O-GGH: THE GGH PUBLIC KEY CRYPTOSYSTEM VIA OCTONION ALGEBRA AND POLYNOMIAL RINGS

Massoud Sokouti [1], Babak Sokouti [2]

[1] Nuclear Medicine Research Center, Mashhad University of Medical Sciences
[2] Biotechnology Research Center, Tabriz University of Medical Sciences
e-mails: b.sokouti@gmail.com; sokoutib@tbzmed.ac.ir
Iran

Abstract: Designing new and improving existing lattice-based public key cryptosystem have attracted attentions in the literature. The Goldreich, Goldwasser and Halevi (GGH) was one of those first proposed lattice based encryption algorithms. The closest vector problem (CVP) and the shortest vector problem (SVP) are considered for lattice complexity and difficulty. Although, the GGH cryptosystem is known as broken for dimensions of 400, however, proposing improvements can make resistance against lattice reductions. In this study, a novel approach for improving GGH cryptosystem is presented by taking advantage of octonion algebra (known as non-commutative and non-associative algebra) and polynomial rings to tackle with the shortcomings of the original GGH and its variants. The new proposed O-GGH increases the security and complexity of GGH. The key generation, encryption, and decryption procedures of O-GGH have been discussed in details. And, it has been shown that O-GGH is resistant to lattice based attacks at even lower values of dimensions (i.e., 50).

Key words: GGH; O-GGH; polynomial ring; octonion algebra; improvement.

1. INTRODUCTION

The rapid growth of network communications, applications use, and information exchange whether they are public or private, clearly presents the need for developing broader security environments [1]. For this purpose, several critical security services need to be satisfied among which confidentiality, integrity, and availability (known as CIA triad) are of great importance [2]. By applying these along with authentication, authorization, identification, and non-repudiation, one may be assured of a secure communication channel, however, emerging high performance and fast computing cryptographic algorithms are still essential for community of information security [3]. For instance, by providing confidentiality, sending and receiving data between sender and receiver via Internet, will be performed using a secure communication channel. Encrypting the data will be a guarantee for a secure sending from sender and decrypting the data will provide a secure way for revealing the data on the receiver part; this will be simple way for keeping a high number of hackers from spying the secure channel. Symmetric and asymmetric ciphers are two well-known cipher systems [4]. The encryption

and decryption in symmetric cryptosystem is done by only one shared key between sender and receiver while two private and public keys are used in asymmetric cipher system for encryption and decryption, respectively. Several studies including the improvement and cryptanalysis on symmetric ciphers (i.e., classic and modern [5-8]) have been conducted but none of them could be considered as secure as the asymmetric ciphers. The RSA and ElGamal are known to be of good asymmetric ciphers in terms of speed and security [9, 10], however, after the successful development of quantum computers, these ciphers can be easily attacked and broken due to the factorization problem [11]. The lattice based ciphers are another kind of asymmetric ciphers that are still resistant against the attacks performed using quantum computers [12]. The GGH is a lattice-based cryptography developed on Closest Vector Problem (CVP) scheme [13] which was proposed by Goldreich, Goldwasser and Halevi in 1997. It was believed that GGH is secure when the dimension n is greater than 200 but Nguyen attacked all the dimensions less than 400 [14]. In [15, 16], Micciancio reduced the size of public key using hermite normal form (HNF). In the recent years several improvements and applications have been proposed for the GGH public key cryptosystem. In[17], an improvement on GGH using complex and quaternion algebras as well as the polynomial quaternion algebra (i.e., Q-GGH) has been presented. In other research, the GGH cryptosystem has been improved in terms of speed and security by also including the Gaussian methodology [18]. Moreover, taking advantage of commutative and non-commutative algebra was another approach for GGH improvement [19]. However, other enhancements have been conducted using the generalized low density lattices as well as the large error vector [20, 21]. An application of padding based GGH cryptosystem has also been applied in the field of medical image encryption achieving good results in terms of image processing factors for privacy preservation [22]. Depending on their improved structure, the only key factor for being prone to lattice-based attacks was their maximum dimension size. In this paper, a new cipher cryptosystem based on GGH using the octonion algebra and polynomial rings, which will be resistant against well-known types of lattice attacks.

2. GOLDREICH-GOLDWASSER-HALEVI (GGH) CRYPTOSYSTEM

One of the cryptosystems that its strength is relying on CVP is GGH. This cipher was presented by Goldreich-Goldwasser-Halevi in 1997 [13]. This cipher used a public key based on lattice strength to generate a trapdoor one-way function to increase its security property. The first person who worked on cryptanalysis of this cipher in 1999 was Phong Q. Nguyen [14]. This cipher system was an improvement of MCEliece cipher [23]. The randomized technique was used in both systems. The security of this cipher was solely based on the lattice dimension n and the security parameter σ, respectively. Taking $n > 400$ was required to have a high level of security. The difficulty of CVP was presented by σ. A secret matrix R, would be used as a private key. The columns of matrix R are defined as basis of lattice $L\mathrm{p}\mathbf{Z}^n$. The parameters used in GGH cipher are illustrated in Table 1.

Table 1. GGH Parameters

Parameter	Description	Knowledge
n	Dimension	public
σ	Security Parameter	public
r	$n \times n$ integral matrix	private
B	$n \times n$ integral matrix	public

2.1. Encryption Decryption, and Key Generation

To produce the basis r, lots of methods were presented in the literature. two of those methods will be described. The first method is generating a random matrix from $\{-4,-3,-2,-1,0,1,2,3,4\}$. The second method is to use $r = k.I_n + E$ where I_n is the $n \times n$ identity matrix, *k* is a medium sized integer more than 1 and E is a random matrix with small entities. The public key denoted by B is a matrix that represents basis of L. The public basis is not reducible as secret basis so it is known as bad basis. To randomly produce public basis B from secret basis *r*, lots of methods were presented in the literature. One of the methods is to multiply a random unimodular matrix say U with private key r as $B = U \cdot r$. The GGH cipher encrypts message vector $m \in \mathbf{Z}^n$ with public key B and error vector e by calculating $c = m \cdot B + e$. This calculation is performed over the field $\mathbf{Z}$. The message space is a set of vectors of length n with entries in $\{-M, -(M-1), \cdots, -1, 0, 1, \cdots, (M-1), M\}$ for some $M \in N$. Error vector with length n has random entities chosen from $\{-\sigma, \sigma\} \in N$. Decrypting the cipher text or in other words solving the CVP requires a nice basis r. This can help us to obtain a lattice point $m \cdot b$ close to c for calculating m. Calculations are performed as follows:

$$c \cdot r^{-1} = (m \cdot B + e) r^{-1} = m \cdot U \cdot r \cdot r^{-1} + e \cdot r^{-1} = m \cdot U + e \cdot r^{-1} \in Q^n$$

Since, $e \cdot r^{-1}$ is small enough, it will be removed by Babai's rounding technique. Matrix m can be calculated using $m = m \cdot U \cdot U^{-1}$. The strength of GGH lattice is based on the error vectors added to the cipher text. The complexity of key generation, encryption, and decryption in GGH cipher is $O(n^3)$, $O(n^2)$ and $O(n^2)$, respectively. The matrix calculations will increase the size of the cipher text even more than the size of plain text, so cryptanalysis of this cipher depends on the size of cipher text. To reduce the size of cipher text, Micciancio [15, 16], proposed two methods. The first method was finding hermite normal form (HNF) of r for calculating B as public key. And, in the second method, instead of encoding message entities in lattice point, we can encode it in the error vector.

2.2. Polynomial Rings

According to [14, 15, 24, 25], a polynomial ring can be defined as $h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_{n-1} x^{n-1}$ where $h(x) \in \mathbf{Z}[x]/(x^n - 1), \{h_0, \cdots, h_{n-1}\} \in \mathbf{Z}^n$. Adding and multiplying of two polynomials $g(x), h(x)$ are

$(g+h)(x)=(g_0+h_0)+(g_1+h_1)x+\cdots+(g_{(n-1)}+h_{(n-1)})x^{(n-1)}$ and

$(g.h)(x)=(g_0h_0)+(g_0h_1+g_1h_0)x+\cdots+\left(\sum_{i+j=k}g_ih_i\right)x^k+\cdots+\left(\sum_{i+j=2(n-1)}g_ih_i\right)x^{2(n-1)}$, respectively.

3. OCTONION ALGEBRA

Since our cryptosystem is based on octonion algebra, a brief information will be given about definition and properties of the octonion algebra. This algebra is known as a non-associative algebra. The brief information is adapted from [26-28].If a single element generating a sub-algebra is associative then that algebra is power-associative and if any two elements that are generating a sub-algebra associative then that algebra is alternative. It means for any two elements in an alternative algebra we have $x(xy)=(xx)y$ and $(yx)x=y(xx)$ and also, they can complete the Moufang identities as: I. $y((xz)x)=((yx)z)x$, II. $(xy)(zx)=(x(yz))x$ and III. $(x(yx))z=x(y(xz))$. Every octonion is a vector space of dimension eighth over R denoted by O and can be shown as follows: $O:=\left\{x_0+\sum_{i=1}^{7}x_i.e_i \mid x_0,\ldots,x_7\in R\right\}$ where $\{1,e_1,\ldots,e_7\}$ are basis and x values are scalars in R. Let $O_1=x_0+\sum_{i=1}^{7}x_i.e_i \mid x_0,\ldots,x_7\in R_1$, $O_2=y_0+\sum_{i=1}^{7}y_i.e_i \mid y_0,\ldots,y_7\in R_2$ Addition of these two octonions will be $O_1+O_2=(x_0+y_0)+\sum_{i=1}^{7}(x_i+y_i)\cdot e_i$.To perform multiplication of 2 octonions, we need to follow the rules below:

$e_i^2=-1, i=1,\ldots,7, e_ie_j=-e_je_i\ i,j\neq 1,\ldots,7$ if $i,j>7$ then $i,j=i,j\ mod\ 7$

The multiplication of two octonions will be as follows:

$$O_1oO_2=(x_0*y_0)-(x_1*y_1)-(x_2*y_2)-(x_3*y_3)-(x_4*y_4)-(x_5*y_5)-(x_6-y_6)-(x_7*y_7)$$
$$+((x_0*y_1)+(x_1*y_0)+(x_2*y_4)+(x_3*y_7)-(x_4*y_2)+(x_5*y_6)-(x_6*y_5)-(x_7*y_3))\cdot e_1$$
$$+((x_0*y_2)-(x_1*y_4)+(x_2*y_0)+(x_3*y_5)+(x_4*y_1)-(x_5*y_3)+(x_6*y_7)-(x_7*y_6))\cdot e_2$$
$$+((x_0*y_3)-(x_1*y_7)-(x_2*y_5)+(x_3*y_0)+(x_4*y_6)+(x_5*y_2)-(x_6*y_4)+(x_7*y_1))\cdot e_3$$
$$+((x_0*y_4)+(x_1*y_2)-(x_2*y_1)-(x_3*y_6)+(x_4*y_0)+(x_5*y_7)+(x_6*y_3)-(x_7*y_5))\cdot e_4$$
$$+((x_0*y_5)-(x_1*y_6)+(x_2*y_3)-(x_3*y_2)-(x_4*y_7)+(x_5*y_0)+(x_6*y_1)+(x_7*y_4))\cdot e_5$$
$$+((x_0*y_6)+(x_1*y_5)-(x_2*y_7)+(x_3*y_4)-(x_4*y_3)-(x_5*y_1)+(x_6*y_0)+(x_7*y_2))\cdot e_6$$
$$+((x_0*y_7)+(x_1*y_3)+(x_2*y_6)-(x_3*y_1)+(x_4*y_5)-(x_5*y_4)-(x_6*y_2)+(x_7*y_0))\cdot e_7$$

where * implements the convolution action. The conjugate, norm and multiplicative inverse of octonion O_1 can be calculated as $O_1^*=x_0-\sum_{i=1}^{7}x_i\cdot e_i$,

$N(O_1) = O_1^* \cdot O_1 = \sum_{i=1}^{7} x_i^2$, $O_1^{-1} = N(O_1)^{-1} \cdot O_1^*$ *where* $N(O_1) \neq 0$ respectively. Associative and power- associative rules don't work in multiplication of two octonions.

3.1. Algebraic Structure of Octonion Polynomials

An octonion polynomials can be defined as $A := \left\{ a_0(x) + \sum_{i=1}^{7} a_i(x).e_i \mid a_0(x), \cdots, a_7(x) \in \mathbf{Z}[x]/\left(x^N - 1\right) \right\}$, assuming $\overrightarrow{O_1}, \overrightarrow{O_2} \in A$ while $\overrightarrow{O_1} = f_0(x) + f_1(x)e_1 + \cdots + f_7(x)e_7, \overrightarrow{O_2} = g_0 + g_1(x)e_1 + \cdots + g_7(x)e_7$. The addition and multiplication of these two octonions will be defined as $\overrightarrow{O_1} + \overrightarrow{O_2} = (f_0 + g_0) + (f_1 + g_1)e_1 + \cdots (f_7 + g_7)e_7$

$$\overrightarrow{O_1} o \overrightarrow{O_2} = (f_0 * g_0 - f_1 * g_1 - f_2 * g_2 - f_3 * g_3 - f_4 * g_4 - f_5 * g_5 - f_6 * g_6 - f_7 * g_7)$$
$$(f_0 * g_1 + f_1 * g_0 + f_2 * g_4 + f_3 * g_7 - f_4 * g_2 + f_5 * g_6 - f_6 * g_5 - f_7 * g_3) \cdot e_1$$
$$(f_0 * g_2 - f_1 * g_4 + f_2 * g_0 + f_3 * g_5 + f_4 * g_1 - f_5 * g_3 + f_6 * g_7 - f_7 * g_6) \cdot e_2$$
$$(f_0 * g_3 - f_1 * g_7 - f_2 * g_5 + f_3 * g_0 + f_4 * g_6 + f_5 * g_2 - f_6 * g_4 + f_7 * g_1) \cdot e_3$$
$$(f_0 * g_4 + f_1 * g_2 - f_2 * g_1 - f_3 * g_6 + f_4 * g_0 + f_5 * g_7 + f_6 * g_3 - f_7 * g_5) \cdot e_4$$
$$(f_0 * g_5 - f_1 * g_6 + f_2 * g_3 - f_3 * g_2 - f_4 * g_7 + f_5 * g_0 + f_6 * g_1 + f_7 * g_4) \cdot e_5$$
$$(f_0 * g_6 + f_1 * g_5 - f_2 * g_7 + f_3 * g_4 - f_4 * g_3 - f_5 * g_1 + f_6 * g_0 + f_7 * g_2) \cdot e_6$$
$$(f_0 * g_7 + f_1 * g_3 + f_2 * g_6 - f_3 * g_1 + f_4 * g_5 - f_5 * g_4 - f_6 * g_2 + f_7 * g_0) \cdot e_7$$

where * implements the convolution action. The conjugate, Norm and multiplicative inverse of octonion $\overrightarrow{O_1}$ can be calculated as $\overrightarrow{O_1^*} = f_0(x) - f_1(x) \cdot e_1 - f_2(x) \cdot e_2 - \cdots - f_7(x) \cdot e_7$,

$N(\overrightarrow{O_1}) = (f_0(x))^2 + (f_1(x))^2 + \cdots + (f_7(x))^2$, $\overrightarrow{O_1^{-1}} = \frac{\overrightarrow{O_1^*}}{N(\overrightarrow{O_1})}$ *where* $N(\overrightarrow{O_1}) \neq 0$.

The complexity of addition and multiplication of two octonions are denoted by $O(8N)$ and $O(64N^2)$, respectively.

4. PROPOSED THE NEW SCHEME O-GGH CRYPTOSYSTEM

The new proposed scheme (O-GGH) is based on the polynomial rings and the octonion algebra that relies on two parameters same as GGH. These two parameters are n (lattice dimension) and σ (security parameter). For a better security it is suggested to consider $n > 50$. The difficulty of CVP is presented by security parameter. The private key will be an octonion polynomial $\vec{r} = \left\{ r_0(x) + r_1(x) \cdot e_1 + \ldots + r_7(x) \cdot e_7 \mid r_0(x), \ldots, r_7(x) \in \mathbf{Z}[x]/(x^N - 1) \right\}$ and its entities are a basis of lattice $L\mathrm{p}A_0$. The parameters of O-GGH are illustrated in Table 2.

Table 2. O-GGH Parameters

Parameter	Description	Knowledge
n	Dimension	public
σ	Security Parameter	public
$\vec{r}$	Octonion polynomial with dimension *n*	private
$\vec{B}$	Octonion polynomial with dimension *n*	public

Same as GGH, there are two methods for generating nice basis for $r_0(x),\ldots,r_7(x)$. The first one is to randomly choose the entities of them from $\{-4,-3,\ldots,3,4\}$. The other method is to use $\vec{r} = k + \vec{E}$ where k is a medium sized integer greater than one and $\vec{E}$ is a random octonion polynomial same as above random entities. The public key is an octonion polynomial (another basis for L) represented by $\vec{B} = B_0(x) + B_1(x)\cdot e_1 + \ldots + B_7(x)\cdot e_7 \mid B_0(x),\ldots,B_7(x) \in \mathbf{Z}[x]/(x^N - 1)$.The public basis is not reducible into secret basis, so it is called bad basis. To generate the public key from private key a random octonion polynomial is required denoted as $\vec{U} = U_0(x) + U_1(x)\cdot e_1 + \cdots + U_7(x)\cdot e_7 \mid U_0(x),\cdots,U_7(x) \in (Z[x])/((x^N - 1))$ and then the public key is calculated as follows: $\vec{B} = \vec{U} o \vec{r}$

Assuming the message octonion polynomial as $\vec{m} = m_0(x) + m_1(x)\cdot e_1 + \ldots + m_7(x)\cdot e_7 \mid m_0(x),\ldots,m_7(x) \in \mathbf{Z}[x]/(x^N - 1)$ and error octonion polynomial as $\overleftarrow{er} = er_0(x) + er_1(x)\cdot e_1 + \ldots + er_7(x)\cdot e_7 \mid er_0(x),\ldots,er_7(x) \in \mathbf{Z}[x]/(x^N - 1)$, cipher octonion polynomial can be calculated as follows: $\vec{c} = \vec{m} o \vec{B} + \vec{e}$

In the decryption procedure, since multiplication of octonions is not associative and commutative, so the following calculations are needed to be applied:

$$\vec{U} o \vec{c} = \vec{U} o\left(\vec{m} o \vec{B} + \vec{e}\right) = \vec{U} o\left(\vec{m} o \vec{B}\right) + \vec{U} o \vec{e} = \vec{U} o\left(\vec{m} o\left(\vec{U} o \vec{r}\right)\right) + \overleftarrow{e_1}$$

$$\xrightarrow{Moufang} = \left(\left(\vec{U} o \vec{m}\right) o \vec{U}\right) o \vec{r} + \overleftarrow{er_1} = \left(\overleftarrow{r^{-1}} o\left(\left(\vec{U} o \vec{m}\right) o \vec{U}\right) o \vec{r}\right) o \overleftarrow{r^{-1}} + \overleftarrow{r^{-1}} o \overleftarrow{e_1} o \overleftarrow{r^{-1}}$$

$$\xrightarrow{Moufang} = \overleftarrow{r^{-1}} o\left(\left(\vec{U} o \vec{m}\right) o \vec{U}\right) + \overleftarrow{er_2} = \vec{r} o \overleftarrow{r^{-1}} o\left(\left(\vec{U} o \vec{m}\right) o \vec{U}\right) + \vec{r} o \overleftarrow{er_2}$$

$$= \left(\vec{U} o \vec{m}\right) o \vec{U} o \vec{U}^{-1} + \overleftarrow{er_3} o \vec{U}^{-1} = \vec{U}^{-1} o \vec{U} o \vec{m} + \vec{U}^{-1} o \overleftarrow{er_4} \cong \vec{m}$$

The complexity of key generation, encryption and decryption in O-GGH cipher are $O\left(64n^2\right)$, $O\left(64n^2\right)$ and $O\left(384n^2\right)$, respectively. The parallel Implementation of this cipher can reduce the complexity to $O\left(n^2\right)$.

5. LATTICE-BASED CRYPTANALYSIS

There are two known lattice attacks that can be performed against GGH which are also applicable to O-GGH according to their structures. The first one is to obtain the private key from the public key. The second one is to solve the CVP using the lattice attack. For conducting both attacks, the dimension should be $n > 50$ which makes the

cipher resistant against lattice attacks. For performing the first lattice attack a lattice reduction algorithm is applied on the public key:

$$\vec{B} = \begin{pmatrix} +B_0 & +B_1 & +B_2 & +B_3 & +B_4 & +B_5 & +B_6 & +B_7 \\ -B_1 & +B_0 & -B_4 & -B_7 & +B_2 & -B_6 & +B_5 & +B_3 \\ -B_2 & +B_4 & +B_0 & -B_5 & -B_1 & +B_3 & -B_7 & +B_6 \\ -B_3 & +B_7 & +B_5 & +B_0 & -B_6 & -B_2 & +B_4 & -B_1 \\ -B_4 & -B_2 & +B_1 & +B_6 & +B_0 & -B_7 & -B_3 & +B_5 \\ -B_5 & +B_6 & -B_3 & +B_2 & +B_7 & +B_0 & -B_1 & -B_4 \\ -B_6 & +B_5 & +B_7 & -B_4 & +B_3 & +B_1 & +B_0 & -B_2 \\ -B_7 & -B_3 & -B_6 & +B_1 & -B_5 & +B_4 & +B_2 & +B_0 \end{pmatrix}$$

The size of this lattice is $8n \times 8n$ that is not possible to be performed due to the fact that the dimensions below 400 could not be attacked for $n > 50$ [14]. The second lattice attack need to be performed on the following lattice:

$$\left(\begin{array}{cccccccc|c} +B_0 & +B_1 & +B_2 & +B_3 & +B_4 & +B_5 & +B_6 & +B_7 & \\ -B_1 & +B_0 & -B_4 & -B_7 & +B_2 & -B_6 & +B_5 & +B_3 & \\ -B_2 & +B_4 & +B_0 & -B_5 & -B_1 & +B_3 & -B_7 & +B_6 & \\ -B_3 & +B_7 & +B_5 & +B_0 & -B_6 & -B_2 & +B_4 & -B_1 & 0 \\ -B_4 & -B_2 & +B_1 & +B_6 & +B_0 & -B_7 & -B_3 & +B_5 & \\ -B_5 & +B_6 & -B_3 & +B_2 & +B_7 & +B_0 & -B_1 & -B_4 & \\ -B_6 & -B_5 & +B_7 & -B_4 & +B_3 & +B_1 & +B_0 & -B_2 & \\ -B_7 & -B_3 & -B_6 & +B_1 & -B_5 & +B_4 & +B_2 & +B_0 & \\ \hline +c_0 & +c_1 & +c_2 & +c_3 & +c_4 & +c_5 & +c_6 & +B_7 & \\ -c_1 & +c_0 & -c_4 & -c_7 & +c_2 & -c_6 & +c_5 & +B_3 & \\ -c_2 & +c_4 & +c_0 & -c_5 & -c_1 & +c_3 & -c_7 & +B_6 & \\ -c_3 & +c_7 & +c_5 & +c_0 & -c_6 & -c_2 & +c_4 & -B_1 & \\ -c_4 & -c_2 & +c_1 & +c_6 & +c_0 & -c_7 & -c_3 & +B_5 & I \\ -c_5 & +c_6 & -c_3 & +c_2 & +c_7 & +c_0 & -c_1 & -B_4 & \\ -c_6 & -c_5 & +c_7 & -c_4 & +c_3 & +c_1 & +c_0 & -B_2 & \\ -c_7 & -c_3 & -c_6 & +c_1 & -c_5 & +c_4 & +B_2 & +B_0 & \end{array}\right)$$

The parts of matrix denoted by 0 and I are of $8n \times 8$ and 8×8 dimensions and hence, the size of this lattice is $(8n+8) \times (8n+8)$ but since multiplying of octonions is not associative and there are no known matrix implementations of octonions, so reduction of this lattice will never calculate the octonion of error. And hence, O-GGH is resistant against this attack. This means it's a great improvement even better than Sokouti et al [17-19, 21] studies. In the first study of Sokouti et al [19], they have implemented complex algebra in GGH matrix. It was resistant against both lattice attacks for $n > 200$. The complexity of key generation, encryption and decryption is increased to $O(4n^3)$, $O(4n^2)$ and $O(8n^2)$, respectively. In the second study of Sokouti et al [17, 19], they have

implemented quaternion algebra in GGH matrix. It was resistant against both lattice attacks for $n > 100$. The complexity of key generation, encryption and decryption is increased to $O(16n^3)$, $O(16n^2)$ and $O(32n^2)$, respectively. In the third study of Sokouti et al, they implemented polynomial quaternion algebra in GGH [18]. It was resistant against both lattice attacks for $n > 100$. The complexity of key generation, encryption and decryption is increased to $O\left(16n^2\right)$, $O\left(16n^2\right)$ and $O\left(32n^2\right)$, respectively.

6. CONCLUSION

By implementing octonion algebra in GGH cipher (O-GGH), we could make this cipher resistant against lattice attacks. It is resistant against first lattice attack when the dimension is greater than 50 ($n > 50$) and it is resistant against the second lattice attack using any dimension but the complexity of key generation, encryption and decryption will be increased to $O\left(64n^2\right)$, $O\left(64n^2\right)$ and $O\left(384n^2\right)$, respectively. Parallel Implementation of this cipher can reduce the complexity to $O\left(n^2\right)$. At last it can be concluded that octonion algebra could make GGH resistant against the second lattice attack forever, however it is also resistant to the first one when the dimension is set to values greater than 50.

REFERENCES

[1] Paar, C., Pelzl, J. Introduction to Cryptography and Data Security, Understanding Cryptography: A Textbook for Students and Practitioners, Paar C, Pelzl J, eds., Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 1-27.

[2] Sammy, F., Maria Celestin Vigila, S. A survey on CIA triad for cloud storage services, *International Journal of Control Theory and Applications*, **14**(vol. 9), 2016, pp. 6701-9.

[3] Thamotharan, B., Ramakrishnan, S., Sharan, A.N.S.P., Rajesh, K. A two phase OTP based approach to achieve confidentiality, integrity and non-repudiation in Cloud, *International Journal of Mechanical Engineering and Technology*, **8**(vol. 8), 2017, pp. 951-7.

[4] Henriques, M.S., Vernekar, N.K. Using symmetric and asymmetric cryptography to secure communication between devices in IoT, *IEEE International Conference on IoT and its Applications, May 2017*, 2017, pp. 1-4.

[5] Riyaldhi, R., Rojali, Kurniawan, A. Improvement of Advanced Encryption Standard Algorithm With Shift Row and S.Box Modification Mapping in Mix Column, *Procedia Computer Science*, (vol. 116), 2017, pp. 401-7.

[6] Bahar, H.B., Sokouti, M., Sokouti, B. A first study of improving transposition cryptosystem, *Journal of Discrete Mathematical Sciences and Cryptography*, **1**(vol. 13), 2010, pp. 1-9.

[7] Sokouti, M., Sokouti, B., Pashazadeh, S., Khanli, L.M. FPGA implementation of improved version of the Vigenere cipher, *Indian Journal of Science and Technology*, **4**(vol. 3), 2010, pp. 459-62.

[8] Sokouti, M., Sokouti, B., Pashazadeh, S. An approach in improving transposition cipher system, *Indian Journal of Science and Technology*, **8**(vol. 2), 2009, pp. 9-15.

[9] Iswari, N.M.S. Key generation algorithm design combination of RSA and ElGamal algorithm, *Proceedings of 2016 8th International Conference on Information Technology and Electrical Engineering: Empowering Technology for Better Future, ICITEE 2016*, 2017, pp. 1-5.

[10] Alam, K., Alam, K.R., Faruq, O., Morimoto, Y. A comparison between RSA and ElGamal based untraceable blind signature schemes, *Proc of International Conference on Networking Systems and Security*, 2016, pp. 1-4.

[11] Wang, Y.H., Zhang, H.G., Wu, W.Q., Han, H.Q. Quantum Algorithms for Breaking RSA Based on Phase Estimation and Equation Solving, *Jisuanji Xuebao/Chinese Journal of Computers*, **12**(vol. 40), 2017, pp. 2688-99.

[12] Mohsen, A.W., Bahaa-Eldin, A.M., Sobh, M.A. Lattice-based cryptography, *Proceedings of ICCES 2017 12th International Conference on Computer Engineering and Systems*, 2018, pp. 462-7.

[13] Herstein, I.N. Topics in Algebra, 2nd Edition. John Wiley, 1975.

[14] Lam, T.Y. A First Course in Noncommutative Rings. New York: Springer-Verlag, 2001.

[15] Lang, S. Algebra (Graduate Texts in Mathematics). New York: Springer-Verlag, 2002.

[16] Schafer, R.D. An introduction to non-associative algebras. Benediction Classics, 2010.

[17] Sokouti, M., Zakerolhosseini, A., Sokouti, B. Improvement of GGH a lattice based cryptography using polynomial rings and quaternion algebra, *The first national conference on modern computer engineering and data recovery*, 2013, pp. 1-7.

[18] Sokouti, M., Zakerolhosseini, A., Sokouti, B. Security and Speed Improvement of GGH based on polynomial rings, quaternion algebra and Gaussian method, *Second National Conference on New Ideas in Electrical Engineering, Isfahan*, 2013, pp. 1-8.

[19] Sokouti, M., Zakerolhosseini, A., Sokouti, B. Improvements over GGH Using Commutative and Non-Commutative Algebra, Encyclopedia of Information Science and Technology, Third Edition, Mehdi Khosrow-Pour DBA, ed., IGI Global, Hershey, PA, USA, 2015, pp. 3404-18.

[20] Kamel, S., Sarkiss, M., Othman, G.R. Generalized low density lattices for GGH cryptosystem, *2016 2nd International Conference on Frontiers of Signal Processing (ICFSP)*, 2016, pp. 25-31.

[21] Yoshino, M., Kunihiro, N. Improving GGH cryptosystem for large error vector, *2012 International Symposium on Information Theory and its Applications*, 2012, pp. 416-20.

[22] Sokouti, M., Zakerolhosseini, A., Sokouti, B. Medical Image Encryption: An Application for Improved Padding Based GGH Encryption Algorithm, *The open medical informatics journal*, (vol. 10), 2016, pp. 11-22.

[23] Hall, F.M. An Introduction to Abstract Algebra. Cambridge: Cambridge University Press, 1969.

[24] Hall, F.M. An Introduction to Abstract Algebra. Cambridge University Press, 2008.

[25] Hernstein, F.M. Topics in Algebra. Wiley, 1975.

[26] Schafer, R.D. An introduction to non-associative algebras. Benediction Classics, 2010.

[27] Baez, J.C. The Octonions, *Bulletin of the American Mathematical Society* **2**(vol. 39), 2002, pp. 145-205.

[28] Conway, J.H., Smith, D.A. On Quaternions and Octonions; Their Geometry, Arithmetic, and Symmetry. A. K. Peters, 2003.

Information about the authors:

Massoud Sokouti - obtained a Master of Science in Computer Engineering (Computer Architecture) and a Bachelor of Science in Information Technology Engineering (IT). Currently, he is a PhD student in Nuclear Medicine with a specialization in Meta-Analysis at Nuclear Medicine Research Center, Mashhad University of Medical Sciences, Mashhad, Iran. His main research is in the area of statistics and meta-analysis, m-/e-commerce, cryptographic algorithms, network security, information security, wavelet, and genetic algorithms.

Babak Sokouti – obtained Bachelor of Science in Electrical Engineering (Control); a Master of Science in Electrical Engineering (Electronics-biomedical engineering); a Master of Science in Information Security with Distinction from Royal Holloway University of London, London, UK; and obtained PhD in Bioinformatics & Systems Biomedicine from Biotechnology Research Center, Tabriz University of Medical Sciences, Tabriz, Iran. His research interests include cryptographic algorithms, information security, network security and protocols, image processing, protein structure prediction, and hybrid intelligent neural network systems based on genetic algorithms.

Manuscript received on 15 September 2018