Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 341490, 7 pages
http://dx.doi.org/10.1155/2014/341490

Research Article

STP-LWE: A Variant of Learning with Error for a Flexible Encryption

Bo Gao,[1,2,3] Yanfeng Shi,[1] Chunli Yang,[2] Lixiang Li,[2] Licheng Wang,[2] and Yixian Yang[1,2]

[1] *School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China*
[2] *Information Security Center, Beijing University of Posts and Telecommunications, P.O. Box 145, Beijing 100876, China*
[3] *School of Computer Information Management, Inner Mongolia University of Finance and Economics, Hohhot 010051, China*

Correspondence should be addressed to Lixiang Li; li_lixiang2006@163.com

Received 28 January 2014; Accepted 20 March 2014; Published 14 April 2014

Academic Editor: Qing-Wen Wang

We construct a flexible lattice based scheme based on semitensor product learning with errors (STP-LWE), which is a variant of learning with errors problem. We have proved that STP-LWE is hard when LWE is hard. Our scheme is proved to be secure against indistinguishable chosen message attacks, and it can achieve a balance between the security and efficiency in the hierarchical encryption systems. In addition, our scheme is almost as efficient as the dual encryption in GPV08.

1. Introduction

Lattices and lattice-based cryptography have become a hot research topic in public key cryptography in recent years. Lattice-based cryptography is attracted from provable worst-case hardness guarantees, good asymptotic efficiency and parallelism, and resistance to quantum attacks [1]. The first provably secure lattice based encryption AD is present by Ajtai and Dwork based on the worst-case hardness of lattice problems [2]. After that, several constructions have been proposed [3, 4]. In 2004, Regev improved $\mathrm{AD}_{\mathrm{GGH}}$ to R04 based on a harder lattice problem. But its huge key size is unacceptable [5]. To overcome its disadvantage, Regev successively constructed Regev05 based on learning with errors (LWE) problem, which can be quantum reduced from traditional SIVP_{γ} problem [6]. Since LWE problem has been proved to be amazingly versatile, a multitude of cryptographic schemes have been proposed, such as the basis for secure public-key encryption under both chosen-plaintext [6] and chosen-ciphertext attacks [7, 8], oblivious transfer [9], identity-based encryption [10], various forms of leakage-resilient cryptography [11], and fully homomorphic encryption [12].

In some applications, such as hierarchical encryption systems, the users in different levels will use private keys with different lengths [13]. They will retrieve their private key from their domain PKG, who has previously requested their domain secret key from the root PKG. In traditional encryptions, the PKG must save all security parameters and public parameters related to the different lengths of keys for the users in different domains [14]. So how to construct a flexible encryption scheme to bring a balance between the security and efficiency requirements is an open problem.

Semitensor product (STP), as a new algebraic approach, is a generalization of the matrix product from the equal dimension case to the multiple dimension case, and it is designed to deal with higher-dimensional data as well as multilinear mappings [15]. Recently, STP is applied widely in control theory [16] and physics [17–19]. However, to the best of our knowledge, all the works in cryptography field based on STP are related to Boolean functions. A method for the conversion between the truth table and the polynomial expression of Boolean functions was proposed [20]. In [21], the authors did research on nonlinear feedback shift register (NLFSR), including the calculation of numbers of fixed points and cycles with different lengths of state sequences generated.

In this paper, we propose a variant of LWE problem called STP-LWE problem, which is essential to extend the standard LWE problem by using STP. In STP-LWE problem, the dimension of public matrix A may not be equal to the secret s. The hardness of STP-LWE can be reduced to the standard LWE problem. In this paper, we will take advantage of the properties of STP-LWE to construct the STP-GPV dual cryptosystem based on the dual encryption in GPV08 [22]. The new scheme is more flexible in hierarchical encryption systems since we can flexibly balance the security and efficiency by adjusting the length of messages with the static security parameter.

The rest of this paper is organized as follows. We first introduce some basic concepts of lattices in Section 2. In Section 3, we detail STP product and STP-LWE problem. In Section 4, we propose the STP-GPV dual cryptosystem and analyze the correctness and security. In Section 5, we discuss the efficiency of the STP-GPV dual cryptosystem. Finally, discussions and conclusions are presented in Section 6.

2. Preliminaries

In this section, we briefly describe the basic concepts about lattices and the learning with errors (LWE) problem.

2.1. Notation. We denote the set of real numbers by $\mathbb{R}$ and the set of integers by $\mathbb{Z}$. For a positive integer n, $[n]$ denotes $\{1,\ldots,n\}$. By convention, vectors are assumed to be in column form and written using bold lowercase letters, for example, $\mathbf{x}$. The ith component of $\mathbf{x}$ will be denoted by x_i. Matrices are written as bold capital letters, for example, $\mathbf{X}$, and the ith column vector of a matrix $\mathbf{X}$ is denoted by $\mathbf{x}_i$. The length of a matrix is the norm of its longest column $\|\mathbf{X}\| = \max_i\|\mathbf{x}_i\|$. We use standard big-$O$ notation to classify the growth of functions and say that $f(n) = \widetilde{O}(g(n))$ if $f(n) = O(g(n)\cdot\log^c n)$ for some fixed constant c. We let poly(n) be an unspecified function $f(n) = O(n^c)$ for some constants c. A *negligible* function, denoted generically by negl(n), is a function $f(n)$ such that $f(n) = o(n^{-c})$ for some fixed constant c. We say that a probability (or fraction) is *overwhelming* if it is $1 - \text{negl}(n)$. The *statistical distance* between two distributions X and Y over a countable domain D is defined to be $(1/2)\sum_{d\in D}|X(d) - Y(d)|$.

2.2. Lattices and Gaussian Measures. A lattice is a discrete additive subgroup of $\mathbb{R}^n$. Let $\mathbf{B} = \{\mathbf{b}_1,\ldots,\mathbf{b}_n\} \subset \mathbb{R}^n$ consist of n linearly independent vectors. The n-dimensional *lattice* Λ generated by the basis $\mathbf{B}$ is

$$\Lambda = \mathscr{L}(\mathbf{B}) = \left\{\mathbf{B}\mathbf{c} = \sum_{i\in[n]} c_i\cdot\mathbf{b}_i : \mathbf{c}\in\mathbb{Z}^n\right\}. \qquad (1)$$

For any (ordered) set $S = \{\mathbf{s}_1,\ldots,\mathbf{s}_n\} \subset \mathbb{R}^n$ of linearly independent vectors, let $\widetilde{S} = \{\widetilde{\mathbf{s}}_1,\ldots,\widetilde{\mathbf{s}}_n\}$ be its Gram-Schmidt orthogonalization, defined iteratively in the following way: $\widetilde{\mathbf{s}}_1 = \mathbf{s}_1$, and for each $i = 2,\ldots,n$, $\widetilde{\mathbf{s}}_i$ is the component of $\mathbf{s}_i$ orthogonal to span$(\mathbf{s}_1,\ldots,\mathbf{s}_{i-1})$. Clearly, $\|\widetilde{\mathbf{s}}_i\| \le \|\mathbf{s}_i\|$.

The following useful lemma says that any full-rank set of vectors in a lattice can be efficiently converted to a basis of the lattice, without increasing the lengths of the Gram-Schmidt vectors.

Lemma 1 (see [23]). *There is a deterministic polynomial-time algorithm that, given an arbitrary basis $\mathbf{B}$ of a n-dimensional lattice $\Lambda = \mathscr{L}(\mathbf{B})$ and a full-rank set of lattice vectors $\mathbf{S} \subset \Lambda$, the output is a basis $\mathbf{T}$ of Λ such that $\|\widetilde{\mathbf{t}}_i\| \le \|\widetilde{\mathbf{s}}_i\|$ for all $i \in [n]$.*

The dual lattice of Λ, denoted Λ^*, is defined as $\Lambda^* = \{\mathbf{x}\in\mathbb{R}^n : \forall\mathbf{v}\in\Lambda, \langle\mathbf{x},\mathbf{v}\rangle\in\mathbb{Z}\}$. By symmetry, it can be seen that $(\Lambda^*)^* = \Lambda$. If $\mathbf{B}$ is a basis of Λ, the dual basis $\mathbf{B}^* = (\mathbf{B}^{-1})^T$ is in fact a basis of Λ^*.

The following standard fact relates to the Gram-Schmidt orthogonalizations of a basis and its dual (the proof can be found in [5]).

Lemma 2. *Let $\{\mathbf{b}_1,\ldots,\mathbf{b}_n\}$ be an ordered basis, and let $\{\mathbf{d}_1,\ldots,\mathbf{d}_n\}$ be its dual basis in reversed order (i.e., $\mathbf{d}_i = \mathbf{b}^*_{n-i+1}$). Then $\widetilde{\mathbf{d}}_i = \widetilde{\mathbf{b}}_i/\|\mathbf{b}_i\|^2$ for all $i\in[n]$. In particular, $\|\widetilde{\mathbf{d}}_i\| = 1/\|\widetilde{\mathbf{b}}_i\|$.*

We now review the Gaussian measures over lattices. For any $s > 0$, the Gaussian function on $\mathbb{R}^n$ centered at $\mathbf{c}$ with parameter s is defined as

$$\forall\mathbf{x}\in\mathbb{R}^n, \quad \rho_{s,\mathbf{c}}(\mathbf{x}) = \exp\left(-\frac{\pi\|\mathbf{x}-\mathbf{c}\|^2}{s^2}\right). \qquad (2)$$

The subscripts s and $\mathbf{c}$ are taken to be 1 and 0 (resp.,) when omitted.

For any $\mathbf{c}\in\mathbb{R}^n$, real $s > 0$, and n-dimensional lattice Λ, the discrete Gaussian distribution over Λ is defined as

$$\forall\mathbf{x}\in\Lambda, \quad D_{\Lambda,s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}, \qquad (3)$$

where $\rho_{s,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x}\in\Lambda}\rho_{s,\mathbf{c}}(\mathbf{x})$.

Micciancio and Regev [24] proposed a lattice quantity called the smoothing parameter.

Definition 3 (see [24]). For any n-dimensional lattice Λ and a positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ is the smallest real $s > 0$ such that $\rho_{1/s}(\Lambda^*\setminus 0) \le \epsilon$, where $\rho_{1/s}(\Lambda^*\setminus 0) = \sum_{\mathbf{x}\in\Lambda^*\setminus 0}\rho_{1/s,0}(\mathbf{x})$.

A bound on the smoothing parameter is also given in [24].

Lemma 4 (see [25]). *For any n-dimensional lattice Λ and real $\epsilon > 0$, one has*

$$\eta_\epsilon(\Lambda) \le \frac{\sqrt{\log(2n/(1+1/\epsilon))/\pi}}{\lambda_1^\infty(\Lambda^*)}. \qquad (4)$$

Then for any $\omega(\sqrt{\log n})$ function, there is a negligible $\epsilon(n)$ for which $\eta_\epsilon(\Lambda) \le \omega(\sqrt{\log n})/\lambda_1^\infty(\Lambda^*)$.

We notice that a sample from a discrete Gaussian with parameter s is at most $s\sqrt{n}$ away from its center (in the ℓ_2 norm), with overwhelming probability.

Lemma 5 (see [24]). *For any n-dimensional lattice Λ, $\mathbf{c} \in span(\Lambda)$, real $\epsilon \in (0,1)$, and $s \geq \eta_\epsilon(\Lambda)$,*

$$\Pr_{\mathbf{x}\sim D_{\Lambda,s,\mathbf{c}}}\left[\|\mathbf{x}-\mathbf{c}\| > s\sqrt{n}\right] \leq \frac{1+\epsilon}{1-\epsilon}\cdot 2^{-n}. \quad (5)$$

2.3. Some Lattice Problems. We now redescribe the learning with errors (LWE) problem [6].

For an integer $q \geq 2$, some probability distribution χ over $\mathbb{Z}_q$, an integer dimension $n \in \mathbb{Z}^+$, and a vector $\mathbf{s} \in \mathbb{Z}_q^n$, define $\mathscr{A}_{\mathbf{s},\chi}$ as the distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ of the variable $(\mathbf{a}, \mathbf{a}^T\mathbf{s}+x)$, where $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ and $x \leftarrow \chi$ are uniform and independent, and all operations are performed in $\mathbb{Z}_q$.

Definition 6 (LWE). For an integer $q = q(n)$ and a distribution χ on $\mathbb{Z}_q$, the goal of the (average-case) *learning with errors* problem $\mathrm{LWE}_{q,\chi}$ is to distinguish (with nonnegligible probability) between the distribution $\mathscr{A}_{\mathbf{s},\chi}$ for some uniform (secret) $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ (via oracle access to the given distribution). In other words, if LWE is hard, then the collection of distributions $\mathscr{A}_{\mathbf{s},\chi}$ is pseudorandom.

$\mathbb{T} = \mathbb{R}/\mathbb{Z}$ as the group of reals $[0,1)$ with mod 1 addition. For $\alpha \in \mathbb{R}^+$, Ψ_α is the distribution on $\mathbb{T}$ of a normal variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$, reduced modulo 1. For any probability distribution ϕ over $\mathbb{T}$ and an integer $q \in \mathbb{Z}^+$ its discretization $\overline{\phi}$ is the discrete distribution over $\mathbb{Z}_q$ of the random variable $\lfloor q \cdot X_\phi \rceil \bmod q$, where X_ϕ has distribution ϕ.

Then, we recall two standard worst-case approximation problems on lattices. In both problems, $\gamma = \gamma(n)$ is the approximation factor as a function of the dimension.

Definition 7 (see [24] shortest vector problem (decision version)). An input to GapSVP_γ is a basis $\mathbf{B}$ of a full-rank n-dimensional lattice. It is a YES instance if $\lambda_1(\mathscr{L}(\mathbf{B})) \leq d$ and is a NO instance if $\lambda_1(\mathscr{L}(\mathbf{B})) > \gamma(n)\cdot d$, where *$d$ is a rational number*.

Definition 8 (see [24] shortest independent vectors problem). An input to SIVP_γ is a full-rank basis $\mathbf{B}$ of an n-dimensional lattice. The goal is to output a set of n linearly independent lattice vectors $\mathbf{S} \subset \mathscr{L}(\mathbf{B})$ such that $\| \mathbf{S} \| \leq \gamma(n)\cdot\lambda_n(\mathscr{L}(\mathbf{B}))$.

Regev demonstrated that for certain modulo q and Gaussian error distributions χ, $\mathrm{LWE}_{q,\chi}$ is as hard as several standard worst-case lattice problems using a quantum algorithm.

Proposition 9 (see [6]). *Let $\alpha = \alpha(n) \in (0,1)$ and let $q = q(n)$ be a prime such that $\alpha \cdot q > 2\sqrt{n}$. If there exists an efficient (possibly quantum) algorithm that solves $\mathrm{LWE}_{q,\overline{\Psi}_\alpha}$, then there exists an efficient quantum algorithm for approximating SIVP and GapSVP in the l_2 norm, in the worst case, within $\widetilde{O}(n/\alpha)$ factors.*

The result can be subsequently extended to SIVP and GapSVP in any l_p norm, $2 \leq p \leq \infty$, for essentially the same $\widetilde{O}(n/\alpha)$ approximation factors [25].

3. STP-LWE

3.1. Semitensor Product. In this section, we introduce the semitensor product (STP) of matrices. The STP-formalism of matrices not only is a generalization of a conventional matrix product, but also makes all the fundamental properties of the conventional matrix product remain true.

Definition 10 (see [15]). (1) Let $\mathbf{a}$ be a row vector of dimension kl, and let $\mathbf{b}$ be a column vector of dimension l. Then we split $\mathbf{a}$ into l equal-size blocks named $\mathbf{a}^1,\ldots,\mathbf{a}^l$, which are row vectors of dimension k. Define a semitensor product, denoted by $\ltimes$, as

$$\begin{gathered}\mathbf{a} \ltimes \mathbf{b} = \sum_{i=1}^{l} \mathbf{a}^i \mathbf{b}_i \in \mathbb{R}^k \\ \mathbf{b}^T \ltimes \mathbf{a}^T = \sum_{i=1}^{l} \mathbf{b}_i \left(\mathbf{a}^i\right)^T \in \mathbb{R}^k.\end{gathered} \quad (6)$$

(2) Let $\mathbf{P} \in M_{r\times l}$ and $\mathbf{Q} \in M_{s\times t}$. If either l is a factor of s, say $kl = s$ and denote it by $\mathbf{P} \prec_k \mathbf{Q}$, or s is a factor of l, say $l = ks$ and denote it by $\mathbf{P} \succ_k \mathbf{Q}$, then define the STP of $\mathbf{P}$ and $\mathbf{Q}$, denoted by $\mathbf{W} = \mathbf{P} \ltimes \mathbf{Q}$, as the following: $\mathbf{W}$ consists of $r \times t$ blocks as $\mathbf{W} = (\mathbf{W}^{ij})$ and each block is

$$\mathbf{W}^{ij} = \mathbf{P}^i \ltimes \mathbf{Q}_j, \quad i = 1,\ldots,r,\ j = 1,\ldots,t, \quad (7)$$

where $\mathbf{P}^i$ is the ith row of $\mathbf{P}$ and $\mathbf{Q}_j$ is the jth column of $\mathbf{Q}$.

The dimension of the STP of two matrices can be described by deleting the largest common factor of the dimensions of the two factor matrices; for example,

$$\begin{gathered}\mathbf{P}_{r\times kl} \ltimes \mathbf{Q}_{l\times t} = (\mathbf{P}(\mathbf{Q}\otimes \mathbf{I}_k))_{r\times kt}, \\ \mathbf{P}_{r\times l} \ltimes \mathbf{Q}_{kl\times t} = ((\mathbf{P}\otimes \mathbf{I}_k)\mathbf{Q})_{kr\times t},\end{gathered} \quad (8)$$

where $\otimes$ is the Kronecker product and $\mathbf{I}_k$ is the identity matrix.

If the related products are well defined, the STP satisfies the following laws.

(1) Distributive rule is as follows:

$$\begin{gathered}\mathbf{P} \ltimes (\alpha\mathbf{Q} + \beta\mathbf{W}) = \alpha\mathbf{P} \ltimes \mathbf{Q} + \beta\mathbf{P} \ltimes \mathbf{W}, \\ (\alpha\mathbf{Q} + \beta\mathbf{W}) \ltimes \mathbf{P} = \alpha\mathbf{Q} \ltimes \mathbf{P} + \beta\mathbf{W} \ltimes \mathbf{P},\end{gathered} \quad (9)$$

where $\alpha, \beta \in \mathbb{R}$.

(2) Associative rule is as follows:

$$\mathbf{P} \ltimes (\mathbf{Q} \ltimes \mathbf{W}) = (\mathbf{P} \ltimes \mathbf{Q}) \ltimes \mathbf{W}. \quad (10)$$

3.2. STP-LWE. In this section, we propose a new hardness problem that is called STP-LWE problem which is based on the STP product. The main idea is that we replace the ordinary multiplication of LWE problem with STP. A distribution $\mathscr{A}_{\mathbf{s},\underbrace{\chi,\chi,\dots,\chi}_{k}}$ should be introduced before giving the definition of STP-LWE problem.

For an integer $q \geq 2$ and some probability distribution χ over $\mathbb{Z}_q$, an integer dimension $n \in \mathbb{Z}^{+}$, and a vector $\mathbf{s} \in \mathbb{Z}_q^{n/k}$, define $\mathscr{A}_{\mathbf{s},\underbrace{\chi,\chi,\dots,\chi}_{k}}$ as the distribution on $\mathbb{Z}_q^n \times \underbrace{\mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q}_{k}$ of the variable $(\mathbf{a}, \mathbf{a}^T \ltimes \mathbf{s} + (x_1, x_2, \dots, x_k))$, where $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ is uniform and $x_1, x_2, \dots, x_k \leftarrow \chi$ are independent, and all operations are performed in $\mathbb{Z}_q$.

Definition 11 (decision n/k-dimensional STP-LWE problem). For an integer $q = q(n)$ and a distribution χ on $\mathbb{Z}_q$, the goal of the decision version (average case) $\text{STP-LWE}_{q,\underbrace{\chi,\chi,\dots,\chi}_{k}}$ is to distinguish (with nonnegligible probability) between the distribution $\mathscr{A}_{\mathbf{s},\underbrace{\chi,\chi,\dots,\chi}_{k}}$ for some uniform (secret) $\mathbf{s} \leftarrow \mathbb{Z}_q^{n/k}$ and the uniform distribution on $\mathbb{Z}_q^n \times \underbrace{\mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q}_{k}$ (via oracle access to the given distribution).

Definition 12 (search n/k-dimensional STP-LWE problem). For an integer $q = q(n)$ and a distribution χ on $\mathbb{Z}_q$, the goal of the search version (average case) $\text{STP-LWE}_{q,\underbrace{\chi,\chi,\dots,\chi}_{k}}$ is to find the vector $\mathbf{s} \in \mathbb{Z}_q^{n/k}$ giving a sample $(\mathbf{a}, \mathbf{a}^T \ltimes \mathbf{s} + (x_1, x_2, \dots, x_k))$ from the distribution $\mathscr{A}_{\mathbf{s},\underbrace{\chi,\chi,\dots,\chi}_{k}}$.

The STP-LWE problem is a generalization of the primal LWE problem. It is obvious that the decision n/k-dimensional STP-LWE problem and the search n/k-dimensional STP-LWE problem are equal to the primal LWE problem when $k = 1$. The STP-LWE problem could be shown in the form of matrices, consisting of m vectors, and each vector is an instance of LWE problem. Then an instance of STP-LWE problem can be express as $(\mathbf{A}, \mathbf{A}^T \ltimes \mathbf{s} + (\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_k))$, where $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \in \mathbb{Z}_q^{n/k}$ is a secret vector, and $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_k)$ are from the distribution χ^m. The following theorem shows the hardness of search version n/k-dimensional STP-LWE problem.

Theorem 13. *The search version n/k-dimensional $\text{STP-LWE}_{q,\underbrace{\chi,\chi,\dots,\chi}_{k}}$ problem is hard under the assumption that $\text{LWE}_{q,\chi}$ is hard.*

Proof. We use proof by contradiction to prove this theorem.

Case 1. Let $k = 2$; then given a search version $\text{STP-LWE}_{q,\chi,\chi}$ instance $[\mathbf{b}_1, \mathbf{b}_2] = \mathbf{A}^T \ltimes \mathbf{s} + [\mathbf{x}_1, \mathbf{x}_2]$, where $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{Z}_q^m$ and $\mathbf{x}_1, \mathbf{x}_2 \leftarrow \chi^m$. Suppose we find the vector $\mathbf{s} \in \mathbb{Z}_q^{n/2}$ is an easy thing.

Based on the property of STP, we have $\mathbf{A}^T \ltimes \mathbf{s} = \mathbf{A}^T(\mathbf{s} \otimes \mathbf{I}_2) = \mathbf{A}^T(\mathbf{s}_1, \mathbf{s}_2)$, where

$$\mathbf{s}_1 = \mathbf{s} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} s_1 \\ 0 \\ \vdots \\ s_{\frac{n}{2}} \\ 0 \end{bmatrix}, \qquad \mathbf{s}_2 = \mathbf{s} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ s_1 \\ \vdots \\ 0 \\ s_{n/2} \end{bmatrix}. \tag{11}$$

Therefore, $[\mathbf{b}_1, \mathbf{b}_2] = \mathbf{A}^T \ltimes \mathbf{s} + [\mathbf{x}_1, \mathbf{x}_2]$ can be written as

$$[\mathbf{b}_1, \mathbf{b}_2] = \mathbf{A}^T [\mathbf{s}_1, \mathbf{s}_2] + [\mathbf{x}_1, \mathbf{x}_2]. \tag{12}$$

It is equivalent to

$$\begin{aligned} \mathbf{A}^T \mathbf{s}_1 + \mathbf{x}_1 &= \mathbf{b}_1, \\ \mathbf{A}^T \mathbf{s}_2 + \mathbf{x}_2 &= \mathbf{b}_2. \end{aligned} \tag{13}$$

It is easy to see that this equation contains two $\text{LWE}_{q,\chi}$ instances. From the assumption that it is a simple question to find the vector $\mathbf{s} \in \mathbb{Z}_q^{n/2}$ in the search version $\text{STP-LWE}_{q,\chi,\chi}$ instance $[\mathbf{b}_1, \mathbf{b}_2] = \mathbf{A}^T \ltimes \mathbf{s} + [\mathbf{x}_1, \mathbf{x}_2]$, then (13) is also easily solved. That is, the $\text{LWE}_{q,\chi}$ instance can be solved. This apparently contradicts with the hardness assumption of $\text{LWE}_{q,\chi}$ problem.

Case 2. It is clear that when $k > 2$, n/k-dimensional the STP-LWE problem still holds. The proof of this case is similar to Case 1. This completes the proof. □

With the increase of k value, the security of the n/k-dimensional STP-LWE problem will be reduced. In order to prevent this from happening, n/k in the STP-LWE problem must match the security requirements when the scheme can be reduced to lattice problems resisted to the quantum computing. In GPV08 [22], n/k should be larger than $2n \log q$.

4. Our Scheme

In this section, we give a variant of GPV dual cryptosystem. First, we recall the dual cryptosystem in GPV08 [22]. Then, we give our construction based on n/k-dimensional STP-LWE problem. Meanwhile, the correctness and security are also shown.

4.1. GPV Dual Cryptosystem. It is parameterized by some $r \geq \omega(\sqrt{\log m})$, which specifies the discrete Gaussian distribution $\mathbb{D}_{\mathbb{Z}^m,r}$ from which secret keys are chosen. All the users share a common matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ (an implicit input to all algorithms) chosen uniformly at random, which is the index of the function $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{A}\mathbf{e} \bmod q$. All the operations are performed over $\mathbb{Z}_q$.

(i) *DualKeyGen*: choose an error vector $\mathbf{e} \leftarrow D_{\mathbb{Z}^m,r}$ (i.e., the input distribution to $f_{\mathbf{A}}$), as the secret key. The public key is the syndrome $\mathbf{u} = f_{\mathbf{A}}(\mathbf{e})$.

(ii) *DualEnc*$(\mathbf{u}, b)$: to encrypt a bit $b \in \{0, 1\}$, choose $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ uniformly and $\mathbf{p} = \mathbf{A}^T\mathbf{s} + \mathbf{x} \in \mathbb{Z}_q^m$, where $\mathbf{x} \leftarrow \chi^m$. Output the ciphertext $(\mathbf{p}, c = \mathbf{u}^T\mathbf{s} + x + b \cdot \lfloor q/2 \rfloor) \in \mathbb{Z}_q^m \times \mathbb{Z}_q$, where $x \leftarrow \chi$.

(iii) *DualDec*$(\mathbf{e}, (\mathbf{p}, c))$: compute $b' = c - \mathbf{e}^T\mathbf{p} \in \mathbb{Z}_q$. Output 0 if b' is closer to 0 than to $\lfloor q/2 \rfloor$ modulo q; otherwise output 1.

The correctness and security are given in GPV08 [22], and readers can refer to it for more details.

4.2. STP-GPV Dual Cryptosystem. Our public-key dual cryptosystem is based on n/k-dimensional STP-LWE problem, and we let $k = 2$. It is parameterized by some $r \geq \omega(\sqrt{\log m})$, which specifies the discrete Gaussian distribution $\mathbb{D}_{\mathbb{Z}^{m/2},r}$ from which secret keys are chosen. All the users share a common matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ (an implicit input to all algorithms) chosen uniformly at random, which is the index of the function $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{A} \ltimes \mathbf{e} \bmod q$. All the operations are performed over $\mathbb{Z}_q$.

(i) *VarKeyGen*: choose an error vector $\mathbf{e} \leftarrow D_{\mathbb{Z}^{m/2},r}$ (i.e., the input distribution to f_A), which is the secret key. The public key is the syndrome $\mathbf{u} = f_{\mathbf{A}}(\mathbf{e}) = \mathbf{A} \ltimes \mathbf{e}$, and let $\mathbf{u} = [\mathbf{u}_1, \mathbf{u}_2]$, where $\mathbf{u}_1, \mathbf{u}_2 \leftarrow \mathbb{Z}_q^n$.

(ii) *VarEnc*$(\mathbf{u}_1, \mathbf{u}_2, b_1, b_2)$: to encrypt two bits $b_1, b_2 \in \{0, 1\}$, choose $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ uniformly and $\mathbf{p} = \mathbf{A}^T\mathbf{s} + \mathbf{x} \in \mathbb{Z}_q^m$, where $\mathbf{x} \leftarrow \chi^m$. Output the ciphertext $(\mathbf{p}, c_1 = \mathbf{u}_1^T\mathbf{s} + x_1 + b_1 \cdot \lfloor q/2 \rfloor, c_2 = \mathbf{u}_2^T\mathbf{s} + x_2 + b_2 \cdot \lfloor q/2 \rfloor) \in \mathbb{Z}_q^m \times \mathbb{Z}_q \times \mathbb{Z}_q$, where $x_1, x_2 \leftarrow \chi$.

(iii) *VarDec*$(\mathbf{e}, (\mathbf{p}, c_1, c_2))$: compute $[b_1', b_2']^T = [c_1, c_2]^T - \mathbf{e}^T \ltimes \mathbf{p} \in \mathbb{Z}_q$. Output 0 if b_1' and b_2' are closer to 0 than to $\lfloor q/2 \rfloor$ modulo q; otherwise output 1.

4.3. Correctness and Security. The correctness of our scheme is mainly inherited by GPV dual cryptosystem. We can show the correctness as follows:

$$\begin{aligned}
&[b_1', b_2']^T \\
&\quad = [c_1, c_2]^T - \mathbf{e}^T \ltimes \mathbf{p} \in \mathbb{Z}_q \\
&\quad = \left[\mathbf{u}_1^T\mathbf{s} + x_1 + b_1 \cdot \lfloor q/2 \rfloor, \mathbf{u}_2^T\mathbf{s} + x_2 + b_2 \cdot \lfloor q/2 \rfloor\right]^T \\
&\qquad - \mathbf{e}^T \ltimes \left(\mathbf{A}^T\mathbf{s} + \mathbf{x}\right) \\
&\quad = \left[\mathbf{u}_1^T\mathbf{s}, \mathbf{u}_2^T\mathbf{s}\right]^T + [x_1, x_2]^T \\
&\qquad + [b_1 \cdot \lfloor q/2 \rfloor, b_2 \cdot \lfloor q/2 \rfloor]^T \\
&\qquad - \left[\mathbf{e}^T \ltimes \mathbf{A}^T\mathbf{s}\right] - \left[\mathbf{e}^T \ltimes \mathbf{x}\right].
\end{aligned} \tag{14}$$

Table 1

	k	Size of public key in bits	Size of private key in bits	Ciphertext expansion rate
GPV08	1	$n \log q$	$m \log q$	$m + 1$
Ours	2	$2n \log q$	$\dfrac{m}{2} \log q$	$\dfrac{m}{2} + 1$

Table 2

	k	Time of VarKeyGen in seconds	Time of VarEnc in seconds	Time of VarDec in seconds
GPV08	1	7.746	0.4641	0.001225
Ours	2	3.860	0.2369	0.000817

Since $[\mathbf{e}^T \ltimes \mathbf{A}^T\mathbf{s}] = [\mathbf{A} \ltimes \mathbf{e}]^T\mathbf{s} = [\mathbf{u}_1, \mathbf{u}_2]^T\mathbf{s} = \left[\begin{smallmatrix} \mathbf{u}_1^T \\ \mathbf{u}_2^T \end{smallmatrix}\right]\mathbf{s} = \left[\begin{smallmatrix} \mathbf{u}_1^T\mathbf{s} \\ \mathbf{u}_2^T\mathbf{s} \end{smallmatrix}\right] = [\mathbf{u}_1^T\mathbf{s}, \mathbf{u}_2^T\mathbf{s}]^T$ and $[x_1, x_2]^T - [\mathbf{e}^T \ltimes \mathbf{x}] = [x_1, x_2]^T - [\mathbf{e}^T \otimes \mathbf{I}_2]\mathbf{x}$, let $\delta_1 = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, $\delta_2 = \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$, $[x_1, x_2]^T - [\mathbf{e}^T \ltimes \mathbf{x}] = [x_1, x_2]^T - [\mathbf{e}^T\delta_1\mathbf{x}, \mathbf{e}^T\delta_2\mathbf{x}]^T = [x_1 - \mathbf{e}^T\delta_1\mathbf{x}, x_2 - \mathbf{e}^T\delta_2\mathbf{x}]^T$. Based on GPV08, we have $\|x_1 - \mathbf{e}^T\delta_1\mathbf{x}\| \leq q/5$ and $\|x_2 - \mathbf{e}^T\delta_2\mathbf{x}\| \leq q/5$. Therefore, $\|[x_1, x_2]^T - [\mathbf{e}^T \ltimes \mathbf{x}]\|_\infty = \max\{\|x_1 - \mathbf{e}^T\delta_1\mathbf{x}\|, \|x_2 - \mathbf{e}^T\delta_2\mathbf{x}\|\} \leq q/5$.

The security of this scheme is similar to that of the GPV dual cryptosystem; that is, our scheme is CPA-secure and anonymous under the n/k-dimensional $\mathrm{LWE}_{q,\chi}$ assumption.

5. Performance

The GPV dual cryptosystem and our scheme are implemented in Matlab 2010 in Windows 7 Service Pack1 64 bits operating system. We use a desktop which has a 4-core Intel(R) Core (TM) i3-2120 processor running at 3.30 GHz and 2 GB of RAM.

In this section, we analyze the efficiency of the above schemes from the following two aspects. On one hand, we compare the size of public keys, private keys, and ciphertext expansion of GPV dual cryptosystem with our scheme. From the Table 1, the efficiency of our algorithm and the ciphertext expansion rate has significant advantage compared with GPV dual cryptosystem. On the other hand, we compare the time cost of VarKeyGen, VarEnc, and VarDec with the GPV dual cryptosystem and the STP-GPV dual cryptosystem. Table 2 has demonstrated the time of key generation, encryption, and decryption for 1 bit in GPV dual cryptosystem, and the

Table 3

k	Time of VarKeyGen	VarEnc for 1 time	VarEnc for 1 bit	VarDec for 1 time	VarDec for 1 bit
5	1.396	0.1552	0.03104	$8.17e-4$	$1.634e-4$
10	0.7361	0.1448	0.01448	$1.14e-3$	$1.14e-4$
50	0.2253	0.1438	0.002876	$7.201e-3$	$1.44e-4$
100	0.06797	0.1465	0.001465	$1.3305e-2$	$1.331e-4$
500	0.01594	0.1555	0.000311	$6.3646e-2$	$1.273e-4$

time of key generation encryption and decryption for 1 time (which encryption and decryption 2 bits) in STP-GPV dual cryptosystem. The experimental parameters are depicted as follows: $n = 250$, $m = 8000$, and $q = 127$. We obtain these results by running 100 times VarKeyGen, VarEnc, and VarDec and taking the averages.

By experiments, it is proved that the key generation time and encryption time of our scheme are only half of that of the GPV dual cryptosystem's, while the decryption time is roughly equal to GPV dual cryptosystem's.

6. Discussion and Conclusions

In this section, we apply n/k-dimensional STP-LWE in the GPV dual cryptosystem problem and build an extended GPV dual cryptosystem. We know that the size of the secret key space varies inversely with the value of k in this proposed extended cryptosystem. For different $k \in \mathbb{Z}$, secret keys of length m/k should satisfy the following security requirements. The first restrict is that the value of m/k should be greater than $2n \log q$ in order to resist the lattice-based reduction algorithm. In this paper, since we pick $n = 250$, $m = 8000$, and $q = 127$, we should choose $k < 3$.

The second condition is that the private key should satisfy the inequality $q^{m/k} > 2^{80}$ in order to resist brute-force attacks. Considering the value n, m, and q, we require $k < 700$. The following table lists the time of key generation, encryption, and decryption for one time in 5 different security levels.

In Table 3, it shows that the time of key generation and the time required for encryption one bit plaintext is reduced gradually with the increasing value of k. At the same time, the time for decrypting one bit ciphertext in different security levels has changed a little.

In this paper, we construct a flexible lattice based scheme based on STP-LWE, which is a variant of learning with errors problem. Our scheme can achieve a balance between the security and efficiency in the hierarchical encryption systems. By using STP-GPV dual cryptosystem, the whole system can reset the security level for messages with the same security parameter.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to thank the reviewers for their helpful advices. The National Natural Science Foundation of China (Grant nos. 61170269 and 61121061), the Beijing Natural Science Foundation (Grant no. 4142016), the Program for New Century Excellent Talents in University (no. NCET-11-0565), the Fundamental Research Funds for the Central Universities (no. 2012JBZ010), and the Program for Changjiang Scholars and Innovative Research Team in University (no. IRT201206) are gratefully acknowledged.

References

[1] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC '96)*, pp. 99–108, ACM, 1996.

[2] M. Ajtai and C. Dwork, "The first and fourth public-key cryptosystems with worst-case/ average-case equivalence," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 14, no. 097, 2007.

[3] O. Goldreich, S. Goldwasser, and S. Halevi, "Eliminating decryption errors in the Ajtai-Dwork cryptosystem," in *Advances in Cryptology—CRYPTO '97*, vol. 1294 of *Lecture Notes in Computer Science*, pp. 105–111, Springer, Berlin, Germany, 1997.

[4] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: a ring-based public key cryptosystem," in *Algorithmic Number Theory*, vol. 1423 of *Lecture Notes in Computer Science*, pp. 267–288, Springer, Berlin, Germany, 1998.

[5] O. Regev, "New lattice-based cryptographic constructions," *Journal of the ACM*, vol. 51, no. 6, pp. 899–942, 2004.

[6] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, article 34, 2009.

[7] N. Dottling, J. Mller-Quade, and A. C. A. Nascimento, "IND-CCA secure cryptography based on a variant of the LPN problem," in *Advances in Cryptology—ASIACRYPT 2012*, vol. 7658 of *Lecture Notes in Computer Science*, pp. 485–503, Springer, Berlin, Germany, 2012.

[8] X.-Y. Yang, L.-Q. Wu, M.-Q. Zhang, and X.-F. Chen, "An efficient CCA-secure cryptosystem over ideal lattices from identity-based encryption," *Computers and Mathematics with Applications*, vol. 65, no. 9, pp. 1254–1263, 2013.

[9] C. Peikert, V. Vaikuntanathan, and B. Waters, "A framework for efficient and composable oblivious transfer," in *Advances in Cryptology—CRYPTO 2008*, vol. 5157 of *Lecture Notes in Computer Science*, pp. 554–571, Springer, Berlin, Germany, 2008.

[10] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," in *Advances in Cryptology—EUROCRYPT 2010*, vol. 6110 of *Lecture Notes in Computer Science*, pp. 553–572, Springer, Berlin, Germany, 2010.

[11] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical leakage-resilient identity-based encryption from simple assumptions," in *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10)*, pp. 152–161, October 2010.

[12] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," in *Proceedings of the 3rd Conference on Innovations in Theoretical Computer Science (ITCS '12)*, pp. 309–325, January 2012.

[13] D. Cash, D. Hofheinz, and E. Kiltz, "How to delegate a lattice basis," *IACR Cryptology EPrint Archive*, vol. 2009, no. 351, 2009.

[14] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Advances in Cryptology—EUROCRYPT 2005*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 440–456, Springer, Berlin, Germany, 2005.

[15] D.-Z. Cheng and L.-J. Zhang, "On semi-tensor product of matrices and its applications," *Acta Mathematicae Applicatae Sinica. English Series*, vol. 19, no. 2, pp. 219–228, 2003.

[16] B. Gao, H. Peng, D. Zhao, W. Zhang, and Y. Yang, "Attractor transformation by impulsive control in boolean control network," *Mathematical Problems in Engineering*, vol. 2013, Article ID 674571, p. 5, 2013.

[17] B. Gao, L. Li, H. Peng et al., "Principle for performing attractor transits with single control in Boolean networks," *Physical Review E*, vol. 88, no. 6, Article ID 062706, 2013.

[18] Z. Wang, S. Kokubo, J. Tanimoto et al., "Insight into the so-called spatial reciprocity," *Physical Review E*, vol. 88, no. 4, Article ID 042145, 2013.

[19] W. J. Yuan, J. F. Zhou, Q. Li et al., "Spontaneous scale-free structure in adaptive networks with synchronously dynamical linking," *Physical Review E*, vol. 88, no. 2, Article ID 022818, 2013.

[20] Y. Zhao, X. Gao, and D. Cheng, "Semi-tensor product approach to Boolean functions," Preprint, 2010.

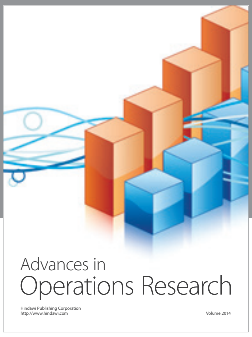
[21] D. W. Zhao, H. P. Peng, L. X. Li et al., "Novel way to research nonlinear feedback shift register," *Science China Information Sciences*, 2014.

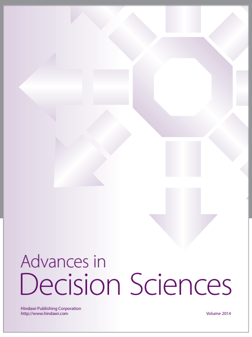
[22] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, pp. 197–206, May 2008.

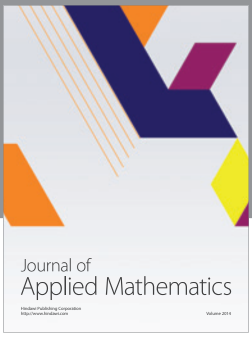
[23] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, Springer, 2002.

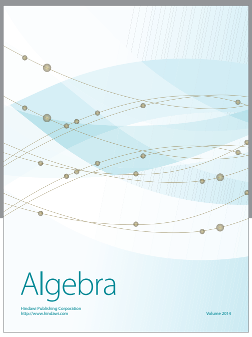
[24] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007.

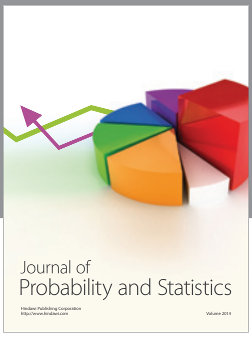
[25] C. Peikert, "Limits on the hardness of lattice problems in l_p norms," *Computational Complexity*, vol. 17, no. 2, pp. 300–351, 2008.


Advances in Operations Research

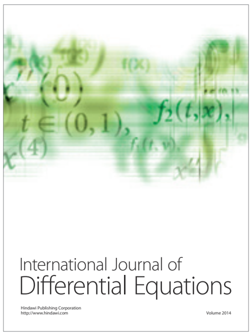

Advances in Decision Sciences


Journal of Applied Mathematics

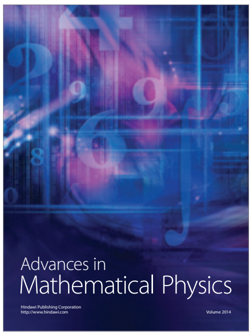

Algebra

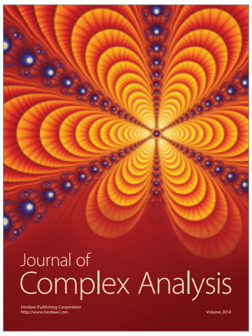

Journal of Probability and Statistics

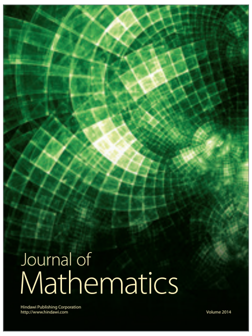
The Scientific World Journal

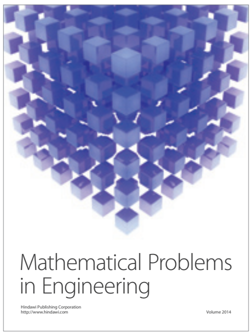

International Journal of Differential Equations

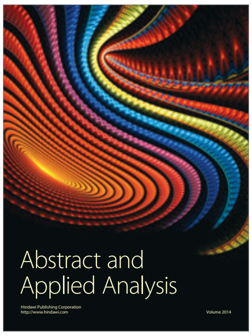
International Journal of Combinatorics

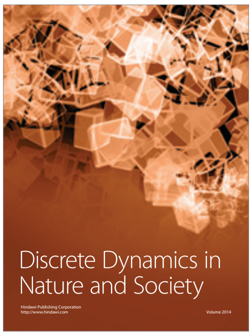

Advances in Mathematical Physics

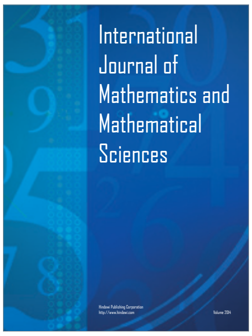

Journal of Complex Analysis


Journal of Mathematics


Mathematical Problems in Engineering

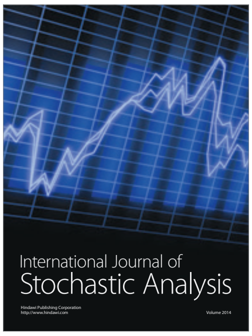

Abstract and Applied Analysis


Discrete Dynamics in Nature and Society


International Journal of Mathematics and Mathematical Sciences

Journal of Discrete Mathematics

Journal of Function Spaces


International Journal of Stochastic Analysis

Journal of Optimization