A New Batch FHE Scheme over the Integers

Kwak Wi Song[1], Kim Chol Un [1]

[1] School of Mathematics,
Kim Il Sung University,
Pyongyang, Democratic People's Republic of Korea

Abstract. The FHE (fully homomorphic encryption) schemes [7, 13] based on the modified AGCD problem (noise-free AGCD problem) are vulnerable to quantum attacks, because its security relies partly on the hardness of factoring, and some FHE schemes based on the decisional AGCD without the noise-free assumption, for example [1], has a drawback that its ciphertexts are very large.

In this paper, we construct a new batch FHE scheme based on the decisional AGCD problem to overcome these weaknesses and prove its security.

Keywords: FHE, AGCD problem, Batch Encryption, Chinese Remainder Theorem.

1 Introduction

In 1978, Rivest, Adleman, and Dertouzos [18] firstly introduced the concept of the FHE scheme. The main goal of their idea is to allow computations on encrypted data without loss of the data security. Three decades later, in 2009, C. Gentry [10, 11] proposed the first FHE scheme based on the ideal lattice. The security of this FHE scheme is based on the Bounded Distance Decoding (BDD) problem and the Sparse Subset Sum (SSS) problem. Later, Gentry's FHE scheme was improved by C. Gentry & S. Halevi [12], N. P. Smart & F. Vercauteren [19], D. Stehlѐ & R. Steinfeld [20], etc.

In 2010, van Dijk, Gentry, Halevi and Vaikuntanathan [21] proposed the alternative FHE scheme. The security of their FHE scheme relies on the SSSP and the Approximate Greatest Common Divisor (AGCD) problem. The efficiency of the DGHV scheme has been improved by D. Benarroch, et al. [1], J. H. Cheon, et al. [7], J. S. Coron, et al. [9], J. H. Cheon & D. Stehlѐ [8], etc.

Nowadays, Many FHE schemes towards the resistance to quantum attacks put their security on two main computational problems: (1) the Learning With Errors (LWE) problem defined by Regev[17] and (2) Howgrave-Graham's AGCD problem[16]. Up to present, there are no polynomial-time quantum algorithms to solve these problems.

Z. Brakerski & V. Vaikuntanathan [4, 5] developed the first LWE-based FHE schemes. These schemes were improved to ones with better efficiency and security by subsequent works such as Z. Brakerski [2], Z. Brakerski and C. Gentry, et al [3], Z. Brakerski and V. Vaikuntanathan [6], C. Gentry and S. Halevi, et al [13, 14], C. Gentry and A. Sahai, et al [15], etc.

At Crypt 2015, Cheon and Stehlѐ [8] brought out a reduction from the LWE problem to the AGCD problem. Therefore, we consider that the AGCD problem, which finds out the hidden common divisor from many approximate multiples of a prime number or a product of primes, are harder than the LWE problem, whose polynomial time quantum algorithm is unknown yet [1].

The AGCD-based FHE schemes firstly proposed by van Dijk, et al. [21], are getting interests of numbers of researchers for its advantage of dependency on relatively easy integer operations [1, 7, 9, 8], and the AGCD-based FHE schemes are often called the **FHE over the integers** (FHE-OI). The FHE scheme suggested in [21] has a drawback that it has to encrypt/decrypt only one bit at a time. Cheon, et al. [7] and Coron, et al.[9] presented the batch FHE schemes that can encrypt/decrypt several bits at once, but the security of their batch version is based on the noise-free variant of the AGCD problem that has a right common multiple among given approximate common multiples. This modified AGCD problem is easier than the general one, and attackers can guess some of the hidden common divisor by factorizing the right common multiple with the help of a quantum computer.

In [8], the authors suggested new AGCD-based FHE scheme invulnerable to quantum attack in order to overcome the defects of [7, 9]. However, they could not overcome the defect of encryption/decryption per one bit. Therefore, they suggested the construction of a batch one of their FHE scheme as an open problem.

On the other hand, Benarroch, et al. [1] proposed a new FHE-OI scheme and its batch version that are resistant to quantum attacks, but they have longer ciphertexts than the one in [8].

Our Contribution: In [8], the authors only constructed the non-batched FHE scheme, and pointed out that their scheme may be extended to a batch version, similarly to [7, 9]. However, there is a serious difference of the schemes in [7, 9] and the one in [8]. The difference is that the security of the scheme in [8] is based on the original AGCD problem and the ones in [7, 9] is based on the noise-free variant of the AGCD problem. To be more exact, the first element of the public-key x_0 has different property in [8] and [7, 9]. In [8], x_0 is an approximate common multiple of primes, but in [7, 9], x_0 is an exact common multiple of the hidden prime. Therefore, there are some issues to construct batch version of [8].

In this paper, we suggest a new batch FHE scheme with much shorter ciphertexts than the one in [1], which can be a partial solution of one open problem in [8], and prove its security.

2 Preliminaries

2.1 Notation

We denote by $a \leftarrow \mathrm{A}$ selecting an element a uniformly at random from a finite set A. When φ is a distribution, we denote by $a \leftarrow \varphi$ selecting a sample a according to the distribution φ. If x is real, then $\lceil x \rfloor$ is the nearest integer to x, rounding upwards if there are two. Given $x \in \mathbf{R}$ and $p \in \mathbf{Z}^+$, we use $[x]_p$ to denote unique number in $(-p/2, p/2]$ that satisfies the condition $(x-[x]_p) \bmod p = 0$.

We use the CRT representations. For given pairwise coprime integers $p_1, \ldots, p_k$, we define $\mathrm{CRT}_{p_1,\ldots,p_k}(a_1,\ldots,a_k)$ as a unique integer in $(-T/2, T/2]$ such that $\mathrm{CRT}_{p_1,\ldots,p_k}(a_1,\ldots,a_k) \equiv a_i \pmod{p_i}$ for $i = 1,\ldots,k$. Exactly

$$\mathrm{CRT}_{p_1,\ldots,p_k}(a_1,\ldots,a_k) = \left[\sum\nolimits_{i=1}^{k} a_i \hat{p}_i \left(\hat{p}_i^{-1} \bmod p_i\right)\right]_T ,$$

where $T := \prod\nolimits_{j=1}^{k} p_j$ and $\hat{p}_i := T/p_i = \prod\nolimits_{j=1}^{k} p_j \Big/ p_i$.

$$\mathrm{CRT}_{p_1,\ldots,p_k}(\mathbf{a}_1,\ldots,\mathbf{a}_k) := \left(\mathrm{CRT}_{p_1,\ldots,p_k}(a_{11},\ldots,a_{k1}), \cdots, \mathrm{CRT}_{p_1,\ldots,p_k}(a_{1l},\ldots,a_{kl})\right)$$

where $\mathbf{a}_i := (a_{i1}, \cdots, a_{il})$, $i = 1,\ldots,k$.

For $n \in \mathbf{Z}^+$, we define the function BD_n: $\mathbf{Z} \cap [0, 2^n) \to \{0,1\}^n$ and $P_n : \mathbf{R} \to \mathbf{R}^n$ as follows:

For $x \in \mathbf{Z} \cap [0, 2^n)$ and $y \in \mathbf{R}$,

$$BD_n(x) := (x_0,\ldots,x_{n-1}) \in \{0,1\}^n \text{ with } x = \sum\nolimits_{i=0}^{n-1} x_i 2^i ,$$

$$P_n(y) := \left(y, 2y, \ldots, 2^{n-1} y\right) \in \mathbf{R}^n .$$

Then we can prove the following expression:

$$\langle BD_n(x), P_n(y) \rangle = \sum\nolimits_{i=0}^{n-1} x_i \left(2^i y\right) = xy .$$

We also recall the tensor product of two given vectors:

$$(u_1,\ldots,u_n) \otimes (v_1,\ldots,v_n) := (u_1 v_1, \ldots, u_1 v_n, \ldots, u_n v_1, \ldots, u_n v_n) .$$

Moreover, it satisfies the following relation with the scalar product:

$$\langle \mathbf{u} \otimes \mathbf{u}', \mathbf{v} \otimes \mathbf{v}' \rangle = \langle \mathbf{u}, \mathbf{v} \rangle \cdot \langle \mathbf{u}', \mathbf{v}' \rangle .$$

2.2 Some Distributions and AGCD problems

For η -bit primes $p_1, \dots, p_k$, we define some distributions as follows:

$$\Phi_\rho(p_1,\dots,p_k) := \left\{ r = \mathrm{CRT}_{p_1,\dots,p_k}(r_1,\dots,r_k) \,\middle|\, r_i \leftarrow \mathrm{Z} \cap \left(-2^\rho, 2^\rho\right) \right\},$$

$$D_{\gamma,\rho}(p_1,\dots,p_k) := \left\{ x = q\prod p_i + r \,\middle|\, q \leftarrow \mathrm{Z} \cap \left[0, \frac{2^\gamma}{\prod p_i}\right), r \leftarrow \Phi_\rho(p_1,\dots,p_k) \right\},$$

$$D_{\gamma,\rho,j}(p_1,\dots,p_k) := \left\{ y = \mathrm{CRT}_{p_1,\dots,p_k}\left(0,\dots,\frac{p_j+1}{2},\dots,0\right) + q\prod p_i + r \,\middle|\, q \leftarrow \mathrm{Z} \cap \left[0, \frac{2^\gamma}{\prod p_i}\right), r \leftarrow \Phi_\rho(p_1,\dots,p_k) \right\}.$$

Definition 1 [7] **(The $(\rho,\eta,\gamma)-k-$AGCD decisional problem).** *Let ρ,η,γ be the security parameters and $p_1,\dots,p_k$ be η -bit primes. The decisional problem is to distinguish between the distribution $D_{\gamma,\rho}(p_1,\dots,p_k)$ and the uniform distribution* $\mathrm{U}(\mathbf{Z} \cap [0,2^\gamma))$.

Definition 2 (The $(\rho,\eta,\gamma,j)-k-$ AGCD decisional problem). *Let ρ,η,γ be the security parameters, $p_1,\dots,p_k$ be η -bit primes, and j be the chosen index. The decisional problem is to distinguish between the distribution $D_{\gamma,\rho}(p_1,\dots,p_k)$ and the uniform distribution* $\mathrm{U}(\mathbf{Z} \cap [0,2^\gamma))$.

The $(\rho,\eta,\gamma)-k-$AGCD decisional problem and the $(\rho,\eta,\gamma,j)-k-$AGCD decisional problem have the same degree of computational complexity, i.e. if there is a polynomial-time quantum algorithm to solve the $(\rho,\eta,\gamma)-k-$AGCD decisional problem then we can construct a polynomial-time quantum algorithm to solve the $(\rho,\eta,\gamma,j)-k-$AGCD decisional problem. Moreover, the inverse argument is correct.

On the other hand, from the known reduction of LWE problem to AGCD problem [8], we can assume that the $(\rho,\eta,\gamma)-k-$AGCD decisional problem is hard:

Main assumption *The $(\rho,\eta,\gamma)-k-$AGCD decisional problem is hard to solve by any quantum computers.*

3 Our Batch Somewhat Homomorphic Encryption scheme

In this section, we generalize the FHE scheme [8] to a new batch Somewhat HE scheme and then prove its security. To construct a new batch SHE(Somewhat Homomorphic Encryption) scheme, we use the CRT representation.

3.1 The Construction

We define some parameters. In this paper, λ is the security parameter, ρ is the maximum bit length of the error, η is the bit length of the secret prime integers, γ is the bit length of the ciphertexts, τ is the number of encryptions of zero in public key, and k is the number of distinct secret primes.

We assume that these parameters satisfy the following constraints by discussions in [1, 8]:

- $\rho \geq \lambda$,
- $\gamma \geq \Omega\left(\lambda/\log\lambda(\eta-\rho)^2\right)$ and $\gamma \geq \eta^2$,
- $\tau \geq \gamma + 2\lambda + 2$.

KeyGen $(\lambda,\rho,\eta,\gamma,\tau,k)$ The secret key is a set of η -bit distinct odd primes $p_1,\dots,p_k : sk := \{p_1,\dots,p_k\}$. Choose $x_i \leftarrow D_{\gamma,\rho}(p_1,\dots,p_k)$ ($i = 0,\dots,\tau$) and relabel the indexes so that $x_0 \geq \max\{x_1,\dots,x_\tau\}$ and $x_0 > \gamma^2 k 2^\eta$. Let

$\mathrm{X} := \{x_0,\ldots,x_\tau\}$. For $j = 1,\ldots,k$, choose a random subset S_j of $\{1,\ldots,\tau\}$.

$$y_j := \left[\mathrm{CRT}_{p_1,\ldots,p_k}\big(0,\ldots,\underset{j}{(p_j+1)/2},\ldots,0\big) + \sum_{i\in \mathrm{S}_j} x_i \right]_{x_0} .$$

Then let $\mathrm{Y} := \{y_1,\ldots,y_k\}$. Choose $z_v^i \in (-1/2, 1/2]$ so that the vector

$$\mathrm{z}_i := p_i/2\left(\left[P_\gamma(2/p_i)\right]_2 \otimes \left[P_\gamma(2/p_i)\right]_2\right) + \left(z_v^i\right)_{1\le v\le\gamma^2}$$

is to be an integer vector for $i = 1,\ldots,k$. Then choose $g_u \leftarrow D_{\gamma,\rho}(p_1,\ldots,p_k)$ ($1 \le u \le \gamma^2$).

Let $\mathbf{y} := (g_u)_{1\le u\le\gamma^2} + \mathrm{CRT}_{p_1,\ldots,p_k}(\mathbf{z}_1,\ldots,\mathbf{z}_k)$, where g_u is smaller than x_0. The public key is $pk := \{\mathrm{X}, \mathrm{Y}, \mathbf{y}\}$.

Encrypt $\left(pk, \mathrm{m} \in \{0,1\}^k\right)$ Choose a random subset S of $\{1,\ldots,\tau\}$ and output $c := \left[\sum_{j\in\mathrm{S}} x_j + \sum_{i=1}^k m_i y_i\right]_{x_0}$.

Decrypt (sk, c) Output $\mathbf{m} = (m_1,\ldots,m_k) := ([2c/p_1] \bmod 2, \ldots, [2c/p_k] \bmod 2)$.

Evaluate $(pk, C, c_1,\ldots,c_t)$ Given the binary circuit C with t inputs, and ciphertexts $c_1,\ldots,c_t$, we apply (addition and multiplication gates of) C to $c_1,\ldots,c_t$ as follows:

$$\mathrm{Add}(c_1, c_2, pk) := [c_1 + c_2]_{x_0},$$

$$\mathrm{Mult}(c_1, c_2, pk) := \left[\left\langle BD_\gamma(c_1) \otimes BD_\gamma(c_2), \mathrm{y}\right\rangle\right]_{x_0} .$$

Then it returns the resulting integer.

3.2 Correctness

Lemma 1 (Encryption noise). *Let* $sk, pk \leftarrow \mathrm{KeyGen}(\lambda, \rho, \eta, \gamma, \tau, k)$ *and* c *be a ciphertext of plaintext* $\mathbf{m} = (m_1,\ldots,m_k)$, $m_i \in \{0,1\}$ *for* $i = 1,\ldots,k$. *Then* $c = p_i Q_i + R_i + m_i(p_i+1)/2$ *for some* $Q_i \in \mathbf{Z}$ *and* $R_i \in \mathbf{Z}$ *with* $|R_i| \le 2\tau(k+1)(2^\rho - 1)$.

Proof. $c = \left[\sum_{j\in\mathrm{S}} x_j + \sum_{l=1}^k m_l y_l\right]_{x_0} = \left[\sum_{l=1}^k m_l \left[\mathrm{CRT}_{p_1,\ldots,p_k}\left(0,\ldots,\frac{p_l+1}{2},\ldots,0\right) + \sum_{t\in\mathrm{S}_l} x_t\right]_{x_0} + \sum_{j\in\mathrm{S}} x_j\right]_{x_0}$

$$= \left[\sum_{l=1}^k m_l\left(\mathrm{CRT}_{p_1,\ldots,p_k}\left(0,\ldots,\frac{p_l+1}{2},\ldots,0\right) + \sum_{t\in\mathrm{S}_l} x_t\right) + \sum_{j\in\mathrm{S}} x_j\right]_{x_0}$$

$$= \left[\sum_{l=1}^k m_l\left(\mathrm{CRT}_{p_1,\ldots,p_k}\left(0,\ldots,\frac{p_l+1}{2},\ldots,0\right)\right) + \sum_{l=1}^k m_l\left(\sum_{t\in\mathrm{S}_l} x_t\right) + \sum_{j\in\mathrm{S}} x_j\right]_{x_0}$$

The above expression is equal to the following one for some $F \in \mathbf{Z}$ and $G \in \mathbf{Z}$ with $G \le k\tau + \tau = \tau(k+1)$.

$$\mathrm{CRT}_{p_1,\ldots,p_k}\left(m_1\frac{p_1+1}{2},\ldots,m_l\frac{p_l+1}{2},\ldots,m_k\frac{p_k+1}{2}\right) + F\prod p_l + \sum_{l=1}^k m_l\left(\sum_{t\in\mathrm{S}_l} x_t\right) + \sum_{j\in\mathrm{S}} x_j - Gx_0 .$$

On the other hand,

$$x_j = p_i q_{ji} + r_{ji} \text{ for some } q_{ji} \in \mathbf{Z},\ r_{ji} \in \mathbf{Z} \cap \left(-2^\rho, 2^\rho\right),$$

because of $x_j \leftarrow D_{\gamma,\rho}(p_1,\ldots,p_k)$. So

$$c \equiv m_i \frac{p_i+1}{2} + \sum_{l=1}^{k} m_i \left(\sum_{t \in S_l} r_{ti} \right) + \sum\nolimits_{j \in S} r_{ji} - Gr_{0i} \equiv R_i + m_i \frac{p_i+1}{2} \quad \left(\bmod\ p_i\right).$$

for $R_i := \sum_{l=1}^{k} m_i \left(\sum_{t \in S_l} r_t \right) + \sum\nolimits_{j \in S} r_j - Gr_0$. Therefore $c = p_i Q_i + R_i + m_i \frac{p_i+1}{2}$ for some $Q_i \in \mathbf{Z}$.

To find upper bound of R_i,

$$\left|R_i\right| = \left| \sum_{l=1}^{k} m_i \left(\sum_{t \in S_l} r_t \right) + \sum\nolimits_{j \in S} r_j - Gr_0 \right| \le \left| \sum_{l=1}^{k} m_i \left(\sum_{t \in S_l} r_t \right) + \sum\nolimits_{j \in S} r_j \right| + \left|Gr_0\right| \le 2\tau(k+1)\left(2^{\rho}-1\right) \qquad \square$$

Lemma 2 (Decryption noise). *Let* $sk = \{p_1, \ldots, p_k\}$ *be a secret key. For given vector* $(m_1, \ldots, m_k)$ ($m_i \in \{0,1\}$) *and an integer* $c = p_i Q_i + R_i + m_i (p_i + 1)/2$, *if* $|R_i| < p_i/4 - 1/2$ *then* $\mathrm{Dec}(sk, c) = (m_1, \ldots, m_k)$. $i = 1, \ldots, k$.

Proof. We have

$$\left[\frac{2c}{p_i} \right] = 2Q_i + m_i + \left[\frac{2R_i + m_i}{p_i} \right].$$

Therefore, if

$$\left|R_i\right| < \frac{p_i}{4} - \frac{1}{2},$$

then

$$\left| \frac{2R_i + m_i}{p_i} \right| < \frac{1}{2}.$$

Therefore

$$\left[\frac{2R_i + m_i}{p_i} \right] = 0.$$

That is,

$$\left[\frac{2c}{p_i} \right] \bmod 2 = m_i. \qquad \square$$

Theorem 1 (Correctness). *Let* $sk, pk \leftarrow \mathrm{KeyGen}(\lambda, \rho, \eta, \gamma, \tau, k)$ *and let* $c = \mathrm{Enc}(pk, \mathbf{m})$ *denote the ciphertext of* $\mathbf{m} = (m_1, \ldots, m_k)$, ($m_i \in \{0,1\}$). *Then we have* $\mathbf{m} = \mathrm{Dec}(pk, c)$ *when* $\eta - \rho > \log(\tau(k+1)) + 4$.

Proof. Assume $\eta - \rho > \log(\tau(k+1)) + 4$. Then

$$\eta - \rho > \log(\tau(k+1)) + 4 \Leftrightarrow 2^{\eta-\rho} > 2^{\log(\tau(k+1))+4} = 16\tau(k+1) \Leftrightarrow \frac{2^{\eta}}{8} > 2^{\rho} 2\tau(k+1)$$

$$\Leftrightarrow \frac{2^{\eta-1}}{4} > 2^{\rho} 2\tau(k+1) \Leftrightarrow \frac{2^{\eta-1}}{4} - \frac{1}{2} > 2\tau(k+1)2^{\rho} - \frac{1}{2}.$$

On the other hand, since

$$2\tau(k+1)2^{\rho} - \frac{1}{2} > 2\tau(k+1)\left(2^{\rho}-1\right),$$

we have

$$\frac{2^{\eta-1}}{4} - \frac{1}{2} > 2\tau(k+1)\left(2^{\rho}-1\right).$$

Since p_i is a η-bit integer, $p_i > 2^{\eta-1}$ and then we also have

$$2\tau(k+1)\left(2^{\rho}-1\right) < \frac{p_i}{4} - \frac{1}{2}.$$

From Lemma 1, for some $Q_i \in \mathbf{Z}$ and some $R_i \in \mathbf{Z}$ with $\left|R_i\right| \le 2\tau(k+1)\left(2^{\rho}-1\right)$,

$$c = p_i Q_i + R_i + m_i \frac{p_i + 1}{2}$$

where $i = 1, ..., k$. Accordingly

$$|R_i| \le 2\tau(k+1)(2^{\rho} - 1) < \frac{p_i}{4} - \frac{1}{2}.$$

Therefore, from Lemma 2, $\mathrm{Dec}(sk, c) = \mathbf{m}$. □

3.3 Security

Lemma 3 (Leftover Hash Lemma) [8]. *The statistical distance of the uniform distribution* $\mathrm{U}(\mathbf{Z}_{x_0}^{\tau+1})$ *and the distribution*

$$\left\{ (x_1, ..., x_\tau, \left[\sum_{i=1}^{\tau} s_i x_i\right]_{x_0}) \middle| x'_1, ..., x'_\tau \leftarrow \mathrm{Z}_{x_0},\ s_1, ..., s_\tau \leftarrow \{0,1\} \right\}$$

is less than $\frac{1}{2}\sqrt{x_0 / 2^{\tau}}$.

Theorem 2 (Security). *Our Batch FHE scheme is CPA-secure under the assumption of hardness of* $(\rho, \eta, \gamma) - k -$ *AGCD problem.*

Proof. From the main assumption, the public key pk and the “pseudo” public key $pk' = \{\{x'_0, ..., x'_\tau\}, \{y'_1, ..., y'_k\}\}$, which was made from uniformly random selection, are computationally indistinguishable.

From the fact that $\tau \ge \gamma + 2\lambda + 2$ and Lemma 3, the probability distance between distribution

$$\left\{ (x'_1, ..., x'_\tau, \left[\sum_{i=1}^{\tau} s_i x'_i\right]_{x_0}) \middle| x'_1, ..., x'_\tau \leftarrow \mathrm{Z}_{x_0}, \mathrm{S} \leftarrow 2^{\{1, ... \tau\}} \right\}$$

and uniform distribution $\mathrm{U}(\mathbf{Z}_{x_0}^{\tau+1})$ are less than $2^{-\lambda}$. Thus we can conclude that the probability for the attacker to precisely distinguish the actual ciphertext from uniformly and randomly selected integer is less than $2^{-\lambda}$. □

4 Batch Leveled Homomorphic Encryption scheme

Definition 3 ($L-$homomorphic scheme). *Let* $(pk, sk, evk) \leftarrow \mathrm{KeyGen}(\lambda)$. *A scheme is called* $L-$*homomorphic scheme if for any binary integer circuit* C *that has the circuit depth* L *and* l *-inputs, it holds that* $\mathrm{Dec}(sk, \mathrm{Eval}(pk, C, (c_1, ..., c_l))) = C(\mathbf{m}_1, ..., \mathbf{m}_l)$ *with a probability greater than* $1 - \lambda^{-\omega(1)}$ *for the plaintexts* $\mathbf{m}_i$ *and the corresponding ciphertexts* $c_i = \mathrm{Enc}(pk, \mathbf{m}_i)$ $(1 \le i \le l)$.

Lemma 4 (Addition noise). *For* $b = 1,2$, *let* $c_b = \mathrm{Enc}(pk, \mathbf{m}_b)$ *denote the ciphertexts of* $\mathbf{m}_b = (m_{b1}, ..., m_{bk})$. *For* $i = 1, ..., k$, *if* $c_b = p_i q_{bi} + r_{bi} + m_{bi}(p_i + 1)/2$ *then*

$$\mathrm{Add}(c_1, c_2, pk) = p_i Q_i + R_i + [m_{1i} + m_{2i}]_2 (p_i + 1)/2$$

for some $Q_i \in \mathbf{Z}$ *and* $R_i \in \mathbf{Z}$ *with* $|R_i| \le |r_{1i} + r_{2i}| + 2^{\rho}$.

Proof. According to the definition of “Addition” operation, $\mathrm{Add}(c_1, c_2, pk) = [c_1 + c_2]_{x_0}$.

$$-\frac{x_0}{2} < c_1, c_2 < \frac{x_0}{2} \Rightarrow x_0 < c_1 + c_2 < x_0.$$

Therefore, there exist some integer $\delta \in \{-1,0,1\}$ such that $[c_1 + c_2]_{x_0} = c_1 + c_2 - \delta x_0$.

On the other hand, $x_0 = p_i Q_{0i} + R_{0i}$ for some $Q_{0i} \in \mathbf{Z}$ and $R_{0i} \in \mathbf{Z} \cap (-2^{\rho}, 2^{\rho})$, because of $x_0 \leftarrow D_{\gamma,\rho}(p_1, ..., p_k)$.

Then $c_1 + c_2 - \delta x_0 = p_i q_{1i} + p_i q_{2i} + r_{1i} + r_{2i} + (m_{1i} + m_{2i})\frac{p_i + 1}{2} - \delta(p_i Q_{0i} + R_{0i})$.

We know the difference between $(m_{1i} + m_{2i})$ and $[m_{1i} + m_{2i}]_2$ is only 2 when $m_{1i} = m_{2i} = 1$, otherwise 0. If $m_{1i} = m_{2i} = 1$, then

$$[m_{1i} + m_{2i}]_2 \frac{p_i + 1}{2} = 0,$$

$$(m_{1i} + m_{2i})\frac{p_i + 1}{2} = 2\frac{p_i + 1}{2} = p_i + 1.$$

Therefore, there is some integer $\delta' \in \{0,1\}$ such that

$$p_i q_{1i} + p_i q_{2i} + r_{1i} + r_{2i} + (m_{1i} + m_{2i})\frac{p_i + 1}{2} - \delta(p_i Q_{0i} + R_{0i}) =$$

$$= p_i q_{1i} + p_i q_{2i} + r_{1i} + r_{2i} + [m_{1i} + m_{2i}]_2 \frac{p_i + 1}{2} - \delta(p_i Q_{0i} + R_{0i}) + \delta'(p_i + 1).$$

And then,

$$\mathrm{Add}(\mathrm{c}_1, c_2, pk) \equiv \left(p_i q_{1i} + p_i q_{2i} + r_{1i} + r_{2i} + [m_{1i} + m_{2i}]_2 \frac{p_i + 1}{2} - \delta(p_i Q_{0i} + R_{0i}) + \delta'(p_i + 1) \right) =$$

$$\equiv \left(r_{1i} + r_{2i} + [m_{1i} + m_{2i}]_2 \frac{p_i + 1}{2} - \delta R_{0i} + \delta' \right) \pmod{p_i}.$$

Therefore,

$$\mathrm{Add}(\mathrm{c}_1, c_2, pk) \equiv \left(R_i + [m_{1i} + m_{2i}]_2 \frac{p_i + 1}{2} \right) \pmod{p_i} \text{ for } R_i := r_{1i} + r_{2i} - \delta R_{0i} + \delta'.$$

From this, we conclude that

$$\mathrm{Add}(\mathrm{c}_1, c_2, pk) = p_i Q_i + R_i + [m_{1i} + m_{2i}]_2 \frac{p_i + 1}{2} \text{ for some } Q_i \in \mathbf{Z}.$$

To find upper bound of R_i,

$$|R_i| = |r_{1i} + r_{2i} - \delta R_{0i} + \delta'| \le |r_{1i} + r_{2i}| + |-\delta R_{0i} + \delta'| \le |r_{1i} + r_{2i}| + 2^{\rho}.$$ □

Lemma 5. *Let* p *be* η*-bit odd prime integer, and* $c = pq + r + m(p+1)/2 \in \mathrm{Z} \cap [0, 2^{\gamma})$. *Then*

$$\langle BD_\gamma(c), [P_\gamma(2/p)]_2 \rangle = 2a + m + \varepsilon$$

for some $a \in \mathbf{Z}$ *with* $|a| < (\gamma - \eta + 4)/2$ *and some* $\varepsilon \in \mathbf{R}$ *with* $|\varepsilon| \le (2|r| + 1)/p$.

Proof. For given c,

$$\frac{2c}{p} = 2q + m + \frac{2r + m}{p}.$$

If

$$\varepsilon := \frac{2r + m}{p},$$

then

$$|\varepsilon| \le \frac{2|r| + 1}{p}, \text{ and } \frac{2c}{p} - (m + \varepsilon) \equiv 0 \pmod{2}.$$

On the other hand,

$$\langle BD_\gamma(c), [P_\gamma(2/p)]_2 \rangle - \langle BD_\gamma(c), P_\gamma(2/p) \rangle \equiv 0 \pmod{2}.$$

Since $\langle BD_\gamma(c), P_\gamma(2/p) \rangle = \frac{2c}{p}$,

$$\left\langle BD_\gamma(c), \left[P_\gamma(2/p)\right]_2\right\rangle - (m+\varepsilon) \equiv 0 \pmod 2.$$

Therefore, there is some integer $a \in \mathbf{Z}$ such that

$$\left\langle BD_\gamma(c), \left[P_\gamma(2/p)\right]_2\right\rangle = 2a + (m+\varepsilon).$$

Since p is η-bit odd prime integer,

$$\frac{2}{p} + \frac{2^2}{p} + \ldots + \frac{2^{\eta-2}}{p} = \frac{2\left(2^{\eta-2}-1\right)}{p} < 1,$$

and then

$$\left\langle BD_\gamma(c), \left[P_\gamma(2/p)\right]_2\right\rangle \le \sum_{i=0}^{\gamma-1}\left|\left[\frac{2^{i+1}}{p}\right]_2\right| = \sum_{i=0}^{\eta-3}\left|\left[\frac{2^{i+1}}{p}\right]_2\right| + \sum_{i=\eta-2}^{\gamma-1}\left|\left[\frac{2^{i+1}}{p}\right]_2\right| < \gamma - \eta + 3.$$

Therefore, $2a + m + \varepsilon < \gamma - \eta + 3$, and the upper bound of a is $|a| < (\gamma - \eta + 4)/2$. □

Lemma 6 (Multiplication noise). *For* $b = 1,2$, *let* $c_b = \mathrm{Enc}(pk, \mathbf{m}_b)$ *denote ciphertexts of* $\mathbf{m}_b = (m_{b1},\ldots,m_{bk})$. *For* $i = 1,\ldots,k$, *if* $c_b = p_i q_{bi} + r_{bi} + m_{bi}(p_i+1)/2$ *then*

$$\mathrm{Mult}(c_1, c_2, pk) = p_i Q_i + R_i + m_{1i}m_{2i}(p_i+1)/2$$

for some $Q_i \in \mathbf{Z}$, *and* $R_i \in \mathbf{Z}$ *with* $|R_i| \le \gamma^2 2^{\rho+1} + (\gamma - \eta + 6)(|r_{1i}| + |r_{2i}| + 1)$.

Proof. We have

$$\left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \mathbf{y}\right\rangle = \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \left((g_u)_{1\le u\le\gamma^2} + \mathrm{CRT}_{p_1,\ldots,p_k}(\mathrm{z}_1,\ldots,\mathrm{z}_k)\right)\right\rangle$$

$$= \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), (g_u)_{1\le u\le\gamma^2}\right\rangle + \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \mathrm{CRT}_{p_1,\ldots,p_k}(\mathbf{z}_1,\ldots,\mathbf{z}_k)\right\rangle.$$

Let

$$A := \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), (g_u)_{1\le u\le\gamma^2}\right\rangle. \quad B := \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \mathrm{CRT}_{p_1,\ldots,p_k}(\mathbf{z}_1,\ldots,\mathbf{z}_k)\right\rangle.$$

Then

$$B = \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \mathrm{CRT}_{p_1,\ldots,p_k}(\mathbf{z}_1,\ldots,\mathbf{z}_k)\right\rangle \le \gamma^2 T < x_0,$$

for any component of the γ^2-dimensional integer vector $\mathrm{CRT}_{p_1,\ldots,p_k}(\mathbf{z}_1,\ldots,\mathbf{z}_k)$ is less than T.

Moreover, since $g_u < x_0$, we have

$$A = \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), (g_u)_{1\le u\le\gamma^2}\right\rangle < \gamma^2 x_0,$$

which implies that there exists an integer $G \in [0, \gamma^2]$ such that

$$\mathrm{Mult}(c_1, c_2, pk) = \left[\left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \mathrm{y}\right\rangle\right]_{x_0} = A + B - Gx_0,$$

and

$$\mathrm{Mult}(c_1, c_2, pk) \equiv (A + B - Gx_0) \equiv \left((A - Gx_0) \bmod p_i + B \bmod p_i\right) \pmod{p_i}.$$

For $i = 1,\ldots,k$, the vector

$$\mathbf{z}_i = \frac{p_i}{2}\left(\left[P_\gamma\left(\frac{2}{p_i}\right)\right]_2 \otimes \left[P_\gamma\left(\frac{2}{p_i}\right)\right]_2\right) + \left(z_v^i\right)_{1\le v\le\gamma^2}$$

is an integer vector, and from Chinese Remainder Theorem,

$$\mathrm{CRT}_{p_1,\ldots,p_k}(\mathbf{z}_1,\ldots,\mathbf{z}_k) = \left[\sum_{i=1}^{k}\mathbf{z}_i\,\hat{p}_i\left(\hat{p}_i^{-1} \bmod p_i\right)\right]_T.$$

Thus, we have

$$B = \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \left(\sum_{i=1}^{k}\left(\frac{p_i}{2}\left(\left[P_\gamma\left(\frac{2}{p_i}\right)\right]_2 \otimes \left[P_\gamma\left(\frac{2}{p_i}\right)\right]_2\right) + \left(z_v^i\right)_{1\le v\le\gamma^2}\right)\hat{p}_i\left(\hat{p}_i^{-1} \bmod p_i\right)\right) \bmod T \right\rangle .$$

Then, there exists a γ^2-dimensional integer vector such that

$$\left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \sum_{i=1}^{k}\left(\frac{p_i}{2}\left(\left[P_\gamma\left(\frac{2}{p_i}\right)\right]_2 \otimes \left[P_\gamma\left(\frac{2}{p_i}\right)\right]_2\right) + \left(z_v^i\right)_{1\le v\le\gamma^2}\right)\hat{p}_i\left(\hat{p}_i^{-1} \bmod p_i\right) - T\mathbf{F} \right\rangle =$$

$$= \sum_{i=1}^{k}\left(\frac{p_i}{2}\left\langle BD_\gamma(c_1), \left[P_\gamma\left(\frac{2}{p_i}\right)\right]_2\right\rangle \cdot \left\langle BD_\gamma(c_2), \left[P_\gamma\left(\frac{2}{p_i}\right)\right]_2\right\rangle + \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \left(z_v^i\right)_{1\le v\le\gamma^2}\right\rangle\right)\hat{p}_i\left(\hat{p}_i^{-1} \bmod p_i\right) -$$

$$- \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), T\mathbf{F}\right\rangle .$$

From Lemma 5, for $i = 1,\ldots,k$, there exist $a_{1i}, a_{2i} \in \mathbf{Z}$ and $\varepsilon_{1i}, \varepsilon_{2i} \in \mathbf{R}$, we can continue as follows.

$$= \sum_{i=1}^{k}\left(\frac{p_i}{2}(m_{1i}+\varepsilon_{1i}+2a_{1i})(m_{2i}+\varepsilon_{2i}+2a_{2i}) + \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \left(z_v^i\right)_{1\le v\le\gamma^2}\right\rangle\right)\hat{p}_i\left(\hat{p}_i^{-1} \bmod p_i\right) -$$

$$- \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), T\mathbf{F}\right\rangle ,$$

where

$$|a_{1i}|, |a_{2i}| \le (\gamma - \eta + 4)/2,\ |\varepsilon_{1i}| \le \frac{(2|r_{1i}|+1)}{p_i}, \text{ and } |\varepsilon_{2i}| \le \frac{(2|r_{2i}|+1)}{p_i}.$$

Let J denote a set of all nonzero component of the γ^2 – dimensional integer vector $BD_\gamma(c_1)\otimes BD_\gamma(c_2)$. Then

$$B \equiv \left\{\sum_{j=1}^{k}\left(\frac{p_j}{2}(m_{1j}+\varepsilon_{1j}+2a_{1j})(m_{2j}+\varepsilon_{2j}+2a_{2j}) + \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \left(z_v^j\right)_{1\le v\le\gamma^2}\right\rangle\right)\hat{p}_j\left(\hat{p}_j^{-1} \bmod p_j\right) -\right.$$

$$\left. - \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), T\mathrm{F}\right\rangle\right\} \equiv \left(\frac{p_i}{2}(m_{1i}+\varepsilon_{1i}+2a_{1i})(m_{2i}+\varepsilon_{2i}+2a_{2i}) + \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2), \left(z_v^i\right)_{1\le v\le\gamma^2}\right\rangle\right)$$

$$\equiv \left(\frac{p_i}{2}(m_{1i}+\varepsilon_{1i}+2a_{1i})(m_{2i}+\varepsilon_{2i}+2a_{2i}) + \sum_{v\in \mathrm{J}} z_v^i\right) \pmod{p_i}$$

On the other hand,

$$\frac{p_i}{2}\left((m_{1i}+2a_{1i})(m_{2i}+2a_{2i}) - m_{1i}m_{2i}\right)$$

is multiple of p_i. Thus,

$$\frac{p_i}{2}(m_{1i}+\varepsilon_{1i}+2a_{1i})(m_{2i}+\varepsilon_{2i}+2a_{2i}) + \sum_{v\in \mathrm{J}} z_v^i \equiv$$

$$\equiv \frac{p_i}{2}\left(\varepsilon_{2i}(m_{1i}+2a_{2i}) + \varepsilon_{1i}(m_{2i}+2a_{1i}) + \varepsilon_{1i}\varepsilon_{2i} + m_{1i}m_{2i}\right) + \sum_{v\in \mathrm{J}} z_v^i \equiv$$

$$\equiv \left(\frac{p_i+1}{2}m_{1i}m_{2i} + \left(\frac{p_i}{2}\left(\varepsilon_{2i}(m_{1i}+2a_{2i}) + \varepsilon_{1i}(m_{2i}+2a_{1i}) + \varepsilon_{1i}\varepsilon_{2i}\right) - \frac{1}{2}m_{1i}m_{2i}\right) + \sum_{v\in \mathrm{J}} z_v^i\right) \pmod{p_i},$$

which implies that

$$B \equiv \left(\frac{p_i+1}{2}m_{1i}m_{2i} + \frac{p_i}{2}\left(\varepsilon_{2i}(m_{1i}+2a_{2i}) + \varepsilon_{1i}(m_{2i}+2a_{1i}) + \varepsilon_{1i}\varepsilon_{2i}\right) - \frac{1}{2}m_{1i}m_{2i} + \sum_{v\in \mathrm{J}} z_v^i\right) \pmod{p_i}.$$

For $y_u \leftarrow D_{\gamma,\rho}(p_1,\ldots,p_k)$, there exist integers q_{ui} and $r_{ui} \in \left(-2^\rho, 2^\rho\right)$ such that $y_u = p_i q_{ui} + r_{ui}$ and similarly, there exists integers Q_{0i} and $R_{0i} \in \left(-2^\rho, 2^\rho\right)$ such that $x_0 = p_i Q_{0i} + R_{0i}$.

In addition, we have,

$$A-Gx_0 \equiv \left\langle BD_\gamma(c_1)\otimes BD_\gamma(c_2),(y_u)_{1\le u\le \gamma^2}\right\rangle - Gx_0 \equiv \left(\sum_{u\in \mathrm{J}} y_u\right)-Gx_0 \equiv \left(\sum_{u\in \mathrm{J}} r_{ui}\right)-GR_{0i} \pmod{p_i}.$$

Combining the above two results, we have,

$$\mathrm{Mult}\,(c_1,c_2,pk)\equiv$$

$$\equiv \frac{p_i+1}{2}m_{1i}m_{2i}+\left(\frac{p_i}{2}\left(\varepsilon_{2i}(m_{1i}+2a_{2i})+\varepsilon_{1i}(m_{2i}+2a_{1i})+\varepsilon_{1i}\varepsilon_{2i}\right)-\frac{1}{2}m_{1i}m_{2i}+\sum_{v\in \mathrm{J}} z_v^i+\sum_{u\in \mathrm{J}} r_{ui}-GR_{0i}\right) \pmod{p_i}.$$

Let

$$R_i := \frac{p_i}{2}\left(\varepsilon_{2i}(m_{1i}+2a_{2i})+\varepsilon_{1i}(m_{2i}+2a_{1i})+\varepsilon_{1i}\varepsilon_{2i}\right)-\frac{1}{2}m_{1i}m_{2i}+\sum_{v\in \mathrm{J}} z_v^i+\sum_{u\in \mathrm{J}} r_{ui}-GR_{0i},$$

then, we have

$$\mathrm{Mult}(c_1,c_2,pk)\equiv \frac{p_i+1}{2}m_{1i}m_{2i}+R_i \pmod{p_i},$$

which implies that there exists an integer Q_i such that $\mathrm{Mult}(c_1,c_2,pk)=p_iQ_i+R_i+\frac{p_i+1}{2}m_{1i}m_{2i}$.

Now, let’s find the upper bound of R_i.

$$\sum_{v\in \mathrm{J}} z_v^i+\sum_{u\in \mathrm{J}} r_{ui}\le 2^\rho|\mathrm{J}|\le \gamma^2 2^\rho,\ GR_{0i}\le \gamma^2\left(2^\rho-1\right)\Rightarrow \left|\sum_{v\in \mathrm{J}} z_v^i+\sum_{u\in \mathrm{J}} r_{ui}-\frac{1}{2}m_{1i}m_{2i}-GR_{0i}\right|\le \gamma^2 2^{\rho+1}.$$

$$\frac{p_i}{2}\left(\varepsilon_{2i}(m_{1i}+2a_{2i})+\varepsilon_{1i}(m_{2i}+2a_{1i})+\varepsilon_{1i}\varepsilon_{2i}\right)=\frac{p_i}{2}\left(\varepsilon_{2i}\left(m_{1i}+\frac{\varepsilon_{1i}}{2}+2a_{2i}\right)+\varepsilon_{1i}\left(m_{2i}+\frac{\varepsilon_{2i}}{2}+2a_{1i}\right)\right)<$$

$$<\frac{p_i}{2}\left((\gamma-\eta+6)(\varepsilon_{2i}+\varepsilon_{1i})\right)=\frac{p_i}{2}\left((\gamma-\eta+6)\left(\frac{(2|r_{1i}|+1)}{p_i}+\frac{(2|r_{2i}|+1)}{p_i}\right)\right)=(\gamma-\eta+6)(|r_{1i}|+|r_{1i}|+1).$$

Therefore,

$$|R_i|\le \gamma^2 2^{\rho+1}+(\gamma-\eta+6)(|r_{1i}|+|r_{2i}|+1).$$ □

Theorem 3. *Our SHE scheme is* $L-$*homomorphic if the following inequality holds:*

$$\eta-\rho\ge L(1+\log(\gamma-\eta+6))+4+\log\left(\frac{\gamma^2}{2(\gamma-\eta+6)-1}+\tau(k+1)\right)$$

Proof. For each $i\in[1,k]$ and $b\in[1,L]$, let c_b be a ciphertext with $c_b=p_iq_{bi}+r_{bi}+m_{bi}\frac{p_i+1}{2}$ after the evaluation of the $b-$th level gates. Let R_b be a bound of r_{bi}.

From Lemma 1, $R_0=2\tau(k+1)(2^\rho-1)$.

From Lemma 4 and Lemma 6, the following relationship holds between R_{j+1} and R_j.

$$R_{j+1}\le \max\left\{\gamma^2 2^{\rho+1}+(\gamma-\eta+6)(2R_j+1), 2R_j+2^\rho\right\}=\gamma^2 2^{\rho+1}+(\gamma-\eta+6)(2R_j+1).$$

The recurrence of the type $R_{j+1}=\mathrm{A}R_j+\mathrm{B}$ has the solution

$$R_{j+1}=\mathrm{A}^{j+1}R_0+\sum_{i=0}^{j}\mathrm{A}^i\mathrm{B}=\mathrm{A}^{j+1}R_0+\mathrm{B}\frac{\mathrm{A}^{j+1}-1}{\mathrm{A}-1}.$$

Therefore, we have

$$R_L\le 2^L(\gamma-\eta+6)^LR_0+\left(\gamma^2 2^{\rho+1}+(\gamma-\eta+6)\right)\left(\frac{2^L(\gamma-\eta+6)^L-1}{2(\gamma-\eta+6)-1}\right).$$

Replacing with $R_0=2\tau(k+1)(2^\rho-1)$,

$$R_L \le 2^L(\gamma-\eta+6)^L\left(2\tau(k+1)(2^\rho-1)+\frac{(\gamma^2 2^{\rho+1}+(\gamma-\eta+6))}{2(\gamma-\eta+6)-1}\right).$$

From Lemma 2, this scheme is $L-$homomorphic if $R_L < \frac{p_i}{4}-\frac{1}{2}$.

From our hypothesis, we have

$$\eta-\rho \ge L(1+\log(\gamma-\eta+6))+4+\log\left(\frac{\gamma^2}{2(\gamma-\eta+6)-1}+\tau(k+1)\right)\Rightarrow$$

$$\Rightarrow 2^L(\gamma-\eta+6)^L 2^{\rho+1}\left(\tau(k+1)+\frac{\gamma^2}{2(\gamma-\eta+6)-1}\right)<\frac{2^{\eta-1}}{4}\Rightarrow$$

$$\Rightarrow 2^L(\gamma-\eta+6)^L\left(2\tau(k+1)(2^\rho-1)+\frac{(\gamma^2 2^{\rho+1}+(\gamma-\eta+6))}{2(\gamma-\eta+6)-1}\right)<\frac{2^{\eta-1}}{4}-\frac{1}{2}.$$

$p_i > 2^{\eta-1}$ since p_i is an $\eta-$bit integer. Thus, we have

$$2^L(\gamma-\eta+6)^L\left(2\tau(k+1)(2^\rho-1)+\frac{(\gamma^2 2^{\rho+1}+(\gamma-\eta+6))}{2(\gamma-\eta+6)-1}\right)<\frac{p_i}{4}-\frac{1}{2},$$

which implies that

$$R_L \le 2^L(\gamma-\eta+6)^L\left(2\tau(k+1)(2^\rho-1)+\frac{(\gamma^2 2^{\rho+1}+(\gamma-\eta+6))}{2(\gamma-\eta+6)-1}\right)<\frac{p_i}{4}-\frac{1}{2}.$$

Therefore, we can conclude that it is $L-$homomorphic. □

References

[1] D. Benarroch, Z. Brakerski, and T. Lepoint: FHE Over the Integers: Decomposed and Batched in the Post-Quantum Regime. IACR Cryptology ePrint Archive, Report 2017/065 (2017)

[2] Z. Brakerski: Fully homomorphic encryption without modulus switching from classical GapSVP. In: R. Safavi-Naini, R. Canetti (Eds.) CRYPTO 2012. (LNCS 7417) pp. 868–886. Springer-Verlag (2012)

[3] Z. Brakerski, C. Gentry, S. Halevi: Packed ciphertexts in LWE-based homomorphic encryption. In: K. Kurosawa, G. Hanaoka (Eds.) Public-Key Cryptography-PKC 2013. (LNCS 7778) pp. 1–13. Springer-Verlag (2013)

[4] Z. Brakerski, V. Vaikuntanathan: Efficient fully homomorphic encryption from (standard) LWE. In Proc. of FOCS, pp. 97–106. IEEE Computer Society Press (2011)

[5] Z. Brakerski, V. Vaikuntanathan: Fully homomorphic encryption from Ring-LWE and security for key dependent messages. In: P. Rogaway (Ed.) CRYPTO 2011. (LNCS 6841) pp. 505–524. Springer-Verlag (2011)

[6] Z. Brakerski, V. Vaikuntanathan: Lattice-based FHE as secure as PKE. In: Proc. of ITCS, pp. 1–12. ACM Press (2014)

[7] J. H. Cheon, J. S. Coron, T. Lepoint, M. Tibouchi, and A. Yun: Batch fully homomorphic encryption over the integers. In: Thomas Johansson Phong Q. Nguyen (Ed.) Advances in Cryptology–EUROCRYPT 2013 (LNCS 7881), pp. 315–335. Springer-Verlag (2013)

[8] J. H. Cheon, D. Stehlè: Fully homomorphic encryption over the integers revisited. In: E. Oswald, M. Fischlin (Eds.) Advances in Cryptology–EUROCRYPT 2015 (LNCS 9056) pp. 513–536. Springer-Verlag (2015)

[9] J. S. Coron, T. Lepoint, M. Tibouchi: Scale-invariant fully homomorphic encryption over the integers. In: H. Krawczyk (Ed.) Public-Key Cryptography-PKC 2014 (LNCS 8383) pp. 311–328. Springer-Verlag (2014)

[10] C. Gentry: A fully homomorphic encryption scheme. PhD thesis, Stanford University (2009).

[11] C. Gentry: Fully homomorphic encryption using ideal lattices. In: M. Mitzenmacher (Ed.) Proceedings of the 41st Annual ACM Symposium on Theory of Computing. STOC 2009, pp. 169–178. ACM (2009)

[12] C. Gentry, S. Halevi: Implementing Gentry’s fully-homomorphic encryption scheme. In: K. G. Paterson (Ed.)

Advances in Cryptology–EUROCRYPT 2011 (LNCS 6632) pp. 129–148. Springer-Verlag (2011)

[13] C. Gentry, S. Halevi, N. P. Smart: Fully homomorphic encryption with polylog overhead. In: D. Pointcheval, T. Johansson (Eds.) Advances in Cryptology–EUROCRYPT 2012. (LNCS 7237) pp. 465–482. Springer-Verlag (2012)

[14] C. Gentry, S. Halevi, N. P. Smart: Homomorphic evaluation of the AES circuit. In: R. Safavi-Naini, R. Canetti (Eds.) CRYPTO 2012. (LNCS 7417) pp. 850–867. Springer-Verlag (2012)

[15] C. Gentry, A. Sahai, B. Waters: Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: R. Canetti, J. A. Garay (Eds.) CRYPTO 2013, Part I. (LNCS 8042) pp. 75–92. Springer-Verlag (2013)

[16] N. Howgrave-Graham: Approximate integer common divisors. In: J. H. Silverman (Ed.) CaLC 2001 (LNCS 2146) pp. 51–66. Springer-Verlag (2001)

[17] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. J. ACM, 56(6):1–40, 2009. Preliminary version in STOC 2005.

[18] R. L. Rivest, L. Adleman, and M. L. Dertouzos: On data banks and privacy homomorphisms. Foundations of Secure Computation, 4(11), pp. 169–180, (1978)

[19] N. P. Smart, F. Vercauteren: Fully homomorphic encryption with relatively small key and ciphertext sizes. In: P. Q. Nguyen, D. Pointcheval (Eds.) Public-Key Cryptography-PKC 2010. (LNCS 6056) pp. 420–443. Springer-Verlag (2010)

[20] D. Stehlѐ, R. Steinfeld: Faster fully homomorphic encryption. In: M. Abe (ed.) Advances in Cryptology–ASIACRYPT 2010. (LNCS 6477) pp. 377–394. Springer-Verlag (2010)

[21] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan: Fully homomorphic encryption over the integers. In: H. Gilbert (Ed.) Advances in Cryptology–EUROCRYPT 2010 (LNCS 6110), pp. 24–43. Springer-Verlag (2010)