Wireless Pers Commun (2017) 95:2973–2988
DOI 10.1007/s11277-017-3979-8

Efficient Chosen-Ciphertext Secure Encryption from R-LWE

Ting Wang[1,2] · Guoqiang Han[1] · Jianping Yu[2] · Peng Zhang[2] · Xiaoqiang Sun[2]

Published online: 1 February 2017
© Springer Science+Business Media New York 2017

Abstract In order to construct efficient public-key encryption scheme that is secure against adaptive chosen-ciphertext attacks (CCA), an efficient signature scheme and an identity-based encryption (IBE) scheme from the learning with errors over rings are presented firstly in this paper, whose security are reducible to the hardness of the shortest vector problem in the worst case on ideal lattices. Secondly, a CCA-secure public key cryptosystem is constructed on the basis of the IBE and signature proposed above. The efficiency analysis indicates the proposed signature and encryption schemes are much more efficient than correlative cryptosystems. The security analysis shows that the IBE scheme is secure against chosen-plaintext attacks, and the public-key encryption scheme is CCA-secure in the random oracle model.

Keywords Chosen-ciphertext security · R-LWE · IBE · Signature

✉ Ting Wang
wangt809@163.com

Guoqiang Han
csgqhan@scut.edu.cn

Jianping Yu
yujp@szu.edu.cn

Peng Zhang
zhangp@szu.edu.cn

Xiaoqiang Sun
xqsun@szu.edu.cn

[1] School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China

[2] ATR Key Laboratory of National Defense Technology, Shenzhen University, Shenzhen 518060, China

1 Introduction

Lattice-based cryptographic constructions hold a great promise for cryptography, as they enjoy very strong security proofs, efficient implementations and great simplicity. Furthermore, lattice-based cryptography is believed to be secure against quantum computers. Ajtai and Dwork [1] constructed a public-key cryptosystem whose security is based on the worst-case hardness of a lattice problem, which was the first of its kind admitting a proof of security based on worst-case hardness assumptions on lattice problems, however, the cryptosystems is quite inefficient. The first version of the cryptosystem together with a security proof stemmed from a work of Regev [2], who proposed a very natural intermediate problem called learning with errors (LWE) and proved that it is at least as hard as worst-case hardness problems under a quantum reduction. Subsequently Peikert [3] gave a classical reduction from variants of the shortest vector problem to corresponding versions of the LWE problem and constructed a chosen ciphertext attack (CCA) secure public-key encryption scheme with a much simpler description based on the LWE problem, but whose public key size, private key size and expansion are large, which leads to its encryption efficiency is not high.

Since the LWE problem has been put forward, it has proved to be versatile for encryption schemes, serving as the basis for secure lattice-based encryption under various cases. Besides its first application in a public-key cryptosystem [2], it has also been applied to identity-based encryption [4, 5], hardness of learning results relating to half spaces [6], and others [7–9], however, the efficiency of the above schemes are not high enough. In order to resolve the intrinsic inefficiency, Lyubashevsky et al. [10] proposed LWE problem over rings (R-LWE) and proved that the R-LWE distribution is pseudorandom, assuming that the worst-case problems on ideal lattices are hard for polynomial-time quantum algorithms.

R-LWE problem has a relatively simpler algebraic structure, which can be used to construct many kinds of cryptographic schemes, such as digital signature [11], encryption [12–14], etc. Literation [11] proposes an efficient signature scheme from the R-LWE problem, which avoids sampling from discrete Gaussians and has the characteristics of the even simpler description. Based on the R-LWE problem, [12] and [13] present a fully homomorphic encryption scheme and a CPA-secure encryption scheme respectively, and [14] proposes a CCA-secure public key encryption from the same difficulty assumption. Compared to the corresponding schemes based on the LWE problem, the above scheme has obvious improvement in efficiency. Here we mainly focuses on CCA-secure encryption from R-LWE.

Security against adaptive chosen-ciphertext attacks (CCA) [15] is a strong and useful notion of security for public-key encryption schemes used in practice, where adversary can request decryption oracle under the limitation that it may not request the decryption of challenge ciphertext itself. This security level is appropriate for encryption schemes used in the presence of active attackers who may potentially modify messages in transit. However, only a few approaches are known for constructing CCA-secure encryption schemes. Naor [16] firstly achieved non-adaptive chosen-ciphertext security, later extended to the case of adaptive chosen-ciphertext security by Dolev [15] using as building blocks any CPA-secure encryption scheme along with any non-interactive zero-knowledge proof system for all of *NP* [17]. Instead of using the approach in previous schemes, Boneh [18] put forward a new approach for constructing CCA-secure encryption schemes, which is the approach adopting in this paper. Later, Peikert [3] firstly constructed a very natural LWE-based CCA-secure cryptosystem, which not only provides a different alternative to traditional constructions but also possesses the advantages of a much simpler description, analysis and tighter underlying approximation factors, as the scheme is designed based on the LWE problem, its efficiency is low, and whose public key and private key size is large. Yang et al. [14] proposed a CCA-secure public key encryption from R-LWE, which could support public ciphertext integrity verification and block encryption, and improves the method of generating trapdoor on ideal lattice, its efficiency has been greatly improved, however, whose public key, private key size and expansion are still large, which leads to its encryption efficiency is not high enough for practical applications.

In order to construct more efficient CCA-secure public-key encryption schemes from R-LWE, first of all, we present an efficient signature scheme and a identity-based encryption (IBE) scheme from the R-LWE. Analysis indicates that the efficiency of our scheme is more eximious to the RSA signature scheme, and the IBE scheme is CPA-secure. After that, on the basis of the signature scheme and the proposed IBE scheme, adopting the paradigm of Boneh et al., we construct a more efficient CCA-secure public-key encryption scheme from R-LWE, which is much better than [3, 14] in efficiency, and has the following new features:

(1) could achieve batch encryption over rings;
(2) has a low encryption expansion factor $2\log q$, and it is invariable with the increase of the security parameter n and message size m;
(3) supports public ciphertext integrity verification;
(4) builds security on the hardness of the shortest vector problem in the worst case on ideal lattices, and has a higher encryption/decryption speed.

The remainder of the paper is organized as follows. In Sect. 2, the preliminaries are introduced. In Sect. 3, an efficient signature scheme from R-LWE problem along with the analyses of the efficiency and security are given. Then the definition of IBE is introduced firstly, and an identity-based encryption scheme is put forward along with its security analysis in Sect. 4. In Sect. 5, a CCA-secure public key cryptosystem is constructed based on the IBE and signature schemes proposed above, furthermore, the efficiency and security analyses of the scheme are discussed in detail. Finally, Sect. 6 concludes the paper, and plans the future work.

2 Preliminaries

2.1 Learning with Errors Over Rings (R-LWE)

Let $f(x) = x^n + 1 \in Z[x]$, where the security parameter n is a power of 2, making $f(x)$ irreducible over the rationals, $R = Z[x]/<f(x)>$ be the ring of integer polynomials modulo $f(x)$. Let $q = 1 \bmod 2n$ be a sufficiently large public prime modulus (bounded by a polynomial in n), and $R_q = R/<q> = Z_q[x]/<f(x)>$ be the ring of integer polynomials modulo both $f(x)$ and q. Elements of R_q are typically represented by integer polynomials of degree less than n, whose coefficients are from $\{0, 1, \ldots, q-1\}$.

In the above-described ring, the R-LWE problem can be described as follows [10]. Let $s \in R_q$ be a uniformly random ring element (secret), and define two distributions on $R_q \times R_q$: (1) $(a, b = a \times s + e) \in R_q \times R_q$, where $a \leftarrow R_q$ is uniformly random and e is some "small" random error term chosen from a certain distribution χ over R_q. (2)(a, c), where a, $c \leftarrow R_q$ are uniformly random. The goal of the R-LWE problem is to distinguish the two distributions described above. In other words, if R-LWE is hard, then the collection of 'random noise equations' $(a, a \times s + e)$ is pseudorandom, and all operations are performed in R_q.

Lyubashevsky et al. [10] proved the hardness of the R-LWE problem under the worst case assumptions on ideal lattices (see Theorem 2).

Theorem 1 *Suppose that it is hard for polynomial-time quantum algorithms to approximate the shortest vector problem (SVP) in the worst case on ideal lattices in R to within a fixed poly*(n) *factor. Then any poly*(n) *number of samples drawn from the R-LWE distribution are pseudorandom to any polynomialtime (even quantum) attacker.*

2.2 Sampling from Discrete Gaussians

Lattice has useful cryptography application because of its natural trapdoor characteristic. Virtually, all kinds of lattice-based cryptography schemes show how to use a trapdoor in a theoretically sound and secure way. A short basis of the lattice is a trapdoor like this.

Theorem 2 (Generating a short basis [19]). *There is a fixed constant* $C > 1$ *and a probabilistic polynomial-time (PPT) algorithm TrapGen*(q, n) *that, for poly(n)-bounded* $m \geq Cn \lg q$, *outputs* $(A \in Z_q^{n \times m}, T \in Z^{m \times m})$ *such that:*

- *A is statistically close to a uniform matrix in* $Z_q^{n \times m}$,
- *T is a basis of* $\wedge_q^{\perp}(A)$,
- *The Euclidean norm of all the rows in* $T(||T||)$ *is bounded by* $O(n \log n)$.

Theorem 3 (Sampling from discrete Gaussians [4]). *There is a PPT algorithm Sample* $\mathrm{ISIS}(A, T, \sigma, u)$, *given a matrix* $A \in Z_q^{n \times m}$, *a basis T of* $\wedge^{\perp}(A)$, *a parameter* $\sigma \geq ||T|| \cdot \omega(\sqrt{\log n})$, *and a vector* $u \in Z^n$, *outputs a sample from a distribution that is statistically close to* $\mathcal{D}_{\wedge_q^u(A), \sigma}$. $\mathcal{D}_{\wedge_q^u(A), \sigma}$ is the discrete Gaussian distribution over $\wedge^{\perp}(A)$ with parameter σ.

Theorem 4 ([4]). *The algorithm Sample* $\mathrm{ISIS}(A, T, \sigma, u)$ *gives a collection of trapdoor one-way functions with preimage sampling, if inhomogeneous smallest integer solution* ($ISIS_{q,m,\sigma\sqrt{m}}$) *problem is hard on the average.*

The $ISIS_{q,m,\sigma\sqrt{m}}$ can be described as follows: Given an integer q, a matrix $A \in Z_q^{n \times m}$, a syndrome $u \in Z_q^n$ and a real β, find an integer vector $\mathbf{e} \in \mathbb{Z}^m$ such that $A \cdot e = u \bmod q$ and $||e|| \leq \beta$.

3 Signature Scheme

3.1 Signature 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 [20], an efficient signature scheme $\mathcal{S} = (KeyGen, Sign, Verify)$ from R-LWE problem can be constructed as follows:

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.

- *KeyGen*(1^n): Choose $s \in R_q$ randomly as the private key. The public key is $(a, b = a \cdot s + pe_1)$, where $a \leftarrow R_q$ is uniformly random and error term e_1 is chosen independently from a probability distribution $\chi \subset R_q$. $H : \{0,1\}^* \to Z_q^n$ is a random oracle that maps the space of message to Z_q^n.
- *Sign*(s, m): Compute $c = H(m) \in Z_q^n$ (view it as an element of R_q by using its coordinates as the coefficients of a polynomial), and output the signature $\sigma = s \cdot c + pe_2$, where e_2 is chosen independently from a probability distribution χ.
- *Verify*$((a,b), m, \sigma)$: If $\sigma \in R_q$ and $a \cdot \sigma \equiv b \cdot H(m) \pmod{p}$, 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 $\sigma = s \cdot c + pe_2$ of a message m under the public key $(a, b = a \cdot s + pe_1)$, then the verification process can be computed as

$$\begin{aligned}[a \cdot \sigma - b \cdot H(m)] \bmod p &= [a \cdot (s \cdot c + pe_2) - (a \cdot s + pe_1) \cdot H(m)] \bmod p \\ &= [p(a \cdot e_2 - e_1 \cdot c)] \bmod p \\ &= 0\end{aligned}$$

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 Let adversary $\mathcal{A}$ be a probabilistic polynomial-time (PPT) adversary that makes at most k signature queries. $\mathcal{A}$ works as follows:

- *Setup* Challenger runs $KeyGen(1^n)$ to get $\{ s, (a, b = a \cdot s + pe_1)\}$, and sends public key $(a, b = a \cdot s + pe_1)$ to $\mathcal{A}$.
- *Queries* $\mathcal{A}$ makes k queries to H on messages $m_i (i = 1, \ldots, k)$ and challenger returns $c_i = H(m_i)(i = 1, \ldots, k)$ to $\mathcal{A}$. Following this, $\mathcal{A}$ makes signature queries on $c_i (i = 1, \ldots, k)$, the challenger chooses $e_1, e_2, \ldots, e_k \in \chi$ at random, runs *Sign* to get $\sigma_i (i = 1, \ldots, k)$ and sends them to $\mathcal{A}$.
- *Output* $\mathcal{A}$ outputs a tuple of the public key, message and signature $\{(a^*, b^*), m^*, \sigma^*\}$, where $m^* \neq m_i (i = 1, \ldots, k)$.

If the challenger never responds signature queries on messages $m_i (i = 1, \ldots, k)$, $\mathcal{A}$ outputs the legal signature σ^* of m^* satisfying $Verify((a,b), m^*, \sigma^*) = 1$, namely,

$$\begin{aligned}[a \cdot \sigma^* - b \cdot H(m^*)] \bmod p &= [a \cdot \sigma^* - (a \cdot s + pe_1) \cdot H(m^*)] \bmod p \\ &= a \cdot [\sigma^* - s \cdot H(m^*)] \mathrm{mod} \\ &= 0\end{aligned}$$

It can be seen that $a = 0 \bmod p$ or $\sigma^* - s \cdot H(m^*) = 0 \bmod p$ from the formula described above for p is a prime number. As a is chosen from R_q randomly, the probability of $a = 0 \bmod p$ is close to $1/p^n$, which is negligible. Hence it can be concluded that $\sigma^* - s \cdot H(m^*) = 0 \bmod p$, and the private key s can be obtained. 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 1.

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 3.0 GHz, with 1.0 GB of RAM. The implementation uses Shoup's NTL library [18] version 5.5.2 for high-level numeric algorithms, and the code is compiled using Microsoft Visual C++ 6.0 compiler.

Tables 2 and 3 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 Tables 2 and 3, 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.

A more detailed simulation result of the two above-described schemes is given in Fig. 1. Figure 1a, b, c show 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. 1d. At the same time, Fig. 1 also indicates 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. 1, the efficiency of the scheme from R-LWE is more eximious to the RSA signature scheme, and the increasing tendency of the scheme from R-LWE in

Table 1 Efficiency analysis of the scheme from R-LWE

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

Table 2 Implementation time of the scheme from R-LWE

Security parameter n	KeyGen (ms)	Signature (ms)	Verification (ms)	Total time (ms)
128	14.1	15.3	28.7	58.6
256	37.0	34.6	68.4	140.0
512	121.8	121.8	240.4	484.0
1024	443.8	440.4	909.2	1793.4
2048	1687.2	1699.8	3531.2	6918.2
4096	6578.1	6685.9	13,252.7	26,516.7

Table 3 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	31,249.6	9539.7	47.7	40,837
4096	217,288.3	121,170.0	172.0	338,630.3

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.

4 Identity-Based Encryption

4.1 Definition

Definition 1 *([18])* An identity-based encryption (IBE) scheme is a tuple of PPT algorithms $(\mathrm{IBE}\mathit{Setup}, \mathrm{IBE}\mathit{Der}, \mathrm{IBE}\mathit{Enc}, \mathrm{IBE}\mathit{Dec})$ such that:

- $\mathrm{IBE}\mathit{Setup}(1^n)$: Take as input a security parameter 1^n. Output a master public key PK and a master secret key msk.
- $\mathrm{IBE}\mathit{Der}(msk, id)$: Take as input the master secret key msk and an identity id. Return the corresponding decryption key SK_{id}, and note $SK_{id} \leftarrow \mathrm{IBE}\mathit{Der}_{msk}(id)$.
- $\mathrm{IBE}\mathit{Enc}(PK, id, M)$: Take as input the master public key PK, an identity id and a message M in some message space. Output a ciphertext C, and note $C \leftarrow \mathrm{IBE}\mathit{Enc}_{PK}(id, M)$.
- $\mathrm{IBE}\mathit{Dec}(SK_{id}, id, C)$: Take as input an identity id, an associated decryption key SK_{id} and a ciphertext C. Output a message M or the symbol $\perp$ (which is not in the message space), and note $M \leftarrow \mathrm{IBE}\mathit{Dec}_{SK_{id}}(id, C)$.

It is required that for all (PK, msk) output by $\mathrm{IBE}\mathit{Setup}$, all id, all SK_{id} output by $\mathrm{IBE}\mathit{Der}$, all M in the message space and all C output by $\mathrm{IBE}\mathit{Enc}$ we have $\mathrm{IBE}\mathit{Dec}_{SK_{id}}(id, C) = M$.

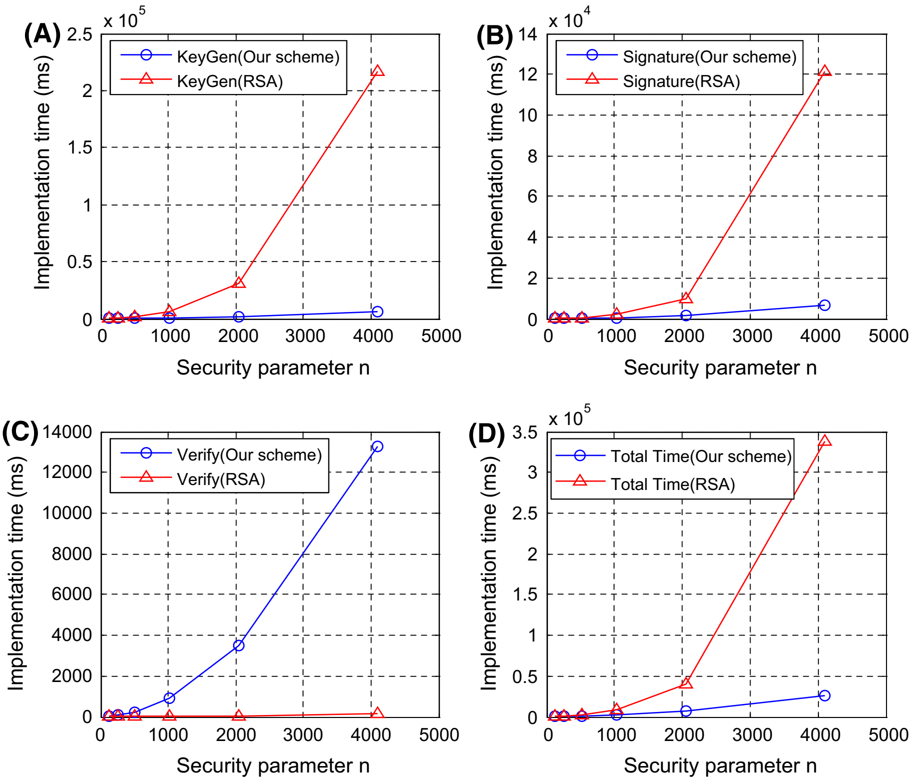

Fig. 1 Efficiency comparison of the signature scheme from R-LWE and RSA scheme

4.2 Encryption Scheme

Let $H_1 : \{0, 1, \ldots, q-1\}^* \rightarrow Z_q^n$ be a random oracle that maps identities to the elements of Z_q^n. Based on R-LWE problem, an efficient IBE scheme $\mathcal{IBE}$ can be constructed as follows.

- IBE$Setup(1^n)$: Take as input a security parameter 1^n, $m \geq Cn\lg q$ ($m = 2^d, d \in Z$ and $C > 1$ is a fixed constant) and a prime modulus $q = 1 \bmod (2\mathrm{m})$. Run $TrapGen(q, n)$ to get a matrix $A \in Z_\mathrm{q}^{\mathrm{n}\times\mathrm{m}}$ and a trapdoor $T \subset \Lambda_\mathrm{q}^{\perp}(A)$, where T is master secret key.
- IBE$Der(T, id)$: (1) If the pair (id, SK_{id}) is in local storage, return SK_{id}; (2) Otherwise, let $u = H_1(id)$ and run $Sample$ISIS$(A, T, \sigma, u)(\sigma \geq ||T|| \cdot \omega(\sqrt{\log n}))$ to get a private key SK_{id}. Store (id, SK_{id}) locally and return SK_{id}; (3) Let public key $PK = (a, b) = (a, a \cdot SK_{id} + e)$, where $a \leftarrow R_q$ is uniformly random and e is some "small" random error term chosen from a probability distribution $\chi \subset R_q$ described in Sect. 3.
- IBE$Enc(PK, id, M)$: To encrypt a message $M \in \{0, 1\}^m \subset R_q$ (view it as an element of R_q by using its bits as the 0–1 coefficients of a polynomial), choose a "small" $t \in R_q$ at random (namely, the coefficient of t is small). Output the ciphertext $(c_1, c_2) = (a \cdot t + e_1, b \cdot t + e_2 + [q/2] \cdot M) \in R_q \times R_q$, where e_1, e_2 are "small" random error terms chosen from the distribution χ.

- IBE$Dec(SK_{id}, id, (c_1, c_2))$: Compute $M' = c_2 - c_1 \cdot SK_{id}$. Output 0 if the coefficient $m_i'(i = 0, 1, \cdots, m-1)$ of M' is closer to 0 than to $[q/2]$ modulo q, otherwise output 1.

Where polynomial addition is the usual coordinate-wise addition, "·" denotes the usual polynomial multiplication followed by reduction modulo $x^n + 1$.

Claim 3 *The IBE scheme $\mathcal{IBE}$ is correct.*

Proof Consider a ciphertext

$$(c_1, c_2) = (a \cdot t + e_1, b \cdot t + e_2 + [q/2] \cdot M) \in R_q \times R_q$$

of an m-bit message $M \in \{0,1\}^m$ under the public key $(a, b = a \cdot SK_{id} + e)$, then the decryption process can be computed as

$$\begin{aligned} M' &= c_2 - c_1 \cdot SK_{id} \\ &= b \cdot t + e_2 + [q/2] \cdot M - (a \cdot t + e_1) \cdot SK_{id} \\ &= (a \cdot SK_{id} + e) \cdot t + e_2 + M \cdot [q/2] - (a \cdot t + e_1) \cdot SK_{id} \\ &= M \cdot [q/2] + (e \cdot t + e_2 - e_1 \cdot SK_{id}) \end{aligned}$$

Obviously the coefficient of private key SK_{id} is small as SK_{id} is obtained from algorithm $Sample$ISIS(A, T, σ, u), and $e, e_1, e_2, t \in R_q$ are "small" polynomials. Hence it outputs the coefficient $m_i(i = 0, 1, \ldots, m-1)$ of M if the coefficients of $(e \cdot t + e_2 - e_1 \cdot SK_{id})$ are at distance at most $q/5$ from 0 (modulo q) via choosing a big prime modulus q.

4.3 Security Analysis

Claim 4 *The IBE scheme $\mathcal{IBE}$ is secure against chosen-plaintext attacks (denoted IND-ID-CPA) in the random oracle model, assuming that the R-LWE is hard.*

Proof Let $\mathcal{A}$ be a PPT adversary that distinguishes between encryptions of messages of its choice on some identity with advantage ε in a chosen-plaintext attack. The adversary $\mathcal{A}$ works as follows:

- *Setup* The challenger takes a security parameter 1^n and runs IBE$Setup(1^n)$ to get a matrix $A \in Z_{\mathrm{q}}^{\mathrm{n \times m}}$ and a trapdoor $T \subset \Lambda_{\mathrm{q}}^{\perp}(A)$, where T is master secret key.
- *Queries*1 $\mathcal{A}$ issues private key extraction queries $q_{id_j}(j = 1, \ldots, \mathrm{s})$. If the pair (id_j, SK_{id_j}) is in local storage, return SK_{id_j} and corresponding public key $PK_j = (a, a \cdot SK_{id_j} + e)$ $(j = 1, \ldots, \mathrm{s})$ to $\mathcal{A}$. Otherwise, let $u = H_1(id_j)$ and run $Sample$ISIS(A, T, σ, u) to get a private key SK_{id_j}, and return SK_{id_j} and public key $PK_j = (a, a \cdot SK_{id_j} + e)$.
- *Challenge* After the queries, $\mathcal{A}$ outputs two different plaintexts $M_0, M_1 \in \{0,1\}^m$ and a "target" identity ID^*, where the ID^* may not be be queried before. A bit $b \in \{0,1\}$ is randomly chosen and the adversary is given a "challenge ciphertext"

$$(a \cdot t + e_1, b \cdot t + e_2 + [q/2] \cdot M_b) \leftarrow \text{IBE}Enc(PK^*, ID^*, M_b).$$

- *Queries*2 $\mathcal{A}$ may continue to issue more extraction queries $q_{id_j}(j = s+1, \ldots, t)$ to get corresponding private key and public key, where the only constraint is $q_{id_j} \neq ID^*(j = s+1, \ldots, t)$.
- *Output* $\mathcal{A}$ outputs a guess b'.

To prove the security of the scheme, we construct a distinguisher D between the two distributions

$$\{(a, a \cdot SK_{ID^*} + e) : a \leftarrow R_q, SK_{ID^*} \in R_q, e \leftarrow \chi\} \quad \text{and} \quad \{\text{Unif}(R_q \times R_q)\}$$

D takes as input a pair of polynomials $(a \in R_q, c \in R_q)$, and runs the adversary $\mathcal{A}$ with (a, b) $(b = a \cdot SK_{ID^*} + e)$ as the public key. Upon receiving messages $M_0, M_1 \in \{0,1\}^m$ from the adversary, D chooses $b \in \{0,1\}$ and $t \in R_q$ at random, returns the challenge ciphertext $(a \cdot t + e_1, c \cdot t + e_2 + [q/2] \cdot M_b)$, and then outputs 1 if $\mathcal{A}$ guesses the right b, and 0 otherwise.

On the one hand, if c is uniformly random, then the challenge ciphertext is also random, regardless of the multiplication and addition. Hence in this case D outputs 1 with probability at most 1/2. On the other hand, if $c = a \cdot SK_{ID^*} + e$, then the challenge ciphertext is $(a \cdot t + e_1, (a \cdot SK_{ID^*} + e) \cdot t + e_2 + [q/2] \cdot M_b)$. This is identical to the output distribution of IBE$Enc(PK^*, ID^*, M_b)$, by assumption $\mathcal{A}$ will guess the right b with probability $(1 + \varepsilon)/2$, which means that D outputs 1 with the same probability, hence D has advantage at least $\varepsilon/2$. Therefore if $\mathcal{A}$ can distinguish between encryptions of messages of its choice on the "target" identity ID^*, then D can distinguish between the two distributions $(a, a \cdot SK_{ID^*} + e)$ and $\{\text{Unif}(R_q \times R_q)\}$, namely, D can solve R-LWE problem successfully.

The efficiency of the IBE scheme will be discussed in Sect. 5.

5 CCA-secure encryption from R-LWE

5.1 Definition

Definition 2 ([22]) A public-key encryption scheme is secure against adaptive chosen-ciphertext attacks (CCA-secure) if the advantage of any PPT adversary $\mathcal{A}$ in the following game is negligible in the security parameter n:

- *Setup* Challenger runs algorithm $Setup(1^n)$ and outputs (PK, SK). Adversary $\mathcal{A}$ is given 1^n and PK.
- *Queries1* The adversary may make polynomially-many queries $q_1, \ldots, q_s$ to a decryption oracle $Decry_{SK}(\cdot)$.
- *Challenge* At some point, $\mathcal{A}$ outputs two messages $M_0, M_1 \in \{0,1\}^m$. A bit $b \in \{0,1\}$ is randomly chosen and $\mathcal{A}$ is given a "challenge ciphertext" $C^* \leftarrow Encry_{PK}(M_b)$.
- *Queries2* $\mathcal{A}$ may continue to make queries $q_j (j = s+1, \ldots, t)$ to $Decry_{SK}(\cdot)$ except that it may not request the decryption of C^*.
- *Output* $\mathcal{A}$ outputs a guess b'.

We say that $\mathcal{A}$ succeeds if $b' = b$, and denote the probability of this event by $\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[Succ]$. The adversary's advantage is defined as $Adv^{PKE}_{\mathcal{A},\mathcal{E}} = |\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[Succ] - 1/2|$.

5.2 Encryption Scheme

Adopting the construction paradigm of Boneh et al., based on the IBE scheme $\mathcal{IBE} = (\text{IBE}Setup, \text{IBE}Der, \text{IBE}Enc, \text{IBE}Dec)$ in Sect. 4 and the signature scheme $\mathcal{S} = (KeyGen, Sign, Verify)$ in Sect. 3, a CCA secure public-key encryption scheme $\mathcal{E} = (Setup, Encry, Decry)$ is constructed as follows.

- *Setup* Run IBE*Setup*(1^n) to get a matrix $A \in Z_q^{n\times m}$ and a trapdoor $T \subset \Lambda_{\mathrm{q}}^{\perp}(A)$, where T is master secret key.
- *Encry* To encrypt a message $M \in \{0,1\}^m$, the sender performs the following operations:

  1. Run $KeyGen(1^n)$ to obtain verification key vk and signing key sk.
  2. Run IBE$Der(T, vk)$ (verification key vk is viewed as a identity) to obtain public key (a, b) and encrypt M with respect to the vk: $(c_1, c_2) \leftarrow \mathrm{IBE}Enc(PK, vk, M)$, where $(c_1, c_2) \leftarrow (a\cdot t + e_1, b\cdot t + e_2 + [q/2]\cdot M)$.
  3. Compute $(\sigma_1, \sigma_2) \leftarrow Sign(sk, (c_1, c_2)) = (Sign(sk, c_1), Sign(sk, c_2))$ and output the ciphertext $(vk, (c_1, c_2), (\sigma_1, \sigma_2))$.

- *Decry*: After receiving ciphertext $(vk, (c_1, c_2), (\sigma_1, \sigma_2))$, the receiver first checks whether $Verify(vk, (c_1, c_2), (\sigma_1, \sigma_2)) \overset{?}{=} 1$, if not, output $\perp$. Otherwise, the receiver runs IBE$Der(T, vk)$ to obtain private key SK_{vk} and outputs $M \leftarrow \mathrm{IBE}Dec(SK_{vk}, vk, (c_1, c_2))$.

Claim 5 *The public-key encryption scheme $\mathcal{E}$ is correct.*

Proof It is clear that the encryption scheme $\mathcal{E}$ satisfies correctness from Claim 3.

5.3 Security Analysis

Claim 6 *The public-key encryption scheme $\mathcal{E}$ is CCA-secure in the random oracle model.*

Proof Let $\mathcal{A}$ be a PPT adversary attacking the encryption scheme $\mathcal{E}$ in an adaptive chosen-ciphertext attack. Define a ciphertext (vk, C, σ) is valid if $Verify(C, \sigma) = 1$. Let (vk^*, C^*, σ^*) be the challenge ciphertext received by $\mathcal{A}$, and Φ denote the event that "$\mathcal{A}$ submits a valid ciphertext (vk^*, C, σ) to the decryption oracle", assuming vk^* is chosen at the beginning of the game. Then the following propositions are correct.

Proposition 1 $\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[\Phi]$ *is negligible.*

Proposition 2 $|\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[Succ \wedge \bar{\Phi}] + \frac{1}{2}\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[\Phi] - \frac{1}{2}|$ *is negligible.*

As

$$\begin{aligned}
&\left|\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[Succ] - 1/2\right| \\
&\quad\le \left|\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[Succ \wedge \Phi] - \frac{1}{2}\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[\Phi]\right| + \left|\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[Succ \wedge \bar{\Phi}] + \frac{1}{2}\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[\Phi] - \frac{1}{2}\right| \\
&\quad\le \frac{1}{2}\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[\Phi] + \left|\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[Succ \wedge \bar{\Phi}] + \frac{1}{2}\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[\Phi] - \frac{1}{2}\right|
\end{aligned}$$

Hence the adversary's advantage is negligible if the propositions described above are correct.

The correctness of Proposition 1 is straightforward. Let $\mathcal{F}$ be a PPT forger who forges a signature with respect to the scheme $\mathcal{S}$ with probability exactly $\Pr^{PKE}_{\mathcal{A},\mathcal{E}}[\Phi]$. Security of $\mathcal{S}$ implies the Proposition 1 is correct from Claim 2 in Sect. 3.

Proof of Proposition 2 A PPT adversary $\mathcal{A}'$ attacking the IBE scheme $\mathcal{IBE}$ can be constructed using $\mathcal{A}$ as follows:

1. *Setup* $\mathcal{A}'$ runs *KeyGen* to get $(vk^* \in R_q \times R_q, sk^* \in R_q)$ and outputs a "target" identity $ID^* = vk^*$. $\mathcal{A}'$ is given the public key PK_{vk^*}, then $\mathcal{A}'$ runs $\mathcal{A}(1^n, PK_{vk^*})$ in turn.
2. *Queries*1 When $\mathcal{A}$ makes decryption oracle query $Decry(vk, (c_1, c_2), (\sigma_1, \sigma_2))$, $\mathcal{A}'$ proceeds as follows:

    1. If $vk = vk^*$ then $\mathcal{A}'$ checks whether $Verify(vk^*, (c_1, c_2), (\sigma_1, \sigma_2)) = 1$. If so, $\mathcal{A}'$ aborts and outputs a random bit. Otherwise, it outputs $\perp$.
    2. If $vk \neq vk^*$ and $Verify(vk, (c_1, c_2), (\sigma_1, \sigma_2)) = 0$, $\mathcal{A}'$ outputs $\perp$.
    3. If $vk \neq vk^*$ and $Verify(vk, (c_1, c_2), (\sigma_1, \sigma_2)) = 1$, $\mathcal{A}'$ makes the private key extraction query IBE$Der(T, vk)$ to get SK_{vk}. It then computes $m \leftarrow$ IBE$Dec(SK_{vk}, vk, (c_1, c_2))$ and returns m to $\mathcal{A}$.

3. *Challenge* At some point, $\mathcal{A}$ outputs two messages $M_0, M_1 \in \{0,1\}^m$. After $\mathcal{A}'$ sends M_0, M_1 to challenger, A bit $b \in \{0,1\}$ is randomly chosen and $\mathcal{A}'$ is given a "challenge ciphertext" $(c_1^*, c_2^*) \leftarrow$ IBE$Enc(PK_{vk^*}, vk^*, M_b)$, $\mathcal{A}'$ then computes $(\sigma_1^*, \sigma_2^*) \leftarrow Sign(sk^*, (c_1^*, c_2^*))$ and returns $(vk^*, (c_1^*, c_2^*), (\sigma_1^*, \sigma_2^*))$ to $\mathcal{A}$.
4. *Queries*2 $\mathcal{A}$ may continue to make queries to $Decry_{SK}(\cdot)$ except that it may not request the decryption of $(vk^*, (c_1^*, c_2^*), (\sigma_1^*, \sigma_2^*))$, and $\mathcal{A}'$ answers them as before.
5. *Output* $\mathcal{A}$ outputs a guess b', and $\mathcal{A}'$ outputs the same guess b'.

As $\mathcal{A}'$ never requests the secret key corresponding to the "target" identity vk^*, $\mathcal{A}'$ is a legal PPT adversary. When $\mathcal{A}$ can not submit a valid ciphertext (vk^*, C, σ), $\mathcal{A}'$ provides a perfect simulation for $\mathcal{A}$. It is easy to see that:

$$\begin{aligned}\left|\Pr_{\mathcal{A}',\mathcal{E}'}^{IBE}[Succ] - \frac{1}{2}\right| &= \left|\Pr_{\mathcal{A}',\mathcal{E}'}^{IBE}[\bar{\Phi} \wedge Succ] + \Pr_{\mathcal{A}',\mathcal{E}'}^{IBE}[\Phi \wedge Succ] - \frac{1}{2}\right| \\ &= \left|\Pr_{\mathcal{A},\mathcal{E}}^{PKE}[Succ \wedge \bar{\Phi}] + \Pr_{\mathcal{A}',\mathcal{E}'}^{IBE}[Succ] \cdot \Pr_{\mathcal{A},\mathcal{E}}^{PKE}[\Phi] - \frac{1}{2}\right| \\ &= \left|\Pr_{\mathcal{A},\mathcal{E}}^{PKE}[Succ \wedge \bar{\Phi}] + \frac{1}{2}\Pr_{\mathcal{A},\mathcal{E}}^{PKE}[\Phi] - \frac{1}{2}\right|\end{aligned}$$

Obviously $\left|\Pr_{\mathcal{A}',\mathcal{E}'}^{IBE}[Succ] - \frac{1}{2}\right|$ is negligible from Claim 4 in Sect. 4, hence Proposition 2 is correct.

5.4 Efficiency Analysis

It is easy to see that the efficiency of the CCA-secure scheme $\mathcal{E}$ is decided by the efficiency of the the IBE scheme $\mathcal{IBE}$ and the signature scheme $\mathcal{S}$ from its encryption process. Because of the special algebraic structure of R-LWE and the method of contribution, the schemes $\mathcal{IBE}$ and $\mathcal{S}$ from the R-LWE problem have the advantages of much simpler description, analysis and high efficiency.

Compared to the CCA-secure encryption schemes presented in [3] and [14], the efficiency improvement of the scheme $\mathcal{E}\ominus$ is shown in Table 4. Where m denotes the message size in our scheme, and it denotes the number of the samples in [3] and [14]. q is a prime modulus and k is a security parameter.

Table 4 Efficiency comparison between the scheme $\mathcal{E}$ and the schemes in [3] and [14]

Cryptosystem	Peikert [3]	Yang [14]	Our scheme $\mathcal{E}$
Private key size	$k[2m^2 + n(m + l)] \log q$	$2m^2n^2 \log q$	$m \log q$
Public key size	$kn(m + l) \log q$	$(2kmn + nl) \log q$	$2m \log q$
Message size (bit)	l	nl	m
Ciphertext size	$(km + l) \log q$	$(kmn + nl) \log q$	$6m \log q$
Expansion	$(km/l + 1) \log q$	$(km/l + 1) \log q$	$6 \log q$
Worst-case problem	GapSVP/SIVP	Ideal-SVP	Ideal-SVP
Operation	Matrix operation	Vector operation	Vector operation

The datum in Table 4 shows that the encryption scheme $\mathcal{E}$ is more efficient than other two cryptosystems, especially its expansion, private key, public key and ciphertext size are incomparable to the Peikert's and Yang's CCA-secure scheme. The expansion of our scheme is invariable with the increase of the security parameter n and message size m while other two schemes don't have the property, and this property make it's advantage is more obvious when security parameter is large.

6 Conclusion

Owing to the flexible structure and implementation simplicity of lattice cryptography, an efficient identity-based encryption (IBE) scheme from R-LWE are proposed, whose security is reducible to the hardness of the shortest vector problem (SVP) in the worst case on ideal lattices. Then we construct a CCA-secure public key cryptosystem based on the IBE scheme adopting the construction paradigm of Boneh et al. The scheme mainly uses modular addition and modular multiplication operations in the ring of integer polynomials, and which based on the special algebraic structure of R-LWE, hence it is more efficient than previous interrelated cryptosystems, and analysis also indicates the efficiency of the CCA-secure $\mathcal{E}$ is more efficient.

Future work mainly includes optimization of the construction of the CCA-secure public key cryptosystem, in order to test the feasibility of the system in the practical application environment, further simulation and analysis of the system running efficiency will be implemented. We also plan to study the latticed-based signature and encryption schemes in the standard model.

Acknowledgements This work is supported by the National Natural Science Foundation of China (61171072) and the Science and Technology Plan Projects of Shenzhen (ZDSYS20140430164957660, JCYJ20150324141711562, JCYJ20150324141711665, JCYJ20150324140036830, 20160224144857159, GJHZ20160226202520268).

References

1. Ajtai, M. & Dwork C. (1997). A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the 29th ACM Symposium on Theory of Computing (STOC)* (pp. 284–293). El Paso, TX, USA.
2. Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the of 37th ACM Symposium on Theory of Computing (STOC)* (pp. 84–93). May 22–24.

3. Peikert, C. (2009). Public-key cryptosystems from the worst-case shortest vector problem. In *Proceedings of 41th ACM Symposium on Theory of Computing (STOC)* (pp. 333–342). May 31–June 2.
4. Gentry, C., Peikert, C. & Vaikuntanathan, V. (2008). Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th ACM Symposium on Theory of Computing (STOC)* (pp. 197–206). May 17–20.
5. Cash, D., Hofheinz, D., Kiltz, E. & Peikert, C. (2010). Bonsai trees, or how to delegate a lattice basis. In *Proceedings of the 29th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)* (pp. 523–552). May 30–June 3.
6. Klivans, A. R. & Sherstov, A. A. (2006). Cryptographic hardness for learning intersections of halfspaces. In *Proceedings of the 47th Symposium on Foundations of Computer Science (FOCS)* (pp. 553–562). October 21–24.
7. Peikert, C., Vaikuntanathan, V. & Waters, B. (2008). A framework for efficient and composable oblivious transfer. In *Proceedings of the 28th International Cryptology Conference (CRYPTO)* (pp. 554–571). August 17–21.
8. Akavia, A., Goldwasser, S. & Vaikuntanathan, V. (2009). Simultaneous hardcore bits and cryptography against memory attacks. In *Proceedings of the 6th Theory of Cryptography Conference (TCC)* (pp. 474–495). March 15–17.
9. Agrawal, S., Boneh, D. & Boyen, X. (2010). Efficient lattice (H) IBE in the standard model. In *Proceedings of the 29th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)* (pp. 553–572). May 30–June 3.
10. Lyubashevsky, V., Peikert, C. & Regev, O. (2010). On ideal lattices and learning with errors over rings. In *Proceedings of the 29th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)* (pp. 1–23). May 30–June 3.
11. Ting, W., Jianping, Y., Peng, Z., & Yong, Z. (2016). Efficient signature schemes from R-LWE. *KSII Transactions on Internet and Information Systems, 10*(8), 3911–3924.
12. Brakerski, Z., Vaikuntanathan, V. (2011). Fully homomorphic encryption from ring-LWE and security for key dependent messages. In *Proceedings of the 31th Annual International Cryptology Conference on Advances in Cryptology*, August (pp. 505–524).
13. Ting, W., Jianping, Y., Peng, Z., & Xuan, X. (2014). Efficient linear homomorphic encryption from LWE over rings [J]. *Wireless Personal Communications, 74*(2), 1005–1016.
14. Yang, X., Wu, L., Zhang, M., & Zhang, W. (2013). Public-key encryption scheme based on R-LWE. *Journal on Communications, 34*(2), 23–30.
15. Dolev, D., Dwork, C., & Naor, M. (2000). Non-malleable cryptography. *SIAM Journal on Computing, 30*(2), 391–437.
16. Naor, M. & Yung, M. (1990). Public-Key Cryptosystems provably-secure against chosen-ciphertext attacks. In *Proceedings of the 22nd ACM Symposium on Theory of Computing (STOC)* (pp. 427–437). May 13–17.
17. Feige, U., Lapidot, D., & Shamir, A. (1999). Multiple non-interactive zero-knowledge proofs under general assumptions. *SIAM Journal on Computing, 29*(1), 1–28.
18. Boneh, D., Canetti, R., Halevi, S., & Katz, J. (2006). Chosen-ciphertext security from identity-based encryption. *SIAM Journal on Computing, 36*(5), 915–942.
19. Alwen, J. & Peikert, C. (2009). Generating shorter bases for hard random lattices. In *Proceedings of the 26th International Symposium on Theoretical Aspects of Computer Science (STACS)* (pp. 75–86). February 26–28.
20. Lyubashevsky, V. (2012). Lattice signatures without trapdoors. In *Proceedings of 31th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)* (pp. 738–755). April 15–19.
21. Shoup, V. (2010). NTL: A library for doing number theory. http://shoup.net/ntl/, Version 5.5.2, 2010.
22. Bellare, M., Desai, A., Pointcheval, D. & Rogaway, P. (1998). Relations among notions of security for public-key encryption schemes. In *Proceedings of the 18th International Cryptology Conference (CRYPTO)* (pp. 26–45). August 23–27.

Ting Wang born in Linyi, Shandong Province in December 1977. He obtained Ph.D. degree in Shenzhen University in 2014. He now is engaged in his post-doctoral study in the School of Computer Science and Technology, South China University of Technology, China. His research interests include cryptography and information security.

Guoqiang Han born in Linchuan, Jiangxi Province in August 1962. He obtained Ph.D. degree in Sun Yat-Sen University in 1988. In 1993 he was promoted as professor. From October 1997 to September 1999, Professor Han was engaged in his post-doctoral study in Tokyo University. His research interests include Multimedia Image Processing, Digital Home and Application and so on.

Jianping Yu born in 1968. He obtained Ph.D. degree in Xidian University in 1995. In 2002 he was promoted as professor. He is now the dean of College of Information Engineering in Shenzhen University, and he is also one of the principal teachers of Guangdong "Thousands-hundreds-tens Talent Project". His main research interests include cryptography, network security and information security.

Peng Zhang born in 1984. She is currently a teacher of College of Computer Science and Software Engineering in Shenzhen University, China. Her research interests include cryptography, network security and information security.

Xiaoqiang Sun born in 1989. He is currently a Ph.D. candidate in the ATR Key Laboratory of National Defense Technology, Shenzhen University, China. Her research interests include cryptography, network security and information security.