A Short and Efficient Redactable Signature Based on RSA

Seongan Lim and Hyang-Sook Lee

The redactable signature scheme was introduced by Johnson and others in 2002 as a mechanism to support disclosing verifiable subdocuments of a signed document. In their paper, a redactable signature based on RSA was presented. In 2009, Nojima and others presented a redactable signature scheme based on RSA. Both schemes are very efficient in terms of storage. However, the schemes need mechanisms to share random prime numbers, which causes huge time consuming computation. Moreover, the public key in the scheme of Johnson and others is designed to be used only once. In this paper, we improve the computational efficiency of these schemes by eliminating the use of a random prime sharing mechanism while sustaining the storage efficiency of them. The size of our signature scheme is the same as that of the standard RSA signature scheme plus the size of the security parameter. In our scheme, the public key can be used multiple times, and more efficient key management than the scheme of Johnson and others is possible. We also prove that the security of our scheme is reduced to the security of the full domain RSA signature scheme.

Keywords: Public key cryptography, RSA, redactable signature.

Manuscript received Sept. 7, 2010; revised Dec. 27, 2010; accepted Jan. 21, 2011.

This work was supported by the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (20090093827).

Seongan Lim (phone: +82 2 3277 6993, email: seongannym@ewha.ac.kr) is with the Institute of Mathematical Sciences, Ewha Womans University, Seoul, Rep. of Korea.

Hyang-Sook Lee (email: hsl@ewha.ac.kr) is with the Department of Mathematics, Ewha Womans University, Seoul, Rep. of Korea.

doi:10.4218/etrij.11.0110.0530

I. Introduction

Digital signatures are designed to prevent the alteration of a signed digital document. For privacy concerns, it is desirable to release a signed document only after revising the sensitive content according to the privacy policy. One of the traditional methods of revising signed documents is blackening sensitive parts from the document. A treatment on a digitally signed document can be done similarly by using a redactable signature scheme. Differently from standard digital signatures, redactable signature schemes permit the deletion of arbitrary blocks of a signed document while preserving the authenticity of the remaining document, without any help from the signer. For this reason, redactable signatures are very attractive when publishing a signed document with sensitive information when the signer of the document is not accessible. In general, a redactable signature is used for documents with unspecific structure, such as bit strings [1]-[6]. Redactable signatures for structured documents are also considered to anonymize medical documents or general XML-documents as in [7], [8] to disclose verifiable partial information of signed clinical document architecture as in [9].

Rivest [10] introduced the notion of homomorphic signature schemes in a series of talks on two new signature schemes in 2000. In [4], Johnson and others formalized the definition of the homomorphic signature scheme and introduced the redactable signatures in the frame of homomorphic signatures. In the paper [4], Johnson and others presented a very short set homomorphic signature scheme based on RSA and a method to convert the set homomorphic signature to a redactable signature. However, their scheme needs a mechanism to share random primes, which causes huge time consuming computations. Recently, Nojima and others presented a

storage-efficient redactable signature based on RSA in [6]. The redactable signature of Nojima and others is based on any regular signature and it uses a mechanism to share random primes to redact message blocks and a hard-core predicate based on RSA to hide the redacted message blocks. Moreover, the redaction of a document in the redactable signature of Nojima and others is done bitwise.

In this paper, we present a short and efficient redactable signature scheme based on RSA. The security of our proposed scheme relies on the security of the full-domain RSA signature. The size of our signature scheme is the same as that of the standard RSA signature scheme plus the size of the security parameter. Our scheme does not need a mechanism to share random prime numbers; hence, our result improves the computational efficiency of the schemes based on RSA in [4], [6]. Moreover, our scheme is practical because it can be directly applied to existing security systems using RSA.

The rest of our paper is organized as follows. Section II provides formal descriptions of a redactable signature and its security model. We also discuss the efficiency of the known redactable signature schemes based on RSA. Section III proposes our redactable scheme based on RSA, and we analyze its security and efficiency. A conclusion is provided in section IV.

II. Redactable Signature Schemes

In this section, we recall the definition of a redactable signature. In subsection II.1, we reformalize the security of redactable signatures by focusing specifically on the operation 'redaction'. In subsection II.2, we review the redactable signature schemes based on RSA, and discuss efficiency problems with the scheme of Johnson and others.

In many redactable signature schemes, each redacted message block is represented by a special symbol, such as #. A redactable signature scheme has various requirements for the erased message block # upon its applications [1]-[9], [11]. In [4], it was noted that the explicit marking for each location of the redaction is necessary to thwart semantic attacks when the sizes of message blocks are small. We consider this type of redactable signature scheme.

Now we describe a few mathematical notations used in this paper.

Notations

- $\sum$: set of messages, that is, $\sum = \{0, 1\}^* \cup \{\#\}$
- M: a message in $\sum$
- $\mathcal{M}$: a document consists of one or more message blocks
- $\sum^t$: set of documents with t message blocks, that is, $\sum^t = \{\mathcal{M} \mid \mathcal{M} = M_1 \cdots M_t, \text{ where } M_i \in \sum\}$
- $\sum^*$: set of documents with arbitrary number of message blocks, that is, $\sum^* = \mathrm{U}_{t>0}(\sum^t)$
- $\preccurlyeq$: partial order defined on $\sum$ and $\sum^*$ with
  - for $M \in \sum$, we say $M' \preccurlyeq M$ if and only if either $M' = M$ or $M' = \#$.
  - for $\mathcal{M} = M_1 \ldots M_t$, $\mathcal{M}' = M'_1 \ldots M'_{t'}$, we say $\mathcal{M}' \preccurlyeq \mathcal{M}$ if and only if $t = t'$ and $M'_i \preccurlyeq M_i$ for all $i = 1, \ldots, t$.
- Trivial document: document with only #'s, that is, $\mathcal{M} = \#\#\cdots\#$
- Singleton document: document with only one non-# component, that is, $\mathcal{M} = \#\cdots\#M\#\cdots\#$.
- $r = a \bmod b$: r is the remainder on division of a by b with $0 \le r < b$.
- $\phi(N)$: number of positive integers relatively prime to N which is less than N; for example, $\phi(N) = (p-1)(q-1)$ for $N = pq$ with prime numbers p and q
- Safe prime p: p is a prime number of the form $p = 2u+1$ with a prime number u

We now provide a formal description of a redactable signature on a set of documents $\sum^*$.

Definition 1. A redactable signature scheme is defined as a tuple of polynomial algorithms (Setup, Sign, Redact, Verify) as follows:

- Setup($\{1\}^\lambda$): On input of a security parameter $\{1\}^\lambda$, it outputs a public key PK and a secret key SK.
- Sign(SK, t, $\mathcal{M}$): On input of a SK and a document $\mathcal{M} = M_1 M_2 \cdots M_t$ with t message blocks, it outputs a signature σ on $\mathcal{M}$.
- Redact(PK, t, $\mathcal{M}$, σ, $\mathcal{M}'$): On input of a PK, documents $\mathcal{M}$, $\mathcal{M}' \in \sum^t$ with $\mathcal{M}' \preccurlyeq \mathcal{M}$, and a valid signature σ on $\mathcal{M}$, it outputs a signature σ' on $\mathcal{M}'$. In this case, we say that $(\mathcal{M}', \sigma')$ is a redaction of $(\mathcal{M}, \sigma)$.
- Verify(PK, t, $\mathcal{M}$, σ): On input of a PK, a document $\mathcal{M} \in \sum^t$, and a signature σ, it outputs 0 (reject) or 1 (accept).

We require that the following should hold for all documents $\mathcal{M}$, $\mathcal{M}' \in \sum^t$ with $\mathcal{M}' \preccurlyeq \mathcal{M}$, and for a legal key pair (PK, SK):

(i) if $\sigma = \text{Sign}(SK, t, \mathcal{M})$, then Verify($PK$, t, $\mathcal{M}$, σ)=1.

(ii) if Verify(PK, t, $\mathcal{M}$, σ) = 1, and $\sigma' = \text{Redact}(PK, t, \mathcal{M}, \sigma, \mathcal{M}')$, then Verify($PK$, t, $\mathcal{M}'$, σ') = 1.

As defined, given a valid signature on $\mathcal{M} \in \sum^*$ of a redactable signature scheme, anyone can compute a valid signature for any document $\mathcal{W} \in \sum^*$ with $\mathcal{W} \preccurlyeq \mathcal{M}$, without any help from the signer.

1. Security of Redactable Signature Schemes

When compared with the standard digital signature scheme,

the redactable signature scheme requires two security features: the unforgeability of the signature except for the redacted signature and the confidentiality of erased message blocks. In [4], a security model of redactable signature was given in the frame of the homomorphic signature. Because a homomorphic signature is defined on a general binary (or unary) operation, the security model cannot use specific properties of the underlying operation. However, if we focus on the specific operation 'redaction' in the security model, the security model of redactable signature can be described in a simpler way.

A. Unforgeability

Unforgeability of the redactable signatures can be defined by using the following security game.

Definition 2. A redactable signature scheme Sig is secure against existential forgeries under a chosen-message attack if every adversary A wins the following game with a negligible probability after making at most q chosen signing queries on documents.

- Setup: The challenger of the security game sets key pairs (PK, SK), system parameters pp, and the number t of message blocks in documents to be queried/forged during the game and sends (PK, t, pp) to A.
- Queries: A adaptively sends signature queries for q documents $\mathcal{M}_j \in \sum^t$ with $j = 1,\ldots, q$ to the challenger.
- Sign: The challenger responds to the signature queries with valid signatures σ_j on $\mathcal{M}_j$ for $j = 1,\ldots, q$.
- Outputs: Finally, A outputs a singleton document $\mathcal{M}^* \in \sum^t$ and a valid signature σ^* on $\mathcal{M}^*$. Here, A wins if $(\mathcal{M}^*, \sigma^*)$ is not a redaction of any $(\mathcal{M}_j, \sigma_j)$ in the signature queries.

We note that the above security game considers the strong unforgeability of the redactable signature scheme. One can also formulate the unforgeability (not the strong unforgeability) of the redactable signature by defining the winning case for the adversary as

- A wins if $\mathcal{M}^*$ is not a redaction of any document $\mathcal{M}_j$ in the signature queries.

B. Privacy

The privacy requirement for the redactable signature is to guarantee the confidentiality of erased message blocks from a given redacted signature. The privacy of a redactable signature can be formalized, as with public key encryption, in terms of indistinguishability in the following way.

Definition 3. A redactable signature scheme Sig is said to be private if every adversary A wins the following game with a negligible probability.

- Setup: The challenger sets key pairs (PK, SK) for Sig and sends the PK to A.
- Submit: A chooses $\mathcal{M}_0$, $\mathcal{M}_1$, $\mathcal{M} \in \Sigma^t$ at random with $\mathcal{M} \preccurlyeq \mathcal{M}_b$ for $b = 0$, 1 and sends $\mathcal{M}_0$, $\mathcal{M}_1$, $\mathcal{M}$ to the challenger.
- Challenge: The challenger chooses $b \in \{0,1\}$ at random and computes
  - $\sigma_b = \mathrm{Sign}(SK, \mathcal{M}_b)$, and
  - $\tilde{\sigma}_b = \mathrm{Redact}(PK, \mathcal{M}_b, \sigma_b, \mathcal{M})$.

  The challenger sends $\tilde{\sigma}_b$ to A.
- Guess: A outputs $b' \in \{0,1\}$. Here, A wins if $b' = b$.

2. Efficiency of Some Redactable Signature Schemes Based on RSA

The efficiency of the redactable signature focuses on the sizes of signatures and the required computations. The redactable signature scheme on bitstrings in [4] employs a Merkle tree and a GGM tree, and the size of the redacted signature varies according to the number or the position of the redacted parts. A set homomorphic signature was presented in [4], and it can be transformed into a redactable signature by the method in [4]. This scheme is the shortest among known the redactable signature schemes although it suffers from heavy computations. Recently, Nojima and others presented a storage efficient redactable signature based on RSA in [6]. The scheme of Nojima and others also needs a mechanism to share random prime numbers. Moreover, the redaction of a document in the redactable signature of Nojima and others is done bitwise and the size of signature is $3|N|+|\mathcal{M}|$, where $|N|$ is the RSA modulus size and $|\mathcal{M}|$ is the bit-size of the document.

Our goal is to develop a practical redactable signature that is as short as the set homomorphic signature of Johnson and others but with improved computational efficiency. We review the redactable signature scheme based on the set-homomorphic signature in [4], which we denote Scheme JMSW.

Scheme JMSW:

- Setup($\{1\}^\lambda$): On input $\{1\}^\lambda$, the algorithm Setup generates an RSA modulus $N = pq$ with safe primes p and q and an element $v \in Z_N^*$ at random.

  It sets a function $h : \{0,1\}^* \to \{y \in Z \,|\, y \le N\}$ with
  - h outputs uniformly distributed odd prime numbers,
  - h extends to $H(U) = \prod_{x \in U} h(x)$ for any $U \subset \{0,1\}^*$.
  - It outputs a key pair (PK, SK) as follows:

    $$PK = (N, v, h), SK = \phi(N) = (p-1)(q-1).$$
- Sign(SK, t, $\mathcal{M}$): For a document $\mathcal{M} = M_1 \| \cdots \| M_t$ with $M_i \in \{0,1\}^*$ to be signed, the algorithm Sign
  - computes $\sigma = v^{H(U)^{-1} \bmod \phi(N)} \bmod N$ for the set $U = \{1\|M_1, 2\|M_2, \ldots, t\|M_t\}$, and
  - outputs σ as a signature on $\mathcal{M}$.

•Redact(PK, t, $\mathfrak{M}$, σ, $\mathfrak{M}'$): Suppose that documents $\mathfrak{M}=M_1\|M_2\|\cdots M_t$ and $\mathfrak{M}'=M'_1\|M'_2\|\cdots M'_t$ with $\mathfrak{M}'\preccurlyeq\mathfrak{M}$ and a signature σ on $\mathfrak{M}$ are given. The algorithm Redact
- computes $\sigma_{\text{redact}}=\sigma^{H(X)} \bmod N$ for the set $X=\{(i\|M_i)\,|\,M_i\neq\#\text{ and }\tilde{M}_i=\#\}$, and
- outputs σ_{redact} as a signature on $\mathfrak{M}'$.

•Verify(PK, t, $\mathfrak{M}$, σ): For a given document $\mathfrak{M}=M_1\|\cdots\|M_t$ and a signature σ on $\mathfrak{M}$, the algorithm Verify checks if $\sigma^{H(U)}=v \bmod N$ for the set $U=\{(i\|M_i)\,|\,M_i\neq\#\}$. It outputs "valid" if it passes and "invalid" otherwise.

First, Scheme JMSW uses a mechanism h to share random primes, and this requires the heaviest computation in the scheme. To date, there has been no method that could efficiently share random prime numbers.

The underlying signature scheme of the above signature scheme is the GHR Signature scheme [12], which introduced a suitable hashing family H and proposed the use of any function $h\in H$ in the GHR Signature scheme. Further, in [13], Coron and Naccache cryptanalyzed the security of using the suitable hashing family H in the GHR signature scheme and suggested the use of a hash function that outputs prime numbers by performing primality tests on the hash output until a prime number is obtained. In [4], Johnson and others did not specify h in their set-homomorphic signature scheme.

Hohenberger and Waters introduced a mechanism for sharing prime numbers as follows [14]. One chooses a random key K for a PRF function $F:\{0,1\}^*\rightarrow\{0,1\}^\lambda$ and a random $c\in\{0,1\}^\lambda$ and then defines a function $h_{K,c}(\cdot):\{0,1\}^*\rightarrow Z$ by

$$h_{K,c}(z)=F_K(i_z,z)\oplus c,$$

where $i_z(\geq 1)$ is the smallest index such that $F_K(i_z,z)\oplus c$ is an odd prime number. Thus, anyone can compute the same prime number $h_{K,c}(z)$ for any z by including K and c in the public information. However, computing the value $h_{K,c}(z)$ is a time consuming process. The main complexity to compute $h_{K,c}(z)$ is searching for the index i_z. As noted in [14], it is expected in $|N|$ primality tests which are estimated by $O(|N|^4)$ to compute $h_{K,c}(z)$ for a given z.

Second, modular exponentiations for redactors and verifiers in the Scheme JMSW involve heavy computations. To compute a redacted signature on $V\subset U$ from a signature σ on U, the redactor has to compute

$$H(U\setminus V)\prod_{x\in U\setminus V}h(x) \text{ and } \sigma^{H(U\setminus V)} \bmod N.$$

Because the redactor does not have any knowledge about $\phi(N)=(p-1)(q-1)$, the redactor has to compute $\sigma^{H(U\setminus V)} \bmod N$ for a very large integer exponent $H(U\setminus V)$. The computation for verifiers is similar to that for redactors. Moreover, the values $H(U\setminus V)$, $H(U)$, and $H(V)$ are message-dependent and cannot be precomputed.

Third, suppose that a valid signature $\sigma_{\mathfrak{W}}$ on a redacted document $\mathfrak{W}\in\sum^t$ is given. Then, for any document $\mathfrak{M}\in\sum^t$ with $\mathfrak{W}\preccurlyeq\mathfrak{M}$ and a valid signature $\sigma_{\mathfrak{M}}$, we note that

$$\text{Redact}(PK, t, \mathfrak{M}, \sigma_{\mathfrak{M}}, \mathfrak{W})=\sigma_{\mathfrak{W}}.$$

This fact assumes that the PK in the Scheme JMSW is designed to be used only once. This problem occurs because $v\in Z_N^*$ is fixed in the Setup phase. A simple way to solve this problem is to generate a fresh $v\in Z_N^*$ in the Sign phase and include $v\in Z_N^*$ in the signature in an authentic manner. For example, the redactable signature on a set U can be

$$(V^{H(U)^{-1} \bmod \phi(N)}, \text{Sig}_0(v)),$$

where Sig_0 is a secure standard signature scheme.

It would be desirable to develop a redactable signature scheme based on RSA which does not require a mechanism to share random prime numbers and supports the multiple use of a public key while sustaining the storage efficiency of Scheme JMSW. We present our scheme in the following section.

III. New Redactable Signature Scheme Based on RSA

In subsection III.1, we present Scheme 1: a short and efficient redactable signature based on RSA. In order to give security analysis of Scheme 1, we introduce the notion of 'Equivalent Redactable Signature' in subsection III.2. In subsection III.3, we present Scheme 2: a redactable signature equivalent to Scheme 1. In subsection III.4, we prove that the existential unforgeability and privacy of Scheme 2, which implies that Scheme 1 is an existentially unforgeable and private redactable signature scheme. In subsection III.5, we compare the efficiency of Scheme 1 with Scheme JMSW.

1. Scheme 1: Redactable Signature Scheme with Short Size

We assume that the number of message blocks in a document is always smaller than the positive integer T, and the T smallest odd prime numbers $e_1, e_2, \ldots, e_T$, (with $e_i<e_{i+1}$) are publicly known to the users of the system. We also assume that $H(\cdot)\neq 1$ for a cryptographically secure hash function $H:\{0,1\}^*\rightarrow Z_N^*$. In fact, the randomness r is included in the input of H in our scheme; therefore, one can refresh r if a computed hash value is 1 for the chosen r, although the possibility is very low. We describe our proposed Scheme 1 as follows.

Scheme 1:

•Setup($\{1\}^\lambda$): The Setup algorithm takes $\{1\}^\lambda$ as input. It generates an RSA modulus $N=pq$ with safe primes p and

q and sets a cryptographically secure full domain hash function $H: \{0,1\}^* \rightarrow Z_N^*$. It outputs a key pair (PK, SK) as

$$PK = (N, H),\ SK = \phi(N) = (p-1)(q-1).$$

•Sign(SK, t, $\mathcal{M}$): For a document $\mathcal{M}=M_1\|M_2\|\cdots M_t$ with $M_i \in \{0,1\}^*$ to be signed, the algorithm Sign

(i) computes $d_i = (e_i)^{-1} \bmod \phi(N)$ for $i = 1,\ldots,t$,

(ii) chooses $r \in \{0,1\}^{\lambda}$ at random,

(iii) computes $m_i = H(i\|M_i\|r)$ for $i = 1,\ldots,t$, and

(iv) outputs a signature $\sigma_{\mathcal{M}} = (\sigma, r)$ on $\mathcal{M}$, where

$$\sigma = m_1^{d_1} m_2^{d_2} \ldots m_t^{d_t} \bmod N.$$

•Redact(PK, t, $\mathcal{M}$, $\sigma_{\mathcal{M}}$, $\mathcal{M}'$): Suppose that documents $\mathcal{M}=M_1\|M_2\|\cdots M_t$, $\mathcal{M}'=M'_1\|M'_2\|\cdots M'_t$ with $\mathcal{M}' \preccurlyeq \mathcal{M}$, and a signature $\sigma_{\mathcal{M}} = (\sigma, r)$ on $\mathcal{M}$ are given. For the following set of indices,

$$V = \{i \mid M_i \neq \#, \tilde{M}_i = \#\}, U = \{i \mid \tilde{M}_i = \#\},$$

the algorithm Redact

(i) computes $v = \prod_{i \in V} e_i$ and $u = \prod_{i \in U} e_i$,

(ii) computes, for $i \in V$,

$$m_i = H(i\|M_i\|r), u_i = \frac{u}{e_i}, \quad \text{and}$$

(iii) outputs a signature $\sigma_{\mathcal{M}'} = (\sigma', r)$ on $\mathcal{M}'$ with

$$\sigma' = \frac{\sigma^V}{\prod_{i \in V} m_i^{u_i}} \bmod N.$$

•Verify(PK, t, $\mathcal{M}$, σ): For a given document $\mathcal{M} = M_1\|M_2\|\cdots M_t$, with $I_M = \{ i \mid M_i \neq \#\}$ and a signature σ on $\mathcal{M}$, the algorithm Verify computes

(i) $e'_i = \frac{e_1 \ldots e_i \ldots e_t}{e_i} \in Z$, $v = \prod_{i \in I_M} e_i$, and

(ii) $m_i = H(i\|M_i\|r)$ for $i \in I_M$.

The algorithm tests if $= \prod_{i \in I_M} m_i^{e'_i} \bmod N$.

It outputs "valid" if it passes and "invalid" otherwise.

2. Equivalent Redactable Signatures

We now define the notion of equivalent redactable signatures.

Definition 4. Two redactable signature schemes $\{(\text{Setup}_i, \text{Sign}_i, \text{Redact}_i, \text{Verify}_i)\}_{i=0,1}$ are said to be equivalent if they have the same Setup_i algorithms and anyone can compute $\sigma_j = \text{Sign}_j(SK, t, \mathcal{M})$ from $\sigma_{1-j} = \text{Sign}_{1-j}(SK, t, \mathcal{M})$, $j = 0, 1$ without knowing the SK, and vice versa.

It is clear that the two equivalent redactable signatures have the same security level because the difference appears only in their representations.

We now show that the following three signing functions define equivalent redactable signatures. For a given document $\mathcal{M} = M_1\|M_2\|\cdots M_t$, for $i = 1$ to t, we set $m_i = H(i\|M_i\|r)$ with randomly chosen r. We now consider the signing functions defined as

$$\text{Sign}_1(SK, t, \mathcal{M}) = (m_1^{d_1} m_2^{d_2} \ldots m_t^{d_t} \bmod N, r),$$
$$\text{Sign}_2(SK, t, \mathcal{M}) = (m_1^{d_1} \bmod N, \ldots, m_t^{d_t} \bmod N, r),$$
$$\text{Sign}_3(SK, t, \mathcal{M}) = (m_1^{e'_1 d_1} \bmod N, \ldots, m_t^{e'_t d_t} \bmod N, r),$$

$$\text{with } e'_i = \frac{e_1 \cdots e_i \cdots e_t}{e_i} \in Z.$$

Theorem 1. Redactable signature schemes with signing functions Sign_1 and Sign_2 are equivalent.

Proof. Theorem 1 can be proven by demonstrating the following implications:

$$\text{Sign}_1 \Rightarrow \text{Sign}_3 \Rightarrow \text{Sign}_2 \Rightarrow \text{Sign}_1.$$

First, we show that one can compute a Sign_3-signature on M from a given Sign_1-signature on $\mathcal{M}$. The equality $e_i \cdot d_i = 1 \bmod \phi(N)$ implies that

$$m_i^{e'_i d_i} = \frac{(m_1^{d_1} m_2^{d_2} \cdots m_t^{d_t})^{e'_i}}{\prod_{j \neq i} m_j^{e'_{ij}}} \bmod N,$$

where $e'_{ij} = \frac{e_1 e_2 \cdots e_t}{e_i e_j}$ for all $i = 1$ to t. Because $e_1, \cdots, e_t$ are publicly known, $m_i^{e'_i d_i}$ can be computed from $\text{Sign}_1(SK, t, \mathcal{M})$ without knowing d_i for all $1 \leq i \leq t$. Therefore, the signature $\text{Sign}_3(SK, t, \mathcal{M})$ can be computed from the signature $\text{Sign}_1(SK, t, \mathcal{M})$.

Second, we show that one can compute a Sign_2-signature on $\mathcal{M}$ from a given Sign_3-signature on $\mathcal{M}$. Because $\gcd(e'_i, e_i)=1$, one can compute integers s_i and t_i with $s_i e_i + t_i e'_i = 1$ by the extended Euclidean algorithm. Note that the integers s_i and t_i can be considered to be public information because e'_i and e_i are publicly known. Thus, for all $i = 1$ to t, $m^{d_i} = (m^{s_i e_i + t_i e'_i})^{d_i} = m^{s_i} \cdot (m^{e'_i d_i})^{t_i} \bmod N$, that is, anyone can compute $(m^{d_i} \bmod N)$ from $(m^{e'_i d_i}) \bmod N$. Hence, the signature $\text{Sign}_2(SK, t, \mathcal{M})$ can be computed from the signature $\text{Sign}_3(SK, t, \mathcal{M})$.

Finally, we show that one can compute a Sign_1-signature on $\mathcal{M}$ from a given Sign_2-signature on $\mathcal{M}$. This is clear because Sign_1-signature on $\mathcal{M}$ is an aggregation of all components of given Sign_2-signature on $\mathcal{M}$ except for the last component. □

3. Scheme 2: Lengthy Representation of Scheme 1

Now we describe Scheme 1 as a representation of the signing function Sign_2. For notational convenience, we call the corresponding scheme Scheme 2. The description for Scheme 2 can be given as follows.

Scheme 2:

•Setup($\{1\}^\lambda$): The Setup algorithm takes $\{1\}^\lambda$ as input. It generates an RSA modulus $N = pq$ with safe primes p and q and sets a cryptographically secure full domain hash function $H : \{0,1\}^* \rightarrow Z_N^*$. It outputs a key pair (PK, SK) by

$$PK = (N, H), \quad SK = \phi(N) = (p-1)(q-1).$$

•Sign(SK, t, $\mathcal{M}$): For a document $\mathcal{M}=M_1\|M_2\|\cdots$, M_t with $M_i \in \{0,1\}^*$ to be signed, the algorithm Sign

(i) computes $d_i = (e_i)^{-1} \bmod \phi(N)$ for $i = 1,\ldots, t$,

(ii) chooses $r \in \{0,1\}^\lambda$ at random,

(iii) computes $m_i = H(i\|M_i\|r)$ for $i = 1,\ldots,t$, and

(iv) outputs a signature $\sigma_{\mathcal{M}} = (\sigma, \mathrm{r})$ on $\mathcal{M}$, where

$$\sigma = (m_1^{d_1} \bmod N, \ldots, m_t^{d_t} \bmod N) = (\sigma_1\sigma_2, \ldots, \sigma_t).$$

•Redact(PK, t, $\mathcal{M}$, σ, $\mathcal{M}'$): Suppose that documents $\mathcal{M}=M_1\|M_2\|\cdots M_t$, $\mathcal{M}'=M'_1\|M'_2\|\cdots M'_t$ with $\mathcal{M}' \preccurlyeq \mathcal{M}$, and a signature on $\mathcal{M}$ are given. We denote $I_{M'} = \{i \mid M'_i \neq \#\}$. The algorithm Redact eliminates the components from σ that correspond to the redacted portion in $\mathcal{M}'$, and obtain

$$\sigma_{\text{redact}} = (\sigma_i)_{i \in I_{M'}},$$

where the order of indices i's is increasing. It outputs the signature $\sigma_{\mathcal{M}'} = (\sigma_{\text{redact}}, r)$ on $\mathcal{M}'$.

•Verify(PK, t, $\mathcal{M}$, σ): For a given document $\mathcal{M} = M_1\|M_2\|\cdots M_t$, with $I_{\mathcal{M}} = \{i \mid M_i \neq \#\}$ and a signature σ on $\mathcal{M}$, the algorithm Verify

(i) computes $m_i = H(i\|M_i\|r)$ for $i \in I_{\mathcal{M}}$,

(ii) tests whether for $(\sigma_i)^{e_i} = m_i \bmod N$ for $i \in I_{\mathcal{M}}$, and

(iii) outputs "valid" if it passes for all $i \in I_{\mathcal{M}}$ and "invalid" otherwise.

4. Security Analysis

This section presents a security proof for Scheme 2 which provides a security proof for Scheme 1 due to the equivalence of Scheme 1 and Scheme 2.

A. Unforgeability

First, we show that Scheme 2 is existentially unforgeable under chosen-message attack as a redactable signature scheme.

We denote RSA_i as the full-domain RSA signature scheme with $pk_i = (N, e_i)$, $sk_i = d_i$ for $i = 1$ to t. It was proven that the full-domain RSA signature scheme is existentially unforgeable under an adaptive chosen-message attack in the random oracle model [15]. Therefore, the full-domain RSA signatures RSA_i for all i are existentially unforgeable under an adaptive chosen-message attack in the Random Oracle Model.

Theorem 2. Scheme 2 is existentially unforgeable under a chosen-message attack as a redactable signature if the full-domain RSA signature RSA_i is existentially unforgeable under a chosen message attack as the standard signature for all $i = 1$ to t.

Proof. We prove the theorem by contraposition. Suppose that there exists a successful adversary A launching a chosen-message attack on Scheme 2. We construct a successful adversary B launching a chosen-message attack on RSA_i for some $i = 1,\ldots, t$. Suppose that $(pk_i = (N, e_i))_{1 \le i \le t}$ is given to B. Then B simulates the challenger in the following security game against A.

•Setup: B sets $PK = N$ and $pp = \{p_1, p_2, \ldots, p_t\}$ and sends (PK, t, pp) to A. Note that pp can be assumed as publicly accessible information.

•Queries: Then A sends q signature queries for documents $\mathcal{M}_j \in \Sigma^t$ with $j = 1,\ldots,q$ to B.

•Sign: Upon a signature query for $\mathcal{M}_j = M_{j1}\| \cdots \|M_{jt}$, B does the following.

- B chooses r_j at random and computes $M'_{ji} = i\|M_{ji}\|r_j$ for $i = 1$ to t.
- B sends M'_{ji} as a signature query to the challenger in the security game against RSA_i.
- When B receives σ_{ji} from RSA_i, for $i=1,\ldots,t$ and $j = 1,\ldots,q$, B responds to A with $\sigma_j = (\sigma_{j1}, \sigma_{j2},\ldots,\sigma_{jt}, r_j)$ as a redactable signature on $\mathcal{M}_j$ for $j = 1,\ldots,q$.

•Outputs: Finally, A outputs a singleton document $\mathcal{M}^* \in \Sigma^t$ that is not a redaction of any documents in the signature query with a valid signature (σ^*, r^*) on $\mathcal{M}^*$.

From the forged signature σ^* on the singleton document $\mathcal{M}^* = (M^*_i)_{1 \le i \le t}$, we assume that $M^*_k \neq \#$ for some k and $\sigma^* = \sigma^*_k$. From the validity of the signature, we see that

$$(\sigma_k^*)^{e_k} = H(k \| M_k^* \| r^*).$$

Thus σ_k^* is a valid RSA_k-signature on $(k \| M_k^* \| r^*)$. There are two possible cases.

Case 1: r^* was never used in the signature queries.

Case 2: r^* was used in the signature queries.

We note that the signature query to the challenger of RSA_k in the above security game has the form of $(k||M_{jk}||r_j)$ where $\mathcal{M}_j = M_{j1}|| \cdots ||M_{jt}$, for $j = 1,\ldots,q$, is a document in the signature query of Scheme 2 from the adversary A.

In case 1, $(k||M^*_k||r^*)$ was never included in the signature query to the challenger of RSA_k because $r^* \neq r_j$ for any $j = 1,\ldots,q$. We now consider case 2, and assume that $r^* = r_j$ for some $j = 1,\ldots,q$. If $M^*_k = M_{jk}$, then we clearly have

$$\mathcal{M}^* \preccurlyeq \mathcal{M}_j, \text{ and } \sigma^*_k = \text{Redact}(PK, t, \mathcal{M}_j, \sigma_j, \mathcal{M}^*).$$

This means that σ^*_k is not a forged signature of Scheme 2 as a redactable signature. Thus, $M^*_k \neq M_{jk}$ for any j, if $r^* = r_j$ in case 2. Therefore, in both cases, $(k||M^*_k||r^*)$ was never included in the signature query to the challenger of RSA_k, and we conclude that

the signature σ^*_k on $(k||M^*_k||r^*)$ is a forged signature of RSA_k under a chosen-message attack. This contradicts to the unforgeability of the full-domain RSA signature scheme RSA_k. □

Theorem 2 and Theorem 1 imply that Scheme 1 is existentially unforgeable under the chosen-message attack as a redactable signature scheme.

B. Privacy

We now show that Scheme 2 satisfies the privacy requirement of the redactable signature scheme. For any given $\mathfrak{M}_0$, $\mathfrak{M}_1$, $\mathfrak{M} \in \Sigma'$ with $\mathfrak{M} \preccurlyeq \mathfrak{M}_0$ and $\mathfrak{M} \preccurlyeq \mathfrak{M}_1$, let S_b be the set of all valid redacted signature for $\mathfrak{M}=M_1||M_2||\cdots M_t$ from the signatures on $\mathfrak{M}_b$ for $b \in \{0, 1\}$, that is,

$$S_b = \left\{ \left(\{ \left[H(i \,||\, M_i \,||\, r_b) \right]^{d_i} \}_{i \in I_M}, r_b \right) \,|\, r_b \in \{0,1\}^{\lambda} \right\},$$

where $I_M = \{i \,|\, M \neq \#\}$.

It is clear that $S_0 = S_1$. This implies that there is no information on b for randomly chosen element from S_b. Hence, Scheme 2 satisfies the privacy requirement. Again, we see that Scheme 1 satisfies the privacy requirement by Theorem 1.

5. Efficiency Analysis

The size of the signature in Scheme 1 is $|N|+\lambda$, and to the authors' knowledge, this is the shortest among redactable signature schemes that support multiple use of the public key. The size of signature in Scheme JMSW is $|N|$, but the scheme does not support multiple use of the public key. When we modify Scheme JMSW so that it supports multiple use of the public key, the signature size increases to $3|N|$.

Scheme JMSW uses a mechanism for sharing random prime numbers that causes heavy computational overhead. Moreover, the computation of random prime numbers is dependent on the message, and it cannot be precomputed.

Table 1 presents the number of operations required in Scheme JMSW and Scheme 1. We denote λ as the security parameter size, t as the total number of message blocks of the document, α as the number of redacted message blocks, and β as the number of remaining message blocks.

The most efficient mechanism [14] of sharing a random prime number has the complexity $O(|N|^4)$ as explained in subsection II.2 of this paper. It is noteworthy that the complexity of multiplication in Z_N is estimated as $O(|N|^2)$, and the complexity of an exponentiation in Z_N is estimated as $O(|k||N|^2)$, where k is the exponent in the exponentiation [16].

The modular exponentiations in Table 1 have diferent sizes of exponents. The complexities of modular exp_0, exp_1, exp_2, and exp_3 are estimated as in Table 2.

Table 1. Operations.

	Scheme 1	Scheme JMSW
Sign	$(2t-1)$ mul t exp_0	t prime share t mul 1 exp_0
Redact	α mul $(\alpha+1)$ exp_1	α prime share 1 exp_2
Verify	β mul $(\beta+1)$ exp_1	β prime share 1 exp_3

Table 2. Complexity of the exp_i.

Operations	Complexity
exp_0	$O(\|N\|^3)$
exp_1	$O(\mu_t\|N\|^2)$, where $\mu_t=(\sum_{1\le i\le t}\|e_i\|)$
exp_2	$O(\alpha\,\|N\|^3)$
exp_3	$O(\beta\,\|N\|^3)$

Table 3. Comparison of average complexity.

	Scheme 1	Scheme JMSW
Sign	$(t\|N\|+2t-1)\|N\|^2$	$(t\|N\|^2+\|N\|+t)\,\|N\|^2$
Redact	$(\alpha-1+\mu_t(\alpha+1))\,\|N\|^2$	$\alpha\,(\|N\|+\|N\|^2)\,\|N\|^2$
Verify	$(\beta-1+\mu_t(\beta+1))\,\|N\|^2$	$\beta\,(\|N\|+\|N\|^2)\,\|N\|^2$

Table 4. Values for μ_t.

t	500	600	700	800	900	1,000
μ_t	5,311	6,548	7,848	9,148	10,448	11,748

Because the computational overhead for prime sharing is a dominant factor of the overall computations, Scheme 1 is much more efficient than Scheme JMSW. Table 3 represents a comparison of average computational complexity of each algorithm.

The Sign algorithm of Scheme 1 is about $|N|$ times faster than that of Scheme JMSW. For the algorithm Redact, Scheme 1 is at least $[\alpha(|N|+|N|^2)]/[2(\mu_t-1)]$ times faster than that of Scheme JMSW. For the algorithm Verify, Scheme 1 is at least $[\beta(|N|+|N|^2)]/[2(\mu_t-1)]$ times faster than that of Scheme JMSW. We note that the value μ_t is much smaller than $|N|^2$ because we take the smallest odd prime e_i's in Scheme 1 (see Table 4).

For $t = 1{,}000$, if $\alpha > 2$, then the Redact algorithm of Scheme 1 is at least 100 times faster than Scheme JMSW. As t gets smaller or α gets larger, the ratio becomes larger. It is similar for the Verify algorithm.

IV. Conclusion

This paper proposed Scheme 1, a short and efficient

redactable signature scheme based on RSA signature. Previously, the shortest known redactable signature scheme based on RSA was Scheme JMSW [4]. However, Scheme JMSW uses a message dependent mechanism for sharing random prime numbers, and it causes the need for heavy computations. Moreover, Scheme JMSW does not support multiple use of the public key. Our scheme does not need a mechanism of sharing random prime numbers and preserves the efficient signature size of the Scheme JMSW. Our scheme represents the first practical redactable signature scheme based on the RSA signature scheme. The proposed scheme can be readily and widely applied to most existing IT services and systems for enhanced privacy.

References

[1] K. Miyazaki, G. Hanaoka, and H. Imai, "Digitally Signed Document Sanitizing Scheme Based on Bilinear Maps," *ASIACCS,* 2006, pp. 343-354.

[2] K. Miyazaki et al., "Digitally Signed Document Sanitizing Scheme with Disclosure Condition Control," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. 88, no.1, 2005, pp. 239-246.

[3] E. Chang, C. Lim, and J. Xu, "Short Redactable Signatures Using Random Trees," *CT-RSA*, *LNCS*, vol. 5473, 2009, pp.133-147.

[4] R. Johnson et al., "Homomorphic Signature Schemes," *CT-RSA*, *LNCS*, vol. 2271, 2002, pp. 244-262.

[5] S. Haber et al., "Efficient Signature Schemes Supporting Redaction, Pseudonymization and Data Deidentification," *ASIACCAS*, 2008, pp. 353-362.

[6] R. Nojima et al., "A Storage Efficient Redactable Signature in the Standard Model," *ISC, LNCS* 5735, 2009, pp. 326-337.

[7] D. Slamanig and S. Rass, "Generalizations and Extensions of Redactable Signatures with Applications to Electronic Healthcare," *CMS*, *LNCS*, vol. 6109, 2010, pp. 201-213.

[8] C. Brzuska et al., "Redactable Signature for Tree-Structured Data: Definitions and Constructions,"*ACNS*, *LNCS*, vol. 6123, 2010, pp. 87-104.

[9] D. Slamanig and C. Stingl, "Disclosing Verifiable Partial Information of Signed CDA Documents Using Generalized Redactable Signatures," *Healthcom*, 2009, pp.146-152.

[10] R. Rivest, "Two New Signature Schemes," Presented at Cambridge seminar, 2001.

[11] G. Ateniese et al., "Sanitizable Signatures," *Esorics*, 2005, pp. 159-177.

[12] R. Gennaro, S. Halevi, and T. Rabin, "Secure Hash-and-Sign Signatures without the Random Oracle," *Eurocrypt*, *LNCS*, vol. 1592, 1999, pp. 123-139.

[13] J. Coron and D. Naccache, "Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme," *Eurocrypt*, *LNCS*, vol. 1807, 2000, pp. 91-101.

[14] S. Hohenberger and B. Waters, "Short and Stateless Signatures from the RSA Assumption,"*Crypto*, *LNCS*, vol. 5677, 2009, pp. 654-670.

[15] Jean-Sebastien Coron, "On the Exact Security of Full Domain Hash,"*Crypto*, *LNCS*, vol. 1880, 2000, pp. 229-235.

[16] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

Seongan Lim received her PhD in mathematics from Purdue University. She is a research professor at Ewha Womans University, Seoul, Rep. of Korea. Her research interests include public key cryptography and privacy preserving mechanisms in IT services.

Hyang-Sook Lee is a professor at the Department of Mathematics, Ewha Womans University, Seoul, Rep. of Korea. She received the PhD from Northwestern University in 1993. Her research interests are pairing based cryptography, especially pairing computations, constructing pairing friendly curves, digital signatures, and PKC. She is currently a Division Director of Natural Sciences of the National Research Foundation of Korea.