Privacy for Private Key in Signatures

Qianhong Wu[1,3,4], Bo Qin[2,3,4], Yi Mu[4], and Willy Susilo[4]

[1] School of Computer, Wuhan University,
Wuhan City, China
[2] Department of Mathematics, School of Science,
Xi'an University of Technology, Xi'an, China
qinboo@xaut.edu.cn
[3] Department of Computer Engineering and Mathematics,
Universitat Rovira i Virgili, Tarragona, Spain
qianhong.wu@urv.cat
[4] Center for Computer and Information Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong NSW 2522, Australia
{wsusilo,ymu}@uow.edu.au

Abstract. One of the important applications of digital signature is anonymous credential or pseudonym system. In these scenarios, it is essential that the identity of the signer is kept secret from any third party, except the trusted authority. The identity in such a system is uniquely identified by the *secret key* (or the signing key) rather than the public key, since the public key may be repeatedly randomized. This paper formalizes this notion by investigating a new property of digital signatures, called *key indistinguishability*. In this notion, given a number of digital signatures generated from two known public keys, an adversary cannot determine whether the signing keys used to generate these public keys, and hence the signatures, are the same. This property ensures that the signatures do not leak any information of the signing keys. Observing that existing digital signatures without random oracles do not provide such a property, we fill the gap with the first key indistinguishable signature scheme which is existentially unforgeable under a chosen message attack without using random oracles. The proposed scheme is also efficient and practical for applications in pseudonym systems.

Keywords: Anonymous identity, Key privacy, Key indistinguishability, Key leakage, Chosen message attack, Pairing groups.

1 Introduction

It is generally believed that *privacy* is the most important goal of cryptography. In this paper, we investigate the issue of key privacy in digital signatures.

M. Yung, P. Liu, and D. Lin (Eds.): Inscrypt 2008, LNCS 5487, pp. 84–95, 2009.
© Springer-Verlag Berlin Heidelberg 2009

1.1 Key Privacy in Digital Signatures

The most important security of signatures is unforgeability. A digital signature must contain enough information of the secret signing key to achieve unforgeability. Now an interesting question is that given a number of signatures under different public keys, whether a polynomial time attacker can computationally extract some useful information of the secret signing keys which is contained in the signatures. The attacker may use its extracted information to compromise high-level systems which use these signatures as underlying blocks.

Unfortunately, the security of the signing keys (or secret keys) in digital signatures is seldom studied. Our work is motivated by the idea of investigating a different and additional security requirement of digital signatures, namely *key indistinguishability* or *key-anonymity*. In this new security requirement, the digital signature schemes must provide *privacy of the signing key* under which the signature was generated, in addition to the conventional unforgeability. Specifically, the key indistinguishability refers to the security requirement that the adversary, possessing a number of signatures verifiable by a set of public keys, *cannot decide* whether there exist two public keys that share a common secret key. In other words, the signer is *anonymous* from the adversary's point of view. We note that in this type of scenario, the identity of the signer is uniquely identified by its secret key, since the public key may be randomized as pseudonyms [21]. Hence, we also call this notion as *key-anonymity* since it refers to the fact that the signer is *anonymous* from the adversary's point of view.

Anonymity of signatures has attracted a lot of attentions since the pioneering work of group signatures due to Chaum and van Heyst [11] and ring signatures introduced by Rivest, Shamir and Tauman [23]. Many other cryptographic systems related to anonymity of signatures have been proposed such as pseudonym systems [21], untraceable RFID tags [2], anonymous credentials [10] and direct anonymous attestation [9]. We observe that the key-anonymity or key indistinguishability of signatures plays an essential role over such anonymous systems. Unfortunately, to date, there is no comprehensive and formal study provided in the literature to investigate this notion.

The new notion of key indistinguishability of digital signatures formalizes the property of key privacy in a way that it captures the intuition of previous research in a strong sense. In our definition, the adversary knows two public keys pk_0, pk_1 corresponding to two secret keys sk_0, sk_1 which identify two entities. The adversary is allowed to obtain signatures as many as requested adaptively (in the adaptive chosen message attacks), and the signatures are verifiable with pk_0 and pk_1. Possession of these signatures *should not* enable the adversary to determine whether $sk_0 = sk_1$ or not. This definition yields the notion of *key indistinguishability under a chosen message attack* (KIND-CMA). Clearly, from this game of key indistinguishability, a signature scheme where the key generation algorithm of the public key is *deterministic* must be key-distinguishable, since one cannot produce two different public keys corresponding to the same secret key. Hence, we require that a signature scheme has a probabilistic key

generation algorithm of public key, where given a single secret key, exponentially many public keys can be produced.

1.2 Related Work

Formal notions on key privacy have appeared in the context of symmetric encryptions such as those in [1,13,15]. Abadi and Rogaway [1] showed that popular modes of operation of block ciphers, such as CBC, provide key privacy if the block cipher is a pseudorandom permutation. The notion provided by Desai [13] is to capture a security property for block cipher-based encryption schemes that implies that exhaustive key-search on these schemes is slowed down proportionally to the size of the ciphertext. In this formalization, the popular chosen-ciphertext attacks in the security definitions of encryption schemes were not considered in the context of key privacy. Fischlin [15] observed that providing decryption oracles access to the adversary in their setting makes the task trivial.

Recently, Bellare *et al.* [4] presented a similar notion of key privacy in public-key encryption schemes. They studied the setting of asymmetric encryptions to capture a security property for public-key-based encryption schemes that an attacker cannot determine the public keys that were used to generate the ciphertexts that it sees. They use the classic chosen plaintext attack (CPA) and chosen ciphertext attack (CCA) to model the adversary in their notion. Their goal is to find public key encryption schemes with *receiver anonymity*. In [4], Bellare *et al.* proved that the ElGamal encryption scheme [14] provides key privacy against chosen plaintext attack and the Cramer-Shoup encryption scheme [5] enjoys key privacy under chosen ciphertext attack assuming the hardness of Decisional Diffie-Hellman problem. Although the RSA-OAEP does not provide key privacy, they showed that by simple modifications to the scheme, key privacy can be achieved. Noting the orthogonal relation between the data-privacy and key privacy in public key encryptions, Halevi [20] gave a very simple sufficient condition for key privacy in public key encryptions: A scheme that provides data privacy is guaranteed to also provide key privacy if the distribution of a random encryption of a random message is *independent* of the public key that is used for the encryption.

Very recently, Yang *et al.* [27] introduced a notion of anonymous signatures. In this definition, the adversary is first provided with a set of public keys and *trained* with a series of valid message-signature pairs. Then, the adversary is provided with a challenge signature corresponding to one of these public keys but *the adversary is not allowed to learn the (signed) message*, which seems a too strong assumption, considering the main functionality of signatures is for public verifiability. Finally, the adversary is required to answer which public key was used to generate the signature. The definition of signer anonymity of signatures due to Yang *et al.* can be viewed as a dual notion of key-privacy in public key encryption [4]. Since the adversary is not allowed to learn the signed message, one can naturally view the signature scheme as an asymmetric encryption scheme where the ciphertext is generated by the signing algorithm. Accordingly, the challenge signature in the signer anonymity game defined in [27] is translated into the challenge ciphertext in the receiver anonymity

(key-privacy) game in [4]. This similarity allows to achieve their signer anonymity with similar techniques for receiver anonymity of public key encryption. In fact, Yang *et al.* achieved the signer anonymity of (extended) RSA signature using essentially the same technique as the one for key privacy of (extended) RSA encryption in [4]. For the signer anonymity of (extended) Schnorr signature [24], their treatments (proofs) are different since the signing algorithm in Schnorr signature, which can be viewed as an encryption algorithm in this model, differs from the encryption algorithm in ElGamal encryption.

In contrast to the key privacy of public key encryption [4] or signer anonymity in anonymous signatures [27], in our setting to keep public verifiability of signatures, the task of the adversary accordingly changes to determine whether the signing keys, corresponding to the signature and public keys, are the same or not. This is due to the fact that the public keys known by the adversary can be used to verify the signatures, and therefore, these public keys are linked with specific signatures. Hence, there is no such straightforward sufficient conditions for key privacy in digital signatures due to the public verifiability of signatures.

1.3 Our Contributions

A number of practical signatures [7,10,16,18] have been proven existentially unforgeable without random oracles. Ideally, we expect to prove that some of the existing signatures are also key indistinguishable without using random oracles or easily improve them to achieve this property. Unfortunately, from our analysis *none* of them is key indistinguishable or easily modified to achieve this security property by using the techniques similar to those used for key privacy in asymmetric encryption [4] and signer anonymity in anonymous signature [27].

Motivated by the above view, we formalize the new notion of key indistinguishability in digital signatures. It addresses the issue of information leakage of the *signing keys* which may be exploited by malicious adversaries. That is, given a number of digital signatures generated from two known public keys, an adversary cannot determine whether the signing keys used to generate these public keys, and hence the signatures, are the same.

Observe that existing random oracle free signatures do not provide key indistinguishability, we fill this gap by proposing the first key indistinguishable signatures secure against adaptive chosen message attacks. The security, including the key indistinguishability as well the classic existential unforgeability, is proven without using random oracles. The schemes are also efficient compared to the state-of-the-art signatures without random oracles. The security of our schemes depends on two new computational assumptions, namely the k-th Roots of Discrete Logarithm (k-RoDL) assumption and the k-th Roots of Decision Diffie-Hellman (k-RoDDH) assumption, which are justified in [26].

2 Key Indistinguishability of Signatures

Before defining the notion of key indistinguishability of signatures, we review the classic unforgeability of signatures. For the purpose of the new notion, we

rewrite the key generation algorithm in the standard definition of signatures into two parts, namely the *global parameter generation* algorithm and the *public key generation* algorithm. Ideally, the global parameters are `null`. The detail of the definition is as follows.

Definition 1. *A signature scheme consists of four polynomial time algorithms,* `ParaGen`*,* `KeyGen`*,* `Sign` *and* `Verify`*, for generating the global parameters and the public keys, signing and verifying signatures, respectively.*

- $\Upsilon \leftarrow$ `ParaGen`(1^λ)*: on input a security parameter* λ*,* `ParaGen` *outputs the global parameters denoted by* Υ*.*
- $pk \leftarrow$ `KeyGen`(Υ, sk)*:* `KeyGen` *takes as inputs the global parameters* Υ *and a random string* sk *in the signing key space, outputs a public key* pk *in the verification key space.*
- $\sigma \leftarrow$ `Sign`(m, sk, pk)*:* `Sign` *takes any message* m*, the signing key* sk*, a public key* pk *and outputs a signature* σ*.*
- $1/0 \leftarrow$ `Verify`(m, σ, pk)*: On input a message-signature pair* (m, σ) *and a public key* pk*,* `Verify` *outputs 1 or 0 to represent whether the signature is valid or not.*

The existential unforgeability under a chosen message attack (EUF-CMA) [19] against a signature scheme is defined by the following game between a simulator $\mathcal{S}$ *and an adversary* $\mathcal{A}$*:*

Setup: $\mathcal{S}$ *runs* `ParaGen` *and* `KeyGen` *and obtains the global parameters* Υ *and a public/private key pair* (pk, sk)*.* Υ *and* pk *are provided to* $\mathcal{A}$*.*

Queries: *Adaptively,* $\mathcal{A}$ *requests signatures under* pk*, on at most* q_s *messages of his choice* $m_1, \cdots, m_{q_s}$*.* $\mathcal{S}$ *responds to each query with* σ_i *such that* `Verify`$(pk, m_i, \sigma_i) = 1$*.*

Output: *Eventually,* $\mathcal{A}$ *outputs a pair* (m, σ) *and wins the game if* `Verify`$(pk, m, \sigma) = 1$ *and* $m \notin \{m_1, \cdots, m_{q_s}\}$*.*

A signature scheme is EUF-CMA secure if for any polynomial time adversary $\mathcal{A}$*, it wins the above game with a negligible probability in* λ*.*

We have two remarks on the above definition for the new notion of Key Indistinguishability of Signatures.

Remark 1. In definition 1, it does not state whether the same secret signing key corresponds to a unique public key. In our following new notion, we explicitly require that for different executions of the public key generation algorithm `KeyGen` with the same input (Υ, sk), the public keys corresponding to the same secret key should be different (i.e., `KeyGen` is probabilistic).

Remark 2. Since we allow the same secret key sk to correspond to two (or more) seemingly independent public keys pk_0, pk_1, another issue arises. Let sk correspond to two public keys pk_0, pk_1. Assume $\sigma_0 =$ `Sign`(m, sk, pk_0) and $\sigma_1 =$ `Sign`(m, sk, pk_1). Clearly, we have that `Verify`$(m, \sigma_0, pk_0) = 1$ and

$\texttt{Verify}(m, \sigma_1, pk_1) = 1$ from the correctness of the signature scheme. However, Definition 1 does not state what are the outputs of $\texttt{Verify}(m, \sigma_0, pk_1)$ and $\texttt{Verify}(m, \sigma_1, pk_0)$. In our following notion we clearly require that both output 0, although both pk_0 and pk_1 correspond to the same secret key sk.

Definition 2. *The key indistinguishability under a chosen message attack (KIND-CMA) against a signature scheme is defined by the following game between a simulator $\mathcal{S}$ and an adversary $\mathcal{A}$:*

Setup: *$\mathcal{S}$ runs $\texttt{ParaGen}$ and obtains the global parameters Υ. Choose at random $\rho \in \{0,1\}$ and $sk_0 \in \{0,1\}^{poly(\lambda)}$. If $\rho = 1$, set $sk_1 = sk_0$. If $\rho = 0$, randomly chose $sk_1 \in \{0,1\}^{poly(\lambda)}$. Compute $pk_0 = \texttt{KeyGen}(\Upsilon, sk_0)$ and $pk_1 = \texttt{KeyGen}(\Upsilon, sk_1)$. Υ, pk_0 and pk_1 are provided to $\mathcal{A}$.*

Queries: *Adaptively, $\mathcal{A}$ requests signatures under sk_0 and sk_1, on at most q_s messages m and the secret key of his choice $i \in \{0,1\}$. $\mathcal{S}$ responds to each query with σ such that $\texttt{Verify}(pk_i, m, \sigma) = 1$.*

Output: *Eventually, $\mathcal{A}$ outputs a bit ρ' and wins the game if $\rho' = \rho$.*

A signature scheme is KIND-CMA secure if for any polynomial time adversary $\mathcal{A}$, it wins the above game with a negligible probability in λ.

Clearly, if an adversary can decide whether $sk_0 \stackrel{?}{=} sk_1$ from only the public keys pk_0 and pk_1 (without querying any signatures), the signature scheme cannot be KIND-CMA secure. To be more precise, such type of information leakage of the secret key in such signature schemes is due to the public keys rather than the signatures that use the secret signing keys. However, if any polynomial time algorithm cannot determine whether $sk_0 \stackrel{?}{=} sk_1$ from only the public keys pk_0 and pk_1 without querying any signatures, then intuitively, the notion of KIND-CMA captures that the information leakage about the secret keys is due to the queried signatures. Such information leakage may cause problems in anonymous systems, such as pseudonym or anonymous credential systems.

Note that Remark 2 is also essential to understand the notion of key indistinguishability of signatures. Without the requirement that $\texttt{Verify}(m, \sigma_0, pk_1) = \texttt{Verify}(m, \sigma_1, pk_0) = 0$, we can construct an adversary to win the KIND-CMA game in any signature scheme and make Definition 2 meaningless. Consider an adversary that requests $s_0 = \texttt{Sign}(m, sk_0, pk_0)$ with a query $(m, 0)$, and then tests whether $\texttt{Verify}(m, \sigma_0, pk_1) = 1$. If so, it decides that $sk_0 = sk_1$, otherwise it decides $sk_0 \neq sk_1$ since $\texttt{Verify}(m, \sigma_0, pk_1) = 0$ in the case of $sk_0 \neq sk_1$ from the correctness of a signature scheme. This adversary wins the game for any scheme. This observation also shows for a signature scheme, if it does not satisfy the requirement $\texttt{Verify}(m, \sigma_0, pk_1) = \texttt{Verify}(m, \sigma_1, pk_0) = 0$, it cannot be KIND-CMA secure.

3 Complexity Assumptions

We first review some general concepts of pairing groups [8]. Let $\texttt{PGen}$ be an algorithm that, on input a security parameter 1^λ, outputs a tuple Υ=$(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, e)$,

where $\mathbb{G}_1$ and $\mathbb{G}_2$ have the same prime order p, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$ is an efficient non-degenerate bilinear map such that $e(g_1, g_2) \neq 1$ for all $g_1 \neq 1 \in \mathbb{G}_1, g_2 \neq 1 \in \mathbb{G}_2$, and for all $u, v \in \mathbb{Z}$, $e(g_1^u, g_2^v) = e(g_1, g_2)^{uv}$. For security reasons, p is chosen such that both $(p-1)/2$ and $2p+1$ are also primes.

A pairing map may enable the solution to the conventional DDH problem in either $\mathbb{G}_1$ or $\mathbb{G}_2$. If the classic DDH holds in $\mathbb{G}_1$, then the pairing groups are called XDH (External Diffie-Hellman) groups [3,6]. If the standard DDH problem is difficult in both $\mathbb{G}_1$ and $\mathbb{G}_2$ [17,25], such pairing groups are called SXDH groups [3], which can be chosen as specific subgroups of MNT curves [22].

Suppose that $\Upsilon = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, e) \leftarrow \mathtt{PGen}(1^\lambda)$, where $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_3$ are public. Let $\mathbb{G}_1 = \langle g_1 \rangle$ and $\mathbb{G}_2 = \langle g_2 \rangle$. Our proposals are based on the following assumptions about pairing groups. Let us first provide a notion of *minimal step set pair* which can be used to simplify the description of the new computational assumptions.

Definition 3. *For a positive integer k, we say a pair $S = (I, J)$ is a minimal step set pair defined by k if (i) $1 \in I$ and $1 \in J$;(ii) for any $\hbar \in I \cup J \cup \{k\}$ and $\hbar \neq 1$, there exist $i \in I$ and $j \in J$ such that $\hbar = i + j$; (iii) for any set S' having property (i) and (ii), $\#S' \geq \#S$, where $\#S$ is the cardinality of set $I \cup J$. Denote the set $\{i + j | i \in I \cup \{0\} \wedge j \in J \cup \{0\}\}$ by $\overline{I + J}$.*

For instance, $(\{1,2\},\{1\})$, $(\{1,2\},\{1,3\})$, $(\{1,2,4\},\{1,3\})$ and $(\{1,2,5\},\{1,3,8\})$ are minimal step set pairs defined by 3, 5, 7 and 13, respectively. Given an integer, it may have more than one minimal step set pairs but their cardinality is unique from property *iii*.

Assumption 1 (k-th Roots of Discrete Logarithm (k-RoDL) assumption). *Let $x \leftarrow \mathbb{Z}_p^*$, $X_1 = g_1^x, X_2 = g_2^x$, and k be an integer satisfying* $\gcd(k, p-1) = 1$ *and $S = (I, J)$ is a minimal step set pair defined by k. Assume that $\mathcal{O}_x(\cdot)$ is an oracle that takes as input a pair (c, h), where $c \in \mathbb{Z}_p, h \neq 1 \in \mathbb{G}_1$, and outputs $(h^{(x+c)^{\frac{1}{k}}}, g_2^{(x+c)^{\frac{j}{k}}})$ for $i \in I, j \in J$. Let $\{c\}$ be the queries to $\mathcal{O}_x(\cdot)$. If the queries are distinct, then for any probabilistic polynomial time (PPT) adversaries $\mathcal{A}(\cdot)$,*

$$\Pr\left[\begin{array}{l|l} x \leftarrow \mathbb{Z}_p^* & (c', a, a_i, b_j) \leftarrow \mathcal{A}^{\mathcal{O}_x(\cdot)}(g_1, g_2, X_1, X_2) \\ X_1 = g_1^x & \wedge c' \notin \{c\} \wedge a \in \mathbb{G}_1 \backslash \{1\} \wedge a_i = a^{(x+c')^{\frac{1}{k}}} \\ X_2 = g_2^x & \wedge \forall i \in I \wedge b_j = g_2^{(x+c')^{\frac{j}{k}}} \wedge \forall j \in J \end{array}\right] \leq 1/poly(\lambda)$$

The key indistinguishability of our signature schemes relies on the DDH assumption in $\mathbb{G}_1$ of pairing groups. More precisely, it is based on a stronger version of DDH assumption in which the adversary can access to the additional information about the DDH instance.

Assumption 2 (k-th Roots of Decision Diffie-Hellman (k-RoDDH) assumption). *Let $x \leftarrow \mathbb{Z}_p^*$, $X = g_1^x$, and k be an integer satisfying* $\gcd(k, p-1) = 1$ *and $S = (I, J)$ be a minimal step set pair defined by k. Let $\mathcal{O}_x(\cdot)$*

be an oracle that takes $c \in \mathbb{Z}_p$ *as input, and outputs* $(g_1^{(x+c)^{\frac{i}{k}}}, g_2^{(x+c)^{\frac{j}{k}}})$ *for* $i \in I, j \in J$, *and* $\mathcal{P}_y(\cdot)$ *be an oracle that takes* $c' \neq c \in \mathbb{Z}_p$ *as input, and outputs* $(g_1^r, g_1^{yr}, g_1^{r(y+c')^{\frac{i}{k}}}, g_2^{(y+c')^{\frac{j}{k}}})$ *for* $i \in I, j \in J$ *and a random* $r \in Z_p^*$. *Let* $\{c\}, \{c'\}$ *be the queries to* $\mathcal{O}(\cdot)$ *and* $\mathcal{P}(\cdot)$, *respectively. If the queries in* $\{c\} \cup \{c'\}$ *are distinct, then for any PPT adversaries* $\mathcal{A}(\cdot)$,

$$|\Pr[\mathcal{A}^{\mathcal{O}_x,\mathcal{P}_x}(g_1, g_1^x, g_2) = 1] - \Pr[\mathcal{A}^{\mathcal{O}_x,\mathcal{P}_y}(g_1, g_1^x, g_2) = 1]| < 1/poly(\lambda).$$

This assumption states that, given (g_1, g_1^x, g_2) and the oracles $\mathcal{O}_x(\cdot)$, $\mathcal{P}_x(\cdot)$ and $\mathcal{P}_y(\cdot)$, any PPT adversary cannot tell whether $x = y$. We justify assumptions 1 and 2 in [26].

4 Efficient Key Indistinguishable Signatures without Random Oracles

A number of practical signature schemes [7,10,16,18] have been proven existentially unforgeable without random oracles. Ideally, we expect to prove that some of the existing signatures are also key indistinguishable without using random oracles or easily improve them to achieve this property. Unfortunately, from our analysis in [26], *none* of the existing schemes is key indistinguishable or easy to improve to meet this property. In the following, we fill this gap by propose a new key indistinguishable signature without using random oracles.

Suppose that $\Upsilon = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g_2, e) \leftarrow \mathtt{PGen}(1^\lambda)$ is the global parameters, where $\mathbb{G}_1$ and $\mathbb{G}_2 = \langle g_2 \rangle$ have prime order p, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$ is an efficient non-degenerate bilinear map. Let $H(\cdot) : \{0,1\}^{\ell_m} \times \mathbb{G}_1^2 \rightarrow \mathbb{Z}_p^*$ be a collision resistant hash function, where ℓ_m is the bitlength of the message to be signed. Although a hash function is used in our constructions, but it does not serve as a random oracle in our security proofs. Now ware ready to describe and prove our signature scheme with key indistinguishability.

KeyGen: Randomly choose $g_1 \neq 1 \leftarrow \mathbb{G}_1, x \leftarrow \mathbb{Z}_p^*$, $X = g_1^x$. The public key is (g_1, X). The secret key is x.

Sign: For $m \in \{0,1\}^*$, compute

$$c = H(m||g_1||X), a_1 = g_1^{(x+c)^{\frac{1}{3}}}, a_2 = g_1^{(x+c)^{\frac{2}{3}}}, b_1 = g_2^{(x+c)^{\frac{1}{3}}}.$$

The resulting signature is (a_1, a_2, b_1).

Verify: For $m \in \mathbb{Z}_p^*$, and a signature (a_1, a_2, b_1), compute $c = H(m||g_1||X)$ and check that

$$e(a_1, g_2) = e(g_1, b_1), e(a_1, b_1) = e(a_2, g_2), e(a_2, b_1) = e(Xg_1^c, g_2).$$

If all checks hold, output 1 for `valid`; otherwise, output 0 for `invalid`.

Theorem 1. *In the standard model, the signature scheme described above is correct and EUF-CMA secure under the k-RoDL assumption. If the DDH holds in $\mathbb{G}_1$, then the signature is KIND-CMA secure under the k-RoDDH assumption for $k = 3$, independent of the fact whether there is an efficient distortion map $\psi : \mathbb{G}_2 \to \mathbb{G}_1$.*

Proof. The correctness is trivial and omitted. Let us first show the EUF-CMA security. Consider the standard EUF-CMA game between a simulator $\mathcal{S}$ and an adversary $\mathcal{A}$ who breaks our signature scheme. We show that in the EUF-CMA game, $\mathcal{A}$ can be used by $\mathcal{S}$ as a subroutine to break the k-RoDL for $k = 3$ with the same advantage.

Let $\mathcal{S}$ be given a k-RoDL challenge (g_1, g_2, X, Y) defined in Section 2.2 for $k = 3$, where $g_1 \neq 1 \in \mathbb{G}_1$, $g_2 \neq 1 \in \mathbb{G}_2$, $X = g_1^x$ and $Y = g_2^x$. $\mathcal{S}$ forwards (g_1, X) to $\mathcal{A}$ as its public key. Now whenever $\mathcal{A}$ requests a signature on message $m \in \mathbb{Z}_p^*$, $\mathcal{S}$ computes $c = H(m||g_1||X)$ and queries the 3-RoDL oracle $\mathcal{O}_x(\cdot)$ with (c, h_1), where $h_1 = g_1^\delta$ for a random $\delta \leftarrow \mathbb{Z}_p^*$. $\mathcal{O}_x(\cdot)$ outputs a tuple $(a_1 = h_1^{(x+c)^{\frac{1}{3}}}, a_2 = h_1^{(x+c)^{\frac{2}{3}}}, b_1 = g_2^{(x+c)^{\frac{1}{3}}})$. $\mathcal{S}$ sends $(a_1^{\delta^{-1}}, a_2^{\delta^{-1}}, b_1)$ to $\mathcal{A}$ as the simulated signature on m. Clearly, the output is a valid signature which will be accepted by the verification algorithm and the simulation of $\mathcal{S}$ is perfect.

Finally, $\mathcal{A}$ outputs a valid signature $\sigma = (a_1', a_2', b_1')$ on some message m' that it did not query for. Since the hash function is collision-resistant and $m' \neq m$, $c' = H(m'||g_1||X)$ is not any of the previous queries in $\{c\}$. Therefore, in order to prove security, we need to show that the forgery $\sigma = (a_1', a_2', b_1')$ on m' that passes the verification equations must be of the forms: $a_1' = g_1^{(x+c')^{\frac{1}{3}}}$, $a_2' = g_1^{(x+c')^{\frac{2}{3}}}$, and $b_1' = g_2^{(x+c')^{\frac{1}{3}}}$ and hence, $(c', g_1, a_1', a_2', b_1')$ is a solution to the 3-RoDL challenge (g_1, g_2, X, Y).

Let $g_3 = e(g_1, g_2), a_1' = g_1^\alpha, a_2' = g_1^\beta, b_1' = g_2^\gamma$. We wish to show that $\alpha = \gamma = (x + c')^{\frac{1}{3}}$, $\beta = (x + c')^{\frac{2}{3}}$. From the verification equations and the bilinearity of e, we obtain that

$g_3^\alpha = e(g_1, g_2)^\alpha = e(g_1^\alpha, g_2) = e(a_1', g_2) = e(g_1, b_1') = e(g_1, g_2^\gamma) = g_3^\gamma$,
$g_3^{\alpha\gamma} = e(g_1, g_2)^{\alpha\gamma} = e(g_1^\alpha, g_2^\gamma) = e(a_1', b_1') = e(a_2', g_2) = e(g_1^\beta, g_2) = g_3^\beta$,
$g_3^{\beta\gamma} = e(g_1, g_2)^{\beta\gamma} = e(g_1^\beta, g_2^\gamma) = e(a_2', b_1') = e(Xg_1^{c'}, g_2) = e(g_1^{x+c'}, g_2)$
$= e(g_1, g_2)^{x+c'} = g_3^{x+c'}$.

As g_3 is a generator of $\mathbb{G}_3$, we can take the logarithm base g_3 on both sides, and obtain $\alpha = \gamma, \alpha\gamma = \beta, \beta\gamma = x+c'$. It follows that $\alpha = \gamma = (x+c')^{\frac{1}{3}}$, $\beta = (x+c')^{\frac{2}{3}}$, which gives us the relation as desired. Hence, using $(c', g_1, a_1', a_2', b_1')$ from $\mathcal{A}$, $\mathcal{S}$ breaks the 3-RoDL assumption.

Now, we show the KIND-CMA security. Assume that there exists a PPT adversary $\mathcal{B}$ breaking the KIND-CMA security of our scheme. We prove that in the KIND-CMA game, $\mathcal{B}$ can be used by $\mathcal{S}$ as a subroutine to break the k-RoDDH for $k = 3$ with the same advantage.

On 3-RoDDH input (g_1, g_1^x, g_2), the simulator $\mathcal{S}$ queries $\mathcal{P}_y$ on a random input, disregard all output except (h_1, h_1^y) for some $h_1 \in \mathbb{G}_1$. $\mathcal{S}$ generates two public keys as $pk_0 = (g_1, g_1^x)$ and $pk_1 = (h_1, h_1^y)$. $\mathcal{S}$ sends $\mathcal{B}$ two public keys

pk_0, pk_1 and the global parameters $(p, \mathbb{G}_1, \mathbb{G}_2, g_2, H(\cdot))$ which are the same as those in the scheme. Let $\mathcal{B}$ request a signature for index $i \in \{0,1\}$ on $m \in \mathbb{Z}_p^*$. If $i = 0$, $\mathcal{S}$ computes $c = H(m||g_1||g_1^x)$. $\mathcal{S}$ queries $\mathcal{O}_x(c)$ to obtain the output $(g_1^{(x+c)^{\frac{1}{3}}}, g_1^{(x+c)^{\frac{2}{3}}}, g_2^{(x+c)^{\frac{1}{3}}})$. and returns the signature $(g_1^{(x+c)^{\frac{1}{3}}}, g_1^{(x+c)^{\frac{2}{3}}}, g_2^{(x+c)^{\frac{1}{3}}})$ to $\mathcal{B}$. If $i = 1$, $\mathcal{S}$ computes $c = H(m||h_1||h_1^y)$. $\mathcal{S}$ resets $\mathcal{O}(\cdot)$ with 3-RoDDH input (h_1, h_1^y, g_2) and queries $\mathcal{O}_y(c)$ to obtain the output $(h_1^{(y+c)^{\frac{1}{3}}}, h_1^{(y+c)^{\frac{2}{3}}}, g_2^{(y+c)^{\frac{1}{3}}})$. It returns the signature $(h_1^{(x+c)^{\frac{1}{3}}}, h_1^{(x+c)^{\frac{2}{3}}}, g_2^{(x+c)^{\frac{1}{3}}})$ to $\mathcal{B}$. It is easy to see that the simulation is perfect.

Eventually, $\mathcal{B}$ outputs a bit 1 or 0 representing that $x = y$ or $x \neq y$, respectively. $\mathcal{S}$ directly uses $\mathcal{B}$'s reply to answer the 3-RoDDH challenge. Indeed, $\mathcal{S}$ and $\mathcal{B}$ will succeed with identical probabilities. □

Efficiency. The public key consists of two elements in $\mathbb{G}_1$ and it is short. A signature consists of three elements $a_1, a_2 \in \mathbb{G}_1$ and $b_1 \in \mathbb{G}_2$. When the elliptic curves described in [7],[8] are used, we obtain a signature in the standard model $5 \log p$ bits in size. Our key generation is more efficient and the public key is shorter than those of the Boneh-Boyen scheme and the Camenisch-Lysyanskaya-04 scheme. Signature generation is comparable to the Camenisch-Lysyanskaya-04 scheme and less efficient than the Boneh-Boyen scheme. The verification overhead is similar to that of the Camenisch-Lysyanskaya-04 scheme. Nevertheless, our scheme is *KIND-CMA secure* while the previous schemes are not. Our signature enjoys an additional advantage: under a fixed public key, one can change the number of elements in $\mathbb{G}_1$ and $\mathbb{G}_2$ to achieve an optimal signature length for different purpose (noting that elements in $\mathbb{G}_1$ and $\mathbb{G}_2$ are significantly different in size).

*Extensions.*Without degrading the security of the scheme above, one can replace the public key $pk = (g_1, g_1^x)$ with $pk = (g_1, e(g_1, g_2)^x)$ and accordingly adapt the verification procedure. We note that the adapted scheme is IND-CMA secure *without* requiring that the DDH holds in $\mathbb{G}_1$, assuming the widely accepted classic DDH in the multiplicative subgroup $\mathbb{G}_3$ of a finite field. The above signature can also be naturally extended for $k > 3$, for instance, $k = 5$. In the same settings, the signature for $k = 5$ is a tuple $(g_1^{(x+c)^{\frac{1}{5}}}, g_1^{(x+c)^{\frac{2}{5}}}, g_2^{(x+c)^{\frac{1}{5}}}, g_2^{(x+c)^{\frac{3}{5}}})$ for public key $pk = (g_1, g_1^x)$, where $c = H(m||g_1||g_1^x)$. It has the same security property as the scheme for $k = 3$.

5 Conclusion

We investigated a new security property called key indistinguishability for conventional digital signatures. On the one hand, this notion captures the information leakage of secret key in signature schemes. This information leakage is due to either the public key or the signatures produced with the corresponding secret key. On the other hand, the key indistinguishability of a signature scheme by its own implies an excellent class of anonymity to be used to construct complex anonymous systems. Finally, we constructed the first family of digital signatures that are provably key indistinguishable. Our schemes are also practical

for applications as an independent conventional signature scheme or an efficient building block of high-level anonymous protocols and pseudonym systems. It is also interesting to find more efficient key indistinguishable signatures and unique applications of the new notion of key privacy in signatures in the future.

Disclaimer and Acknowledgments

This work was mainly supported by the Australian ARC Discovery Grants DP0663306 and DP0877123, and partially by the China NSF projects 60673071 and 60873268, the China NSF key project 90718006, the China 863 projects 2008AA01Z40, 2006AA01Z442 and 2007AA01Z411, the China 973 project 2007C-B310801, and the Spanish Ministry of Science and Innovation through projects TSI2007-65406-C03-01 "E-AEGIS" and CONSOLIDER CSD2007-00004 "ARES", and by the Government of Catalonia under grant 2005 SGR 00446. The authors being with the UNESCO Chair in Data Privacy are solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organization.

References

1. Abadi, M., Rogaway, P.: Reconciling Two Views of Cryptography (The Computational Soundness of Formal Encryption). In: Watanabe, O., Hagiya, M., Ito, T., van Leeuwen, J., Mosses, P.D. (eds.) TCS 2000. LNCS, vol. 1872, pp. 3–22. Springer, Heidelberg (2000)
2. Ateniese, G., Camenisch, J., de Medeiros, B.: Untraceable RFID Tags via Insubvertible Encryption. In: Meadows, C. (ed.) ACM CCS 2005, pp. 92–101. ACM Press, New York (2005)
3. Ballard, L., Green, M., de Medeiros, B., Monrose, F.: Correlation-resistant Storage. Technical Report TR-SP-BGMM-050705, Johns Hopkins University (2005), `http://spar.isi.jhu.edu/~mgreen/correlation.pdf`
4. Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 566–582. Springer, Heidelberg (2001)
5. Bellare, M., Rogaway, P.: Optimal Asymmetric Encryption-How to Encrypt with RSA. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 92–111. Springer, Heidelberg (1995)
6. Boneh, D., Boyen, X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
7. Boneh, D., Boyen, X.: Short Signatures Without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004)
8. Boneh, D., Lynn, B., Shacham, H.: Short Signatures from the Weil Pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001)
9. Brickell, E., Camenisch, J., Chen, L.: Direct Anonymous Attestation. In: Pfitzmann, B. (ed.) ACM CCS 2004, pp. 132–145. ACM Press, New York (2004)

10. Camenisch, J.L., Lysyanskaya, A.: Signature Schemes and Anonymous Credentials from Bilinear Maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)
11. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
12. Cramer, R., Shoup, V.: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)
13. Desai, A.: The Security of All-or-Nothing Encryption: Protecting against Exhaustive Key Search. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 359–375. Springer, Heidelberg (2000)
14. ElGamal, T.: A Public Key Cryptosystem and Signature Scheme Based on Discrete Logarithms. IEEE Transaction on Information Theory 31, 467–472 (1985)
15. Fischlin, M.: Pseudorandom Function Tribe Ensembles Based on One-Way Permutations: Improvements and Applications. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 432–445. Springer, Heidelberg (1999)
16. Fischlin, M.: The Cramer-Shoup Strong-RSASignature Scheme Revisited. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 116–129. Springer, Heidelberg (2002)
17. Galbraith, S.-D., Rotger, V.: Easy Decision Diffie-Hellman Groups. Journal of Computation and Mathematics 7, 201–218 (2004)
18. Gennaro, R., Halevi, S., Rabin, T.: Secure Hash-and-Sign Signatures without the Random Oracle. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 123–139. Springer, Heidelberg (1999)
19. Goldwasser, S., Micali, S., Rivest, R.: A Digital Signature Scheme Secure against Adaptive Chosen-message Attacks. SIAM J. Computing 17(2), 281–308 (1988)
20. Halevi, S.: A Sufficient Condition for Key-privacy. Technique report (2005), `http://eprint.iacr.org/`
21. Lysyanskaya, A., Rivest, R.L., Sahai, A., Wolf, S.: Pseudonym Systems. In: Heys, H.M., Adams, C.M. (eds.) SAC 1999. LNCS, vol. 1758, pp. 184–199. Springer, Heidelberg (2000)
22. Miyaji, A., Nakabayashi, M., Takano, S.: New Explicit Conditions of Elliptic Curves for FR-reduction. IEICE Transactions on Fundamentals E84-A(5), 1234–1243 (2001)
23. Rivest, R.L., Shamir, A., Tauman, Y.: How to Leak a Secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer, Heidelberg (2001)
24. Schnorr, C.-P.: Efficient Identification and Signatures for Smart Cards. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 239–252. Springer, Heidelberg (1990)
25. Verheul, E.R.: Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 195–210. Springer, Heidelberg (2001)
26. Wu, Q., Qin, B., Mu, Y., Susilo, W.: Privacy for Private Key in Signatures. Full version (2009), `http://eprint.iacr.org/`
27. Yang, G., Wong, D., Deng, X., Wang, H.: Anonymous Signature Schemes. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 347–363. Springer, Heidelberg (2006)