Efficient Signature Schemes from R-LWE

Ting Wang[1,2], Jianping Yu[1], Peng Zhang[1] and Yong Zhang[1]*
[1] ATR Key Laboratory of National Defense Technology, Shenzhen University
Shenzhen, 518060, China
[e-mail: wangt809@163.com, yzhang@szu.edu.cn]
[2] School of Computer Science and Engineering , South China University of Technology
Guangzhou 510006, China
*Corresponding author: Yong Zhang

Received July 17, 2015; revised June 14, 2016; accepted July 3, 2016; published August 31, 2016

Abstract

Compared to the classical cryptography, lattice-based cryptography is more secure, flexible and simple, and it is believed to be secure against quantum computers. In this paper, an efficient signature scheme is proposed from the ring learning with errors (R-LWE), which avoids sampling from discrete Gaussians and has the characteristics of the much simpler description etc. Then, the scheme is implemented in C/C++ and makes a comparison with the RSA signature scheme in detail. Additionally, a linearly homomorphic signature scheme without trapdoor is proposed from the R-LWE assumption. The security of the above two schemes are reducible to the worst-case hardness of shortest vectors on ideal lattices. The security analyses indicate the proposed schemes are unforgeable under chosen message attack model, and the efficiency analyses also show that the above schemes are much more efficient than other correlative signature schemes.

Keywords: Signature, R-LWE, linearly homomorphic, lattice

This work is supported by the National Natural Science Foundation of China (61171072) and the Science & Technology Plan Projects of Shenzhen (ZDSYS20140430164957660, JCYJ20150324141711562, JCYJ20150324141711665, JCYJ20150324140036830, 20160224144857159)

http://dx.doi.org/10.3837/tiis.2016.08.026 **ISSN : 1976-7277**

1. Introduction

Digital signature is one of the most important and widely used cryptographic primitives. At present all signature schemes from classical cryptography were proved to be either insecure or function-limited especially under quantum attacks [1-3], so lattice-based cryptography has become a hot research topic because of its security. Since new trapdoors for hard lattices were developed successfully [4], many lattice-based signature schemes have been proposed owing to the excellent algebraic characteristic, implementation simplicity, stronger security proofs of the lattice cryptography [5-7].

Homomorphic signature is intriguing because which has been proved to be well-suited to guarantee information security in message-operated scenario, such as network coding, sensor networks and cloud storage etc [1, 8-12]. Homomorphic signature can sign n-dimensional vectors $v_1,\cdots,v_l$ from a message space $\mathcal{M}$ and outputs the signature σ_i of every vector v_i. Given these signatures, the homomorphic property of signature scheme is that anyone can evaluate a signature on the vector $v = f(v_1,\cdots,v_l)$ in $\mathcal{M}$.

Homomorphic signature schemes were first given by Micali and Rivest for undirected graphs [13]. Subsequently Johnson proposed the basic definitions of homomorphic signature scheme and showed that a variety of homomorphic signature schemes can be designed [14]. The signature scheme from [5] was the first linear homomorphic scheme that authenticated vectors from binary fields, and its security was based on a new lattice problem, which is named $k-SIS$. Based on the trapdoor functions with preimage sampling [4] and a homomorphic hash function family, WANG FengHe gave a linely homomorphic signature scheme over binary field [15]. Using ideal lattices, Boneh et al presented the first homomorphic signature scheme for polynomial functions [6], and then Catalano, Fiore and Warinschi provided an alternative to the homomorphic signature scheme of Boneh and Freeman [16]. All of the above homomorphic signature schemes have their corresponding advantages and application scenes, the more detailed descriptions are shown in **Table 1**. However, they tend to be inefficient for practical applications.

Table 1. The properties of the current homomorphic signature schemes

Scheme	Techniques	Assumption	Limitations
[5]	preimage sampling functions (PSF)	k-SIS	The construction is inefficient for basing on PSF and Bonsai primitives
[6]	The intersection method, PSF	Ideal-SVP	Not leak information for linear functions but is unknown for higher degree polynomials.
[15]	PSF, linear homomorphic hash function	SIS	The construction is based on PSF
[16]	Leveled multilinear maps, graded encodings	APMDH	Insecure under quantum attacks

In order to resolve the efficiency problem, unlike GPV08 scheme that needs to generate a trapdoor and sample from discrete Gaussians, we give a more efficient signature scheme from the ring learning with errors (R-LWE) using the idea from Lyubashevsky [17]. Subsequently, based on the work of WANG FengHe, a more efficient linearly homomorphic signature scheme without trapdoor on signed data is presented in this paper. Because of the much more compact algebraic structure of the R-LWE problem, the efficiency of the proposed signature

schemes is improved greatly, and the analyses show that schemes are secure in adaptive chosen message attack model, assuming that it is hard for probabilistic polynomial-time even quantum adversary to resolve the shortest vector problem on ideal lattices.

The remainder of this paper is arranged as follows. In Section 2, the preliminaries are introduced firstly, and then a general lattice-based signature scheme is given and discussed in detail in Section 3. In Section 4, the definition of homomorphic signature is expounded firstly. Secondly, we propose an efficient linearly homomorphic signature scheme from R-LWE assumption. Finally, the security and the efficiency are analyzed in this Section. The whole paper is concluded in Section 5.

2. Preliminaries

2.1 Lattices

Lattice can be regarded as the set of discrete points with a regular structure in geometry, which can be described formally as follows.

Definition 1. Suppose that $b_1,\cdots,b_n \in R^n$ are linearly independent n-dimensional vectors, then the lattice can be defined as

$$L(b_1,...,b_n)=\left\{\sum_{i=1}^{n} x_i b_i \mid x_i \in Z, 1\le i\le n\right\} \tag{1}$$

Where $b_1,\cdots,b_n$ is a basis of the lattice, and its rank is n.

The standard worst-case approximation lattice problem $GapSVP_\gamma$ is given in the decision version.

Definition 2 (Shortest Vector Problem). Given a lattice basis B, $d \in R$. If $\lambda_1(L(B)) \le d$, it is a YES instance. If $\lambda_1(L(B)) > \gamma(n)\cdot d$, it is a NO instance, where the parameter $\gamma(n)\ge 1$ is a approximation factor and $\lambda_1(L(B))$ is the minimum distance of a lattice $L(B)$.

2.2 Learning with Errors over Rings (R-LWE)

Let $f(x)=x^n+1 \in Z[x]$, where $n=2^k (k\in Z)$ is a security parameter, which makes $f(x)$ irreducible over the rational number field, $R=Z[x]/<f(x)>$ be the integer polynomial ring modulo $f(x)$, and assume that $q=1 \bmod 2n$ is a large prime modulus (bounded by poly(n)), $R_q=R/<q>=Z_q[x]/<f(x)>$ is the integer polynomial ring modulo $f(x)$ and q. It is obvious that the elements of R_q are typically represented by integer polynomials of degree less than n, and its coefficients are chosen from $\{0,1,\cdots,q-1\}$.

In the integer polynomial ring R_q, the R-LWE problem can be defined as follows [18]. For a uniformly random $s \in R_q$ (secret key), define two distributions on $R_q \times R_q$: (1) $(a, b=a\times s+e) \in R_q \times R_q$, where a is chosen uniformly at random from R_q, and e is an independent error term from the distribution $\chi \subset R$. (2) (a,c), where $a, c \leftarrow R_q$ are uniformly random. The R-LWE problem is to distinguish the two distributions described above with non-negligible advantage. In other words, if R-LWE is hard, then the independent

samples of 'random noise equations' $(a, a \times s + e)$ is pseudorandom, and all operations are performed in R_q.

Lyubashevsky, Peikert and Regev proved that the R-LWE problem is hard under the worst-case assumptions on ideal lattices [18] (see Theorem 1).

Theorem 1. For a approximation factor $\gamma \geq 1$(bounded by a fixed poly(n)), assume that it is hard for any polynomial-time even quantum algorithms to find an approximation of the shortest vector on ideal lattices. Then any poly(n) independent samples $(a_i, a_i \times s + e_i)$ from the R-LWE distribution $A_{s,\chi} \subset R_q \times R_q$ are pseudorandom.

2.3 A Hash Function Family

Lyubashevsky et al. [19] defined a hash function family $\mathcal{H}_{Z_q,n}$ that maps Z_q^n to Z_q. The function $h \in \mathcal{H}_{Z_q,n}$ is indexed by a certain fixed vector $\alpha = (a_1, \cdots, a_n) \in Z_q^n$. h takes as input an element $\beta = (b_1, \cdots, b_n) \in Z_q^n$, and the output is the dot product as $<\alpha, \beta>= a_1 b_1 + \cdots + a_n b_n$. It is denoted by $h_\alpha(\beta) =< \alpha, \beta >$. The hardness of the hash function is based on the approximate worst-case lattice problems, and the hash function is a collision resistant hash.

$\mathcal{H}_{Z_q,n}$ is a linear hash function family. That is to say, for every $\beta, \gamma \in Z_q^n$, $k \in Z_q$ and $h_\alpha \in H_{Z_q,n}$, the following two properties are satisfied:

$$\text{(i)} \quad h_\alpha(\beta + \gamma) = h_\alpha(\beta) + h_\alpha(\gamma) \tag{2}$$

$$\text{(ii)} \quad h_\alpha(k\beta) = k h_\alpha(\beta) \tag{3}$$

3. Signature Scheme

3.1 The Proposed Scheme

First we give the probability distribution χ which will be used in the following, and χ is derived from a Gaussian. For any $\beta > 0$, the density function of a Gaussian distribution over the real domain is given by $D_\beta(x) = 1/\beta \cdot \exp(-\pi(x/\beta)^2)$. For an integer $q \geq 2$, define $\bar{\psi}_\beta(q)$ to be the distribution on Z_q obtained by drawing $y \leftarrow D_\beta$ and outputting $\lfloor q \cdot y + 1/2 \rfloor \pmod q$. Let $\chi \subset R_q$ denotes the set of polynomials whose coefficients are chosen from $\bar{\psi}_\beta(q)$.

Unlike GPV08 scheme that needs to generate a trapdoor and sample from discrete Gaussians, using the idea from Lyubashevsky, an efficient signature scheme $\mathcal{S} = (KeyGen, Sign, Verify)$ from R-LWE problem can be constructed in **Fig. 1**.

Let $n = 2^k (k \in Z)$, a prime number $p << q = 1 \bmod (2n)$ (q be a sufficiently large public prime modulus), $\chi \subset R_q$ be the error distribution and $R_q = Z_q[x]/ < x^n + 1 >$ be the ring of integer polynomials modulo $x^n + 1$ and q. For a set R, $s \xleftarrow{\$} R$ means that s is chosen uniformly at random from R.

$KeyGen(1^n)$	$Sign(s,m)$	$Verify\{(a,b),m,(\sigma,\ c)\}$
Signing Key: $s \xleftarrow{\$} R_p$	1: $t \xleftarrow{\$} R_q$	1: Accept iff
Verification Key:	2: $c = H(a \cdot t \bmod p, m)$	$\sigma \in R_q$ and
$a \xleftarrow{\$} R_q$, $b = a \cdot s + pe_1$	3: $\sigma = s \cdot c + t + pe_2$	$c = H[(a \cdot \sigma - b \cdot c) \bmod p, m]$
Random Oracle:	4: output (σ, c)	
$H : \{0,1\}^* \to \{-1,0,1\}^n$		

Fig. 1. The proposed signature sheme from R-LWE

- $KeyGen(1^n)$: Choose $s \in R_p$ randomly as the private key. The public key is $(a, b = a \cdot s + pe_1)$, where a is uniformly random chosen from R_q and error term e_1 is chosen independently from a probability distribution $\chi \subset R_q$.
- $Sign(s,m)$: To sign a message $m \in R_p$, pick a polynomial $t \xleftarrow{\$} R_q$ and compute $c = H(a \cdot t \bmod p, m)$ (view it as an element of R_q by using its coordinates as the coefficients of a polynomial). Output the signature $(\sigma = s \cdot c + t + pe_2,\ c)$, where e_2 is chosen independently from a probability distribution χ.
- $Verify\{(a,b),m,(\sigma,\ c)\}$: If $\sigma \in R_q$ and $c = H[(a \cdot \sigma - b \cdot c) \bmod p, m]$, output 1. Else, output 0.

Polynomial addition is the usual coordinate-wise addition, and multiplication is the usual polynomial multiplication followed by reduction modulo $x^n + 1$.

Claim 1. The signature scheme described above is correct.

Proof. Consider a signature $(\sigma = s \cdot c + t + pe_2,\ c)$ of a message m under the public key $(a, b = a \cdot s + pe_1)$, as the verification process can be computed as

$$\begin{aligned}[a \cdot \sigma - b \cdot c] \bmod p &= [a \cdot (s \cdot c + t + pe_2) - (a \cdot s + pe_1) \cdot c] \bmod p \\ &= [a \cdot t + p(a \cdot e_2 - e_1 \cdot c)] \bmod p = a \cdot t \bmod p \end{aligned} \quad (4)$$

So $c = H[(a \cdot \sigma - b \cdot c) \bmod p, m]$ and we can conclude the signature scheme is correct.

3.2 Security Analysis

Claim 2. The scheme $\mathcal{S}$ described above is secure against chosen-plaintext attacks (CPA) in the random oracle model, assuming that the R-LWE is hard and hash function H is secure.

Proof. Assume there is a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ which can win the unforgeability game with probability ε. We can construct a PPT challenger $\mathcal{C}$ to solve the R-LWE problem with probability close to ε. Assume that $\mathcal{A}$ queries the random oracle H h times and the sign algorithm k times. And queries H on every message $m_i (i = 1, ..., h)$ before making a sign query.

Let $l = h + k$ be the bound of the query times on random oracle H during $\mathcal{A}$'s attack, pick $r_1, r_2, \cdots, r_l$ from $\{-1,0,1\}^n$ uniformly at random, which will correspond to the responses of the H. The challenger $\mathcal{C}$ takes as input $(a, b, r_1, r_2, \cdots, r_l)$ and runs $\mathcal{A}$ by giving it the public key $(a, b = a \cdot s + pe_1)$. When $\mathcal{A}$ makes queries to the H, the reply will be the first r_i in the list $(r_1, r_2, \cdots, r_l)$ that has not been used. When $\mathcal{A}$ makes sign queries, $\mathcal{C}$ programs the random

oracle output so that the signatures are valid even though $\mathcal{C}$ don't know the signing key, and the responses of the H is first unused r_i in the list $(r_1, r_2, \cdots, r_l)$, if the same query is made again, it will respond with the previous answer r_i. When $\mathcal{A}$ finishes the queries and outputs a forgery sucessfully with probability ε, $\mathcal{C}$ outputs the same output.

Suppose $\mathcal{A}$ outputs a message m and its signature (σ, c) such that $\sigma \in R_q$ and $c = H[(a \cdot \sigma - b \cdot c) \bmod p, m]$. If H was not queried or pragrammed on $(a \cdot \sigma - b \cdot c) \bmod p$, then the probability that $\mathcal{A}$ produces a c such that $c = H[(a \cdot \sigma - b \cdot c) \bmod p, m]$ is 3^{-n}, hence c is one of the r_i from $(r_1, r_2, \cdots, r_l)$ with probability $1-3^{-n}$. Assume j is such that $c = r_j$, which was a responses to the oracle query H made by $\mathcal{A}$. From the "forking lemma" of Pointcheval and Stern [20], we can produce two different signatures of the message m, (σ, c) and (σ', c') with the probability $\varepsilon - 3^{-n}$, such that

$$H[(a \cdot \sigma - b \cdot c) \bmod p, m] = H[(a \cdot \sigma' - b \cdot c') \bmod p, m]$$

which means that $(a \cdot \sigma - b \cdot c) = (a \cdot \sigma' - b \cdot c') \bmod p$, as $b = a \cdot s + pe_1$, we can obtain $a(\sigma' - sc' - \sigma + sc) = 0$, so $(\sigma' - \sigma) - s(c - c') = 0$, namely $(\sigma' - \sigma) = s(c - c')$, then $\mathcal{C}$ can obtain the private key s with the probability $\varepsilon - 3^{-n}$ by multiplying $(c - c')^{-1}$, So R-LWE problem is solved successfully.

3.3 Efficiency Analysis

Because of the special algebraic structure of R-LWE, the signature scheme from the R-LWE problem has the advantages of much simpler description, analysis and very high efficiency. The efficiency analysis of the scheme is shown in **Table 2**.

In the following parts, the scheme from R-LWE is compared with the RSA scheme on the same parametric conditions and operation environment. We use the same usual personal computer to evaluate the implementation performance of the two schemes: Running them on a Microsoft Windows XP Professional 2002 System, featuring a Pentium (R) D CPU processor, running at 3.0GHz, with 1.0GB of RAM. The implementation uses Shoup's NTL library version 5.5.2 for high-level numeric algorithms, and the code is compiled using Microsoft Visual C++ 6.0 compiler.

Table 2. Efficiency analysis of the scheme from R-LWE

Private key size	Public key size	Message length	Signature length	Verification computation
$n \log p$	$2n \log q$	$n \log p$	$2n \log q$	$\tilde{O}(n^2)$

Table 3. Implementation time of the scheme from R-LWE

Security parameter n	KeyGen (ms)	Signature(ms)	Verification (ms)	Total Time(ms)
128	14.6	30.6	28.7	73.9
256	37.0	69.2	68.4	174.6
512	121.8	243.6	240.4	605.8
1024	443.8	880.8	909.2	2233.8
2048	1687.2	3399.6	3531.2	8618
4096	6578.1	13371.8	13252.7	33202.6

Table 4. Implementation time of the RSA scheme

Security parameter n	KeyGen (ms)	Signature(ms)	Verification (ms)	Total Time(ms)
128	14.0	10.1	5.8	29.9
256	1028.4	120.8	6.9	1156.1
512	2017.3	279.1	7.1	2303.5
1024	5973.7	2232.5	15.2	8221.4
2048	31249.6	9539.7	47.7	40837
4096	217288.3	121170.0	172.0	338630.3

Table 3 and **Table 4** show the simulation results of the two different schemes respectively. Each test is repeated ten times and the datum shown in the two tables are the means of these ten different repetitions. As can be seen from **Table 3** and **Table 4**, the runtime of the scheme from R-LWE is more efficient than the RSA scheme under the same conditions, especially the key generation time and signature time. Regardless of the inefficiency of the verification compared to RSA scheme, the total runtime of our scheme is much more efficient than that of the RSA scheme with the increase of security parameter n.

Modulus q takes the minimum integer satisfying corresponding conditions in the two schemes, and the length of messages encrypted in the two scheme is $n \log q$ bit.

More detailed simulation results of the two above-described schemes are shown in **Fig. 2** to **Fig. 5**. And **Fig. 2, Fig. 3** and **Fig. 4** indicate the efficiency of the key generation, signature and verification in the two schemes respectively, and the comparison of the total implementation time of the two schemes is shown in **Fig. 5**. At the same time, the figures also show the change tendencies of the implementation time of the two encryption schemes along with the change of the security parameter n.

As can be seen from **Fig. 2** to **Fig. 5**, the efficiency of the scheme from R-LWE is more eximious than the RSA signature scheme, and the increasing tendency of the scheme from R-LWE in runtime is much slower than that of the RSA scheme with the increase of security parameter n. Furthermore, the scheme from R-LWE is believed to be secure against quantum computers.

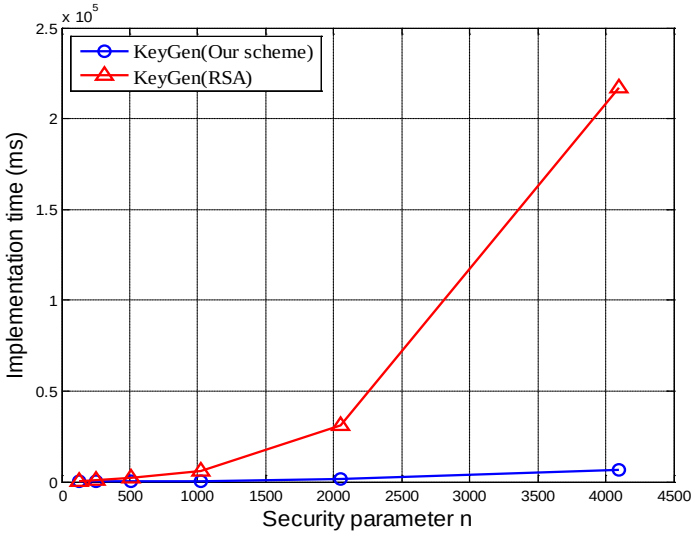

Fig. 2. Efficiency comparison of key generation between our signature scheme and RSA scheme. Security parameter $n = 128, 256, 512, 1024, 2048, 4096$

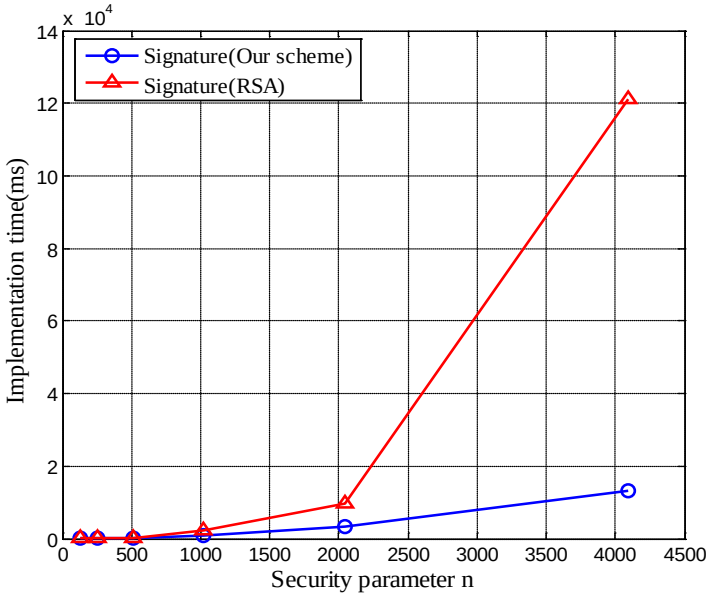

Fig. 3. Efficiency comparison of signature between our signature scheme and RSA scheme. Security parameter $n = 128, 256, 512, 1024, 2048, 4096$

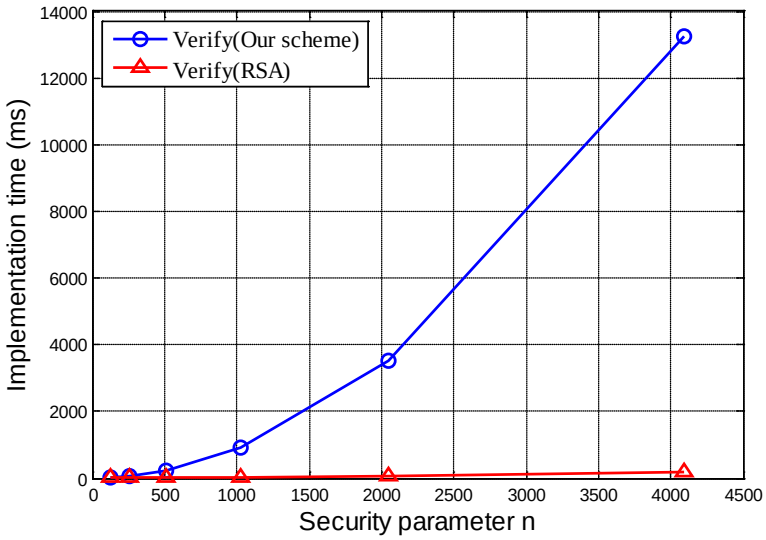

Fig. 4. Efficiency comparison of verification between our signature scheme and RSA scheme. Security parameter $n = 128, 256, 512, 1024, 2048, 4096$

4. Linearly Homomorphic Signature Scheme

4.1. Scheme

Definition 3. A homomorphic signature scheme is composed of four probabilistic polynomial-time (PPT) algorithms $(Setup, Sign, Evaluate, Verify)$ such that:

- $Setup(1^n, 1^l)$: Take as input a security parameter n and the maximum evaluation data set

size l. Algorithm outputs the private key sk and the public key pk.

- $Sign(\tau, sk, m_i)$: Take as input a tag $\tau \in \{0,1\}^*$, the private key sk and a message $m_i (i \in \{1,\cdots l\})$ in some message space $\mathcal{M}$. Algorithm outputs a signature $\sigma_i \in \Sigma$, where Σ is a signature space.
- $Evaluate(\tau, pk, \{\sigma_1,\cdots,\sigma_l\}, g)$: Take as input a tag τ, a public key pk, a tuple of signatures $\sigma_i \in \Sigma (i = 1,\cdots,l)$, and a multivariate function $g \in \mathcal{F}$. Outputs a signature $\sigma = g(\sigma_1,\cdots,\sigma_l)$.
- $Verify(\tau, pk, \{m_1,\cdots,m_l\}, g, \sigma)$: Take as input a tag τ, a public key pk, a tuple of messages $m_i \in \mathcal{M} (i = 1,\cdots l)$, a function g and a signature σ. Algorithm outputs either 0 or 1.

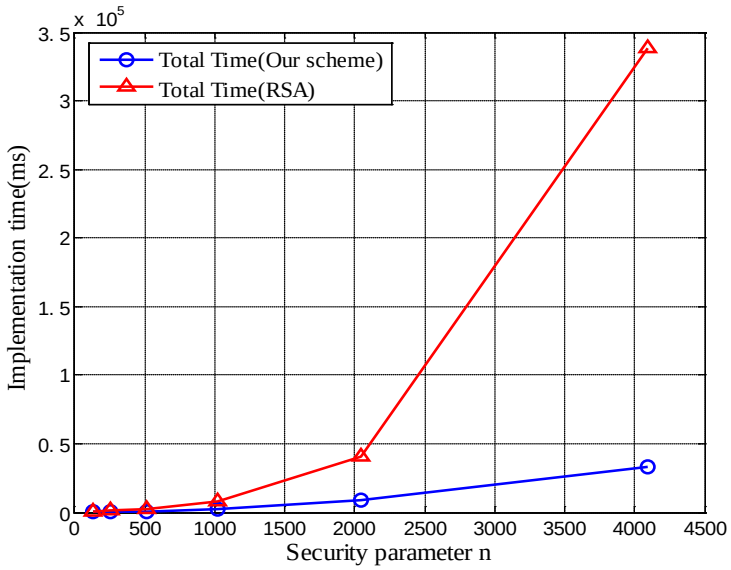

Fig. 5. Comparison of total implementation time between our signature scheme and RSA scheme. Security parameter $n = 128, 256, 512, 1024, 2048, 4096$

It is required that for any $(pk, sk) \leftarrow Setup(1^n, 1^l)$, the following hold:

1) In fact, for any tag $\tau \in \{0,1\}^*$ and any message $m' \in \mathcal{M}$, if $\sigma' \leftarrow Sign(\tau, sk, m')$, then $Verify(\tau, pk, m', \sigma') = 1$.
2) For any tag $\tau \in \{0,1\}^*$, all sets $\{(m_i, \sigma_i)\}_{i=1}^l$ and all functions $g \in \mathcal{F}$, if $Verify(\tau, pk, m_i, \sigma_i) = 1$ for all i, then

$$Verify(\tau, pk, g(m_1,\cdots,m_l), Evaluate(\tau, pk, \{\sigma_1,\cdots,\sigma_l\}, g)) = 1$$

The homomorphic signature scheme described above is defined as $\mathcal{F}$-homomorphic. Especially, if $\mathcal{F}$ is composed of all integer linear functions, we say that the scheme is a linearly homomorphic signature scheme.

Now we begin to describe the linearly homomorphic signature scheme proposed in this paper, and **Fig. 6** provides an overview of the scheme.

For any positive parameter $\delta > 0$, the Gaussian function with center 0 over the real domain is given by $D_\delta(x) = 1/\delta \cdot \exp(-\pi(x/\delta)^2)$. On an integer $q \geq 2$, define $\bar{\psi}_\delta(q)$ to be the distribution over Z_q obtained by choosing $y \leftarrow D_\delta$ and outputting $\lfloor q \cdot y + 1/2 \rfloor \pmod q$. Let

the error distribution $\chi \subset R_q$ denotes the set of polynomials whose coefficients are chosen from $\bar{\psi}_\delta(q)$, $R_q = Z_q[x]/<x^n+1>$ be the integer polynomial ring modulo $f(x)$ and q, and $H:\{0,1\}^* \to Z_q^n$ is a random oracle that maps $\{0,1\}^*$ to Z_q^n.

Using a homomorphic hash function family [18], an efficient linearly homomorphic signature scheme $\mathcal{S} = (Setup, Sign, Evaluate, Verify)$ without trapdoor from R-LWE assumption is constructed as follows:

<table>
<tr><td colspan="3">$Setup(1^n, 1^l)$
private Key: $s \xleftarrow{\$} R_p$, public key: $a \xleftarrow{\$} R_q$, $b = a \cdot s + pe^*$, $H:\{0,1\}^* \to Z_q^n$</td></tr>
<tr><td>$Sign(\tau, s, m_i)$
1: For $j = 1, \cdots, n$
compute $\alpha_j = H(\tau \| j, t)$
2: $h_{m_i} = (h_{i_1}, \cdots, h_{i_n})$
$= (<m_i, \alpha_1>, \cdots, <m_i, \alpha_n>)$
3: $v_i \xleftarrow{\$} R_q, \sigma_i = s(h_{m_i} + v_i) + pe_i$
4: output (σ_i, v_i)</td><td>$Evaluate(\tau, pk, \{(k_i, \sigma_i, v_i)\}_{i=1}^l)$
Given a tag τ, (a,b) and
$\{(k_i, \sigma_i, v_i)\}_{i=1}^l$ $(k_i \in Z_p)$
Outputs $(\sum_{i=1}^l k_i\sigma_i, \sum_{i=1}^l k_i v_i)$</td><td>$Verify\{\tau, (a,b), m, (\sigma, v)\}$
1: $\alpha_j = H(\tau \| j)(j = 1, \cdots, n)$
2: $h_m = (h_i, \cdots, h_i)$
$= (<m, \alpha_1>, \cdots, <m, \alpha_n>)$
3: If $\sigma, v \in R_q$ and
$a \cdot \sigma - b \cdot v = b \cdot h_m \pmod p$
output 1. Else, output 0</td></tr>
</table>

Fig. 6. The signature scheme $\mathcal{S}$ from R-LWE

- $Setup(1^n, 1^l)$: Given the security parameter $n = 2^k (k \in Z)$, the maximum data set size l and a prime number $p << q = 1 \bmod (2n)$ (q is a large prime modulus). Choose $s \in R_p$ randomly as the private key. The public key is $(a, b = a \cdot s + pe^*)$, where a is chosen uniformly at random from R_q and error term and e^* is chosen independently from a probability distribution $\chi \subset R_q$.
- $Sign(\tau, s, m_i)$: Given a tag τ and a private key s, to sign a message $m_i \in R_p (i \in \{1, \cdots l\})$, the signer performs the following operations:

1) For $j = 1, \cdots, n$, compute $\alpha_j = H(\tau \| j)$.

2) $h_{m_i} = (h_{i_1}, \cdots, h_{i_n}) = (<m_i, \alpha_1>, \cdots, <m_i, \alpha_n>)$.

3) $v_i \xleftarrow{\$} R_q, \sigma_i = s(h_{m_i} + v_i) + pe_i$.

where e_i is chosen independently from a probability distribution χ. Output the signature $(\tau, m_i, \sigma_i, v_i)$.

- $Evaluate(\tau, (a,b), \{(k_i, \sigma_i, v_i)\}_{i=1}^l)$: Given a tag τ, a public key (a,b) along with a tuple of $\{(k_i, \sigma_i, v_i)\}_{i=1}^l$ $(k_i \in Z_p)$. Outputs $(\sum_{i=1}^l k_i\sigma_i, \sum_{i=1}^l k_i v_i)$.
- $Verify\{\tau, (a,b), m, (\sigma, v)\}$: Given a tag τ, a public key (a,b), a message $m \in \mathcal{M}$ and a signature σ, do the following:

1) $\alpha_j = H(\tau \| j)(j = 1, \cdots, n)$.

2) $h_m = (h_i, \cdots, h_i) = (<m, \alpha_1>, \cdots, <m, \alpha_n>)$.

3) If $\sigma \in R_q$ and $a \cdot \sigma - b \cdot v = b \cdot h_m (\text{mod } p)$, output 1. Else, output 0.

The scheme described above is correct, in fact:

$$\begin{aligned}[a \cdot \sigma - bv - b \cdot h_m] \bmod p &= \{a \cdot [s \cdot (h_m + v) + pe] - (a \cdot s + pe^*)(v + h_m)\} \bmod p \\ &= [p(a \cdot e - e^* v - e^* h_m)] \bmod p = 0 \end{aligned} \tag{6}$$

Claim 3. The polynomial ring signature scheme over R_p described above is linearly homomorphic.

Proof. Given messages m_i such that $Verify\{\tau, (a,b), m_i, (\sigma_i, v_i)\} = 1$ for all i. As all operations are performed in R_q, the signature $(\sum_{i=1}^{l} k_i \sigma_i, \sum_{i=1}^{l} k_i v_i)$ output by $Evaluate(\tau, (a,b), \{(k_i, \sigma_i, v_i)\}_{i=1}^{l})$ satisfies the condition $\sigma, v \in R_q$. On the other hand, as

$$[a \cdot (\sum_{i=1}^{l} k_i \sigma_i) - b \cdot (\sum_{i=1}^{l} k_i v_i) - b \cdot (\sum_{i=1}^{l} k_i h_{m_i})] = \left\{ a \cdot \sum_{i=1}^{l} k_i [s \cdot (h_{m_i} + v_i) + pe_i] - (a \cdot s + pe^*) \cdot (\sum_{i=1}^{l} k_i v_i + \sum_{i=1}^{l} k_i h_{m_i}) \right\}$$

$$= a \cdot \sum_{i=1}^{l} k_i \{s \cdot [(< m_i, \alpha_1 >, ..., < m_i, \alpha_n >) + v_i] + pe_i\} - (a \cdot s + pe^*) \cdot \sum_{i=1}^{l} k_i [(< m_i, \alpha_1 >, ..., < m_i, \alpha_n >) + v_i]$$

$$= p \left\{ a \cdot \sum_{i=1}^{l} k_i e_i - e^* \cdot \sum_{i=1}^{l} k_i [(< m_i, \alpha_1 >, ..., < m_i, \alpha_n >) + v_i] \right\} = 0 \bmod p \tag{7}$$

Hence the conclusion is correct.

4.2. Security Analysis

A homomorphic signature scheme $\mathcal{S} = (Setup, Sign, Evaluate, Verify)$ is unforgeable under chosen-message attack, if for all probabilistic polynomial-time adversary (PPT) $\mathcal{A}$, the success probability of $\mathcal{A}$ in the following game is negligible in the security parameter n.

- *Setup* : Challenger runs $Setup(1^n, 1^l)$ to get $\{s, (a, b = a \cdot s + pe^*)\}$, and sends public key (a,b) to $\mathcal{A}$.
- *Queries* : $\mathcal{A}$ makes queries on a sequence of messages $m_i \in R_p$ $(i = 1, \cdots, Q)$, the challenger gives the hash h_{m_i} and the signatures σ_i to $\mathcal{A}$.
- *Output* : $\mathcal{A}$ outputs a tuple of the tag, message and signature $\{\tau^*, m^*, \sigma^*\}$.

The adversary succeeds if $Verify(\tau^*, (a,b), m^*, \sigma^*) = 1$ but $m^* \neq m_i (i = 1, \cdots, Q)$.

Claim 4. For any parameters n, q and polynomial $f(x)$ satisfying the condition of the R-LWE problem, the signature scheme $\mathcal{S}$ is unforgeable in the chosen message attack model (CMA), assuming that the R-LWE problem is hard.

Proof. The proof is similar to that of the Claim 2 except that the random oracle query. Assume there is a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ which can win the unforgeability game with probability ε. We can construct a PPT challenger $\mathcal{C}$ to solve the R-LWE problem with probability close to ε. Assume that $\mathcal{A}$ queries the sign algorithm k times. Then $\mathcal{C}$ runs $\mathcal{A}$ by giving it the public key $(a, b = a \cdot s + pe^*)$.

When $\mathcal{A}$ makes sign queries, $\mathcal{C}$ programs the random oracle output so that the signatures are valid even though $\mathcal{C}$ don't know the signing key. When $\mathcal{A}$ finishes the queries and outputs a forgery sucessfully with probability ε, $\mathcal{C}$ outputs the same output.

Suppose $\mathcal{A}$ outputs a message m and its signature (σ, v) such that $\sigma, v \in R_q$ and $a \cdot \sigma - b \cdot v = b \cdot h_m \pmod{p}$. If H was not queried or pragrammed on $(a \cdot \sigma - b \cdot v) \bmod p$, then the probability that $\mathcal{A}$ produces a $c = b \cdot h_m$ such that $a \cdot \sigma - b \cdot v = b \cdot h_m \pmod{p}$ is q^{-n}, From the "forking lemma" of Pointcheval and Stern [20], we can produce two different signatures of the message m, (σ, v) and (σ', v') with the probability $\varepsilon - q^{-n}$, such that

$$a \cdot \sigma - b \cdot v = a \cdot \sigma' - b \cdot v' \bmod p$$

as $b = a \cdot s + pe^*$, we can obtain $a(\sigma' - sv' - \sigma + sv) = 0$, so $(\sigma' - \sigma) - s(v - v') = 0$, namely $(\sigma' - \sigma) = s(v - v')$, then $\mathcal{C}$ can obtain the private key s with the probability $\varepsilon - q^{-n}$ by multiplying $(v - v')^{-1}$, So R-LWE problem is solved successfully.

4.3. Efficiency Analysis

Because of the special algebraic structure of R-LWE, the linearly homomorphic signature scheme from R-LWE problem has the advantages of much simpler description, analysis and very high efficiency. Compared with the signatures scheme of [5, 15], the efficiency improvement of our scheme is shown in **Table 5**.

In the scheme of Boneh, $m = \lfloor 6n \lg 2q + 1 \rfloor$. psf and bt denote the computational cost of running preimage sampling functions (PSF) [4] and ExtBasis algorithm [21] respectively. The scheme of Boneh needs to use the ExtBasis algorithm and PSF to sign messages, and the PSF is a sub-algorithm of the ExtBasis algorithm. As the PSF algorithm is rather inefficient, whose time complexity is $\Omega(n^3)$, the operations for signature of the scheme of Boneh is more than $2psf \geq 2\Omega(n^3)$. The data in **Table 5** indicates that the scheme from R-LWE is more efficient than other correlative sign schemes, especially its public key, private key and operations for signature are incomparable to the scheme based on the PSF algorithm.

Table 5. Efficiency comparison.

cryptosystem	Private key size	Public key size	Signature length	Signature cost	Verification cost
[5]	$m(m+n)(1+\log q)$	$mn(1+\log q)$	$2m(1+\log q)$	$1psf + 1bt$	$\tilde{O}(nm)$
[15]	$m^2 \log q$	$mn \log q$	$m \log q + n$	$1psf + n(\mathrm{m}+1)$	$\tilde{O}(nm)$
[17]	$mk \log q$	$n(m+k) \log q$	$(m+k) \log q$	$\tilde{O}[m(n+k)]$	$\tilde{O}[n(m+k+1)]$
Our scheme	$n \log q$	$2n \log q$	$n \log q$	$\tilde{O}(n^2)$	$\tilde{O}(n^2)$

5. Conclusion

Digital signature can solve many security issues from internal and external malicious attacks in network coding, sensor networks and cloud storage etc. In order to guarantee the security of the network data, owing to the flexible structure and implementation simplicity of lattice cryptography, two efficient digital signature schemes from R-LWE assumption are proposed, and the analyses show that they are unforgeable in the chosen message attack model. The schemes mainly use modular addition and modular multiplication operations of the ring of integer polynomials, especially based on the special algebraic structure of R-LWE assumption, hence they are more efficient than previous interrelated signature schemes using ExtBasis or PSF algorithm. In the future, we will explore the fully homomorphic signature from lattice.

References

[1] D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a Linear Subspace: Signature Schemes for Network Coding," in *Proc. of PKC 2009, Lecture Notes in Computer Science*, vol. 5443, pp. 68-87, March 18-20, 2009. Article (CrossRef Link).

[2] Y. Wang, "Insecure 'Provably Secure Network Coding' and Homomorphic Authentication Schemes for Network Coding," *IACR Cryptology ePrint Archive*, no. 60, pp. 1-9, June, 2010. Article (CrossRef Link)

[3] H. Xiong, Z. Chen, and F. Li, "Bidder-anonymous English auction protocol based on revocable ring signature," *Expert Systems with Applications*, vol. 39, no. 8, pp. 7062-7066, June, 2012. Article (CrossRef Link).

[4] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for Hard Lattices and New Cryptographic Constructions," in *Proc. of the 40th Annual ACM Symposium on Theory of Computing (STOC 2008)*, pp. 197-206, May 17-20, 2008. Article (CrossRef Link).

[5] D. Boneh and D. M. Freeman, "Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures," in *Proc. of PKC 2011, Lecture Notes in Computer Science*, vol. 6571, pp. 1-16, March 6-9, 2011. Article (CrossRef Link).

[6] D. Boneh and D. M. Freeman, "Homomorphic Signatures for Polynomial Functions," in *Proc. of Eurocrypt 2011, Lecture Notes in Computer Science*, vol. 6632, pp. 149-168, May 15-19, 2011. Article (CrossRef Link).

[7] S. D. Gordon, J. Katz and V. Vaikuntanathan, "A Group Signature Scheme from Lattice Assumptions," in *Proc. of Asiacrypt 2010, Lecture Notes in Computer Science*, vol. 6477, pp. 395-412, December 5-9, 2010. Article (CrossRef Link).

[8] H. Feng and F. Zhao, "Research on Dynamic Data Integrity Detection on Cloud Storage," *Journal of Chinese Computer Systems*, vol. 35, no. 2, pp. 239-243, February, 2014. Article (CrossRef Link).

[9] A. Jain and, B. V. R. Reddy, "Eigenvector centrality based cluster size control in randomly deployed wireless sensor networks," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2657-2669, April, 2015. Article (CrossRef Link).

[10] Z. Li and G. Gong, "Data Aggregation Integrity Based on Homomorphic Primitives in Sensor Networks," in *Proc. of the 9th International Conference on Ad-hoc, Mobile and Wireless Networks, Lecture Notes in Computer Science*, vol. 6288, pp. 149-162, August 20-22, 2010. Article (CrossRef Link).

[11] W. Liao, Y. Kao and Y. Li, "A sensor deployment approach using glowworm swarm optimization algorithm in wireless sensor networks," *Expert Systems with Applications*, vol. 38, no. 10, pp. 12180-12188, September, 2011. Article (CrossRef Link).

[12] Y. Yong, N. Jianbing, H. A. Man, L. Hongyu, W. Hua and X. Chunxiang, "Improved security of a dynamic remote data possession checking protocol for cloud storage," *Expert Systems with Applications*, vol. 41, no. 17, pp. 7789-7796, December, 2014. Article (CrossRef Link).

[13] S. Micali and R. L. Rivest, "Transitive signature schemes," in *Proc. of CT-RSA 2002, Lecture Notes in Computer Science*, vol. 2271, pp. 236-243, February 18-22, 2002. Article (CrossRef Link).

[14] R. Johnson, D. Molnar, D. Song and D. Wagner, "Homomorphic signature schemes," in *Proc. of CT-RSA 2002, Lecture Notes in Computer Science*, vol. 2271, pp. 244-262, February 18-22, 2002. Article (CrossRef Link).

[15] W. FengHe, H. YuPu and W. BaoCang, "Lattice-based linearly homomorphic signature scheme over binary field," *Science China Information Sciences*, vol. 56, no. 11, pp. 1-9, November, 2013. Article (CrossRef Link).

[16] D. Catalano, D. Fiore and B. Warinschi, "Homomorphic Signatures with Efficient Verification for Polynomial Functions," in *Proc. of CRYPTO 2014, Part I, Lecture Notes in Computer Science*, vol. 8616, pp. 371-389, August 17-21, 2014. Article (CrossRef Link).

[17] V. Lyubashevsky, “Lattice signatures without trapdoors,” in *Proc. of 31th Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pp. 738-755, April 15-19, 2012. Article (CrossRef Link).
[18] V. Lynbashevsky, C. Peikert and O. Regev, “On Ideal Lattices and Learning with Errors over Rings,” in *Proc. of 29th Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Lecture Notes in Computer Science*, vol. 6110, pp. 1-23, May 30 - June 3, 2010. Article (CrossRef Link).
[19] V. Lyubashevsky and D. Micciancio, "Asymptotically efficient lattice-based digital signatures," in *Proc. of the TCC 2008, Lecture Notes in Computer Science*, vol. 4948, pp. 37–54, March 19-21, 2008. Article (CrossRef Link).
[20] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology* , vol. 13, no. 3, pp. 361-396, June, 2000. Article (CrossRef Link).
[21] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert, “Bonsai Trees, or How to Delegate a Lattice Basis,” *Journal of Cryptology*, vol. 25, no. 4, pp. 601-639, October, 2012. Article (CrossRef Link).

Ting Wang received his B.S. degree in applied mathematics from Qufu Normal University in 2003, received his M.S. degree from Wuhan University in 2006, and received his Ph.D. from Shenzhen University in 2014.He is currently a postdoctoral researcher in ATR Key Laboratory of National Defense Technology, College of Information Engineering, Shenzhen University. His research interests include public key cryptography and information security.

Jianping Yu received his B.S. and M.S. degrees from Northwest Polytechnical University in 1989 and 1992, received his Ph.D. from Xidian University, Xi China, in 1995.He is currently a professor with ATR National Defense Technology Key Laboratory,Collegeof Information Engineering, Shenzhen University. He has published more than 100 papers in the journals. His research interests include cryptography and information security.

Peng Zhang received her B.S. degree from Naval University of Engineering in 2005, and M.S. degree and Ph.D from Shenzhen University respectively in 2008 and 2011. She is currently a lecturer in Shenzhen University. Her research interests include cryptography, sensor network, information security and cloud computing. She has published over 10 academic research papers.

Yong Zhang received his B.S., M.S. and Ph.D. degrees in Communication Engineering from the PLA Science and Technology University, Nanjing, China, in 1997, 2001 and 2004 respectively. He is currently working as a professor in ATR Key Laboratory of National Defense Technology, College of Information Engineering, Shenzhen University. His research interests include information security and multimedia information processing, etc.