Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080221

Efficient Chosen-Ciphtertext Secure Public Key Encryption Scheme From Lattice Assumption

Fenghe Wang[1,*], *Chunxiao Wang*[1] *and Yupu Hu*[2]

[1] Department of Mathematics and Physics, Shandong Jianzhu University, Jinan , China
[2] Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University , Xi'an, China

Received: 25 Mar. 2013, Revised: 26 Jul. 2013, Accepted: 28 Jul. 2013
Published online: 1 Mar. 2014

Abstract: Using the Bonsai trees primitive and Gentry's CPA-secure (chosen-plaintext attack) public-key encryption (PKE) scheme, we propose an efficient chosen-ciphtertext secure PKE scheme over lattice. If the decision variant of the learning with errors (LWE) problem is hard and the one-time signature used in this scheme is strong unforgeable, the proposed PKE scheme is indistinguishable against the adaptive chosen-ciphtertext attack (IND-CCA2). One of the characters for this scheme is that, before any encryption operation, the encryption algorithm uses a new choice rule to fix the public parameter matrixes used in the encryption operation. With the help of this new choice rule, we can achieve the chosen-ciphtertext security with much shorter the public key size in contrast to the lattice-based encryption scheme proposed in STOC'09 by Peikert. Moreover, as a CCA-secure PKE scheme, the message-to-ciphtertext expanse factor of this scheme which is controlled efficiently is nearly closed to the message-to-ciphtertext expanse factor of Gentry's scheme which is CPA secure. Due to the quantum intractability of the LWE problem on which the scheme is based, the proposed PKE scheme is secure even in quantum-era.

Keywords: Lattice-based cryptography; chosen-ciphtertext attack; bonsai tree; learning with errors problem, message-to-ciphtertext expanse factor.

1. Introduction

Post-quantum cryptography provides the security protection even in the quantum era and it has been a hot topic in recent years. As a typical post-quantum cryptography, lattice-based cryptography has gained more and more attentions in the public key cryptography field. Regev defined a natural intermediate problem called the learning with errors (LWE) problem and gave the quantum reduction between the LWE problem and the standard lattice hard problem in 2005 [16]. Since then the LWE problem has provided the foundations for many lattice-based cryptosystems, including the PKE schemes [8,16], (H)IBE ((hierarchical) identity-based encryption) schemes [1,2,5,7], CCA-secure encryption schemes [13, 14] and others cryptosystems [6,9,10,15,17]. Peikert constructed a natural LWE- based encryption scheme which acts as a KEM (key encapsulation machine) in [13] to against the adaptive chosen-ciphtertext attack [12]. This construction can be seen as an alternative to the other CCA-secure encryption scheme in [14]. One of the interesting techniques in the construction of [13] is that $2k$ matrices are used to simulate the decryption oracle in the security proof. The other interesting techniques in [13] (also [14]) is that hybrid encryption technical is used to reduce the ciphtertext size which is important to present a higher efficiency. Even then, the public key in [13] consists of $2k + 1$ random matrices which do increase the overhead at computation, memory and transfers. So it is necessary to reduce the public key size in the lattice-based CCA-secure encryption scheme. On the other hand, note that the proposed lattice-based PKE schemes are secure against chosen-plaintext attack (CPA) and there still no an efficient lattice-based CCA-secure PKE scheme is proposed which can be used to encrypt the message directly. In fact, we can transform a lattice-based HIBE into a CCA-secure PKE scheme by [4], while the message-to-ciphtertext expanse factor (M-C factor) in this case is very large. Hence, it is interesting to build an IND-CCA2 secure PKE scheme with the small M-C factor and the short public key size.

In this paper we combine a lattice-based CPA-secure

* Corresponding author e-mail: fenghe2166@163.com

PKE scheme [8] and the bonsai trees primitive [5] to design an efficient CCA-secure PKE scheme over lattice. Based on the hardness of the decision variant LWE problem and the strong unforgeability of a one-time signature scheme, this scheme is provably IND-CCA2 secure. It is similar with [13] and [14] in this paper that we also use some random matrices to achieve the IND-CCA2 security. While it is differ from [13] that we give a new choice rule to choose the public matrices used in the encryption process. This choice rule help us successfully simulate the decryption oracle by only $k+1$ random matrices in the security proof of the proposed scheme. As a result, the public key size of the proposed scheme is efficiently reduced. Moreover, the M-C factor of this scheme is also controlled effectively. More precisely, the M-C factor is shorter than that in the CCA-secure KEM of [13] and it is only little larger than that of [**?**] which is CPA-secure.

This paper is organized as follows, Section 2 introduces some basic tools and notations for our construction; Section 3 proposes our lattice-based chosen-ciphertext secure PKE scheme and Section 4 proves the security of the proposed scheme and analyzes its efficiency. At last, we give an summarize in Section 5.

2. Primitives

2.1. Notations

Throughout the paper, we use bold lower-case letters to denote vectors in column form, and bold upper-case letters to denote matrices. Let $\|\cdot\|$ be the Euclidean norm. By convention, we say a norm of a matrix is the norm of its the longest column. If O is a description of classify the growth of functions, then the function $poly(n)$ denotes an unspecified function $f(n)=O(n^c)$ for some constant c. We see a function $g(n)$ is negligible if $g(n)=1/poly(n)$. We see a function $g(n)$ is in $\omega(f(n))$ if it grows faster than $cf(n)$ for any constant c. For any matrix $\mathbf{T}$, $\tilde{\mathbf{T}}$ denotes the Gram-Schmidt orthogonalized matrix. D_α denotes the Gaussian distribution over R with parameter α.

2.2. Lattice

Let $\mathbf{B}=\{\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_n\}$ be a set of n linearly independent vectors. The n-dimensional lattice generated by $\mathbf{B}$ is defined as $\Lambda=\{\mathbf{Bc}=\sum_{i\in[n]}c_i\mathbf{b}_i, c_i\in Z\}$, where $\mathbf{B}$ acts as a basis for this lattice. A trapdoor basis of a lattice is such a basis that vectors from this basis are the smallest vectors of this lattice. In fact, if the norms of vectors from a basis are small enough, they can still be recognized as a trapdoor basis. In cryptographic applications, any trapdoor basis is kept secret by its holder.

In our construction, more attentions should be pay to two special integer lattices which defined by a matrix $\mathbf{A}\in Z_q^{n\times m}$. More precisely, for a prime number q and a vector $\mathbf{y}\in Z_q^n$, those two lattices are defined as follows: $\Lambda_q^\perp(\mathbf{A})=\{\mathbf{x}\in Z_q^m, \mathbf{Ax}=0(\mathrm{mod}q)\}$ and $\Lambda_q^y(\mathbf{A})=\{\mathbf{x}\in Z_q^m, \mathbf{Ax}=\mathbf{y}(\mathrm{mod}q)\}$.

2.3. Learning with Errors Problem

Definition 1. *For parameters (n,m,q), $\boldsymbol{s}\in Z_q^n$ and an error distribution χ over Z_q^m , $A_{s,\chi}$ is a distribution obtained by computing $\{\boldsymbol{A},\boldsymbol{A}^t\boldsymbol{s}+\boldsymbol{x}(mod q)\}$ where $\boldsymbol{A}\in Z_q^{n\times m}$ is chosen uniformly and randomly and errors vector $\boldsymbol{x}$ is chosen according to the distribution χ. The Learning with Errors problem is defined as follows: Given a sample from $A_{s,\chi}$, output $\boldsymbol{s}$ with a noticeable probability. The decision variant LWE problem is to distinguish $A_{s,\chi}$ from the uniform distribution.*

Regev [16] shows that for certain noise distributions, denoted $\bar{\Phi}_\alpha^m$, the LWE problem is as hard as the worst-case SIVP problem (shortest independent vectors problem) under a quantum reduction. This standard error distribution $\bar{\Phi}_\alpha^m$ is a Gaussian distribution over Z_q^m with deviation $q\alpha>\sqrt{n}$. We can sample an errors vector according to the distribution $\bar{\Phi}_\alpha^m$ as follows: Sample m numbers $\eta_1,\eta_2,\cdots\eta_m$ according to a Gaussian distribution D_α over R , and compute $e_i=\lfloor q\eta_i\rceil(\mathrm{mod}q)$ where symbol $\lfloor x\rceil$ denotes the closest integer to x. Then let $\mathbf{e}=(e_1,\cdots,e_m)$ be an error vector in the LWE problem.

We should note that a trapdoor basis $\mathbf{T}$ of lattice $\Lambda_q^\perp(\mathbf{A})$ can be used to solve a LWE instance $\mathbf{y}=\mathbf{A}^t\mathbf{s}+\mathbf{e}(\mathrm{mod}q)$ as follows and more details are referred to [**?**].

1. Compute $\mathbf{Ty}=\mathbf{Te}(\mathrm{mod}q)$. Due to the fact that both $\mathbf{T}$ and $\mathbf{e}$ with short norm, then $\mathbf{Te}(\mathrm{mod}q)=\mathbf{Te}$ holds with an overwhelming probability.
2. Compute $\mathbf{e}=\mathbf{T}^{-1}\mathbf{Te}(\mathrm{mod}q)$.
3. Find vector $\mathbf{s}$ from $\mathbf{A},\mathbf{e},\mathbf{y}$.

2.4. Discrete Gaussian Distribution

The Gaussian distribution over lattice has been widely used in the lattice-based cryptography. The Gaussian function on R^m with parameter $\sigma>0$ can be defined as: $\rho_\sigma(x)=\exp(\pi||x||/\sigma^2)$. For a matrix $\mathbf{A}\in Z_q^{n\times m}$, the discrete Gaussian distribution on lattice $\Lambda_q^\perp(\mathbf{A})$ is defined by

$$D_{\Lambda_q^\perp(\mathbf{A}),\sigma}(x)=\frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\Lambda_q^\perp(\mathbf{A}))}.$$

In fact, the distribution $D_{\Lambda_q^\perp(\mathbf{A}),\sigma}(x)$ can be viewed as a "conditional" distribution, resulting from sampling

$\mathbf{x} \in R^n$ from a Gaussian with the parameter σ, and under the condition of the event $\mathbf{x} \in \Lambda_q^{\perp}(\mathbf{A})$.

For an n-dimension lattice Λ and positive real number $\epsilon > 0$, there is an important notion called the smoothing parameter $\eta_\epsilon(\Lambda)$ which is defined to be the smallest positive σ such that $\rho_{1/\sigma}(\Lambda^* \backslash \{0\}) \leq \epsilon$ [11]. The key property of the smoothing parameter is that if $\sigma > \eta_\epsilon(\Lambda)$, then every coset of the lattice Λ has roughly equal mass. Moreover, for almost all matrixes $\mathbf{A} \in Z_q^{n \times m}$, there is a negligible ϵ such that $\eta_\epsilon(\Lambda_q^{\perp}(\mathbf{A}))$ is less than $\omega(\sqrt{\log m})$.

We recall two main results in the lattice-based cryptography as the following Propositions which are important to our constructions. More details can be found in [5,3].

Proposition 1.*[5] (Bonsai tree)Let $\boldsymbol{B}_S$ be a trapdoor basis of lattice $\Lambda_q^{\perp}(\boldsymbol{A}_S)$ where $\boldsymbol{A}_S \in Z_q^{n \times m}$, whose columns generate the entire group Z_q^n. Let $\boldsymbol{A}' \in Z_q^{n \times m'}$ be a arbitrary matrix and $s \geq \|\tilde{\boldsymbol{B}}_S\| \omega(\log n)$ be a Gaussian parameter. Hence, there exists a probabilistic polynomial-time (PPT) algorithm $ExBasis(\boldsymbol{B}_S, \boldsymbol{A} = (\boldsymbol{A}', \boldsymbol{A}_S), s)$ that outputs a trapdoor basis $\boldsymbol{T}$ of the lattice $\Lambda_q^{\perp}(\boldsymbol{A})$ satisfying $\|\tilde{\boldsymbol{T}}\| \leq \|\tilde{\boldsymbol{B}}_S\|$.*

Proposition 1 as know as the bonsai trees primitive, shows that a trapdoor basis of the lattice $\Lambda_q^{\perp}(\mathbf{A}_S)$ can be used to sample a trapdoor basis of relate lattice $\Lambda_q^{\perp}((\mathbf{A}', \mathbf{A}_S))$.

Proposition 2.*[3] (The Trapdoor Sampling Algorithm)There is a PPT algorithm that, on input 1^n, outputs a matrix $\boldsymbol{A} \in Z_q^{n \times m}$, and a full-rank set $\boldsymbol{S}$, where the distribution of $\boldsymbol{A}$ is statistically close to the uniform distribution over $Z_q^{n \times m}$ and $\|\boldsymbol{S}\| \leq O(n \log q)$. In particularly, the set $\boldsymbol{S}$ can be efficiently converted to be a trapdoor basis of the lattice $\Lambda_q^{\perp}(\boldsymbol{A})$.*

Proposition 2 shows how to sample an essentially uniform matrix $\mathbf{A} \in Z_q^{n \times m}$ with a trapdoor basis of lattice $\Lambda_q^{\perp}(\mathbf{A})$.

2.5. Gentry's Encryption Scheme

We introduce Gentry's encryption scheme as follows. The details are referred to [**?**].

KeyGen Run the trapdoor sampling algorithm in Proposition 2 to obtain a matrix $\mathbf{A} \in Z_q^{n \times m}$ together with a trapdoor basis $\mathbf{T}$ of lattice $\Lambda_q^{\perp}(\mathbf{A})$. Matrix $\mathbf{A}$ is the public key and $\mathbf{T}$ the secret key.

Encryption To encrypt a message $\mathbf{M} \in Z_2^{m \times m}$, choose a uniform random matrix $\mathbf{S} \in Z_q^{n \times m}$ and an "error matrix" $\mathbf{X} \in Z_q^{m \times m}$ according to the distribution $\bar{\Phi}_\alpha^{m \times m}$. Output the ciphertext $\mathbf{C} = \mathbf{A}^t\mathbf{S} + 2\mathbf{X} + \mathbf{M} (\mathrm{mod} q)$.

Decryption Computes $\mathbf{E} = \mathbf{T}^t\mathbf{C} (\mathrm{mod} q)$, and then output $\mathbf{M} = \mathbf{T}^{-t}\mathbf{E} (\mathrm{mod} 2)$.

Gentry's encryption scheme is CPA-secure and its correctness is used to prove that the correctness of our scheme is satisfied. Moreover it is clear that the M-C factor of this scheme is $\log q$.

2.6. One-time Signature Scheme

Definition 2.*A signature scheme is a triple of the PPT algorithms as follows: **KeyGen**. Outputs a verification key vk and signing key sk. **Sign**.Given sk and a message μ, outputs a signature σ. **Verification**. Given a verification key vk, a message μ and a signature σ, either accepts the signature or rejects the signature for message μ.*

The notion of the security we required in our construction is the strong existential unforgeability under one-time chosen-message attack which defined as follows: generate vk and sk by the KeyGen algorithm and sends vk to the adversary. And then choose a message μ and computes its signature σ, sends σ to the adversary. The adversary wins the game if he can output some $(\mu^*, \sigma^*) \neq (\mu, \sigma)$ which can be accepted by the Verification algorithm. The signature scheme is a one-time strong existential unforgeable signature if the advantage of any adversary in above game is negligible.

2.7. IND-CCA2 Security of the Encryption Scheme

Definition 3.*A Cryptosystem is indistinguishable against adaptive chosen-ciphtertext attack (IND-CCA2) if for any efficient adversary, its advantage in the follows attack game is negligible.*

***Setup Phase**. The challenger runs the key generation algorithm to generate the public key and the secret key of the cryptosystem. The challenger sends the public key to the adversary.*

***Decryption query**. The adversary makes a series of arbitrary queries to the decryption oracle. The decryption oracle decrypts the queried ciphertext into corresponding plaintext, sends the plaintext to the adversary.*

***Challenge**. The adversary prepares two messages M_0, M_1 with the same length, and sends them to the encryption oracle. The encryption oracle randomly chooses a bit $b \in \{0, 1\}$, encrypts M_b into a target ciphtertext c_b.*

***Decryption query**. The adversary continues to submit a series of arbitrary queries to the decryption oracle except $c = c_b$.*

***Guess**. At lastly, the adversary should output a guess b'. If $b' = b$ the adversary wins the attack game.*

The advantage of the adversary in above game is defined to be $adv = |p(b = b') - 1/2|$.

3. Lattice-based CCA-secure Encryption Scheme

Parameters. Let n be a secure parameter and $m = \lfloor 8n \log q \rfloor$ for $q = poly(n)$. An errors distribution

parameter $\alpha = 1/poly(n)$. There is a Gaussian sample parameter s which is the same as the definition of the Proposition 1. Let k be the length of the verification key in a strong unforgeable one-time signature scheme.

Key Generation. Let Ssign be a strong unforgeable one-time signature scheme whose verification key is $vk \in \{0,1\}^k$. We assume that the hamming weight l of the verification key equals to $\lfloor k/2 \rfloor$ or $\lfloor k/2 \rfloor + 1$. Runs the trapdoor sampling algorithm in Proposition 2, outputs a matrix $\mathbf{A}$ statistically close to the uniform distribution and the trapdoor basis $\mathbf{T}$ of the lattice $\Lambda_q^{\perp}(\mathbf{A})$. Randomly chooses matrixes $\mathbf{A}_i \in Z_q^{n\times m}$ for $i = 1, 2, \cdots, k$. Then, the public keys are matrixes $(\mathbf{A}, \mathbf{A}_i)$ and secret key is $\mathbf{T}$.

Encryption To encrypt a message $\mathbf{M} \in Z_2^{(l+1)m\times(l+1)m}$, the encryption algorithm operates the following steps:

Step 1. Chooses a signing key sk and a verification key vk whose hamming weigh is l. Set $vk = (vk_1, vk_2, \cdots, vk_k)$ where $vk_i \in \{0,1\}$.

Step 2. Chooses public matrixes $\mathbf{A}_i$ as follows, if $vk_i = 1$, matrix $\mathbf{A}_i$ is chosen, otherwise, if $vk_i = 0$, no matrix is chosen. Supposing $vk_{j_i} = 1$ where $i = 1, 2, \cdots, l$, then let $\overline{\mathbf{A}} = (\mathbf{A}, \mathbf{A}_{j_1}, \mathbf{A}_{j_2}, \cdots, \mathbf{A}_{j_l})$.

Step 3. Chooses a random matrix $\mathbf{S} \in Z_q^{n\times(l+1)m}$ and an errors matrix $\mathbf{X} \in \bar{\Phi}_{\alpha}^{(l+1)m\times(l+1)m}$. Then computes $\mathbf{C} = \overline{\mathbf{A}}^t\mathbf{S} + 2\mathbf{X} + \mathbf{M}(\mathrm{mod}q)$.

Step 4. Computes an one-time signature σ on $\mathbf{C}$ using signing key sk which is generated in Step 1.

Hence, $(\mathbf{C}, vk, \sigma)$ is the ciphtertext of $\mathbf{M}$.

Decryption In order to decrypt a ciphtertext $(\mathbf{C}, vk, \sigma)$, the decryption algorithm operates as follows:

Step 1. Inputs $(\mathbf{C}, vk, \sigma)$ to the verification algorithm of the Ssign scheme, if output "1" goes to step 2, otherwise, aborts.

Step 2. Chooses public matrixes $\mathbf{A}_i$ as shown as Step 2 in the encryption algorithm. Then parse $\overline{\mathbf{A}} = (\mathbf{A}, \mathbf{A}_{j_1}, \mathbf{A}_{j_2}, \cdots, \mathbf{A}_{j_l})$.

Step 3. Inputs $(\mathbf{A}, \overline{\mathbf{A}}, \mathbf{T}, s)$ to the algorithm in Proposition 1 which outputs a trapdoor basis $\mathbf{T}_1$ of the lattice $\Lambda_q^{\perp}(\overline{\mathbf{A}})$.

Step 4. Computes $\mathbf{E} = \mathbf{T}_1^t\mathbf{C}(\mathrm{mod}q)$, and then computes $\mathbf{M} = \mathbf{T}_1^{-t}\mathbf{E}(\mathrm{mod}2)$.

4. Analysis on the Proposed scheme

4.1. Correctness

Let $(\mathbf{C}, vk, \sigma)$ be the ciphtertext generated by the encryption algorithm. Since σ is generated by the Ssign scheme, then it can be accepted by the verification algorithm of the Ssign signature scheme in Step 1. It is clear that the decryption algorithm can finish the step 2 to fix public matrixes and get matrix $\overline{\mathbf{A}}$. The decryption algorithm can sample a trapdoor basis of $\Lambda_q^{\perp}(\overline{\mathbf{A}})$ from Proposition 1. Then Step 3 is finished. Since $\mathbf{T}_1$ is a trapdoor basis of lattice $\Lambda_q^{\perp}(\overline{\mathbf{A}})$ and the errors matrix $\mathbf{X}$ is sampled from the distribution $\bar{\Phi}_{\alpha}^{(l+1)m\times(l+1)m}$, all entries of $\mathbf{T}_1$ and $\mathbf{X}$ are sufficiently small. Then $\mathbf{E} = \mathbf{T}_1^t\mathbf{C} = \mathbf{T}_1^t(2\mathbf{X} + \mathbf{M})(\mathrm{mod}q)$ will equal to $\mathbf{T}_1^t(2\mathbf{X} + \mathbf{M})$ over integer with an overwhelming probability [**?**]. Hence, $\mathbf{T}_1^{-t}\mathbf{E} = 2\mathbf{X} + \mathbf{M}$. So $\mathbf{M} = \mathbf{T}_1^{-t}\mathbf{E}(\mathrm{mod}2)$.

The correctness is proven.

4.2. Security

Theorem 1.*If the LWE problem whose errors matrix is sampled from the distibution $\bar{\Phi}_{\alpha}^{(l+1)m\times(l+1)m}$ is hard and the one-time signature scheme used in our construction is strong unforgeable, the proposed PKE scheme is IND-CCA2 secure.*

Proof. In order to prove Theorem 1, we give four games and we show that Game i and Game $i+1$ are indistinguishable for any PPT adversary. Hence we will prove that Theorem 1 holds.

Game 1. It is the same as the standard IND-CCA2 game in Section 2.7.

Game 2. It is the same as Game 1, but, for any decryption query $(vk^*, *, *)$, an errors symbol $\perp$ is always returned as the answer.

Game 3. Game 3 is the same as Game 2, but, in the setup phase, if $vk_{j_i}^* = 1$ then choose a random matrix as the $j_i th$ public matrix. Otherwise, the public matrixes are all the outputs of the trapdoor sampling algorithm in Proposition 2. Namely, the trapdoor basis of lattice $\Lambda_q^{\perp}(\mathbf{A}_i)$ are known to the challenger when $vk_i^* = 0$.

Game 4. It is the same as Game 3, except, in the challenge ciphtertext $(vk^*, \mathbf{C}^*, \sigma^*)$, $\mathbf{C}^*$ is generated uniformly and randomly, moreover, it is independent on vk^* and σ^*.

We give four claims to show that Game 1 $\sim$ Game 4 are indistinguishable.

Claim 1. If the one-time signature scheme used in our construction is strong existential unforgeable, then Game 1 and Game 2 are indistinguishable for any PPT adversary.

The proof of Claim 1 can be found in [14] and we omit it.

Claim 2. Game 2 and Game 3 are statistically indistinguishable for any PPT adversary.

Proof. By proposition 2, we know that the distribution of the output matrix in trapdoor sampling algorithm is statistically close to the uniform distribution. Hence, if we replace some public matrixes with the outputs of the trapdoor sampling algorithm, the adversary can not distinguish it. Then Claim 2 holds.

Claim 3. Game 3 and Game 4 are computational indistinguishable under the hardness hypothesis of the the decision version LWE problem whose the errors distribution is distributed according to $\bar{\Phi}_{\alpha}^{(l+1)m\times(l+1)m}$.

Proof. If there is a PPT adversary $\mathcal{A}$ can distinguish Game 3 and Game 4 with advantage ε, then we can construct a challenger $\mathcal{C}$ to solve the decision version LWE problem.

Suppose the challenger $\mathcal{C}$ wants to distinguish the uniform distribution over $Z_q^{n\times(l+1)m} \times Z_q^{(l+1)m\times(l+1)m}$ and the distribution $\{(\mathbf{B},\mathbf{C})|\mathbf{C}=\mathbf{B}^t\mathbf{S}+\mathbf{X}(\mathrm{mod}q)\}$ where $\mathbf{B} \in Z_q^{n\times(l+1)m}$, $\mathbf{S} \in Z_q^{n\times(l+1)m}$ and the errors matrix $\mathbf{X} \in \overline{\Phi}_\alpha^{(l+1)m\times(l+1)m}$. $\mathcal{C}$ interacts with $\mathcal{A}$ to simulate either Game 3 or Game 4 as follows:

Setup Phase. $\mathcal{C}$ generates a signing key and a verification key of the Ssign scheme, denoted vk^* and sk^* respectively. Let $vk^*_{j_i} = 1$ for $i = 1,2,\cdots,l$ and $vk^*_{j'_i} = 0$ for $i = 1,2,\cdots,k-l$. Running the trapdoor sampling algorithm $k-l$ times to output $k-l$ matrixes $\overline{\mathbf{B}}_i$ with the trapdoor basis of the corresponding lattice $\Lambda_q^\perp(\overline{\mathbf{B}}_i)$. Let $\mathbf{B} = (\mathbf{B}_0,\mathbf{B}_2,\cdots,\mathbf{B}_l)$ where $\mathbf{B}_i \in Z_q^{n\times m}$. Then set $\mathbf{A}_{j_i} = \mathbf{B}_i$ for $i = 1,2,\cdots,l$ and $\mathbf{A}_{j'_i} = \overline{\mathbf{B}}_i$ for $i = 1,2,\cdots,k-l$. Hence, $\mathbf{A} = \mathbf{B}_0$ and $\mathbf{A}_i$ for $i = 1,2,\cdots,k$ are public key matrixes .

Decryption Oracle. The adversary can adaptively query the decryption oracle, and the challenger simulates the decryption oracle in this phase. For a ciphtertext $(vk,\mathbf{C},\sigma)$, if $vk = vk^*$ outputs an error symbol $\perp$, otherwise, $vk \neq vk^*$, since vk and vk^* are with the same hamming weigh, then there exist some position satisfies $vk_j = 1$ and $vk^*_j = 0$. As shown as the setup phase, $\mathcal{C}$ knows the trapdoor basis of lattice $\Lambda_q^\perp(\mathbf{A}_j)$. Hence, $\mathcal{C}$ can run the Bonsai trees algorithm in Proposition 1 to generate a trapdoor basis of lattice $\Lambda_q^\perp(\overline{\mathbf{A}})$ where $\overline{\mathbf{A}}$ satisfies $\mathbf{C} = \overline{\mathbf{A}}^t\mathbf{S}+\mathbf{X}(\mathrm{mod}q)$. Then he decrypts the ciphtertext into a message by the trapdoor basis of $\Lambda_q^\perp(\overline{\mathbf{A}})$.

Challenge. $\mathcal{A}$ randomly chooses two message $\mathbf{M}_b$ with the same length for $b \in \{0,1\}$ and sends them to $\mathcal{C}$. The challenger $\mathcal{C}$ randomly chooses a bit $b \in \{0,1\}$, samples a matrix $\mathbf{C}'^*$ from the uniform distribution or a LWE problem instance defined above and computes $\mathbf{C}^* = 2\mathbf{C}'^* + \mathbf{M}_b$. Generates the one-time signature σ^* of $\mathbf{C}^*$ using the signing key sk^*. Hence $(\sigma^*,\mathbf{C}^*,vk^*)$ as the challenge ciphtertext. $\mathcal{C}$ sends $(\sigma^*,\mathbf{C}^*,vk^*)$ as the challenge to $\mathcal{A}$.

Decryption Oracle. The adversary $\mathcal{A}$ continues to query the decryption oracle which are answered as described above. In this phase, any form of $(vk^*,*,*)$ is queried would return an error symbol $\perp$.

It is clear that, if $\mathbf{C}'^*$ is an uniform matrix, $2\mathbf{C}'^* + \mathbf{M}_b(\mathrm{mod}q)$ is also an uniform matrix and if $\mathbf{C}'^*$ is a LWE problem instance then $2\mathbf{C}'^* + \mathbf{M}_b(\mathrm{mod}q)$ is identical to the distribution of the encryption algorithm in the proposed scheme. Hence, if the adversary can distinguish the Game 3 and Game 4 with some advantage ε, then $\mathcal{C}$ can distinguish the uniform distribution and the distribution obtained by computing LWE peoblem instance with the same advantage. Hence, the LWE problem can be solved by $\mathcal{C}$. Claim 3 is proven.

Table 1 Efficiency Comparison

Schemes	Public key length (bit)	the M-C factor	Security
[12]	$(2kmn+nl)\log q$	$(km/l+1)\log q' + vs/l$	CCA
Our scheme	$(k+1)mn\log q$	$\log q + vs/(l+1)^2m^2$	CCA
[8]	$mn\log q$	$\log q$	CPA

Claim 4. The advantage for any adversary in Game 4 is 0.

Proof. Since $\mathbf{C}^*$ is chosen uniformly and randomly, then the adversary wins in game 4 always with probability $1/2$, so Claim 4 is proven.

Put four Claims together, we know that any PPT adversary wins the standard IND-CCA2 game with a negligible advantage.

Theorem 1 is proven.

4.3. Efficiency

We firstly note one fact is that the scheme in [13] is more efficient at computation cost than our scheme, for, the first scheme is built by hybrid encryption techniques which the PKE algorithm only used to encrypt the symmetric key while our scheme is in the public key setting which is used to encrypt the message. The advantage of our scheme is that both the public key size and the M-C factor are short. Table 4.1 shows the comparison details in which vs denotes the length of the verification key and the one-time signature. Namely, in contrast to Peikert's construction, we efficiently reduce the public key size of our scheme down to $(k+1)mn\log q$ bits. So our scheme presents good efficiency at memory and transfers. At the same time, a logical assumption is that $vs \ll (l+1)^2m^2$, then the M-C factor of this scheme is only little larger than the M-C factor of [8] $\log q$.

5. Conclusions

We present an efficient IND-CCA2 secure PKE scheme using the Bonsai tree primitive and Gentry's encryption scheme in this paper. The public key size of the propose scheme is reduced efficiently and the M-C factor of the propose scheme is also controlled to be a logical number. Based on the hardness of the decision variant of the LWE problem and the strong unforgeability of the one-time signature scheme used in this paper, we prove that the propose scheme is IND-CCA2 secure.

6. Acknowledgement

This work was supported by the National Natural Science Foundation of China (Grant No. 61303198,61173151,

61173152), this work was also supported by Huawei Co. (YBCB2012026) and the Doctor Foundation of Shandong Jianzhu University.

References

[1] Agrawal S, Boneh D, Boyen X. Efficient Lattice (H)IBE in the Standard Model. Proceedings of Eurocrypt 2010, LNCS 6110, Nice, France, 553-572 (2010).
[2] Agrawal S, Boneh D, Boyen X. Lattice Basis Delegation in Fixed Dimension and Shorter-ciphtertext Hierarchical IBE. Proceedings of Crypto 2010, LNCS 6223, Santa Barbara, CA, USA, 98–115 (2010).
[3] Alwen J, Peikert C. Generating Shorter Bases for Hard Random Lattices. Proceedings of STACS, Freiburg, Germany, **09001**, 75-86 (2009).
[4] Boneh D, Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption. SIAM J. of Computing (SICOMP), **36**, 915-942 (2006).
[5] Cash D, Hofheinz D, Kiltz E, Peikert C. Bonsai Trees, or How to Delegate a Lattice Basis. Proceedings of Eurocrypt 2010, LNCS 6110, Nice, France, 523-552 (2010).
[6] Dodis Y, Goldwasser S, Kalai Y T, Peikert C, Vaikuntanathan V. Public-Key Encryption Schemes with Auxiliary Inputs. Proceedings of TCC 2010, LNCS 5978, Zurich, Switzerland, 361-381 (2010).
[7] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for Hard Lattices and New Cryptographic Constructions. Proceedings of STOC 2008, Victoria, British Columbia, 197-206 (2008).
[8] Gentry C, Halevi S, Vaikuntanathan V. A Simple BGN-type Cryptosystem from LWE. Proceedings of Eurocrypt 2010, LNCS 6110, Nice, France, 506-522 (2010).
[9] Gordon S.D, Katz J.J, Vaikuntanathan V. A group signature scheme from lattice assumptions, Proceedings of ASIACRYPT 2010, LNCS, **6477**, 395-412 (2010).
[10] Goldwasser S, Kalai Y, Peikert C, Vaikuntanathan V. Robustness of the Learning with Errors Assumption. Proceedings of ICS 2010, Beijing, China, 230-240 (2010).
[11] Micciancio D, Regev O. Worst-case to Average-case Reductions Based on Gaussian Measures. Proceedings of 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS), Rome, Italy, 372-381 (2004).
[12] Naor M, Yung M. Public-key cryptosystems provably secure against chosen ciphertext attacks. Proceedings of STOC 1990, Baltimore, Maryland, USA, 427-437 (1990).
[13] Peikert C. Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem. Proceedings of STOC 2009, Bethesda, Maryland, USA, 333-342 (2009).
[14] Peikert C, Waters B. Lossy trapdoor function and its application. Proceedings of STOC 2008, Victoria, British Columbia, 187-196 (2008).
[15] Peikert C, Vaikuntanathan V, Waters B. A Framework for Efficient and Composable Oblivious Transfer. Proceedings of CRYPTO 2008, LNCS 5157, Santa Barbara, CA, USA, 554-571 (2008).
[16] Regev O. On Lattice, Learning with Errors, Random Linear Codes, and Cryptography. Proceedings of STOC 2005, Baltimore, 84-93 (2005).
[17] Wang F, Hu Y, Wang C. A Post-Quantum Secure Hybrid Signcryption from Lattice Assumption. Applied mathmatics and information sciences, **6**, 45-56 (2012).

Wang Fenghe received the PhD degree in Cryptgraphy at Xidian University. His research interests are in the areas of public key cryptography, information security. He has published 10 research articles in some international journals of computer science.

Wang Chunxiao is Associate Professor of Shandong Jianzhu University of China. She received the Master degree at Xidian University of Xian (China). She has published about 12 research articles and Her research areas consists cryptography and applied mathmatics.

Yupu Hu was born in 1955, is Professor and Ph.D. supervisor in State Key Laboratory of Integrated Service Networks, Xidian University, China. His current research interests include stream ciphers, block ciphers, digital signature, lattice cryptography and network security.