Towards Fully Homomorphic Encryption From Gentry-Peikert-Vaikuntanathan Scheme

Gang Du[1], Chunguang Ma[1](✉), Zengpeng Li[1], and Ding Wang[2]

[1] College of Computer Science and Technology, Harbin Engineering University,
Harbin, China
{dugang,machunguang,lizengpeng}@hrbeu.edu.cn

[2] School of Electronics Engineering and Computer Science, Peking University,
Beijing, China
wangdingg@pku.edu.cn

Abstract. Despite the convenience brought by cloud computing, internet users, meanwhile, are faced with risks of data theft, tampering, forgery, etc. Fully homomorphic encryption (FHE) has the ability to deal with the ciphertext directly, which can solve the problem of data security in cloud computing. Therefore, fully homomorphic encryption (FHE) has been widely used in cloud computing as well as multiparty computing, functional encryption and private information retrieval, etc. However, previous FHE schemes are based on standard (ring) learning with errors (LWE) assumption and the most typical schemes were created by Brakerski (CRYPTO2012) and Gentry-Sahai-Waters (GSW) (CRYPTO2013). Moreover, inspired by the work of Li et al. at ICPADS2016, they made use of Brakerski's scale-invariant technology and constructed a new FHE scheme with errorless key switching under Dual-First-is-errorless LWE (Dual-Ferr.LWE) problem. Hence, armed with Li et al.'s work, in this paper, we use Gentry-Peikert-Vaikuntanathan's scheme (i.e., under dual LWE assumption) as building block to construct a FHE scheme. Lastly, under the assumption of decisional learning with errors (LWE), we prove that our scheme is CPA (chosen-plaintext-attack) secure.

Keywords: Cloud computing · Lattice based cryptography · Fully homomorphic encryption · Dual learning with errors · First of errorless LWE

1 Introduction

As a new mode of commercial applications, cloud computing services have greatly changed people's way of life. Cloud computing can be understood as a process in which the user gives the computing task to the cloud server, and then, the server returns the results of the computation to the user [23,24]. With the rapid development of cloud computing, increasingly more people store data in the cloud, but it cannot be overlooked that applications of cloud computing are also accompanied by security risks, such as data storage, transmission security and

X. Sun et al. (Eds.): ICCCS 2017, Part II, LNCS 10603, pp. 256–267, 2017.
https://doi.org/10.1007/978-3-319-68542-7_21

user privacy [8,25,26]. The security problem of cloud computing which exerts a negative effect on its application and popularization is a crucial issue in cloud computing research. Fully homomorphic encryption is a new cryptographic technology based on computational complexity theory of mathematical problems, which can provide a method to protect the privacy of the outsourcing data.

Moreover, the hard problem of lattice-based cryptography is considered as a useful tool for the foundation of secure cryptographic constructions. Attractive features of lattice cryptography include apparent resistance to quantum attacks (in contrast with most number-theoretic cryptography), high asymptotic efficiency and parallelism, security under worst-case intractability assumptions, and solutions to long-standing open problems in cryptography.

FHE has long been a holy grail in cryptography [20]. However, it is only in the past few years that candidate FHE schemes have been proposed. The first scheme was constructed by Gentry [9], and his work inspired a tremendous amount of research showing efficient improvements to his scheme (e.g. [21,22]), realizations of FHE based on different assumptions (e.g. [2–7,12,15]), implementations of FHE (e.g. [10,13,14]), etc.

1.1 Our Contribution and Techniques

We note that most of existing FHE schemes are constructed based on LWE assumption. However, the FHE scheme based on dual LWE has only been proposed by Brakerski [2] and just two constructions proposed by Li et al. [17–19]. Therefore, it is an interesting work to construct a FHE based on dual LWE roughly following their novel techniques.

The main observation is that the errorless key-switching procedure [17] doesn't have noise elements and not against key recovery attack [16].

$$<\mathbf{c}_{out}, sk_{out}> = <\mathbf{c}_{in}, sk_{in}> (mod\ q)$$

Hence, we propose a variant of Key-Switching procedure based on Dual LWE

$$<\mathbf{c}_{out}, sk_{out}> = <\mathbf{c}_{in}, sk_{in}> + <\mathbf{c}_{in}, \mathbf{x}_{in\to out}> (mod\ q)$$

We add some noise to the $KeySwitch$ phase to make it work more efficiently and security.

2 Preminary

In this section we introduce some notations and learning with errors problem for both the search and decision variants. More details are as follows:

2.1 Notation

We use bold lower-case letters like $\mathbf{x}$ to denote column vectors; for row vectors we use the transpose $\mathbf{x}^T$. We use bold upper-case letters like $\mathbf{A}$ to denote matrices and sometimes identify a matrix with its ordered set of column vectors. We will be using norms in many of the inequalities in this work. For that reason, we will give three well known norms and inequalities related to norms that we will use in the following sections. l_∞ norm is: $||\mathbf{v}||_\infty = max\{|v_1|, \cdots, |v_n|\}$; l_1 norm is: $||\mathbf{v}||_1 = \sum_{i=1}^{n} |v_i|$ and Euclidean norm is: $||\mathbf{v}||_2 = \sqrt{\sum_{i=1}^{n} |v_i|^2}$.

Lemma 1 *([1] Lemma 12). Let vector* $\mathbf{x}$ *be some vector in* $\mathbb{Z}^m$ *and let* $\mathbf{e} \leftarrow D_{\mathbb{Z}^m,r}$. *Then the quantity* $| \mathbf{x}^T \cdot \mathbf{e} |$ *when treated as an integer in* $[0, \cdots, q-1]$ *satisfies*

$$| \mathbf{x}^T \cdot \mathbf{e} | \leq ||\mathbf{x}|| r\omega(\sqrt{log\ m}) + ||\mathbf{x}||\sqrt{m}/2$$

with all but negligible probability in m.

Lemma 2 *([11] Corollary 5.4). Let* n *and* q *be positive integers with* q *prime, and let* $m \geq 2nlg\ q$. *Then for all but a* $2q^n$ *fraction of all* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *and for any* $r \geq \omega(\sqrt{log\ m})$, *the distribution of the syndrome* $\mathbf{u} = \mathbf{A} \cdot \mathbf{e}$ *mod* q *is statistically close to uniform over* $\mathbb{Z}_q^n$, *where* $\mathbf{e} \leftarrow D_{\mathbb{Z}^m,r}$.

2.2 Learning with Errors

We survey the main foundational work that directly underlies most modern lattice-based cryptographic schemes. Here we just describe LWE, its hardness, and a basic LWE-based cryptosystem in some detail.

Definition 1 *(Learning with Errors Distribution). For a vector* $\mathbf{s} \in \mathbb{Z}_q^n$ *called the secret, the LWE distribution* $\mathcal{A}_{\mathbf{s},\chi}$ *over* $\mathbb{Z}_q^n \times \mathbb{Z}_q$ *is sampled by choosing* $\mathbf{a} \in \mathbb{Z}_q$ *uniformly at random, choosing* $\mathbf{e} \leftarrow \chi$, *and outputting* $\big(\mathbf{a}, b = <\mathbf{s}, \mathbf{a}> + e\ (mod\ q)\big)$.

There are two versions of the LWE problem: search version, which is to find the secret given LWE samples, and decision version, which is to distinguish between LWE samples and uniformly random ones.

Definition 2 *(*$Search - LWE_{n,q,\chi,m}$*). Given* m *independent samples* $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ *drawn from* $\mathcal{A}_{\mathbf{s},\chi}$ *for a uniformly random* $\mathbf{s} \in \mathbb{Z}_q^n$ *(fixed for all samples), find* $\mathbf{s}$.

Definition 3 *(*$Decision - LWE_{n,q,\chi,m}$*). Given* m *independent samples* $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ *where every sample is distributed according to either: (1)* $\mathcal{A}_{\mathbf{s},\chi}$ *for a uniformly random* $\mathbf{s} \in \mathbb{Z}_q^n$ *(fixed for all samples), or (2) the uniform distribution, distinguish which is the case (with non-negligible advantage).*

3 Fully Homomorphic Encryption from GPV Scheme

In this section, we use GPV scheme [11] as a building block to construct a variant of FHE scheme.

3.1 New Key Switching

In this subsection, we construct a new key switching procedure.

- **SwitchKeyGen**: $\mathbf{P}_{sk_{in}\Rightarrow sk_{out}} \leftarrow SwitchKeyGen(sk_{in}, sk_{out})$:
  1. For the input secret key $sk_{in} = [1, \mathbf{e}_{in}]^T \in D_{\mathbb{Z}_q^{n_{in}\times 1}, r}$ and the output secret key $sk_{out} = [1, \mathbf{e}_{out}]^T \in D_{\mathbb{Z}_q^{n_{out}\times 1}, r}$, where the input secret key $\mathbf{e}_{in} \in D_{\mathbb{Z}_2^{(n_{in}-1)\times 1}}$ and the output secret key $\mathbf{e}_{out} \in D_{\mathbb{Z}_2^{(n_{out}-1)\times 1}}$;
  2. Compute $\mathbf{u}_{in\Rightarrow out} = \mathbf{A}_{in\Rightarrow out} \cdot \mathbf{e}_{out} \in \mathbb{Z}_q^{\hat{n}_{in}\times 1}$, let $\hat{n_{in}} = n_{in} \times \lfloor log\ q \rfloor$. $Powerof2_q(sk_{in}) \in \mathbb{Z}_q^{\hat{n}_{in}}$, and choose a random matrix $\mathbf{A}_{in\Rightarrow out}$ which from $\mathbb{Z}_q^{\hat{n}_{in}\times(n_{out}-1)}$;
  3. Here in order to get the secure scheme and prevent one from learning all the secret keys, we add some noise $\mathbf{x} \leftarrow \chi^{n_{in}\times 1}(\mathbf{x}_{in\Rightarrow out} := Powerof2_q(\mathbf{x}) \in \chi^{\hat{n_{in}}\times 1})$ to the $\mathbf{u}_{in\Rightarrow out}$. Then compute:
  $$\mathbf{b}_{in\Rightarrow out} = \mathbf{A}_{in\Rightarrow out} \cdot \mathbf{e}_{out} + Powerof2_q\left(sk_{in} + \mathbf{x}\right) \in \mathbb{Z}_q^{\hat{n}_{in}\times 1};$$
  4. Output $\mathbf{P}_{in\Rightarrow out} = [\mathbf{b}_{in\Rightarrow out} \mid -\mathbf{A}_{in\Rightarrow out}] \in \mathbb{Z}_q^{\hat{n}_{in}\times n_{out}}$.
- **SwitchKey** $\mathbf{c}_{out} \leftarrow SwitchKey(\mathbf{P}_{in\Rightarrow out}, BitDecomp(\mathbf{c}_{in}))$:
  1. To switch a ciphertext from a secret key sk_{in} to sk_{out}, first compute
  $$\mathbf{P}_{in\Rightarrow out} \cdot (sk_{out}) = \mathbf{b}_{in\Rightarrow out} - \mathbf{A}_{in\Rightarrow out} \cdot \mathbf{e}_{out} = Powerof2_q(sk_{in} + \mathbf{x}) \tag{1}$$
  2. Then output $\mathbf{c}_{out} = \mathbf{P}_{in\Rightarrow out}^T \cdot BitDecomp(\mathbf{c}_{in}) \in \mathbb{Z}_q^{n_{out}\times 1}$, where we note that $BitDecomp(\mathbf{c}_{in}) \in \mathbb{Z}_q^{\hat{n}_{in}\times 1}$.

  We usually omit the subscripts when they are clear in the context.

Lemma 3 *(Correctness). Let $sk_{in} \in \mathbb{Z}^{n_{in}}$, $sk_{out} \in \mathbb{Z}^{n_{out}}$ and $\mathbf{c}_{in} \in \mathbb{Z}_q^{n_{in}}$ be any vectors. Let $\mathbf{P}_{in\Rightarrow out} \leftarrow SwitchKeyGen(sk_{in}, sk_{out})$ and set $\mathbf{c}_{out} \leftarrow SwitchKey(\mathbf{P}_{in\Rightarrow out}, \mathbf{c}_{in})$. Then:*

$$<\mathbf{c}_{out}, sk_{out}> \;=\; <\mathbf{c}_{in}, sk_{in}> + <\mathbf{c}_{in}, \mathbf{x}> (mod\ q) \tag{2}$$

Proof. We will give a more detailed proof than that of [2] and [5].

$$\begin{aligned} <\mathbf{c}_{out}, sk_{out}> &= BitDecomp(\mathbf{c}_{in})^T \cdot Powerof2_q(sk_{in} + \mathbf{x}) \\ &= <\mathbf{c}_{in}, sk_{in}> + <\mathbf{c}_{in}, \mathbf{x}> (mod\ q) \end{aligned}$$

Lemma 4. *$|\pounds|$ is the noise inflicted by the key switching process, We bound $|\pounds|$ using the bound on χ, therefore $|\pounds| := |<\mathbf{c}_{in}, \mathbf{x}>| \le n_{in} \cdot B = O((m\lceil log\ q\rceil)^2)B$, where $\mathbf{x} \leftarrow \chi^{n_{in}}$.*

Lemma 5 *(Security). Let the input secret key $sk_{in} \in \mathbb{Z}^{n_{in}}$ be any vector.If we generate the output secret key $sk_{out} \leftarrow GPV.SecretKeyGen(params)$ and $\mathbf{P}_{sk_{in}\Rightarrow sk_{out}} \leftarrow SwitchKeyGen(sk_{in}, sk_{out})$: then $\mathbf{P}_{sk_{in}\Rightarrow sk_{out}}$ is computationally indistinguishable from uniform random distribution over $\mathbb{Z}_q^{\hat{n}_{in}\times n_{out}}$ under $DLWE_{n,q,\chi}$ assumption.*

3.2 Our Construction

In this subsection, we use the new key-switching procedure as described in Sect. 3.1 to construct a variant of FHE (vFHE) scheme which is based on GPV scheme.

- $params \leftarrow vFHE.Setup(1^\lambda, 1^L)$:
  We choose security parameter λ, the number of level L and output the scheme parameters $params := (m, n, q, \chi)$;
- $(pk, evk, sk) \leftarrow vFHE.KeyGen(params)$:

1. For $i = L$ down to 0, we sample $L + 1$ secret vector $\mathbf{e}_i \leftarrow D_{\mathbb{Z}_q^m, r}$ and output: $sk := \mathbf{e}_L$.
2. Set $\mathbf{u}_i = f_{\mathbf{A}}(\mathbf{e}_i) = \mathbf{A} \cdot \mathbf{e}_i$ and compute $pk_i := \mathbf{P}_i = (\mathbf{u}_i \mid -\mathbf{A}) = (\mathbf{A}\mathbf{e}_i \mid -\mathbf{A})$;
3. For user's secret key sk, for the convenience, we define $\hat{sk_i}$:

$$\begin{aligned}\hat{sk}_{i-1} = (1, \hat{\mathbf{e}}_{i-1})^T &= \big(BitDecomp(sk_{i-1} \otimes sk_{i-1})\big) \in \{0,1\}^{((m+1)\cdot\lceil log\ q\rceil)^2}\\ &= BitDecomp\Big((1, \mathbf{e}_{i-1})^T\Big) \otimes BitDecomp\Big((1, \mathbf{e}_{i-1})^T\Big)\end{aligned}$$

   Compute:

$$\begin{aligned}\mathbf{P}_{\hat{sk}_{i-1} \Rightarrow sk_i} &\leftarrow SwitchKeyGen(\hat{sk}_{i-1}, sk_i)\\ &= SwitchKeyGen\Big((1, \hat{\mathbf{e}}_{i-1})^T, (1, \hat{\mathbf{e}}_i)^T\Big)\end{aligned}$$

4. Output: $pk = \mathbf{P}_0$, $sk = (1, \mathbf{e}_L)^T$, $evk = \mathbf{P}_{\hat{sk}_{i-1} \Rightarrow sk_i}$, $i \in [L]$.

- $\mathbf{c} \leftarrow vFHE.Encrypt(params, pk, m)$:
  1. Set $\mathbf{m} = \big(m, 0, \cdots, 0\big) \in \mathbb{Z}_q^{(m+1)\times 1}$, $m \in \{0,1\}$, then choose $\mathbf{s} \leftarrow \mathbb{Z}_q^{n\times 1}$, $\mathbf{x}^T := (x \leftarrow \{0\}, \mathbf{x}_1^T \leftarrow \chi^{1\times m}) \in D_{\mathbb{Z}^{1\times(m+1)}}$;
  2. Compute $\mathbf{c} := \mathbf{P}^T \cdot \mathbf{s} + \lfloor \frac{q}{2} \rfloor \cdot \mathbf{m} + \mathbf{x} \in \mathbb{Z}_q^{(m+1)\times 1}$, where the size of ciphertext is $O((m+1)log^2\ q)$.
- $m' \leftarrow vFHE.Decrypt(params, sk, \mathbf{c})$:
  1. Compute $<\mathbf{c}, \tilde{\mathbf{e}}> = \lfloor \frac{q}{2} \rfloor \cdot m + small\ (mod\ q)$, where secret keys $sk := \tilde{\mathbf{e}} = (1, \mathbf{e})^T$.
- $vFHE.Evaluate(params, evk, \mathbf{c}_1, \cdots, \mathbf{c}_l)$:
  - $Eval.Add(evk, \mathbf{c}_1, \mathbf{c}_2)$, $\mathbf{c}_{add} \leftarrow SwitchKey(\mathbf{P}_{(\mathbf{i-1})\Rightarrow \mathbf{i}}, \hat{\mathbf{c}}_{add}) \in \mathbb{Z}_q^{n+1}$:
    Assume w.l.o.g that both input ciphertexts are encrypted under the same secret key sk_{i-1}. Where $\hat{\mathbf{c}}_{add} := Powerof2(\mathbf{c}_1 + \mathbf{c}_2) \otimes Powerof2((1, 0, \cdots, 0))$.
  - $Eval.Mult(evk, \mathbf{c}_1, \mathbf{c}_2)$, $\mathbf{c}_{mult} \leftarrow SwitchKey(\mathbf{P}_{(\mathbf{i-1})\Rightarrow \mathbf{i}}, \hat{\mathbf{c}}_{mult}) \in \mathbb{Z}_q^{n+1}$:
    Assume w.l.o.g that both input ciphertexts are encrypted under the same secret key sk_{i-1}. Where $\hat{\mathbf{c}}_{mult} = \lfloor \frac{2}{q} \cdot (Powerof2(\mathbf{c}_1 \otimes \mathbf{c}_2)) \rceil = \lfloor \frac{2}{q} \cdot (Powerof2(\mathbf{c}_1) \otimes Powerof2(\mathbf{c}_2)) \rceil$.

Lemma 6 *(Correctness). Suppose the parameters* $r := B \geq \omega(\sqrt{log\ n}) \cdot \sqrt{n}$ *(refer to [2]),* $m = nlog\ q + 2\lambda$*. A E-noise ciphertext of some message* $m \in \{0,1\}$ *under secret key* $sk := \tilde{\mathbf{e}} \in \mathbb{Z}_q^{(m+1)\times 1}$ *under ciphertext vector* $\mathbf{c} := \mathbf{P}^T \cdot \mathbf{s} + \lfloor \frac{q}{2} \rfloor \cdot \mathbf{m} + \mathbf{x}\ (mod\ q) \in \mathbb{Z}_q^{(m+1)\times 1}$*. It holds that:*

$$\mathbf{c}^T \cdot \tilde{\mathbf{e}} := \lfloor \frac{q}{2} \rfloor \cdot m + \underbrace{x + \mathbf{x}_1^T \cdot \mathbf{e}}_{small}\ (mod\ q)$$

with $m \in \{0,1\}$ *and* $|small| < E \leq \lfloor q/2 \rfloor /2$*. Then* $m \leftarrow Decrypt(sk, \mathbf{m})$*.*

Proof. Where $\mathbf{x} \leftarrow \{0\} \times \chi^m$. Then For $\forall x_i \leftarrow \chi, i \neq 1$, $|x_i| \leq B$(where $B \ll q$ is a bound on the values of χ), $\mathbf{x}_1 \leftarrow \chi^m$. By definition, We can get

$$<\mathbf{c}, \tilde{\mathbf{e}}> = \mathbf{s}^T \cdot \mathbf{P} \cdot \tilde{\mathbf{e}} + \lfloor \frac{q}{2} \rfloor \cdot m + \underbrace{x + \mathbf{x}_1^T \cdot \mathbf{e}}_{small}, (By\ Lemma\ 1)$$
$$= \lfloor \frac{q}{2} \rfloor \cdot m + small\ (mod\ q)$$

with $||small|| \leq ||x|| + ||\mathbf{x}_1^T \cdot \mathbf{e}|| \leq E$, the norm of the error elements is bounded by $B_\chi \cdot r \cdot \omega(\sqrt{log\ m}) + B_\chi \sqrt{m}/2$, i.e. $||B_\chi \cdot r\omega(\sqrt{log\ m}) + B_\chi\sqrt{m}/2|| < E \leq \frac{q}{4}$, for the sake of simplicity we set the norm of error elements expressed by E. □

3.3 Homomorphic Operation Analysis

Choose $m_0, m_1 \in \{0,1\}$, then generate the $\mathbf{m}_0 = \big(m_0, 0, \cdots, 0\big) \in \mathbb{Z}_q^{(m+1)\times 1}$ and $\mathbf{m}_1 = \big(m_1, 0, \cdots, 0\big) \in \mathbb{Z}_q^{(m+1)\times 1}$ separately. Run the $Encrypt(params, pk, \mathbf{m}_i)$, $i \in \{0,1\}$:

$$\mathbf{c}_0 = \mathbf{P}^T \cdot \mathbf{s} + \lfloor \frac{q}{2} \rfloor \cdot \mathbf{m} + \mathbf{x} \in \mathbb{Z}_q^{(m+1)\times 1}; \mathbf{c}_1 = \mathbf{P}^T \cdot \mathbf{s} + \lfloor \frac{q}{2} \rfloor \cdot \mathbf{m} + \mathbf{x} \in \mathbb{Z}_q^{(m+1)\times 1};$$

Then run the $Decrypt(params, sk, \mathbf{c}_i), \in \{0,1\}$ separately, we get:

$$<\mathbf{c}_0, \tilde{\mathbf{e}}_0> \ = \ <\mathbf{c}_0, (1, \mathbf{e}_0)^T> \ = \lfloor \frac{q}{2} \rfloor \cdot m_2 + small_0;$$
$$<\mathbf{c}_1, \tilde{\mathbf{e}}_1> \ = \ <\mathbf{c}_1, (1, \mathbf{e}_1)^T> \ = \lfloor \frac{q}{2} \rfloor \cdot m_1 + small_1$$

Homomorphic Addition Analysis

Lemma 7. *For* $Eval.Add(evk, \mathbf{c}_0, \mathbf{c}_1)$*, we have*

$$\hat{\mathbf{c}}_{add} := Powerof2(\mathbf{c}_0 + \mathbf{c}_1) \otimes Powerof2((1, 0, \cdots, 0)) \in \mathbb{Z}_q^{\big((m+1)\lceil log\ q \rceil\big)^2}$$

then we get $\mathbf{c}_{add} \leftarrow SwitchKey(\mathbf{P}_{(\mathbf{i-1})\Rightarrow \mathbf{i}}, \hat{\mathbf{c}}_{add}) \in \mathbb{Z}_q^{n+1} := [\mathbf{P}^T_{(\mathbf{i-1})\Rightarrow \mathbf{i}} \cdot \hat{\mathbf{c}}_{add}]_q$*, for* $<\mathbf{c}_{add}, (1, \mathbf{e}_{add})> \ = \ <\hat{\mathbf{c}}_{add}, (1, \hat{\mathbf{e}}_{add})> + <\hat{\mathbf{c}}_{add}, \mathbf{x}>\ (mod\ q)$*, there exists:*

$$<\hat{\mathbf{c}}_{add}, (1, \hat{\mathbf{e}}_{add})>(mod\ q) = \lfloor \frac{q}{2} \rfloor \cdot (m_0 + m_1) + error^{Add} + k' \cdot q$$

where the $|error^{Add} + <\hat{\mathbf{c}}_{add}, \mathbf{x}>| \leq 2E + O\big((m\lceil log\ q \rceil)^2\big) \cdot B < \lfloor q/2 \rfloor /2$*.*

Proof. For $||<\hat{\mathbf{c}}_{add}, \mathbf{x}>|| \leq (n_{in}log\ q)^2 \cdot B = O\big((m\lceil log\ q\rceil)^2\big) \cdot B$, where $\mathbf{x} \leftarrow \chi^{\left((m+1)\lceil log\ q\rceil\right)^2}$, by Lemma 4. For $\mathbf{c}_{add} = \mathbf{c}_1 + \mathbf{c}_2$, by Lemma 3 there exists:

$$<\hat{\mathbf{c}}_{add}, \hat{sk}_{i-1}> = \lfloor\frac{q}{2}\rfloor(m_1 + m_2) + \underbrace{(small_1 + small_2)}_{error^{Add}} + \underbrace{(k_1 + k_2)}_{k'} \cdot q$$
$$= \lfloor\frac{q}{2}\rfloor(m_1 + m_2) + error^{Add} + k' \cdot q.$$

The above Lemma 7 is proven using the Lemma 6 and Triangle-Inequality, $||error^{Add}|| \leq ||small_1|| + ||small_2|| \leq 2E$. By Lemmas 4 and 6, putting it together, the bound on error of addition is $|<\mathbf{c}, \mathbf{x}> + error^{Add}| \leq 2E + O((m\lceil log\ q\rceil)^2)B \leq \frac{q}{4}$.

Homomorphic Multiplication Analysis. Homomorphic multiplication has an even more significant problem than the error growth: the dimension of the ciphertext also grows extremely fast, i.e., exponentially with the number of multiplied ciphertexts, due to the use of the tensor product. To resolve this issue, [5] introduced a clever dimension reduction—also called key switching technique. But we make a little modification to the technique, as shown in the new key switching procedure Subsect. 3.1, so that the new key switching procedure will help us analyze the behave of error elements.

Lemma 8. *If $|k| \leq O(m \log q)$, then there exists:*

$$\left\langle (Powerof2(\mathbf{c}), BitDecomp\Big(\ (1, \mathbf{e}_{i-1})^T\ \Big)\right\rangle = \langle \mathbf{c}, (1, \mathbf{e}_{i-1})^T \rangle$$
$$= \left\lfloor \frac{q}{2} \right\rfloor \cdot m + small + kq.$$

Proof

$$|k| = \frac{\left|\left\langle (Powerof2(\mathbf{c}), BitDecomp\Big(\ (1, \mathbf{e}_{i-1})^T\ \Big)\right\rangle - \lfloor\frac{q}{2}\rfloor \cdot m - small\right|}{q}$$
$$\leq \frac{1}{2} \cdot (m+1)\lceil log\ q\rceil + 1 = O(mlog\ q)$$

Lemma 9. *For $Eval.Mult(evk, \mathbf{c}_0, \mathbf{c}_1)$, we have $\hat{\mathbf{c}}_{mult} = \lfloor\frac{2}{q}(Powerof2(\mathbf{c}_1 \otimes \mathbf{c}_2))\rceil = \lfloor\frac{2}{q}(Powerof2(\mathbf{c}_1) \otimes Powerof2(\mathbf{c}_2))\rceil$, then we get*

$$\mathbf{c}_{mult} \leftarrow SwitchKey(\mathbf{P}_{(\mathbf{i-1})\Rightarrow\mathbf{i}}, \hat{\mathbf{c}}_{mult}) := [\mathbf{P}^T_{(\mathbf{i-1})\Rightarrow\mathbf{i}} \cdot \hat{\mathbf{c}}_{mult}]_q \in \mathbb{Z}_q^{n+1}.$$

Hence for $<\mathbf{c}_{mult}, (1, \mathbf{e}_{mult})> = <\hat{\mathbf{c}}_{mult}, (1, \hat{\mathbf{e}}_{mult})> + <\hat{\mathbf{c}}_{mult}, \mathbf{x}>(mod\ q)$, there exists:

$$<\hat{\mathbf{c}}_{mult}, (1, \hat{\mathbf{e}}_{mult})>(mod\ q) = \lfloor\frac{q}{2}\rfloor \cdot (m_0 m_1) + error^{Mult}(mod\ q)$$

where the $||error^{Mult} + \langle\hat{\mathbf{c}}_{mult}, \mathbf{x}\rangle|| \leq 2E + 2 \cdot O(m \log\ q)E + \frac{E^2}{q} + O\big((m\lceil log\ q\rceil)^2\big) \cdot B \leq \frac{q}{4}$.

Proof. By Lemma 4, we get $||{<}\hat{\mathbf{c}}_{mult}, \mathbf{x}{>}|| \leq O\big((m\lceil log\ q\rceil)^2\big) \cdot B$. For $\hat{\mathbf{c}}_{mult} = \lfloor \frac{2}{q} \cdot (Powerof2(\mathbf{c}_1 \otimes \mathbf{c}_2))\rceil = \lfloor \frac{2}{q} \cdot (Powerof2(\mathbf{c}_1) \otimes Powerof2(\mathbf{c}_2))\rceil$ by Lemma 3, there exits

$$\begin{aligned} {<}\hat{\mathbf{c}}_{mult}, \hat{sk}_{mult}{>} &:= \Big\langle \lfloor \frac{2}{q} \cdot (Powerof2(\mathbf{c}_1) \otimes Powerof2(\mathbf{c}_2))\rceil, \\ &\qquad BitDecomp\Big((1, \mathbf{e}_{i-1})^T \Big) \otimes BitDecomp\Big((1, \mathbf{e}_{i-1})^T \Big) \Big\rangle \\ &= \Big\langle \Big(\frac{2}{q} \cdot \big(Powerof2(\mathbf{c}_1 \otimes \mathbf{c}_2)\big) + \mathbf{c}_\delta \Big), \\ &\qquad BitDecomp\Big((1, \mathbf{e}_{i-1})^T \otimes (1, \mathbf{e}_{i-1})^T \Big) \Big\rangle \end{aligned}$$

Observe that $\mathbf{c}^*_{mult} = \frac{2}{q} \cdot \mathbf{c}_{mult} = \frac{2}{q} \cdot \mathbf{c}_1 \otimes \mathbf{c}_2$ since $\mathbf{c}_{mult} = 2 \cdot \mathbf{c}_1 \otimes \mathbf{c}_2$, therefore:

$$\begin{aligned} \langle \mathbf{c}^*_{mult}, sk_{mult} \rangle &= \Big\langle \Big(\frac{2}{q} \cdot \big(Powerof2(\mathbf{c}_1 \otimes \mathbf{c}_2)\big) \Big), \\ &\qquad BitDecomp\Big((1, \mathbf{e}_{i-1})^T \otimes (1, \mathbf{e}_{i-1})^T \Big) \Big\rangle \\ &= \frac{2}{q} \left\lfloor \frac{q}{2} \right\rfloor^2 \cdot \underbrace{m_1 m_2}_{Eq.1} + \frac{2}{q} \left\lfloor \frac{q}{2} \right\rfloor \cdot Eq.2 + \frac{2}{q} q Eq.3 + \frac{2}{q} \cdot Eq.4 + 2 \cdot Eq.5 \\ &= \left\lfloor \frac{q}{2} \right\rfloor \cdot m_1 m_2 + error^{Mult}\ (mod\ q) \end{aligned}$$

For further convenience, we denote $Eq.\,2 = \Big(\big(m_1 \cdot small_2 + m_2 \cdot small_1\big) \Big)$, $Eq.\,3 = (small_1 k_2 + small_2 k_1)$, $Eq.\,4 = (small_1 small_2)$ and $Eq.\,5 = qk_1k_2 + \left\lfloor \frac{q}{2} \right\rfloor (m_1 k_2 + m_2 k_1)$. Hence, we easily observe that $error^{Mult} := \frac{2}{q} \cdot \left\lfloor \frac{q}{2} \right\rfloor \cdot Eq.\,2 + \frac{2}{q} q \cdot Eq.\,3 + \frac{2}{q} \cdot Eq.\,4 + 2 \cdot Eq.\,5$.

We can get the result of $||error^{Mult}|| \leq 2E + 2 \cdot O(m \log\ q)E + E^2 \leq \frac{q}{4}$ by Lemmas 6 and 8.

Lemma 10. *By definition:*

$$\begin{aligned} \Delta &:= \Big\langle \mathbf{c}_\delta, \hat{sk}_{i-1} \Big\rangle \\ &= \Big\langle \underbrace{\Big(\lfloor \frac{2}{q} \cdot (Powerof2(\mathbf{c}_1 \otimes \mathbf{c}_2))\rceil - \frac{2}{q} \cdot (Powerof2(\mathbf{c}_1 \otimes \mathbf{c}_2)) \Big)}_{\mathbf{c}_\delta}, \hat{sk}_{i-1} \Big\rangle \end{aligned}$$

Now, since $||\mathbf{c}_\delta||_\infty \leq \frac{1}{2}$ *and since* $\hat{sk}_{i-1} \in \{0,1\}^{\big((m+1)\lceil log\ q\rceil\big)^2}$*, then* $||\hat{sk}_{i-1}||_1 \leq \big((m+1)\lceil log\ q\rceil\big)^2$*. It follows that* $|\Delta| \leq ||\mathbf{c}_\delta|| \cdot ||\hat{sk}_{i-1}|| \leq \frac{1}{2} \cdot \big((m+1)\lceil log\ q\rceil\big)^2 = O(m^2 log^2 q)$*.*

Proof. Because $\left\langle \hat{\mathbf{c}}_{mult}, \hat{sk}_{i-1}\right\rangle =: \left\langle \lfloor \frac{2}{q}\cdot(Powerof2(\mathbf{c}_1\otimes\mathbf{c}_2))\rceil, \hat{sk}_{i-1}\right\rangle$, therefore:

$$\begin{aligned}\left\langle \hat{\mathbf{c}}_{mult}, \hat{sk}_{i-1}\right\rangle - \Delta &= \left\langle \frac{2}{q}\cdot(Powerof2(\mathbf{c}_1\otimes\mathbf{c}_2)), \hat{sk}_{i-1}\right\rangle \\ &= \frac{2}{q}<\mathbf{c}_1,(1,\mathbf{e}_1)^T>\cdot<\mathbf{c}_2,(1,\mathbf{e}_2)^T>\end{aligned}$$

By Lemmas 4, 6 and 9, putting them together, the bound of multiplication noise is $||\lfloor error^{mult}\rceil|| + ||<\mathbf{c}_{mult},\mathbf{x}>|| \le ||\Delta|| + ||errror^{mult}|| = O((m\lceil log\ q\rceil)^2) + 2E + 2\cdot O(m\log\ q)E + E^2 \le \frac{q}{4}$.

Theorem 1. *The decryption works correctly as long as*

$$\begin{aligned}||error|| = max\{&2E + O((m\lceil\log q\rceil)^2)\cdot B,\\ &O((m\lceil\log q\rceil)^2) + 2E + 2\cdot O(m\log q)E + E^2\} \le \frac{q}{4}\end{aligned}$$

Proof. The proof of Theorem 1 is deferred to Lemmas 7 and 9. We omit further details here.

Theorem 2. *If the scheme $vFHE$ with parameters $n, q, |\chi| \le B$, L, then we say the scheme $vFHE$ is L-homomorphic.*

Proof. Set the L is the circuit depth, then let E_i be a bound on the noise in the ciphertext after the evaluation of i-th ($i \in [L]$) level of gates. Firstly, assume that $E_0 := (r\cdot\omega(\sqrt{log\ m})+\sqrt{m}/2)\cdot B_\chi$, it hold that $E_{i+1} = (r\cdot\omega(\sqrt{log\ m})+\sqrt{m}/2)\cdot E_i$. Then, we get $E_L = (r\cdot\omega(\sqrt{log\ m})+\sqrt{m}/2)^{L+O(1)}\cdot B_\chi$. Lastly, if $E_L < \lfloor q/2\rfloor/2$ by Lemma 6, the scheme can decrypted successfully. □

3.4 Security Analysis

We now sketch the security proof.

Theorem 3. *The above system is IND-CPA-secure and anonymous, assuming that LWE is hard.*

Proof. The proof contains three steps:

- Firstly, we argue that the distribution of the syndrome $\mathbf{u} = \mathbf{Ae}$ is statistically close to uniform over $\mathbb{Z}_q^n$ follows directly from Lemma 2 and the public key $\mathbf{P}_0 := [\mathbf{u}_0, -\mathbf{A}]$ is computationally indistinguishable from uniform distribution based on Lemma 5.
- Secondly, we argue that the evaluate key $\mathbf{P}_{sk_0:sk_1}, \cdots, \mathbf{P}_{sk_{L-1}:sk_L}$, we replace all $\mathbf{P}_{sk_{i-1}:sk_i}$, $i \in [L]$ with uniform distribution in descending order (one by one).
- Finally, we can use the leftover hash lemma to replace the ciphertext $\mathbf{c}$ with a uniformly random value $\mathbf{c}'$, which are indistinguishable from uniform assuming the hardness of $LWE_{n,m,q,\chi}$. In this case, the challenge ciphertext is statistically independent of the encrypted message.

This concludes the proof of the theorem. □

4 Conclusion

In Table 1, we provide a comparison between our scheme and the FHE schemes [2,17], where all of the schemes are adaptive indistinguishable chosen plaintext security and can be proved secure under the LWE assumption.

In this work, we revisited Brakerski's key-Switching approach from LWE-based FHE cryptosystems and constructed a Brakerski style of FHE scheme based on dual LWE assumption. Besides, we also conducted a theoretical comparison of Brakerski [2] scheme and our scheme.

Table 1. Comparison four scheme

Scheme	$\|pk\|$	$\|sk\|$	$\|evk\|$	$\|bit\|$	$\|Ct\|$	Assumption
[2]	$O(mnlog\ q)$	$O(nlog\ q)$	$O(n^2 log\ q)$	1	$O(n \cdot log\ q)$	LWE
[17]	$O(mnlog\ q)$	$O(mlog\ q)$	$O(m^2 log^2\ q)$	1	$O(m \cdot log\ q)$	Dual-Ferr-LWE
vFHE	$O(mnlog\ q)$	$O(mlog\ q)$	$O(m^2 log^2\ q)$	1	$O(m \cdot log\ q)$	Dual-LWE

Acknowledgements. We would like to thank all anonymous reviewers for their helpful advice and comments. This work is supported by the National Natural Science Foundation of China (Grant No. 61472097) and Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund (Fujian Normal University) (No. 15003).

References

1. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_28
2. Brakerski, Z.: Fully homomorphic encryption without modulus switching from classical GapSVP. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 868–886. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32009-5_50
3. Brakerski, Z., Gentry, C., Halevi, S.: Packed ciphertexts in LWE-based homomorphic encryption. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 1–13. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36362-7_1
4. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, pp. 309–325, ACM (2012)
5. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, pp. 97–106. IEEE (2011)
6. Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 505–524. Springer, Heidelberg (2011). doi:10.1007/978-3-642-22792-9_29

7. Brakerski, Z., Vaikuntanathan, V.: Lattice-based the as secure as PKE. In: Proceedings of the 5th Conference on Innovations in Theoretical Computer Science, pp. 1–12 (2014)
8. Fu, Z., Ren, K., Shu, J., Sun, X., Huang, F.: Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Trans. Parallel Distrib. Syst. **27**(9), 2546–2559 (2016)
9. Gentry, C., et al.: Fully homomorphic encryption using ideal lattices. STOC **9**, 169–178 (2009)
10. Gentry, C., Halevi, S., Smart, N.P.: Homomorphic evaluation of the AES circuit. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 850–867. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32009-5_49
11. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, pp. 197–206. ACM (2008)
12. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 75–92. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40041-4_5
13. Halevi, S., Shoup, V.: Algorithms in HElib. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 554–571. Springer, Heidelberg (2014). doi:10.1007/978-3-662-44371-2_31
14. Halevi, S., Shoup, V.: Bootstrapping for `HElib`. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 641–670. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46800-5_25
15. Hiromasa, R., Abe, M., Okamoto, T.: Packing messages and optimizing bootstrapping in GSW-FHE. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 699–715. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_31
16. Li, Z., Galbraith, S.D., Ma, C.: Preventing adaptive key recovery attacks on the GSW levelled homomorphic encryption scheme. In: Proceedings of the Provable Security - 10th International Conference, ProvSec 2016, Nanjing, China, 10–11 November 2016, pp. 373–383 (2016)
17. Li, Z., Ma, C., Du, G., Ouyang, W.: Dual LWE-based fully homomorphic encryption with errorless key switching. In: IEEE ICPADS 2016, pp. 1169–1174 (2016)
18. Li, Z., Ma, C., Morais, E., Du, G.: Multi-bit leveled homomorphic encryption via mathsf dual.LWE-based. In: Proceedings Inscrypt 2016, Revised Selected Papers, Beijing, China, 4–6 November 2016, pp. 221–242 (2016)
19. Li, Z., Ma, C., Wang, D.: Leakage resilient leveled the on multiple bit message. IEEE Trans. Big Data (2017)
20. Rivest, R.L., Adleman, L., Dertouzos, M.L.: On data banks and privacy homomorphisms. Found. Secure Comput. **4**(11), 169–180 (1978)
21. Smart, N.P., Vercauteren, F.: Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 420–443. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13013-7_25
22. Stehlé, D., Steinfeld, R.: Faster fully homomorphic encryption. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 377–394. Springer, Heidelberg (2010). doi:10.1007/978-3-642-17373-8_22
23. Wang, D., He, D., Wang, P., Chu, C.-H.: Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans. Dependable Secure Comput. **12**(4), 428–442 (2015)

24. Wang, D., Wang, N., Wang, P., Qing, S.: Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity. Inf. Sci. **321**, 162–178 (2015)
25. Xia, Z., Wang, X., Sun, X., Wang, Q.: A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans. Parallel Distrib. Syst. **27**(2), 340–352 (2016)
26. Xia, Z., Wang, X., Zhang, L., Qin, Z., Sun, X., Ren, K.: A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. IEEE Trans. Inf. Forensics Secur. **1**(11), 2594–2608 (2016)