Octonion Algebra and Noise-Free Fully Homomorphic Encryption (FHE) Schemes

Yongge Wang
Department of SIS, UNC Charlotte, USA.
yongge.wang@uncc.edu

January 28, 2016

Abstract

Brakerski showed that linearly decryptable fully homomorphic encryption (FHE) schemes cannot be secure in the chosen plaintext attack (CPA) model. In this paper, we show that linearly decryptable FHE schemes cannot be secure even in the ciphertext only security model. Then we consider the maximum security that a linearly decryptable FHE scheme could achieve. This paper designs fully homomorphic symmetric key encryption (FHE) schemes without bootstrapping (that is, noise-free FHE schemes). The proposed FHE schemes are based on quaternion/octonion algebra and Jordan algebra over finite rings $\mathbb{Z}_q$ and 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 $\mathbb{Z}_q$. It is up to our knowledge that this is the first noise-free FHE scheme that has ever been designed with a security proof (even in the weak ciphertext-only security model). It is argued that the weak ciphertext-only security model is sufficient for various applications such as privacy preserving computation in cloud. As an example, the proposed FHE schemes are used to construct obfuscated programs. This example could be further used to show that the scheme presented in this paper could be combined with existing FHE schemes with bootstrapping to obtain more efficient FHE schemes with bootstrapping in the fully CPA model. At the end of the paper, we point out the insecurity of several recently proposed noise-free FHE schemes.

1 Introduction

It had been an open question to design fully homomorphic encryption schemes (FHE) until Gentry [15] proposed a framework for 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 slow for various practical applications.

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 [5] 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.

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 [15] 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 provable 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. It is expected that the weak ciphertext-only security model for FHE is sufficient for various applications such as outsourcing of private algorithm implementations. Furthermore, for a given CPA secure FHE scheme `noiseFHE` with bootstraping, one can obtain a CPA secure FHE scheme with bootstrapping by combing the scheme `noiseFHE` with the propsoed scheme in this paper. The combined FHE scheme requires smaller parameters

for noiseFHE. Thus the combined scheme could be much more efficient.

The reader may ask whether it is possible to implement the proposed FHE scheme over finite field $\mathbb{F}_q$ with $q = p^m$ for a prime p? The answer is no. The problem of recovering a secret message for the proposed FHE scheme can be reduced to the problem of solving univariate polynomial equations. In a small size finite field $\mathbb{F}_q$, a univariate polynomial equation can be solved using the Berlekamp algorithm. For a large size finite field $\mathbb{F}_q$, efficient algorithms for factoring polynomials over finite fields (see [14] for a survey) could be used to solve univariate polynomial equations. For example, one may use the extended version of Tonelli-Shanks randomized algorithm and Cipolla's randomized algorithm.

The structure of paper is as follows. Section 2 shows that linearly decryptable FHE schemes cannot be secure in the ciphertext-only security model. Section 3 reviews octonion algebra and proves some basic results that will be used throughout the paper. Section 4 discusses octonions over finite fields $\mathbb{F}_q$ and finite rings $\mathbb{Z}_q$. Section 5 reviews the basic results regarding the automorphism group for octonions. Section 6 describes the fully homomorphic encryption scheme OctoM based on octonions. Section 7 discusses several facts regarding OctoM. Section 8 shows that the scheme OctoM is secure in the weak ciphertext-only security model assuming the hardness of solving quadratic multivariate equation systems in $\mathbb{Z}_q$. Section 9 introduces the fully homomorphic encryption scheme JordanM based on Jordan (Alberta) algebra. Section 10 describes the application of proposed FHE schemes to software obfuscation problems. Section 11 recommends some practical strategies for the FHE scheme implementation, presents sample security parameters for the proposed FHE schemes, and compares the performance of the schemes against the RSA encryption scheme. Section 12 shows that several FHE schemes (claimed as "noise-free") in the literature are insecure.

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 of V is defined as all linear combinations of vectors in V. That is, we have

$$\text{span}(V) = \left\{ \sum_{i=0}^{k-1} v_i \mathbf{a}_i : v_i \in \mathbb{Z}_q, \mathbf{a}_i \in V \right\}.$$

2 Security of linearly decryptable encryption schemes

Brakerski [5] called an encryption scheme to be linearly decryptable if the decryption circuit can be described as an inner product calculation. In the following, we

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 $\mathbb{F}_q$. It should be noted that our Inner Product Encryption Scheme IPE is different from various Inner Product Encryption Schemes used in the construction of Attribute Based Encryption (ABE) schemes in the literature.

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.

Definition 2.1 *(Ciphertext-only security 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 *generates the secret key by running* $\texttt{key} \leftarrow \texttt{xx.KeySetup}(\kappa)$ *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* xx *is said to be* (t, ε)*-secure in the ciphertext-only attack (COA) security model for* $\varepsilon = \texttt{negl}(\kappa)$ *if for all PPT algorithms* $A = (A_0, A_1)$*, we have*

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

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 2.2 *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* xx.Dec *is equivalent to* IPE.Dec *of dimension* n*. Then* 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 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. □

After proving Theorem 2.2, we 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.

Definition 2.3 *(Weak ciphertext-only security 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 *generates the secret key by running* $\mathtt{key} \leftarrow \mathtt{xx.KeySetup}(\kappa)$ *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 above experiment is defined to be 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* `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*

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

3 Octonions

Octonion (see, e.g., Baez [2]) 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. Specifically, 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 the paper, we will use the following notations for real and imaginary part of an octonion $\mathbf{a} \in \mathbb{O}$,

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

It is straightforward to check that for a complex number (or a quaternion or an octonion), 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). Though Cayley-Dickson construction provides a nice approach to study normed division algebras systematically, it is more intuitive to use vectors in $\mathbb{R}^4$ to denote quaternion numbers and vectors in $\mathbb{R}^8$ to denote octonion numbers.

Each octonion number 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

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

In the following, we first present some properties of the two associate matrices. For any octonion $\mathbf{a} = [a_0, \cdots, a_7]$, it is straightforward to show that

$$B_{\mathbf{a}}\alpha^T = B^T_{\mathbf{a}}\alpha^T = a_0\alpha^T \tag{5}$$

and

$$\begin{array}{rcl} B_{\mathbf{a}}B_{\mathbf{a}} & = & \alpha^T\alpha - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} + 2a_0B_{\mathbf{a}} \\ B^T_{\mathbf{a}}B^T_{\mathbf{a}} & = & \alpha^T\alpha - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} + 2a_0B^T_{\mathbf{a}} \\ B_{\mathbf{a}}B^T_{\mathbf{a}} & = & -\alpha^T\alpha + \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \\ B^T_{\mathbf{a}}B_{\mathbf{a}} & = & -\alpha^T\alpha + \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{array} \tag{6}$$

Thus we have

$$\begin{array}{rcl} A^l_{\mathbf{a}}A^r_{\mathbf{a}} & = & \begin{pmatrix} a_0^2 - \alpha\alpha^T & a_0\alpha + \alpha B^T_{\mathbf{a}} \\ -a_0\alpha^T - B_{\mathbf{a}}\alpha^T & -\alpha^T\alpha + B_{\mathbf{a}}B^T_{\mathbf{a}} \end{pmatrix} \\ & = & \begin{pmatrix} a_0^2 - \alpha\alpha^T & a_0\alpha + \alpha B^T_{\mathbf{a}} \\ -a_0\alpha^T - B^T_{\mathbf{a}}\alpha^T & -\alpha^T\alpha + B^T_{\mathbf{a}}B_{\mathbf{a}} \end{pmatrix} \\ & = & A^r_{\mathbf{a}}A^l_{\mathbf{a}} \\ & = & \begin{pmatrix} a_0^2 - \alpha\alpha^T & 2a_0\alpha \\ -2a_0\alpha^T & -\alpha^T\alpha + B_{\mathbf{a}}B^T_{\mathbf{a}} \end{pmatrix} \end{array} \tag{7}$$

By substituting (6) into (7), we get

$$\begin{array}{rcl} A^l_{\mathbf{a}}A^r_{\mathbf{a}} & = & A^r_{\mathbf{a}}A^l_{\mathbf{a}} \\ & = & \begin{pmatrix} 2a_0^2 - \|\mathbf{a}\|^2 & 2a_0\alpha \\ -2a_0\alpha^T & -2\alpha^T\alpha + \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{pmatrix} \end{array} \tag{8}$$

Similarly, we can get

$$\begin{array}{rcl} A^l_{\mathbf{a}}A^l_{\mathbf{a}} & = & \begin{pmatrix} a_0^2 - \alpha\alpha^T & a_0\alpha + \alpha B_{\mathbf{a}} \\ -a_0\alpha^T - B_{\mathbf{a}}\alpha^T & -\alpha^T\alpha + B_{\mathbf{a}}B_{\mathbf{a}} \end{pmatrix} \\ & = & \begin{pmatrix} 2a_0^2 - \|\mathbf{a}\|^2 & 2a_0\alpha \\ -2a_0\alpha^T & 2a_0B_{\mathbf{a}} - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{pmatrix} \\ & = & 2a_0A^l_{\mathbf{a}} - \|\mathbf{a}\|^2\mathbf{I}_{8\times 8} \end{array} \tag{9}$$

and

$$\begin{aligned} A^r_{\mathbf{a}}A^r_{\mathbf{a}} &= \begin{pmatrix} a_0^2 - \alpha\alpha^T & a_0\alpha + \alpha B_{\mathbf{a}} \\ -a_0\alpha^T - B_{\mathbf{a}}\alpha^T & -\alpha^T\alpha + B^T_{\mathbf{a}}B^T_{\mathbf{a}} \end{pmatrix} \\ &= \begin{pmatrix} 2a_0^2 - \|\mathbf{a}\|^2 & 2a_0\alpha \\ -2a_0\alpha^T & 2a_0B^T_{\mathbf{a}} - \|\mathbf{a}\|^2\mathbf{I}_{7\times 7} \end{pmatrix} \\ &= 2a_0A^r_{\mathbf{a}} - \|\mathbf{a}\|^2\mathbf{I}_{8\times 8} \end{aligned} \tag{10}$$

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 3.1 *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 3.2 *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 $(\mathbf{ab})^{-1} = (\mathbf{b}^*\mathbf{a}^*)/(\|\mathbf{a}\|^2\|\mathbf{b}\|^2)$. Since $(\mathbf{ab})^{-1} = (\mathbf{ab})^*/(\|\mathbf{ab}\|^2)$, the theorem is proved. □

Theorem 3.3 *(Moufang identities [7]) Let* $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{O}$*. Then we have*

$$\begin{aligned} \mathbf{c}(\mathbf{a}(\mathbf{cb})) &= ((\mathbf{ca})\mathbf{c})\mathbf{b} \\ \mathbf{a}(\mathbf{c}(\mathbf{bc})) &= ((\mathbf{ac})\mathbf{b})\mathbf{c} \\ (\mathbf{ca})(\mathbf{bc}) &= (\mathbf{c}(\mathbf{ab}))\mathbf{c} \\ (\mathbf{ca})(\mathbf{bc}) &= \mathbf{c}((\mathbf{ab})\mathbf{c}) \end{aligned}$$

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 construction of 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 [20, 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 [20] 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 [23] or Dembowski [9, Page 47])

$$\frac{(q^{n-k} - q^{n/2-k} + q^{n/2} - 1) \prod_{i=1}^{k-1} (q^{n-2i} - 1)}{\prod_{i=1}^{k} (q^i - 1)}, \tag{11}$$

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

$$2(q+1)(q^2+1)(q^3+1) \tag{12}$$

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 3.1 holds for $\mathbb{O}(\mathbb{Z}_q)$. We use an alternative proof to show that Theorem 3.2 holds for $\mathbb{O}(\mathbb{Z}_q)$ also. Note that the proof of Theorem 3.2 is not valid for $\mathbb{O}(\mathbb{Z}_q)$ since it uses octonion inverse properties.

Theorem 4.1 *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 $A_{\mathbf{a}^*}^r = (A_{\mathbf{a}}^r)^T$. First, the identity $\mathbf{1}\mathbf{b}^*\mathbf{a}^* = \mathbf{1}(A_{\mathbf{b}}^r)^T(A_{\mathbf{a}}^r)^T = \mathbf{1}(A_{\mathbf{a}}^r A_{\mathbf{b}}^r)^T$ implies that $\mathbf{b}^*\mathbf{a}^*$ is the first column of $A_{\mathbf{a}}^r A_{\mathbf{b}}^r$. Secondly, the identity $\mathbf{1}\mathbf{a}\mathbf{b} = \mathbf{1}(A_{\mathbf{a}}^r A_{\mathbf{b}}^r)$ implies that $(\mathbf{ab})^*$ is also the first column of $A_{\mathbf{a}}^r A_{\mathbf{b}}^r$. It follows that $(\mathbf{ab})^* = \mathbf{b}^*\mathbf{a}^*$. □

Finally, Theorem 3.1 implies the following result.

Theorem 4.2 *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 $\mathbb{O}(\mathbb{F}_q)$.

In the following, we describe some useful properties of $G_2(q)$ for the proposed homomorphic encryption scheme design. Since an automorphism group must fix the identity element $\mathbf{1}$, it needs to fix its orthogonal complement (that is, the purely imaginary octonions spanned by $i_1, \cdots, i_7$). Thus $G_2(q)$ is a subgroup of the orthogonal group $\mathrm{O}(7, \mathbb{Z}_q)$ of 7×7 orthogonal matrices over $\mathbb{Z}_q$. On the other hand, given the images of two octonions $\mathbf{e}_1, \mathbf{e}_2 \in \mathrm{Im}(\mathbb{O}(\mathbb{Z}_q))$, the image of $\mathbf{e}_1\mathbf{e}_2$ is fixed. Thus $G_2(q)$ is a proper subgroup of the special orthogonal group $\mathrm{SO}(7, \mathbb{Z}_q)$ of 7×7 orthogonal matrices of determinant 1 over $\mathbb{Z}_q$.

Given vector spaces V_1, V_2, V_3 over $\mathbb{Z}_q$, a triality is a trilinear map

$$t : V_1 \times V_2 \times V_3 \to \mathbb{Z}_q$$

that is non-degenerate (see, e.g., Lounesto [22]). That is, if we fix two arguments to non-zero values, then the linear map induced on the third vector space is non-zero. A normed triality is a collection of inner product spaces V_1, V_2, V_3 over $\mathbb{Z}_q$ with a triality map t having the property $|t(v_1, v_2, v_3)| \leq \|v_1\|\|v_2\|\|v_3\|$ and for all v_1, v_2, there exists $v_3 \neq 0$ for which the bound is attained. An automorphism of a normed triality t is a triple of norm-preserving maps $f_i : V_i \to V_i$ such that $t(f_1(v_1), f_2(v_2), f_3(v_3)) = t(v_1, v_2, v_3)$. These automorphisms form a group $\mathrm{Aut}(t)$.

Let V_8 be the vector space of $\mathbb{Z}_q^8$ and let $S_8^+ = \mathbb{Z}_q^8$ and $S_8^- = \mathbb{Z}_q^8$ denote the right-handed and left-handed spinor representations. Then there is a normed triality map

$$t_8 : V_8 \times S_8^+ \times S_8^- \to \mathbb{Z}_q$$

that gives $\mathbb{O}(\mathbb{Z}_q)$ (see, e.g., Baez [2]). In particular, we have

$$G_2(q) \subset \text{Aut}(t_8) = \text{Spin}(8, \mathbb{Z}_q)$$

where the spin group $\text{Spin}(8, \mathbb{Z}_q)$ consists of all products of even number unit vectors in $\mathbb{Z}_q^8$ and $\text{Spin}(8, \mathbb{Z}_q)$ is a double cover of the special orthogonal group $\text{SO}(8, \mathbb{Z}_q)$. Octonions can be constructed from t_8 by fixing unit vectors in any of the two vector spaces. Thus $G_2(q)$ can be considered as a subgroup of $\text{Spin}(8, \mathbb{Z}_q)$ fixing unit vectors in V_8 and S_8^+. The subgroup of $\text{Spin}(8, \mathbb{Z}_q)$ fixing a unit vector in V_8 is isomorphic to $\text{Spin}(7, \mathbb{Z}_q)$ and, by restricting the representation S_8^+ to $\text{Spin}(7, \mathbb{Z}_q)$, we get the spinor representation S_7. Thus $G_2(q)$ is isomorphic to the subgroup of $\text{Spin}(7, \mathbb{Z}_q)$ fixing a unit vector in S_7. That is, $\text{Spin}(7, \mathbb{Z}_q)/G_2(q) = S^7$ where S^7 is the sphere with dimension 7. It follows that the dimension of $G_2(q)$ is

$$\dim(\text{Spin}(7, \mathbb{Z}_q)) - \dim S^7 = 21 - 7 = 14.$$

A subgroup H of a group G is said to be normal if it is the union of whole conjugacy classes in G. The group G is simple if it has only two trivial normal subgroups 1 and G. It can be shown that $G_2(q)$ is simple for $q \neq 2$. Generally, the structure of $G_2(q)$ is characterized by the following theorem.

Theorem 5.1 *(See e.g., [2]) The compact real form of the Lie algebra $\mathfrak{g}_2$ is given by*

$$\mathfrak{g}_2 = \mathfrak{Der}(\mathbb{O}) \subset \mathfrak{so}(\text{Im}(\mathbb{O})) \subset \mathfrak{so}(\mathbb{O})$$

where $\mathfrak{so}(\text{Im}(\mathbb{O})) = \mathfrak{Der}(\mathbb{O}) \oplus \text{ad}_{\text{Im}(\mathbb{O})}$ and $\mathfrak{so}(\mathbb{O}) = \mathfrak{Der}(\mathbb{O}) \oplus L_{\text{Im}(\mathbb{O})} \oplus R_{\text{Im}(\mathbb{O})}$ are built from natural bilinear operations on the summands, $L_{\text{Im}(\mathbb{O})}$ is the space of linear transformations of $\mathbb{O}$ given by left multiplication by imaginary octonions, $R_{\text{Im}(\mathbb{O})}$ is the space of linear transformations of $\mathbb{O}$ given by right multiplication by imaginary octonions, and $\mathbf{ad}_a = L_a - R_a$.

Theorem 5.1 still holds if octonions $\mathbb{O}$ over $\mathbb{R}$ is replaced by octonions $\mathbb{O}(\mathbb{Z}_q)$ over $\mathbb{Z}_q$. Thus $G_2(q)$ has a 7-dimensional representation $\text{Im}(\mathbb{O}(\mathbb{Z}_q))$.

A vector-valued product of two vectors is called a cross product if the vector is orthogonal to the two vectors and has length equal to the parallelogram formed by the two vectors. A cross product of two vectors exists only in the 3 dimensional and 7 dimensional spaces (see, e.g., Lounesto [22]). Though the 3-dimensional cross product is invariant under all rotations of $SO(3)$, the 7-dimensional cross

product is not invariant under all rotations of $SO(7)$. Indeed, the 7-dimensional cross product is only invariant under the proper subgroup G_2 of $SO(7)$.

Furthermore, $\mathrm{Im}(\mathbb{O}(\mathbb{Z}_q))$ has three natural structures that are preserved by automorphisms in $G_2(q)$. First, a linear transformation of $\mathrm{Im}(\mathbb{O}(\mathbb{Z}_q))$ preserves the cross product on $\mathrm{Im}(\mathbb{O}(\mathbb{Z}_q))$ if and only if it is an element of $G_2(q)$. Second, let $\phi(x, y, z) = \langle x, yz\rangle$ be an alternating trilinear functional over $\mathrm{Im}(\mathbb{O}(\mathbb{Z}_q))$. Then a linear transformation of $\mathrm{Im}(\mathbb{O}(\mathbb{Z}_q))$ preserves ϕ if and only if it is an element of $G_2(q)$. Third, let $[x, y, z] = (xy)z - x(yz)$ be the trilinear associator over $\mathrm{Im}(\mathbb{O}(\mathbb{Z}_q))$. Then a linear transformation T of $\mathrm{Im}(\mathbb{O}(\mathbb{Z}_q))$ preserves the associator $[\cdot, \cdot, \cdot]$ if and only if both T and $-T$ are elements of $G_2(q)$.

We conclude this section by showing how to select and represent an element in $G_2(q)$. 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 4.2, 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 $\mathbf{z} \in \mathbb{Z}_q^8$, $\mathrm{span}\{\mathbf{z}\}$ is a dimension one totally isotropic subspace that is closed under octonion multiplications. The comment 3 in Section 7 will show that there exist dimension two totally isotropic subspaces that are closed under octonion multiplications. By formulas (11) and (12) 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 $q = p_1p_2p_3p_4$. The protocol could be implemented over any finite rings $\mathbb{Z}_q$ with $q = p_1^{r_1} \cdots p_m^{r_m}$ and $m \geq 3$.

Key Setup. Select $q = p_1p_2p_3p_4$ according to the given security parameter κ and let $q_0 = p_1p_2$. 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 (q_0, K, ϕ, V) and the system public parameter is $\mathbb{Z}_q$.

Encryption. For a message $m \in \mathbb{Z}_{q_0}$, choose random $r \in \mathbb{Z}_q$ and $\mathbf{z} \in V$ with the property that $|A^l_{\mathbf{m}'}| = 0$, where $\mathbf{m}' = \phi\left((m + rq_0)\mathbf{1} + \mathbf{z}\right)$ 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., [6]). Let the ciphertext

$$C_m = \texttt{OctoM.Enc}(\texttt{key}, m) = K^{-1}A^l_{\mathbf{m}'}K \in \mathbb{Z}_q^{8\times 8}.$$

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

$$m = \texttt{OctoM.Dec}(\texttt{key}, C_m) = \phi^{-1}(\mathbf{1}(KC_mK^{-1})) \mod V \mod q_0.$$

It should be noted that $\mathbf{1}(KC_mK^{-1}) = \mathbf{1}A_{\mathbf{m}'} = \mathbf{m}'$.

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 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.

$$
\begin{aligned}
& \texttt{OctoM.Dec}(\texttt{key}, C_{m_0 m_1}) \\
= \;& \phi^{-1}(\mathbf{1}(A^l_{\mathbf{m}'_1} A^l_{\mathbf{m}'_0})) \mod V \mod q_0 \\
= \;& \phi^{-1}(\mathbf{m}'_0(\mathbf{m}'_1\mathbf{1})) \mod V \mod q_0 \\
= \;& \phi^{-1}(\mathbf{m}'_0\mathbf{m}'_1) \mod V \mod q_0 \\
= \;& \phi^{-1}(\phi\left(m_0\mathbf{1} + r_0 q_0 \mathbf{1} + \mathbf{z}_0\right)\phi\left(m_1\mathbf{1} + r_1 q_0 \mathbf{1} + \mathbf{z}_1\right)) \mod V \mod q_0 \\
= \;& \left(m_0\mathbf{1} + r_0 q_0 \mathbf{1} + \mathbf{z}_0\right)\left(m_1\mathbf{1} + r_1 q_0 \mathbf{1} + \mathbf{z}_1\right) \mod V \mod q_0 \\
= \;& (m_0 + r_0 q_0)(m_1 + r_1 q_0)\mathbf{1} \mod q_0 \\
= \;& m_0 m_1 \mathbf{1}.
\end{aligned}
$$

We conclude this section by showing that the decryption process of OctoM is weakly equivalent to the decryption process IPE.Dec of a dimension 64 IPE scheme of Section 2. Let $\texttt{key} = (q_0, K, \phi, V) = \texttt{OctoM.KeySetup}(\kappa)$ be the secret key of the encryption scheme OctoM. Let $\beta = [1, b_1, \cdots, b_7] \in \mathbb{Z}_q^8$ be a vector that is orthogonal to $\phi(V)$. Then we have $\phi((m + rq_0)\mathbf{1} + \mathbf{z})\beta^T = m$. 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

$$
\begin{aligned}
m + rq_0 &= \phi((m + rq_0)\mathbf{1} + \mathbf{z})\beta^T \\
&= (\mathbf{1} K C_m K^{-1})\beta^T \\
&= \left[\textstyle\sum_{i,j=0}^{7} a_{0,i,j} c_{i,j}, \cdots, \sum_{i,j=0}^{7} a_{7,i,j} c_{i,j}\right] \beta^T \\
&= \textstyle\sum_{i,j=0}^{7} k_{i,j} c_{i,j} \\
&= \mathbf{k} \cdot \mathrm{vec}(C_m) \\
&= \texttt{IPE.Dec}(\mathbf{k}, \mathrm{vec}(C_m))
\end{aligned}
\tag{13}
$$

for some $a_{0,i,j}, \cdots, a_{7,i,j} \in \mathbb{Z}_q$ and $\mathbf{k} = [k_{0,0}, \cdots, k_{0,7}, k_{1,0}, \cdots, k_{7,7}] \in \mathbb{Z}_q^{64}$. From $m + rq_0$, one still needs the value q_0 to recover the plaintext message m.

Given n linearly independent ciphertexts $\mathbf{c}_i$ with known plaintext messages m_i, one can recover the private key $\mathbf{k}$ of a dimension n IPE scheme. However, the private key K for OctoM could be recovered only if one has n linearly independent ciphertexts $\mathbf{c}_i$ together with corresponding values $m_i + r_i q_0$. Thus we say that OctoM.Dec is weakly equivalent to IPE.Dec. At the end of Section 8, we will show that one can actually recover the IPE decryption key $\mathbf{k}$ for OctoM from plaintext-ciphertext pairs $(m_i, \mathbf{c}_i)$ without knowing $r_i q_0$.

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 scheme OctoM, a message m is encoded to an octonion $\mathbf{m}' = \phi((m+rq_0)\mathbf{1}+\mathbf{z})$ and $\mathbf{m}'$ is converted to an associated matrix. The associated matrix is further multiplied using private matrices from both sides. The reader may be curious and ask what happens if we directly encrypt an octonion message $\mathbf{m} \in \mathbb{Z}_q^8$ to $K^{-1}A^l_{\mathbf{m}}K$ without employing the first encoding $\mathbf{m}' = \phi((m + rq_0)\mathbf{1} + \mathbf{z})$? That is, the plaintext space is the collection of octonion numbers in $\mathbb{O}(\mathbb{Z}_q)$ instead of numbers in $\mathbb{Z}_q$. Though the resulting scheme is additive homomorphic, it is not multiplicative homomorphic. Let $\mathbf{m}_0, \mathbf{m}_1, \mathbf{m}_2$ be octonions such that $\mathbf{m}_0(\mathbf{m}_1\mathbf{m}_2) \neq (\mathbf{m}_0\mathbf{m}_1)\mathbf{m}_2$. By definition, we have

$$\begin{array}{rcl} \texttt{OctoM.Dec}(\texttt{key}, C_{\mathbf{m}_2}C_{\mathbf{m}_0\mathbf{m}_1}) & = & \texttt{OctoM.Dec}(\texttt{key}, K^{-1}A^l_{\mathbf{m}_2}A^l_{\mathbf{m}_1}A^l_{\mathbf{m}_0}K) \\ & = & \mathbf{1}A^l_{\mathbf{m}_2}A^l_{\mathbf{m}_1}A^l_{\mathbf{m}_0} \\ & = & \mathbf{m}_0(\mathbf{m}_1\mathbf{m}_2) \\ & \neq & (\mathbf{m}_0\mathbf{m}_1)\mathbf{m}_2 \end{array} \tag{14}$$

It follows that $C_{(\mathbf{m}_0\mathbf{m}_1)\mathbf{m}_2} \neq C_{\mathbf{m}_2}C_{\mathbf{m}_0\mathbf{m}_1}$.

Comment 2: In the encryption scheme OctoM, the message m is encoded to $\mathbf{m}' = \phi((m + rq_0)\mathbf{1} + \mathbf{z})$ with a randomly selected $r \in \mathbb{Z}_q$ and 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 $V = \text{span}\{\mathbf{z}_0\}$. That is, each message m is encoded to $\mathbf{m}' = \phi((m + rq_0)\mathbf{1} + r'\mathbf{z}_0)$ for randomly selected $r, r' \in \mathbb{Z}_q$.

It is natural to ask whether it is possible to randomly select two independent isotropic octonions $\mathbf{z}_0, \mathbf{z}_1$ from which a subspace V is constructed for the encoding process? Generally, the answer is no. In order for the encoding process to be multiplicative homomorphic, V needs to be closed under octonion multiplications. By the fact that octonion algebra is alternative, the subspace

$$V = \text{span}\{\mathbf{z}_0, \mathbf{z}_1, \mathbf{z}_0\mathbf{z}_1, \mathbf{z}_1\mathbf{z}_0, \mathbf{z}_1\mathbf{z}_0\mathbf{z}_1, \mathbf{z}_0\mathbf{z}_1\mathbf{z}_0\}$$

is closed under octonion multiplications. Though the above V has a basis consisting of isotropic vectors and is closed under octonion multiplications, it may not be a totally isotropic subspace. That is, there may exist an octonion $\mathbf{z} \in V$ with $\|\mathbf{z}\| \neq 0$. By Theorem 3.1, we have $\mathbf{z}^2 = 2\text{Re}(\mathbf{z})\mathbf{z} - \|\mathbf{z}\|^2\mathbf{1}$. Since $\mathbf{z}^2 \in V$ and V is a linear subspace, we have $\mathbf{1} \in V$. Assume that a message m is encoded as $\mathbf{m}' = \phi((m + rq_0)\mathbf{1} + \mathbf{r})$ where $\mathbf{r}$ is randomly selected from V. For any $m' \in \mathbb{Z}_q$,

we have $\mathbf{r}' = \mathbf{r} - m'\mathbf{1} \in V$. Thus

$$(m + rq_0)\mathbf{1} + \mathbf{r} = (m + m' + rq_0)\mathbf{1} + \mathbf{r}' \mod V.$$

That is, $\mathbf{m}'$ could not be decoded to m uniquely in case $\mathbf{1} \in V$.

Comment 3: 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

$$\begin{aligned} \|r_0\mathbf{z}_0 + r_1\mathbf{z}_1\|^2 &= (r_0\mathbf{z}_0 + r_1\mathbf{z}_1)(r_0\mathbf{z}_0^* + r_1\mathbf{z}_1^*) \\ &= r_0r_1\mathbf{z}_0\mathbf{z}_1^* + r_0r_1\mathbf{z}_1\mathbf{z}_0^* \\ &= r_0r_1(\mathbf{z}_0\mathbf{z}_1^* + (\mathbf{z}_0\mathbf{z}_1^*)^*) \\ &= 2r_0r_1\mathrm{Re}(\mathbf{z}_0\mathbf{z}_1^*). \end{aligned}$$

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

$$\|\mathbf{z}_0\| = \|\mathbf{z}_1\| = \mathrm{Re}(\mathbf{z}_0\mathbf{z}_1^*) = 0, \tag{15}$$

the subspace $\mathrm{span}(\mathbf{z}_0, \mathbf{z}_1)$ 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 (15) holds and there exist $r_0, r_1, r_2, r_3 \in \mathbb{Z}_q$ satisfying

$$\begin{aligned} \mathbf{z}_0\mathbf{z}_1 &= r_0\mathbf{z}_0 + r_1\mathbf{z}_1 \\ \mathbf{z}_1\mathbf{z}_0 &= r_2\mathbf{z}_0 + r_3\mathbf{z}_1 \end{aligned} \tag{16}$$

Combing identities (15) and (16), 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.

Comment 4: In the FHE scheme `OctoM`, the automorphism $\phi \in G_2(q)$ in the private key introduces randomness in the message encoding process. That is, the totally isotropic subspace V is mapped to another totally isotropic subspace $\phi(V)$. However, the scheme should still be secure if ϕ is not used.

Comment 5: The scheme `OctoM` recommends the use of "$q = p_1p_2p_3p_4$ and $q_0 = p_1p_2$". Alternatively, we may also use "$q = p_1p_2p_3$ and $q_0 = p_1$" or "$q = q_0 = p_1p_2$" in the parameter selection process. Furthermore, one may also use $q_0 = 2$ to obtain an FHE scheme that only encrypts binary messages. The security proof in next sections works for these parameter choices also.

8 Proof of Security

The preceding section shows that the decryption process of the scheme OctoM is weakly 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 and session randomness (that is, $m + rq_0$). Furthermore, by Theorem 2.2, 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 weakly 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 8.1 *Let κ be the security parameter, $n \leq t \leq poly(\kappa)$, 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 the weak ciphertext-only security model.*

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 $\mathbf{k} = [k_0, \cdots, k_{n-1}]$:

$$\mathbf{k}[\mathbf{c}_0^T, \cdots, \mathbf{c}_{t-1}^T] = \mathbf{m}. \tag{17}$$

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 (17) 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 (17). 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 8.2 *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* $\mathrm{vec}(C_m^0) = \mathrm{vec}(\mathbf{I}), \mathrm{vec}(C_m^1), \cdots, \mathrm{vec}(C_m^8)$ *are linearly dependent.*

Proof. For an $n \times n$ matrix $A \in \mathbb{Z}_q^{n \times n}$, the minimal polynomial of A is the monic polynomial $\mu_A(x)$ over $\mathbb{Z}_q$ of the least degree such that $\mu_A(A) = 0$. The minimal polynomial $\mu_A(x)$ is a divisor of A's characteristic polynomial

$$p_A(x) = \det(x\mathbf{I} - A) = x^n - \mathrm{tr}(A)x^{n-1} + \cdots + (-1)^n \det(A).$$

This implies that the minimal polynomial of C_m has a degree less than or equal to 8. The Claim is proved. □

It is known that (see, e.g., [12, 13, 27]), with probability $(1 - 1/q^5)/(1 + 1/q^3)$, the characteristic polynomial of a random matrix over $\mathbb{F}_q$ is equal to its minimal polynomial for large enough q. This implies that with high probability, $\mathrm{vec}(C_m^0), \mathrm{vec}(C_m^1), \cdots, \mathrm{vec}(C_m^7)$ are linearly independent for a ciphertext C_m. Furthermore, by the fact that the characteristic polynomial $p_A(x)$ is invariant under matrix equivalence transformations, we have

$$\mathrm{tr}(C_m) = \mathrm{tr}(A_{\mathbf{m}}^l) = 8(m + rq_0 + \mathrm{Re}(\mathbf{z})) \tag{18}$$

where r and $\mathbf{z}$ are randomly chosen in the OctoM encryption process.

Theorem 8.3 *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* 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 8.1, 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 8.1 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 (q_0, 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 8.4 *Given t ciphertexts for the FHE scheme* `OctoM`*, the problem of finding the private key (q_0, 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 $KC_m = A^l_{\mathbf{m}'}K$. If we assign 8 variables for $\mathbf{m}' = m + rq_0 + \mathbf{r}$ 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 $m + rq_0$. 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 $\mathbf{m}' = \phi((m + rq_0)\mathbf{1} + \mathbf{r}) = [m_0, \cdots, m_7]$ where $\mathbf{r} \in V$. From the identity $KC_m = A^l_{\mathbf{m}'}K$ for the ciphertext C_m and from the identity (9), we have

$$\begin{aligned}
&C_m = K^{-1}A^l_{\mathbf{m}'}K \\
&C^2_m = K^{-1}(2m_0A^l_{\mathbf{m}'} - \|\mathbf{m}'\|^2 I_{8\times 8})K \\
&C^3_m = K^{-1}((4m_0^2 - \|\mathbf{m}'\|^2)A^l_{\mathbf{m}'} - 2m_0\|\mathbf{m}'\|^2 I_{8\times 8})K \\
&C^4_m = K^{-1}((8m_0^3 - 4m_0\|\mathbf{m}'\|^2)A^l_{\mathbf{m}'} - (4m_0^2 - \|\mathbf{m}'\|^2)\|\mathbf{m}'\|^2 I_{8\times 8})K \\
&\cdots
\end{aligned} \tag{19}$$

where $C^i_m = \texttt{OctoM.Enc}(K, m^i)$. This implies that

$$\begin{aligned}
&KC_m = A^l_{\mathbf{m}'}K \\
&KC^2_m = (2m_0A^l_{\mathbf{m}'} - \|\mathbf{m}'\|^2 I_{8\times 8})K \\
&KC^3_m = ((4m_0^2 - \|\mathbf{m}'\|^2)A^l_{\mathbf{m}'} - 2m_0\|\mathbf{m}'\|^2 I_{8\times 8})K \\
&KC^4_m = ((8m_0^3 - 4m_0\|\mathbf{m}'\|^2)A^l_{\mathbf{m}'} - (4m_0^2 - \|\mathbf{m}'\|^2)\|\mathbf{m}'\|^2 I_{8\times 8})K \\
&\cdots
\end{aligned} \tag{20}$$

which further implies

$$\begin{array}{l} KC_m^2 = 2m_0 KC_m - \|\mathbf{m}'\|^2 K \\ KC_m^3 = (4m_0^2 - \|\mathbf{m}'\|^2) KC_m - 2m_0 \|\mathbf{m}'\|^2 K \\ KC_m^4 = (8m_0^3 - 4m_0 \|\mathbf{m}'\|^2) KC_m - (4m_0^2 - \|\mathbf{m}'\|^2)\|\mathbf{m}'\|^2 K \\ \cdots \end{array} \tag{21}$$

It is straightforward to check that the identities in (21) are dependent and the only independent identity that one can get is $KC_m^2 = 2m_0 KC_m - \|\mathbf{m}'\|^2 K$. In other words, if we consider $\|\mathbf{m}'\|^2$ as one variable, the identities (21) 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 8.5 *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 polynomial equation of degree at most* 8*.*

Proof. Let $C = \texttt{OctoM.Enc}(\texttt{key}, m) \in \mathbb{Z}_q^{8\times 8}$. By the multiplicative homomorphic property of `OctoM`, we have

$$C^i = \texttt{OctoM.Enc}(\texttt{key}, m^i) \in \mathbb{Z}_q^{8\times 8} \tag{22}$$

for all integers $i \geq 1$. Let $\mathbf{c}_i = \texttt{vec}(C^i)$ and $\mathbf{c}_0 = \texttt{vec}(\mathbf{I})$. By the identity (22) and by the relationship between `OctoM` and `IPE`, there exists $\mathbf{k} \in \mathbb{Z}_q^{64}$ such that $(m + rq_0)^i = \mathbf{k}\mathbf{c}_i^T$ for $i \geq 1$. By the the minimal polynomial arguments in the proof of Lemma 8.2, the ciphertexts $\mathbf{c}_0, \mathbf{c}_2, \ldots, \mathbf{c}_8$ are linearly dependent. Let $x = m + rq_0$. Then we have

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_8 x^8 = 0 \tag{23}$$

for some $a_0, \cdots, a_8 \in \mathbb{Z}_q$. This completes the proof of the Claim. □

By Claims 8.4 and 8.5, in order for one to recover the secret key or secret messages from the ciphertexts, one needs to solve a degree 8 univariate polynomial equation in Claim 8.5 or to solve the multivariate equation system in Claims 8.4. By the assumption, it is computationally infeasible to solve univariate nonlinear polynomial equations over $\mathbb{Z}_q$ obtained in Claim 8.5. In the following, we show that it is computationally infeasible to solve the multivariate equation systems obtained in Claims 8.4.

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 $x_i x_j$ 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 [18] 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 8.4, there are $64t$ (not necessarily homogeneous) quadratic equations in $64 + 2t$ variables. Thus the relinearization algorithm in Kipnis and Shamir [18] might be applied to the equation system in Claim 8.4 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 8.4 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., [24]). 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). In the following, we briefly describe the Gröbner basis algorithm for the quadratic equation systems constructed in Claim 8.4.

The Gröbner basis eliminates top order monomial (in a given order such as lexicographic order) by combining two equations with appropriate coefficients. This process continues until one obtains a univariate polynomial equation. The resulting univariate polynomial equation normally has a very high degree and Buchberger's algorithm runs in exponential time on average (the worst case complexity is double exponential time). Thus Buchberger's algorithm cannot solve quadratic equation systems with more than 20 variables in practice (see, e.g., Courtois et al [8]). But it should also be noted that though the worst-case Gröbner basis algorithm is double exponential, the generic behavior is generally much better. In particular, if the algebraic system has only a finite number of common zeros at infinity, then Gröbner basis algorithm for any ordering stops in a polynomial time in d^n where $d = \max\{d_i : d_i \text{ is the total degree of } f_i\}$ and n is the number of variables (see,

e.g., [3]).

There are a few improved variants of Buchberger's algorithm. For example, Faugere introduced the F_4 [11] and F_5 [10] algorithms. Courtois et al [8] introduced XL (eXtended linearization) techniques which are a combination of bounded degree Gröbner basis and linearization. Ars [1] showed that XL is a redundant version of F_4. For a reasonable large size ring $\mathbb{Z}_q$, the complexity of F_4 and F_5 is at least $O(2^{2.7n})$ for n variables. Thus they are not practical for cryptanalysis of the encryption scheme `OctoM` in the ciphertext-only security model with the multivariate equation systems constructed in Claim 8.4 (where $n = 64 + 2t$). Similarly, algorithms F_4, F_5, and XL are not effective for the cryptanalysis of `OctoM` with the multivariate quadratic equation systems constructed in Claim 8.4. Furthermore, 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 a summary, with the assumption of the theorem, it is computationally infeasible to solve the equation systems constructed in Claim 8.4. The theorem is proved. □

We conclude this section by showing that the scheme `OctoM` is insecure when sufficiently many plaintext-ciphertext pairs are known.

Theorem 8.6 *Given plaintext-ciphertext pairs* $(m_1, \mathbf{c}_1), \cdots, (m_t, \mathbf{c}_t)$ *of the FHE scheme* `OctoM`*, one may recover the equivalent* `IPE` *decryption key* $\mathbf{k}$ *for* `OctoM.Dec` *and recover the factor* q_0 *of* q*.*

Proof. For the plaintext-ciphertext pairs $(m_1, \mathbf{c}_1), \cdots, (m_t, \mathbf{c}_t)$, one may use the full homomorphism property to obtain further plaintext-ciphertext pairs

$$(f(m_1, \cdots, m_t), \mathbf{c}_f)$$

where f is a multivariate polynomial. Without loss of generality, we may assume that we have obtained 64 linearly independent ciphertext $\mathbf{c}_1, \cdots, \mathbf{c}_{64}$ for the encoded messages $m_1 + r_1 q_0, \cdots, m_{64} + r_{64} q_0$ respectively, where $r_1, \cdots, r_{64}, q_0$ are unknowns. Then the `IPE` decryption key $\mathbf{k}$ could be expressed as polynomials in $(r_1, \cdots, r_{64}, q_0)$:

$$\mathbf{k} = [m_1 + r_1 q_0, \ldots, m_{64} + r_{64} q_0][\mathbf{c}_1^T, \ldots, \mathbf{c}_{64}^T]^{-1}. \tag{24}$$

That is, for each $1 \leq i \leq 64$, we have $k_i = a_i + r_i' q_0$ for unknowns $r_i', q_0 \in \mathbb{Z}_q$ and a known value a_i. Let $\mathbf{c} = [c_1, \cdots, c_{64}]$ be the ciphertext of a known message m, then we have

$$m + r q_0 = \mathbf{k}\mathbf{c}^T = b + r' q_0$$

for some $r, r' \in \mathbb{Z}_q$ and the values of b, m are known. In other words, we have

$$m - b = (r - r')q_0 \mod q,$$

which implies $q_0|(m-b)$. In case that $m - b \neq 0 \mod q$, one can recover q_0 as $q_0 = \gcd(q, m-b)$. The value of q_0 together with the identity $k_i = a_i + r'_i q_0$ could be used to decrypt any ciphertext. □

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. In this section, we investigate these possibilities.

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 $\mathbb{C}$ (see, Kestelman [17] and Yale [32]). For $\mathbb{H}$, the norm preserving automorphism is the group of real-linear transformations of 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 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 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 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 [20, 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 (11), 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 8.4 could be used to construct a quadratic equation system of $16t$ equations in $16 + 2t$ unknown variables. 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

$$\det \begin{bmatrix} a & \mathbf{c} & \mathbf{b} \\ \mathbf{c}^* & b & \mathbf{a} \\ \mathbf{b}^* & \mathbf{a}^* & c \end{bmatrix} = abc - (a\|\mathbf{a}\|^2 + b\|\mathbf{b}\|^2 + c\|\mathbf{c}\|^2) + 2\mathrm{Re}(\mathbf{abc})$$

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 symmetric key encryption scheme `JordanM`.

Key Setup. Select $q = p_1p_2p_3p_4$ according to the given security parameter κ and let $q_0 = p_1p_2$. Randomly select isotropic vectors $\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3 \in \mathbb{O}(\mathbb{Z}_q)$ satisfying the following identity

$$\mathbf{z}_2\mathbf{z}_1^* = \mathbf{z}_3 \quad \text{and} \quad \mathrm{Re}(\mathbf{z}_1\mathbf{z}_2\mathbf{z}_3) \neq 0 \tag{25}$$

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 (25) 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 $\mathtt{key} = (q_0, \phi, K, \mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3)$.

Encryption. For a message $m \in \mathbb{Z}_{q_0}$, 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

$$E_m = (m + rq_0, r_4, r_5, r_1\mathbf{z}_1, r_2\mathbf{z}_2, r_3\mathbf{z}_3) = \begin{bmatrix} m + rq_0 & r_3\mathbf{z}_3 & r_2\mathbf{z}_2 \\ r_3\mathbf{z}_3^* & r_4 & r_1\mathbf{z}_1 \\ r_2\mathbf{z}_2^* & r_1\mathbf{z}_1^* & r_5 \end{bmatrix}.$$

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

$$m = \mathtt{JordanM.Dec}(\mathtt{key}, C_m) = \mathbf{1}\phi^{-1}(KC_mK^{-1})\mathbf{1}^T \mod q_0.$$

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 (25), 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 4.1, the multiplication homomorphism of `JordanM` follows from the following equations

$$
\begin{aligned}
E_{m_0} \circ E_{m_1} &= \begin{bmatrix} m_0 + r_0 q_0 & r_{0,3}\mathbf{z}_3 & r_{0,2}\mathbf{z}_2 \\ r_{0,3}\mathbf{z}_3^* & r_{0,4} & r_{0,1}\mathbf{z}_1 \\ r_{0,2}\mathbf{z}_2^* & r_{0,1}\mathbf{z}_1^* & r_{0,5} \end{bmatrix} \circ \begin{bmatrix} m_1 + r_1 q_0 & r_{1,3}\mathbf{z}_3 & r_{1,2}\mathbf{z}_2 \\ r_{1,3}\mathbf{z}_3^* & r_{1,4} & r_{1,1}\mathbf{z}_1 \\ r_{1,2}\mathbf{z}_2^* & r_{1,1}\mathbf{z}_1^* & r_{1,5} \end{bmatrix} \\
&= \begin{bmatrix} m_0 m_1 + r q_0 & x_1\mathbf{z}_3 + x_2\mathbf{z}_2\mathbf{z}_1^* & x_3\mathbf{z}_2 + x_4\mathbf{z}_3\mathbf{z}_1 \\ x_1\mathbf{z}_3^* + x_2\mathbf{z}_1\mathbf{z}_2^* & r_{0,4}r_{1,4} & x_5\mathbf{z}_1 + x_6\mathbf{z}_3^*\mathbf{z}_2 \\ x_3\mathbf{z}_2^* + x_4\mathbf{z}_1^*\mathbf{z}_3^* & x_5\mathbf{z}_1^* + x_6\mathbf{z}_2^*\mathbf{z}_3 & r_{0,5}r_{1,5} \end{bmatrix} \\
&= \begin{bmatrix} m_0 m_1 + r q_0 & (x_1 + x_2)\mathbf{z}_3 & x_3\mathbf{z}_2 \\ (x_1 + x_2)\mathbf{z}_3^* & r_{0,4}r_{1,4} & x_5\mathbf{z}_1 \\ x_3\mathbf{z}_2^* & x_5\mathbf{z}_1^* & r_{0,5}r_{1,5} \end{bmatrix}
\end{aligned}
$$

for some $x_1, \cdots, x_6, r \in \mathbb{Z}_q$.

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 $\mathrm{tr}(A) = 1$. That is, ϕ is defined by

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

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 [2]), 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.

Theorem 9.1 *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 $t \leq poly(\kappa)$.*

Proof. For given t ciphertexts of the scheme `JordanM`, the approach in the proof of Claim 8.4 could be used to construct a quadratic equation system of $72t$ equations in $9+27t$ (or $25+6t$) unknown variables. The other parts in the proof of Theorem 8.3 remain the same for the proof of this theorem. □

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 Applications of FHE schemes in ciphertext-only security model

The efficient FHE schemes designed in this paper are expected to have a wide range of applications. In this section, we show its potential applications in software obfuscation and outsourced implementation of software with protected algorithms. Software obfuscation concept has been introduced many years ago. For example, it has already been presented in Diffie-Hellman (1976) invention of public key cryptography. In this paper, we consider a special case of the reusable software obfuscation 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.

The essential difference between the above software obfuscation problem and the general software obfuscation problem in the literature is that the cloud does not

need to learn the software inputs and outputs in our case. However, for the general software obfuscation problem, the evaluator should be able to run the obfuscated software on his own inputs and learn the actual outputs.

In this section, we show how to use FHE schemes proposed in this paper to solve the above reusable software obfuscation problem. The general one-time private software evaluation problem has been solved by Yao [33] using the concept of garbled circuits. Yao's garbled circuit 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 $f(x)$. However, Yao's garbled circuits are not re-usable and a garbled circuit could only be run once. The goal of this section is to design reusable garbled circuits.

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 an 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 [19, 25]. 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 Efficient FHE applied to software obfuscation and more efficient FHE scheme in CPA model

For the software obfuscation problem 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 the reusable garbled software as $\mathcal{C} = \texttt{FHE.Enc}(\texttt{key}, C)$ and uploads $\mathcal{C}$ to the cloud.
- For each evaluation, the software owner provides the 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 software owner decrypts the actual output:

$$C(x) = \texttt{FHE.Dec}(\texttt{key}, \texttt{FHE.Enc}(\texttt{key},C(x))).$$

10.3 Efficient FHE scheme in the fully secure CPA model

Existing CPA secure FHE schemes with noise generally have very large parameters to keep the scheme secure. For example, for the FHE scheme `FHEint` over integers [26], the module prime p is required to be at least 16000 bits. However, if combined with our scheme `OctoM`, one can choose smaller modules and the bootstrapping process could be much more efficient when the bootstrapping process is considered

as a software obfuscation problem as we have dicussed in the preceeding section. The resulting scheme could be shown to be secure in the standard CPA model (note that the resulting scheme is then a secret key scheme instead of a public key scheme).

11 Practical considerations

11.1 Dictionary attacks

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.

11.2 Bits of Security

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 [4] recommends the security strength of $\mathbb{Z}_q$ for $q = p_1 p_2$. For the FHE schemes proposed in this paper, we recommend the use of $q = p_1 p_2 p_3 p_4$. Hinek [16] and Wang [28] list the security strength of $\mathbb{Z}_q$ when q is a multiplication of more than two primes. Following [4, 16, 28], we recommend the use of ring sizes for $\mathbb{Z}_q$ in Table 1.

Table 2 lists the number of ring multiplications for proposed FHE schemes. For the performance comparison, we also include the number of ring multiplications

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

Bits of Security	80	112	128	192	256
$q = p_1p_2$ **in bits [4]**	1024	2048	3072	7680	15360
$q = p_1p_2p_3$ **in bits [16, 28]**	1536	2335	3072	7680	15360
$q = p_1p_2p_3p_4$ **in bits [16, 28]**	2048	3072	4562	7680	15360

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 Insecure FHE without bootstrapping schemes in the literature

Though it has been a very challenging open question to design noise-free FHE schemes, several noise-free FHE schemes with or without security proofs have been posted as IACR ePrint technical reports. In this section, we show that these schemes do not work.

12.1 Insecure octonion based FHE schemes

Yagisawa [31, 30] proposed a fully homomorphic encryption scheme using octonions. The schemes in [31] and [30] are identical except that the message encoding approaches are different. In this section, we show that the scheme in [31] does not decrypt and the scheme in [30] is insecure. First we note that the schemes in both [31] and [30] are over finite fields $\mathbb{F}_q$ and the recommended q is 80 bits. The protocol proceeds as follows.

Key Setup. Let $\mathbf{x}$ be an octonion variable and let $\mathbf{z} \in \mathbb{F}_q^8$ be a randomly selected isotropic octonion over the finite field $\mathbb{F}_q$. Choose random invertible octonions $\mathbf{k}_0, \cdots, \mathbf{k}_{t-1}, \mathbf{w}_0, \cdots, \mathbf{w}_{t-1}, \mathbf{u}_0, \cdots, \mathbf{u}_{t-1} \in \mathbb{F}_q^8$. The private key is

$$\texttt{key} = \{\mathbf{z}, \mathbf{k}_0, \cdots, \mathbf{k}_{t-1}, \mathbf{w}_0, \cdots, \mathbf{w}_{t-1}, \mathbf{u}_0, \cdots, \mathbf{u}_{t-1}\}.$$

Encryption. For a message $m \in \mathbb{F}_q$, it is first encoded to an octonion in $\mathbb{F}_q^8$. In Yagisawa [31], m is encoded as follows: choose random $r_0, r_1 \in \mathbb{F}_q$ such that $m + r_0 + r_1 = 0$ and let $\mathbf{m}' = \mathbf{u}_0(\cdots(\mathbf{u}_{t-1}(m\mathbf{1} + r_0\mathbf{z} + r_1\mathbf{z}^*)\mathbf{u}_{t-1}^{-1})\cdots)\mathbf{u}_0^{-1}$. In Yagisawa [30], m is encoded as follows: choose random $a, b, r \in \mathbb{F}_q$ such that $m = a + 2\text{Re}(\mathbf{z})b$ and let $\mathbf{m}' = \mathbf{u}_0(\cdots(\mathbf{u}_{t-1}(a\mathbf{1} + b\mathbf{z} + r\mathbf{z}^*)\mathbf{u}_{t-1}^{-1})\cdots)\mathbf{u}_0^{-1}$. The ciphertext $\texttt{YO.Enc}(\texttt{key}, m)$ in both [31] and [30] is

$$\mathbf{c}_m(\mathbf{x}) = (\mathbf{k}_0(\cdots((\mathbf{k}_{t-1}(\mathbf{m}'[(\mathbf{k}_{t-1}^{-1}(\cdots((\mathbf{k}_0^{-1}\mathbf{x})\mathbf{w}_0)\cdots))\mathbf{w}_{t-1}]))\mathbf{w}_{t-1}^{-1})\cdots))\mathbf{w}_0^{-1}.$$

Decryption. Let

$$g_0(\mathbf{x}) = \mathbf{k}_{t-1}^{-1}((\cdots(\mathbf{k}_0^{-1}(\mathbf{x}\mathbf{w}_0))\cdots)\mathbf{w}_{t-1})$$
$$g_1(\mathbf{x}) = \mathbf{k}_0((\cdots(\mathbf{k}_{t-1}(\mathbf{x}\mathbf{w}_{t-1}^{-1}))\cdots)\mathbf{w}_0^{-1})$$

For a received ciphertext $\mathbf{c}_m(\mathbf{x})$, compute $\mathbf{m}' = g_0(\mathbf{c}_m(g_1(\mathbf{1})))$. Let

$$\mathbf{m} = \texttt{YO.Dec}(\texttt{key}, \mathbf{c}_m(\mathbf{x})) = \mathbf{u}_{t-1}^{-1}(\cdots(\mathbf{u}_0^{-1}\mathbf{m}'\mathbf{u}_0)\cdots)\mathbf{u}_{t-1}.$$

Yagisawa [31, 30] claims that the original message m can be "recovered" from $\mathbf{m}$ and the scheme YO is secure. We first show that the scheme in [30] is insecure

in the wCOA security model. Our analysis techniques for the scheme OtcoM in this paper could be used to show that the problem of recovering a message in the scheme [30] can be reduced to the problem of solving a univariate polynomial equation. This problem is trivially solvable for the parameters recommended by [30]. Furthermore, By the fact that $\mathbf{z} = 2\mathrm{Re}(\mathbf{z}) - \mathbf{z}^*$, we have

$$a\mathbf{1} + b\mathbf{z} + r\mathbf{z}^* = (a + 2b\mathrm{Re}(\mathbf{z}))\mathbf{1} + (r - b)\mathbf{z}^* = m\mathbf{1} + (r - b)\mathbf{z}^*.$$

Thus the message $m = 0$ is encrypted to $\mathbf{c}_m(\mathbf{x})$ such that $\mathbf{c}_m(\mathbf{1})$ is an isotropic octonion while non-zero messages m are encrypted to $\mathbf{c}_m(\mathbf{x})$ such that $\mathbf{c}_m(\mathbf{1})$ have positive norms. This observation has been pointed out by Wang [29] already.

Next, we show that the scheme in [31] is not multiplicative homomorphic and the plaintext m could not be recovered from the decrypted $\mathbf{m}$. For the scheme YO in [31], the addition of two ciphertexts $\mathbf{c}_{m_0}(\mathbf{x})$ and $\mathbf{c}_{m_1}(\mathbf{x})$ is defined as the component wise addition $\mathbf{c}_{m_0+m_1}(\mathbf{x}) = \mathbf{c}_{m_0}(\mathbf{x}) + \mathbf{c}_{m_1}(\mathbf{x})$. Yagisawa [31] defined the multiplication of two ciphertexts $\mathbf{c}_{m_0}(\mathbf{x})$ and $c_{m_1}(\mathbf{x})$ as $\mathbf{c}_{m_1 m_0} = \mathbf{c}_{m_1}(\mathbf{c}_{m_0}(\mathbf{x}))$. However, this ciphertext multiplication does not work. Using our matrix based approach, we have

$$\mathbf{c}_m(\mathbf{x}) = \mathbf{x}A^l_{\mathbf{k}_0^{-1}}A^r_{\mathbf{w}_0}\cdots A^l_{\mathbf{k}_{t-1}^{-1}}A^r_{\mathbf{w}_{t-1}}A^l_{\mathbf{m}'}A^l_{\mathbf{k}_{t-1}}A^r_{\mathbf{w}_{t-1}^{-1}}\cdots A^l_{\mathbf{k}_0}A^r_{\mathbf{w}_0^{-1}}$$

Thus

$$\begin{aligned}\mathbf{c}_{m_1}(\mathbf{c}_{m_0}(\mathbf{x})) &= \mathbf{x}A^l_{\mathbf{k}_0^{-1}}A^r_{\mathbf{w}_0}\cdots A^l_{\mathbf{k}_{t-1}^{-1}}A^r_{\mathbf{w}_{t-1}}A^l_{\mathbf{m}'_0}A^l_{\mathbf{k}_{t-1}}A^r_{\mathbf{w}_{t-1}^{-1}}\cdots A^l_{\mathbf{k}_0}A^r_{\mathbf{w}_0^{-1}}\\ &\quad A^l_{\mathbf{k}_0^{-1}}A^r_{\mathbf{w}_0}\cdots A^l_{\mathbf{k}_{t-1}^{-1}}A^r_{\mathbf{w}_{t-1}}A^l_{\mathbf{m}'_1}A^l_{\mathbf{k}_{t-1}}A^r_{\mathbf{w}_{t-1}^{-1}}\cdots A^l_{\mathbf{k}_0}A^r_{\mathbf{w}_0^{-1}}\\ &\neq \mathbf{c}_{m_1 m_0}(\mathbf{x})\end{aligned}$$

For the scheme in [31], even if one can find an approach to revise the above encryption process so that it is multiplicative homomorphic, the original message m could not be decoded from $\mathbf{m}$ for the following reasons. For two encoded messages

$$\begin{aligned}\mathbf{m}'_0 &= m_0\mathbf{1} + r_{0,0}\mathbf{z} + r_{0,1}\mathbf{z}^*\\ \mathbf{m}'_1 &= m_1\mathbf{1} + r_{1,0}\mathbf{z} + r_{1,1}\mathbf{z}^*\end{aligned}$$

we have

$$\mathbf{m}'_0\mathbf{m}'_1 = m_0m_1\mathbf{1} + r_{3,0}\mathbf{z} + r_{3,1}\mathbf{z}^*$$

for some $r_{3,0}, r_{3,1} \in \mathbb{F}_q$. But generally it does not satisfy the condition $m_0m_1 + r_{3,0} + r_{3,1} = 0$ as required in the encryption process. Thus $\mathbf{m}'_0\mathbf{m}'_1$ could not be uniquely decrypted to m_0m_1. The root cause for this decoding failure is that $\mathbf{1} \in \mathrm{span}\{\mathbf{z}, \mathbf{z}^*\}$.

12.2 Insecure IPE based FHE schemes

Liu [21] proposed a noise-free FHE scheme over a finite field $\mathbb{F}_q$. The design in [21] is quite sophisticated and we use the simplified description from Wang [29]. Though Wang [29] describes a potential attack on [21], it is not clear whether the attack in [29] is effective for large enough q. In the following, we present several efficient attacks on the FHE scheme in [21]. Let $\mathbf{a} = [a_0, \cdots, a_n]$ and $\mathbf{b} = [b_0, \cdots, b_n]$ be two vectors. Then the tensor (outer) product of $\mathbf{a}$ and $\mathbf{b}$ is defined as a length $(n+1)^2$ vector $\mathbf{a} \otimes \mathbf{b} = [a_0b_0, a_0b_1, \cdots, a_nb_n]$. Let $l \leq n-2$ be two given integers where Liu [21] recommends the use of $n = 5$ and $l = 3$. The protocol proceeds as follows.

Key Setup.

- The private key is a randomly selected vector $\mathbf{k} = [k_0, \cdots, k_n] \in \mathbb{F}_q^{n+1}$.
- The public key (Φ, P) consists of two random matrices $\Phi \in \mathbb{F}_q^{(l+1)\times(n+1)}$ and $P \in \mathbb{F}_q^{(n+1)^2\times(n+1)}$ such that $\Phi\mathbf{k}^T$ contains an entry 1 and $(\mathbf{k} \otimes \mathbf{k})^T = P\mathbf{k}^T$.

Encryption. For a message $m \in \mathbb{F}_q$, select a random vector $\mathbf{r} \in \mathbb{F}_q^{l+1}$ such that $m = \mathbf{r}\Phi\mathbf{k}^T$. The ciphertext of m is $\mathbf{c}_m = \mathbf{r}\Phi$.
Decryption. For a received ciphertext $\mathbf{c}$, compute $m = \texttt{IPE.Dec}(\mathbf{k}, \mathbf{c}) = \mathbf{c}\mathbf{k}^T$.
Ciphertext addition. The addition of two ciphertexts $\mathbf{c}_{m_0}$ and $\mathbf{c}_{m_1}$ is defined as the regular component wise vector addition $\mathbf{c}_{m_0+m_1} = \mathbf{c}_{m_0} + \mathbf{c}_{m_1}$.
Ciphertext multiplication. For ciphertexts $\mathbf{c}_{m_0} = [c_0, \cdots, c_n]$ and $\mathbf{c}_{m_1} = [c'_0, \cdots, c'_n]$, The multiplication of $\mathbf{c}_{m_0}$ and $\mathbf{c}_{m_1}$ is defined as $\mathbf{c}_{m_0m_1} = (\mathbf{c}_{m_0} \otimes \mathbf{c}_{m_1})P$.

The scheme could be further simplified to the plain Inner Product Encryption IPE scheme with a published public evaluation matrix P by removing the matrix Φ from the public key since there exists an $(n+1)\times(l+1)$ matrix A such that $\Phi A = I$. The ciphertext can be rewritten as $\mathbf{c} = \mathbf{c}_m A = \mathbf{r}\Phi A = \mathbf{r}$ and the private key can be rewritten as $\mathbf{k}\Phi^T$. Liu [21] recommends the use of $q = 100000000000031$ as the public parameter.

The correctness of the protocol could be verified by the fact that

$$mm' = (c_0k_0 + \cdots + c_nk_n)(c'_0k_0 + \cdots + c'_nk_n) = \sum_{i,j=0}^{n} c_ic'_jk_ik_j \tag{26}$$

in case that $[c_0, \cdots, c_n]$ and $[c'_0, \cdots, c'_n]$ are the ciphertexts of m and m' respectively. However, the protocol is insecure since the private key $\mathbf{k}$ could be recovered from the public evaluation matrix P. In the following, we present various attacks on the protocol.

First, Liu [21] requires the public key contains a ciphertext $\mathbf{c}$ of the plaintext 1. By the multiplicative homomorphism property, one can get different ciphertext vectors $\mathbf{c}_i$ of $1^i = 1$ for $i > 0$. Thus the key space could be significantly reduced by using the linear equation system $\mathbf{k}\mathbf{c}_i^T = 1$. Furthermore, if one can obtain n independent ciphertext vectors $\mathbf{c}_i$ for $1^i = 1$ by the multiplicative homomorphism property, then one can completely recover the entire key $\mathbf{k}$ from the equation system $\mathbf{k}\mathbf{c}_i^T = 1$.

Secondly, we note that, for $i \neq j$, if the rows $\mathbf{p}_{i,j}$ and $\mathbf{p}_{j,i}$ in P (corresponding to k_ik_j and k_jk_i respectively) are not identical, then $\mathbf{p}_{i,j} - \mathbf{p}_{j,i} \neq \mathbf{0}$ is a ciphertext of the message 0. By deriving $n+1$ linearly independent ciphertexts for 0 from P, one can recover the private key $\mathbf{k}$ by solving the linear equation system consisting of $n+1$ equations $(\mathbf{p}_{i,j} - \mathbf{p}_{j,i})\mathbf{k} = 0$ for $i \neq j$. Liu [21] does not require $\mathbf{p}_{i,j} = \mathbf{p}_{j,i}$ for $i \neq j$.

Thirdly, even if $\mathbf{p}_{i,j} = \mathbf{p}_{j,i}$ for all $i, j \leq n$, the private key $\mathbf{k}$ could still be recovered from P using the relinearization algorithm in Kipnis and Shamir [18]. Let $P' \in \mathbb{F}_q^{\frac{n(n+1)}{2} \times (n+1)}$ be the matrix obtained from P by taking rows corresponding to the entries k_ik_j with $i \leq j$. Then there exists a matrix $M \in \mathbb{F}_q^{\frac{n^2-n-2}{2} \times \frac{n(n+1)}{2}}$ such that $MP' = 0$ and rows of M are linearly independent. It follows that

$$M[k_0k_0, \cdots, k_ik_j, \cdots, k_nk_n]^T = MP'[k_0, \cdots, k_n]^T = 0 \tag{27}$$

is a homogeneous quadratic equation system with $\frac{n^2-n-2}{2}$ equations in $n+1$ variables. Since $\frac{n^2-n-2}{2} > 0.09175(n+1)^2$ for $n \geq 3$, the relinearization algorithm in Kipnis and Shamir [18] could be used to efficiently recover the private keys $k_0, \cdots, k_n$.

The reader may ask whether the scheme in Liu [21] could be made secure by using finite rings $\mathbb{Z}_q$ for large enough $q = p_1p_2$ instead of $\mathbb{F}_q$ for $q = p^m$ since the quadratic equations could not be efficiently solved in $\mathbb{Z}_q$ unless one knows the factorization of the q. The answer is no. In the relinearization attack, one obtains all values k_ik_j for $i, j \leq n$ by solving a linear equation. Thus one can use the equation system $(\mathbf{k} \otimes \mathbf{k})^T = P\mathbf{k}^T$ to obtain the value of $\mathbf{k}$ directly by solving a linear equation system instead of a quadratic equation system. Alternatively, one can use the identity (26), the ciphertext c_1 of the message 1 which is contained in the rows of Φ (as required by Liu [21]), and the calculated values k_ik_j to decrypt any ciphertexts directly.

Lastly, by the fact that $(\mathbf{k} \otimes \mathbf{k})^T = P\mathbf{k}^T$, we can establish $n+1$ equation systems

$$(k_iI - P_i)\mathbf{k} = 0 \tag{28}$$

for $i = 0, \cdots, n$ and $P_i \in \mathbb{F}_q^{(n+1)\times(n+1)}$. From the equation system $(k_0I - P_0)\mathbf{k} =$

0, one can obtain univariate polynomials $p_{0,0}, \cdots, p_{0,n}$:

$$p_{0,0}(k_0) = |k_0 I - P_0| = 0, \quad p_{0,1}(k_0) = k_1, \quad \cdots, \quad p_{0,n}(k_0) = k_n.$$

The private key $\mathbf{k}$ can be recovered from these univariate polynomials efficiently.

13 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 of software obfuscation problems. 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. One potential approach could be to add sufficiently many random decimal bits as postfix to the plaintext integers and then convert them to elements of $\mathbb{Z}_q$.

Acknowledgment

I would like to thank Jared Weinstein, Qutaibah Malluhi, and Martin Strand for several valuable comments and discussions on related topics.

References

[1] G. Ars, J.-C. Faugere, H. Imai, M. Kawazoe, and M. Sugita. Comparison between XL and Gröbner basis algorithms. In *ASIACRYPT 2004*, pages 338–353. Springer, 2004.

[2] J. Baez. The octonions. *Bullet. American Mathematical Society*, 39(2):145–205, 2002.

[3] M. Bardet, J.-C. Faugere, and B. Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proc. Int. Conference on Polynomial System Solving*, pages 71–74, 2004.

[4] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. NIST special publication 800-57. *NIST Special Publication*, 800(57):1–142, 2007.

[5] Z. Brakerski. When homomorphism becomes a liability. In *Theory of Cryptography*, pages 143–161. Springer, 2013.

[6] 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.

[7] J. Conway and D. Smith. On quaternions and octonions. *AMC*, 10:12, 2003.

[8] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *EUROCRYPT 2000*, pages 392–407. Springer, 2000.

[9] P. Dembowski. *Finite Geometries: Reprint of the 1968 Edition*. Springer Science, 2012.

[10] J.-C. Faugere. A new efficient algorithm for computing Gröbner bases without reduction to 0 (F5). In *Proc. ISSAC*, pages 75–83.

[11] J.-C. Faugere. A new efficient algorithm for computing Gröbner bases (F4). *J. Pure and Applied Algebra*, 139(1):61–88, 1999.

[12] J Fulman. *Probability in the classical groups over finite fields*. PhD thesis, Harvard Univ., 1997.

[13] J. Fulman. Random matrix theory over finite fields. *Bullet. AMS*, 39(1):51–85, 2002.

[14] J. Von Zur Gathen and D. Panario. Factoring polynomials over finite fields: A survey. *J. Symbolic Computation*, 31(1):3–17, 2001.

[15] C. Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, volume 9, pages 169–178, 2009.

[16] M.J. Hinek. On the security of multi-prime RSA. *J. Math. Cryptology*, 2(2):117–147, 2008.

[17] H. Kestelman. Automorphisms of the field of complex numbers. *Proc. London Math. Soc.*, 2(1):1–12, 1951.

[18] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem. In *Proc. Crypto*, 1999.

[19] V. Kolesnikov and T. Schneider. A practical universal circuit construction and secure evaluation of private functions. In *Financial Cryptography*, pages 83–97. Springer, 2008.

[20] R. Lidl and H. Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.

[21] D. Liu. Practical fully homomorphic encryption without noise reduction. Technical report, Cryptology ePrint Archive, Report 2015/468. http://eprint.iacr.org/2015/468, 2015.

[22] P. Lounesto. Octonions and triality. *Adv. Applied Clifford Algebras*, 11(2):191–213, 2001.

[23] 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.

[24] B. Sturmfels. What is a Gröbner basis. *Notices Amer. Math. Soc*, 52(10):1199–1200, 2005.

[25] L. Valiant. Universal circuits. In *Proc. 8th ACM STOC*, pages 196–203. ACM, 1976.

[26] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In *Advances in cryptology–EUROCRYPT 2010*, pages 24–43. Springer, 2010.

[27] G.E. Wall. Counting cyclic and separable matrices over a finite field. *Bulletin of the Australian Mathematical Society*, 60(02):253–284, 1999.

[28] Y. Wang. PKCS: Public-key cryptography standards. In H. Bidgoli, editor, *Handbook of Information Security*, pages 966–978. Wiley, 2006.

[29] Y. Wang. Notes on two fully homomorphic encryption schemes without bootstrapping. Cryptology ePrint Archive, Report 2015/519, 2015. http://eprint.iacr.org/.

[30] M. Yagisawa. Fully homomorphic encryption on octonion ring. Technical report, Cryptology ePrint Archive, Report 2015/733. http://eprint.iacr.org/2015/733, 2015.

[31] M. Yagisawa. Fully homomorphic encryption without bootstrapping. Technical report, Cryptology ePrint Archive, Report 2015/474. http://eprint.iacr.org/2015/474, 2015.

[32] P.B. Yale. Automorphisms of the complex numbers. *Math. Magazine*, pages 135–141, 1966.

[33] A. Yao. How to generate and exchange secrets. In *Proc. 27th IEEE FOCS*, pages 162–167. IEEE, 1986.