, sk_{\overrightarrow{id'}})\}$.
4. The adversary continues to issuing queries to $\mathcal{KO}(\cdot)$ adaptively, except that it may not ask for the key of any identity hierarchy which is a prefix of $\overrightarrow{id}^{(*)}$.
5. Finally, $\mathcal{A}$ outputs $m' \in \mathcal{M}$ and wins if and only if $m = m'$. The advantage of $\mathcal{A}$ in the experiment is defined to be its winning probability.

Definition 11 (One-Way under Chosen-Identity Attack, OW-CIA)
An HIBE scheme is one-way under adaptive chosen-identity attack (OW-CIA) if there is no PPT adversary $\mathcal{A}$ which has a non-negligible advantage in the experiment $\mathsf{ID\text{-}OWE}_{\mathcal{A},\Sigma}(1^k)$.

Similar to Def. 3, we also modify the experiment by additionally providing $\mathcal{A}$ a leakage oracle $\mathcal{LO}(\cdot)$, and have the following definition.

Definition 12 (Leakage-Resilient and One-Way under Chosen-Identity Attack, LR-OW-CIA)
An HIBE scheme is λ-leakage-resilient and one-way under chosen-identity attack (LR-OW-CIA) if there is no probabilistic polynomial-time $\mathcal{A}$ which has a non-negligible advantage in the modified experiment.

3. Leakage-Resilient Identity-Based Signature

3.1. From Leakage-Resilient Signature

It is known that given a standard signature scheme, one can construct an IBS scheme [44, 45]. Let $\mathcal{LRS} = (\mathsf{Kg}, \mathsf{Sig}, \mathsf{Ver})$ be a standard signature scheme. An IBS scheme $\mathcal{LR}\text{-}\mathcal{IBS} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{IB\text{-}Sig}, \mathsf{IB\text{-}Ver})$ can be constructed as follows.

Construction 1
Setup: The KGC runs Kg to obtain a master signing/verification key pair, i.e. $(mpk, msk) \leftarrow \mathsf{Kg}(1^k)$.

Extract: Given an identity ID, the KGC computes the corresponding private key as follows.

1. Run the Kg algorithm to obtain a key pair, i.e. $(upk, usk) \leftarrow \mathsf{Kg}(1^k)$.
2. Sign $upk\|ID$ with its master key msk, i.e. $\delta \leftarrow \mathsf{Sig}(msk, upk\|ID)$.

3. Return (usk, upk, δ) to the user (via secure channel).

4. Set its secret key to be $sk_{ID} := usk$, and set an auxiliary key $Q_{ID} = (upk, \delta)$ which could be public.

$\mathsf{IB\text{-}Sig}$: A user with secret key sk_{ID} signs a message $m \in \{0,1\}^*$ as follows:

1. Sign m with its secret key sk_{ID}, i.e. $\sigma \leftarrow \mathsf{Sig}(sk_{ID}, m)$.

2. Return the signature $\sigma' := (\sigma, Q_{ID})$.

$\mathsf{IB\text{-}Ver}$: Given a tuple (ID, m, σ'), parse the signature σ' as (σ, upk, δ), output 1 for acceptance if and only if both $\mathsf{Ver}(mpk, upk||ID, \delta) = 1$ and $\mathsf{Ver}(upk, m, \sigma) = 1$ hold. Otherwise, output 0 for rejection.

Below we are going to show that the construction above also works in the leakage setting. That is, if the underlying signature scheme is leakage-resilient, so is the resulting IBS scheme. We have the following theorem.

Theorem 1

If $\mathcal{LRS}$ is a λ-LR-EUF-CMA secure signature scheme, then $\mathcal{LR}\text{-}\mathcal{IBS}$ is a λ-LR-EUF-CMIA secure identity-based signature scheme.

(*Proof Intuition.*) If there exists a probabilistic polynomial-time forger $\mathcal{F}$ outputs a valid forgery $(\hat{ID}, \hat{m}, (\hat{\sigma}, \hat{vk}, \hat{\delta}))$ of $\mathcal{LR}\text{-}\mathcal{IBS}$, we consider the following cases. Note that the $\hat{ID}$ is not allowed to be queried in the extract query phase.

Type 1. $\overline{\mathsf{Query}}$: $\hat{ID}$ is never quired in the signing query phase. Then $(\hat{vk}||\hat{ID}, \hat{\delta})$ is exactly a forgery with respect to the signing key of the KGC.

Type 2. Query : $\hat{ID}$ has been quired in the signing query. This implies that $\hat{m}$ is never quired along with $\hat{ID}$ in the signing query phase, and therefore $(\hat{m}, \hat{\sigma})$ is a forgery with respect to the user's signing key.

Let Forge denote by the event that $\mathcal{F}$ succeeds in forging a valid signature. Then, we have

$$\Pr[\mathsf{Forge}] = \Pr[\mathsf{Forge} \wedge \overline{\mathsf{Query}}] + \Pr[\mathsf{Forge} \wedge \mathsf{Query}].$$

Below we show that each of the terms on the right-hand side is negligible, thus proving the theorem.

Lemma 1

$\Pr[\mathsf{Forge} \wedge \overline{\mathsf{Query}}]$ is negligible if $\mathcal{LRS}$ is λ-LR-EUF-CMA secure.

Proof. Let $\mathcal{F}$ be a PPT adversary against our IBS scheme. Suppose that the output of $\mathcal{F}$ is a Type 1 forgery, i.e. $\overline{\mathsf{Query}}$ happens. We use it to build another PPT algorithm $\mathcal{A}_1$ to break the leakage-resilient unforgeability of the underlying signature scheme. Consider the following experiment.

1. $\mathcal{A}_1$ receives mpk from its challenger and is given access to oracles $\mathcal{SO}(\cdot)$ and $\mathcal{LO}(\cdot)$.

2. $\mathcal{A}_1$ sets two initially empty list Q_e, Q_s and the system state $\mathcal{S} = \{\mathcal{S}_0, \mathcal{S}_1\} = \{\{KGC, msk\}, \phi\}$. It invokes $\mathcal{F}$ on input mpk and answers queries from $\mathcal{F}$ as follows.

   CreateUser Query. On input identity ID, if ID has already been created, nothing is to be taken. Otherwise, execute the following operations.

   (a) Run $(upk, usk) \leftarrow \mathsf{Kg}(1^k)$.

   (b) Obtain the signature $\delta \leftarrow \mathcal{SO}(upk\|ID)$.

   (c) Update $\mathcal{S}_1 = \mathcal{S}_1 \cup \{(ID, upk, usk, \delta)\}$.

   Extract Query. Given an identity ID, check the list $\mathcal{S}_1$ and return the corresponding (upk, usk, δ). Set $Q_e = Q_e \cup \{ID\}$.

   Signing Query. Given (ID, m), $\mathcal{A}_1$ does as follows:

   (a) Retrieve the tuple (upk, usk, δ) where $(ID, upk, usk, \delta) \in \mathcal{S}_1$.

   (b) Return (σ, upk, δ) to $\mathcal{F}$ where $\sigma \leftarrow \mathsf{Sig}(usk, m)$.

   (c) Set the signing query list $Q_s = Q_s \cup \{(ID, m)\}$.

   Leakage Query. Given a leakage function $f(\mathcal{S})$, construct an equivalent leakage function $f'(\mathcal{S}_0)$ where we hard-code the $\mathcal{S}_1$ part into f'. Return $\Lambda := \mathcal{LO}(f')$.

3. $\mathcal{F}$ outputs $(\hat{ID}, \hat{m}, (\hat{\sigma}, \hat{upk}, \hat{\delta}))$ s.t. $\hat{ID} \notin Q_e$ and $(\hat{ID}, \hat{m}) \notin Q_s$. $\mathcal{A}_1$ outputs $(\hat{upk}\|\hat{ID}, \hat{\delta})$ and wins if and only if $\mathsf{Ver}(mpk, \hat{upk}\|\hat{ID}, \hat{\delta}) = 1$ and $(\hat{ID}, *) \notin Q_s$.

The probability that $\mathcal{A}_1$ wins is

$$\begin{aligned}
\Pr[\mathcal{A}_1 \text{ wins}] &= \Pr[\mathsf{Ver}(mpk, \hat{upk}\|\hat{ID}, \hat{\delta}) = 1 \wedge (\hat{ID}, *) \notin Q_s] \\
&\geq \Pr[\mathsf{Ver}(mpk, \hat{upk}\|\hat{ID}, \hat{\delta}) = 1 \wedge \mathsf{Ver}(\hat{upk}, \hat{m}, \hat{\sigma}) = 1 \wedge \hat{ID} \notin Q_e \wedge (\hat{ID}, \hat{m}) \notin Q_s] \\
&= \Pr[\mathsf{Forge} \wedge \overline{\mathsf{Query}}]
\end{aligned}$$

Since $\mathcal{LRS}$ is λ-LR-EUF-CMA secure, we have $\Pr[\mathcal{A}_1 \text{ wins}] \leq \text{negl}_1(k)$, where $\text{negl}_1(k)$ is a negligible function in k. Then we have $\Pr[\mathsf{Forge} \wedge \overline{\mathsf{Query}}] \leq \text{negl}_1(k)$.

Next, we prove the term $\Pr[\mathsf{Forge} \wedge \mathsf{Query}]$ is negligible in k as well.

Lemma 2

$\Pr[\mathsf{Forge} \wedge \overline{\mathsf{Query}}]$ is negligible if LRS is λ-LR-EUF-CMA secure.

Proof. Let q_s denote by the number of identities only queried in signing query phase and not in extract query phase.

Let q_e denote by the number of identities ever queried in extract query phase. Consider a PPT adversary $\mathcal{A}_2$ who breaks the security of $\mathcal{LRS}$ in the following experiment.

C runs $(vk^*, sk^*) \leftarrow \mathsf{Kg}(1^k)$ and gives vk^* to $\mathcal{A}_2$. $\mathcal{A}_2$ does as follows.

1. Run Setup to obtain a key pair $(mpk, msk) \leftarrow \mathsf{Setup}(1^k)$.
2. Set two initially empty list Q_e, Q_s and the system state $\mathcal{S} = \{\mathcal{S}_0, \mathcal{S}_1\} = \{\{KGC, msk\}, \phi\}$.
3. Select a random value $i^* \overset{\$}{\leftarrow} [q_s + q_e]$.
4. Invoke $\mathcal{F}(mpk)$ and answer following queries.

   CreateUser Query. Given the ith new identity ID_i, initialize as follows.

   (a) For any $i \neq i^*, compute(upk_i, usk_i) \leftarrow \mathsf{Kg}(1^k)$. Otherwise set $(upk_{i^*}, usk_{i^*}) := (vk^*, \perp)$.

   (b) Sign upk_i with msk, i.e. $\delta_i \leftarrow \mathsf{Sig}(msk, upk_i \| ID_i)$.

   (c) Update $\mathcal{S}_1 = \mathcal{S}_1 \cup \{(ID_i, usk_i, upk_i, \delta_i)\}$.

   Extract Query. Given an identity ID, check the list $\mathcal{S}_1$ and return the corresponding (usk, upk, δ). If $usk =\perp$, abort. Set $Q_e = Q_e \cup \{ID\}$.

   Signing Query. Given an identity ID and a message m, $\mathcal{A}_2$ does as follows:

   (a) Retrieve the tuple (usk, upk, δ) form $\mathcal{S}_1$. If $usk =\perp$, ask the signing oracle $\mathcal{SO}(\cdot)$ for a signature σ on m; otherwise, compute $\sigma \leftarrow \mathsf{Sig}(usk, m)$. Return (σ, upk, δ) to $\mathcal{F}$.

   (b) Update the signing query list $Q_s = Q_s \cup \{(ID, m)\}$.

   Leakage Query. Given a leakage function $f(\mathcal{S})$, construct an equivalent leakage function $f'_{\mathcal{S}/sk^*}(sk^*) := f(\mathcal{S})$ and return $\Lambda = \mathcal{LO}(f')$.
5. Finally, $\mathcal{F}$ outputs $(\hat{ID}, \hat{m}, (\hat{\sigma}, \hat{upk}, \hat{\delta}))$ s.t. $\hat{ID} \notin Q_e$ and $(\hat{ID}, \hat{m}) \notin Q_s$. $\mathcal{A}_2$ outputs $(\hat{m}, \hat{\sigma})$ and wins if and only if $\hat{ID} = ID_{i^*}$, $\mathsf{Ver}(vk^*, \hat{m}, \hat{\sigma}) = 1$.

Let $\overline{\mathsf{Abort}}$ be the event that the experiment does not abort in extract query phase. Then we have $\Pr[\overline{\mathsf{Abort}}] = 1 - q_e/(q_e + q_s) = q_s/(q_e + q_s)$. Then, the probability that $\mathcal{A}_2$ wins is

$$\begin{aligned}
\Pr[\mathcal{A}_2 \text{ wins}] &= \Pr[\mathsf{Ver}(vk^*, \hat{m}, \hat{\sigma}) = 1 \wedge \hat{ID} = ID_{i^*} \wedge (\hat{ID}, \hat{m}) \notin Q_s \wedge \overline{\mathsf{Abort}}] \\
&\geq \Pr[\mathsf{Forge} \wedge \mathsf{Query} \wedge \hat{ID} = ID_{i^*}] \cdot \Pr[\overline{\mathsf{Abort}}] \\
&= \Pr[\mathsf{Forge} \wedge \mathsf{Query}] \cdot \Pr[\hat{ID} = ID_{i^*}] \cdot \frac{q_s}{q_e + q_s} \\
&= \Pr[\mathsf{Forge} \wedge \mathsf{Query}] \cdot \frac{1}{q_s} \cdot \frac{q_s}{q_e + q_s} \\
&= \frac{1}{q_s + q_e} \cdot \Pr[\mathsf{Forge} \wedge \mathsf{Query}]
\end{aligned}$$

Since $\mathcal{LRS}$ is λ-LR-EUF-CMA secure, we have that $\Pr[\mathcal{A}_2 \text{ wins}] \leq \text{negl}_2(k)$, where $\text{negl}_2(k)$ is a negligible function in k. Thus we have $\Pr[\mathsf{Forge} \wedge \mathsf{Query}] \leq (q_s + q_e)\text{negl}_2(k)$, where both q_s, q_e are polynomial in k. □

Combing the two lemmas above together, we obtain that

$$\Pr[\mathsf{Forge}] = \Pr[\mathsf{Forge} \wedge \overline{\mathsf{Query}}] + \Pr[\mathsf{Forge} \wedge \mathsf{Query}] \leq \text{negl}_1(k) + (q_s + q_e) \cdot \text{negl}_2(k),$$

which is negligible in k. This competes the proof of Theorem 1.

3.2. From Leakage-Resilient 2-level HIBE

Sect. 3.1 describes a method of constructing identity-based signature schemes from standard ones in the bounded leakage setting. Although Construction 1 satisfies the definition of IBS, it is essentially a certificate-based transformation and not a pure identity-based one. It does not have the full advantage of identity-based cryptography. In this part, therefore, we study another generic construction of IBS, which is based on a 2-level hierarchical IBE scheme. Let $\mathcal{HIBE} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Enc}, \mathsf{Dec})$ be a 2-level HIBE scheme. IBS scheme $\mathcal{LR}\text{-}\mathcal{IBS} = (\mathsf{IB\text{-}Setup}, \mathsf{Extract}, \mathsf{IB\text{-}Sig}, \mathsf{IB\text{-}Ver})$ can be constructed as follows.

Construction 2

Setup: KGC runs $(mpk, msk) \leftarrow \mathsf{Setup}(1^k)$ to generate the system parameters.

$\mathsf{Extract}$: For a user with identity ID, KGC calculates the corresponding user secret key by running $sk_{ID} \leftarrow \mathsf{KeyDer}(msk, ID)$.

$\mathsf{IB\text{-}Sig}$: A user with secret key sk_{ID} signs a message $m \in \{0,1\}^*$ as follows:

1. Construct an ID-tuple $\overrightarrow{id} = (ID, m)$.
2. Obtain the decryption key of $\overrightarrow{id}$ by running $S_{\overrightarrow{id}} \leftarrow \mathsf{KeyDer}(sk_{ID}, \overrightarrow{id})$.
3. Return the signature $\sigma := S_{\overrightarrow{id}}$.

$\mathsf{IB\text{-}Ver}$: Given the signature σ of message m for identity ID,

1. Construct an ID-tuple $\overrightarrow{id} = (ID, m)$.
2. Encrypt a randomly chosen message $m' \leftarrow \mathcal{M}$, i.e. $c \leftarrow \mathsf{Enc}(mpk, \overrightarrow{id}, m')$.
3. Output 1 (accept) if and only if $\mathsf{Dec}(\sigma, c) = m'$ holds. Otherwise, output 0 (reject).

Theorem 2

If $\mathcal{HIBE}$ is λ-LR-OW-CIA secure, then $\mathcal{LR}\text{-}\mathcal{IBS}$ is λ-LR-EUF-CMA secure.

Proof. Suppose that $\mathcal{F}$ is a probabilistic polynomial-time forger which breaks the security of our leakage-resilient IBS scheme $\mathcal{LR}\text{-}\mathcal{IBS}$. We use it to construct another probabilistic polynomial-time algorithm $\mathcal{A}$ which breaks the leakage-resilience security of the underlying $\mathcal{HIBE}$ scheme. Consider the following experiment.

1. $\mathcal{A}$ is given the system parameters and the master public key mpk of the $\mathcal{HIBE}$ scheme, as well as oracle access to a key derivation oracle $\mathcal{KO}(\cdot)$ and a leakage oracle $\mathcal{LO}(\cdot)$.

2. $\mathcal{A}$ sets the system state $\mathcal{S} = \{KGC, \text{msk}\}$ and invokes $\mathcal{F}(\text{mpk})$. It then answers the queries from $\mathcal{F}$ as follows.

   CreateUser Query. On input an identity ID, if ID has already been created, nothing is to be taken. Otherwise, obtain $sk_{ID} \leftarrow \mathcal{KO}(ID)$ from its own key derivation oracle and update $\mathcal{S} = \mathcal{S} \cup \{(ID, sk_{ID})\}$.

   Extraction Query. Given identity ID, search the list $\mathcal{S}$ and return the corresponding sk_{ID}. Set $Q_e = Q_e \cup \{ID\}$.

   Signing Query. Given a tuple (ID, m), search the corresponding sk_{ID} in $\mathcal{S}$ and return $\sigma \leftarrow \mathsf{KeyDer}(sk_{ID}, (ID, m))$. Set $Q_s = Q_s \cup \{(ID, m)\}$.

   Leakage Query. Given a leakage function $f(\mathcal{S})$, construct an equivalent leakage function $f'_{S/msk}(msk)$. $\mathcal{A}$ returns $\Lambda := \mathcal{LO}(f')$.

3. When $\mathcal{F}$ outputs $(\hat{ID}, \hat{m}, \hat{\sigma})$, then $\mathcal{A}$ outputs $\overrightarrow{id}^* = (\hat{ID}, \hat{m})$ to C and receives a ciphertext c of a randomly chosen message m.

4. Finally, $\mathcal{A}$ outputs $m' = \mathsf{Dec}(\hat{\sigma}, c)$. $\mathcal{A}$ wins if and only if $m' = m$.

The rest of the proof is straightforward. If $\mathcal{F}$ outputs a valid signature $(\hat{ID}, \hat{m}, \hat{\sigma})$, then $\hat{\sigma}$ is exactly the decryption key of $\overrightarrow{id} = (\hat{ID}, \hat{m})$ and therefore $\mathcal{A}$ is able to correctly decrypt the ciphertext $\hat{c}$. Notice that, $\hat{ID}$, which is a prefix of $\overrightarrow{id}^* = (\hat{ID}, \hat{m})$, was never queried in the extraction query step. This ensures that $\hat{ID}$ was never queried in the key derivation query step before being submitted by $\mathcal{F}$ as the challenging identity tuple $\overrightarrow{id}^*$. Since $\mathcal{HIBE}$ is λ leakage-resilient, then $\mathcal{A}$ is able to correctly answer the leakage queries from $\mathcal{F}$.

Therefore, if $\mathcal{F}$ succeeds in forging a valid signature, our algorithm $\mathcal{A}$ breaks the LR-OW-CIA security of $\mathcal{HIBE}$.

□

4. Leakage-Resilient Certificateless Signature

In this section we are going to show a construction of leakage-resilient certificateless signature scheme. More precisely, let $\mathcal{LR}$-$\mathcal{IBS} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{IB\text{-}Sig}, \mathsf{IB\text{-}Ver})$ be an ID-based signature scheme, and $\mathcal{LRS} = (\mathsf{Kg}, \mathsf{Sig}, \mathsf{Ver})$ be a signature scheme. Consider Hu et al.'s (non-leakage-resilient) CLS construction [47] $\mathcal{LR}$-$\mathcal{CLS} = (\mathsf{MKg}, \mathsf{PKg}, \mathsf{UKg}, \mathsf{CL\text{-}Sig}, \mathsf{CL\text{-}Ver})$, which is described as below.

Construction 3

MKg: Return the key pair $(mpk, msk) \leftarrow \mathsf{Setup}(1^k)$.

PKg: On input the master secret key msk and ID, return $psk \leftarrow \mathsf{PKg}(msk, ID)$.

UKg: Return $(upk, usk) \leftarrow \mathsf{Kg}(1^k)$.

$\mathsf{CL\text{-}Sig}$: On input (psk, usk, m), sign the message m as follows:

1. Run $\sigma_0 \leftarrow \mathsf{Sig}(usk, m \| mpk \| ID \| upk)$.
2. Run $\sigma_1 \leftarrow \mathsf{IB\text{-}Sig}(psk, m \| mpk \| ID \| upk \| \sigma_0)$.
3. Return the signature $\sigma := (\sigma_0, \sigma_1)$.

$\mathsf{CL\text{-}Ver}$: On input $(ID, m, (\sigma_0, \sigma_1))$, output 1 (accept) if and only if the following equations hold. Otherwise, output 0 (reject).

$$\mathsf{Ver}(upk, m \| mpk \| ID \| upk, \sigma_0) = 1, \text{ and}$$
$$\mathsf{IB\text{-}Ver}(mpk, m \| mpk \| ID \| upk \| \sigma_0, \sigma_1) = 1.$$

We prove that Hu et al.'s scheme is leakage-resilient if the underlying building blocks are leakage-resilient as well. We have the following theorem.

Theorem 3

If $\mathcal{LR}\text{-}\mathcal{IBS}$ is λ_1-LR-EUF-CMIA and $\mathcal{LRS}$ is λ_2-LR-EUF-CMA secure, then $\mathcal{LR}\text{-}\mathcal{CLS}$ is λ-LR-CL-EUF-CMIA secure, where $\lambda = \min\{\lambda_1, \lambda_2\}$.

Below we show that each of adversaries $\mathcal{A}_{\mathrm{I}}$ and $\mathcal{A}_{\mathrm{II}}$ has negligible advantage in Type-I experiment and Type-II experiment.

Proof. We first construct a probabilistic polynomial-time forger $\mathcal{F}$ which breaks the security of leakage-resilient IBS scheme $\mathcal{LR}\text{-}\mathcal{IBS}$ by running $\mathcal{A}_{\mathrm{I}}$. Consider the following experiment.

1. $\mathcal{F}$ obtains the master public key from its challenger, and is given access to oracles $\mathcal{CO}(\cdot), \mathcal{EO}(\cdot), \mathcal{SO}(\cdot), \mathcal{LO}(\cdot)$.

2. $\mathcal{F}$ prepares the system initial state $\mathcal{S} = \{\mathcal{S}_0, \mathcal{S}_1\}$ where $\mathcal{S}_0 = \{(KGC, msk)\}, \mathcal{S}_1 = \phi$ and four initially empty query lists $Q_{rpk}, Q_{rsk}, Q_{rk}, Q_s$. It then invokes $\mathcal{A}_I(mpk)$ and answers the adversary's queries as below.

   CreateUser. On input an identity ID, if ID has already been created, nothing is to be taken. Otherwise, send ID to $\mathcal{CO}(\cdot)$ and generate the user key pair $(upk, usk) \leftarrow \mathsf{Kg}(1^k)$. Update the system state $\mathcal{S}_1 = \mathcal{S}_1 \cup \{(ID, \perp, upk, usk)\}$. In both case, upk is returned.

   RevealPartialKey. Given an identity ID, check list $\mathcal{S}_1$ and retrieve the corresponding tuple (ID, psk, upk, usk) from $\mathcal{S}_1$. If $psk = \perp$, send ID to oracle $\mathcal{EO}(\cdot)$, obtain the corresponding partial private key psk and fill it in the tuple. Set $Q_{rpk} = Q_{rpk} \cup \{ID\}$ and return psk.

   RevealSecretKey. Given an identity ID, check list $\mathcal{S}_1$ and retrieve the corresponding tuple (ID, psk, upk, usk) from $\mathcal{S}_1$. Set $Q_{rsk} = Q_{rsk} \cup \{ID\}$, and return the corresponding usk.

   ReplaceKey. Given an identity ID and user public/secret key pair (upk, usk), replace the original public/secret key pair of ID with (upk, usk) in $\mathcal{S}_1$. Set $Q_{rk} = Q_{rk} \cup \{ID\}$.

   Signing. Given an identity ID and a message m, retrieve the user key pair (upk, usk) from $\mathcal{S}_1$. Set $m' = m||mpk||ID||upk$ and compute the signature $\sigma_0 \leftarrow \mathsf{Sig}(usk, m')$. Send (ID, m'') to $\mathcal{SO}(\cdot)$ and obtain σ_1 where $m'' = m'||\sigma_0$. Set $Q_s = Q_s \cup \{(ID, m)\}$ and return $\sigma = (\sigma_0, \sigma_1)$.

   Leakage. Given a leakage function $f(\mathcal{S}_0, \mathcal{S}_1)$, Let $\mathcal{S}_e \subset \mathcal{S}_1$ be the set whose tuples are queried in the RevealPartialKey phase. Construct an equivalent leakage function $f'(\mathcal{S}_0, \mathcal{S}_1/\mathcal{S}_e)$ where we hardcode the $\mathcal{S}_e$ part into the function f. Return $\Lambda \leftarrow \mathcal{LO}(f')$.

3. Finally, when $\mathcal{A}_{\mathrm{I}}$ outputs $\{\hat{ID}, \hat{m}, (\hat{\sigma}_0, \hat{\sigma}_1)\}$, $\mathcal{F}$ outputs $(\hat{ID}, \hat{m}'', \hat{\sigma}_1)$ where $\hat{m}'' = \hat{m}||mpk||\hat{ID}||upk_{\hat{ID}}||\hat{\sigma}_0$. $\mathcal{F}$ wins if and only if $\mathsf{IB\text{-}Ver}(mpk, \hat{ID}, upk_{\hat{ID}}, \hat{m}'', \hat{\sigma}_1) = 1$, and $\hat{ID} \notin Q_{rpk}$ and $\hat{ID} \notin Q_{rk}$.

The probability that $\mathcal{A}_{\mathrm{I}}$ wins is

$$\begin{aligned}\Pr[\mathcal{A}_I \text{ wins }] &= \Pr[\mathsf{CL\text{-}Ver}(mpk, \hat{ID}, upk_{\hat{ID}}, \hat{m}, (\hat{\sigma}_0, \hat{\sigma}_1)) = 1 \wedge \hat{ID} \notin Q_{rpk} \wedge (\hat{ID}, \hat{m}) \notin Q_s] \\ &\leq \Pr[\mathsf{IB\text{-}Ver}(mpk, \hat{ID}, upk_{\hat{ID}}, \hat{m}'', \hat{\sigma}_1) = 1 \wedge \hat{ID} \notin Q_{rpk} \wedge (\hat{ID}, \hat{m}) \notin Q_s] \\ &= \Pr[\mathcal{F} \text{ wins }]\end{aligned}$$

Since $\mathcal{LR}\text{-}\mathcal{IBS}$ is λ_1-LR-EUF-CMIA secure, we have

$$\Pr[\mathcal{F} \text{ wins }] \leq \mathrm{negl}_1(k),$$

where $\mathrm{negl}_1(k)$ is a negligible function in k. Then we have $\Pr[\mathcal{A}_I \text{ wins}] \leq \mathrm{negl}_1(k)$.

Next, we construct a probabilistic polynomial-time forger $\mathcal{F}'$ to break the security of leakage-resilient signature scheme $\mathcal{LRS}$ by running $\mathcal{A}_{\text{II}}$. Denote by q_s the number of identities queried in the signing phase. Consider the following experiment.

1. $\mathcal{F}'$ obtains vk^* from its challenger and is given access to oracles $\mathcal{SO}(\cdot), \mathcal{LO}(\cdot)$.

2. $\mathcal{F}'$ invokes the adversary $\mathcal{A}_{\text{II}}$, and receives from $\mathcal{A}_{\text{II}}$ a master key pair (mpk, msk). It then prepares the system state $\mathcal{S} = \{\mathcal{S}_0, \mathcal{S}_1\} := \{\{(KGC, msk)\}, \phi\}$ and four initially empty query lists Q_{rsk}, Q_{rk}, Q_s. It then selects a random value $i^* \overset{\$}{\leftarrow} [q_s]$, and answers the adversary's queries as below.

   CreateUser. On input an identity ID, if ID has already been created, nothing is to be taken. Otherwise, if ID is the i^*-th newly queried identity, set the corresponding user public/secret key pair to be $(upk, usk) = (vk^*, \perp)$; else, generate the user partial key $psk \leftarrow \mathsf{Extract}(msk, ID)$ and user key pair $(upk, usk) \leftarrow \mathsf{Kg}(1^k)$. Update the system state $\mathcal{S}_1 = \mathcal{S}_1 \cup \{(ID, psk, upk, usk)\}$. Return upk.

   RevealSecretKey. Given an identity ID, check the list $\mathcal{S}_1$ and retrieve the corresponding tuple (ID, psk, upk, usk). If $usk = \perp$, abort. Otherwise, set $Q_{rsk} = Q_{rsk} \cup \{ID\}$ and return usk.

   ReplaceKey. Given an identity ID and a user public/secret key pair (upk, usk), replace the original public/secret key pair of ID with (upk, usk) in $\mathcal{S}_1$. Set $Q_{rk} = Q_{rk} \cup \{ID\}$.

   Signing. Given an identity ID and a message m, $\mathcal{F}'$ does as follows:

   (a) Retrieve (ID, psk, usk, upk) from $\mathcal{S}_1$ and set $m' = m \| mpk \| ID \| upk$.

   (b) If $usk = \perp$ (which means $ID = ID_{i^*}$), send m' to oracle $\mathcal{SO}(\cdot)$ and obtain the corresponding signature σ_0; otherwise, compute $\sigma_0 \leftarrow \mathsf{Sig}(usk, m')$.

   (c) Set $m'' = m' \| \sigma_0$ and compute $\sigma_1 \leftarrow \mathsf{IB\text{-}Sig}(psk, m'')$.

   (d) Set $Q_s = Q_s \cup \{(ID, m)\}$ and return $\sigma = (\sigma_0, \sigma_1)$.

   Leakage. Given a leakage function $f(\mathcal{S}) := f(\mathcal{S}_0, \mathcal{S}_1)$, construct an equivalent leakage function $f'_{\mathcal{S}/usk_{ID_{i^*}}}(usk_{ID_{i^*}}) = f(\mathcal{S})$, where $usk_{ID_{i^*}}$ is implicitly defined to be the unknown secret key sk^*. Return $\Lambda \leftarrow \mathcal{LO}(f')$.

3. Finally, $\mathcal{A}_{\text{II}}$ outputs $\{\hat{ID}, \hat{m}, (\hat{\sigma}_0, \hat{\sigma}_1)\}$. If $\hat{ID} \neq ID_{i^*}$, $\mathcal{F}'$ aborts. Otherwise, suppose that $\mathcal{A}_{\text{II}}$ wins in the experiment, and thus $\hat{ID}$ has not been queried as a RevealSecretKey query nor a ReplaceKey query. $\mathcal{F}'$ outputs $(\hat{ID}, \hat{m}', \hat{\sigma}_0)$ where $\hat{m}' = \hat{m} \| mpk \| \hat{ID} \| upk_{\hat{ID}}$. $\mathcal{F}'$ wins if and only if $\mathsf{Ver}(upk_{\hat{ID}}, \hat{m}', \hat{\sigma}_1) = 1$, $upk_{\hat{ID}} = vk^*$ and $\mathcal{SO}(\hat{m}')$ was never queried before.

The probability that $\mathcal{F}'$ wins is

$$\begin{aligned}
\Pr[\mathcal{F}' \text{ wins}] &= \Pr[\mathsf{Ver}(upk_{\hat{ID}}, \hat{m}', \hat{\sigma}_0) = 1 \wedge upk_{\hat{ID}} = vk^* \wedge \mathcal{SO}(\hat{m}') \text{ was not queried}] \\
&= \Pr\left[\begin{array}{c} \mathsf{Ver}(upk_{\hat{ID}}, \hat{m}', \hat{\sigma}_0) = 1 \wedge \hat{ID} = ID_{i^*} \wedge \\ \hat{ID} \notin Q_{rsk} \wedge (\hat{ID}, *, *) \notin Q_{rk} \wedge (\hat{ID}, \hat{m}) \notin Q_s \end{array}\right] \\
&\geq \Pr\left[\begin{array}{c} \mathsf{CL\text{-}Ver}(mpk, \hat{ID}, upk_{\hat{ID}}, \hat{m}, (\hat{\sigma}_0, \hat{\sigma}_1)) = 1 \wedge \\ \hat{ID} \notin Q_{rsk} \wedge (\hat{ID}, *, *) \notin Q_{rk} \wedge (\hat{ID}, \hat{m}) \notin Q_s \end{array}\right] \cdot \Pr\left[\hat{ID} = ID_{i^*}\right] \\
&= \frac{1}{q_s} \cdot \Pr[\mathcal{A}_{II} \text{ wins}]
\end{aligned}$$

Since $\mathcal{LRS}$ is λ_2-LR-EUF-CMA secure, we have that

$$\Pr[\mathcal{F}' \text{ wins}] \leq \text{negl}_2(k),$$

where $\text{negl}_2(k)$ is a negligible function in k. Thus, $\Pr[\mathcal{A}_{II} \text{ wins}] \leq q_s \cdot \text{negl}_2(k)$, where q_s is polynomial in k.

Therefore, we have $\Pr[\mathcal{A}_I \text{ wins}] \leq \text{negl}_1(k)$ and $\Pr[\mathcal{A}_{II} \text{ wins}] \leq q_s \cdot \text{negl}_2(k)$, which implies that our $\mathcal{LR}$-$\mathcal{CLS}$ scheme is λ-LR-CL-EUF-CMIA secure. The leakage bound λ takes the minimum value of λ_1 and λ_2. The initiation is that we reduce the security of our construction to primitives with different amount of leakage resilience, then *buckets effect* happens. To be more concretely, a minimum leakage bound of $\mathcal{F}$ and $\mathcal{F}'$ ensure that they are both able to answer the leakage queries from $\mathcal{A}_{\mathsf{I}}$ and $\mathcal{A}_{\mathsf{II}}$, respectively. This competes the proof. □

5. Instantiations

In this section we discuss about how to instantiate our black-box construction of leakage-resilient IBS and CLS schemes. There are not many choices of leakage-resilient signature schemes in the literature, and the efficiency and leakage resilience of the resulting scheme depend highly on the underlying schemes. Below we show the instantiations of leakage-resilient IBS and CLS, respectively.

(*Leakage-Resilient IBS*). To get a leakage-resilient IBS scheme, we can apply the transform present in Sec. 3.1 to any of the leakage-resilient signature schemes in [15, 19]. For example, if we instantiate the underlying signature scheme with Boyle *et al.*'s scheme [15] whose leakage rate is $1 - o(1)$, the resulting IBS scheme enjoys $1/2 - o(1)$ leakage rate, where we consider leakage on the user signing keys and the master signing key of KGC.

We can also apply the transform present in Sec. 3.2 to Lewko *et al.*'s leakage-resilient HIBE scheme [49]. Note that Lewko *et al.*'s leakage-resilient HIBE scheme is (l_{MK}, l_{SK})-master-leakage secure where $l_{MK} = l_{SK} = (n - 1 - 2c) \log p_2$ and c is a constant value and p_2 is a prime number whose length is polynomial in n. The resulting IBS scheme is then $(n - 1 - 2c) \log p_2$-leakage-resilient.

(*Leakage-Resilient CLS*). To get a leakage-resilient CLS scheme, we can apply the transform present in Sec. 4 to the IBS scheme obtained above and any of the leakage-resilient signature schemes in [15, 19], and the resulting scheme could have leakage rate as high as $1/3 - o(1)$.

$$\begin{tikzcd}
\mathcal{LR}\text{-}\mathcal{HIBE} \arrow[d, "3"'] & \mathcal{LRS} \arrow[dl, "2"'] \arrow[d, "4"] \arrow[dr, "1"] & \mathcal{LR}\text{-}\mathcal{OTS} \arrow[d, "1"] \\
\mathcal{LR}\text{-}\mathcal{IBS} \arrow[r, "4"] & \mathcal{LR}\text{-}\mathcal{CLS} & \mathcal{LR}\text{-}\mathcal{SS}
\end{tikzcd}$$

Figure 1: Transforms among various signature notions

(*Full Leakage Resilience*). We note that if the underlying signature is *fully leakage-resilient* [15], which allows the leakage of the randomness used in the key generation and signature generation, the IBS scheme obtained via the transform in Sec. 3.1 would be fully leakage-resilient as well. The proof is similar with that of Theorem 1. It also applies to the construction of leakage-resilient CLS. The only drawback is that it depends on NIZK proof system, which results in low efficiency. To propose a signature scheme with high efficiency and leakage rate is one of our future works.

(*Strong Unforgeability*). Wang *et al.* [19] and Huang *et al.* [20] studied the construction of leakage-resilient and *strongly unforgeable* signature schemes, independently. Applying their techniques to the black-box constructions of IBS and CLS schemes shown in this paper, we can obtain leakage-resilient and strongly unforgeable IBS and CLS schemes. For example, when instantiating the underlying signature scheme with Wang *et al.*'s scheme [19], we can get a $(1/2 - o(1))|sk|$-leakage-resilient and strongly unforgeable IBS scheme.

6. Conclusion

The works on the generic construction of (standard, identity-based, certificateless) signature scheme are summarized in Fig. 1, where $\mathcal{LR}$-$\mathcal{OTS}$ is a leakage-resilient strong one-time signature scheme and $LRSS$ is a leakage-resilient strongly unforgeable signature scheme. Note that the transform labelled by 1 is completed by [19, 20]. In this paper we focus on the other transforms described in Fig. 1. We present a black-box transform (labelled by 4 in the figure) to certificateless signature scheme from a standard signature scheme and an IBS scheme and prove its security in the leakage setting. Furthermore, we present a black-box construction (labelled by 2 in the figure) of leakage-resilient IBS scheme from a leakage-resilient signature scheme, and a construction (labelled by 3 in the figure) of IBS from a leakage-resilient 2-level HIBE scheme.

However, the technique we used in the security proof suffers from *bucket effect*. That is, the leakage rate is restricted by the lower rate of the underlying leakage-resilient components. How to improve the leakage rate in the black-box construction is one of our future work.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (No. 61472146), Guangdong Natural Science Funds for Distinguished Young Scholar (No. 2014A030306021), Guangdong Program for Special Support of

Top-notch Young Professionals (No. 2015TQ01X796), Pearl River Nova Program of Guangzhou (No. 201610010037), and the CICAEET fund and the PAPD fund (No. KJR1615).

References

[1] A. Shamir, Identity-based cryptosystems and signature schemes, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1984, pp. 47--53.

[2] S. S. Al-Riyami, K. G. Paterson, Certificateless public key cryptography, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2003, pp. 452--473.

[3] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, E. W. Felten, Lest we remember: cold-boot attacks on encryption keys, Communications of the ACM 52 (5) (2009) 91--98.

[4] P. C. Kocher, Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems, in: Advances in Cryptology-CRYPTO'96, Springer, 1996, pp. 104--113.

[5] J.-J. Quisquater, D. Samyde, Electromagnetic analysis (ema): Measures and counter-measures for smart cards, in: Smart Card Programming and Security, Springer, 2001, pp. 200--210.

[6] J.-S. Coron, Resistance against differential power analysis for elliptic curve cryptosystems, in: Cryptographic Hardware and Embedded Systems, Springer, 1999, pp. 292--302.

[7] D. Boneh, R. A. DeMillo, R. J. Lipton, On the importance of checking cryptographic protocols for faults, in: Advances in Cryptology-EUROCRYPT'97, Springer, 1997, pp. 37--51.

[8] S. Dziembowski, K. Pietrzak, Leakage-resilient cryptography, in: Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on, IEEE, 2008, pp. 293--302.

[9] S. Micali, L. Reyzin, Physically observable cryptography, in: Theory of Cryptography, Springer, 2004, pp. 278--296.

[10] A. Akavia, S. Goldwasser, V. Vaikuntanathan, Simultaneous hardcore bits and cryptography against memory attacks, in: Theory of Cryptography, Springer, 2009, pp. 474--495.

[11] J. Katz, V. Vaikuntanathan, Signature schemes with bounded leakage resilience, in: Advances in Cryptology--ASIACRYPT 2009, Springer, 2009, pp. 703--720.

[12] T. Malkin, I. Teranishi, Y. Vahlis, M. Yung, Signatures resilient to continual leakage on memory and computation, in: Theory of Cryptography Conference, Springer, 2011, pp. 89--106.

[13] S. Faust, C. Hazay, J. B. Nielsen, P. S. Nordholt, A. Zottarel, Signature schemes secure against hard-to-invert leakage, Journal of Cryptology 29 (2) (2016) 422--455.

[14] T. H. Yuen, S. M. Yiu, L. C. Hui, Fully leakage-resilient signatures with auxiliary inputs, in: Australasian Conference on Information Security and Privacy, Springer, 2012, pp. 294--307.

[15] E. Boyle, G. Segev, D. Wichs, Fully leakage-resilient signatures, Journal of cryptology 26 (3) (2013) 513--558.

[16] Y. Wang, K. Tanaka, Generic transformation to strongly existentially unforgeable signature schemes with leakage resiliency, in: International Conference on Provable Security, Springer, 2014, pp. 117--129.

[17] Y. Wang, K. Tanaka, Generic transformation to strongly existentially unforgeable signature schemes with continuous leakage resiliency, in: Australasian Conference on Information Security and Privacy, Springer, 2015, pp. 213--229.

[18] D. Boneh, E. Shen, B. Waters, Strongly unforgeable signatures based on computational diffie-hellman, in: Public Key Cryptography-PKC 2006, Springer, 2006, pp. 229--240.

[19] Y. Wang, K. Tanaka, Generic transformations for existentially unforgeable signature schemes in the bounded leakage model, Security and Communication Networks 9 (12) (2016) 1829--1842.

[20] J. Huang, Q. Huang, C. Pan, A black-box construction of strongly unforgeable signature schemes in the bounded leakage model, in: Provable Security, Springer Nature, 2016, pp. 320--339.

[21] Q. Huang, D. S. Wong, Y. Zhao, Generic transformation to strongly unforgeable signatures, in: Applied Cryptography and Network Security, Springer, 2007, pp. 1--17.

[22] K. G. Paterson, Id-based signatures from pairings on elliptic curves, Electronics Letters 38 (18) (2002) 1025--1026.

[23] F. Hess, Efficient identity based signature schemes based on pairings, in: International Workshop on Selected Areas in Cryptography, Springer, 2002, pp. 310--324.

[24] J. C. Choon, J. H. Cheon, An identity-based signature from gap diffie-hellman groups, in: International Workshop on Public Key Cryptography, Springer, 2003, pp. 18--30.

[25] J. H. Cheon, Y. Kim, H. Yoon, et al., A new id-based signature with batch verification., IACR Cryptology ePrint Archive 2004 (2004) 131.

[26] X. Chen, F. Zhang, K. Kim, A new id-based group signature scheme from bilinear pairings., IACR Cryptology ePrint Archive 2003 (2003) 116.

[27] T. Li, J. Li, Leakage-resilient traceable identity-based signature scheme, Journal of Computational and Theoretical Nanoscience 13 (1) (2016) 878--889.

[28] J.-D. Wu, Y.-M. Tseng, S.-S. Huang, Leakage-resilient id-based signature scheme in the generic bilinear group model, Security and Communication Networks.

[29] D. Galindo, S. Vivek, A practical leakage-resilient signature scheme in the generic group model, in: International Conference on Selected Areas in Cryptography, Springer, 2012, pp. 50--65.

[30] Z. Zhang, D. S. Wong, J. Xu, D. Feng, Certificateless public-key signature: security model and efficient construction, in: International Conference on Applied Cryptography and Network Security, Springer, 2006, pp. 293--308.

[31] W.-S. Yap, S.-H. Heng, B.-M. Goi, An efficient certificateless signature scheme, in: International Conference on Embedded and Ubiquitous Computing, Springer, 2006, pp. 322--331.

[32] X. Huang, Y. Mu, W. Susilo, D. S. Wong, W. Wu, Certificateless signatures: new schemes and security models, The Computer Journal 55 (4) (2012) 457--474.

[33] R. Tso, X. Huang, W. Susilo, Strongly secure certificateless short signatures, Journal of Systems and Software 85 (6) (2012) 1409--1417.

[34] S. Duan, Certificateless undeniable signature scheme, Information Sciences 178 (3) (2008) 742--755.

[35] S. Chang, D. S. Wong, Y. Mu, Z. Zhang, Certificateless threshold ring signature, Information Sciences 179 (20) (2009) 3685--3696.

[36] H. Yuan, F. Zhang, X. Huang, Y. Mu, W. Susilo, L. Zhang, Certificateless threshold signature scheme from bilinear maps, Information Sciences 180 (23) (2010) 4714--4728.

[37] Y.-C. Chen, C.-L. Liu, G. Horng, K.-C. Chen, A provably secure certificateless proxy signature scheme, International Journal of Innovative Computing, Information and Control 7 (9) (2011) 5557--5569.

[38] S.-H. Seo, K. Y. Choi, J. Y. Hwang, S. Kim, Efficient certificateless proxy signature scheme with provable security, Information Sciences 188 (2012) 322--337.

[39] J. K. Liu, M. H. Au, W. Susilo, Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model, in: Proceedings of the 2nd ACM symposium on Information, computer and communications security, ACM, 2007, pp. 273--283.

[40] H. Xiong, Z. Qin, F. Li, An improved certificateless signature scheme secure in the standard model, Fundamenta Informaticae 88 (1-2) (2008) 193--206.

[41] X. Huang, Y. Mu, W. Susilo, D. S. Wong, W. Wu, Certificateless signature revisited, in: Australasian Conference on Information Security and Privacy, Springer, 2007, pp. 308--322.

[42] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, G. Yang, Malicious kgc attacks in certificateless cryptography, in: Proceedings of the 2nd ACM symposium on Information, computer and communications security, ACM, 2007, pp. 302--311.

[43] Y. Yuan, D. Li, L. Tian, H. Zhu, Certificateless signature scheme without random oracles, in: International Conference on Information Security and Assurance, Springer, 2009, pp. 31--40.

[44] C. Gentry, A. Silverberg, Hierarchical id-based cryptography, in: International Conference on the Theory and Application of Cryptology and

Information Security, Springer, 2002, pp. 548--566.

[45] M. Bellare, C. Namprempre, G. Neven, Security proofs for identity-based identification and signature schemes, Journal of Cryptology 22 (1) (2009) 1--61.

[46] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, SIAM journal on computing 32 (3) (2003) 586--615.

[47] B. C. Hu, D. S. Wong, Z. Zhang, X. Deng, Certificateless signature: a new security model and an improved generic construction, Designs, Codes and Cryptography 42 (2) (2007) 109--126.

[48] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, in: Annual International Cryptology Conference, Springer, 2001, pp. 213--229.

[49] A. Lewko, Y. Rouselakis, B. Waters, Achieving leakage resilience through dual system encryption, in: Theory of Cryptography Conference, Springer, 2011, pp. 70--88.