JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 33, 939-952 (2017)
DOI: 10.6688/JISE.2017.33.4.5

Optimizing LWE-based FHE for Better Security and Privacy Protection of Smart City*

WEI-TAO SONG, BIN HU AND XIU-FENG ZHAO
Department of Information Research and Security
Zhengzhou Information Science Technology Institute
Zhengzhou, 450001 P.R. China
E-mail: weitaosong@163.com; hb2110@126.com; zhaoxiufeng@163.com

As a hot information technique, cloud computing is an excellent choice for building a "smart city". But cloud computing couldn't well balance convenience and privacy. This greatly influences its advantage to play. With the appearance of fully homomorphic encryption (FHE), it is possible for cloud computing to be consistent with privacy. But, the efficiency of FHE schemes is still far from the actual needs. The main reason is the additional noise reduction manipulations which take lots of time.

Up to now, the effective FHE schemes are mostly constructed based on the learning with error (LWE), and re-linearization technique is an essential technique to construct LWE-based FHE scheme. Meanwhile it is also the main cause of the noise expansion, which greatly affects the efficiency of LWE-based FHE, although binary decomposition is used to reduce the noise effectively by publishing the "encryptions" of key components.

In this paper, we are the first to directly study how to further reduce the noise (caused by the "relinearization" technique) in a natural way. First, we verify that, according to original processing method of "relinearization" technique, the binary is optimal in performance on noise reduction, compared to other scale numbers. Then we propose a new way to use multi-band decomposition for noise reduction. If we choose a quaternary representation as our way, noise can be reduced to about half of the original "relinearization" technique for one homomorphic multiplication, which means less additional noise reduction manipulations needed for same depth of homomorphic evaluation circuit. Moreover, the larger the number of scale number we choose, the better the performance. Besides, we present an algorithm changing a somewhat LWE-based FHE into a leveled LWE-based FHE based on our optimized "relinearization" technique.

Keywords: fully homomorphic encryption, learning with error, re-linearization technique, noise reduction, bootstrapping

1. INTRODUCTION

Recently, more and more countries have set out to build "smart cities", which aim to improve the quality and comfort of citizens' lives by using information and communication technologies [1-4]. With the rise of cloud computing, it has been the main task to apply the cloud computing into the building of "smart city" to render the citizens a more accurate, convenient and extensive service. See Fig. 1.

Cloud computing moves computing and data away from desktop computers and mobile devices. While cloud computing offers a great deal of advantages in costs and

Received July 1, 2016; revised July 31, 2016; accepted August 30, 2016.
Communicated by Zhe Liu.
* This work was sponsored in part by the National Natural Science Foundation of China [Grant No. 61272041, 61202491, 61272488, 61601515], and was also supported by the Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-15-006).

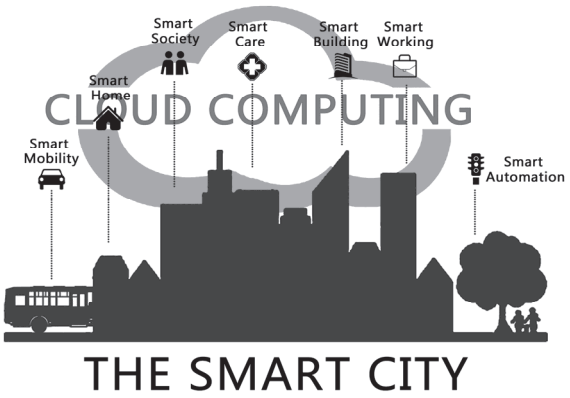

Fig. 1. Diagram of the smart city based on cloud computing.

functionality, it raises grave questions of confidentiality, since data stored in the cloud often contains sensitive information (*e.g.* medical records or account information) [5, 6]. It is unsuitable or illegal to put them online "in the cloud" unencrypted. On the other hand, encrypting one's data seems to nullify the benefits of cloud computing with an "ordinary" encryption scheme. Thus greatly limits the application of cloud computing. Fortunately, the appearance of fully homomorphic encryption (FHE) makes it possible for cloud computing consistent with privacy [7-10].

FHE allows evaluation of arbitrarily complex programs on encrypted data. Based on FHE, the users can enjoy the powerful data processing capabilities of the cloud server, without leaking privacy data. The idea of FHE is firstly proposed by Rives *et al.* in 1978 [11], yet the first plausible candidate comes thirty years later with Gentry's breakthrough work in 2009 [12]. Then many optimized FHE schemes are proposed.

The first generation of FHE schemes [13-20] that follows with Gentry's blueprint: it starts with constructing a somewhat homomorphic encryption (SWHE) scheme using the circuit model [13, 21], namely an encryption scheme capable of evaluating "low-degree" polynomials homomorphically. Since all the schemes are probabilistic encryption, that all the ciphertexts outputed by these schemes are "noisy", and the noise expands during homomorphic addition, but explosively during homomorphic multiplication, which results in the limitation of low-degree polynomials. To obtain FHE, Gentry proposed a meritorious bootstrapping theorem, which transform SWHE into a "leveled" FHE scheme by squaring decryption function on it homomorphically [12]. This "refreshes" a ciphertex of which the noise closes to the upper limit. With iterated use of bootstrapping technique, you can get a FHE scheme. But bootstrapping is a time-consuming process.

A second generation of schemes begins with the work of Brakerski and Vaikuntanathan [22]. Based on the learning with errors (LWE) assumption [23, 24], Brakerski and Vaikuntanathan propose a FHE scheme in a simpler way, and whose security can be reduced to the approximating short vector problems in standard lattices.

Their schemes are then improved by works [25-34]. But no works of them are immune from expensive "relinearization technique" proposed in BV11. Since the ciphertexts are vectors in LWE-based FHE. For n-dimensional ciphertexts, it involves tensor products of vectors during homomorphic multiplication. This blows up the size of ci-

phertext from n to approximate $n^2/2$. This means it can only be used for a constant number of step for homomorphic multiplication. For efficiency, the evaluator must relinearize [22] the ciphertext after tensoring. The linearization technique can compresse the long ciphertexts into a normal-sized n-dimensional ciphertexts, which is ingenious and crucial technique that led to LWE-based FHE.

But linearization is expensive, which introduces a $\Theta(n^4)$ noise. Note that, nowadays the efficiency of FHE schemes is still a great distance from practicality. The main reason is the additional noise reduction manipulations which take lots of time. Thus, if we find a natural way to reduce the noise caused by the "relinearization" technique, which means we requires less additional noise reduction to achieve LWE-based FHE. That is, the efficiency of LWE-based FHE would be significantly improved.

Relevant Works

We are the first to directly study how to reduce the noise (caused by the "relinearization" technique) in a natural way. So far, most researchers mostly construct a SWHE by utilizing "relinearization" technique directly, based on LWE assumptions. Then they introduce many additional noise-reduction technologies during evaluation operations homomorphically, in order to support a bigger depth of evaluation circuit [25-30].

In CRYPTO 2013, by using an approximate eigenvector method and a flatten technique, Gentry, Sahai and Waters (GSW) propose an easier FHE scheme [31], whose homomorphic multiplication size of ciphertext remains unchanged by a natural matrix multiplication, liberated from expensive "relinearization" technique. But GSW13 couldn't completely replace the previous way of LWE-based FHE. Since the size of the GSW13 ciphertext goes up from n+1 elements to $(n \cdot \log q) \times (n \cdot \log q)$, and it doesn't have any advantages for construct FHE based on R-LWE assumptions [32-34], compared to previous methods using "relinearization" technique. Thus, it is of great significance to study how to optimize "relinearization" technique directly.

2. PRELIMINARIES

2.1 Homomorphic Encryption Schemes

Definition 1: A homomorphic encryption scheme can be described as a 4-tuple of algorithms HE = (*HE.KeyGen*, *HE.Enc*, *HE.Dec*, *HE.Eval*) as follows.

- *HE.KeyGen*(1^λ): Take the security parameter λ and output (*pk*, *sk*, *evk*), where *pk* and *sk* are public key and secret key respectively, and *evk* is the evaluation key.
- *HE.Enc*(*pk*, μ): Take the encryption key *pk* and a single-bit message $\mu \in \mathbb{Z}_2$, and output a ciphertext c, denoted as c = *HE.Enc*(*pk*, μ).
- *HE.Dec*(*sk*, c): Take the decryption key *sk* and a ciphertext c, and output a plaintext μ, denoted as μ = *HE.Dec*(*sk*, c).
- *HE.Eval*(*evk*, f, c_1, c_2, …, c_ℓ): Take the evaluation key *evk*, a function f: $\{0, 1\}^\ell \to \{0, 1\}$ and ℓ ciphertexts c_1, c_2, …, c_ℓ, and output a ciphertext c_f, satisfying *HE.Dec*(*sk*, c_f) = f(*HE.Dec*(*sk*, c_1)), …, *HE.Dec*(*sk*, c_ℓ)).

Definition 2: (*L-Homomorphic*) A scheme is *L*-Homomorphic if for arithmetic circuit *f*(over *GF*(2)) with depth no more than *L*, and respective inputs $\mu_1, \mu_2, \ldots, \mu_\ell \in \mathbb{Z}_2$, it holds that

$$Pr[Dec_{sk}(Eval_{evk}(f, c_1, c_2, \ldots, c_\ell)) \neq f(\mu_1, \mu_2, \ldots, \mu_\ell)] = negl(n)$$

where $(pk, sk, evk) \leftarrow HE.KeyGen(1^\lambda)$ and $c_i = HE.Enc_{pk}(\mu_i)$.

2.2 Learning with Errors (LWE)

The LWE assumption is introduced by Regev [24], which is defined as follows.

Definition 3 (*LWE*): For security parameter λ, let $n = n(\lambda)$, $m = m(\lambda)$ be integer dimension, and $q = q(\lambda) \geq 2$ be an integer. Meanwhile, let $\chi = \chi(\lambda)$ be a small 'noise' distribution over $\mathbb{Z}$. Given a matrix $A \in \mathbb{Z}_q^{m \times n}$ and a vector $b \in \mathbb{Z}_q$. The $LWE_{n,q,\chi}$ problem is to distinguish the following two distributions: In the first distribution, one samples $\vec{b} = A \cdot \vec{s} + \vec{e}$ with $\vec{s} \xleftarrow{u} \mathbb{Z}_q^n$, and $\vec{e} \xleftarrow{\$} \chi$. In the second distribution, one samples $\vec{b}$ uniformly from $\mathbb{Z}_q^n$. The $LWE_{n,q,\chi}$ assumption is that the $LWE_{n,q,\chi}$ problem is infeasible.

$LWE_{n,q,\chi}$ problem can be reduced to approximating short vector problems in standard lattices through classical algorithm [28] or quantum algorithm [24] for certain parameters. Specifics are Theorem 1:

Theorem 1: Let $q = q(n) \in N$ be a product of small (size *poly*(*n*)) coprime numbers $q = \prod q_i$ or a power of prime $q = p^r$. And let $B \geq \omega(\log n) \cdot \sqrt{n}$. Then there exists an efficient algorithm that solves the $LWE_{n,q,\chi}$ problem with a *B*-bounded distribution χ. Then:

- If $q \geq \tilde{O}(2^{n/2})$, then there is an efficient classical algorithm for solving $GapSVP_{\tilde{O}(nq/B)}$ on any *n*-dimensional lattice.
- There is an efficient quantum algorithm that solves $GapSVP_{\tilde{O}(nq/B)}$ on any *n*-dimensional lattice.

3. ANALYSIS OF NOISE CAUSED BY "RELINEARIZATION" TECHNIQUE

3.1 "Relinearization" Technique

We begin with introducing the linearization technique through a SWHE scheme. It is fairly straightforward to an LWE-based FHE scheme.

- $HE.KeyGen(1^\lambda)$: Suppose *q*, *n*, *m* are instantiated according to the LWE assumption. Randomly choose vector *a*, $s \in \mathbb{Z}_q^n$ and sample an error *e*, with $|e| \leq B$. The secret key is *s*.
- $HE.Enc(\mu, s)$: To encrypt a message $\mu \in \mathbb{Z}_2$, we compute

$$c = (a, b = < a, s > + 2e + \mu) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$$

• *HE.Dec*(c, s): To recover the message μ, we compute $\mu = [[b - \langle a, s\rangle]_q]_2$.

Correctness is guaranteed only when $2e < \lfloor q/2 \rfloor$. And security is guaranteed when $n = poly(\lambda)$, $B = poly(n)$, $q = 2^{n^{\varepsilon}}$ with $\varepsilon \in (0, 1)$, and $m = O(n\log q)$. Besides, for the above scheme, the additive homomorphism is rather straightforward, but the multiplication homomorphism was not easy to analyze until 2011. In 2011, Brakerski and Vaikuntanathan (BV11) are the first to study the homomorphism of above scheme according to decryption algorithm, which makes it easy to analyse multiplication homomorphism. Suppose (a, b) is a ciphertext, according to the decryption algorithm, they construct a symbolic linear function $f_{a,b}$: $\mathbb{Z}_q^n \to \mathbb{Z}_q$ defined as:

$$f_{a,b}(x) = b - < a, x > (\text{mod } q) = b - \sum_{i=1}^{n} a[i] \cdot x[i] \in \mathbb{Z}_q$$

where $x = (x[1], x[2], \ldots, x[n])$ denotes the function variables, and the coefficients of linear function is just defined by ciphertext. Meanwhile, the decryption equation can be written by $m = f_{a,b}(s) \bmod 2$.

Homomorphism can now be easily described in terms of this function f. Firstly, for the addition of two ciphertexts ($a+a'$, $b+b'$), it corresponds to the addition of two linear functions $f_{a+a',\, b+b'}(x) = f_{a,b}(x) + f_{a',b'}(x)$. Homomorphism is obvious. Then for the multiplication of two ciphertexts, it corresponds to a symbolic multiplication of these linear equations

$$\begin{aligned} & f_{a,b}(x) \bullet f_{a',b'}(x) \\ & = (b - \langle a, x \rangle)(b' - \langle a', x \rangle) \\ & = (b - \sum_{i=1}^{n} a[i]x[i])(b' - \sum_{i=1}^{n} a'[i]x[i]) \\ & = h_0 + \sum h_i x[i] + \sum h_{i,j} x[i]x[j]. \end{aligned}$$

By this way, we can get a degree-2 polynomial on the variables $x = (x[1], x[2], \ldots, x[n])$, of which the coefficients $h_{i,j}$ can be directly computed from ciphertexts (a, b) and (a', b').

To decrypt, we need know all the coefficients of above degree-2 polynomial, which means that the size of the ciphertext just expands from $n+1$ elements to (roughly) $n^2/2$. This is a serious challenge for the homomorphic multiplication of ciphertexts. For that reason, BV11 introduces a "relinearization" technique, which can pull back the size of the ciphertext from $n^2/2$ to $n+1$. The main idea is that they encrypt all the linear and quadratic terms under another secret key t as follows:

$$\begin{aligned} b_i &= < a_i, t > + 2e_i + s[i] \approx < a_i, t > + s[i] \\ b_{i,j} &= < a_{i,j}, t > + 2e_{i,j} + s[i]s[j] \approx < a_{i,j}, t > + s[i]s[j] \end{aligned}$$

where $x \approx y$ means that the absolute difference between x and y is small.

Thus,

$$h_0 + \sum h_i s[i] + \sum h_{i,j} s[i]s[j] \approx h_0 + \sum h_i (b_i - < a_i, t >) + \sum h_{i,j} (b_{i,j} - < a_{i,j}, t >)$$

where the right side of the (approximate) equation is a linear function on $t = (t[1], t[2], \ldots, t[n])$ (with $n+1$ coefficients).

But note that, when the coefficients $h_{i,j}$ (similarly as h_i) are potentially large, the approximate equation $h_{i,j}s[i]s[j] \approx h_{i,j}(b_{i,j} - <a_{i,j}, t>)$ may not hold even though $(b_{i,j} - <a_{i,j}, t>) \approx s[i]s[j]$. Since at this time, the absolute difference $2h_{i,j}e_{i,j}$ between both sides of equation may be great. This is handled by considering the binary representation of $h_{i,j}$, namely $h_{i,j} = \sum_{\tau=0}^{l-1} h_{i,j,\tau} 2^{\tau}$, where $l = \lceil \log q \rceil$.

Thus,

$$h_{i,j}s[i]s[j] = \sum_{\tau=0}^{l-1} (h_{i,j,\tau} 2^{\tau} s[i]s[j]).$$

Then encrypt each term $2^{\tau}s[i]s[j]$ under another secret key t as follows:

$$b_{i,j,\tau} = < a_{i,j,\tau}, t > + 2e_{i,j,\tau} + 2^{\tau} s[i]s[j] \approx < a_{i,j,\tau}, t > + 2^{\tau} s[i]s[j].$$

Thus, we can get that

$$h_{i,j}s[i]s[j] \approx \sum_{\tau=0}^{l-1} h_{i,j,\tau}(b_{i,j,\tau} - < a_{i,j,\tau}, t >)$$

where $h_{i,j,\tau} \in \{0, 1\}$. That is, it needs to publish the "encryptions" of all the 2^{τ}-multiples of $s[i]s[j]$, instead of just the encryptions of $s[i]s[j]$. This expands the size of public key by a factor of approximate $\log q$, which is polynomial. But by this way, for each quadratic term, the error caused by the "relinearization" technique is reduced from $q \cdot 2e_{i,j}$ to approximate $\log q \cdot 2B$ (since $|h_{i,j,\tau}| \le 1$, $|e_{i,j,\tau}| \le B$). This is a great progress, since it makes it possible for LWE-based FHE scheme to support arbitrary depth of homomorphic evaluation circuit. Theorem 3.1 specifically presents the total errors after multiplication of two fresh ciphertexts based on the "relinearization" technique with binary representation.

Theorem 3.1: Suppose ζ is a LWE-based FHE scheme with parameter q, n, m. e denotes the error after the multiplication of two fresh ciphertexts based on the "relinearization" technique with binary representation. Then we can get

$$|e| \le n \cdot (n+3) \cdot (\log q + 1) \cdot B.$$

***Proof*:** Assume fresh ciphertexts are both encrypted by secret key s. Then, after a homomorphic multiplication of ciphertexts c_1, c_2, we can get a degree-2 polynomial $f_{a,b}(s) \cdot f_{a',b'}(s) = h_0 + \sum h_i s[i]s[j]$, which has $n(1+n)/2$ quadratic terms and n linear terms. And for each term, the error caused by the "relinearization" technique based on binary is approximate $(\log q + 1) \cdot 2B$. Thus,

$$|e| \le \frac{n \cdot (n+3)}{2} \cdot (\log q + 1) \cdot 2B = n \cdot (n+3) \cdot (\log q + 1) \cdot B. \quad \square$$

This naturally leads to another problem. Wouldn't it be better to change $h_{i,j}$ into

other scale numbers (such as four hexadecimal, octal, *etc.*) instead of binary on the performance of noise reduction? Considering the efficiency of computer implementation, we mainly discuss the case that scale numbers is power of 2.

3.2 Performance for "Relinearization" Technique Based on Other Scale Numbers

Consider the 2^k-ary representation of $h_{i,j}$, namely

$$h_{i,j} = \sum_{\tau=0}^{l'-1} h_{i,j,\tau} \left(2^k\right)^\tau$$

where $l' = \lceil \log_{2^k} q \rceil = \lceil \log_2 q/k \rceil$, $h_{i,j,\tau} \in \{0, 1, \ldots, 2^k - 1\}$,

Thus,

$$h_{i,j} s[i]s[j] = \sum_{\tau=0}^{l'-1} (h_{i,j,\tau} \left(2^k\right)^\tau s[i]s[j]).$$

Then encrypt each term $(2^k)^\tau s[i]s[j]$ under another secret key t as follows:

$$b_{i,j,\tau} = \left\langle a_{i,j,\tau}, t \right\rangle + 2e_{i,j,\tau} + \left(2^k\right)^\tau s[i]s[j] \approx \left\langle a_{i,j,\tau}, t \right\rangle + \left(2^k\right)^\tau s[i]s[j].$$

Thus, we can get that

$$h_{i,j} s[i]s[j] \approx \sum_{\tau=0}^{l'-1} h_{i,j,\tau} (b_{i,j,\tau} - \left\langle a_{i,j,\tau}, t \right\rangle)$$

where $h_{i,j,\tau} \in \{0, 1, \ldots, 2^k - 1\}$. Similarly as binary, for each quadratic term, the error caused by the "relinearization" technique is no more than $l' \cdot (2^k - 1) \cdot 2B = (\log q/k+1) \cdot (2^k - 1) \cdot 2B$ (Since $h_{i,j,\tau} \in \{0, 1, \ldots, 2^k - 1\}$, $|e_{i,j,\tau}| \le B$). Theorem 3.2 specifically discusses the total errors after multiplication of two fresh ciphertexts based on the "relinearization" technique with 2^k-ary representation.

Theorem 3.2: Suppose ζ is a LWE-based FHE scheme with parameter q, n, k. e denotes the error after multiplication of two fresh ciphertexts based on the "relinearization" technique with 2^k-ary representation. Then we can get the following two conclusions:

(1) $|e| \le n \cdot (3+n) \cdot (\log q/k+1) \cdot (2^k-1) \cdot B$
(2) The upper bound of absolute value of e is rigid monotony increase on k.

***Proof*:** For Theorem 3.2 (1), the proof is same as Theorem 3.1 and is omitted. For Theorem 3.2 (2) let

$$\begin{aligned} y(k) &= n \cdot (3+n) \cdot (\log q / k + 1) \cdot (2^k - 1) \cdot B \\ &= n \cdot (3+n) \cdot \log q \cdot B \cdot \frac{2^k - 1}{k} + n \cdot (3+n) \cdot B \cdot (2^k - 1) \\ &= a_1 \cdot \frac{2^k - 1}{k} + a_2 \cdot (2^k - 1) \end{aligned}$$

where $a_1 = n \cdot (3+n) \cdot \log q \cdot B$, $a_2 = n \cdot (3+n) \cdot B$. And let $y_1(k) = a_1 \cdot (2^k - 1)/k$, $y_2(k) = a_2 \cdot (2^k - 1)$, that is, $y(k) = y_1(k) + y_2(k)$. It can be easily proved that $y_1(k)$ and $y_2(k)$ are both rigid monotony increase on k, since $a_1, a_2 \in \mathbb{Z}^+$. Thus, $y(k)$ is rigid monotony increase on k. ❑

Note that, the security of LWE-based FHE is guaranteed when $n = poly(\lambda)$, $B = poly(n)$, $q = 2^{n^\varepsilon}$ with $\varepsilon \in (0, 1)$. And from the above proof, we can see that monotonicity of the upper bound of $|e|$ on k is not related to the value of q, B, n. We take $n = B = 1024$, $q = 2^{\sqrt{1024}} = 2^{32}$ as an example, generating Fig. 2 to display the relationship between the upper bound of $|e|$ and k visually.

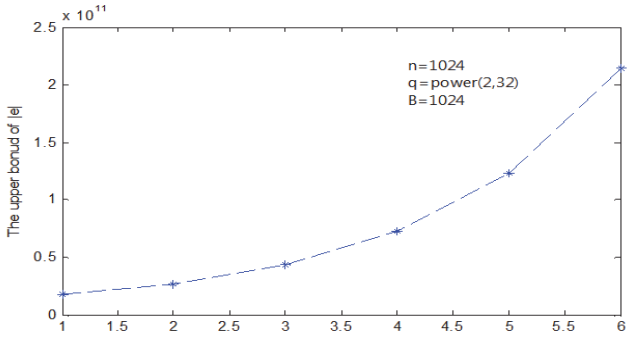

Fig. 2. The performance of noise reduction on one homomorphic multiplication based on "re-linearization" technique with 2^k-ary representation.

Since $k \geq 1$, the absolute value of e is least when $k = 1$, which corresponds to binary representation.

In this section, we prove that the total errors caused by "relinearization" technique based on binary representation is smaller than other 2^k-ary representation, in the situation of following the approach of BV11. Through analysis we find the main reason is that the weight of each component for 2^k-ary representation of $h_{i,j}$ (belonging to $\mathbb{Z}_{2^k}$) is too large compared to binary representation (belonging to $\mathbb{Z}_2$), although the numbers of components is reduced.

In next section, using the idea of space-time transform, we get a better performance on noise reduction based on 2^k-ary representation in a new way.

4. OPTIMIZED "RELINEARIZATION" TECHNIQUE ON NOISE REDUCTION

We take the quaternary as an example to illustrate our ideas. Assume the quaternary representation of $h_{i,j}$ is

$$h_{i,j} = \sum_{\tau=0}^{l'-1} h_{i,j,\tau} 4^\tau \quad (h_{i,j,\tau} \in \{0,1,2,3\})$$

where $l' = \lceil \log_4 q \rceil = \lceil \log q/2 \rceil$. Next, we express $h_{i,j,\tau}$ as a product of $h_{i,j,\tau,z}$ and z, with $h_{i,j,\tau,z} \in \{0, 1\}$, $z \in \{0, 1, 2, 3\}$. Specifics are as shown in Table 1:

Table 1. Express $h_{i,j,\tau}$ as a Product $h_{i,j,\tau,z}$ of z.

$h_{i,j,\tau}$	$h_{i,j,\tau,z}$	z
0	0	1
1	1	1
2	1	2
3	1	3

Thus,

$$h_{i,j}s[i]s[j] = \sum_{\tau=0}^{l'-1} h_{i,j,\tau}4^{\tau}s[i]s[j] = \sum_{\tau=0}^{l'-1} h_{i,j,\tau,z}z4^{\tau}s[i]s[j]$$

Then, publish the "encryptions" of all the z-multiples of $4^{\tau}s[i]s[j]$, instead of just the encryptions of $4^{\tau}s[i]s[j]$, as follows:

$$b_{i,j,\tau,1} = < a_{i,j,\tau,1}, t > +2e_{i,j,\tau,1} + 4^{\tau}s[i]s[j] \approx < a_{i,j,\tau,1}, t > +4^{\tau}s[i]s[j]$$
$$b_{i,j,\tau,2} = < a_{i,j,\tau,2}, t > +2e_{i,j,\tau,2} + 2\bullet 4^{\tau}s[i]s[j] \approx < a_{i,j,\tau,2}, t > +2\bullet 4^{\tau}s[i]s[j]$$
$$b_{i,j,\tau,3} = < a_{i,j,\tau,3}, t > +2e_{i,j,\tau,3} + 3\bullet 4^{\tau}s[i]s[j] \approx < a_{i,j,\tau,3}, t > +3\bullet 4^{\tau}s[i]s[j]$$

Thus indeed

$$h_{i,j}s[i]s[j] = \sum_{\tau=0}^{l/2-1} h_{i,j,\tau,z}z4^{\tau}s[i]s[j] \approx \sum_{\tau=0}^{l'-1} h_{i,j,\tau,z}(b_{i,j,\tau,r} - < a_{i,j,\tau,z}, t >)$$

Similarly, for each quadratic term, we can get that the error caused by the "relinearization" technique is no more than $l' \cdot B = (\log q/2+1) \cdot B$ (Since $h_{i,j,\tau,z} \in \{0, 1\}$, $z \in \{0, 1, 2, 3\}$ $|e_{i,j,\tau}| \le B$). Theorem 3.3 specifically discusses the total errors after multiplication of two fresh ciphertexts based on the "relinearization" technique with variant of quaternary representation.

Theorem 4.1: Suppose ζ is a LWE-based FHE scheme with parameter q, n, m. e denotes the error after multiplication of two fresh ciphertexts based on the "relinearization" technique with variant of quaternary representation. Then we can get $|e| \le n \cdot (3+n) \cdot (\log q/2+1) \cdot B$.

The proof is same as Theorem 3.1 and is omitted. From Theorem 4.1, we can get that our method has a smaller noise expansion. Specifically, if choose variant of quaternary representation as our way, noise can be reduced to about half of the origina "relinearization" technique for one homomorphic multiplication. Moreover, the larger the number of scale number we choose, the better the performance. Specifics are as Theorem 3.4.

Theorem 4.2: Suppose ζ is a LWE-based FHE scheme with parameter q, n, m. e denotes the error after multiplication of two fresh ciphertexts based on the "relinearization" technique with variant of 2^k-ary representation in our way. Then we can get $|e| \le n \cdot (3+n) \cdot (\log q/k+1) \cdot B$.

The proof is same as Theorem 3.1 and is omitted. Next we show our performance intuitively by Fig. 3.

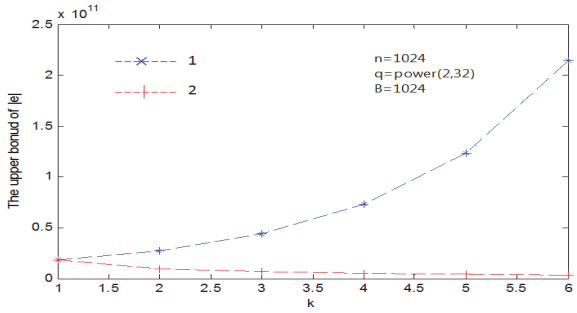

Fig. 3. The comparison of performance of noise reduction on one homomorphic multiplication based on "relinearization" technique with 2^k-ary representation between our way and BV11's.

Where dashed line 2 represents the performance of noise reduction on one homomorphic multiplication based on "relinearization" technique in our way, and dashed line 1 represents the performance following BV11's way. Besides, It is easy to see from Fig. 4 that if we choose a quaternary representation ($k = 2$) as our way, noise can be reduced to about half of the original "relinearization" technique for one homomorphic multiplication. Moreover, the larger the number of scale number we choose, the better the performance.

Next, in order to further increase the practicality of our method, Algorithm 1 shows how to use our optimization "relinearization" techniques to change a somewhat LWE-based FHE into a leveled LWE-based FHE.

Algorithm 1: Assume $HE = (HE.KeyGen, HE.Enc, HE.Dec, HE.Eval)$ is somewhat LWE-based FHE.

Step 1: Let $l = \lceil \log_2 q \rceil - 1\}$. Then, the user generates a prestored table for $L + 1$ secret keys $s_0, \cdots, s_L \xleftarrow{\$} \mathbb{Z}_q^n$ as follows: for all $\ell \in [L]$, $0 \le i \le j \le n$, $\tau \in \{0, \ldots, l\}$, and $1 \le z \le \lceil \log_2 q \rceil - 1$, compute $\psi_{\ell,i,j,\tau,z} := (a_{\ell,i,j,\tau,z}, b_{\ell,i,j,\tau,z}, := \langle a_{\ell,i,j,\tau,z}, s_\ell \rangle + 2e_{\ell,i,j,\tau,z} + z \cdot 2^\tau s_{\ell-1}[i]s_{\ell-1}[j] \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ and send the table to the server.

Step 2: Let $c_1 = ((a_1, b_1), \ell)$, $c_2 = ((a_2, b_2), \ell)$ be two ciphertexts. The server implements homomorphic addition or homomorphic multiplication on them. If implement homomorphic addition, then the server outputs $c^+ = ((a_1 + a_2, b_1 + b_2), \ell)$, and terminate.

Step 3: Run polynomial multiplication

$$
\begin{aligned}
& f_{((a,b),\ell)}(x) \bullet f_{((a',b'),\ell)}(x) \\
&= ((b - \langle a, x \rangle)(b' - \langle a', x \rangle), \ell) \\
&= (((b - \sum_{i=1}^{n} a[i]x[i])(b' - \sum_{i=1}^{n} a'[i]x[i])), \ell) \\
&= h_{\ell,0} + \sum_{i=1}^{n} h_{\ell,i} x[i] + \sum_{1 \le i \le j \le n} h_{\ell,i,j} x[i]x[j]
\end{aligned}
$$

$$= \sum_{0 \le i \le j \le n} h_{\ell,i,j} x[i]x[j]$$

where $h_{\ell,i,0} = h_{\ell,i}$, $x[0] = 1$, $0 \le i \le n$.

Step 4: For all the linear and quadratic coefficients $h_{\ell,i,j}$, compute the 2^k-ary representation of $h_{\ell,i,j}$, namely

$$h_{\ell,i,j} = \sum_{\tau=0}^{l} h_{\ell,i,j,\tau} \cdot z \cdot \left(2^k\right)^{\tau} \text{, where } h_{\ell,i,j,\tau} \in \{0, 1\}, z \in \{1, 2, 3, \ldots, 2^z - 1\}.$$

Then

$$h_{\ell,i,j} x[i]x[j] = \sum_{\tau=0}^{l} h_{\ell,i,j,\tau} \cdot z \cdot \left(2^k\right)^{\tau} x[i]x[j]$$

Step 5: For all the $1 \le z \le \lceil \log_{2^k} q \rceil - 1$, and $\tau \in \{0, \ldots, l\}$, compute

$$b_{\ell,i,j,\tau,z} = <a_{\ell,i,j,\tau,z}, s_\ell> + 2e_{\ell,i,j,\tau,z} + z \cdot (2^k)^{\tau} s_{\ell-1}[i]s_{\ell-1}[j] \approx <a_{\ell,i,j,\tau,z}, s_\ell> + z \cdot (2^k)^{\tau} s_{\ell-1}[i]s_{\ell-1}[j].$$

Step 6: Replace $z \cdot (2^k)^{\tau} s_{\ell-1}[i]s_{\ell-1}[j]$ with $(b_{\ell,i,j,\tau,z} - <a_{\ell,i,j,\tau,z}, s_\ell>)$, we can get

$$h_{\ell,i,j} x[i]x[j] = \sum_{\tau=0}^{l'-1} h_{\ell,i,j,\tau} \cdot (b_{\ell,i,j,\tau,z} - < a_{\ell,i,j,\tau,z}, s_\ell >).$$

Step 7: Compute

$$\begin{aligned} f_{((a,b),\ell)}(x) \bullet f_{((a',b'),\ell)}(x) &= \sum_{0 \le i \le j \le n} h_{\ell,i,j} x[i]x[j] \\ &= \sum_{0 \le i \le j \le n} \sum_{\tau=0}^{l'-1} h_{\ell,i,j,\tau} \cdot (b_{\ell,i,j,\tau,z} - < a_{\ell,i,j,\tau,z}, s_\ell >) \\ &= b' - < a', s_\ell > \end{aligned}$$

The first Then $c^{\times} = ((a', b'), \ell+1)$.

Step 8: We can get a leveled LWE-based FHE by implementing homomorphic addition and multiplication on ciphertexts according to former steps.

5. CONCLUSIONS

Nowadays, the efficiency of FHE schemes is still far from the actual needs. And the main reason is the additional noise reduction manipulations which take lots of time. This greatly influences its advantage to play. In this paper, we are the first to directly reduce the noise (caused by the "relinearization" technique which is an essential technique to construct LWE-based FHE scheme) in a natural way. If we choose a quaternary representation as our way, noise can be reduced to about half of the original "relinearization" technique for one homomorphic multiplication, which means less additional noise reduction manipulations needed for same depth of homomorphic evaluation circuit. Moreover,

the larger the number of scale number we choose, the better the performance. This is a great progress, and it further promotes the practical process of FHE in cloud computing, for the sake of providing better security and privacy protection of smart city.

REFERENCES

1. T. Nam and T. A. Pardo, "Conceptualizing smart city with dimensions of technology, people, and institutions," in *Proceedings of the 12th Annual International Digital Government Research Conference on Digital Government Innovation in Challenging Times*, 2011, pp. 282-291.
2. J. A. C. Soto, O. Werner-Kytölä, and M. Jahn *et al.*, "Towards a federation of smart city services," in *Proceedings of International Conference on Recent Advances in Computer Systems*, 2015, pp. 163-168.
3. Z. Liu, and X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On emerging family of elliptic curves to secure internet of things: ECC comes of age," *IEEE Transactions on Dependable and Secure Computing*, Vol. 99, 2016, pp. 3301-3310.
4. A. Krylovskiy, M. Jahn, and E. Patti, "Designing a smart city internet of things platform with microservice architecture," in *Proceedings of the 3rd Future Internet of Things and Cloud*, 2015, pp. 25-30.
5. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, Vol. E98-B, 2015, pp. 190-200.
6. Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," *Journal of Internet Technology*, Vol. 16, 2015, pp. 317-323.
7. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 27, 2015, pp. 340-352.
8. Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Transactions on Parallel and Distributed Systems*, DOI: 10.1109/TPDS.2015.2506573, 2015.
9. A. Bouti and J. Keller, "Towards practical homomorphic encryption in cloud computing," in *Proceedings of the 4th Network Cloud Computing and Applications*, 2015, pp. 67-74.
10. O. Kocabas and T. Soyata, "Utilizing homomorphic encryption to implement secure and private medical cloud computing," in *Proceedings of the 8th International Conference on Cloud Computing*, 2015, pp. 540-547.
11. R. L. Rivest, L. Adlman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, Vol. 4, 1978, pp. 169-180.
12. C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, 2009, pp. 169-178.
13. C. Gentry, "Computing on arbitrary functions of encrypted data," *Communications of the ACM*, Vol. 53, 2010, pp. 97-105.

14. M. van Dijk, C. Gentry, S. Halevi, *et al.*, "Fully homomorphic encryption over the integers," in *Proceedings of the 29th International Conference on Theory and Application of Cryptographic Techniques*, 2010, pp. 24-43.
15. N. P. Smart and F. Vercautern, "Fully homomorphic encryption with relatively small key and ciphertext sizes," in *Proceedings of the 13th International Conference on Pronctice and Theory in Public Key Cryptography*, 2010, pp. 420-443.
16. D. Stehl and R. Steinfeld, "Faster fully homomorphic encryption," in *Proceedings of the 16th International Conference on Theory and Application of Cryptographic and Information Security*, 2010, pp. 377-394.
17. T. Plantard, W. Susilo, and Z. Zhang, "Fully homomorphic encryption using hidden ideal lattice," *IEEE Transactions on Information Forensics and Security*, Vol. 8, 2013, pp. 2127-2137.
18. J. Cheon, J. S. Coron, J. Kim, *et al*., "Batch fully homomorphic encryption over the integers," in *Proceedings of the 32nd International Conference on Theory and Application of Cryptographic*, 2013, pp. 315-335.
19. J. S. Coron, T. Lepoint, and M. Tibouchi, "Scale-invariant fully homomorphic encryption over the integers," in *Proceedings of the 17th International Conference on Practice and Theory in Public Key Cryptography*, 2014, pp. 311-328.
20. J. H. Cheon, J. Kim, M. S. Lee, and A. Yun, "CRT-based fully homomorphic encryption over the integers," *Information Sciences*, 2015, pp. 149-162.
21. Z. Liu, H. Seo, J. Groschl, and H. Kim, "Efficient implementation of *NIST*-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes," *IEEE Transactions on Information Forensics and Security*, Vol. 11, 2016, pp. 1385-1397.
22. Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in *Proceedings of the 52nd Annual Symposium on Foundations of Computer Science*, 2011, pp. 97-106.
23. O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, Vol. 56, 2009, p. 34.
24. Z. Liu, H. Seo, S. S. Roy, J. Groschl, H. Kim, and I. Verbauwhede, "Efficient ring-LWE Encryption on 8-bit *AVR* processors," in *Proceedings of the 17th Workshop on Cryptographic Hardware and Embedded Systems*, Vol. 9293, 2015, pp. 663-682.
25. Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-LWE and security for key dependent messages," in *Proceedings of the 31st Annual Conference on Advances in Cryptology*, 2011, pp. 505-524.
26. Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 2012, pp. 309-325.
27. Z. Brakerski, "Fully homomorphic encryption without modulus switching from classical GapSVP," in *Proceedings of the 32nd Cryptology Conference*, 2012, pp. 868-886.
28. C. Gentry, S. Halevi, C. Peikert, *et al*., "Ring switching in BGV-style homomorphic encryption," in *Proceedings of the 8th International Security and Cryptography for Networks*, 2012, pp. 19-37.
29. J. Alperin-Sheriff and C. Peikert, "Practical bootstrapping in quasilinear time," in *Proceedings of the 33rd Annual Cryptology Conference*, 2013, pp. 1-20.

30. C. Gentry, S. Halevi, and N. Smart, "Better bootstrapping in fully homomorphic encryption," in *Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography*, 2012, pp. 1-16.
31. C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based," in *Proceedings of the 33rd Annual Cryptology Conference*, 2013, pp. 75-92.
32. J. Alperin-Sheriff and C. Peikert, "Faster bootstrapping with polynomial error," *Lecture Notes in Computer Science*, 2014, pp. 297-314.
33. L. Ducas and D. Micciancio, "FHEW: Bootstrapping homomorphic encryption in less than a second," in *Proceedings of EUROCRYPT*, LNCS, 2015, pp. 617-640.
34. R. Hiromasa, M. Abe, and T. Okamoto, "Packing messages and optimizing bootstrapping in GSW-FHE," in *Proceedings of the 18th International Conference on Practice and Theory in Public-Key Cryptography*, 2015, pp. 699-715.

Wei-Tao Song (宋巍濤) received the B.S. and M.S. degrees in Cryptography from Information Science Technology Institute. Now he is a Ph.D. student at Information Science Technology Institute. His research interests include cloud computing, fully homomorphic encryption and private information retrieval.

Bin Hu (胡斌) is a Professor of Information Science and Technology Institute, Zhengzhou, China. His research interests include Boolean function, fully homomorphic and security protocol, *etc.*

Xiu-Feng Zhao (趙秀鳳) 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 Ph.D. degree in Shandong University. She is now a teacher of Information Science and Technology Institute. Her recent interests include cryptography, privacy protection and provable security.