One Improved RLWE-based FHE and Fast Private Information Retrieval

Wei-Tao Song*, Bin Hu and Xiu-Feng Zhao
The PLA Strategic Support Force Information Engineering University
Zhengzhou 450001, China
[e-mail: weitaosong@163.com, hb2110@126.com, and zhaoxiufeng@163.com]
*Corresponding author: Wei-Tao Song

Received January 5, 2019; revised May 3, 2019; accepted June 24, 2019; published December 31, 2019

Abstract

With the rapid development of cloud computing, it raises real questions on privacy protection, which greatly limits the use of cloud computing. However, fully homomorphic encryption (FHE) can make cloud computing consistent with privacy. In this paper, we propose a simpler FHE scheme based on ring LWE problem, with a smaller size of ciphertext and a lower noise-expansion factor for homomorphic multiplication. Then based on our optimized RLWE-based FHE scheme, we propose a fast single-database private information retrieval protocol, combining with batching and number theoretic transform technology.

Keywords: Cloud Computing, Privacy Protection, Fully Homomorphic Encryption, Private Information Retrieval, Ring Learning with Error.

The authors would like to thank the anonymous reviewers for helpful comments. This work was sponsored in part by the National Natural Science Foundation of China [Grant-No. 61902428,61601515], and was also supported by the Foundation of Science and Technology on Information Assurance Laboratory (No.KJ-15-006).

http://doi.org/10.3837/tiis.2019.12.025 **ISSN : 1976-7277**

1. Introduction

With the development of information technology, cloud computing has turned into a hot topic [1, 2]. Users can enjoy the excellent data computing performance of cloud computing, and not need care about the complex hardware management. However, for some private data (e.g.medical records or account informations), it is unsuitable or illegal to publicly stored in the cloud. Thus greatly limit the applications of cloud computing. Fortunately, the appearance of fully homomorphic encryption (FHE) makes cloud computing easier to be consistent with privacy.

In 1978, FHE was firstly proposed by Rivest et al.[3]. It allows arbitrarily complex evaluation on encrypted data. It is an encryption scheme ε with an efficient algorithm $Evaluate_\varepsilon$ that, for any effective ciphertexts $c_i \leftarrow Enc_\varepsilon(pk, m_i)$ and function f, outputs $c = Evaluate_\varepsilon(f, c_1, c_2, ..., c_t)$ with

$$Dec(sk, c) = Dec(sk, Evaluate_\varepsilon(f, c_1, c_2, ..., c_t)) = f(m_1, m_2, ..., m_t).$$

Based on FHE, users can take advantage of the excellent data computing ability of the cloud server, without leaking private data.

For example, an user Alice can upload her private data encrypted with an FHE scheme to the cloud server. When she wants the cloud server to manipulate some private data $m_1, ..., m_t$, she sends a description of manipulation f and the corresponding encrypted data to cloud server. The cloud server runs an *Evaluate* algorithm and sends the result to Alice later. Thus, Alice can derive $f(m_1, ..., m_t)$ after decryption. The cloud never gets any unencrypted data throughout this process. Moreover, the fuction f in *Evaluate* algorithm can also be encrypted with the same FHE scheme. See **Fig. 1**.

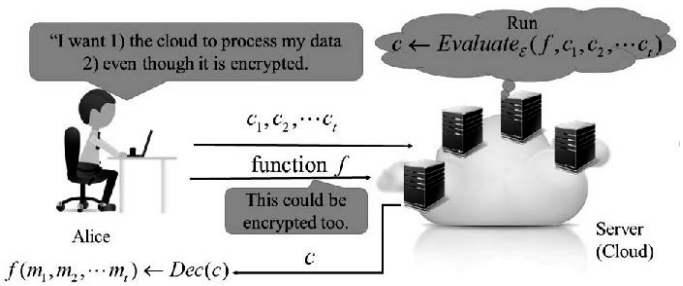

Fig. 1. Private Cloud Computing based on FHE

However, how to construct an FHE scheme has puzzled people for more than 30 years[4]. In 2009, Gentry constructed the first FHE scheme[5]. After Gentry's breakthrough work, many of its implementations and improved schemes are proposed. They are based on different cryptographic assumptions: approximate greatest common divisors [6-10], standard learning with errors (LWE) [11-16], and ring-LWE (RLWE) [17-21].

Note that, for a pure FHE scheme, Gentry's bootstrapping technology is still essential. Unfortunately, the computation of bootstrapping technology is very expensive, despite a lot of efforts have been taken to improve its efficiency. Recent studies on FHE schemes are divided into two categories: improving the efficiency of bootstrapping technology or building

efficient leveled FHE scheme without bootstrapping. For the latter, the key lies in reducing the noise-expansion factor for homomorphic multiplication.

The Number Theoretic Transform (NTT), analogous to the well known fast fourier transform (FFT), can be used to effectively speed up the modular polynomial multiplications as described in Schonhage-Strassen multiplication algorithm [22]. Thus, our research is readily portable to the RLWE world. Note that, one of key features in the Gentry-Sahai-Waters (GSW) FHE scheme[15] is asymmetric noise growth on homomorphical multiplications. By taking advantage of the feature, it can get a a polynomial-factor error growth when performing a long chain of homomorphic multiplications , which this often incurs an exponential-factor error growth for other FHE schemes. This feature of asymmetric noise growth is important for building high-performance leveled FHE scheme without bootstrapping.

But so far, the study for improving the noise performance of RLWE-based GSW system is seldom. Most relevant works are focused on improving the bootstrapping technology of GSW system[23,24], introducing packing technology into GSW system[25], or establishing new identity-based/attribute-based FHE based on GSW system, etc. [26]. The main achievement is the work [17] of Khedr *et al.,* "They propose an optimized RLWE-based implementation of GSW-FHE schemes, and reduce the size of ciphertext in [15,16] from $N \times N$ to $N \times 2$, where $N = n \times logq$. But same as [15,16], the expansion factor for noise over homomorphic multiplication is still $N = n \times logq$. Moreover, there are some security problems in their scheme.

The quest for private information retrieval (PIR) protocol. PIR plays a very important role in private outsourcing storage and computation for cloud computing. It provides a protocol to retrieve a database from cloud server, but the cloud server does not learn any information on which item is retrieved. More formally, we model the database of cloud server as a t-bit string x. And a user wants to retrieve the i-th bit x_i privately while the server does not learn i at all. The main functionality indexes for PIR protocol are communication complexity and computational complexity. The security of PIR protocol can be divided into computational security and information-theoretic security. Their difference lies in which capable adversary to resist. The former need to resist an adversary with unlimited computational capability, and the latter only need to resist an adversary with limited computational capability. In this paper, the security of PIR protocol is referred to computational security.

The first computational PIR protocol was introduced by Kushilevitz and Ostrovsky [27]. In 2007, paper [28] studied on the computational practicality of PIR protocol. They concluded that any computational PIR scheme is less efficient than trivial PIR scheme, since for every bit of database, computational PIR protocol need one or more modular multiplications. Later, by revisiting the performance analysis, paper [29] proposed an lattice-based PIR protocol, which is efficient than the trivial PIR.

In all these constructions, the key lies in how to find an efficient scheme based on a difficult computational problem. The aforementioned scheme use various methods and tools to construct computational PIR protocols. However, it is obvious that given an FHE scheme implementing a PIR construction is conceptually as simple as performing normal informat computational ion retrieval. Besides, Based on FHE schemes, it can evidently reduce the communication complexity of PIR protocol. Thus , we focus only on computational PIR protocol from FHE in this paper.

Prior works. In 2009, a single-database PIR protocol with sub-linear communication complexity is sketchily described by Gentry [5]. Later, a general framework that combines FHE with encryption scheme of symmetric key is proposed by Brakerski and Vaikuntanathan in 2011 [12]. In TKDE13 [31], a more efficient PIRprotocol was proposed, called XMREF-PIR protocol for short. In 2014, a somewhat FHE scheme based on number theory research unit (NTRU) was customized [32]. In 2015, a fast PIR protocol based on RLWE-based GSW-FHE scheme was proposed.[17]. And in [33], an analysis of PIR scheme based on FHE was made. In 2016, a PIR protocol based on RLWE-based FHE scheme was proposed [34], which has the currently best performance on communication complexity for single database server. However, one of the drawbacks of their scheme is the need to perform expensive key switching operations.

Contributions. In this paper, we improve the RLWE-based GSW [17] in the aspect of safety, efficiency, and ciphertext size. In [17], they proposed an RLWE-based GSW based on only one RLWE distribution instance, which is not safe. Note that, it needs many RLWE distribution instancesinstances for RLWE-based FHE schemes to ensure the safety. For example, it needs $\Omega(((n+\ell)logq)+\omega(log\lambda))$ RLWE distribution instances for Regev scheme. In [17], although they introduced (LWE+LWE) model, which can reduce the number of LWE distribution instances, their scheme[17] still needs at least $n+\ell$ RLWE distribution instances to ensure the safety. Thus, we firstly improved the safety of scheme [17] by introducing adequate RLWE distribution instances. In this paper, we cut down the noise-growth rate for homomorphic multiplication for paper [17] from $\Theta(nlogq)$ to $\Theta(n)$. This mainly benefits from an important property of GSW scheme found by us. The property is as follows. When executing an encryption operation, multiplying the plaintext by an integer $k \in Z_q$, the error after one homomorphic multiplication of GSW scheme can be reduced to approximately $1/t$. See section 3 for more details. Meanwhile, by taking full advantage of this property, we eliminate "flatten" operation of paper [17] and obtain a technically simpler variant and smaller sizes of keys and ciphertexts.

Next, combining with batching and NTT technology, a fast single-database PIR protocol based on our optimized RLWE-based GSW scheme is proposed.

Organization. The rest of this paper is organized as follows. We define notational conventions and present some definitions and theorems on FHE, bootstrapping and RLWE assumption In Section 2. In Section 3, an improved RLWE-based GSW-FHE scheme is presented. In Section 4, a fast single-database PIR from our optimized RLWE-based GSW scheme is presented. And in Section 5, we make an implementation of PIR protocol based on our optimized RLWE-based GSW scheme, together with other three representative PIR protocols from FHE. Finally, Section 6 concludes.

2. Preliminaries

Basic Notations. In our construction, R represents either an integer ring or a polynomial ring. An element of R is written in lower-case letters, e.g., $r \in R$. The ℓ_∞ norm (the maximum norm) of vector v is denoted by $\|v\|_\infty$. If v is a polynomial ring vector, then $\|v\|_\infty = max\{\|v_i\|_\infty\}$. A matrix of ring elements is written in capital letter, e.g., $A \in R^{n\times m}$, and the i-th column vector of matrix A is denoted by a_i.

We denote the integer ring by $\mathbb{Z}$, and denote the scalar multiplication by '$\cdot$'. Rounding to the nearest integer is denoted by $\lfloor x \rceil$, and rounding down to the nearest integer is denoted by $\lfloor x \rfloor$. By $x \xleftarrow{\$} \mathbb{D}$, we denote the x is sampled form a distribution $\mathbb{D}$, and $a \xleftarrow{u} \mathbb{G}$, means that, a is chosen uniformly from.

2.1 Fully Homomorphic Encryption

Definition 2.1 (Homomorphic), For and any plaintexts $\mu_1,\ldots,\mu_l$, any ciphertexts $c_1,\ldots,c_l$, and any depth circuit f, if it holds that

$$\Pr[Dec_{sk}\left(Eval_{evk}\left(f,c_1,\ldots,c_l\right)\right) \neq f\left(\mu_1,\ldots,\mu_l\right)] = negl(n)$$

where $\left(pk,sk,evk\right) \leftarrow KeyGen(1^{\lambda})$ and $c_i = Enc_{pk}\left(\mu_i\right)$. Then the scheme is L-Homomorphic

Definition 2.2 (Compactness, Leveled and Fully Homomorphic Decryption), A homomorphic scheme is compact if and only if its decryption circuit and evaluated function are independent. If, A homomorphic scheme puts 1^L as an additional input in key generation, then it is leveled fully homomorphic if it. If, for any polynomial L, A homomorphic scheme is compact and L-Homomorphic, then it is FHE scheme.

2.2 RLWE Assumption

The LWE assumption was firstly introduced by Regev [35] in 2009. In Eurocrypt 2010, Lyubashevsky et al., "[36] extended LWE assumptions from integers to polynomial rings, and got a better performance on efficiency.

Definition 2.3 (RLWE Assumption), Let $R = \mathbb{Z}[X]/\Phi_m(X)$ be a polynomialring, where $\Phi_m(X)$ is an irreducible m-th cyclotomic polynomial. Let χ be a standard deviation of the discrete Gaussian error distribution over R_q. Sample polynomial $s \xleftarrow{u} R_q$, and $a_i \xleftarrow{u} R_q$. For any given k pairs $(a_i, b_i = a_i \cdot s + e_i)_{i=1}^{k}$, b_i is computationally indistinguishable from uniform over R_q, where $e_i \xleftarrow{\$} \chi_i$.

3. Improved RLWE-Based GSW-FHE Scheme

In this section, we begin by presenting our improved RLWE-based GSW-FHE scheme (IRGSW) with an analysis of correctness and security. Then we discuss the performance on noise reduction and size of ciphertext for our IRGSW scheme, compared to the scheme of [17].

3.1 IRGSW scheme

Our IRGSW scheme is described detailed as follows.

- $IRGSW.Setup(1^{\lambda},1^{L})$: The parameters of the scheme are the security parameter λ, the upper bound L for tolerant multiplicative depth, a lattice dimension $n = n(\lambda, L)$, a modulus

$q = q(\lambda, L) \in \mathbb{Z}^+$ of l bits, an irreducible polynomial $g(x) = x^{n-1} + 1$, a ring $R = \mathbb{Z}[x]/(g(x))$ and its quotient ring modulo $q, R_q = \mathbb{Z}_q[x]/(g(x))$, a standard deviation of discrete gaussian error distribution χ over R_q with $\|\chi\|_\infty \le B$, and parameter $m = m(\lambda, L)$, appropriately chosen in order to achieve at least 2^λ security against known LWE attacks.

• $IRGSW.KeyGen(1^\lambda, 1^L)$: Sample a ring vector $\mathbf{a} \xleftarrow{u} R_q^m$, a secret polynomial $t \xleftarrow{\$} \chi$, and an error vector $\mathbf{e} \xleftarrow{\$} \chi^m$. Compute $\mathbf{b} = t \cdot \mathbf{a} + \mathbf{e}$. Then set secret key vector $sk = \mathbf{s} = (1, t) \in R_q^2$, and public key $pk = A$ to be the 2-column matrix made up of $\mathbf{b}$ followed by the $-\mathbf{a}$, namely $A = [\mathbf{b} - \mathbf{a}] \in R_q^{m \times 2}$. Note that

$$A \times \mathbf{s} = \mathbf{b} - t \cdot \mathbf{a} = \mathbf{e}.$$

(Note that, in the paper [17], the public key is $A = [b - a] \in R_q^{1 \times 2}$. This means their RLWE-based GSW scheme is based on only one RLWE distributioninstance. It is unsafe. In our paper, we set the numbers of RLWE distribution instances be m.)

• $IRGSW.Enc(pk, \mu)$: To encrypt a constant polynomial $\mu \in R_p (p << q)$, sample $K \xleftarrow{u} R_2^{2 \times m}$, $X \xleftarrow{\$} \chi^{2 \times 2}$ and output the ciphertext C given below

$$C = \left[\left\lfloor \frac{q}{p} \right\rfloor \cdot \mu \cdot I_2 + K \cdot A + X \right]_q \in R_q^{2 \times 2}.$$

(As opposed to $C_{N \times 2}$ in [17], where $N = 2 \times logq$, we have a smaller size of ciphertext.)

• $IRGSW.Dec(sk, C)$: First, compute

$$C \cdot s = \left\lfloor \frac{q}{p} \right\rfloor \cdot \mu \cdot \mathbf{s} + K \cdot \mathbf{e} + X \cdot \mathbf{s} \approx \left\lfloor \frac{q}{p} \right\rfloor \cdot \mu \cdot \mathbf{s} \; mod \; q$$

Let the first component of vector $C \cdot \mathbf{s}$ be denoted by x. Then μ can be extracted from x by $\left[\left\lfloor \frac{p}{q} \cdot x \right\rceil \right]_p$. Actually, to decrypt, we only compute $\mu = \left[\left\lfloor p \cdot [< \mathbf{c}_1, \mathbf{s} >]_q / q \right\rceil \right]_p$, where $\mathbf{c}_1$ is the first row vector of C.

(As opposed to $Dec(sk, C) = C_{N \times 2} \times s_{2 \times 1}$ in [17], we have fewer operations in Dec by a factor of $logn$ times.)

• $C_1 \oplus C_2$: Output $C_{add} = [C_1 + C_2]_q \in \mathbb{R}_q^{2 \times 2}$ as the result of homomorphic addition between the input ciphertexts.

• $C_1 \otimes C_2$: Output $C_{mult} = [\lfloor \frac{p}{q} C_1 \cdot C_2 \rceil]_q \in \mathbb{R}_q^{2 \times 2}$ as the result of homomorphic multiplication between the input ciphertexts.

3.2 Correctness and Security

Correctness. We discuss the noise magnitude at encryption and decryption. Firstly, Lemma 3.1 gives the noise magnitude at encryption of our scheme IRGSW.

Lemma 3.1 *(Encryption Noise),* Let the parameters n, m, q, l, and χ be the parameters of our scheme IRGSW, and $\mu \in R_p (p << q)$. Set $(sk, pk) = (\mathbf{s}, A) \leftarrow IRGSW.KeyGen(1^{\lambda}, 1^{L})$ and $C \leftarrow IRGSW.Enc(A, \mu)$. Then for some $\mathbf{e}$ with $\|\mathbf{e}\|_{\infty} \le m \cdot n \cdot B + n \cdot B^2 + B$ it holds that

$$[C \cdot \mathbf{s}]_q = [\lfloor q / p \rfloor \cdot \mu \cdot \mathbf{s} + \mathbf{e}]_q$$

Proof. By definition

$$[C \cdot \mathbf{s}]_q = [\lfloor q / p \rfloor \cdot \mu \cdot \mathbf{s} + K \cdot \mathbf{e} + X \cdot \mathbf{s}]_q$$

Since $g(x) = x^{n-1} + 1$, $K \xleftarrow{u} R_2^{2 \times m}$, $\mathbf{e} \xleftarrow{\$} \chi^m$, $X \xleftarrow{\$} \chi^{2 \times 2}$, $t \xleftarrow{\$} \chi$, $s = (1, t)$, and $\|\chi\|_{\infty} \le B$, then $\|[K \cdot \mathbf{e} + X \cdot \mathbf{s}]_q\|_{\infty} \le m \cdot n \cdot B + n \cdot B^2 + B$. Lemma 3.1 is proved.

Next, we discuss the correctness of decryption for ciphertexts in Lemma 3.2. The proof is easily proved according to Regev[35] and is omitted.

Lemma 3.2 (Decryption Noise),Let parameters n, m, q, l, and χ be the parameters of our scheme IRGSW. Suppose secret key $s \in R_q^2$ and $C \in R_q^{2 \times 2}$ be such that $[C \cdot \mathbf{s}]_q = [\lfloor q / p \rfloor \cdot \mu \cdot \mathbf{s} + \mathbf{e}]_q$ with $\mu \in R_p (p \ll q)$ and $\|e\|_{\infty} \le \lfloor q / p \rfloor / 2$. Then $IRGSW.Dec(sk, C) = \mu$.

From Lemma 3.2 we can get that the upper bound of decryption noise in our scheme is $\lfloor q / p \rfloor / 2$. Since the encryption noise $\|e\|_{\infty} \le m \cdot n \cdot B + n \cdot B^2 + B \ll \lfloor q / p \rfloor / 2$, then the correctness of our decryption function $IRGSW.Dec(sk, C)$ is guaranteed.

Security. The security of our scheme is guaranteed if we can prove that the joint distribution $(A, K \cdot A + X)$ is computationally indistinguishable from uniform over $R_q^{m \times 2} \times R_q^{2 \times 2}$. Since the rows of $(K \cdot A + X)$ are simply encryptions of 0 of Lindner and Peikert(LP)[42] for dimension n. Thus, the security of our scheme follows in a straightforward way from Lemma 3.3 below, which is used to prove the security of the encryption scheme of Lindner and Peikert[42].

Lemma 3.3 (Implicit in [42]) Let $params = (n, q, \chi, m)$ be what the $RLWE_{n,q,\chi,m}$ assumption holds, and sample a ring vector $\mathbf{a} \xleftarrow{u} R_q^m$, a secret polynomial $\mathbf{t} \xleftarrow{\$} \chi$, and an error vector $\mathbf{e} \xleftarrow{\$} \chi^m$. Compute $\mathbf{b} = t \cdot \mathbf{a} + \mathbf{e}$. Then let A be the 2-column matrix made up of $\mathbf{b}$ followed by the $-\mathbf{a}$, namely $A = [\mathbf{b} - \mathbf{a}] \in R_q^{m \times 2}$. Sample $K \xleftarrow{u} R_2^{2 \times m}$, and $X \xleftarrow{\$} \chi^{2 \times 2}$. If $m > n + log\, q$, then it holds that the joint distribution $(A, K \cdot A + X)$ is computationally indistinguishable from uniform over $R_q^{m \times 2} \times R_q^{2 \times 2}$.

Proof. The proof is easy. Assume that there exists a distinguisher $\mathcal{D}$ with probability polynomial-time. And distinguisher $\mathcal{D}$ can distinguish $(A, K \cdot A + X)$ from uniform over

$R_q^{m\times 2} \times R_q^{2\times 2}$ with non-negligible advantage ε. It is straightforward that $\mathcal{D}$ gives a distinguisher of LP scheme [42]. From the proof of LP scheme, we know that there is no such distinguisher. Thus, Lemma 3.3 is proved.

3.3 Homomorphic Performance

1) **Homomorphic Noise**

a) C_{add} : Set $\mathbf{s} \leftarrow (1,t) \in R_q^2$. Let $C_1 \in R_q^{2\times 2}$, and $C_2 \in R_q^{2\times 2}$ be both 'fresh' ciphertexts encrypted under the same key $\mathbf{s}$, $B' = m \cdot n \cdot B + n \cdot B^2 + B$ be the original bound on the error of a fresh encryption of R_p, and $C_{add} = C_1 \oplus C_2$. It is easy to prove that $\mathbf{e}_{add} = \mathbf{e}_1 + \mathbf{e}_2 \ mod\ q$. Meanwhile, since C_1 and C_2 are both 'fresh' ciphertexts, thus

$$\| \mathbf{e}_{add} \|_\infty \le 2B' \ll \lfloor q / p \rfloor / 2$$

, then homomorphic addition on ciphertexts is guaranteed.

b) C_{mult} : Set $C_1 \in R_q^{2\times 2}$, and $C_2 \in R_q^{2\times 2}$ be both input 'fresh' ciphertexts encrypted under the same key $\mathbf{s} = (1,t)$, and

$$C_{mult} = C_1 \otimes C_2 = \lfloor \frac{p}{q} C_1 \cdot C_2 \rceil$$

. Then compute

$$\begin{aligned}
\left[C_{mult} \cdot \mathbf{s}\right]_q &= \left[\lfloor \frac{p}{q} C_1 \cdot C_2 \rceil \cdot \mathbf{s}\right]_q = \left[\frac{p}{q} C_1 \cdot C_2 \cdot \mathbf{s} + \delta_1\right]_q \\
&= \left[\frac{p}{q} \cdot C_1 \left(\left\lfloor \frac{q}{p} \right\rfloor \cdot \mu_2 \cdot \mathbf{s} + \mathbf{e_2} \right) + \delta_1 \right]_q \\
&= \left[\mu_2 \cdot (C_1 \cdot \mathbf{s}) + \frac{p}{q} \cdot C_1 \cdot \mathbf{e_2} + \delta_1 + \delta_2 \right]_q \\
&= \left[\mu_2 \cdot \left(\left\lfloor \frac{q}{p} \right\rfloor \cdot \mu_1 \cdot \mathbf{s} + \mathbf{e_1} \right) + \delta_1 + \delta_2 + \delta_3 \right]_q \\
&= \left[\left\lfloor \frac{q}{p} \right\rfloor \cdot (\mu_1 \cdot \mu_2) \cdot \mathbf{s} + \delta_1 + \delta_2 + \delta_3 + \delta_4 \right]_q
\end{aligned}$$

Where

$$\boldsymbol{\delta_1} = \left[\left(\lfloor \frac{p}{q} C_1 \cdot C_2 \rceil - \frac{p}{q} C_1 \cdot C_2 \right) \cdot \mathbf{s} \right]_q, \quad \boldsymbol{\delta_2} = \left[\frac{p}{q} \cdot \left(\left\lfloor \frac{q}{p} \right\rfloor - \frac{q}{p} \right) \cdot \boldsymbol{\mu}_2 \cdot C_1 \cdot \mathbf{s} \right]_q, \ \boldsymbol{\delta_3} = \left[\frac{p}{q} \cdot C_1 \cdot \mathbf{e_2} \right]_q,$$

and $\boldsymbol{\delta_4} = \left[\boldsymbol{\mu}_2 \cdot \mathbf{e_1}\right]_q$.

Thus,

$$\begin{aligned}\| \mathbf{e}_{\mathbf{mult}} \|_\infty &= \| \delta_1 + \delta_2 + \delta_3 + \delta_4 \|_\infty \le \| \delta_1 \|_\infty + \| \delta_2 \|_\infty + \| \delta_3 \|_\infty + \| \delta_4 \|_\infty \\ &\le \frac{1}{2} \| s \|_\infty + p \cdot (p-1) \cdot (n \cdot B + 1) + 2p \cdot n \| \mathbf{e}_2 \|_\infty + (p-1) \cdot \| \mathbf{e}_1 \|_\infty \\ &< (2n+1) \cdot p \cdot B'\end{aligned}$$

Since $\| \mathbf{e}_{\mathbf{mult}} \|_\infty < (2n+1) \cdot p \cdot B' \ll \lfloor q / p \rfloor / 2$, correctness is guaranteed. Meanwhile, as opposed to [17], the error of $C_{mult} = C_1 \odot C_2$ is about n times of fresh error, of which in [17] is $n \times logn$. That is, we have a better performance on noise reduction than [17].

Next, we compare our scheme to [17] in detail.

2) **Advantage**

Suppose we have the same set of $params = (n, q, \chi, m)$ with scheme [16, 17]. Let the bit-string length of $q = \Theta(2^n)$ is $l = \lceil \log_2 q \rceil$ be the of of modulus, and $N = n \cdot l = \Theta(n^2)$. **Table 1** shows the concrete comparisons of parameters among [16], [17] and IRGSW scheme.

Table 1. Comparisons of parameters among scheme [16], [17] and IRGSW scheme

Scheme	Public key bitsize	Ciphertext bitsize	Noise-growth rate	Security hardness problems
Scheme [16]	$\Theta(n^2 \cdot log^2\ q)$	$\Theta(n^2 \cdot log^2\ q)$	$\Theta(\sqrt{n \cdot log\ q})$	$LWE + LHL$
Scheme [17]	$\Theta(n^2 \cdot log\ q)$	$\Theta(n \cdot log^2\ q)$	$\Theta(n \cdot log\ q)$	$RLWE + RLWE$
IRGSW	$\Theta(n^2 \cdot log\ q)$	$\Theta(n \cdot log\ q)$	$\Theta(n)$	$RLWE + RLWE$

From **Table 1**, compared to [17], we can get that our scheme has a smaller dimension of ciphertext and a better performance on noise reduction from $\Theta(n \cdot log\ q)$ to $\Theta(n)$. And although scheme [16] has a slight advantage on performance of noise-growth rate than our scheme, it has a poor performance on the efficiency and sizes of public key and ciphertext, compared to other two RLWE-based schemes. In summary, our scheme is the fastest, and has the best performance almost in all aspects among the three FHE schemes.

4. Fast Single-Database PIR Based on Our IRGSW Scheme

In this section, we propose a fast PIR protocol by taking full advantage of our IRGSW scheme, combined with batching and NTT technology.

4.1 Our Basic PIR Protocol from IRGSW

We present our PIR protocol $PIR = (PIR.Setup, PIR.Query, PIR.Response, PIR.Decode)$ in formal description and sketch the flaw of PIR protocol given in **Fig. 2**. Let t be the size of retrieval database, and the index k be written in the binary representation, denoted as $k = (k_1, ..., k_l)$, where $k_i \in \mathbb{Z}_2$ with $1 \le i \le l$ and $l = \lfloor log\ t \rfloor + 1$.

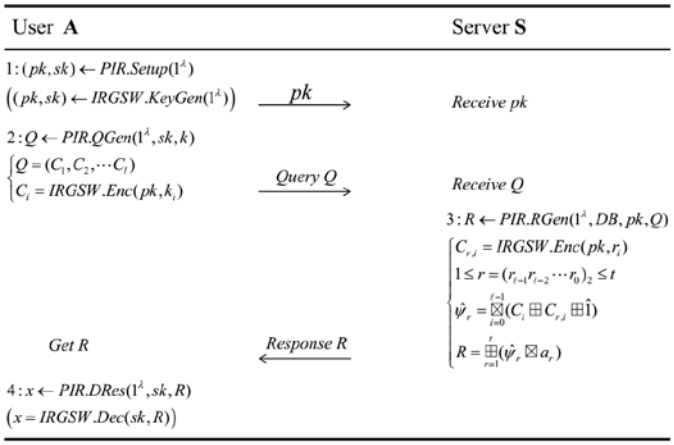

Fig. 2. Our PIR protocol interacts with sender S and receiver R

- $(pk,sk) \leftarrow PIR.Setup(1^\lambda)$: At the setup phase, the user A generates keys based on our IRGSW system $(pk,sk) \leftarrow IRGSW.KeyGen(1^\lambda)$ and sends the public key sk to the server S.

- $Q \leftarrow PIR.QGen(1^\lambda, sk, k)$: At the query generation phase, firstly, the user A computes $C_i = IRGSW.Enc(pk,k_i)$ with $1 \le i \le l$ and generates the query $Q=(C_1,C_2,...,C_l)$, then he sends query Q to the server S.

- $R \leftarrow PIR.RGen(1^\lambda, DB, pk, Q)$: At response phase, after receiving the query Q, server S computes the response R as algorithm 4.1:

Algorithm4.1: *PIR.Response algorithm from IRGSW*

Input: Datebase $DB = a_1a_2,...,a_t$, query $Q = (C_1,C_2,...,C_l)$, and index k.

Output: Response c'.

Step1. For each index $r \in \{1,2,...,t\}$, and each bit r_i $(1 \le i \le l = \lceil \log t \rceil)$, database server computes $C_{r,i} = IRGSW.Enc(pk,r_i)$;

Step2. Compute $\hat{\psi}_r = \bigotimes_{i=1}^{l}(C_i \oplus C_{r,i} \oplus \hat{1})$, where $\hat{1}$ is an encryption of 1;

Step3. Compute $R = \bigoplus_{a_r=1} \hat{\psi}_r$.

- $x \leftarrow PIR.DRes(1^\lambda, sk, R)$: At decode phase, user A runs the decryption algorithm of IRGSW scheme, and decrypts the ciphertext associated with R, outputting $x = IRGSW.Dec(sk,R)$.

Theorem 4.1 (Correctness). Let λ be the security parameter, and L be the bound of depth of evaluation circuit for multiplication supported by IRGSW, and $DB \in \{0,1\}^t$ with $\log t < 2^L - 1$. Then for each $k \in \{1,2,...,t\}$, it holds that

$$\Pr[IRGSW.Dec(sk,R) \neq DB[k]] = negl(\lambda)$$

Proof. From our IRGSW-PIR protocol, it is easy to see that $\hat{\psi}_r = \hat{1}$ when $r = k$ and an encryption of 0 otherwise. And on the basis of FHE properties, since $\log t < 2^L - 1$, we can get that if

$$a_k = 1,\ R = \bigoplus_{a_i=1} \hat{\psi}_r = \hat{\psi}_k = \hat{1}$$

, and if

$$a_k = 0, R = \bigoplus_{a_i=1} \hat{\psi}_r = \hat{0}$$

Thus

$$\Pr[IRGSW.Dec(sk, R) \neq DB[k]] = 0 = negl(\lambda).$$

That is to say our IRGSW-PIR protocol satisfies perfect correctness.

Theorem 4.2 (Security). The PIR protocol from IRGSW is semantically secure when the underlying IRGSW scheme is semantically secure.

Proof. For our IRGSW-PIR protocol, suppose that there is an adversary who can gain an unnegligible advantage in semantic security game. Then, we can find an adversary $\mathcal{A}'$ (built on $\mathcal{A}$) with an unnegligible advantage in destroying the semantic security of IRGSW as follows:

The adversary $\mathcal{A}'$ uses some challenger $\mathcal{C}'$ to initiate the semantic security game for the IRGSW. And $\mathcal{C}'$ runs the IRGSW.KeyGen algorithm, gives pk to $\mathcal{A}'$ and makes the secret key sk private. Then $\mathcal{A}'$ chooses $m_0 = 0 \in \mathbb{Z}_2$ and $m_1 = 1 \in \mathbb{Z}_2$, and sends m_0, m_1 to $\mathcal{C}'$. $\mathcal{C}'$ randomly chooses one bit $b \in \mathbb{Z}_2$, computes $e_b = IRGSW.Enc(pk, m_b)$ and then sends e_b to $\mathcal{A}'$.

Next, $\mathcal{A}'$, playing a challenger $\mathcal{C}$, initiates the semantic security game for PIR protocol from IRGSW scheme with the adversary $\mathcal{A}$. Firstly, $\mathcal{A}$ chooses $m_0 = i$ and $m_1 = j$ with $1 \le i < j \le t$, and sends m_0, m_1 to $\mathcal{A}'$. Then $\mathcal{A}'$ randomly chooses one bit $b \in 0,1$, and bulids a Q_q as follows: Suppose that $(x_{q,1},...,x_{q,l})$ be the binary expression of x_q, where $l = \lfloor log\ t \rfloor + 1$. And $\mathcal{A}'$ takes the place of all zeros with $\hat{0}$ and all ones with $\hat{0} \boxplus e_b$ to build the encryption of x_q. We denote the result as $Y_q = (\hat{y}_{q,1},...,\hat{y}_{q,l})$. Then $\mathcal{A}'$ sends $Q_q = (pk, Y_q)$ to $\mathcal{A}$.

Next $\mathcal{A}$ returns a guess q'. Since $e_b = \hat{0}$ with probability 1/2, that is, Y_q is the encryption of all zeros, and for all $1 \le r \le t$, $\hat{\psi}_r = \bigotimes_{i=1}^{l} (\hat{y}_{q,i} \oplus C_{r,i} \oplus \hat{1}) = \hat{0}$. Then $R = \bigoplus_{a_r=1} \hat{\psi}_r$. In this event, A's guess has no connection with q, and hence the probability $q' = q = 1/2$.

However, since $e_b = \hat{1}$ with probability 1/2, that is, Y_q is the encryption result of x_q. In this case, the adversary $\mathcal{A}$ will guess q correctly with probability $1/2 + \varepsilon$. The adversary $\mathcal{A}'$ gets his guess b' as follows: $\mathcal{A}'$ will set $b' = 1$ when $\mathcal{A}$ guesses $q' = q$ correctly, and otherwise $\mathcal{A}'$ will set $b' = 0$. Above all, we can get the correct probability of the guess of $\mathcal{A}'$:

$$Pr(b' = b) = \frac{1}{2}(\frac{1}{2}) + \frac{1}{2}(\frac{1}{2} + \varepsilon) = \frac{1}{2} + \frac{\varepsilon}{2}$$

Therefore, $\mathcal{A}'$ has got a nonnegligible advantage in the semantic security game for the IRGSW scheme, wich is a contradiction to our assumption in the theorem. Then the semantically secure of IRGSW-PIR protocol is proven.

In order to improve the implementation performance on efficiency of our PIR protocol from IRGSW, two optimizations are introduced:

Optimization: Speedups via batching and NTT technology. By introducing the batching and the NTT technology, we can remarkably increase the efficiency of our basic PIR protocol from IRGSW. Batching was firstly introduced by Smart and Vercauteren [37]. It allows SIMD (Single Instruction MultipleData) operations to be performed on homomorphically encrypted data. (see e.g. [8, 10, 20, 38]). This makes it be one of the most important and powerful tools in FHE schemes. Using batching, we can split the database into a few small partial databases and run the same query against all parts in parallel. The encoding is always achieved by taking advantage of the chinese remainder theorem. And NTT is used to speed up the polynomial multiplications with a linear cost in N [22,39].

5. Implementation and Discussions

In this section, we implemented our PIR protocol based on IRGSW scheme. Meanwhile, we implemented PIR protocols [16,17,34], where [17] is the best we know in previous PIR constructions of RLWE-based GSW-FHE schemes, [34] is the best we know in previous PIR constructions of other FHE schemes based on RLWE assumption, and [16] is the best we know in previous PIR constructions of standard LWE-based GSW-FHE schemes. Let the polynomial ring be $R = \mathbb{Z}[X]/(\Phi_m(X))$, where $\Phi_m(X)$ is the m-th cyclotomic polynomial.

5.1 Concert parameters

Let L be the multiplicative depth that the scheme can be homomorphically evaluated, and let $error_L(B', n, q)$ denote the value of noise growth when evaluating any function f (with multiplicative depth L) on ciphertexts in $\mathbb{R}_q$, where the initial error of magnitude is B'. Set $error_{UB}$ be the upper bound that corresponding FHE scheme can bear (for our IRGSW-FHE scheme, $error_{UB} = \lfloor q/p \rfloor / 2$). For correct decryption, we need

$$error_L(B', n, q) < error_{UB} \tag{1}$$

As for RLWE-based FHE schemes, we set the corresponding parameters following inequality (1) and the analysis of Peikert [43]. Note that, it's an open problem to evaluate the practical security gap between RLWE problem and SLWE problem [37], we can only make a simple comparison at the same lattice dimension for SLWE-based scheme[16] and our IRGSW scheme. **Table 2** summarizes our final parameters selection.

Table 2. Parameters of four PIR from FHE schemes

Scheme	Cyclotomic ring m	Lattice dimension	Number of slots	Depth modulus L	Plaintext modulus p	Ciphertext modulus q
SLWE-based FHE of [16]	18631=601 × 31	1524	720	5	2	2^{32}
RLWE-based FHE of [34]	18631=601 × 31	2280	720	5	2	2^{115}
RLWE-based GSW-FHE of [17]	18631=601 × 31	1896	720	5	2	2^{61}
Our IRGSW	18631=601 × 31	1524	720	5	2	2^{48}

Where the last three schemes are based on RLWE problems with the same safety level $\lambda = 80$, and scheme [16] is based on standard LWE problems with the same lattice dimension with our IRGSW and following the analysis of Regev [35].

5.2 Implementation Results

We ran a test for all the following four PIR protocols separately. These tests were run on a four-year-old IBM system x3850 server, and it had 32GB of RAM at 3.0 GHz, 35MB L2 cache and two 64-bit 4-core Intel Xeon E5450 processors. Besides, based on Shoup's NTL library [40] version 9.10.0 ((used for high-level numeric algorithms)), GNU's GMP library(used for the underlying integer arithmetic operations) [41], and gcc compiler (version 4.9.1), we made the implementation.The results are given in **Table 3**.

Table 3. Comparisons of four PIR from FHE scheme

Scheme	Database size (KB)	Packed Enc time (ms)	Packed Dec time (ms)	Query time (s)	Communication bandwidth (MB)
PIR of [16]	100	106	25	146.81	805
PIR of [34]	100	28	2	73.52	5.04
PIR of [17]	100	73	6	22.13	106.33
Ours	100	49	4	7.21	23.65

5.3 Discussions

From **Table 3**, we can get that the performance of [16] on efficiency and communication bandwidth is the worst, although it has a stronger security hypothesis. That's because the other three schemes all choose RLWE-based FHE schemes to build PIR system and [16] choose standard LWE-based FHE schemes. Among [17,34] and our scheme, the query time of [34] costs most, although [34] has an advantage in communication bandwidth. That's because [17] and our scheme both choose RLWE-based GWE-FHE schemes to build PIR system. They eliminate expensive key switching operations for [34]. Compared with [17], it's easy to see our scheme has a better performance in all aspects. That's because our scheme has a smaller size of ciphertexts and a lower expansion factor for noise over homomorphic multiplication. Lower expansion factor for noise means a smaller q needed to homomorphic retrieve the database correctly. In summary, our scheme is the fastest, and has the best performance almost in all aspects among the four PIR systems.

6. CONCLUSION

In this paper, we eliminate "flatten" operation of paper and obtain a technically simpler variant of RLWE-based GSW and smaller sizes of keys and ciphertexts. Meanwhile, since RLWE-based FHE schemes facilitate major efficiency and storage benefits over their non-ring counterparts (standard LWE-based FHE schemes), and combined with the batching and NTT technology, a fast PIR protocol for better privacy protection of cloud computing from our RLWE-based GSW-FHE scheme is proposed.

References

[1] Silva L V, Barbosa P, Marinho R, et al., "Security and privacy aware data aggregation on cloud computing," *Journal of Internet Services and Applications*, 9(1), 6, 2018. Article (CrossRef Link)

[2] Awasthi P, Mittal S, Mukherjee S, et al., "A Protected Cloud Computation Algorithm Using Homomorphic Encryption for Preserving Data Integrity," *Recent Findings in Intelligent Computing Technologys. Springer, Singapore*, 509-517, 2019. Article (CrossRef Link)

[3] R. L. Rivest, L. Adlman, M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, 4(11), 169-180, 1978. Article (CrossRef Link)

[4] Acar A, Aksu H, Uluagac A S, et al., "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys (CSUR)*, 51(4), 79, 2018. Article (CrossRef Link)

[5] C. Gentry. Fully homomorphic encryption using ideal lattices," in *Proc. of the 41st Annual ACM Symposium on Theory of Computing, New York, ACM Press*, 169-178, 2009. Article (CrossRef Link)

[6] M. Van Dijk, C. Gentry, S. Halevi, et al., "Fully homomorphic encryption over the integers," in *Proc. of the 29th International Conference on Theory and Application of Cryptographic Technologys, Berlin: Springer*, 24-43, 2010. Article (CrossRef Link)

[7] Aung K M M, Lee H T, Tan B H M, et al., "Fully homomorphic encryption over the integers for non-binary plaintexts without the sparse subset sum problem," *Theoretical Computer Science*, vol. 771, pp. 49-70, 2018. Article (CrossRef Link)

[8] Hu C, Zhao J., "An Improved Multiple to One Fully Homomorphic Encryption on the Integers," *Journal of Computer and Communications*, 6(09), 50-59, 2018. Article (CrossRef Link)

[9] J . S. Coron, A. Mandal, D. Naccache, et al., "Fully homomorphic encryption over the integers with shorter public keys," in *Proc. of the 31st Conference on Advances in Cryptology, Berlin,Springer*, 487-504, 2011. Article (CrossRef Link)

[10] J. H. Cheon a, J. Kim, M. S. Lee, A. Yun, "CRT-based fully homomorphic encryption over the integers," *Information Sciences*, 310,149-162, 2015. Article (CrossRef Link)

[11] Chillotti I, Gama N, Georgieva M, et al., "Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds," in *Proc. of International Conference on the Theory and Application of Cryptology and Information Security, Springer, Berlin, Heidelberg*, 3-33, 2016. Article (CrossRef Link)

[12] Z. Brakerski, V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in *Proc. of the 52nd Annual Symposium on Foundations of Computer Science. Washington DC:IEEE Computer Society*, 97-106, 2011. Article (CrossRef Link)

[13] Z. Brakerski, C. Gentry, V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," in *Proc. of the 3rd Innovations in Theoretical Computer Science Conference. NewYork, ACM Press*, 309-325, 2012. Article (CrossRef Link)

[14] Z. Brakerski, "Fully homomorphic encryption without modulus switching from classical GapSVP," in *Proc. of the 32nd Cryptology Conference, Berlin, Springer*, 868-886, 2012. Article (CrossRef Link)

[15] C. Gentry, A. Sahai, B. Waters, "Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based," in *Proc. of the 33rd Annual Cryptology Conference, Berlin, Springer*, 75-92, 2013. Article (CrossRef Link)

[16] J. Alperin-Sheriff, C. Peikert, "Faster Bootstrapping with Polynomial Error," *Lecture Notes in Computer Science*, 8616, 297-314, 2014. Article (CrossRef Link)

[17] Alhassan Khedr, Glenn Gulak, and Vinod Vaikuntanathan, "SHIELD: Scalable Homomorphic Implementation of Encrypted Data-Classifiers," *IEEE TRANS. ON COMPUTERS*, vol. 65, no. 9, pp. 2848-2858, 2015. Article (CrossRef Link)

[18] V. Lyubashevsky, C. Peikert, O. Regev, "A toolkit for ring-LWE cryptography," in *Proc. of the 32nd International Conference on Theory and Application of Cryptographic Techniques. Berlin: Springer*, 35-54, 2013. Article (CrossRef Link)

[19] C. Gentry, S. Halevi, C. Peikert, et al., "Ring switching in BGV-style homomorphic encryption," in *Proc. of the 8th International Security and Cryptography for Networks. Berlin: Springer*, 19-37, 2012. Article (CrossRef Link)

[20] Castryck W, Iliashenko I, Vercauteren F, "Homomorphic SIM $$^ 2$$ D Operations: Single Instruction Much More Data," in *Proc. of Annual International Conference on the Theory and Applications of Cryptographic Technologys, Springer, Cham*, 338-359, 2018. Article (CrossRef Link)

[21] Wei Zhang, Shuguang Liu, and Yang Xiaoyuan, "RLWE-based homomorphic encryption and private information retrieval," in *Proc. of the 5th International Conference on Intelligent Networking and Collaborative Systems*, pp. 535-540, 2013. Article (CrossRef Link)

[22] A. Schonhage and V. Strassen, "Schnelle multiplikation groerzahlen," *Computing*, vol. 7, no. 3-4, pp. 281-292, 1971. Article (CrossRef Link)

[23] Cheon J H, Han K, Kim A, et al., "Bootstrapping for Approximate Homomorphic Encryption," in *Proc. of Annual International Conference on the Theory and Applications of Cryptographic Technologys. Springer, Cham*, 360-384, 2018. Article (CrossRef Link)

[24] Chillotti I, Gama N, Georgieva M, et al., "Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds," in *Proc. of Advances in Cryptology-ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22. Springer Berlin Heidelberg*, 3-33, 2016. Article (CrossRef Link)

[25] Hiromasa R, Abe M, Okamoto T. Packing messages and optimizing bootstrapping in GSW-FHE," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 99(1), 73-82, 2016. Article (CrossRef Link)

[26] Clear M, McGoldrick C, "Multi-identity and multi-key leveled FHE from learning with errors," in *Proc. of Annual Cryptology Conference, Springer, Berlin, Heidelberg*, 630-656, 2015. Article (CrossRef Link)

[27] E.Kushilevitz and R.Ostrovsky. "Replicationis not needed: Single data base, computationally-private information retrieval." *in FOCS*, pp.364-373, 1997. Article (CrossRef Link)

[28] Olumofin F, Goldberg I. Revisiting the computational practicality of private information retrieval," in *Proc. of International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg*, 158-172, 2011. Article (CrossRef Link)

[29] Olumofin, F., Goldberg, I., "Revisiting the Computational Practicality of Private Information Retrieval," *Financial Cryptography and Data Security*, LNCS 7035, pp 158-172, 2012. Article (CrossRef Link)

[30] Aguilar-Melchor, C., Gaborit, P., "A Lattice-Based Computationally-Efficient Private Information Retrieval Protocol," in *Proc. of WEWORC 2007*, July 2007.

[31] Yi X, Kaosar M G, Paulet R, et al., "Single-database private information retrieval from fully homomorphic encryption," *IEEE Transactions on Knowledge and Data Engineering*, 25(5), 1125-1134, 2013. Article (CrossRef Link)

[32] Dorz Y, Sunar B, Hammouri G, "Bandwidth efficient PIR from NTRU," in *Proc. of International conference on financial cryptography and data security, Springer*, p. 195-207, 2014. Article (CrossRef Link)

[33] Ichibane Y, Gahi Y, Guennoun M, et al., "Performance analysis of private information retrieval scheme based on homomorphic encryption," in *Proc. of 2015 5th International Conference on Information Communication Technology and Accessibility (ICTA), IEEE*, 1-6, 2015. Article (CrossRef Link)

[34] Carlos Aguilar-Melchor, Joris Barrier, Laurent Fousse, Marc-Olivier Killijian, "XPIR : Private Information Retrieval for Everyone," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 2, pp. 155-174, 2015. Article (CrossRef Link)

[35] Oded Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, 56(6), 34, 2009. Article (CrossRef Link)

[36] V. Lyubashevsky, C. Peikert, O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. of Eurocryt 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Technologys*, pp.1-23, 2010. Article (CrossRef Link)

[37] Smart N P, Vercauteren F, "Fully homomorphic SIMD operations," *Designs, codes and cryptography*, 71(1), 57-81, 2014. Article (CrossRef Link)

[38] Hiromasa R, Abe M, Okamoto T, "Packing Messages and Optimizing Bootstrapping in GSW-FHE," *Public-Key Cryptography-PKC 2015, Springer Berlin Heidelberg*, 699-715, 2015. Article (CrossRef Link)

[39] Song W T, Hu B, Zhao X F, "Privacy Protection of IoT Based on Fully Homomorphic Encryption," *Wireless Communications and Mobile Computing*, vol. 2018, p. 7, 2018. Article (CrossRef Link)

[40] V. Shoup. NTL: A Library for doing Number Theory. http:/shoup.net/ntl/, Version 9.10.0,2016.

[41] The GNU Multiple Precision Arithmetic Library. http://gmplib.org/, Version 6.1.1, 2016.

[42] Lindner R, Peikert C, "Better Key Sizes (and Attacks) for LWE-Based Encryption," *CT-RSA*, 6558, 319-339, 2011. Article (CrossRef Link)

[43] Peikert C, "A decade of lattice cryptography," *Foundations and Trends? in Theoretical Computer Science*, 10(4), 283-424, 2014. Article (CrossRef Link)

Wei-Tao Song received the B.S. and M.S. degrees in cryptography from PLA Strategic Support Force Information Engineering University. Now he is now a teacher of the PLA Strategic Support Force Information Engineering University. His research interests include cloud computing, Fully Homomorphic Encryption and private information retrieval.

Bin Hu is a professor of PLA Strategic Support Force Information Engineering University, Zhengzhou, China. His research interests include boolean function, fully homomorphic and security protocol, etc.

Xiu-Feng Zhao received her B.S. degree from Qufu Teacher University in 2000, and M.S. degree in Northwestern Polytechnical University in 2003. In 2012, she received her PhD. Degree in Shandong University. She is now a teacher of the PLA Strategic Support Force Information Engineering University. Her recent interests include