IEEE Access
Multidisciplinary Rapid Review Open Access Journal

Received May 5, 2020, accepted June 14, 2020, date of publication July 7, 2020, date of current version August 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007717

Noise Free Fully Homomorphic Encryption Scheme Over Non-Associative Algebra

IQRA MUSTAFA[1,2], HASNAIN MUSTAFA[2], AHMAD TAHER AZAR[3,4], (Senior Member, IEEE), SHERAZ ASLAM[5], (Member, IEEE), SYED MUHAMMAD MOHSIN[2], MUHAMMAD BILAL QURESHI[6], AND NOUMAN ASHRAF[7]

[1]Department of Computing, Cork Institute of Technology (CIT), Cork T12 P928, Ireland
[2]Department of Computer Science, COMSATS University Islamabad, Islamabad 45550, Pakistan
[3]Robotics and Internet-of-Things Lab (RIOTU), Prince Sultan University, Riyadh 11586, Saudi Arabia
[4]Faculty of Computers and Artificial Intelligence, Benha University, Benha 13518, Egypt
[5]Department of Electrical Engineering, Computer Engineering, and Informatics, Cyprus University of Technology, 3036 Limassol, Cyprus
[6]Department of Computer Science, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad 44000, Pakistan
[7]Telecommunications Software and Systems Group (TSSG), Waterford Institute of Technology, Waterford X91 K0EK, Ireland

Corresponding author: Sheraz Aslam (sheraz.aslam@cut.ac.cy)

This work was supported by the Prince Sultan University, Riyadh, Saudi Arabia.

ABSTRACT Among several approaches to privacy-preserving cryptographic schemes, we have concentrated on noise-free homomorphic encryption. It is a symmetric key encryption that supports homomorphic operations on encrypted data. We present a fully homomorphic encryption (FHE) scheme based on sedenion algebra over finite Z_n rings. The innovation of the scheme is the compression of a 16-dimensional vector for the application of Frobenius automorphism. For sedenion, we have p^{16} different possibilities that create a significant bijective mapping over the chosen 16-dimensional vector that adds permutation to our scheme. The security of this scheme is based on the assumption of the hardness of solving a multivariate quadratic equation system over finite Z_n rings. The scheme results in $256n$ multivariate polynomial equations with $256 + 16n$ unknown variables for n messages. For this reason, the proposed scheme serves as a security basis for potentially post-quantum cryptosystems. Moreover, after sedenion, no newly constructed algebra loses its properties. This scheme would therefore apply as a whole to the following algebras, such as 32-dimensional trigintadunion.

INDEX TERMS Sedenion, Frobenius automorphism ϕ, automorphism Aut(V), fully homomorphic encryption, totally isotropic subspaces, multivariate polynomial equations.

I. INTRODUCTION

The Fully Homomorphic Encryption (FHE) scheme was referred to as the "Holy Grail" of the cryptography [1]. They have the ability to perform encrypted data processing without prior decryption. As a result, FHE has gained accumulated interest from cryptographers. Moreover, the normal evaluation of the IT environment has changed computing principles from parallel computing to cloud computing, as IT cost reduction is one of its main benefits. Gentry [2] has implemented the first FHE candidate scheme. Gentry 's technical dilemma of designing the 2009 FHE scheme was seen as a significant innovation that addressed the security and confidence problems of the IT world. Initially, his concept was based on NTRU, a lattice-based cryptosystem known as somewhat homomorphic i.e. homomorphic for a fixed number of operations (often referred to as the depth of the circuit) which was transformed into an FHE scheme by bootstrapping [3]. Gentry's bootstrapping technique is used to refresh ciphers in a homomorphic way by computing the decryption function, which decreases cipher noise to an appropriate amount. This bootstrapping is still the key constraint that affects the efficiency of all known FHE schemes. Many researchers followed Gentry's initial work and suggested variations and enhancements to Gentry 's system, which is considered to be the first generation of the FHE system, i.e. [4]–[6], [8]–[10], [16]. Subsequently, nowadays FHE has been widely adopted for cloud security [11], [12], e-health care privacy [13], blockchain, [14] i.e., artificial intelligence Cortex blockchain adopted somewhat FHE (SWFHE) to train

The associate editor coordinating the review of this manuscript and approving it for publication was Lo'ai A. Tawalbeh.

and infer the model. The first generation methods, however, were somewhat similar, but they had different theoretical assumptions with complex methodologies. Later Brakerski and Vaikuntanathan [15], on the other hand, developed a simplified technique based on error learning (LWE) assumptions. The security of their construction was based on the quantum hardness of the worst-case lattices. They used ''Dimension modulus Reduction'' to simplify the decryption circuit and prevent squashing. In [16], Brakerski, Gentry, and Vaikuntanathan (BGV) strengthened the scheme by using ''modulus switching'' to minimize noise and eliminate the need for bootstrapping. Their methodology started the second generation of the homomorphic scheme.

Therefore, over the last few years, a variety of studies have been performed to examine the efficiency and safety of FHE schemes on more criteria and well-understood security assumptions. From a security perspective, a series of papers [15]–[20] led to a graded FHE scheme based on the same complexity as the underlying non-homomorphic lattice-based encryption. According to Brakerski [17], in the Chosen Plaintext Attack (CPA) security model such as OctoM, linearly decryptable FHE schemes can not be secured. Since then, Yonge [21] has implemented an Octonion-based FHE noise-free scheme over finite Zq rings, which is secure in the Weak Ciphertextonly Attack (wCOA) security model. It shows that linearly decryptable FHE schemes are not even secure in the Ciphertext only Attack (COA) security model.

Concluding all, following are the main contributions of this research.

- The proposed scheme is constructed on 16-dimensional sedenions, which is defined over a ring of integers Z_n.
- We have applied Frobenius automorphism over a compressed 16-dimensional vector belonging to a ring Z_n^{16}. Up to our knowledge, the idea of vector compression and Frobenius automorphism haven not been applied in any of the techniques designed earlier for noise-free FHE schemes. This contribution is made under the required security demand of cryptosystems in response to the emerging quantum computers.
- The security of the proposed scheme is based on the decoding problem of linear-codes and does not succumb to known quantum algorithms.
- The proposed solution is validated by using mathematical modeling.

For quite a long time, sedenions have been overlooked for not being part of algebra division. However, the development of the proposed scheme is based on the fact that irrespective of 84 pairs of zero divisors, as described in [24], the inverse of the rest of the sedenions, exists. So, the only assumption made in the proposed model is that the sedenion inverse exists and 84 pairs of zero divisors are not considered.

However, the security and efficiency of systems based on hyper-complex numbers relies on its high dimension and matrix-vector multiplication. On that basis, the new scheme provides strong security with a negligible speed difference over OctoM compared to the previous [21] scheme. In addition, to increase the efficiency of the scheme, we use a quick [25] algorithm for sedenion multiplication, which saves 134real multiplication, requiring 15 % fewer arithmetic operations than direct evaluation. We conclude this section by adding some notations, such as finite rings $Zq = Z/qZ$, a totally isotropic subspace V with dimension $k \leq n/2$, i.e. $8 \leq 16/2$ which includes a private key, random isotropic vector $v \epsilon V$ and Frobenius automorphism ϕ.

The rest of the paper is organized as follows: In Section II, terminologies are defined which are used in later sections. Section III describes that why we moved towards $16D$ vector space sedenion. In Section IV, the construction of the proposed noise-free encryption scheme over a finite ring of integers Z_n has been introduced. In Section V, security analysis of the proposed scheme and different concepts are discussed and finally, the paper is concluded in Section VI.

II. PRELIMINARIES

Various terminology related to linear algebra and cryptography as background knowledge are discussed in this section. This section will help the reader to understand the proposed FHE scheme.

A. TOTALLY ISOTROPIC SUBSPACES

A subspace V is said to be totally isotropic if all the elements belonging to it are orthogonal to each other i.e., if $\exists x \in V$ and:

$$V = \{x \in V | \, x \bot x \forall x \in V\}$$

The number of isotropic subspaces can get determined for an odd q and even n by using the formula given in paper [26] i.e.,

$$(q^{n-k} - q^{n/2-k} + q^{n/2-1} - 1) \Pi_{i=1}^{k-1} (q^{n-2i} - 1) \div \Pi_{i=1}^{k} (q^i - 1)$$

So totally isotropic subspaces with dimension $k \leq n/2$ i.e., $8 \leq 16/2$ are:

$$2(q+1)(q^2+1)(q^3+1)(q^4+1)(q^5+1)(q^6+1)(q^7+1)$$

Totally isotropic subspace of dimension one is involved in the proposed scheme, which means that the subspace span is a single vector, i.e. the entire subspace is generated by this vector. Similarly, if the isotropic subspace is of dimension two, the span set consists of two vectors. The V subspace is characterized as being closed under sedenion multiplication, forming an ideal set i.e., $v_0 v_1 \in V$ and $v_1 v_0 \in V \, \forall v_0, v_1 \in V$. These vectors of zero norm are involved in changing our plaintext message $m \in Z_n$ to a sedenion message $m' \in Z_n^{16}$.

B. DIFFUSION

According to Claude Shannon, this property should be a fundamental feature of any cryptographic system. According to him, a minor change in the plaintext results in a huge change of numbers of ciphertext characters. This property helps prevent the study of ciphertext by statistical frequency.

C. CONFUSION

Similar to diffusion, confusion is another major property described by Shannon to satisfy any cryptographic scheme. It is responsible for establishing a complex statistical relationship between the key and the cipher. That is, even though the adversary has some plaintext-ciphertext pairs, he is still unable to extract the key from them. Therefore, each bit of cipher text depends on the key, and any small bit shift has a drastic effect on the cipher text.

D. AUTOMORPHISM

It is a bijective homomorphism among same group $\phi : H \rightarrow H$ i.e., the mapping is:

- injective(one-to-one)
- surjective(onto)

A mapping is invertible if and only if it is bijective. i.e., inverse function exists. If $(H, +)$ is an additive group than the mapping defined is homomorphic.

$$\phi(a+b) = \phi(a) + \phi(b)$$

Similarly, if $(H, *)$ is a multiplicative group.

$$\phi(ab) = \phi(a).\phi(b)$$

$\forall a, b \in H$. Such an isomorphism, that maps a sedenion over itself is an automorphism. The special structure of the set $Aut(V)$ is that since automorphism is an isomorphism first whose inverse also exists, so the set $Aut(V)$ qualifies as a group and satisfies all group properties i.e., closed, identity, inverse and associative.

E. MULTIPOINT EVALUATION

The multi-point evaluation [28], [30] help us compute polynomial $f \in R[x]$ at multiple points $t_0, t_1, \ldots, t_{n-1}$ of R, where R itself is a commutative ring and $n = 2^k$ for $k \in N$, such that the mapping can be defined as:

$$\begin{aligned} \rho : R[x]/ < m > &\rightarrow R^n \\ f &\rightarrow (f(t_0), f(t_1), \ldots, f(t_{n-1})) \end{aligned}$$

In order to perform multi-point evaluation, we recursively split our set of points in two halves; $t_0, t_1, \ldots, t_{n/2-1}$, and $t_{n/2}, \ldots, t_{n-1}$, such that two polynomials are described as:

$$\begin{aligned} W_0 &= \Pi_{l=0}^{n/2-1}(x - t_l) \\ W_1 &= \Pi_{l=0}^{n/2-1}(x - t_{n/2+l}) \end{aligned}$$

and we define $r_0, r_1 \in R[x]$, such that [line 6-8]:

$$\begin{cases} r_0(t_i) = f(t_i), & \text{if } \forall 0 \le i \le n/2 - 1 \\ r_1(t_i) = f(t_i), & \text{if } \forall\, n/2 \le i \le n - 1 \end{cases}$$

this is due to:

$$\begin{aligned} r_0 &= fmodW_0 \\ r_1 &= fmodW_1 \end{aligned}$$

A polynomial is required which is precomputed i.e., $W_{i,j} = \Pi_{l=0}^{2^i-1}(x - t_{j.2^i+l})$ for $0 \le i \le k$ and $0 \le j \le 2^{k-i}$ [line 2], where $degW_{i,j} = 2^i$. In order to evaluate r_0 and r_1 we precomputed all $W_{i,j}$'s such that:

$$\begin{aligned} W_{0,j} &= (x - t_j) \\ W_{i+1,j} &= W_{i,2j}.W_{i,2j+1} \end{aligned}$$

$W_{i+1,j}$ can be computed from $W_{i,2j}$ and $W_{i,2j+1}$ in $\mathcal{O}(M(2^i)$ operations as $deg(W_{i,j}) = 2^i$, where $\mathcal{O}$ is complexity of an algorithm (worst case), $M(2^i)$ denotes the complexity of multiplying two polynomials (degree of each is bounded by 2^i). Now for $0 \le j \le 2^{k-i-1}$, the number of operations required for a fixed $i+1 = \mathcal{O}(M(n))$. In Algorithm 1 [line 5], the division algorithm is used to compute r_0 and r_1, so the total time taken by algorithm is:

$$= \mathcal{O}(M(n)log(n)) \tag{1}$$

Algorithm 1 Multipoint Evaluation

```
1: procedure Multipoint Evaluation
2:     Pre-compute: $W_{i,j} \forall 0 \le i \le k$ and $0 \le j \le 2^{k-i}$.
3:     For $n = 1$
4:     return $f$.
5:     Take $r_0 = fmodW_{k-1,0}$ and $r_1 = fmodW_{k-1,1}$.
6:     Evaluate recursively $r_0$ at $t_0, t_1, \ldots, t_{n/2-1}$ and $r_1$
7:       at $t_{n/2}, \ldots, t_{n-1}$.
8:     Output: $r_0(t_0), \ldots, r_0(t_{n/2-1}), r_1(t_{n/2}), \ldots, r_1(t_{n-1})$.
9: end procedure
```

F. CONSTRUCTION OF FINITE FIELD

The proposed scheme is based on sedenion defined over Z_n i.e., sedenion element $s \in Z_n^{16}$, over it's modulus with a prime number p and frobenius automorphism. In order to apply frobenius automorphism, a finite field of p^n elements is constructed through a prime field Z_p, and an integer n which defines the dimension of selected vector space, which in case of sedenion is $n = 16$. So, the order of field over which frobenius is applied is p^{16}. Hence, finite field of order p^n is created through a polynomial ring defined over Z_p i.e.,

$$Z_p[x] = \{f = \sum_{i=0}^{n} c_i x^i | n \in N, c_i \in Z_p\}$$

For construction of a finite field, a monic irreducible polynomial $f \in Z_p[x]$ of degree n is selected to generate an ideal. The ideal I generated from f i.e., $I(f)$ or $< f >$ is a non-empty subset such that for $g_1, g_2 \in I$, it satisfies:

- $g_1 - g_2 \in I$
- $g_1 * g_2 \in I$

where g belongs to polynomial ring. Now to get elements p^n of the field, residue classes of the polynomials $Z_p[x]$modulo$< f >$ are considered. These elements or the residue classes belong to the factor ring.

$$Z_p[x]/ < f >= g+ < f > |g \in Z_p[x]$$

The set $Z_p[x]/ < f >$ with addition and multiplication forms a commutative ring with multiplicative inverse for each element.

Theorem 1: If f is a monic, irreducible polynomial in $Z_p[x]$ for degree n and prime p the residue class ring $Z_p[x]/ < f >$ is a field of order p^n.

Proof: *The co-sets mod $< f >$ are represented by remainders*:

$$c_0 + c_1x + \cdots + c_{n-1}x^{n-1}, \quad c_i \in Z_p \tag{2}$$

and there exist p^n such polynomials. Since, modulus $< f >$ is irreducible, the ring $Z_p[x]/ < f >$ is a field. This is similar to the proof, that $Z/ < m >$ is a field if m is prime. □

G. PRIMITIVE ELEMENTS

A Primitive element is a non-zero element which exists for every finite field and generates multiplicative group of finite field [31]. An element is primitive if it's order is $n - 1$ for Galios field GF(n), where each power of primitive element generates elements of F_{p^n} i.e., we can say that each primitive element forms a cyclic group under multiplication of order $n - 1$.

$$\begin{aligned}\phi(\alpha) &= \alpha^p\\ \phi^2(\alpha) &= \phi(\phi(\alpha)) = (\alpha^p)^2\\ \phi^3(\alpha) &= \phi(\phi^2(\alpha)) = (\alpha^{p^2})^2 \ldots\ldots\end{aligned}$$

Example 1: Let us construct a finite field of 2^4 elements from a polynomial ring $Z_2[x]$.

$$Z_2[x] = \{x^4 + x^3 + x^2 + x + 1 | n \in N, k_i \in Z_2\}$$

Hence, co-efficients are either 0 or 1. It generates an ideal $< x^4 + x + 1 >$ to form a residue classes of polynomial in modulo $< x^4 + x + 1 >$ which is similar to Z/nZ for n belonging to a set of integers i.e., any polynomial which is a multiple of $x^4 + x + 1$ in $Z_2[x]$ is divided by $< x^4 + x + 1 >$.

$$F = Z_2[x]/ < x^4 + x + 1 >$$

Let α be the root of irreducible polynomial i.e., when α replaces x in an irreducible polynomial, the solution obtained is 0 such that:

$$\begin{aligned}\alpha^4 + \alpha + 1 &= 0\\ \alpha^4 &= \alpha + 1\end{aligned}$$

α turns out to be the primitive element of the field. This primitive element, generates a cyclic group of 15 elements, which is a field [20].

$$\begin{aligned}\alpha^0 &= 1\\ \alpha^1 &= \alpha\\ \alpha^2 &= \alpha^2\\ \alpha^3 &= \alpha^3\\ \alpha^4 &= \alpha + 1\\ \alpha^5 &= \alpha^2 + \alpha\\ \alpha^6 &= \alpha^3 + \alpha^2\\ \alpha^7 &= \alpha^3 + \alpha + 1\\ \alpha^8 &= \alpha^2 + 1\\ \alpha^9 &= \alpha^3 + \alpha\\ \alpha^{10} &= \alpha^2 + \alpha + 1\\ \alpha^{11} &= \alpha^3 + \alpha^2 + \alpha\\ \alpha^{12} &= \alpha^3 + \alpha^2 + \alpha + 1\\ \alpha^{13} &= \alpha^3 + \alpha^2 + 1\\ \alpha^{14} &= \alpha^3 + 1\end{aligned}$$

H. FROBENIUS AUTOMORPHISM

Frobenius automorphism is a mapping from finite field to itself and fixing each element in F_{p^n}.

$$\phi : F_{p^n} \rightarrow F_{p^n} : \alpha \rightarrow \alpha^p \tag{3}$$

$$\phi(\alpha) = \alpha^p \tag{4}$$

For a finite field of order p^n, there are n frobenius automorphisms satisfying:

$$\phi^d = x \longrightarrow x^{p^d}$$

For $0 \leq d \leq n$. From the polynomials generated through primitive elements, in the above example mapping is obtained through which it is explicitly clear that 0 maps to itself and the non-zero elements of F_{2^4} are represented as the power of primitive element maps α to power of α. Where, the last element of each of these rows is mapped onto the first element in each row i.e.,

$$\begin{aligned}&0 \rightarrow 0\\ &1 \rightarrow 1\\ &\alpha \rightarrow \alpha^2 \rightarrow \alpha^4 \rightarrow \alpha^8\\ &\alpha^3 \rightarrow \alpha^6 \rightarrow \alpha^{12} \rightarrow \alpha^9\\ &\alpha^5 \rightarrow \alpha^{10}\\ &\alpha^7 \rightarrow \alpha^{14} \rightarrow \alpha^{13} \rightarrow \alpha^{11}\end{aligned}$$

I. ITERATED FROBENIUS ALGORITHM

If $f \in Z_p$ is irreducible, then $R = Z_p[x]/ < f >$ can be generalized as $R = F_{p^n}$ such that it satisfies most specifically the following rule [32]:

$$g(\alpha^p) = g(\alpha)^p$$

for $g \in Z_p[x]$ and $\alpha \in F_{q^n}$.

We define $\zeta = wmodf \in R$, such that it forms the basis of R i.e., the powers are $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ and we can write $\alpha \in R$ as:

$$\begin{aligned}\alpha &= a_{n-1}\zeta^{n-1} + \cdots + a_1\zeta^1 + a_0\\ &= a(\zeta) = (amodf)\end{aligned}$$

where $a_{n-1}, \ldots, a_0 \in Z_p$. a can be represented as $\breve{\alpha}$, where image of α under frobenius map can be computed as:

$$\alpha^q = a(\zeta)^q = a(\zeta^q) = \breve{\alpha}(\zeta^q)$$

Algorithm 2 Iterated Frobenius

```
procedure Iterated Frobenious
    Take $f \in Z_p[x]$ as a square free polynomial with degree
        n, $\zeta^q \in R$ where $\zeta = wmodf$ and $\alpha \in R$ with
        $d \in N$ such that $d \leq n$.
    $\alpha, alpha_p, \ldots, \alpha^{p^d} \in R$.
    $\xi_0 \longleftarrow \zeta$
    $\xi_0 \longleftarrow \zeta$
    for $i = 0, 1, \ldots, l$
    call algorithm 1 to evaluate
        $\xi_{2^{i-1}+j} = \check{\xi}_{2^{i-1}}(\xi_j)$ for $1 \leq j \leq 2^{i-1}$.
    call algorithm 1 over R to evaluate
    $\delta_k = al\check{p}ha(\xi_k)$ for $0 \leq k \leq d$.
    return $\delta_0, \ldots, \delta_d$.
end procedure
```

III. SEDENIONS

Brakerski's linearly decryptable encryption scheme defined the decryption circuit as an inner product. Wang and Malluhi [22] have shown that even in ciphertext only the security model is insecure. They proposed the OctoM scheme, whose decryption was also similar to IPE decryption. However, it has an edge of the multivariate quadratic equation which makes it efficient and infeasible to solve. In this paper, we have moved toward a 16D vector space belonging to the Cayley-Dickson algebra, which contributes to enhance the security of the proposed noise-free FHE scheme.

Cayley-Dickson construction [23] provides us a method to construct an algebra from the existing one. Each time the newly constructed division algebra loses its property, while its dimension increases by a power of 2. Similar to an octonion construction from quaternions, sedenions are constructed from octonions which lose the property of even being a division algebra due to zero-divisors.

These extensions in complex numbers through Cayley-Dickson construction are called hyper-complex numbers. All these extensions have both a real and a vector part, each with a different dimension. Due to this, each hyper-complex number can be described as a $4D$, $8D$, and $16D$ vector space. Sedenions are 16-dimensional, non-commutative, non-associative, and non-division Caley-Dickson algebra. Sedenion algebra constitutes all the former division algebra as sub-algebra in its set. The structure of sedenion is identified by its sub-algebras. Similarly, its properties and basic sub-algebras are identified by the sub-loops of a sedenion loop called a Cayley-Dickson Sedenion loop. Sedenion in hyper-complex form can be written as:

$$e = a_0e_0 + a_1e_1 + a_2e_2 + \cdots\cdots\cdots + a_{14}e_{14} + a_{15}e_{15}$$

where:

- $e_0, e_1, e_2, \ldots\ldots., e_{14}, e_{15}$ are unit sedenions which contribute in the formation of a sedenion.
- $a_0, a_1, a_2 \ldots.., a_{15}$ are the co-efficient of the sedenion.

Here e_0 represents unitary part and $e_1, \ldots\ldots\ldots, e_{15}$ is an imaginary part.

A sedenion $a \epsilon S$ is represented in its real and vector part as:

$$a = \sum_{i=0}^{15} a_ie_i = a_0 + \sum_{i=1}^{15} a_ie_i$$

Let $\theta = [e_1, e_2, e_3, \ldots\ldots, e_{14}, e_{15}]$ such that an associated matrix of $16 * 16$ is generated from sedenion multiplication table M_a.

$$A_a^l = \begin{pmatrix} e_0 & \theta \\ -\theta^T & M_a \end{pmatrix}$$

The properties of sedenion with an example for each property is discussed in the following subsections.

A. IMPROPER ORDER

Other than real numbers, all hyper-complex numbers have improper order i.e., we cannot compare any two numbers belonging to the hyper-complex numbers. For example, consider the real numbers:

$$a < b$$
$$0 < c$$

we deduce:

$$ac < bc$$

However, in case of complex numbers $i = 0 + 1i$ and $0 = 0 + 0i$, we know:

$$0 < i$$

and

$$-1 < 1 \tag{5}$$

Multiplying both sides of equation 5 by i, we get:

$$-i < i$$

but

$$-i^2 \nless i^2 \tag{6}$$

The equation 6 does not hold as $1 \nless -1$. However, such results exist for complex or higher dimension algebra.

The improper order for non divisional algebra such as sedenion can also be proved from Sedenion Multiplication Table.

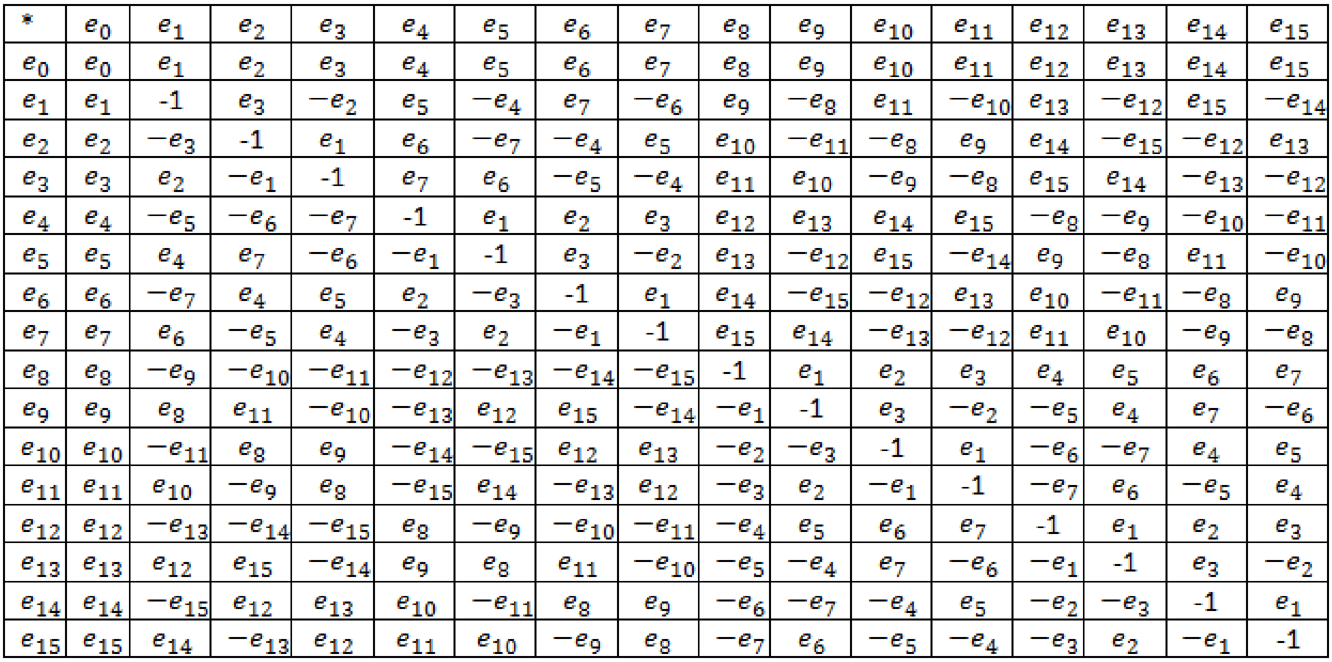
B. POWER ASSOCIATIVITY

Since octonion is alternative associative, sedenion looses alternativity as well. Let us consider three imaginary components from sedenion $e \in S$ i.e., e_2, e_4 and e_5. By associative law:

$$e_2.(e_4.e_5) = (e_2.e_4).e_5 \tag{7}$$

From multiplication table of sedenion, both side of equations should be equal, however equation 7 implies:

$$e_3 = -e_3$$



*	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}
e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	e_7	$-e_6$	e_9	$-e_8$	e_{11}	$-e_{10}$	e_{13}	$-e_{12}$	e_{15}	$-e_{14}$
e_2	e_2	$-e_3$	-1	e_1	e_6	$-e_7$	$-e_4$	e_5	e_{10}	$-e_{11}$	$-e_8$	e_9	e_{14}	$-e_{15}$	$-e_{12}$	e_{13}
e_3	e_3	e_2	$-e_1$	-1	e_7	e_6	$-e_5$	$-e_4$	e_{11}	e_{10}	$-e_9$	$-e_8$	e_{15}	e_{14}	$-e_{13}$	$-e_{12}$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3	e_{12}	e_{13}	e_{14}	e_{15}	$-e_8$	$-e_9$	$-e_{10}$	$-e_{11}$
e_5	e_5	e_4	e_7	$-e_6$	$-e_1$	-1	e_3	$-e_2$	e_{13}	$-e_{12}$	e_{15}	$-e_{14}$	e_9	$-e_8$	e_{11}	$-e_{10}$
e_6	e_6	$-e_7$	e_4	e_5	e_2	$-e_3$	-1	e_1	e_{14}	$-e_{15}$	$-e_{12}$	e_{13}	e_{10}	$-e_{11}$	$-e_8$	e_9
e_7	e_7	e_6	$-e_5$	e_4	$-e_3$	e_2	$-e_1$	-1	e_{15}	e_{14}	$-e_{13}$	$-e_{12}$	e_{11}	e_{10}	$-e_9$	$-e_8$
e_8	e_8	$-e_9$	$-e_{10}$	$-e_{11}$	$-e_{12}$	$-e_{13}$	$-e_{14}$	$-e_{15}$	-1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_9	e_9	e_8	e_{11}	$-e_{10}$	$-e_{13}$	e_{12}	e_{15}	$-e_{14}$	$-e_1$	-1	e_3	$-e_2$	$-e_5$	e_4	e_7	$-e_6$
e_{10}	e_{10}	$-e_{11}$	e_8	e_9	$-e_{14}$	$-e_{15}$	e_{12}	e_{13}	$-e_2$	$-e_3$	-1	e_1	$-e_6$	$-e_7$	e_4	e_5
e_{11}	e_{11}	e_{10}	$-e_9$	e_8	$-e_{15}$	e_{14}	$-e_{13}$	e_{12}	$-e_3$	e_2	$-e_1$	-1	$-e_7$	e_6	$-e_5$	e_4
e_{12}	e_{12}	$-e_{13}$	$-e_{14}$	$-e_{15}$	e_8	$-e_9$	$-e_{10}$	$-e_{11}$	$-e_4$	e_5	e_6	e_7	-1	e_1	e_2	e_3
e_{13}	e_{13}	e_{12}	e_{15}	$-e_{14}$	e_9	e_8	e_{11}	$-e_{10}$	$-e_5$	$-e_4$	e_7	$-e_6$	$-e_1$	-1	e_3	$-e_2$
e_{14}	e_{14}	$-e_{15}$	e_{12}	e_{13}	e_{10}	$-e_{11}$	e_8	e_9	$-e_6$	$-e_7$	$-e_4$	e_5	$-e_2$	$-e_3$	-1	e_1
e_{15}	e_{15}	e_{14}	$-e_{13}$	e_{12}	e_{11}	e_{10}	$-e_9$	e_8	$-e_7$	e_6	$-e_5$	$-e_4$	$-e_3$	e_2	$-e_1$	-1

FIGURE 1. Sedenion multiplication table.

This shows that associative property does not hold in sedenions. However, each sedenion element is multiplied with itself and output remains the same irrespective of its order i.e., let $e_1 \in e$ such that:

$$(e_1(e_1.e_1))e_1 = (e_1.e_1).(e_1e_1)$$

such an algebra is defined as power associative algebra.

C. ZERO DIVISOR

Sedenions are not a divisional algebra as zero divisors exist. In division algebra, the equation:

$$ab = 0$$

holds, if $a = 0$ or $b = 0$. In non-division algebra the equation:

$$ab = 0$$

holds, even if $a \neq 0, b \neq 0$. Moreno introduced 84 pairs of zero-divisors in sedenions. Each constitutes two base elements from sedenion, while one of them is from the triplets of octonions i.e.,

$$(o \pm s) = 0$$
$$(o - s)\,(o + s) = 0$$

For example:

$$\begin{aligned}&(a_1 + a_{13})(a_2 - a_{14})\\ &\quad = a_1 * a_2 - a_1 * a_{14} + a_{13} * a_2 - a_{13} * a_{14}\\ &\quad = a_3 - a_{15} + a_{15} - a_3\\ &\quad = 0\end{aligned}$$

D. OPERATION ON SEDENIONS

1) SEDENION MULTIPLICATION

Similar to octonions [33], sedenions are 16-dimensional vector space with an additional operation i.e., multiplication. Each sedenion is representable in the form of a matrix. This multiplication matrix is represented as follows:

- $e_0.e_i = e_i.e_0 = e_i$
- $e_i.e_i = -e_0$
- $e_i.e_j = -e_j.e_i \;\; i \neq j \neq 0$
- $e_i(e_j.e_k) = -(e_ie_j)e_k$ for $i \neq j$ and $i, j \neq 0$ and $e_ie_j \neq \pm e_k$

represents anti-commutativity of sedenions. The multiplication between to sedenions $a, b \in S$ are formally defined as:

$$a.b = [a_0.b_0 - a.b, b_0.a + a_0.b + a * b]$$

2) SEDENION ADDITION

In sedenion addition, we add the real part with the real one and imaginary part with the imaginary one. Let 'a' and 'b' be two sedenions.

$$\begin{aligned}a &= a_0e_0 + a_1e_1 + a_2e_2 +, \ldots\ldots, +a_{15}e_{15}\\ b &= b_0e_0 + b_1e_1 + b_2e_2 + +, \cdots\cdots, +b_{15}e_{15}\end{aligned}$$

The real parts in a and b are a_0 and b_0, while the rest are imaginary.

$$a + b = a_0e_0 + b_0e_0, \ldots\ldots\ldots\ldots\ldots, a_{15}e_{15} + b_{15}e_{15}$$

E. CONJUGATION

In abstract algebra the conjugate of a vector is, taking negative value of the imaginary part. According to Cayley-Dickson construction, conjugate value for sedenion is:

$$\begin{aligned} a &= \{a_0e_0 + a_1e_1 + a_2e_2+, \cdots\cdot, +a_{14}e_{14} + a_{15}e_{15}\} \\ a^* &= \{a_0e_0 - a_1e_1 - a_2e_2 - \cdots\cdots\cdot, a_{14}e_{14} - a_{15}e_{15}\} \end{aligned} \tag{8}$$

F. NORM OF SEDENION

Norm is the product of an element with its conjugate. The application of a norm is to assign a positive length to each vector in a vector space. The norm of sedenion 'a' i.e.,

$$a = [e_0 + e_1 \ldots\ldots\ldots\ldots\ldots e_{15}]$$

is:

$$\|a\| = \sqrt{e_0 + e_1 \ldots\ldots\ldots\ldots\ldots\ldots .e_{15}} \tag{9}$$

We know that $\|a\|^2 = aa^*$, which in case of isotropic vectors becomes $aa^* = 0$.

G. INVERSE AND DIVISION

The inverse of sedenion can be calculated by using the formula:

$$a^{-1} = a^*/||a|| \tag{10}$$

while, the norm and conjugate of 'a' can be calculated by using equation 9 and 8.

IV. NOISE FREE ENCRYPTION SCHEME

In this Section, efficient noise free encryption scheme is constructed over finite ring of integers Z_n. We assume a totally isotropic subspace of dimension one, to be closed under sedenion multiplication. It is known that a totally isotropic subspace of dimension $k \geq 8$ is actually determined by k isotropic sedenions since they constitute to form basis of subspace. In addition, each message is converted to a sedenion number which is compressed in terms of 1's and 0's to apply permutation through frobenius automorphism, as stated in preliminaries section.

A. KEY GENERATION

We choose two large prime numbers q_1 and q_2 according to our given security parameter k [line 2] such that $n = q_1 \times q_2$, which is an output mentioned in Algorithm 3 [line 3]. $V \in Z_n^{16}$ is the totally isotropic subspace which is closed under multiplication [line 7]. Let ϕ be the frobenius automorphism whose elements are obtained from Algorithm 2 [line 5]. Select a random invertible 16×16 matrix $K \in Z_n^{16\times16}$ [line 6]. The private key in Algorithm 3 is declared as (K, V) [line 9]. The system public parameter in Algorithm 3 is declared as (Z_n, ϕ).

Algorithm 3 KeyGeneration

```
 1: procedure KeyGen
 2:     Input: Given two prime numbers $q_1$ and $q_2$.
 3:     Output: $n = q_1q_2$
 4:     $Z_n$ : set of integers from 0 to $n - 1$.
 5:     $\phi$ : frobenius automorphism for $F_{p^{16}}$.
 6:     $K$ : random invertible $16 \times 16$ matrix.
 7:     $V$ : totally isotropic subspace contained in $Z_n^{16}$.
 8:     Public Key: $(Z_n, \phi)$
 9:     Private Key: $(K, V)$
10: end procedure
```

B. ENCRYPTION

Take a message $m \in Z_n$ and multiply it with the sedenion $i = [0, 1, 0, \ldots\ldots\ldots, 0]_{1\times16}$ to obtain the product mi, as shown in Algorithm 4 [line 4-5]. Select a random isotropic vector $z\epsilon V$, to convert chosen message belonging to Z_n to a sedenion $mi + z \in Z_n^{16}$ [line 6-7]. We take modulus of $mi + z$; $(mi + z)modp = a\epsilon F_{p^{16}}$, such that $F_{p^{16}}$ is a field constructed from polynomial ring $Z_p[x]$ [line 8-9]. Since $a \in F_{p^{16}}$, apply frobenius automorphism [line 11].

$$\phi(a) \longrightarrow (a^{p^d} = a')$$

An Associated matrix $A^l_{a'}$ is formed for sedenion message a', as mentioned in Algorithm 4 [line 12]. Hence, the cipher text is obtained by multiplying associated matrix $A^l_{a'}$ with the private key K, as mentioned in Algorithm 3 [line 14].
$C_m = K^{-1}A^l_{a'}K\epsilon Z_{16\times16}$.

Algorithm 4 CipherText Generation

```
 1: procedure CipherGen
 2:     Input: $m \in Z_n$
 3:     Output: $C_m \in Z_n^{16\times16}$
 4:     Since $i = [0, 1, 0, \ldots, 0]_{1\times16}$
 5:        $mi \longleftarrow m$
 6:     call algorithm 3 to obtain $V$. Since $z \in V \subset Z_n^{16}$
 7:        $mi + z \longleftarrow mi$
 8:     Take modulus of $mi + z$ with prime $p$;
 9:        $a \longleftarrow (mi + z)modp$
10:     call algorithm 2 to apply frobenius automorphism,
11:        $a' \longleftarrow \phi(a)$
12:     Take $\theta, -\theta^T, m'_0$ and $M_{a'}$ to generate $A^l_{a'}$.
13:     call Algorithm 3 to obtain invertible matrix $K$. Take
        $K$ and $K^{-1}$ such that:
14:        $C_m \longleftarrow K^{-1}A^l_{a'}K$
15: end procedure
```

C. DECRYPTION

Since the proposed scheme involves frobenius automorphism in encryption which is bijective, hence it's inverse mapping also exists and we require ϕ^{-1} in decryption with
$1 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]_{1\times16}$
such that

$$mi = ((\phi^{-1}(1(KC_mK^{-1})))modp)modV \tag{11}$$

Algorithm 5 Plaintext Generation

```
1:  procedure PlainGen
2:      Input:call algorithm 4 to obtain $C_m \in Z_n^{16\times 16}$.
3:      Output: $mi \in Z_n^{16}$
4:      $A^l_{a'} \longleftarrow KC_mK^{-1}$.
5:      Take $1 = [0, 1, 0, \dots, 0]_{1\times 16} \in Z_n^{16}$
6:        $a' \longleftarrow 1A^l_{a'}$.
7:      Since $\phi(a) = a'$
8:        $\phi(a) \longleftarrow a'$
9:      Apply $\phi^{-1}$ to get $a$.
10:     Since $a = (mi + z)modp$
11:       $(mi + z) \longleftarrow amodp$
12:     Since $z \in V$
13:       $mi \longleftarrow (mi + z)modV$
14: end procedure
```

We know that $C_m = K^{-1}A^l_{a'}K$ hence, Step 1 of Algorithm 5 clearly shows when we replace C_m in equation 11 we get

$$mi = ((\phi^{-1}(1(KK^{-1}A^l_{a'}K^{-1}K)))modp)modV$$

while we know that

$$\begin{aligned} KK^{-1} &= K^{-1}K = I \\ mi &= ((\phi^{-1}(1(A^l_{a'})))modp)modV \end{aligned}$$

Since we know

$$1 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]_{1\times 16}$$

and

$$A^l_{a'} = \begin{pmatrix} a'_0 & \theta \\ -\theta^T & M_a \end{pmatrix}$$

While, we know that

$$\begin{aligned} 1A^l_{a'} &= [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]_{1\times 16} \begin{pmatrix} a_{0'} & \theta \\ -\theta^T & M_a \end{pmatrix} \\ &\times [1, 0, 0, \dots\dots, 0]_{1\times 16} \\ &\times \begin{pmatrix} a'_0 & a'_1 & - & - & - & a'_{15} \\ -a'_1 & -a_0 & - & - & - & -a_{14} \\ -a'_2 & -a_3 & - & - & - & a_{13} \\ -a'_3 & a_2 & - & - & - & -a_{12} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -a'_{15} & a_{14} & - & - & - & -a_0 \end{pmatrix} \end{aligned}$$

Step 2 shows that the product of 1 and $A^l_{a'}$ results in an array of sedenion elements a' i.e., $a' = [a'_0, a'_1, a'_2, \dots\dots, a'_{15}]$, as stated in algorithm 5 [line 7]. In [line 9] of algorithm 5 inverse mapping is applied $mi = ((\phi^{-1}(\phi(a)))modp)modV$ $\because a = (mi + z)modp \Leftrightarrow (mi + z) = amodp$ [line 10-11]. While in step 5 and 6 modulus is applied [line 11-13] such that;

$$\begin{aligned} mi &= (amodp)modV \\ &= (mi + z)modV \end{aligned}$$

$$(mi + z)modV = mi \tag{12}$$

since $z \in V$

D. HOMOMORPHIC OPERATIONS

The proposed scheme is designed to perform homomorphic operations on the produced ciphertext. The operations performed are:

- Addition
- Multiplication

1) ADDITION

The ciphertext C_{m_0}, C_{m_1} obtained for messages m_0 and m_1 are 16 ∗ 16 matrices. These matrices addition and subtraction is component wise, similar to normal matrix addition/subtraction i.e.,

$$C_{m_0+m_1} = C_{m_0} + C_{m_1} \tag{13}$$

2) MULTIPLICATION

Multiplication of ciphertexts obtained through pre-defined encryption scheme is similar to matrix multiplication as each ciphertext $C_{m_0}, C_{m_1} \in Z_n^{16*16}$ such that

$$\begin{aligned} C_{m_0*m_1} &= C_{m_0}C_{m_1} \\ &= K^{-1}A^l_{a'_0}KK^{-1}A^l_{a'_1}K \\ &= K^{-1}A^l_{a'_0}A^l_{a'_1}K \end{aligned} \tag{14}$$

However it's decryption also requires ciphertext of -1 i.e.,

$$\begin{aligned} &C_{-1} \\ &= ((\phi^{-1}(1(K^{-1}KA^l_{a'_0}K^{-1}KA^l_{a'_1}K^{-1}KA^l_{-1}K)))modp)modV \end{aligned}$$

Since,

$$KK^{-1} = K^{-1}K = I$$

The result obtained is:

$$= \phi^{-1}(1(A^l_{a'_0}A^l_{a'_1}A^l_{-1}))$$

where we know that the product of 1 with $A^l_{a'_0}A^l_{a'_1}A^l_{-1}$ results in $a'_0a'_1a'_{-1}$.

$$\begin{aligned} Dec(key, C_{m_0*m_1}) &= \phi^{-1}(a'_0a'_1a'_{-1})modV \\ &= ((\phi^{-1}(\phi(a_0)\phi(a_1)\phi(a_{-1})))modp)modV \\ &= ((a_0modp)(a_1modp)(a_{-1}modp))modV \end{aligned}$$

where we know that:

$$(m_0i + z_0)modp = a_0 \Longleftrightarrow (m_0i + z_0) = a_0modp \tag{15}$$

$$(m_1i + z_1)modp = a_1 \Longleftrightarrow (m_1i + z_1) = a_1modp \tag{16}$$

$$(-i + z_2)modp = a_{-1} \Longleftrightarrow (-i + z_2) = a_2modp \tag{17}$$

we obtain equation:

$$= ((m_0i + z_0)(m_1i + z_1)(-i + z_2))modV$$

Since $z_0, z_1, z_2 \in V$ i.e an totally isotropic subspace we obtain:

$$= (m_0 m_1 i^2)(-i)$$

Ciphertext of -1 is necessary to be involved in ciphertext multiplication because if it's not involved than the product of $m_0 i$ and $m_1 i$ results in $-m_0 m_1$ which is not the original message we had before homomorphic multiplication.

$$= (m_0 m_1(-1))(-i) = (m_0 m_1)(-(-i))$$

which implies;

$$= m_0 m_1 i$$

E. APPLICATION OF NOISE-FREE ENCRYPTION SCHEME

In this section, we present an application to propose a noise-free encryption scheme in a *cloud*. Two parties are involved: one is *Alice* who is a credit controller, and the second one is *cloud* who is the service provider.

Being a Credit Controller, *Alice* is involved in recoveries from clients and deals with client aging files. She wants to place her confidential documents on the *cloud*. However, she wants them to be encrypted in a way that she can work over them without decrypting. The *cloud* provides her with the computation resources and is unaware of what computations have been performed by *Alice* or what output she had gained. Each time the protocol performs computation on the garbled data, the system design receives obfuscated data and encrypts her document according to the scheme propose.

However, before encryption, cryptographic public and private keys are required which are generated using Algorithm 3. Oracle chooses two larger prime numbers p and q to form their product n Algorithm 3 [line 2 and 3]. This n provides *Alice* with the total number of integers present in the set Z i.e., Z_n Algorithm 3 [line 4]. This is *Alice*'s public key.

Moreover, the key K_{16*16} is formed by the oracle Algorithm 3 [line 6] in a way that the absolute value of the diagonal element of each row is greater than the sum of absolute values of non-diagonal row elements. The text is then converted into a 16-dimensional vector space by multiplying it with an $i \in S$ given in Algorithm 4 [line 5], (the second component of sedenion number while other remain zero) and then added by a randomly chosen isotropic vector from totally isotropic vector subspace Algorithm 4 [line 6-7]. The oracle compresses this 16-dimensional sedenion by taking it's modulus from p i.e., $(mi + z)modp$ to obtain $a \in Z_p^{16}$ 4 Algorithm 4 [line 8-9]. Now apply frobenius automorphism over it which returns modified form of a i.e a' (16-dimensional vector space) Algorithm 4 [line 10-11]. This automorphism performed over a involves permutation over our compressed message. An associated matrix A_a^l is formed for each a' Algorithm 4 [line 12], which is then multiplied with randomly chosen invertible key K_{16*16}. The product provides a ciphertext C_m [line 14] of our message in the form of 256 + 16 variables and 256 multivariate equations.

To perform some operations over the ciphertext obtained, *Alice* doesn't need to decrypt her files according to the proposed scheme. The introduced scheme also helps her to perform operations over encrypted text. Lets assume *Alice* has encrypted two text messages m_0 and m_1, for which the ciphertext she has obtained is C_{m_0} and C_{m_1}. She can perform addition operation over these ciphertext using equation 13 and performs multiplication operation over these ciphertexts through matrix multiplication using equation 14.

Since, the ciphertext obtained is a $16*16$ matrices as given in Algorithm 5 [line 2]. In order, to obtain her desired result, *Alice* decrypts her document. To do that, ciphertext of -1 i.e., C_{-1} and inverse mapping ϕ^{-1} is necessary. In a nutshell, the decryption of the product of two ciphers is reverse of encryption. The system design apply these operations in reverse that is we know that the associated matrices $A^l_{a'_0}$, $A^l_{a'_1}$ and A^a_{-1} are obtained from the sedenion messages a_0, a_1 and -1. So in order to obtain each of these messages we multiply unit sedenion i.e., $1 = [1, 0, 0, \ldots.., 0]$ with these associated matrices and obtain a'_0, a'_1, a'_{-1} [line 6] which are obtained from $\phi(a_0), \phi(a_1), \phi(a_{-1})$ over which inverse frobenius mapping ϕ^{-1} is applied [line 9]. Since, we know each a'_0, a'_1, a'_{-1} is obtained from $(m_0 i + z_0)modp$, $(m_1 i + z_1)modp$ and $(-i + z_2)modp$, by using modulus property, we calculate $m_0 i + z_0$, $m_1 i + z_1$ and $-i + z_2$ [line 11]. Now, the vectors z_0, z_1, z_2 are isotropic i.e., $z_0, z_1, z_2 \in V$. The oracle provides *Alice* with her desire result.

Hence, the technique propose isn't just convenient for the user but also provide user with the remote access, requiring data to move back and forth between user and *cloud*.

V. SECURITY ANALYSIS AND DISCUSSION

In this section, we are discussing the credibility and efficiency of the proposed scheme. This scheme isn't just responsible for providing secure and efficient encryption but homomorphic operations are also applied over chosen ciphertexts. Since it is based on finite field and linear algebra, it lies under the umbrella of a multivariate cryptosystem. Moreover, many mathematical concepts are involved which enhance the potency of the proposed scheme.

Till now, a lot of work has been done to analyze the security and efficiency of FHE schemes. According to Brakerski [4], the decryption of scheme should not be weakly learnable, if it evaluates function homomorphically. Hence, FHE schemes which are linearly decryptable such as OctoM and Sedenion based, they are not secure in chosen plaintext attacks. While in [22] wang *et al.* showed that they are not secure even in ciphertext only attack and have relaxed the definition to weak ciphertext only attack. Since the proposed scheme is also linearly decryptable, the same analysis of security is performed.

To begin with, ciphers which are based on hyper-complex numbers, their efficiency relies on high dimension and matrix-vector multiplication. Whereas, the security of the scheme depends on several factors. The scheme presented ensures the avalanche effect which is a fundamental cryptographic property, achieve by any encryption scheme. It makes statistical analysis as complex as possible. Similarly, the two properties of cryptography 'confusion' and 'diffusion' for the proposed scheme are discussed as below.

A. DIFFUSION

Any change in the message $m \in Z_n$, that we select for encryption before converting it to a 16- dimensional sedenion number is enough to have an impact on the ciphertext matrix C_m that we obtain. This impact is due to the matrix multiplication involve. For each message m we have $mi + z$ which is different in each case. Thus, the matrix multiplication, to obtain ciphertext is sufficient to cause diffusion in introducing the scheme.

Now, we move to the modulus of $mi+z$ with p, over which finite field $F_{p^{16}}$ is defined. It is a major feature other than matrix-vector multiplication for improving the security of the presented scheme. The Frobenius automorphism over a finite field $F_{p^{16}}$ is made public because modulus p, compresses mi+z in terms of $1's$ and $0's$. This compression results in a 16-dimensional vector which belongs to $F_{p^{16}}$ and proves to be substantially resistant against cryptanalysis.

In theorem 2, we show that the probability of finding a statistical relationship between plaintext and ciphertext is approximately zero.

Theorem 2: For a randomly selected messages $m_0, m_1 \cdots m_n$ *and ciphertext* $c_0, c_1 \cdots c_n$*. If there is a probabilistic polynomial-time algorithm 'D' that is used to guess some relationship between plain text and ciphertext, then we have*:

$$Prob(D(m_0, m_1 \cdots m_n = C_0, C_1 \cdots C_n) = 1) = negl(\kappa) \tag{18}$$

Proof: As invertible matrix and associated matrix contribute to ciphertext generation while the plaintext is a normal message. For the adversary to perform some statistical analysis to fetch relevant information from a given plaintext and ciphertext is:

$$C_m = K^{-1}A^l_{m'}K \epsilon Z_n^{16*16} \tag{19}$$

$$m \in Z_n \tag{20}$$

From equation 19, the ciphertext consist of associated matrix and invertible matrix. Since the associated matrix consists of real and imaginary parts $mi + z$. The ciphertext is a combination of real and imaginary parts. In equation 20, the message consists of the only real part.

As a result, according to equation 18 to perform statistical analysis on two ensembles that have different distributions is equal to negligible function. There is no such probabilistic polynomial-time algorithm that is used to perform statistical analysis on two different ensembles. □

B. CONFUSION

The matrix key involves the encryption of plaintext is itself a non-linear pattern sufficient for creating a drastic effect on output. In the proposed scheme, ciphertext security is proportional to the non-linearity of randomly chosen matrix K_{16*16}. Similarly, a totally isotropic subspace involve as part of a private key is also responsible for generating confusion. The sum of our message mi with randomly chosen $z \epsilon V \subset Z_n^{16}$ causes confusion in the matrix multiplication. Hence, any change in the unit component of a sedenion message $mi + z$ before modulus with p results in a different $a \in F_{p^{16}}$, a different mapping, leading to the formation of a different associated matrix $A^l_{a'}$, which creates a complex statistical relationship between $A^l_{a'}$ and C_m. So, the small differences before the matrix multiplication result in large differences after the matrix multiplication.

In theorem 3, we show that the probability for an adversary to retrieve the private key from the given cipher text is approximately equal to zero.

Theorem 3: For a randomly selected message m_1*, we have a ciphertext* $C_{m_1} = K^{-1}A^l_{m_1}K$*. If an adversary has access to a set of ciphertext and also have a knowledge of plain text, then for all probabilistic polynomial time algorithm that is used to select correct plain text and guess the private key is*:

$$Prob(((C_{m_1} = m_1) = 1) = PK = 1) = negl(\kappa)$$
$$where \begin{cases} C_{i'} = 1 & if \quad for\ each\ C_i\ we\ have\ the\ correct\ m_i; \\ C_{i'} = 0 & otherwise; \end{cases} \tag{21}$$

where Pk is the private key

$$where = \begin{cases} PK = 1, & if\ private\ key\ is\ guessed\ correctly; \\ PK = 0, & otherwise; \end{cases}$$

Proof: First the probability to guess a real number from imaginary number is approximately zero. As the ciphertext consists of associated matrix which is combination of real and imaginary part while the plain text only consists of real part. The probabilistic polynomial time algorithm that is used to guess plaintext from ciphertext is:

$$Prob((C_{m_1} = m_1) = 1) = negl(\kappa) \tag{22}$$

From the above equation, there is no probabilistic polynomial time algorithm that is used to find the corresponding plaintext for the given ciphertext, as the ensemble belongs to two different distributions. Now lets assume that in known ciphertext attack, the adversary also has access to a set of plaintext for the given ciphertext. Then for the adversary to correctly guess the private key (K, V) is

$$Prob(((C_{m_1} = m_1) = 1) = PK = 1) = negl(\kappa) \tag{23}$$

In this scheme, we have multiple private keys. First for the adversary to choose the isotropic subspace which is closed under Z_n^{16} require a lot of computation. The second challenge for the adversary is to choose isotropic vector for each message from the given isotropic subspace. The third challenge for the adversary is to choose random invertible matrix K from Z_n^{16*16}. At the end a lot of computation is required for the adversary to have access to all the private keys and the probability that he is successful in finding the correct private keys is equal to negligible function. □

In the proposed scheme, we have multiple private keys. Lets assume the adversary has access to one of the private keys. For the adversary to correctly decrypt the given cipher text by knowing one of the private key is not possible as given in theorem 4:

Theorem 4: If one of the private key is compromised what is its effect on rest of the keys? The private keys are isotropic subspace "V", and Invertible matrix "K".

Proof: In the proposed scheme, we have two private keys. The first one is isotropic subspace. The isotropic vector for each message belongs to this isotropic subspace. The second private key is invertible matrix which is chosen randomly. As both of the private keys belong to different distributions, so they are independent. To correctly decrypt the cipher text, one must have accessed to both the private keys. As a result, if an adversary has access to one of the private key, still he is not able to decrypt the given ciphertext. □

Theorem 5: For a randomly selected $a \in F_{2^{16}}$, the probabilistic polynomial time algorithm to determine $mi + z$ from a is negligible.

$$Pr[(mi + z = amodp) = 1] = negl(\kappa) \tag{24}$$

Proof: We know that $mi + z \in Z_n^{16}$, it is impossible for an adversary to deduce $mi + z$ from $amodp$, since $z \in V$, which is a private key. Thus, its security lies in a fact that it is computationally infeasible for an adversary to deduce an isotropic vector from V. □

C. COMPUTATIONAL COMPLEXITY OF FROBENIUS AUTOMORPHISM

The Frobenius automorphism defined over sedenion involves 65536 mapping. This number itself is an untouchable number, which cannot be expressed as the sum of proper divisors belonging to Z^+. Moreover, the multi-point evaluation algorithm is introduced in the above section since it is effective in reducing the computational complexity of Frobenius automorphism, according to which: for polynomial in $R[x]$ of degree less than n at n points involves $O(M(n)logn)$ operations. According to theorem [22] i.e.,

Theorem 6: Algorithm works correctly as specified and uses $\mathcal{O}(M(n)^2 lognlogd)$ operations in F_q.

Proof: For correctness, invariant $\xi_k = \zeta^{q^k}$ for $0 \leq k \leq 2^i$ by induction on i. For induction step it is sufficient to prove the claim for $k > 2^{i-1}$. For $1 \leq j \leq 2^{i-1}$, we have that

$$\xi_{2^{i-1}+j} = \check{\xi}_{2^{i-1}}(\xi_j) = \check{\xi}_{2^{i-1}}(\zeta^{q^j}) = (\check{\xi}_{2^{i-1}}(\zeta))^{q^j} = \xi_{2^{i-1}}^{q^k}$$

$$\xi_{2^{i-1}+j} = (\zeta^{q^{2^{i-1}}})^{q^j} = \zeta^{q^{2^{i-1}+j}}$$

by step 2. Finally in step 3, we correctly compute

$$\delta_k = \check{\alpha}(\xi_k) = \check{\alpha}(\zeta^{q^k}) = \check{\alpha}(\zeta)^{q^k} = \alpha^{q^k}$$

for $0 \leq k \leq d$. In step 2, 3 of algorithm, we solve $l + 1 \in \mathcal{O}(logd)$ multi-point evaluation problems at a cost of $\mathcal{O}(M(n)^2 lognlogd)$ operation in F_q. □

D. MULTIVARIATE/UNIVARIATE EQUATIONS

For a message m' we have 16 variables and 256 variables for matrix K. What we get is 256 equations with 256 + 16 unknown variables. So for t messages we have $256t$ equations with $256 + 16t$ unknowns variables. The multivariate equations resulting from sedenion encryption are large enough to not be solved by a linearlization, relinearlization or Grobner base algorithm that makes them computationally infeasible.

In the Grobner [34] algorithm, monomials with appropriate coefficients are removed after the combination of two equations. This cycle is repeated until we have a univariate equation, i.e. all variables except one are removed. Since the degree of the remaining monomials increases rapidly during the elimination process and the time complexity of the algorithms makes it impractical to solve. Linearlization is known to be a naive algorithm, as each monomial is replaced by a new variable to solve the resulting linear system of equations, such that a number of equations are equal to a number of variables, using the Gauss elimination process. If we find all the yij values, we consider two possible values for each xi since we have a square root of yii. When relinearlizing, it adds a variety of variables. This substitution results in the development of more linearly independent equations that are practically impossible to solve by relinearlization. It is important to have a single solution for such equations, because variables represent a text message in cryptographic techniques defined over finite fields. Thus, these methods are not helpful and show that the proposed scheme is NP-hard to the adversary.

VI. CONCLUSION

In this paper, we have presented an efficient noise-free FHE scheme over sedenion. In the proposed scheme, a 16-dimensional vector is first used to convert the original message into a 16-dimensional vector space. For each message, one sedenion vector is required so for n messages, n sedenion vectors are required to convert it. Then the isotropic vector is used as padding to this message and compresses it by taking $modp$. The compressed message is permuted by using Frobenius automorphism. An associated matrix is generated for each permuted value and then multiplied with a randomly chosen invertible matrix. The ciphertext generated is in the form of a multivariate polynomial equation. For n messages the number of multivariate polynomial equations is $256+16n$. The hardness of the multivariate polynomial equation lies in solving these equations. These techniques add more security to the proposed scheme. Similarly, matrices are involved to perform different operations which are considered fast. So the proposed scheme is effective both in terms of security and efficiency.

ACKNOWLEDGMENT

The authors would like to show their gratitude to Prince Sultan University, Riyadh, Saudi Arabia for funding this paper. They specially thank the Robotics and Internet-of-Things

Lab (RIOTU) at the Prince Sultan University, Riyadh, Saudi Arabia.

REFERENCES

[1] M. C. Compagnucci, J. Meszaros, T. Minssen, A. Arasilango, T. Ous, and M. Rajarajan, ‘‘Homomorphic encryption: The ‘holy grail’ for big data analytics and legal compliance in the pharmaceutical and healthcare sector?’’ *Eur. Pharmaceutical Law Rev.*, vol. 3, no. 4, pp. 144–155, 2019.

[2] C. Gentry, ‘‘Fully homomorphic encryption using ideal lattices,’’ in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, 2009, pp. 169–178.

[3] I. Mustafa, I. U. Khan, S. Aslam, A. Sajid, S. M. Mohsin, M. Awais, and M. B. Qureshi, ‘‘A lightweight post-quantum lattice-based RSA for secure communications,’’ *IEEE Access*, vol. 8, pp. 99273–99285, 2020.

[4] Z. Brakerski and V. Vaikuntanathan, ‘‘Fully homomorphic encryption from ring-LWE and security for key dependent messages,’’ in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2011, pp. 505–524.

[5] J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, ‘‘Fully homomorphic encryption over the integers with shorter public keys,’’ in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2011, pp. 487–504.

[6] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, ‘‘Fully homomorphic encryption over the integers,’’ in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2010, pp. 24–43.

[7] C. Gentry and S. Halevi, ‘‘Fully homomorphic encryption without squashing using depth-3 arithmetic circuits,’’ in *Proc. IEEE 52nd Annu. Symp. Found. Comput. Sci.*, Oct. 2011, pp. 107–109.

[8] J. Alperin-Sheriff and C. Peikert, ‘‘Practical bootstrapping in quasilinear time,’’ in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2013, pp. 1–20.

[9] N. P. Smart and F. Vercauteren, ‘‘Fully homomorphic encryption with relatively small key and ciphertext sizes,’’ in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, 2010, pp. 420–443.

[10] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, ‘‘TFHE: Fast fully homomorphic encryption over the torus,’’ *J. Cryptol.*, vol. 33, no. 1, pp. 34–91, Jan. 2020.

[11] G. Du, C. Ma, Z. Li, and D. Wang, ‘‘Towards fully homomorphic encryption from gentry-Peikert-Vaikuntanathan scheme,’’ in *Proc. Int. Conf. Cloud Comput. Secur.* Cham, Switzerland: Springer, 2017, pp. 256–267.

[12] A. El-Yahyaoui and M. D. E.-C. El Kettani, ‘‘A verifiable fully homomorphic encryption scheme for cloud computing security,’’ *Technologies*, vol. 7, no. 1, p. 21, Feb. 2019.

[13] K. L. Offner, E. Sitnikova, K. Joiner, and C. R. MacIntyre, ‘‘Towards understanding cybersecurity capability in Australian healthcare organisations: A systematic review of recent trends, threats and mitigation,’’ *Intell. Nat. Secur.*, vol. 35, no. 4, pp. 556–585, Jun. 2020.

[14] Z. Chen, W. Wang, X. Yan, and J. Tian, ‘‘Cortex-AI on blockchain,’’ Cortex Labs Pte. Ltd., Singapore, Tech. Rep. 201803307C, 2018.

[15] Z. Brakerski and V. Vaikuntanathan, ‘‘Efficient fully homomorphic encryption from (standard) LWE,’’ *SIAM J. Comput.*, vol. 43, no. 2, pp. 831–871, 2014.

[16] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, ‘‘(Leveled) fully homomorphic encryption without bootstrapping,’’ *ACM Trans. Comput. Theory*, vol. 6, no. 3, pp. 1–36, Jul. 2014.

[17] Z. Brakerski, ‘‘Fully homomorphic encryption without modulus switching from classical GapSVP,’’ in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2012, pp. 868–886.

[18] D. W. H. A. da Silva, C. P. de Araujo, E. Chow, and B. S. Barillas, ‘‘A new approach towards fully homomorphic encryption over geometric algebra,’’ in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2019, pp. 241–249.

[19] J. Alperin-Sheriff and C. Peikert, ‘‘Faster bootstrapping with polynomial error,’’ in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2014, pp. 297–314.

[20] M. Li, ‘‘Leveled certificateless fully homomorphic encryption schemes from learning with errors,’’ *IEEE Access*, vol. 8, pp. 26749–26763, 2020.

[21] Y. Wang and Q. M. Malluhi, ‘‘Privacy preserving computation in cloud using noise-free fully homomorphic encryption (FHE) schemes,’’ in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2016.

[22] Y. Wang and Q. M. Malluhi, ‘‘Privacy preserving computation in cloud using noise-free fully homomorphic encryption (FHE) schemes,’’ in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2016, pp. 301–323.

[23] A. Korniłowicz, ‘‘Cayley-dickson construction,’’ *Formalized Math.*, vol. 20, no. 4, pp. 281–290, Dec. 2012.

[24] C. Kızılateş and S. Kırlak, ‘‘A new generalization of fibonacci and Lucas type sedenions,’’ Dept. Math., Zonguld, Bulent Ecevit Univ., Zonguldak, Turkey, Tech. Rep. 2020030133, 2020.

[25] A. Cariow and G. Cariowa, ‘‘An algorithm for fast multiplication of sedenions,’’ *Inf. Process. Lett.*, vol. 113, no. 9, pp. 324–331, May 2013.

[26] P. Dembowski, *Finite Geometries: Reprint of the 1968 Edition*. Berlin, Germany: Springer, 1977.

[27] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann, *Error-Correcting Linear Codes: Classification by Isometry and Applications*, vol. 18. Berlin, Germany: Springer, 2006.

[28] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, ‘‘Efficient algorithms for solving overdefined systems of multivariate polynomial equations,’’ in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2000, pp. 392–407.

[29] J. Von Zur Gathen and J. Gerhard, *Modern Computer Algebra*. Cambridge, U.K.: Cambridge Univ. Press, 2013.

[30] A. Bostan and É. Schost, ‘‘On the complexities of multipoint evaluation and interpolation,’’ *Theor. Comput. Sci.*, vol. 329, nos. 1–3, pp. 223–235, Dec. 2004.

[31] B. Petrenko, ‘‘Primitive elements in finite fields,’’ ProQuest Dissertations Publishing, Univ. Illinois Urbana-Champaign, Champaign, IL, USA, 2004.

[32] J. Von Zur Gathen and J. Gerhard, ‘‘Modern computer algebra,’’ in *Iterated Frobenius, Berlekamp, Kaltofen-Lobos*. Cambridge, U.K.: Cambridge Univ. Press, 2013, pp. 1–399.

[33] I. Mustafa, T. Khan, M. Alam, N. Javaid, A. Khan, and A. Akhunzada, ‘‘Post-quantum cryptographic communication protocol,’’ U.S. Patent 10 581 604, Mar. 3, 2020.

[34] D. Smith-Tone, ‘‘Extracting linearization equations from noisy sources,’’ IACR, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 2018/539, 2018, p. 539.

IQRA MUSTAFA received the master's degree in information security from COMSATS University Islamabad, Pakistan, in 2019. She is currently pursuing the Ph.D. degree in cybersecurity with the Nimbus Research Center, Cork Institute of Technology (CIT), Ireland. Her research interests include cryptography, data science, machine learning, generative adversarial networks, blockchain, network security, wireless networks, smart grid, and cloud computing. She also served as TPC member and an invited Reviewer for international journals and conferences.

HASNAIN MUSTAFA is currently pursuing the master's degree with COMSATS University Islamabad, Pakistan. He is also working as a Software Engineer and a Data Analyst with Telecom Regulatory Authority, Dubai, UAE. He has also more than five years of hands-on experience in object-oriented analysis and design (OOAD), database design and implementation, .NET framework, C#, ASP.NET, ASP.NET MVC, T-SQL, Web API, Python, big data analysis tools (Tableau and Sisense), complete global distribution system integration, B2B software development, robotic process automation, and system administration. His research interests include machine learning, artificial intelligence, network security, and cryptography.

AHMAD TAHER AZAR (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees from the Faculty of Engineering, Cairo University, Egypt, in 2006 and 2009, respectively. He is a Research Professor with Prince Sultan University, Riyadh, Saudi Arabia. He is also an Associate Professor with the Faculty of Computers and Artificial Intelligence, Benha University, Egypt. He worked in the areas of control theory and its applications, process control, chaos control and synchronization, nonlinear control, robust control, and computational intelligence. He workied as an Associate Editor for the IEEE Transactions on Neural Networks and Learning Systems, from 2013 to 2017, and *ISA Transactions* (Elsevier), from 2018 to 2020. He is the Editor-in-Chief of the *International Journal of System Dynamics Applications* (IJSDA) (IGI Global, USA) and the *International Journal of Intelligent Engineering Informatics* (IJIEI) (Inderscience Publishers, Olney, U.K.). He is currently an Associate Editor of the IEEE Systems Journal.

SHERAZ ASLAM (Member, IEEE) received the B.S. degree in computer science from Bahauddin Zakariya University (BZU), Multan, Pakistan, in 2015, and the M.S. degree in computer science with a specialization in energy optimization in the smart grid from COMSATS University Islamabad (CUI), Islamabad, Pakistan, in 2018. He is currently pursuing the Ph.D. degree with the DICL Research Laboratory, Cyprus University of Technology (CUT), Limassol, Cyprus, under the supervision of Dr. H. Herodotou. He also worked as a Research Associate with Dr. N. Javaid during the M.S. degree period at the same University. He has authored more than 35 research publications in ISI-indexed international journals and conferences such as the IEEE Internet of Things (IoT) Journal, the IEEE Access, *Electrical Power System Research*, and *Energies*. He is also a part of European Union funded research project named as STEAM. He also served as a TPC member and an invited Reviewer for international journals and conferences. His research interests include data analytics, generative adversarial networks, network security, wireless networks, smart grid, and cloud computing.

SYED MUHAMMAD MOHSIN is currently pursuing the Ph.D. degree with COMSATS University Islamabad, Pakistan. His research work appears in impact factor international journals and high-ranked national/international conferences. His areas of interest include cyber security, the Internet of Things, edge computing, energy management, and quantum computing.

MUHAMMAD BILAL QURESHI is working as an Assistant Professor with the Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, Pakistan. He has worked with HPC Lab, KAU, Saudi Arabia, on many funded projects. He is currently working on the 2030 Vision Project with IAU, KSA. He has authored many research publications in SCI-E journals, including IEEE Access, the *Journal of Grid Computing*, *Parallel Computing*, the *Journal of Parallel and Distributed Computing*, *The Journal of Supercomputing*, and *Sustainable Cities and Society*. His research interests span the areas of data-intensive real-time systems, data-intensive smart systems, resource allocation problems in HPC systems, and the energy efficient IoT. He was a recipient of many prestigious awards, including Gold Medal in undergraduate degree, the HEC Pakistan Indigenous Scholarship for the M.S. and Ph.D. degree studies, and research productivity awards, in 2014 and 2015.

NOUMAN ASHRAF received the B.S. degree in electrical (telecommunication) engineering and the M.S. degree in electrical (control systems) engineering from COMSATS University Islamabad, Pakistan, in 2012 and 2015, respectively, and the Ph.D. degree in electrical engineering from Frederick University, Nicosia, Cyprus, through the Erasmus Mundus Scholarship Program. He is currently a Postdoctoral Researcher with the Telecommunication Software and Systems Group, Waterford Institute of Technology, Ireland. His research interests include the applications of control theory for the management of emerging networks.