Privacy Preserving Computation in Cloud Using Noise-Free Fully Homomorphic Encryption (FHE) Schemes*

Yongge Wang[1], Qutaibah m. Malluhi[2]

[1] Department of SIS, UNC Charlotte, USA.
[2] KINDI Center, Qatar University, Qatar.
yonwang@uncc.edu, qmalluhi@qu.edu.qa

Abstract. With the wide adoption of cloud computing paradigm, it is important to develop appropriate techniques to protect client data privacy in the cloud. Encryption is one of the major techniques that could be used to achieve this goal. However, data encryption at the rest alone is insufficient for secure cloud computation environments. Further efficient techniques for carrying out computation over encrypted data are also required. Fully homomorphic encryption (FHE) and garbled circuits are naturally used to process encrypted data without leaking any information about the data. However, existing FHE schemes are inefficient for processing large amount of data in cloud and garbled circuits are one time programs and cannot be reused. Based on quaternion/octonion algebra and Jordan algebra over finite rings $\mathbb{Z}_q$, this paper designs efficient fully homomorphic symmetric key encryption (FHE) schemes without bootstrapping (that is, noise-free FHE schemes) that are secure in the weak ciphertext-only security model assuming the hardness of solving multivariate quadratic equation systems and solving univariate high degree polynomial equation systems in $\mathbb{Z}_q$. The FHE scheme designed in this paper is sufficient for privacy preserving computation in cloud.

1 Introduction

Cloud computing techniques become pervasive and users begin to store their private encrypted data in cloud services. In order to take full advantage of the cloud computing paradigm, it is important to design efficient techniques to protect client data privacy in the cloud. From a first look, encryption at rest seems to be a feasible solution to address these challenges. But a truly optimal solution is still far from us since encryption is not a good or even an acceptable solution for cloud data storage. If encryption at rest is the only solution, then the functionality of cloud computing is limited to: encrypt data at the user's location, transmit encrypted data to the cloud, and then bring the data back to the user's location for decryption before being used locally. This is against one of the cloud computing paradigms "moving computation is cheaper than moving data". Indeed, in many scenarios, it is less expensive to store data locally than in the cloud. So using the

* The work reported in this paper is supported by Qatar Foundation Grants NPRP8-2158-1-423 and NPRP X-063-1-014.

cloud for data-storage without the capability of processing these data remotely may not be an economic approach.

This shows the importance of developing techniques for processing encrypted data at the cloud without downloading them to the local site. A natural solution is to use garbled computing techniques such as garbled circuits or fully homomorphic encryption schemes. That is, an adversary observing the computations of a garbled computation learns nothing about what it is doing, what data it is operating on (whether inputs or intermediate values), and the outputs it is producing. Yao [15] introduced the garbled circuit concept which allows computing a function f on an input x without leaking any information about the input x or the circuit used for the computation of $f(x)$. Since then, garbled circuit based protocols have been used in numerous places and it has become one of the fundamental components of secure multi-party computation protocols. However, there are two disadvantages in Yao's approach. Firstly, Yao's garbled circuit is not reusable. Secondly, using a garbled circuit to evaluate an algorithm on encrypted data takes the worst-case runtime of the algorithm on all inputs of the same length since Turing machines are simulated by circuits via unrolling loops to their worst-case runtime, and via considering all branches of a computation.

Gentry [6] proposed the first fully homomorphic encryption scheme (FHE) design using two phases: first design a somewhat-homomorphic encryption scheme and then use bootstrapping techniques to convert it to a fully homomorphic encryption scheme. Since Gentry's initial FHE design, the performance of FHE scheme has improved a lot though it is still impractical for cloud garbled computation applications. For example, the most efficient implementation (until 2016) takes 4 minutes to carry out a garbled AES encryption on a 128 bit input.

The main performance bottleneck for Gentry's approach is the "noise" reduction process since the homomorphic operations increase the noise in ciphertexts. After a homomorphic operation (e.g., a circuit gate evaluation) is performed on the ciphertexts, Gentry's [6] bootstrapping technique is used to refresh the ciphertexts by homomorphically computing the decryption function and bringing the noise of the ciphertexts back to acceptable levels. The bootstrapping operation accounts for the major performance cost in FHE implementations. The performance of FHE schemes would be significantly improved if one could design noise-free FHE schemes. Using quaternion/octonion/Jordan algebra based coding techniques, this paper introduces noise-free fully homomorphic symmetric key encryption schemes. The proposed FHE schemes are secure in the weak ciphertext-only security model with the assumption that it is computationally infeasible to solve multivariate quadratic equation systems and it is computationally infeasible to solve univariate high degree polynomial equation systems in the underlying rings $\mathbb{Z}_q$. The hardness assumption for the security is reasonable for large enough $\mathbb{Z}_q$ (e.g., $|\mathbb{Z}_q| \geq 2^{1000}$) since it is known that finding square roots modulo a composite number is equivalent to factoring. This fact has been used in the literature to show the security of Rabin cryptosystem. The weak ciphertext-only security model for FHE is sufficient for garbled cloud computation applications (e.g., outsourcing of private algorithm implementations) mentioned in the preceding paragraphs.

We conclude this section by introducing some notations. The schemes in this paper will be based on finite rings $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ with $q = p_1^{r_1} \cdots p_m^{r_m}$ for some primes

$p_1, \cdots, p_m$ and non-negative integers $r_1, \cdots, r_m$. Let $\mathbb{Z}_q^*$ denote of the set of invertible elements in $\mathbb{Z}_q$. Bold face letters such as $\mathbf{a}, \mathbf{b}, \mathbf{e}, \mathbf{f}, \mathbf{g}$ are used to denote row vectors over $\mathbb{Z}_q$. For a vector subset $V = \{\mathbf{a}_i : i \leq k-1\} \subset \mathbb{Z}_q^n$, the span$(V)$ of V is defined as all linear combinations of vectors in V.

2 Linearly decryptable encryption schemes

In the past few years, numerous works have been done to analyze the security and performance of FHE schemes (due to the space limit, we are unable to list these important works here). Brakerski [3] investigated the relationship between decryption circuit complexity and FHE scheme security. In particular, Brakerski showed that if a scheme can homomorphically evaluate the majority function, then its decryption cannot be weakly-learnable. A corollary of this result is that linearly decryptable FHE schemes cannot be secure in the CPA (chosen plaintext attacks) security model. In this paper, we show that linearly decryptable FHE schemes cannot be secure even in the ciphertext-only security model. With these impossibility results, one may wonder what kind of maximum security an FHE scheme with simple decryption circuit could achieve? By relaxing the definition of the ciphertext-only attacks to the weak ciphertext-only attacks, this paper is able to design efficient secure FHE schemes with linear decryption circuits.

Brakerski [3] called an encryption scheme to be linearly decryptable if the decryption circuit can be described as an inner product. We first formally define the Inner Product Encryption Scheme $\texttt{IPE} = (\texttt{IPE.Setup}, \texttt{IPE.Enc}, \texttt{IPE.Dec})$ over finite rings $\mathbb{Z}_q$. The definition remains the same for the IPE scheme over finite fields $\mathbb{F}_q$.

Setup $\texttt{IPE.Setup}(n, \kappa)$: For the given security parameter κ and the dimension $n \geq 3$, choose a finite ring $\mathbb{Z}_q$ and a random $\mathbf{k} = [k_0, \cdots, k_{n-1}] \in \mathbb{Z}_q^n$ such that $k_i \in \mathbb{Z}_q^*$ for at least one $i < n$. Let $\mathbf{k}$ be the private key.

Encryption IPE.Enc: For a message $m \in \mathbb{Z}_q$, select a random $\mathbf{c} \in \mathbb{Z}_q^n$ such that $m = \mathbf{c}\mathbf{k}^T$ where $\mathbf{c}\mathbf{k}^T$ is the inner product of $\mathbf{c}$ and $\mathbf{k}$. Let $\texttt{IPE.Enc}(\mathbf{k}, m) = \mathbf{c}$.

Decryption IPE.Dec: For a ciphertext $\mathbf{c}$, let $m = \texttt{IPE.Dec}(\mathbf{k}, \mathbf{c}) = \mathbf{k}\mathbf{c}^T$.

The definition of ciphertext-only security for an encryption scheme is closely related to the perfect secrecy definition for one-time pad encryption schemes. The commonly used security definition for one-time pad encryption scheme includes indistinguishability based IND-onetime and simulation based SIM-onetime security. We will use the indistinguishability based security definition for ciphertext-only security (COA).

Definition 1. *(COA model) Let* $\texttt{xx} = (\texttt{KeySetup}, \texttt{Enc}, \texttt{Dec})$ *be a symmetric key encryption scheme over a message space* $\mathcal{M}$*. For a pair of probabilistic polynomial time (PPT) algorithms* $A = (A_0, A_1)$*, define the following experiments:*

- A_0 *runs* $\texttt{key} \leftarrow \texttt{xx.KeySetup}(\kappa)$ *where* κ *is the security parameter.*
- A_0 *chooses* t *messages* $p_0, \cdots, p_{t-1}$ *according to the distribution of* $\mathcal{M}$ *and outputs* t *ciphertexts* $C_{p_0}, \cdots, C_{p_{t-1}}$ *by running* $C_{p_i} = \texttt{xx.Enc}(\texttt{key}, p_i)$.
- A_1 *selects* 2 *messages* $m_0, m_1 \in \mathcal{M}$ *and gives them to* A_0.
- A_0 *selects a random bit* $b \in \{0, 1\}$ *and outputs* $C_{m_b} = \texttt{xx.Enc}(\texttt{key}, m_b)$.
- A_1 *outputs a bit* b'.

The output of the above experiment is defined to be 1 if $b' = b$*, and* 0 *otherwise. We write* $\texttt{COA}^{(A_0, A_1)}(\kappa) = 1$ *if the output is* 1 *and in this case we say that* A_1 *succeeded.*

The encryption scheme $\mathtt{xx}$ *is said to be* (t, ε)*-secure in the ciphertext-only attack (COA) security model for* $\varepsilon = \mathtt{negl}(\kappa)$ *if for all PPT algorithms* $A = (A_0, A_1)$*, we have*

$$Prob[\mathtt{COA}^{(A_0,A_1)}(\kappa) = 1] \leq \frac{1}{2} + \varepsilon.$$

The following theorem shows that an IPE encryption scheme cannot be fully homomorphic and secure in the ciphertext-only security model at the same time.

Theorem 1. *Let* $\mathtt{xx} = (\mathtt{KeySetup}, \mathtt{Enc}, \mathtt{Dec})$ *be a fully homomorphic symmetric key encryption scheme over* $\mathbb{Z}_q$ *such that the decryption process* $\mathtt{xx.Dec}$ *is equivalent to* $\mathtt{IPE.Dec}$ *of dimension* n*. Then* $\mathtt{xx}$ *is not secure in the ciphertext-only security model.*

Proof. Let $\mathbf{k} \in \mathbb{Z}_q^n$ be the private key and $\mathtt{xx.Dec}(\mathbf{c}) = \mathbf{k}\mathbf{c}^T$ for ciphertexts $\mathbf{c} \in \mathbb{Z}_q^n$. Without loss of generality, we may assume that the messages selected by the PPT algorithm A_1 during the experiment is $m_0 = 0$ and $m_1 = 1$. Let $\mathbf{c}_b \in \mathbb{Z}_q^n$ be the ciphertext output by the algorithm A_0 during the experiment where $b = 0, 1$.

By using the multiplicative homomorphism property of $\mathtt{xx}$, the algorithm A_1 can calculate ciphertexts $\mathbf{c}_{b,i} \in \mathbb{Z}_q^n$ of $b^i = b$ for $i \geq 1$. It is straightforward that, for $d = n + 1$, the ciphertexts $\mathbf{c}_{b,1}, \ldots, \mathbf{c}_{b,d}$ are linearly dependent. In other words, there exist $a_1, \cdots, a_d \in \mathbb{Z}_q$ such that $a_1\mathbf{c}_{b,1} + a_2\mathbf{c}_{b,2} + \cdots + a_d\mathbf{c}_{b,d} = 0$. This implies that

$$a_1 b + a_2 b^2 + \cdots + a_d b^d = 0 \tag{1}$$

If $a_1 + \cdots + a_d = 0$, the algorithm A_1 outputs $b' = 1$. Otherwise, it outputs $b' = 0$. The algorithm A_1 may repeat the above process for ciphertexts $\mathbf{c}_{b,i+1}, \ldots, \mathbf{c}_{b,i+d}$ with different $i > 1$ to get more accurate prediction b' of the value b. Thus it can be shown that $b' = b$ with a non-negligible probability. The theorem is proved. □

One may wonder whether it is possible at all to design a linearly decryptable FHE scheme that is secure in some relaxed security model? Alternatively we may ask: what is the maximum security one can achieve with linearly decryptable FHE schemes? In next sections, we show that it is possible to design linearly decryptable FHE schemes that are secure in the following weak ciphertext-only security model (wCOA).

Definition 2. *(wCOA model) Let* $\mathtt{xx} = (\mathtt{KeySetup}, \mathtt{Enc}, \mathtt{Dec})$ *be a symmetric key encryption scheme over a message space* $\mathcal{M}$*. For a pair of PPT algorithms* $A = (A_0, A_1)$*, define the following experiments:*

- A_0 *runs* $\mathtt{key} \leftarrow \mathtt{xx.KeySetup}(\kappa)$ *where* κ *is the security parameter.*
- A_0 *chooses* t *messages* $p_0, \cdots, p_{t-1}$ *according to the distribution of* $\mathcal{M}$ *and outputs* t *ciphertexts* $C_{p_0}, \cdots, C_{p_{t-1}}$ *by running* $C_{p_i} = \mathtt{xx.Enc}(\mathtt{key}, p_i)$*.*
- A_1 *outputs a message* $m' \in \mathcal{M}$*.*

The output of the experiment is 1 if $m' \in \{p_0, \cdots, p_{t-1}\}$*, and* 0 *otherwise. We write* $\mathtt{wCOA}^{(A_0,A_1)}(\kappa) = 1$ *if the output is* 1 *and in this case we say that* A_1 *succeeded. The scheme* $\mathtt{xx}$ *is said to be* (t, ε)*-secure in the weak ciphertext-only attack (wCOA) security model for* $\varepsilon = \mathtt{negl}(\kappa)$ *if for all PPT algorithms* $A = (A_0, A_1)$*, we have*

$$Prob[\mathtt{wCOA}^{(A_0,A_1)}(\kappa) = 1] \leq \varepsilon.$$

By the definition, wCOA model does not allow the adversary to ask the oracle to decrypt any ciphertext. In other words, the adversary sees a list of ciphertext and tries to guess a plaintext for one of these ciphertexts. On the other hand, in COA model, after seeing a list of ciphertexts, the adversary submits two messages (normally bit 0 and bit 1) to the oracle for encryption. The oracle encrypts one of the messages and returns the ciphertext. The adversary tries to guess which message the oracle has encrypted.

3 Octonions

Octonion (see, e.g., Baez [1]) is the largest among the four normed division algebras: real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, quaternions $\mathbb{H}$, and octonions $\mathbb{O}$. The real numbers have a complete order while the complex numbers are not ordered. The quaternions are not commutative and the octonions are neither commutative nor associative. Quaternions were invented by Hamilton in 1843. Octonions were invented by Graves (1844) and Cayley (1845) independently.

In mathematics, a vector space commonly refers to a finite dimensional module over the real number field $\mathbb{R}$. An algebra A refers to a vector space that is equipped with a multiplication map $\times : A^2 \to A$ and a nonzero unit $1 \in A$ such that $1 \times a = a \times 1 = a$. The multiplication $a \times b$ is usually abbreviated as $a \cdot b$ or ab. An algebra A is a division algebra if, for any $a, b \in A$, $ab = 0$ implies either $a = 0$ or $b = 0$. Equivalently, A is a division algebra if and only if the operations of left and right multiplication by any nonzero element are invertible. A normed division algebra is an algebra that is also a normed vector space with $\|ab\| = \|a\|\|b\|$.

An algebra is power-associative if the sub-algebra generated by any single element is associative and an algebra is alternative if the sub-algebra generated by any two elements is associative. It is straightforward to show that if the sub-algebra generated by any three elements is associative, then the algebra itself is associative. Artin's theorem states that an algebra is alternative if and only if for all $a, b \in A$, we have

$$(aa)b = a(ab), \qquad (ab)a = a(ba), \qquad (ba)a = b(aa).$$

It is well known that $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ are the only normed division algebras and $\mathbb{O}$ is an alternative division algebra. It is also known that division algebras can only have dimension 1, 2, 4, or 8.

Using the same approach of interpreting a complex number $a + bi$ as a pair $[a, b]$ of real numbers, quaternions $\mathbb{H}$ (respectively, octonions $\mathbb{O}$) can be constructed from $\mathbb{C}$ (respectively, from $\mathbb{H}$) using the Cayley-Dickson construction formula $[a, b]$ where $a, b \in \mathbb{C}$ (respectively, $a, b \in \mathbb{H}$). The addition and multiplication are defined as follows.

$$[a, b] + [c, d] = [a + c, b + d], \quad [a, b][c, d] = [ac - db^*, a^*d + cb] \tag{2}$$

where $a, b, c, d \in \mathbb{C}$ (respectively, $a, b, c, d \in \mathbb{H}$) and a^* is the conjugate of a. The conjugate of a real number a is defined as $a^* = a$ and the conjugate of a complex number or a quaternion number $[a, b]$ is defined by $[a, b]^* = [a^*, -b]$. Throughout paper, we will use the following notations for real and imaginary part of an octonion $\mathbf{a} \in \mathbb{O}$,

$$\mathrm{Re}(\mathbf{a}) = (\mathbf{a} + \mathbf{a}^*)/2 \in \mathbb{R}, \qquad \mathrm{Im}(\mathbf{a}) = (\mathbf{a} - \mathbf{a}^*)/2.$$

It is straightforward to check that for numbers in $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$, we have

$$[a,b][a,b]^* = [a,b]^*[a,b] = \|[a,b]\|^2[1,0].$$

Thus all of $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ are division algebras (that is, each non-zero element has a multiplicative inverse).

Each octonion is a vector $\mathbf{a} = [a_0, \cdots, a_7] \in \mathbb{R}^8$. The norm of an octonion $\mathbf{a} = [a_0, \cdots, a_7]$ is defined as $\|\mathbf{a}\| = \sqrt{a_0^2 + \cdots + a_7^2}$. By the inductive Cayley-Dickson construction, the conjugate of an octonion $\mathbf{a}$ is $\mathbf{a}^* = [a_0, -a_1, \cdots, -a_7]$ and the inverse is $\mathbf{a}^{-1} = \mathbf{a}^*/\|\mathbf{a}\|^2$. For each octonion number $\mathbf{a} = [a_0, \cdots, a_7]$, let $\alpha = [a_1, \cdots, a_7]$ and

$$B_{\mathbf{a}} = \begin{pmatrix} a_0 & a_4 & a_7 & -a_2 & a_6 & -a_5 & -a_3 \\ -a_4 & a_0 & a_5 & a_1 & -a_3 & a_7 & -a_6 \\ -a_7 & -a_5 & a_0 & a_6 & a_2 & -a_4 & a_1 \\ a_2 & -a_1 & -a_6 & a_0 & a_7 & a_3 & -a_5 \\ -a_6 & a_3 & -a_2 & -a_7 & a_0 & a_1 & a_4 \\ a_5 & -a_7 & a_4 & -a_3 & -a_1 & a_0 & a_2 \\ a_3 & a_6 & -a_1 & a_5 & -a_4 & -a_2 & a_0 \end{pmatrix}$$

Using the matrix $B_{\mathbf{a}}$, we can define two associated 8×8 matrices

$$A^l_{\mathbf{a}} = \begin{pmatrix} a_0 & \alpha \\ -\alpha^T & B_{\mathbf{a}} \end{pmatrix} \quad \text{and} \quad A^r_{\mathbf{a}} = \begin{pmatrix} a_0 & \alpha \\ -\alpha^T & B^T_{\mathbf{a}} \end{pmatrix} \tag{3}$$

Then for two octonions $\mathbf{a} = [a_0, \cdots, a_7]$ and $\mathbf{b} = [b_0, \cdots, b_7]$, we can add them as $\mathbf{a} + \mathbf{b} = [a_0 + b_0, \cdots, a_7 + b_7]$ and multiply them as $\mathbf{ab} = \mathbf{b}A^l_{\mathbf{a}} = \mathbf{a}A^r_{\mathbf{b}}$. We also note that

$$A^l_{\mathbf{a}^{-1}} = \frac{1}{\|\mathbf{a}\|^2}\begin{pmatrix} a_0 & -\alpha \\ \alpha^T & B^T_{\mathbf{a}} \end{pmatrix} \quad \text{and} \quad A^r_{\mathbf{a}^{-1}} = \frac{1}{\|\mathbf{a}\|^2}\begin{pmatrix} a_0 & -\alpha \\ \alpha^T & B_{\mathbf{a}} \end{pmatrix} \tag{4}$$

For any octonion $\mathbf{a} = [a_0, \cdots, a_7]$, it is straightforward to show that

$$\begin{aligned} B_{\mathbf{a}}\alpha^T &= B^T_{\mathbf{a}}\alpha^T = a_0\alpha^T \\ B_{\mathbf{a}}B_{\mathbf{a}} &= \alpha^T\alpha - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} + 2a_0B_{\mathbf{a}} \\ B^T_{\mathbf{a}}B^T_{\mathbf{a}} &= \alpha^T\alpha - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} + 2a_0B^T_{\mathbf{a}} \\ B_{\mathbf{a}}B^T_{\mathbf{a}} &= -\alpha^T\alpha + \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \\ B^T_{\mathbf{a}}B_{\mathbf{a}} &= -\alpha^T\alpha + \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{aligned} \tag{5}$$

Thus we have

$$A^l_{\mathbf{a}}A^r_{\mathbf{a}} = A^r_{\mathbf{a}}A^l_{\mathbf{a}} = \begin{pmatrix} a_0^2 - \alpha\alpha^T & 2a_0\alpha \\ -2a_0\alpha^T & -\alpha^T\alpha + B_{\mathbf{a}}B^T_{\mathbf{a}} \end{pmatrix} \tag{6}$$

By substituting (5) into (6), we get

$$A^l_{\mathbf{a}}A^r_{\mathbf{a}} = A^r_{\mathbf{a}}A^l_{\mathbf{a}} = \begin{pmatrix} 2a_0^2 - \|\mathbf{a}\|^2 & 2a_0\alpha \\ -2a_0\alpha^T & -2\alpha^T\alpha + \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{pmatrix} \tag{7}$$

Similarly, we can get

$$\begin{array}{l} A^l_{\mathbf{a}} A^l_{\mathbf{a}} = 2a_0 A^l_{\mathbf{a}} - \|\mathbf{a}\|^2 \mathbf{I}_{8\times 8} \\ A^r_{\mathbf{a}} A^r_{\mathbf{a}} = 2a_0 A^r_{\mathbf{a}} - \|\mathbf{a}\|^2 \mathbf{I}_{8\times 8} \end{array} \tag{8}$$

Finally, it is easy to check that $A^l_{\mathbf{a}} A^l_{\mathbf{a}^{-1}} = A^l_{\mathbf{a}^{-1}} A^l_{\mathbf{a}} = A^r_{\mathbf{a}} A^r_{\mathbf{a}^{-1}} = A^r_{\mathbf{a}^{-1}} A^r_{\mathbf{a}} = \mathbf{I}_{8\times 8}$. But generally, we have $A^l_{\mathbf{a}} A^r_{\mathbf{a}^{-1}} \neq \mathbf{I}_{8\times 8}$. We conclude this section with the following theorem that will be used frequently throughout this paper.

Theorem 2. *For* $\mathbf{a} \in \mathbb{O}$*, we have* $\mathbf{a}^2 = 2\mathrm{Re}(\mathbf{a})\mathbf{a} - \|\mathbf{a}\|^2\mathbf{1}$ *where* $\mathbf{1} = [1,0,0,0,0,0,0,0]$.

Proof. The identity $\mathbf{a}^* = 2\mathrm{Re}(\mathbf{a})\mathbf{1} - \mathbf{a}$ implies $\|\mathbf{a}\|^2 = \mathbf{a}\mathbf{a}^* = 2\mathrm{Re}(\mathbf{a})\mathbf{a} - \mathbf{a}^2$. □

Theorem 3. *For all* $\mathbf{a}, \mathbf{b} \in \mathbb{O}$*, we have* $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$.

Proof. By the fact that the octonion algebra is alternative, we have $(\mathbf{ab})(\mathbf{b}^*\mathbf{a}^*) = \mathbf{a}(\mathbf{b}\mathbf{b}^*)\mathbf{a}^* = \|\mathbf{a}\|^2\|\mathbf{b}\|^2$. Thus $(\mathbf{ab})^{-1} = (\mathbf{b}^*\mathbf{a}^*)/(\|\mathbf{a}\|^2\|\mathbf{b}\|^2)$. Theorem follows from the fact that $(\mathbf{ab})^{-1} = (\mathbf{ab})^*/(\|\mathbf{ab}\|^2)$. □

4 Octonions $\mathbb{O}(\mathbb{Z}_q)$ over $\mathbb{Z}_q$

In the preceding section, we briefly discussed the properties of octonions. Instead of using real numbers, one may also construct "octonions" over any field $\mathbb{F}_q$ with $q = p^m$ or over any ring $\mathbb{Z}_q$ with $q = p_1^{r_1} \cdots p_m^{r_m}$. In this section, we discuss octonions $\mathbb{O}(\mathbb{Z}_q)$ over $\mathbb{Z}_q$. Generally, all theorems except division-related results for octonions hold in $\mathbb{O}(\mathbb{Z}_q)$. It is straightforward to show that $\mathbb{O}(\mathbb{Z}_q)$ is a normed algebra. However, it is not a division algebra. In our FHE schemes, the division operation is not used.

An octonion $\mathbf{z} \in \mathbb{O}(\mathbb{Z}_q)$ is isotropic if $\|\mathbf{z}\| = 0$. By Theorem 6.26 in Lidl and Niederreiter [10, page 282], there are $q^7 + q^4 - q^3 = (q^4-1)(q^3+1) + 1$ isotropic vectors in $\mathbb{F}_q^8$. A slightly modified proof of the Theorem 6.26 in [10] could be used to show that the number of isotropic vectors in $\mathbb{Z}_q^8$ is approximately in the same order of $q^7 + q^4 - q^3$ (the exact number is not important for our construction of the FHE scheme and the details are omitted here). A subspace V of $\mathbb{Z}_q^8$ is called totally singular or totally isotropic if all vectors in V are isotropic.

For an odd q and even n, the number of totally isotropic subspaces of dimension $k \leq n/2$ in $\mathbb{F}_q^n$ is given by the formula (see Pless [11] or Dembowski [5, Page 47])

$$\frac{(q^{n-k} - q^{n/2-k} + q^{n/2} - 1)\prod_{i=1}^{k-1}(q^{n-2i} - 1)}{\prod_{i=1}^{k}(q^i - 1)}, \tag{9}$$

and totally isotropic subspaces of dimension $k > n/2$ in $\mathbb{F}_q^n$ do not exist. It follows that the number of dimension 4 totally isotropic subspaces of $\mathbb{F}_q^8$ is given by

$$2(q+1)(q^2+1)(q^3+1) \tag{10}$$

Similar results for the number of totally isotropic subspaces of dimension k over $\mathbb{Z}_q^n$ could be obtained and the details are omitted in this paper.

Let $\mathbf{a} \in \mathbb{O}(\mathbb{Z}_q)$ be a non-zero isotropic octonion. Then $\mathbf{a}\mathbf{a}^* = \|\mathbf{a}\|^2 = 0$. That is, $\mathbf{a}$ has no multiplicative inverse. It follows that $\mathbb{O}(\mathbb{Z}_q)$ is not a division algebra. This also

shows that $\mathbb{O}(\mathbb{Z}_q)$ is not nicely normed. Note that an algebra over $\mathbb{Z}_q$ is nicely normed if $\mathbf{a}+\mathbf{a}^* \in \mathbb{Z}_q$ and $\mathbf{a}\mathbf{a}^* = \mathbf{a}^*\mathbf{a} > 0$ for all non zero $\mathbf{a} \in \mathbb{O}(\mathbb{Z}_q)$.

It is straightforward that Theorem 2 holds for $\mathbb{O}(\mathbb{Z}_q)$. We use an alternative proof to show that Theorem 3 holds for $\mathbb{O}(\mathbb{Z}_q)$ also. Note that the proof of Theorem 3 is not valid for $\mathbb{O}(\mathbb{Z}_q)$ since it uses octonion inverse properties.

Theorem 4. *For all* $\mathbf{a}, \mathbf{b} \in \mathbb{O}(\mathbb{Z}_q)$*, we have* $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$.

Proof. By the definition in (3), we have $A^r_{\mathbf{a}^*} = (A^r_{\mathbf{a}})^T$. First, the identity $\mathbf{1b}^*\mathbf{a}^* = \mathbf{1}(A^r_{\mathbf{b}})^T(A^r_{\mathbf{a}})^T = \mathbf{1}(A^r_{\mathbf{a}}A^r_{\mathbf{b}})^T$ implies that $\mathbf{b}^*\mathbf{a}^*$ is the first column of $A^r_{\mathbf{a}}A^r_{\mathbf{b}}$. Secondly, the identity $\mathbf{1ab} = \mathbf{1}(A^r_{\mathbf{a}}A^r_{\mathbf{b}})$ implies that $(\mathbf{ab})^*$ is also the first column of $A^r_{\mathbf{a}}A^r_{\mathbf{b}}$. It follows that $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$. □

Finally, Theorem 2 implies the following result.

Theorem 5. *For an isotropic octonion* $\mathbf{a} \in \mathbb{O}(\mathbb{Z}_q)$*, we have* $\mathbf{a}^2 = 2\mathrm{Re}(\mathbf{a})\mathbf{a}$.

5 The exceptional Lie group G_2 and its finite version $G_2(q)$

A Lie algebra $\mathfrak{g}$ over a field $\mathbb{F}$ is a vector space over $\mathbb{F}$ with a bilinear map (called a bracket or a commutator) $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ with the following properties:

- Anti-commutativity: $[y,x] = -[x,y]$ for all $x, y \in \mathbb{F}$
- Jordan identity: $[[x,y],z] + [[y,z],x] + [[z,x],y] = 0$ for all $x, y, z \in \mathbb{F}$.

The classical example of Lie algebra is the special linear algebra $\mathfrak{sl}_n$ of $n \times n$ matrices of trace 0 with $[x,y] = xy - yx$. The Lie algebra $\mathfrak{sl}_n$ corresponds to the Lie group SL_n of determinant 1 matrices.

The automorphism group G_2 of octonions $\mathbb{O}$ (over $\mathbb{R}$) has dimension 14 and is the smallest among the ten families of exceptional Lie groups (G_2, F_4, E_6, E_7, E_8, ${}^2E_6$, ${}^3D_4$, ${}^2B_2$, ${}^2G_2$, and ${}^2F_4$). The corresponding Lie algebra $\mathfrak{g}_2$ for G_2 is the derivations $\mathfrak{Der}(\mathbb{O})$ of the octonions $\mathbb{O}$. We will use $G_2(q)$ to denote the finite automorphism group of octonions $\mathbb{O}(\mathbb{Z}_q)$. It should be noted that in the literature, the notation $G_2(q)$ is generally used to denote the finite automorphism group of octonions $\mathbb{O}(\mathbb{F}_q)$ over a finite field $\mathbb{F}_q$. However, for the finite automorphism group related results that we will use in this paper, they hold for $G_2(q)$ over $\mathbb{O}(\mathbb{Z}_q)$ as well as for $G_2(q)$ over $\mathbb{O}(\mathbb{F}_q)$.

A basic triple for octonions $\mathbb{O}(\mathbb{Z}_q)$ is three elements $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ of norm -1 such that

- $\mathbf{e}_1\mathbf{e}_2 = -\mathbf{e}_2\mathbf{e}_1$, $\mathbf{e}_2\mathbf{e}_3 = -\mathbf{e}_3\mathbf{e}_2$, and $\mathbf{e}_1\mathbf{e}_3 = -\mathbf{e}_3\mathbf{e}_1$.
- $(\mathbf{e}_1\mathbf{e}_2)\mathbf{e}_3 = -\mathbf{e}_3(\mathbf{e}_1\mathbf{e}_2)$.

It is straightforward to observe that $\mathbf{e}_1$ generates a sub-algebra of $\mathbb{O}(\mathbb{Z}_q)$ that is isomorphic to $\mathbb{C}(\mathbb{Z}_q)$, $(\mathbf{e}_1, \mathbf{e}_2)$ generates a sub-algebra of $\mathbb{O}(\mathbb{Z}_q)$ that is isomorphic to $\mathbb{H}(\mathbb{Z}_q)$, and $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ generates all $\mathbb{O}(\mathbb{Z}_q)$. In other words, given $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$, there is a unique way to define the imaginary octonion units $i_1, \cdots, i_7$. It follows that given any two basic triples, there exists a unique automorphism in $G_2(q)$ that maps the first triple to the second triple. We can interpret this observation as follows to determine the size of $G_2(q)$. In order to construct an automorphism in $G_2(q)$, one first maps $\mathbf{e}_1$ to any point $\mathbf{e}'_1$ on the 6-sphere of unit imaginary octonions, then maps $\mathbf{e}_2$ to any point $\mathbf{e}'_2$ on the 5-sphere of unit imaginary octonions that are orthogonal to $\mathbf{e}'_1$, and finally maps $\mathbf{e}_3$ to any point $\mathbf{e}'_3$ on the 3-sphere of unit imaginary octonions that are orthogonal to $\mathbf{e}'_1, \mathbf{e}'_2$, and $\mathbf{e}'_1\mathbf{e}'_2$. By counting the number of such kind of triples, one can show that $|G_2(q)| = q^6(q^6-1)(q^2-1)$.

6 Fully homomorphic encryption scheme OctoM

In this section, we introduce an efficient noise-free symmetric key FHE scheme OctM. It is shown in the next section that the scheme OctoM is secure in the weak ciphertext-only security model. A totally isotropic subspace $V \subset \mathbb{Z}_q^8$ is said to be closed under octonion multiplications if for any $\mathbf{r}_0, \mathbf{r}_1 \in V$, we have both $\mathbf{r}_0\mathbf{r}_1 \in V$ and $\mathbf{r}_1\mathbf{r}_0 \in V$ where $\mathbf{r}_0\mathbf{r}_1$ and $\mathbf{r}_1\mathbf{r}_0$ are the octonion multiplications (based on the definition, we may also call such kind of subspaces as "totally isotropic ideal subspaces"). By Theorem 5, for any isotropic vector $\mathbf{z} \in \mathbb{Z}_q^8$, we have $\mathbf{z}^2 = 2\mathrm{Re}(\mathbf{z})\mathbf{z}$. Thus for any nonzero isotropic vector $\mathbf{z} \in \mathbb{Z}_q^8$, span$\{\mathbf{z}\}$ is a dimension one totally isotropic subspace that is closed under octonion multiplications. The comment 2 in Section 7 will show that there exist dimension two totally isotropic subspaces that are closed under octonion multiplications. By formulas (9) and (10) in Section 4, there exist dimension 3 and 4 totally isotropic subspaces for octonions $\mathbb{Z}_q^8$. It is also known that there is no dimension $d \geq 5$ totally isotropic subspace for octonions $\mathbb{Z}_q^8$. It remains an open question whether there exist dimension 3 or 4 totally isotropic subspaces in $\mathbb{Z}_q^8$ that are closed under octonion multiplications.

It is noted that a totally isotropic subspace V of dimension d is uniquely determined by d isotropic octonions (that is, a basis of the subspace). For the construction of FHE scheme OctoM, it suffices to have a dimension one totally isotropic subspace that is closed under octonion multiplications. In the following, we present the FHE protocol using the parameter $q = p_1p_2$. The protocol could be implemented over any finite rings $\mathbb{Z}_q$ with $q = p_1^{r_1} \cdots p_m^{r_m}$ and $m \geq 3$. In the following, we will use i to denote the octonion $[0, 1, 0, 0, 0, 0, 0, 0]$.

Key Setup. Select $q = p_1p_2$ according to the given security parameter κ. Select a totally isotropic subspace $V \subset \mathbb{Z}_q^8$ that is closed under octonion multiplications. Select a random $\phi \in G_2(q)$ and a random invertible 8×8 matrix $K \in \mathbb{Z}_q^{8\times 8}$. The private key is (K, ϕ, V) and the system public parameter is $\mathbb{Z}_q$.

Encryption. For a message $m \in \mathbb{Z}_q$, choose random $r \in \mathbb{Z}_q$ and $\mathbf{z} \in V$ with the property that $|A^l_{\mathbf{m}'}| = 0$, where $\mathbf{m}' = \phi(mi + \mathbf{z})$ and $A^l_{\mathbf{m}'}$ is the associated matrix for the octonion number $\mathbf{m}'$. Note that such kind of r and $\mathbf{z}$ could be chosen in constant rounds since the probability for $|A^l_{\mathbf{m}'}| = 0$ converges to a uniform limit (see, e.g., [4]). Let the ciphertext $C_m = \mathtt{OctoM.Enc}(\mathtt{key}, m) = K^{-1}A^l_{\mathbf{m}'}K \in \mathbb{Z}_q^{8\times 8}$.

Decryption. For a received ciphertext $C_{\mathbf{m}}$, decrypt the plaintext as

$$m = \mathtt{OctoM.Dec}(\mathtt{key}, C_m) = \phi^{-1}(\mathbf{1}(KC_mK^{-1})) \mod V.$$

It should be noted that $\mathbf{1}(KC_mK^{-1}) = \mathbf{1}A_{\mathbf{m}'} = \mathbf{m}'$. In order to carry out homomorphic operations on the ciphertext, the owner also needs to publish a ciphertext of -1. That is, let C_{-1} be the ciphertext of -1.

Ciphertext addition. The addition of ciphertexts C_{m_0} and C_{m_1} is defined as the regular component wise matrix addition $C_{m_0+m_1} = C_{m_0} + C_{m_1}$.

Ciphertext multiplication. The multiplication of ciphertexts C_{m_0} and C_{m_1} is defined as the regular matrix multiplication $C_{m_0m_1} = C_{m_1}C_{m_0'} = K^{-1}A^l_{\mathbf{m}_1'}KK^{-1}A^l_{\mathbf{m}_0}K = K^{-1}A^l_{\mathbf{m}_1}A^l_{\mathbf{m}_0}K$.

It is straightforward to verify that the above encryption scheme is additive homomorphic. The multiplication homomorphic property follows from the following equations.

$$\begin{aligned}
&\texttt{OctoM.Dec}(\texttt{key}, C_{m_0 m_1}) \\
&= \phi^{-1}(\mathbf{1}(A^l_{\mathbf{m}'_1} A^l_{\mathbf{m}'_0} A^l_{-1})) \mod V \\
&= \phi^{-1}(\mathbf{m}'_0(\mathbf{m}'_1 \cdot (-i + \mathbf{z}_2))) \mod V \\
&= \phi^{-1}(\phi(m_0 i + \mathbf{z}_0)\, \phi(m_1 i + \mathbf{z}_1)\, \phi(-i + \mathbf{z}_2)) \mod V \\
&= (m_0 i)(m_1 i)(-i) \\
&= m_0 m_1 i.
\end{aligned}$$

We conclude this section by showing that the decryption process of OctoM is equivalent to the decryption process IPE.Dec of a dimension 64 IPE scheme of Section 2. Let $\texttt{key} = (K, \phi, V) = \texttt{OctoM.KeySetup}(\kappa)$ be the secret key of the encryption scheme OctoM. Let $\beta = [b_1, 1, b_2, \cdots, b_7] \in \mathbb{Z}_q^8$ be a vector that is orthogonal to $\phi(V)$. Then $\phi(mi + \mathbf{z})\beta^T = mi$. For a ciphertext C_m, let $\mathrm{vec}(C_m) = [c_{0,0}, \cdots, c_{7,0}, \cdots, c_{7,7}]^T$ be the vectorization of C_m. The decryption process $\texttt{OctoM.Dec}(\texttt{key}, C_m)$ could be reformulated as

$$\begin{aligned}
mi &= \phi(mi + \mathbf{z})\beta^T \\
&= (\mathbf{1} K C_m K^{-1})\beta^T \\
&= \left[\textstyle\sum_{i,j=0}^{7} a_{0,i,j} c_{i,j}, \cdots, \sum_{i,j=0}^{7} a_{7,i,j} c_{i,j}\right] \beta^T \\
&= \textstyle\sum_{i,j=0}^{7} k_{i,j} c_{i,j} \\
&= \mathbf{k} \cdot \mathrm{vec}(C_m) \\
&= \texttt{IPE.Dec}(\mathbf{k}, \mathrm{vec}(C_m))
\end{aligned} \tag{11}$$

for some $a_{0,i,j}, \cdots, a_{7,i,j} \in \mathbb{Z}_q$ and $\mathbf{k} = [k_{0,0}, \cdots, k_{0,7}, k_{1,0}, \cdots, k_{7,7}] \in \mathbb{Z}_q^{64}$.

7 Some comments on the design of OctoM

In this section, we present some comments on the design principles of OctoM. The first time reader may skip this section.

Comment 1: In the encryption scheme OctoM, the message m is encoded to $\mathbf{m}' = \phi(mi + \mathbf{z})$ with a randomly selected octonion $\mathbf{z}$ from a totally isotropic subspace that is closed under octonion multiplications. As a special case of the scheme, one can choose a random isotropic octonion $\mathbf{z}_0$ and let $V = \mathrm{span}\{\mathbf{z}_0\}$. That is, each message m is encoded to $\mathbf{m}' = \phi(mi + r\mathbf{z}_0)$ for randomly selected $r \in \mathbb{Z}_q$.

Comment 2: In order to construct a dimension 2 totally isotropic subspace $V \subset \mathbb{Z}_q^8$, it suffices to choose linearly independent isotropic octonions $\mathbf{z}_0, \mathbf{z}_1$ (which forms a basis of V) in such a way that $r_0\mathbf{z}_0 + r_1\mathbf{z}_1$ is isotropic for all $r_0, r_1 \in \mathbb{Z}_q$. First we note that

$$\begin{aligned}
\|r_0\mathbf{z}_0 + r_1\mathbf{z}_1\|^2 &= (r_0\mathbf{z}_0 + r_1\mathbf{z}_1)(r_0\mathbf{z}_0^* + r_1\mathbf{z}_1^*) \\
&= r_0 r_1 \mathbf{z}_0\mathbf{z}_1^* + r_0 r_1 \mathbf{z}_1\mathbf{z}_0^* \\
&= r_0 r_1 (\mathbf{z}_0\mathbf{z}_1^* + (\mathbf{z}_0\mathbf{z}_1^*)^*) \\
&= 2 r_0 r_1 \mathrm{Re}(\mathbf{z}_0\mathbf{z}_1^*).
\end{aligned}$$

Thus, for any nonzero octonions $\mathbf{z}_0, \mathbf{z}_1$ satisfying

$$\|\mathbf{z}_0\| = \|\mathbf{z}_1\| = \mathrm{Re}(\mathbf{z}_0\mathbf{z}_1^*) = 0, \tag{12}$$

the subspace span$(\mathbf{z}_0, \mathbf{z}_1)$ is a dimension 2 totally isotropic subspace of $\mathbb{Z}_q^8$. In order to construct a totally isotropic subspace V that is closed under octonion multiplications, it suffices to choose linearly independent isotropic octonions $\mathbf{z}_0, \mathbf{z}_1 \in \mathbb{Z}_q^8$ such that the identity (12) holds and there exist $r_0, r_1, r_2, r_3 \in \mathbb{Z}_q$ satisfying

$$\begin{aligned} \mathbf{z}_0\mathbf{z}_1 &= r_0\mathbf{z}_0 + r_1\mathbf{z}_1 \\ \mathbf{z}_1\mathbf{z}_0 &= r_2\mathbf{z}_0 + r_3\mathbf{z}_1 \end{aligned} \tag{13}$$

Combing identities (12) and (13), we get 19 equations with 20 unknowns. Thus there exist dimension 2 totally isotropic subspaces $V \subset \mathbb{Z}_q^8$ that are closed under octonion multiplications. For $k \geq 3$, we conjecture that there exists no dimension k totally isotropic subspaces $V \subset \mathbb{Z}_q^8$ that are closed under octonion multiplication.

8 Proof of Security

The preceding section shows that the decryption process of the scheme `OctoM` is equivalent to the decryption process of the dimension 64 `IPE`. Thus the scheme `OctoM` is not secure against adversaries who have access to sufficiently many linearly independent ciphertexts with known plaintexts . Furthermore, by Theorem 1, `OctoM` is not secure in the ciphertext only attack (COA) security model. In this section, we show that `OctoM` is secure in the weak ciphertext-only (wCOA) security model.

We first show `OctoM` is secure in the wCOA model assuming that the only attack one could mount on `OctoM` is to guess the `IPE` decryption key via ciphertexts only without using the homomorphic properties and without using other algebraic attacks. Since the decryption process of `OctoM` is equivalent to `IPE.Dec`, it is sufficient for the adversary to recover the inner product decryption secret $\mathbf{k}$. Though we think that it is a folklore that the probability for one to recover the `IPE.Dec` secret $\mathbf{k}$ from `IPE` ciphertexts only is negligible (without limit on the number of ciphertexts), we did not find a literature reference for this. For completeness, we present a proof for this "folklore".

Theorem 6. *Let κ be the security parameter, $n \leq t \leq$ poly(κ), and assume that the plaintext messages are uniformly distributed over $\mathbb{Z}_q$. Given t ciphertexts $\mathbf{c}_0, \cdots, \mathbf{c}_{t-1} \in \mathbb{Z}_q^n$ of a dimension n encryption scheme* `IPE`*, the probability for one to guess the correct private key $\mathbf{k} \in \mathbb{Z}_q^n$ or for one to guess at least one correct plaintext for the given ciphertexts is at most $\frac{1}{q^n}$. In other words, the scheme* `IPE` *is secure in wCOA.*

Proof. For the given t ciphertexts, one can formulate t linear equations in $t + n$ variables $\mathbf{m} = [m_0, \cdots, m_{t-1}]$ and $\mathbf{k} = [k_0, \cdots, k_{n-1}]$:

$$\mathbf{k}[\mathbf{c}_0^T, \cdots, \mathbf{c}_{t-1}^T] = \mathbf{m}. \tag{14}$$

Assume that the ciphertexts $\mathbf{c}_0, \cdots, \mathbf{c}_{n-1}$ are linearly independent. Then for any fixed $m_0, \cdots, m_{n-1} \in \mathbb{Z}_q$, the equation system (14) has a unique solution. On the other hand, if no n ciphertexts are linearly independent, then for any fixed $m_0, \cdots, m_{n-1} \in \mathbb{Z}_q$, there are more than one solutions for the equation system (14). In a summary, the probability that the adversary recovers the private key is less than or equal to the

probability that the adversary has a correct guess of the messages $m_0, \cdots, m_{n-1}$. This probability is at most $\frac{1}{q^n}$. Thus the Theorem is proved. □

Before proving the main theorem, we first prove a Lemma. For a ciphertext C_m, we use C_m^0 to denote the identity matrix I.

Lemma 1. *Let* $C_m = \texttt{OctoM.Enc}(\texttt{key}, m)$ *and* $C_m^2, \cdots, C_m^8$ *be ciphertexts of* $m^2, \cdots, m^8$ *respectively. Then* $\mathrm{vec}(C_m^0) = \mathrm{vec}(\mathbf{I}), \mathrm{vec}(C_m^1), \mathrm{vec}(C_m^2)$ *are linearly dependent.*

Proof. By (8), we know that for any octonion $\mathbf{a}$, we have $A_{\mathbf{a}}^l A_{\mathbf{a}}^l = 2a_0 A_{\mathbf{a}}^l - \|\mathbf{a}\|^2 \mathbf{I}_{8\times 8}$. It follows that $C_m^2 = K^{-1} A_{\mathbf{a}}^l A_{\mathbf{a}}^l K = 2a_0 C_m^1 - \|\mathbf{m}'\|^2 \mathbf{I}_{8\times 8}$. The Lemma is proved. □

Theorem 7. *Assuming that it is computationally infeasible to solve multivariate/univariate quadratic equation systems in* $\mathbb{Z}_q$*, and the plaintext messages are uniformly distributed over* $\mathbb{Z}_q$*. Then the encryption scheme* OctoM *over* $\mathbb{Z}_q$ *is* $(t, negl(\kappa))$*-secure in the weak ciphertext-only security model for any* $t \leq poly(\kappa)$*.*

Proof. Let $C_{p_0}, \cdots, C_{p_{t-1}}$ be the ciphertext output by the PPT algorithm A_0. By Theorem 6, if the most efficient attack on OctoM in the weak ciphertext-only security model is to recover the IPE decryption key from ciphertexts without employing fully homomorphic or other algebraic properties, then the theorem follows from Theorem 6 already. Thus it is sufficient to show that it is computationally infeasible to use fully homomorphic properties and other algebraic attacks to recover the secret key or to recover secret messages for OctoM.

In the following, we established two claims to show that the problem of recovering OctoM's secret key (K, ϕ, V) from ciphertexts could be reduced to the problem of solving multivariate quadratic equation systems and the problem of recovering a secret message from OctoM's ciphertexts could be reduced to the problem of solving univariate high degree equation systems. By the hardness assumption of the theorem, these equation systems are computationally infeasible to be solved.

Claim 8 *Given* t *ciphertexts for the FHE scheme* OctoM*, the problem of finding the private key* (K, ϕ, V) *and corresponding private messages could be reduced to a multivariate quadratic equation system with* $64t$ *equations in* $64 + 2t$ *unknown variables.*

Proof. As a warming up exercise, we first show that, given t ciphertexts, one can obtain $64t$ equations in $64 + 8t$ or $64 + 8d + (d+1)t$ unknown variables where $d = \dim(V)$. For each ciphertext C_m, we have the identity $KC_m = A_{\mathbf{m}'}^l K$. If we assign 8 variables for $\mathbf{m}' = mi + \mathbf{r}$ and 64 variables for K. Then we get 64 equations in $64+8$ unknowns. For t ciphertexts, we obtain $64t$ equations in $64 + 8t$ unknowns. Alternatively, let d be the dimension of V (in our case, $d = 1$ or $d = 2$). Then we can assign $8d$ variables for a basis of V, d variables for $\mathbf{r}$ (note that $\mathbf{r}$ is uniquely determined by the d coordinates relative to the basis), and one variable for each message m. In other words, each ciphertext could be converted to 64 equations in $64 + 8d + d + 1$ unknowns and t ciphertext could be converted to $64t$ equations in $64 + 8d + (d+1)t$ unknowns.

We next reduce the number of unknown variables to $64 + 2t$ by using the homomorphic properties of OctoM. Let C_m be the ciphertext and $\mathbf{m}' = \phi(mi + \mathbf{r}) =$

$[m_0, \cdots, m_7]$ where $\mathbf{r} \in V$. From the identity $KC_m = A^l_{\mathbf{m}'}K$ for the ciphertext C_m and by Lemma 1, we have

$$KC_m^2 = 2m_0KC_m - \|\mathbf{m}'\|^2K \tag{15}$$

If we consider $\|\mathbf{m}'\|^2$ as one variable, the identities (15) can be used to derive 64 multivariate quadratic equations in 66 variables (64 for K, one for m_0, and one for $\|\mathbf{m}'\|^2$). For t ciphertexts, one obtains $64t$ quadratic multivariate polynomial equation in $64+2t$ variables. □

Claim 9 *Given one ciphertext C for the FHE scheme* `OctoM`*, the problem of finding the secret message m could be reduced to the problem of solving a univariate quadratic equation.*

Proof. Let $C_m = \texttt{OctoM.Enc}(\texttt{key}, m)$ be a ciphertext of m and $\mathbf{m}' = [m_0, \cdots, m_7] = [r_0, m + r_1, \cdots, r_7]$. By Lemma 1 and using the values of C_m and C_m^2, one learns the values of $\|\mathbf{m}'\|^2 = r_0^2 + (m + r_1)^2 + r_2^2 + \cdots + r_7^2$ and $m_1 = m + r_1$. Since $r_0^2 + \cdots + r_7^2 = 0$, one obtains $m^2 + 2mr_1 = \|\mathbf{m}'\|^2$. This completes the proof of the Claim. □

By Claims 8 and 9, in order for one to recover the secret key or secret messages from the ciphertexts, one needs to solve a quadratic univariate polynomial equation in Claim 9 or to solve the multivariate equation system in Claims 8. By the assumption, it is computationally infeasible to solve univariate nonlinear polynomial equations over $\mathbb{Z}_q$ obtained in Claim 9. In the following, we show that it is computationally infeasible to solve the multivariate equation systems obtained in Claims 8.

For a system of $n(n+1)/2$ homogeneous quadratic equations with n variables $x_0, \cdots, x_{n-1}$, the folklore linearization technique replaces each quadratic monomial x_ix_j with a new variable y_{ij} and obtains $n(n+1)/2$ linear equations with $n(n+1)/2$ variables. The resulting equation system could be efficiently solved using Gauss elimination algorithm. The value of the original variable x_i can be recovered as one of the square roots of y_{ii}. Kipnis and Shamir [8] introduced a relinearization algorithm to solve quadratic equation systems with $l \geq 0.09175n^2$ linearly independent homogeneous quadratic equations in n variables. This is achieved by adding additional nonlinear equations. In the simplest form, we have $(x_{i_0}x_{i_1})(x_{i_2}x_{i_3}) = (x_{i_0}x_{i_2})(x_{i_1}x_{i_3}) = (x_{i_0}x_{i_3})(x_{i_1}x_{i_2})$. Thus we can add $y_{i_0i_1}y_{i_2i_3} = y_{i_0i_2}y_{i_1i_3} = y_{i_0i_3}y_{i_1i_2}$.

For the quadratic equation system obtained in Claim 8, there are $64t$ (not necessarily homogeneous) quadratic equations in $64 + 2t$ variables. Thus the relinearization algorithm in Kipnis and Shamir [8] might be applied to the equation system in Claim 8 only if $11 \leq t \leq 100$. Note that in order to apply the relinearization algorithm, these quadratic equations need to be converted to homogeneous quadratic equations first. Furthermore, the last step in the re-linearization approach is to compute square roots in $\mathbb{Z}_q$. By the assumption of the theorem, this is computationally infeasible over $\mathbb{Z}_q$. For $t \leq 10$ and $t \geq 101$, the linearization and re-linearization approaches could not be applied to the equation systems constructed in Claim 8 since there is insufficient number of equations.

The most popular algorithm for solving multivariate polynomial equation systems over finite fields is Buchberger's Gröbner basis algorithm based on S-polynomials (see,

e.g., [12]). The Gröbner basis algorithm is designed for polynomials over finite fields and the algorithm will not work in case any of the required inverses does not exist during the monomial elimination process. However, the algorithm could continue for polynomials over the ring $\mathbb{Z}_q$ in case all of the required inverses do exist. Indeed, we may assume that the algorithm can always continue since the probability for finding a non-invertible element is negligible (which is equivalent to finding a factor of q). However, it should also be noted that the last essential step for Gröbner basis algorithm family is to solve a univariate high degree polynomial equation which is computationally infeasible in $\mathbb{Z}_q$ by the theorem assumption. In summary, with the assumption of the theorem, it is computationally infeasible to solve the equation systems constructed in Claim 8. □

9 FHE over other algebras such as Jordan algebra

The preceding sections propose a fully homomorphic encryption scheme based on octonion algebra. One may wonder whether it is possible to use other normed finite algebras corresponding to $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, etc. to design FHE schemes. There is only one norm preserving automorphism (identity map) for $\mathbb{R}$. There are two norm preserving automorphisms (the identity map and the dual map) for $\mathbb{C}$. In addition to these two automorphisms for $\mathbb{C}$, there are infinitely many "wild" automorphisms for the complex number $\mathbb{C}$. For $\mathbb{H}$, the norm preserving automorphism is the group of real-linear transformations of $\mathrm{Im}(\mathbb{H})$ preserving the cross product $a \times b = \frac{1}{2}(ab - ba)$. Thus the automorphism group for $\mathbb{H}$ is just the special orthogonal group $\mathrm{SO}(3)$. That is, the group of 3×3 orthogonal matrices of determinant 1.

The corresponding finite algebras for the four division algebras are $\mathbb{F}_q$, $\mathbb{C}(\mathbb{F}_q)$, $\mathbb{H}(\mathbb{F}_q)$, and $\mathbb{O}(\mathbb{F}_q)$. For $\mathbb{F}_q$ with $q = p^m$, there are exactly m Frobenius automorphisms for $\mathbb{F}_q$ which are given by $\varphi^k : x \mapsto x^{p^k}$ for $0 \leq k < m$. It should be noted that all Frobenius automorphism fixes elements in $\mathbb{F}_q$. For $\mathbb{C}(\mathbb{F}_q)$, the automorphisms could be obtained by combining the Frobenius automorphism and the dual automorphism. The automorphism group for $\mathbb{H}(\mathbb{F}_q)$ could be obtained by combining the Frobenius automorphism and the special orthogonal group $\mathrm{SO}(3, \mathbb{F}_q)$. Based on these facts, it is straightforward to check that it is insecure to use automorphism groups of $\mathbb{F}_q$ and $\mathbb{C}(\mathbb{F}_q)$ to design fully homomorphic encryption schemes.

In order to use the automorphism group for $\mathbb{H}(\mathbb{Z}_q)$ to design fully homomorphic encryption schemes, it is necessary to guarantee that the size of the automorphism group $\mathrm{SO}(3)$ for $\mathbb{H}(\mathbb{Z}_q)$, the number of isotropic vectors in $\mathbb{Z}_q^4$, and the number of totally isotropic dimension 2 subspaces of $\mathbb{Z}_q^4$ are sufficiently large. By Theorem 6.26 of Lidl and Niederreiter [10, page 282], there are $q^3 + q(q-1)\eta(-1)$ isotropic vectors in $\mathbb{F}_q^4$, where η is the quadratic character of $\mathbb{F}_q$. That is, $\eta(-1) = 1$ if there is $x \in \mathbb{F}_q$ such that $x^2 = -1$. Otherwise, $\eta(-1) = -1$. By (9), the number of totally isotropic dimension 2 subspaces of $\mathbb{F}_q^4$ is $2(q+1)$. These arguments could be revised to show that the number of isotropic vectors in $\mathbb{Z}_q^4$ and the number of totally isotropic dimension 2 subspaces of $\mathbb{Z}_q^4$ are large enough for the design of an FHE scheme `QuatM` over $\mathbb{H}(\mathbb{Z}_q)$ in the same way that `OctoM` is designed. The security analysis for `QuatM` is the same as that for `OctoM`. In particular, for t ciphertexts, the approach in Claim 8 could be used to construct a quadratic equation system of $16t$ equations in $16 + 2t$ unknown vari-

ables. Similarly, the security of QuatM depends on the hardness of solving multivariate quadratic equations in $\mathbb{Z}_q$ and the hardness of solving high degree univariate polynomial equations in $\mathbb{Z}_q$. Similar to the scheme OctoM, it can be shown that the scheme QuatM is weakly equivalent to the inner product encryption scheme IPE of dimension 16. Since quaternion multiplication is associative, for the design of QuatM, one may also choose the private matrix $K \in \mathbb{H}(\mathbb{Z}_q)^{4\times 4}$. Thus the ciphertext is a matrix in $\mathbb{H}(\mathbb{Z}_q)^{4\times 4}$ also. Consequently, the revised QuatM is weakly equivalent to the inner product encryption scheme IPE of dimension 64.

One may also use other Lie groups to design fully homomorphic encryption schemes. For example, one can use the second smallest exceptional Lie group F_4 which is the automorphism group for the exceptional Jordan algebra (or Alberta algebra) $\mathfrak{h}_3(\mathbb{O})$ over $\mathbb{R}$. Specifically, $\mathfrak{h}_3(\mathbb{O})$ consists of the following 3×3 Hermitian matrices (matrices that are equal to their own conjugate transposes):

$$(a,b,c,\mathbf{a},\mathbf{b},\mathbf{c}) = \begin{bmatrix} a & \mathbf{c} & \mathbf{b} \\ \mathbf{c}^* & b & \mathbf{a} \\ \mathbf{b}^* & \mathbf{a}^* & c \end{bmatrix}$$

where $a,b,c \in \mathbb{R}$ and $\mathbf{a},\mathbf{b},\mathbf{c} \in \mathbb{O}$ and the Jordan product $\circ$ is defined by $\alpha\circ\beta = \frac{1}{2}(\alpha\beta+\beta\alpha)$ for $\alpha,\beta \in \mathfrak{h}_3(\mathbb{O})$. It is straightforward that Jordan algebra is of 27-dimension over $\mathbb{R}$. The Lie algebra $\mathfrak{f}_4$ of F_4 is isomorphic to $\mathfrak{so}(\mathbb{O})\oplus\mathbb{O}^3$.

For the finite exceptional Jordan algebra $\mathfrak{h}_3(\mathbb{O}(\mathbb{Z}_q))$, the 52-dimension $F_4(q) = \mathrm{Aut}(\mathfrak{h}_3(\mathbb{O}(\mathbb{Z}_q)))$ is the automorphism group of algebra $\mathfrak{h}_3(\mathbb{O}(\mathbb{Z}_q))$ which is a collection of the Hermitian 3×3 matrices restricted to $\mathbb{O}(\mathbb{Z}_q)$. It can be shown that

$$|F_4(q)| = q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1))$$

and $G_2(q) \subset F_4(q)$.

The determinant of a matrix in $\mathfrak{h}_3(\mathbb{O}(\mathbb{Z}_q))$ is defined by

$$\det(a,b,c,\mathbf{a},\mathbf{b},\mathbf{c}) = abc - (a\|\mathbf{a}\|^2 + b\|\mathbf{b}\|^2 + c\|\mathbf{c}\|^2) + 2\mathrm{Re}(\mathbf{abc})$$

This can be expressed as $\det(x) = \frac{1}{3}\mathrm{tr}(x^3) - \frac{1}{2}\mathrm{tr}(x^2)\mathrm{tr}(x) + \frac{1}{6}\mathrm{tr}(x)^3$ for $x \in \mathfrak{h}_3(\mathbb{O}(\mathbb{Z}_q))$. Thus the determinant of a Jordan algebra matrix is invariant under all automorphism $F_4(q)$ of $\mathfrak{h}_3(\mathbb{O}(\mathbb{Z}_q))$. That is, for all $\phi \in F_4(q)$, we have $\det(x) = \det(\phi(x))$.

In the following, we first describe the protocol for the FHE scheme JordanM.

Key Setup. Select $q = p_1p_2$ according to the given security parameter κ. Randomly select isotropic vectors $\mathbf{z}_1,\mathbf{z}_2,\mathbf{z}_3 \in \mathbb{O}(\mathbb{Z}_q)$ satisfying the following identity

$$\mathbf{z}_2\mathbf{z}_1^* = \mathbf{z}_3 \quad \text{and} \quad \mathrm{Re}(\mathbf{z}_1\mathbf{z}_2\mathbf{z}_3) \neq 0 \tag{16}$$

Note that such kind of $\mathbf{z}_1,\mathbf{z}_2,\mathbf{z}_3$ could be obtained by solving an equation system of 11 equations (eight obtained from (16) and three obtained from the identity $\|\mathbf{z}_1\| = \|\mathbf{z}_2\| = \|\mathbf{z}_3\| = 0$) in 24 variables. Let $\phi \in F_4(q)$ be a randomly selected automorphism and let $K \in {\mathbb{Z}_q}^{3\times 3}$ be a randomly selected 3×3 nonsingular matrix. The private key is $\mathtt{key} = (\phi, K, \mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3)$.

Encryption. For a message $m \in \mathbb{Z}_q$, choose random $r_1,r_2,r_3,r_4,r_5,r \in \mathbb{Z}_q$ such that $\det(E_m) \neq 0$, where E_m is the Hermitian matrix $E_m = (m, r_4, r_5, r_1\mathbf{z}_1, r_2\mathbf{z}_2, r_3\mathbf{z}_3)$. Let the ciphertext $C_m = \mathtt{JordanM.Enc}(\mathtt{key}, m) = K^{-1}\phi(E_m)K$.

Decryption. For a received ciphertext C_m, decrypt the plaintext as

$$m = \texttt{JordanM.Dec}(\texttt{key}, C_m) = \mathbf{1}\phi^{-1}(KC_mK^{-1})\mathbf{1}^T.$$

Ciphertext addition. The addition of two ciphertexts C_{m_0} and C_{m_1} is defined as the regular component wise matrix addition $C_{m_0+m_1} = C_{m_0} + C_{m_1}$.
Ciphertext multiplication. The multiplication of two ciphertexts C_{m_0} and C_{m_1} is defined as the Jordan product $\circ$:

$$\begin{aligned} C_{m_0m_1} &= C_{m_1} \circ C_{m_0} \\ &= (K^{-1}\phi(E_{m_0})\phi(E_{m_1})K + K^{-1}\phi(E_{m_1})\phi(E_{m_0})K)/2 \\ &= K^{-1}((\phi(E_{m_0})\phi(E_{m_1}) + \phi(E_{m_1})\phi(E_{m_0}))/2)K \\ &= K^{-1}\phi(E_{m_0} \circ E_{m_1})K. \end{aligned}$$

In the encryption process JordanM.Enc, the random numbers are chosen in such a way that $\det(E_m) \neq 0$ no matter whether $m = 0$ or not.

By the identity (16), we have $\mathbf{z}_2\mathbf{z}_1^* = \mathbf{z}_3$. This implies that $\mathbf{z}_3\mathbf{z}_1 = \mathbf{0}$ and $\mathbf{z}_3^*\mathbf{z}_2 = \mathbf{0}$. By these arguments and by the identity $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$ from Theorem 4, the multiplication homomorphism of JordanM could be verified straightforwardly and the details are omitted due to space limit.
Remark. In the key setup process JordanM.KeySetup, it is sufficient to use $\phi \in F_4(q)$ that are represented by the primitive idempotents $A \in \mathfrak{h}_3(\mathbb{O}(\mathbb{Z}_q))$ with $A \circ A = A$ and $\text{tr}(A) = 1$. That is, ϕ is defined by

$$\phi : B \mapsto B + 4\text{tr}(A \circ B)A - 4B \circ A$$

It is further noted that the primitive idempotents in the Jordan algebra are exactly the elements $(a, b, c, \mathbf{a}, \mathbf{b}, \mathbf{c})$ satisfying

$$\begin{aligned} &a + b + c = 1 \\ &a^2 + \|\mathbf{b}\|^2 + \|\mathbf{c}\|^2 = a \\ &\mathbf{b}^*\mathbf{a} = c\mathbf{c}^* \end{aligned}$$

and the equations obtained from these by cycling a, b, c and $\mathbf{a}, \mathbf{b}, \mathbf{c}$.

It should be noted that (see, e.g., Baez [1]), for any $(a, b, c, \mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathfrak{h}_3(\mathbb{O}(\mathbb{Z}_q))$, there exists $\phi \in F_4(q)$ such that $\phi((a, b, c, \mathbf{a}, \mathbf{b}, \mathbf{c}))$ is diagonalized. The security analysis for JordanM is similar to that of OctoM and we have the following theorem (proof is omitted due to space limit).

Theorem 10. *Assuming that it is computationally infeasible to solve univariate polynomial equation systems of degree larger than* 2*, it is computationally infeasible to solve multivariate/univariate quadratic equation systems in $\mathbb{Z}_q$, and the plaintext messages are uniformly distributed over $\mathbb{Z}_{q_0}$. Then the encryption scheme* JordanM *over $\mathbb{Z}_q$ is $(t, negl(\kappa))$-secure in the weak ciphertext-only security model for any $t \leq poly(\kappa)$.*

Remark In the scheme JordanM, the private key K is chosen as a 3×3 matrix over $\mathbb{Z}_q$. If K were chosen as a 3×3 matrix over $\mathbb{O}(\mathbb{Z}_q)$, then the scheme would not be multiplicative homomorphic since octonion multiplication is not associative. However,

one may use Jordan algebra restricted to quaternions $\mathbb{H}(\mathbb{Z}_q)$ to design an FHE scheme `JordanQuaterM`. Then one can use a 3×3 matrix $K \in \mathbb{H}(\mathbb{Z}_q)^{3\times 3}$ as the private key since quaternion multiplication is associative. Furthermore, one may also use high dimension Hermitian matrices for the design of `JordanM` scheme. For example, one may use the n-dimension Hermitian matrices design `JordanM`.

10 Privacy preserving garbled computation in cloud

The efficient FHE schemes designed in this paper are expected to have a wide range of applications. In this section, we show its applications to privacy preserving garbled computation in cloud. Specifically, we consider the following special case of reusable privacy preserving software outsourcing problem:

> The owner has a software (e.g., with a slow but feasible secret algorithm to break RSA when powerful computing resources are available) and the cloud has a powerful computing resource. The software owner wants to run his software in the cloud but he does not want to leak his secret algorithm. The cloud provides computing resources to the software owner and it does not need to learn the software output. The actual protocol could work like this: the software owner uploads his re-usable obfuscated software to the cloud. Each time when the software owner wants to run the obfuscated software in the cloud, he provides obfuscated inputs to the cloud. The cloud runs the obfuscated software and the obfuscated software output is returned to the software owner. The software owner decrypts the obfuscated output and learns the actual output.

In the following paragraphs, we show how to use FHE schemes proposed in this paper to solve the above reusable privacy preserving software outsourcing problem.

10.1 Straight line programs, arithmetic circuits, and universal circuits

Arithmetic circuits have been used as a model for computing polynomials. An arithmetic circuit takes either variables or numbers as inputs. The only allowed gates in arithmetic circuits are additions and multiplications. For the Boolean circuit model, it uses AND, OR, and NOT gates. Since these gates could be redesigned using NAND gates, we assume that all circuits contain `NAND` gates only. Each `NAND` gate can be converted to two arithmetic gates using the formula "x `NAND` $y = 1 - xy$". Thus each Boolean circuit could be converted to an arithmetic circuit that computes the same function. By the above discussion, each Boolean circuit could be converted to a straight line program where a straight-line program is a sequence of operations that only uses additions and multiplications as follows.

Input: $x_0, \cdots, x_{n-1}$
$v_0 = w_{0,0}$ `op` $w_{0,1}$
$\cdots$
$v_{t-1} = w_{t-1,0}$ `op` $w_{t-1,1}$

where $v_0, \cdots, v_{t-1}$ are temporary variables. Each operator op is either $+$ or $\times$, and the variables $w_{i,0}, w_{i,1}$ are either constants within $\{1, -1\}$ or variables from the list $x_0, \cdots, x_{n-1}, v_0, \cdots, v_{i-1}$.

For a universal straight line program U, it takes an input (C, x) where C is an encoded straight line program and $U(C, x) = C(x)$. The construction of universal Boolean circuits could be found in [9,13]. When a universal straight line program U (alternatively, a universal arithmetic circuit or a universal circuit) is used, the structure of U is public knowledge and there is no need to protect the control flow within U. It is sufficient to protect the input privacy (that is, both C and x). It should be noted that this is also sufficient for the protection of keyed programs, where the obfuscation does not depend on hiding the entire structure of the obfuscated program from the adversary and it only hides a short secret key embedded in the program.

10.2 Protocol for garbled computation in cloud

For the garbled computation in cloud that we have mentioned in the preceding paragraphs, the cloud does not need to know the software output. Thus an efficient FHE scheme together with a universal straight line program is sufficient for this kind of software obfuscation. In the proposed obfuscation approach, one only needs to homomorphically encrypt all input variables (that is, both C and x where C is the private circuit that the software owner wants to protect). That is, each variable x_i is homomorphically encrypted to $c_i = \texttt{FHE.Enc}(\texttt{key}, x_i)$. Each operator can then be evaluated homomorphically as $c = \texttt{FHE.Eval}(c_1, c_2; \texttt{op})$.

Let U be a universal straight line program and C be the straight line program that the software owner wants to obfuscate. Then the protocol proceeds as follows:

- The software owner constructs a reusable garbled software $\mathcal{C} = \texttt{FHE.Enc}(\texttt{key}, C)$ and uploads $\mathcal{C}$ to the cloud.
- For each evaluation, software owner provides an encrypted input $\texttt{FHE.Enc}(\texttt{key},x)$ to the cloud.
- The cloud runs the universal straight line program U on $(\mathcal{C}, \texttt{FHE.Enc}(\texttt{key},x))$ to obtain the encrypted output $\texttt{FHE.Enc}(\texttt{key},C(x)) = \texttt{FHE.Eval}(\mathcal{C}, \texttt{FHE.Enc}(\texttt{key},x); U)$
- The owner decrypts the actual output: $C(x) = \texttt{FHE.Dec}(\texttt{key}, \texttt{FHE.Enc}(\texttt{key},C(x)))$.

11 Practical considerations

The preceding sections show that the proposed FHE schemes OctoM, QuatM, JordanM are secure in the wCOA security mode. Furthermore, we also showed that known plaintext-ciphertext pairs of these FHE schemes could lead to the complete recovery of the private key. This gives the adversary the possibility of carrying out an exhaustive search based dictionary attacks in case that the guessable message space is small. As an example, assume that for given ciphertexts $\mathbf{c}_1, \cdots, \mathbf{c}_t$ of the scheme OctoM, one can obtain 64 independent ciphertext vectors from $\mathbf{c}_1, \cdots, \mathbf{c}_t$ using the fully homomorphic property. If the corresponding message $(m_1, \cdots, m_t) \in \mathcal{M}'$ for some $\mathcal{M}'$ with $|\mathcal{M}| \leq N$, then the adversary could do an exhaustive search of $\mathcal{M}'$ to obtain the candidate key space of size N. Furthermore, if the adversary can guess that some ciphertexts

corresponds to the same plaintext, then the adversary can use the additive homomorphism operations to obtain a valid ciphertext for the message 0. Based on these observations, an implementation of proposed FHE schemes should always take these factors into consideration. In particular, if possible, one should apply an appropriate message padding scheme before the FHE encryption process is used. These padding schemes should be compatible with the homomorphic operations.

The security of the FHE schemes `OctoM`, `QuatM`, `JordanM` depends on the hardness of solving multivariate quadratic equations and univariate high degree polynomial equations within $\mathbb{Z}_q$. The hardness of these problems are more or less related to the hardness of factoring q. For example, the problem of solving quadratic equations in $\mathbb{Z}_q$ is equivalent to the problem of factoring q. NIST SP 800-57 [2] recommends the security strength of $\mathbb{Z}_q$ for $q = p_1p_2$. For the FHE schemes proposed in this paper, we recommend the use of $q = p_1p_2p_3p_4$. Wang [14] list the security strength of $\mathbb{Z}_q$ when q is a multiplication of more than two primes. Following [2,14], we recommend the use of ring sizes for $\mathbb{Z}_q$ in Table 1.

Table 1. Bits of Security and $\mathbb{Z}_q$

Bits of Security	80	112	128	192	256
$q = p_1p_2$ **in bits [2]**	1024	2048	3072	7680	15360
$q = p_1p_2p_3$ **in bits [14]**	1536	2335	3072	7680	15360
$q = p_1p_2p_3p_4$ **in bits [14]**	2048	3072	4562	7680	15360

Table 2 lists the number of ring multiplications for proposed FHE schemes. For the performance comparison, we also include the number of ring multiplications needed for the RSA encryption scheme. In the table, we assume that the RSA public key is 3 and the private key size is the same as the modulus length. Furthermore, we assume that the RSA private key contains around 50% ones and the "square-and-multiply" algorithm is used for the RSA decryption process. From the table, it is observed that both the schemes `OctoM` and `QuatM` are more efficient than the RSA decryption process for all parameters. For the scheme `JordanM`, if the automorphism ϕ is implemented as a regular Jordan product, then it requires 1734 multiplications at most. Thus the total number of multiplications for a `JordanM.Enc` or `JordanM.Dec` is 2127 and both `JordanM` encryption and decryption processes are more efficient than the RSA decryption process for the security strength of 128-bits or more. However, if special automorphism ϕ were chosen and ϕ were implemented more efficiently than the RSA decryption process, then both `JordanM` encryption and decryption processes are more efficient than the RSA decryption process for all parameters.

Table 2. Performance comparison in terms of field multiplications

	`OctoM`	`QuatM`	`JordanM`	RSA
Encryption	1026	130	$393+1734 = 2127$	3
Decryption	578	82	$393+1734 = 2127$	$1.5\|q\|$
Homo Multi.	512	64	3456	

We conclude this section by pointing out ciphertext expansion factors for schemes `OctoM`, `QuatM`, and `JordanM`. The ciphertext expansion factor for a scheme `xx` is defined as $\max\left\{\frac{|\mathbf{c}_m|}{|m|} : m \in \mathcal{M}\right\}$ where $\mathbf{c}_m = \texttt{xx}(\mathbf{k}, m)$ is the ciphertext of m. For the

scheme OctoM (respectively QuatM and JordanM), the ciphertext $\mathbf{c}_m$ for $m \in \mathbb{Z}_{q_0}$ is a collection of 64 elements (respectively, 16 and 72) from $\mathbb{Z}_q$. Thus the message expansion factors for the schemes OctoM, QuatM, and JordanM are 128, 32, and 144 respectively.

12 Conclusion

This paper introduces efficient noise-free FHE schemes in the weak ciphertext-only security model. The proposed schemes are used to solve a specific type problem for privacy preserving garbled cloud computation. It is expected that there is a wide range of applications for the proposed FHE schemes. For an implementation of the proposed FHE schemes, if the message space in the application has a small guessable size and an appropriate padding scheme is not employed, then one may mount a dictionary attack on the implementation. It will be interesting to investigate FHE compatible "padding" techniques to defeat the potential dictionary attacks on these implementations.

13 Acknowledgments

The first author would like to thank Martin Strand for several comments on an early version of this paper and thank Craig Gentry for pointing out the reference [7].

References

1. J. Baez. The octonions. *Bullet. American Mathematical Society*, 39(2):145–205, 2002.
2. E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. NIST special publication 800-57. *NIST Special Publication*, 800(57):1–142, 2007.
3. Z. Brakerski. When homomorphism becomes a liability. In *Theory of Cryptography*, pages 143–161. Springer, 2013.
4. L.S. Charlap, H.D. Rees, and D.P. Robbins. The asymptotic probability that a random biased matrix is invertible. *Discrete Mathematics*, 82(2):153–163, 1990.
5. P. Dembowski. *Finite Geometries: Reprint of the 1968 Edition*. Springer Science, 2012.
6. C. Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, volume 9, pages 169–178, 2009.
7. A. Kipnis and E. Hibshoosh. Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification. *IACR ePrint Archive*, 2012:637, 2012.
8. A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem. In *Proc. Crypto*, 1999.
9. V. Kolesnikov and T. Schneider. A practical universal circuit construction and secure evaluation of private functions. In *Financial Cryptography*, pages 83–97. Springer, 2008.
10. R. Lidl and H. Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.
11. V. Pless. The number of isotropic subspaces in a finite geometry. (Italian summary). *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 39:418–421, 1965.
12. B. Sturmfels. What is a Gröbner basis. *Notices Amer. Math. Soc*, 52(10):1199–1200, 2005.
13. L. Valiant. Universal circuits. In *Proc. 8th ACM STOC*, pages 196–203. ACM, 1976.
14. Y. Wang. PKCS: Public-key cryptography standards. In H. Bidgoli, editor, *Handbook of Information Security*, pages 966–978. Wiley, 2006.
15. A. Yao. How to generate and exchange secrets. In *Proc. 27th IEEE FOCS*, pages 162–167. IEEE, 1986.