Provably Security Identity-based Sanitizable Signature Scheme without Random Oracles

Yang Ming
School of Information Engineering, Chang'an University, Xi'an 710064, China
Email: yangming@chd.edu.cn

Xiaoqin Shen
School of Sciences, Xi'an University of Technology, Xi'an 710054, China
Email: elle_shen@sohu.com

Yamian Peng
College of Science, Hebei Polytechnic University, Tang Shan 063009, China
Email: pym806@163.com

***Abstract*—A sanitizable signature scheme is a signature which allows a semi-trusted party called sanitizer to hide parts of the original message after the message is signed, without interacting with the signer. A verifier can confirm the integrity of disclosed parts of the sanitized document from the signature. Sanitizable signatures are quite useful in governmental or military offices, where there is a dilemma between disclosure requirements of documents and private secret. In this paper, we give a formal definition and secure model of identity-based sanitizable signature by combining identity-based cryptography and sanitizable signature. Motivated by Waters' signature scheme, we present an identity-based sanitizable signature scheme without random oracles (in the standard model) using bilinear pairing. Finally, security analysis shows that our proposed scheme satisfies all the security requirements.**

***Index Terms*—identity-based signature, sanitizable signature, random oracle, bilinear pairing, security**

I. INTRODUCTION

In 1984, Identity-based (ID-based) public key cryptography which was introduced by Shamir [1], has rapidly emerged in recent years and been widely applied. The main idea of ID-based cryptography is that the user's public key can be calculated directly from his/her identity such as email addresses rather than being extracted from a certificate issued by a certificate authority (CA). Private keys are generated for the users by a trusted third party, called Private Key Generation (PKG) using master key related to the global parameters for the system. The direct derivation of public keys eliminates the need for certificates and some of the problems associated with them. ID-based cryptography is supposed to provide a more convenient alternative to conventional public key infrastructure. Since Boneh and Franklin [2] proposed a practical ID-based encryption scheme, many papers have been published in this area such as [3-6].

The digital signature has been an essential tool in E-society which is designed to prevent alteration of a signed digital document. However, applications like E-Government, E-Education and E-Health systems need appropriate alteration of some signed documents in order to hide sensitive information other than protect the integrity of the document. For example, in the disclosure of official information, national secret information is masked when an official document is sanitized so that its nonsensitive information can be disclosed when it is demanded by a citizen. If this disclosure is done digitally by the traditional digital signature schemes, the citizen cannot verify the disclosed information correctly because the information has been changed to prevent the leakage of sensitive information. That is, with current digital signature schemes, the confidentiality of official information is incompatible with the integrity of that information. This is called the *digital document sanitizing problem* in [7]. Similar solutions for this problem have been proposed in [8] as *content extraction signature*; and in [9] as *redactable signature*. In 2005, a sanitizable signature scheme was introduced by Ateniese et al. in [10], which can alter the signed document instead of hiding the signed document. The main goal of sanitizable signatures is to protect the confidentially of a specified part of the document while ensuring the integrity of the document. A sanitizable signature scheme is a new kind of digital signature which allows a designated part, called the sanitizer, to hide certain parts of the original document after the document is signed, without interacting with the signer. The verifier confirms the integrity of disclosed parts of the sanitized document from the signature and sanitized document. In other words, a sanitizable signature scheme allows a semi-trusted sanitizer to modify designated parts of the document and produce a valid signature on the legitimately modified document without any interaction with the signer. These designated portions of the document are blocks or segments explicitly indicated as mutable under prior valid signature only if it modifies

This work is supported by the NaturaL Science Fundation of Shaanxi Province (No. 2010JQ8017) and the Special Found for Basic Scientific Research of Central Colleges, Chang'an University (No. CHD2009JC099). Corresponding author: Yang Ming.

doi:10.4304/jsw.6.10.1890-1897

there portions an no other parts of the message. The sanitizable signatures have several important applications. For example, a sanitizable signatures can be used to ensure the integrity, authenticity, and anonymity of public health information in medical records [10]. In general, sanitizable signatures can accommodate different levels of data de-identification, supporting the minimum necessary disclosure standard of the existing privacy laws. This provides flexibility not available in redactable signatures. Following these works, several authors[11-23] proposed various sanitizable signature schemes with different properties.

To the best of my knowledge, all the sanitizable signature schemes are based on Public Key Infrastructure setting, there is no construction of identity-based sanitizable signature (IDSS) scheme in the literature. However, it would be of great practical interest to design an IDSS scheme. As it avoids the need to distribute public key certificates, identity-based cryptography has found many advantages in the systems such as ad hoc networks, mobile networks, etc. Also, provably security is the basic requirement for IDSS schemes. the schemes [8, 12, 14, 15] were only proven secure in the random oracles model. The random oracle model was introduced by Bellare and Rogaway in [24]. The model is a formal model in analyzing cryptographic schemes, where a hash function is considered as a black-box that contains a random function. Although this model is efficient and useful, it has received a lot of criticism that the proofs in the random oracle model are not proofs. Canetti et al.[25] have shown that security in the random oracle model does not imply the security in the real world in that a scheme can be secure in the random oracle model and yet be broken without violating any particular intractability assumption, and without breaking the underlying hash functions. Therefore, to design a provable secure identity-based sanitizable signature scheme in the standard model (without random oracles) remains an open and interesting research problem.

In this paper, motivated by Waters' signature [6, 26] and sanitizable signature [17, 22], we first present the precise the model of the IDSS and propose an identity-based sanitizable signature scheme scheme without random oracles. Finally, we provide a fully security proof for our proposed scheme according to our model.

II. PRELIMINARIES

In this section, we briefly review the basic concepts on bilinear pairings and corresponding complexity assumption which our scheme is based on.

A. Bilinear Pairings

Let G_1 and G_2 be two multiplicative cyclic groups of prime order q and let g be a generator of G_1. The map $e: G_1 \times G_1 \to G_2$ is said to be an admissible bilinear pairing with the following properties:

(1)**Bilinearity**: For all $u, v \in G_1$, and $a, b \in Z_q$, $e(u^a, v^b) = e(u, v)^{ab}$.

(2)**Non-degeneracy**: $e(g, g) \neq 1$.

(3)**Computability**: There exists an efficient algorithm to compute $e(u, v)$ for all $u, v \in G_1$.

We note the modified Weil and Tate pairings associated with supersingular elliptic curves are examples of such admissible pairings.

B. Complexity Assumptions

The security of our scheme relies on the hardness of the following problem.

Computational Diffie-Hellman (CDH) Problem. Given $g, g^a, g^b \in G_1$, for unknown $a, b \in Z_q^*$, compute g^{ab} .

The success probability of a polynomial time algorithm A in solving CDH problem is denoted as

$$Succ_A^{CDH} = \Pr[A(g, g^a, g^b) = g^{ab}] \geq \varepsilon$$

Definition 1. The computational (t, ε) CDH assumption holds if no t -time adversary has at least ε in solving CDH problem.

III. FORMAL MODEL OF IDENTITY-BASED SANITIZABLE SIGNATURE SCHEME

In the section, we will give the syntax of an Identity based sanitizable signature scheme and its formal security model.

A. Syntax

Identity-based sanitizable signature (IDSS) scheme enables the authenticity of a disclosed document to be verified in four-party model consisting of a private key generator (PKG), a signer, a sanitizer, and a verifier. An IDSS scheme consists of the algorithms (**Setup, Extract, Sign, Sanitize, Verify**). Let $ID = (ID_1 \cdots ID_n) \in \{0,1\}^n$ and $M = (m_1 \cdots m_n) \in \{0,1\}^n$, where ID_i and m_i is defined as i th bit of the identity ID and the message M , respectively. Let $K_s \subseteq \{1, \cdots, n\}$ denote the set of indices that the sanitizer is allowed to alter. In the following, we give the detail definitions of these algorithms.

Setup. Given a security parameter k , the private key generator (PKG) generates system parameters *params* and a master key *msk* . *params* is made public while *msk* is kept secret.

Extract. Given an identity ID , PKG computes private key d_{ID} with the master key *msk* and sends it to the corresponding user through a secure channel.

Sign. Given *params* , a signer's identity ID_s , a message M and the private key of signer d_{ID_s} , the signer outputs a signature σ and a secret information ψ for the sanitizer.

Sanitize. Given *params* , the signer's identity ID_s , the secret information ψ from signer and the corresponding signature σ on the message M , the sanitizer outputs a message $\bar{M}$ and sanitized signature $\bar{\sigma}$.

Verify. Given $params$, the signer's identity ID_s, an unsanitized message/signature pair (M,σ) or a sanitized message/signature pair $(\bar{M},\bar{\sigma})$, the verifier outputs *accept* or *reject*.

Sign correctness. We require that Verify($params, ID_s, M, \sigma$) = *accept* for an unsanitized message M, if

(1) $(params, msk) \leftarrow \text{Setup}(1^k)$

(2) $(d_{ID_s}) \leftarrow \text{Extract}(params, msk, ID_s)$

(3) $(\sigma,\psi) \leftarrow \text{Sign}(params, ID_s, M, d_{ID_s})$

Sanitize correctness. We require that Verify($params, ID_s, \bar{M}, \bar{\sigma}$) = *accept* for a sanitized message $\bar{M}$, if:

(1) $(params, msk) \leftarrow \text{Setup}(1^k)$

(2) $(d_{ID_s}) \leftarrow \text{Extract}(params, msk, ID_s)$

(3) $(\bar{M},\bar{\sigma}) \leftarrow \text{Sanitize}(params, ID_s, M, \sigma, \psi)$

B. Security Model

According to [11], there are several security requirements that sanitizable signatures need to satisfy. In the following, we extend these notions to adapt for ID-based sanitizable signatures.

Unforgeability. For a signature scheme, the well-known security notion is existential unforgeability against chosen message attacks [27]. The property requires that no any one can forge the signer's or sanitizer's signature (this can be thought of as an outsider attack). For the unforgeability, we consider the following game played between a challenger C and an adversary A:

Setup. C runs the Setup algorithm of IDSS with a security parameter k and obtains system parameters $params$ and the master secret key msk. It then sends $params$ to A and keeps msk secret itself.

Query. A can perform a polynomially bounded number of the following queries. These queries may be made adaptively, i.e. each query may depend on the answers to the previous queries.

Private key extraction query. The adversary A chooses an identity ID, C runs the Extract algorithm on ID to return the private key d_{ID} to A.

Signature query. The adversary A chooses an identity ID and a message M, C runs Extract algorithm and Sign algorithm on (ID, M) to return σ to A.

Forgery. Finally, A outputs a signature σ^* for the message M^* on the identity ID^* such that

(1) ID^* has not been requested as one of private key extraction queries.

(2) (ID^*, M^*) has not been requested as one of signature queries.

(3) σ^* is a valid signature.

The advantage of an adversary A is defined as the success probability that it wins above game.

Definition 2. (Unforgeability) An ID-based sanitizable signature scheme is said to $(\varepsilon, t, q_e, q_s)$ existential unforgeability against adaptive chosen message attacks (EUF-IDSS-CMA) if no t time adversary winning the unforgeability game with advantage at least ε after asking at most q_e private key extraction queries and q_s signature queries.

Note that in unforgeability game the adversary A is not allowed to make a sanitized signature query. The reason is that our scheme satisfies the strong transparency [17], which property needs the any verifier does not know if the message has been sanitized. In the other word, a sanitized signature is indistinguishable from a normal signature by the signer for the same message on the same identity.

Indistinguishability. For the indistinguishability, we consider the following game played between a challenger C and a distinguisher D:

Setup. The challenger C runs the Setup algorithm with a security parameter k to obtain the system parameter $params$ and master key msk, then it sends $params$ to D and keeps msk secret.

Phase 1. D performs a polynomially bounded number of private key extraction queries and signature queries adaptively just like in the unforgeability game.

Challenge. After the phase 1 is over, D outputs two message/signature pairs (M_0^*, σ_0^*) and (M_1^*, σ_1^*) on the identity ID^* and set K^* of indices which are permitted to modify, it submits them to C. Then C picks a random bit $b \in \{0,1\}$. If $b = 0$, C runs the Sanitize algorithm and returns $(\bar{M}_0^*, \bar{\sigma}_0^*)$ to D. Otherwise, if $b = 1$, C runs again the Sanitize algorithm and returns $(\bar{M}_1^*, \bar{\sigma}_1^*)$ to D.

Phase 2. D can again ask a polynomial bounded number of queries adaptively as in the phase 1.

Guess. Finally, D outputs a bit b' and wins the game if $b' = b$.

The advantage of D is defined as

$$Adv(D) = |\Pr[b' = b] - 1/2|$$

where $\Pr[b' = b]$ denotes the probability that $b' = b$.

Definition 3. (Indistinguishability) An ID-based sanitizable signature scheme is said to be $(\varepsilon, t, q_e, q_s)$ unconditionally indistinguishable if there is no t time distinguisher winning the indistinguishability game with the advantage at least ε after asking at most q_e private key extraction queries and q_s signature queries.

In [11], the property of accountability requires that a part (the signer and the sanitizer) should not be held responsible for message originating from the other party. Note that accountability is not need in our security model as it compromises the unconditional indistinguishability of our scheme.

Immutability. The property requires that the sanitizer should not be able to produce a valid signature for a message where it has altered other than the parts are allowed to sanitized (this can be thought of as an insider attack). For the immutability, we consider the game played between a challenger C and an adversary A:

Initial. A sends a challenge K_s to C, which is the set of indices that the sanitizer is allowed to alter.

Setup. C runs the Setup algorithm with a security parameter k and obtains system parameters *params* and the master secret key *msk*. C sends *params* to A and keeps *msk* secret.

Query. A performs a polynomially bounded number of queries adaptively just like in the unforgeability game. Note that, in the signature query, C also sends the secret information ψ to A.

Forgery. Finally, A outputs a signature σ^* for the message $M^* = (m_1^* \cdots m_n^*)$ on the identity ID^* such that

(1)for any $j \in \{1, \cdots, q_s\}$, there exists $i \notin K_s : m_{j,i} \neq m_i^*$.

(2) σ^* is a valid signature.

The advantage of A is defined as the success probability that it wins above game.

Definition 4. (Immutability) An ID-based sanitized signature scheme is $(\varepsilon, t, q_e, q_s)$ immutable if no t time adversary winning the immutability game with advantage at least ε after asking at most q_e private key extraction queries and q_s signature queries.

IV. The Proposed Scheme

In this section, we describe the our IDSS scheme that is provably secure in the standard model (without random oracles). Our IDSS scheme is inspired by scheme in [6, 17, 22]. The IDSS consists of the following algorithms:

Setup. Given a security parameter k, PKG chooses two cyclic groups G_1 and G_2 of prime order q, a generator $g \in G_1$ and a admissible bilinear pairing $e: G_1 \times G_1 \to G_2$. It then chooses a random value $\alpha \in Z_q^*$, computes $g_1 = g^\alpha$ and selects $g_2 \in G_1$. Furthermore, PKG picks $u', m' \in G_1$ and two vectors $\mathrm{u} = (u_i)$, $\mathrm{v} = (v_i)$ of length n, whose entries are random elements from G_1. The system parameters are $params = (G_1, G_2, e, q, g, g_1, g_2, u', m', \mathrm{u}, \mathrm{v})$ and the master key is g_2^α.

Extract. Let ID be the n-bit identity $ID_1, \cdots, ID_n$. For a user with identity ID, its private key d_{ID} is generated as follow. PKG randomly picks $r_{ID} \in Z_q^*$ and computes

$$d_{ID} = (d_1, d_2) = \left(g_2^\alpha (u' \prod_{i=1}^{n} u_i^{ID_i})^{r_{ID}}, g^{r_{ID}} \right)$$

Sign. Let m be the n-bit message $m_1, \cdots, m_n$ and K_s be the set of indices that the sanitizer is permitted to modify. The signer randomly chooses $r \in Z_q^*$ and computes

$$\sigma_1 = d_1 (v' \prod_{i=1}^{n} v_i^{m_i})^r = g_2^\alpha (u' \prod_{i=1}^{n} u_i^{ID_i})^{r_{ID}} (v' \prod_{i=1}^{n} v_i^{m_i})^r$$

$$\sigma_2 = d_2 = g^{r_{ID}}, \sigma_3 = g^r$$

The resultant signature is $\sigma = (\sigma_1, \sigma_2, \sigma_3)$. Then the signer sends the secret information $(v_i)^r (i \in K_s)$ to the sanitizer via a secure channel. Alternately, these values may be encrypted by the sanitizer and sent across.

Sanitize. Let $\bar{M} = (\bar{m}_1, \cdots, \bar{m}_n)$ be the message whose signature differ from $M = (m_1, \cdots, m_n)$ at indices $K \subseteq K_s$. Let $K' = \{i \in K : m_i = 0, \bar{m}_i = 1\}$ and $K'' = \{i \in K : m_i = 1, \bar{m}_i = 0\}$ such that $K' \cup K'' = K$ and $K' \cap K'' = \Phi$. When receiving $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ and $(v_i)^r (i \in K_s)$ from the signer, the sanitizer does as follows.

(1)check the validity of the signature σ.

(2)choose $\bar{r}_{ID}, \bar{r} \in Z_q^*$ and compute

$$\bar{\sigma}_1 = \sigma_1 (u' \prod_{i=1}^{n} u_i^{ID_i})^{\bar{r}_{ID}} \frac{\prod_{i \in K'} v_i^r}{\prod_{i \in K''} v_i^r} (v' \prod_{i=1}^{n} v_i^{\bar{m}_i})^{\bar{r}}$$

$$\bar{\sigma}_2 = \sigma_2 g^{\bar{r}_{ID}}, \bar{\sigma}_3 = \sigma_3 g^{\bar{r}}$$

The resultant sanitized signature is $\bar{\sigma} = (\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3)$.

Verify. The verifier accepts the signature if and only if the following equality holds:

$$e(\sigma_1, g) = e(g_1, g_2) e(u' \prod_{i=1}^{n} u_i^{ID_i}, \sigma_2) e(v' \prod_{i=1}^{n} v_i^{m_i}, \sigma_3)$$

Note that the verify algorithm is same for a sanitized signature and non-sanitized signature

Correctness: To show correctness, we need to show that the validation of the normal signature and sanitized signature.

$$\begin{aligned} e(\sigma_1, g) &= e\left(g_2^\alpha (u' \prod_{i=1}^{n} u_i^{ID_i})^{r_{ID}} (v' \prod_{i=1}^{n} v_i^{m_i})^r, g \right) \\ &= e(g_2^\alpha, g) e\left((u' \prod_{i=1}^{n} u_i^{ID_i})^{r_{ID}}, g \right) e\left((v' \prod_{i=1}^{n} v_i^{m_i})^r, g \right) \\ &= e(g_1, g^{\alpha}) e(u' \prod_{i=1}^{n} u_i^{ID_i}, g^{r_{ID}}) e(v' \prod_{i=1}^{n} v_i^{m_i}, g^r) \\ &= e(g_1, g_2) e(u' \prod_{i=1}^{n} u_i^{ID_i}, \sigma_2) e(v' \prod_{i=1}^{n} v_i^{m_i}, \sigma_3) \end{aligned}$$

From the $K' = \{i \in K : m_i = 0, \bar{m}_i = 1\}$ and $K'' = \{i \in K : m_i = 1, \bar{m}_i = 0\}$, we can obtain $\bar{m}_i - m_i = \{1, i \in K'; 0, i \in K''\}$.

$$\begin{aligned} \bar{\sigma}_1 &= \sigma_1 (u' \prod_{i=1}^{n} u_i^{ID_i})^{\bar{r}_{ID}} \frac{\prod_{i \in K'} v_i^r}{\prod_{i \in K''} v_i^r} (v' \prod_{i=1}^{n} v_i^{\bar{m}_i})^{\bar{r}} \\ &= g_2^\alpha (u' \prod_{i=1}^{n} u_i^{ID_i})^{r_{ID}} (v' \prod_{i=1}^{n} v_i^{m_i})^r (u' \prod_{i=1}^{n} u_i^{ID_i})^{\bar{r}_{ID}} \prod_{i=1}^{n} v_i^{r(\bar{m}_i - m_i)} (v' \prod_{i=1}^{n} v_i^{\bar{m}_i})^{\bar{r}} \\ &= g_2^\alpha (u' \prod_{i=1}^{n} u_i^{ID_i})^{(r_{ID} + \bar{r}_{ID})} v'^{r r} v'^{\bar{r}} (\prod_{i=1}^{n} v_i^{m_i})^r (\prod_{i=1}^{n} v_i^{r(\bar{m}_i - m_i)}) (\prod_{i=1}^{n} v_i^{\bar{m}_i})^{\bar{r}} \\ &= g_2^\alpha (u' \prod_{i=1}^{n} u_i^{ID_i})^{(r_{ID} + \bar{r}_{ID})} v'^{(r + \bar{r})} (\prod_{i=1}^{n} v_i^{\bar{m}_i})^{(r + \bar{r})} \\ &= g_2^\alpha (u' \prod_{i=1}^{n} u_i^{ID_i})^{(r_{ID} + \bar{r}_{ID})} (v' \prod_{i=1}^{n} v_i^{\bar{m}_i})^{(r + \bar{r})} \end{aligned}$$

$$\bar{\sigma}_2 = \sigma_2 g^{\bar{r}_{ID}} = g^{r_{ID}} g^{\bar{r}_{ID}} = g^{(r_{ID} + \bar{r}_{ID})}$$

$$\bar{\sigma}_3 = \sigma_3 g^{\bar{r}} = g^r g^{\bar{r}} = g^{(r + \bar{r})}$$

V. ANALYSIS OF THE PROPOSED SCHEME

In the section, we analyze the security of our proposed scheme and give the comparison with sanitizable signature schemes.

A. Security Proof

In this subsection, we prove that our proposed ID-based sanitizable signature scheme constructed in the previous section satisfies the required security property, i.e. unforgeability, indistinguishability and immutability.

Theorem 1. (Unforgeability) The IDSS scheme is $(\varepsilon, t, q_e, q_s)$ -existentially unforgeable against adaptively chosen message and identity attacks in the standard model, assuming that (ε', t') -CDH assumption holds, where

$$\varepsilon' = \frac{1}{16q_s(q_e+q_s)(n+1)^2}\varepsilon,\ t' = t + (5q_e + (2n+4)q_s)t_e$$

here t_e denotes the time of an exponentiation in G_1 and n denotes length of bit string of message.

Proof. Assume that there is a polynomial bounded adversary A that is able to break the unforgeability of our scheme, then there exists an algorithm B that can compute g^{ab} with a non-negligible advantage when receiving a random CDH problem instance g, g^a, g^b. B runs A as subroutine and acts as the challenger in unforgeability game and interacts with A as described below.

Setup. B randomly chooses the following elements.

(1)two integers $0 \le l_u \le q$ and $0 \le l_m \le q$.

(2)two integers $0 \le k_u \le n$ and $0 \le k_m \le n$ ($l_u(n+1) < q$, $l_m(n+1) < q$).

(3)an integer $x' \in Z_{l_u}$ and n-dimensional vector $(x_1, \cdots, x_n) \in Z_{l_u}$.

(4)an integer $y' \in Z_{l_m}$ and n-dimensional vector $(y_1, \cdots, y_n) \in Z_{l_m}$.

(5)an integer $z' \in Z_q$ and n-dimensional vector $(z_1, \cdots, z_n) \in Z_q$.

(6)an integer $\omega' \in Z_q$ and n-dimensional vector $(\omega_1, \cdots, \omega_n) \in Z_q$.

For ease of analysis, we define four functions for the identity $ID = (ID_1, \cdots, ID_n)$ and the message $M = (m_1, \cdots, m_n)$, where $(ID_i, m_i) \in \{0,1\}, (1 \le i \le n)$:

$$F(ID) = x' + \sum_{i=1}^{n} x_i ID_i - l_u k_u \quad \text{and} \quad J(ID) = z' + \sum_{i=1}^{n} z_i ID_i$$

$$K(M) = y' + \sum_{i=1}^{n} y_i m_i - l_m k_m \quad \text{and} \quad L(M) = \omega' + \sum_{i=1}^{n} \omega_i m_i$$

Then B assigns system parameters as follows:

(1) $g_1 = g^a$ and $g_2 = g^b$.

(2) $u' = g_2^{-l_u k_u + x'} g^{z'}$ and $u_i = g_2^{x_i} g^{z_i}$ ($1 \le i \le n$), which means that, for any identity ID, we have $u' \prod_{i=1}^{n} u_i^{ID_i} = g_2^{F(ID)} g^{J(ID)}$

(3) $v' = g_2^{-l_m k_m + y'} g^{\omega'}$ and $v_i = g_2^{y_i} g^{\omega_i}$ ($1 \le i \le n$), which means that, for any message M, we have $v' \prod_{i=1}^{n} v_i^{m_i} = g_2^{K(M)} g^{L(M)}$.

Finally, B returns all parameters to A. We can see that all distributions are identical to that in real world.

Query. B answers the private key extraction queries and signature queries as follows.

Private key extraction query. When A issues a private key extraction query on an identity ID, B acts as follows:

(1)If $F(ID) = 0 \bmod l_u$, B aborts and reports failure.

(2)If $F(ID) \ne 0 \bmod l_u$, B can construct a private key by picking a random $r_{ID} \in Z_q^*$ and computing:

$$d_{ID} = (d_1, d_2) = \left(g_1^{-\frac{J(ID)}{F(ID)}} (g_2^{F(ID)} g^{J(ID)})^{r_{ID}}, g_1^{-\frac{1}{F(ID)}} g^{r_{ID}} \right)$$

Signature query. When A issues a signature query for the message $M = (m_1, \cdots, m_n)$ on the identity $ID = (ID_1, \cdots, ID_n)$, B acts as follows:

(1)If $F(ID) \ne 0 \bmod l_u$, B can construct a private key for ID as in private key extraction query, and then use the Sign algorithm to create a signature on M.

(2)If $F(ID) = 0 \bmod l_u$ and $K(M) \ne 0 \bmod l_m$, B picks $r', r'' \in Z_q^*$ and computes

$$(\sigma_1, \sigma_2, \sigma_3) = \left((u' \prod_{i=1}^{n} u_i^{ID_i})^{r'} g_1^{-\frac{L(m)}{K(m)}} (v' \prod_{i=1}^{n} v_i^{m_i})^{r''}, g^{r'}, g_1^{-\frac{1}{K(m)}} g^{r''} \right)$$

where $\overline{r''} = r'' - \frac{a}{K(m)}$. This equation shows that B's replies to A's signature queries are distributed as they would be in an interaction with a real challenger.

(3)If $F(ID) = 0 \bmod l_u$ and $K(M) = 0 \bmod l_m$, B aborts and reports failure.

Forgery. If B did not abort, A will output a valid signature $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$ on M^* and ID^*. If $F(ID^*) \ne 0 \bmod q$ and $K(M^*) \ne 0 \bmod q$, then B aborts. Otherwise, $F(ID^*) = 0 \bmod q$ and $K(M^*) = 0 \bmod q$, then we can compute $\frac{\sigma_1^*}{(\sigma_2^*)^{J(ID^*)} (\sigma_3^*)^{L(M^*)}}$, which is the solution to given CDH problem.

It remains only to analyze the success probability and running time of B.

Analogy to [26], we can obtain the success probability of B is $\varepsilon' = \frac{1}{16q_s(q_e+q_s)(n+1)^2}\varepsilon$.

Algorithm B 's running time is the same as A 's running time plus the time it takes to respond to q_e private key extraction queries and q_s signature queries. Each private key extraction query needs B to perform 5 exponentiation in G_1. Each signature query needs B to perform $2n+4$ exponentiation in G_1. We assume that an exponentiation in G_1 takes time t_e. Hence, the total running time is at most $t' = t + (5q_e + (2n+4)q_s)t_e$.

Theorem 2. (Indistinguishability) The proposed scheme is unconditionally indistinguishability against a $(\varepsilon, t, q_e, q_s)$ adaptive chosen message distinguisher D.

Proof. The Challenger C interacts with the distinguisher D as follows.

Setup. C sets the system parameters as follows:

(1)choose randomly $u', u_1, \cdots, u_n \in G_1$.

(2)choose randomly $s_s, \cdots, s_n \in Z_q^*$ and computes $v_i = g^{s_i} (i = 1, \cdots, n)$.

(3)choose other system parameters which are identical to Setup algorithm in section V.

Then, C sends system parameters $(G_1, G_2, e, q, g, g_1, g_2, u', m', u_1, \cdots, u_n, v_1, \cdots, v_n)$ to D.

Phase 1. Because C has know the master key, he can runs Extract algorithm, Sign algorithm to response to private key extraction queries and signature queries, respectively.

Challenge. At the end of Phase 1, D chooses two signatures $\sigma_0^* = (\sigma_{0,1}^*, \sigma_{0,2}^*, \sigma_{0,3}^*)$ and $\sigma_1^* = (\sigma_{1,1}^*, \sigma_{1,2}^*, \sigma_{1,3}^*)$ for $M_0^* = (m_{0,1}^*, \cdots, m_{0,n}^*)$ and $M_1^* = (m_{1,1}^*, \cdots, m_{1,n}^*)$ on ID^*. Additionally, D chooses a set K^* of indices which is permitted to modify. Without loss generalization, we assume $K^* = (n-l+1, \cdots, n)$ such that $|K^*| = l$. Let $K_1^* = \{i \in K^*, j \in \{0,1\} : m_{j,i}^* = 0, m_i^* = 1\}$ and $K_2^* = \{i \in K^*, j \in \{0,1\} : m_{j,i}^* = 1, m_i^* = 0\}$ such that $K_1^* \cup K_2^* = K^*$ and $K_1^* \cap K_2^* = \Phi$. C picks a random bit $\gamma \in \{0,1\}$.

If $\gamma = 0$, C randomly chooses $\bar{r}_0^*, \hat{r}_0^* \in Z_q^*$ and computes

$$\bar{\sigma}_{0,1}^* = \sigma_{0,1}^* (u' \prod_{i=1}^{n} u_i^{ID_i^*})^{\bar{r}_0^*} \frac{\prod_{i \in K_1^*} (\sigma_{0,3}^*)^{s_i}}{\prod_{i \in K_2^*} (\sigma_{0,3}^*)^{s_i}} (v' \prod_{i=1}^{n} v_i^{m_{0,i}^*})^{\hat{r}_0^*}$$

$$\bar{\sigma}_{0,2}^* = \sigma_{0,2}^* g^{\bar{r}_0^*}, \bar{\sigma}_{0,3}^* = \sigma_{0,3}^* g^{\hat{r}_0^*}$$

and sets $\bar{\sigma}^* = \bar{\sigma}_0^* = (\bar{\sigma}_1^* = \bar{\sigma}_{0,1}^*, \bar{\sigma}_2^* = \bar{\sigma}_{0,2}^*, \bar{\sigma}_3^* = \bar{\sigma}_{0,3}^*)$.

If $\gamma = 1$, C randomly chooses $\bar{r}_1^*, \hat{r}_1^* \in Z_q^*$ and computes

$$\bar{\sigma}_{1,1}^* = \sigma_{1,1}^* (u' \prod_{i=1}^{n} u_i^{ID_i^*})^{\bar{r}_1^*} \frac{\prod_{i \in K_1^*} (\sigma_{1,3}^*)^{s_i}}{\prod_{i \in K_2^*} (\sigma_{1,3}^*)^{s_i}} (v' \prod_{i=1}^{n} v_i^{m_{1,i}^*})^{\hat{r}_1^*}$$

$$\bar{\sigma}_{1,2}^* = \sigma_{1,2}^* g^{\bar{r}_0^*}, \bar{\sigma}_{1,3}^* = \sigma_{1,3}^* g^{\hat{r}_1^*}$$

and sets $\bar{\sigma}^* = \bar{\sigma}_1^* = (\bar{\sigma}_1^* = \bar{\sigma}_{1,1}^*, \bar{\sigma}_2^* = \bar{\sigma}_{1,2}^*, \bar{\sigma}_3^* = \bar{\sigma}_{1,3}^*)$.

Finally, C returns $\bar{\sigma}^* = (\bar{\sigma}_1^*, \bar{\sigma}_2^*, \bar{\sigma}_3^*)$ to D.

Stage 2. After D receiving the challenge message/ signature pair from C, the distinguisher D still asks private key extraction queries and signature queries.

We show that the two sanitized signatures are indistinguishable, i.e. the following distributions are identical:

$$\Pr[\bar{\sigma}_0^* = \bar{\sigma}^*] = \Pr\begin{bmatrix} \bar{\sigma}_{0,1}^* = \bar{\sigma}_1^* \\ \bar{\sigma}_{0,2}^* = \bar{\sigma}_2^* \\ \bar{\sigma}_{0,3}^* = \bar{\sigma}_3^* \end{bmatrix} = \Pr\begin{bmatrix} \bar{r}_0^* = \bar{r}^* \\ \hat{r}_0^* = \hat{r}^* \end{bmatrix} = \frac{1}{q^2}$$

$$\Pr[\bar{\sigma}_1^* = \bar{\sigma}^*] = \Pr\begin{bmatrix} \bar{\sigma}_{1,1}^* = \bar{\sigma}_1^* \\ \bar{\sigma}_{1,2}^* = \bar{\sigma}_2^* \\ \bar{\sigma}_{1,3}^* = \bar{\sigma}_3^* \end{bmatrix} = \Pr\begin{bmatrix} \bar{r}_1^* = \bar{r}^* \\ \hat{r}_1^* = \hat{r}^* \end{bmatrix} = \frac{1}{q^2}$$

which means both distributions of probabilities are the same, and advantage of D is negligible. Therefore, our proposed scheme satisfies indistinguishability property.

Theorem 3. (Immutability) Assume there is an adversary A that is able to break the immutability of our scheme with an advantage ε when running in a time t and making at most q_e private key extraction queries and q_s signature queries. Then there exists an algorithm B that can produce a valid signature in a time $t' = t + (lq_e + 2lq_s)t_e$ with the advantage $\varepsilon' = \varepsilon$, where t_e denotes the time of an exponentiation in G_1 and l denotes the number of the bit positions which is allowed to alter.

Proof. Assume that there exists a polynomial bounded adversary A that is able to break the immutability of our scheme, then there exists an algorithm B that can generate a valid signature with a non-negligible advantage. B runs A as subroutine and acts as the challenger in immutability game and interacts with A as described below.

Initial. We assume that $K_s \subseteq \{1, \cdots, n\}$ is a set which sanitizer is allowed to alter. A provides B the challenge set $K \subseteq K_s$. For the ease of analysis, we assume $K = \{n-l+1, \cdots, n\}$, where $|K| = l$.

Setup. The adversary A interacts with B and B 's challenger C in unforgeability game as follows:

(1) B make a query to the challenger C in unforgeability game, C returns the system parameters $(G_1, G_2, e, q, g, g_1, g_2, u', v', u_1, \cdots, u_{n-l}, v_1, \cdots, v_{n-l})$ to B.

(2) B chooses $t_i \in Z_q^*$ for $i = n-l+1, \cdots, n$ and sets $u_i = g^{t_i} (i = n-l+1, \cdots, n)$.

(3) B chooses $s_i \in Z_q^*$ for $i = n-l+1, \cdots, n$ and sets $v_i = g^{s_i} (i = n-l+1, \cdots, n)$.

At last, B provided the system parameters $(G_1, G_2, e, q, g, g_1, g_2, u', v', u_1, \cdots, u_n, v_1, \cdots, v_n)$ to A.

Query. B answers the private key extraction queries and signature queries as follows.

Private key extraction query. When A issues a private key extraction query on the identity $ID = (ID_1, \cdots, ID_n)$, B acts as follows:

(1) B requests a private key from the C on the identity $(ID_1,\cdots,ID_{n-l})$ and obtains (d_1,d_2).

(2) B sets $\bar{d}_1 = d_1 \cdot \prod_{i=n-l+1}^{n} d_2^{ID_i t_i}$ and $\bar{d}_2 = d_2$.

Finally, B sends $(\bar{d}_1,\bar{d}_2)$ to A.

Signature query. When A issues a signature query for the message $M=(m_1,\cdots,m_n)$ on the identity $ID=(ID_1,\cdots,ID_n)$, B acts as follows:

(1) B requests a signature from C for the message $(m_1,\cdots,m_{n-l})$ on the identity $(ID_1,\cdots,ID_{n-l})$ and obtains $(\sigma_1,\sigma_2,\sigma_3)$.

(2) B sets $\bar{\sigma}_1 = \sigma_1 \cdot \prod_{i=n-l+1}^{n} \sigma_2^{ID_i t_i} \cdot \prod_{i=n-l+1}^{n} \sigma_3^{m_i s_i}$, $\bar{\sigma}_2 = \sigma_2$ and $\bar{\sigma}_3 = \sigma_3$.

Finally, B sends $(\bar{\sigma}_1,\bar{\sigma}_2,\bar{\sigma}_3)$ and $\sigma_3^{m_i s_i} (i=n-l+1,\cdots,n)$ to A.

Forgery. A outputs a valid signature $\bar{\sigma}^* = (\bar{\sigma}_1^*,\bar{\sigma}_2^*,\bar{\sigma}_3^*)$ for the message $\bar{M}^* = (\bar{m}_1^*,\cdots,\bar{m}_n^*)$ on the identity $I\bar{D}^* = (I\bar{D}_1^*,\cdots,I\bar{D}_n^*)$, B can obtain a valid signature as follows:

(1) A sends $\bar{\sigma}^* = (\bar{\sigma}_1^*,\bar{\sigma}_2^*,\bar{\sigma}_3^*)$ to B for the message $\bar{M}^* = (\bar{m}_1^*,\cdots,\bar{m}_n^*)$ on the identity $I\bar{D}^* = (I\bar{D}_1^*,\cdots,I\bar{D}_n^*)$. For any $j \in \{1,\cdots,q_s\}$, there exists $i \notin \{n-l+1,\cdots,n\}$ such that $m_{j,i} \neq \bar{m}_i^*$.

(2) B sets $ID^* = (ID_1^*,\cdots,ID_{n-l}^*)$ and $M^* = (m_1^*,\cdots,m_{n-l}^*)$, where $m_i^* = \bar{m}_i^*$ for all $i = 1,\cdots,n-l$. We all known that for any $j \in \{1,\cdots,q_s\}$, there exists $i \notin \{1,\cdots,n-l\}$ such that $m_{j,i} \neq m_i^*$. B computes

$$\sigma_1^* = \frac{\bar{\sigma}_1^*}{\prod_{i=n-l+1}^{n} (\bar{\sigma}_2^*)^{\overline{ID}_i^* \bar{t}_i^*} \cdot \prod_{i=n-l+1}^{n} (\bar{\sigma}_3^*)^{\bar{m}_i^* \bar{s}_i^*}}$$

$$\sigma_2^* = \bar{\sigma}_2^*,\ \sigma_3^* = \bar{\sigma}_3^*$$

Thus, $\sigma^* = (\sigma_1^*,\sigma_2^*,\sigma_3^*)$ is a valid signature for the message $M^* = (m_1^*,\cdots,m_{n-l}^*)$ on the identity $ID^* = (ID_1^*,\cdots,ID_{n-l}^*)$. According to Theorem 1, we can solve CDH problem.

It remains only to analyze the success probability and running time of B. Algorithm B succeeds when A does, that is, with probability at least ε.

Algorithm B's running time is the same as A's running time plus the time it takes to respond to q_e private key extraction queries and q_s signature queries. Each private key extraction query needs B to perform l exponentiation in G_1. Each signature query needs B to perform $2l$ exponentiation in G_1. We assume that an exponentiation in G_1 takes time t_e. Hence, the total running time is at most $t' = t + (lq_e + 2lq_s)t_e$.

B. Comparison

We compare our IDSS scheme with existing sanitizable signature schemes in Table I. In the table, let

TABLE I.
COMPARISON OF OUR SCHEME WITH EXISTING SCHEMES

Schemes	Security	Model	ID-based	Strong Transparency
[8]	RSA	ROM	×	×
[9]	US	SM	×	×
[7]	US	SM	×	×
[10]	US+CH	SM	×	×
[11]	UD+CT	SM	×	×
[12]	Co-GDH	ROM	×	×
[13]	-	-	×	√
[14]	CDH	ROM	×	×
[15]	Co-GDH	ROM	×	×
[16]	Strong RSA	SM	×	×
[17]	CDH+XDH	SM	×	×
[18]	US+CT+PRG	SM	×	×
[20]	US+CH	SM	×	×
[21]	US+CT+PRG	SM	×	√
[22]	CDH	SM	×	√
[23]	GS	ROM	×	√
Our Scheme	CDH	SM	√	√

SM be standard model, ROM be random oracle model, US be underlying signature scheme, CT be commitment scheme, CH be chameleon hash, PRG be pseudo random generator and GS be group signature.

From Table I, we know that our scheme and [13, 21, 22] satisfy strong transparency property. But there is no formally security proof in [13]. To the best of my knowledge, our proposed scheme is the first scheme under the identity-based setting, which eliminates the need for public key certificate and provides a more convenient alternative to conventional scheme based on public key infrastructure. Our scheme requires no pairing operation in the Sign and Sanitize algorithm, and needs 3 pairing operations in Verify algorithm. Our scheme is more efficient and may be suitable for secure routing and multicast and database applications.

VI. CONCLUSION

As a special signature, ID-based sanitizable signatures are widely applicable, it is very suitable for the cases in which the sanitizer can alter the signed document in order to hide personal sensitive information. In this paper, we study IDSS based on Waters' signature scheme by combining Identity-based cryptography and sanitizable signature. We firstly proposed the model and a concrete scheme of IDSS in the standard model. And we show that the proposed scheme is security in our model.

REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes", in *CRYPTO'84*, LNCS 196, G. R. Blakley and D. Chaum, Eds. Berlin: Springer-Verlag, 1984, pp. 47-53.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", in *CRYPT'01*, LNCS 2139, J. Kilian, Ed. Berlin: Springer-Verlag, 2001, pp. 213-229.

[3] K.G. Paterson, "ID-based signatures from pairings on elliptic curves", *IEEE Communication Letter*, vol. 38, pp. 1025-1026, August 2002.

[4] J.C. Cha and J.H. Cheon, "An identity-based signature from gap Diffie-Hellman groups", in *PKC'03*, LNCS 2567, Y. Desmedt, Ed. Berlin: Springer-Verlag, 2003, pp.18-30.

[5] F. Hess, "Efficient identity based signature schemes based on pairings", in *SAC'02*, LNCS 2595, K. Nyberg and H. Heys, Eds. Berlin: Springer-Verlag, 2002, pp. 310 -324.

[6] K.G. Paterson and J.C.N. Schuldt, "Efficient identity based signatures secure in the standard model", in *ACISP'06*, LNCS 4058, L. M. Batten and R. Safavi-Naini, Eds. Berlin: Springer-Verlag, 2006, pp. 207-222.

[7] K. Miyazaki, S. Susaki, M. Iwamura, T. Matsumoto, R Sasaki, and H. Yoshiura, "Digital documents sanitizing problem", *IEICE*, vol. 195, pp. 61-67, 2003.

[8] R. Steinfeld, L. Bull, and Y. Zheng, "Content extraction signatures", in *ICISC'01*, LNCS 2288, K. Kim, Ed. Berlin: Springer-Verlag, 2002, pp. 285-304.

[9] R. Johnson, D. Molnar, D.X. Song, and D. Wagner, "Homomorphic signature schemes", in *CT-RSA'02*, LNCS 2271, B. Preneel, Ed. Berlin: Springer-Verlag, 2002, pp. 244-262.

[10] G. Ateniese, D.H. Chou, B. de Medeiros, and G. Tsudik, "Sanitizable Signatures", in *ESORIC'05*, LNCS 3679, S. De Capitani di Vimercati, Paul F. Syverson, D. Gollmann, Eds. Berlin: Springer-Verlag, 2005, pp. 159-177.

[11] M. Miyazaki, M. Iwamura, T. Matsumoto, et al, "Digitally signed document sanitizing scheme with disclosure condition control", *IEICE Transactions*, vol. 88-A, pp. 239-246, 2005.

[12] M. Suzuki, T. Isshiki, and K. Tanaka, "Sanitizable signature with secret information", in *SCIS'06*, vol. 4A1-2, 2006, pp. 273.

[13] M. Klonowski and A. Lauks, "Extended sanitizable signatures", in *ICISC'06*, LNCS 4296, M.S. Rhee and B. Lee, Eds. Berlin: Springer-Verlag, 2006, pp. 343-355.

[14] K. Miyazaki, G. Hanaoka, and H. Imai, "Digitally signed document sanitizing scheme based on bilinear maps", in *ASIACCS'06*, New York: ACM, 2006, pp. 343-354.

[15] T. Izu, N. Kunihiro, K. Ohta, M. Takenaka, and T. Yoshioka, "A sanitizable signature scheme with aggregation", in *ISPEC'07*, LNCS 4464, E. Dawson and D.S. Wong, Eds. Berlin: Springer-Verlag, 2007, pp. 51-64.

[16] E.-C. Chang, C.L. Lim, and J. Xu, "Short sanitizable signatures for strings using random trees", Private Communication, 2007.

[17] T.H. Yuen, W. Susilo, J.K. Liu, and Y. Mu, "Sanitizable signatures revisited", in *CANS'08*, LNCS 5339, M. Franklin, Lucas C.K. Hui and D.S. Wong, Eds. Berlin: Springer-Verlag, 2008, pp. 80-97.

[18] S. Haber, Y. Hatano, Y. Honda, et al, "Efficient signature schemes supporting redaction, pseudonymization, and data deidentification", in *ASIACCS'08*, M. Abe and V. Gligor, Eds. New York: ACM, 2008, pp. 353-362.

[19] S. Canard, F. Laguillaumie, and M. Milhau, "Trapdoor sanitizable signatures and their application to content protection", in *ACNS'08*, LNCS 5037, S.M. Bellovin, R. Gennaro, A.D. Keromytis, and M. Yung, Eds. Berlin: Springer-Verlag, 2008, pp. 258-276.

[20] C. Brzuska, M. Fischlin, T. Freudenreich, et al, "Security of sanitizable signatures revisited", in *PKC'09*, LNCS 5443, S. Jarecki and G. Tsudik, Eds. Berlin: Springer-Verlag, 2009, pp. 317-336.

[21] S. Canard and A. Jambert, "On extended sanitizable signature schemes", in *CT-RSA'10*, LNCS 5985, J. Pieprzyk, Ed. Berlin: Springer-Verlag, 2010, pp. 179-194.

[22] S. Agrawal, S. Kumar, A. Shareef, and C. Pandu Rangan, "Sanitizable signatures with strong transparency in the standard model", Cryptology ePrint Archive, Report 2010/175. Available at http://eprint.iacr.org/2010/175.

[23] C. Brzuska, M. Fischlin, A. Lehmann, and D. Schroder, "Unlinkability of sanitizable signatures", in *PKC'10*, LNCS 6056, P.Q. Nguyen and D. Pointcheval, Eds. Berlin: Springer-Verlag, 2010, pp. 444-461.

[24] M. Bellare and P. Rogaway, "The exact security of digital signatures-how to sign with RSA and Rabin", in *EUROCRYPT'96*, LNCS 0950, U. M. Maurer, Ed. Berlin: Springer-Verlag, 1996, pp. 399-416.

[25] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited", in *STOC'98*, New York: ACM, 1998, pp. 209-218.

[26] R. Waters, "Efficient identity based encryption without random oracles", in *EUROCRYPT'05*, LNCS 3494, R. Cramer, Ed. Berlin: Springer-Verlag, 2005, pp. 114-127.

[27] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptively chosen message attacks", *SIAM Journal on Computing*, vol. 17, pp. 281-308, April 1998.

Yang Ming was born in Shaanxi Province, China in 1979. He received the B.S. and M.S. degrees in mathematics from Xi'an University of Technology in 2002 and 2005 respectively, the Ph.D. degree in cryptography from Xidian University in 2008. Currently he is a supervisor of postgraduate and assistant professor of Chang'an University. He is a member of Chinese Institute of Cryptography. His research interests include public key cryptography and information security.

Xiaoqin Shen was born in Hubei Province, China in 1981. She received the B.S. degrees in mathematics from Xi'an University of Technology in 2002 and Ph.D. degree in mathematics from Xi'an Jiaotong University in 2007. Currently she is a lecturer of Xi'an University of Technology. Her research interests include computational mathematics and probability.

Yamian Peng was born in Hebei Province, China in 1980. She received the B.S. and M.S. degrees in mathematics from Xi'an University of Technology in 2002 and 2005 respectively. Currently she is a lecturer of Hebei Polytechnic University. Her research interests include probability and applied mathematic.