Published by
NIGERIAN SOCIETY OF PHYSICAL SCIENCES
Available online @ https://journal.nsps.org.ng/index.php/jnsps

J. Nig. Soc. Phys. Sci. 4 (2022) 874

Journal of the Nigerian Society of Physical Sciences

Application of hourglass matrix in Goldreich-Goldwasser-Halevi encryption scheme

Olayiwola Babarinsa[a,*], Olalekan Ihinkalu[b], Veronica Cyril-Okeme[a], Hailiza Kamarulhaili[c], Arif Mandangan[d], Azfi Zaidi Mohammad Sofi[e], Akeem B. Disu[f]

[a]*Department of Mathematics, Federal University Lokoja, Kogi State, Nigeria*
[b]*Department of Computer Sciences, Federal University Lokoja, Kogi State, Nigeria*
[c]*School of Mathematical Sciences, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia*
[d]*Faculty of Science and Natural Resources, Universiti Malaysia Sabah, 88400 Kota Kinabalu, Malaysia*
[e]*Faculty of Bioengineering & Technology, Universiti Malaysia Kelantan, 16100 Kota Bharu, Malaysia*
[f]*Department of Mathematics, National Open University of Nigeria, Abuja, Nigeria*

Abstract

Goldreich-Goldwasser-Halevi (GGH) encryption scheme is lattice-based cryptography with its security based on the shortest vector problem (SVP) and closest vector problem (CVP) with immunity to almost all attacks, including Shor's quantum algorithm and Nguyen's attack of higher lattice dimension. To improve the efficiency and security of the GGH Scheme by reducing the size of the public basis to be transmitted, we use an hourglass matrix obtained from quadrant interlocking factorization as a public key. The technique of quadrant interlocking factorization to yield a nonsingular hourglass matrix compensates the encryption scheme with better efficiency and security.

DOI:10.46481/jnsps.2022.874

Keywords: Goldreich-Goldwasser-Halevi encryption scheme, Hourglass matrix, Quadrant interlocking factorization.

Article History :
Received: 18 June 2022
Received in revised form: 25 July 2022
Accepted for publication: 27 July 2022
Published: 08 October 2022

Communicated by: S. Fadugba

1. Introduction

Cryptography aims to achieve information security in confidentiality, data integrity, authentication, and non-repudiation [1]. Integer factorization problem (IFP), elliptic curve discrete logarithm problem (ECDLP), and discrete logarithm problem (DLP) are number theoretic hard problems established in cryptographic schemes based on the hardness of their security, which is mostly deployed in Rivest-Shamir-Adleman (RSA), El-Gamal and elliptic curve cryptosystems [2-4]. Notwithstanding, the security goals of the schemes can be attacked by a powerful algorithm, for instance, Shor's quantum algorithm, to compute the problems in less amount of time, see [5-7]. The immunity of some lattice problems such as the shortest vector problem (SVP) and closest vector problem (CVP) against Shor's quantum algorithm is exploited by the idea behind lattice-based cryptography [8,9]. The security of GGH cryptosystem relies on the smallest-basis problem (SBP) and CVP [10].

The earliest lattice-based encryption scheme which was the

*Corresponding author tel. no: +2348060032554
Email address: olayiwola.babarinsa@fulokoja.edu.ng (Olayiwola Babarinsa)

most considered practical scheme is Goldreich-Goldwasser-Halevi encryption scheme or GGH scheme [11]. The security of this scheme lies in the hardness of the underlying GGH-CVP instance which is proven to be NP-hard [12]. However, the security of GGH Scheme has been compromised by Nguyen's attack [13]. There are significant efforts to improve the efficiency of the GGH Scheme, such as the application of Hermite Normal Form (HNF) or Jensen-Based cryptographic scheme as the public key [14, 15]. The GGH Scheme survives against Nguyen's attack when being implemented in lattice dimensions above 400 [16]. However, the implementation of the scheme in lattice dimensions beyond 400 immediately makes the GGH Scheme inefficient, impractical, and uncompetitive compared to other existing encryption schemes. This is due to the large key sizes involve in the scheme once it is implemented in a large lattice dimensions. This is because the keys of this scheme are bases of lattice which could be represented in matrices form. That means the implementation of the scheme in a large lattice dimension requires the submission of a large lattice basis as a public key from Alice to Bob. For instance, in a lattice dimension of 400, the public basis can be represented as a 400×400 matrix with $400^2 = 160000$ entries. The transmission of a matrix with 160000 entries from Alice to Bob requires a high computational cost. By transforming the underlying GGH-CVP instance into its simpler form, Nguyen's attack successfully breaks the security of the GGH Scheme when being implemented in lattice dimensions smaller than 400. From the simplified GGH-CVP instance, Nguyen's attack derives an easier SVP instance which could be solved by using lattice reduction methods such as LLL and BKZ algorithms. In low lattice dimension, these algorithms efficiently work for solving the derived SVP-instance which makes Nguyen's attack succeeds. As the lattice dimension increases, the efficiency of these algorithms declines significantly. Consequently, the attack failed to break the security of the GGH Scheme in a lattice dimension of 400 and above [17].

To systematically reduce the number of non-zero elements in the public basis while maintaining all the required properties of the public basis, especially the linear independency and orthogonality properties, we use a nonsingular hourglass matrix H as a public basis and its corresponding factorization matrix R as a private basis of the GGH Scheme. These matrices are related as $R = UH$ where U is unimodular matrix. Section 2 gives the detail of an hourglass matrix and its factorization algorithm, while Section 3 entails the application of hourglass matrix and its factorization technique in GGH encryption scheme.

2. Hourglass matrix

Babarinsa and Kamarulhaili [18] gave details on hourglass matrix and its factorization algorithm by restricting the computed entries of the factorization to be nonzero in comparison with an hourglass device. They also suggested its applications in mathematics, graph theory, statistics, and computer science, see [19-24]. An hourglass matrix is defined as a nonsingular matrix of order $n\,(n \geq 3)$ with nonzero entries from the ith to the $(n-i+1)$ element of the ith and $(n-i+1)$ row of the matrix, 0's otherwise for $i = 1, 2, ..., \lfloor \frac{n+1}{2} \rfloor$ [18]. Unlike Z-matrix with nonzero restricted entries, hourglass matrix conforms with the shape of an hourglass device, see Figure 1 which illustrates the structural comparison between the hourglass device and hourglass matrix with nonzero elements denoted with black dots. To buttress the shape of hourglass matrix, Figure 1

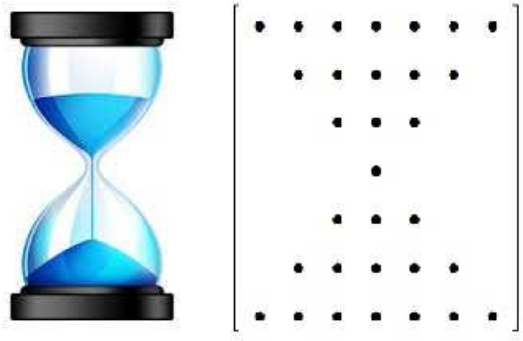

Figure 1. Structural comparison between hourglass device and hourglass matrix.

For the factorization algorithm of hourglass matrix, we compute $w_{i,k}^{(k)}$ and $w_{i,n-k+1}^{(k)}$ from a dense square matrix R by solving 2×2 linear systems in equation (1) using Cramer's rule to generalize for every update of R to H and proceed similarly for the inner square matrices of size $(n-2k)$ and so on, for $k = 1, 2, ..., \lfloor \frac{n-1}{2} \rfloor$.

$$\begin{cases} h_{k,k}^{(k-1)} w_{i,k}^{(k)} - h_{n-k+1,k}^{(k-1)} w_{i,n-k+1}^{(k)} = h_{i,k}^{(k-1)} \\ h_{k,n-k+1}^{(k-1)} w_{i,k}^{(k)} - h_{n-k+1,n-k+1}^{(k-1)} w_{i,n-k+1}^{(k)} = h_{i,n-k+1}^{(k-1)} \end{cases} \tag{1}$$

Then we compute for kth steps of $h_{i,j}^{(k)}$ as:

$$h_{i,j}^{(k)} = h_{i,j}^{(k-1)} + w_{i,k}^{(k)} h_{k,j}^{(k-1)} + w_{i,n-k+1}^{(k)} h_{n-k+1,j}^{(k-1)} \tag{2}$$

where $i, j = k+1, ..., n-k$. From equation (2), if one of the computed entries is zero, then apply possible row-interchange in no more than $(n-2k)$ times in $H^{(k-1)}$ and re-factorize, else the factorization breakdown to produce H. From every successful loop for each stage (with $\lfloor \frac{n-1}{2} \rfloor$ total stages in the factorization), there are $\sum_{k=1}^{\lfloor \frac{n}{2}-1 \rfloor} (n-2k)$ of 2×2 linear systems to be solved during the factorization using Cramer's rule.

Hourglass matrix (H-matrix) is nonsingular and its W-matrix is a unimodular matrix with $det(W) = (-1)^{Pn} = \pm 1$, where Pn is the number of permutation matrix in the factorization. Based on the structure of hourglass matrix, the matrix could be potentially used as the key (basis) in the GGH encryption scheme. The usage of hourglass matrix is expected to be able to reduce the size of bases, especially the public key. Almost half of the entries of the hourglass matrix are zero entries, which means the size of the public key can be reduced if the public key is generated in the form of hourglass matrix. This reduction will allow the GGH Scheme to be implemented in a higher lattice dimensions while still being able to be efficient and practical.

Hourglass matrix has linearly independent columns forming the basis of a lattice, which makes it suitable for GGH scheme. The fixed zero entries in hourglass matrix will not only minimize the memory cache used but also reduce computational time. In addition, the generation of hourglass matrix from *QIF* can be executed in polynomial time.

3. GGH scheme with hourglass matrix

Consider $(n,\sigma) \in N$ to be the security parameter, where n is a lattice dimension and σ is a threshold parameter. Denote $\vec{m},\vec{e} \in \mathscr{Z}^n$ as the message vector and error vector respectively, where the entries of $\vec{e}$ are $e_i \in \{-\sigma,+\sigma\}$. Let $i = 1,2,...,n$, then denote H as hourglass matrix such that $H = [\vec{h}_1,\vec{h}_2,...,\vec{h}_n]$, where $\vec{h}_i \in \mathscr{Z}^n$ are the column vectors of H, denote R as a non-singular matrix such that $R = [\vec{r}_1,\vec{r}_2,...,\vec{r}_n]$ where $\vec{r}_i \in \mathbb{Z}^n$ are the column vectors of R, and denote U as a unimodular matrix such that $U = [\vec{u}_1,\vec{u}_2,...,\vec{u}_n]$, where $\vec{u}_i \in \mathbb{Z}^n$ are the column vectors of U and $det(U) = \pm 1$.

Proposition 3.1. *[22] Any two bases for a lattice $\mathbb{L}$ are related by a unimodular matrix U that has integer coefficients and $det(U) = \pm 1$.*

Definition 3.1. *[23] Let $\vec{b}_1,\vec{b}_2,...,\vec{b}_n$ be n linearly independent vectors of $\mathbb{R}^m$ with $n \leq m$. The set of all integer linear combinations of the vectors $\vec{b}_1,\vec{b}_2,...,\vec{b}_n$ is called lattice and can be denoted in the form*

$$\mathscr{L}(\vec{b}_1,,...,\vec{b}_n) = \left\{ \sum_{i=1}^{n} m_i \vec{b}_i | m_i \in \mathbb{Z} \right\} \tag{3}$$

The linearly independent vectors $\vec{b}_1,\vec{b}_2,...,\vec{b}_n$ form the columns of the basis for the lattice $\mathscr{L}(B)$. Suppose that $B,H \in \mathbb{R}^{n\times n}$ be nonsingular square matrices with linearly independent vectors $\vec{b}_1,\vec{b}_2,...,\vec{b}_n$ and $\vec{h}_1,\vec{h}_2,...,\vec{h}_n$ as their columns respectively. The lattice $L(B) \subset \mathbb{R}^n$ that is spanned by the basis B is defined as follows [22].

$$L(B) = \left\{ \sum_{i,j=1}^{n} \mu_{i,j}\vec{b}_i \mid \vec{b}_i \in B \text{ and } \mu_{i,j} \in \mathbb{Z}, \forall i,j = 1,2,...,n \right\} \tag{4}$$

and the lattice $L(H) \subset \mathbb{R}^n$ that spanned by the basis and the lattice $L(B) \subset \mathbb{R}^n$ that spanned by the basis B is defined as follows

$$L(H) = \left\{ \sum_{i,j=1}^{n} \tau_{i,j}\vec{h}_i \mid \vec{h}_i \in H \text{ and } \tau_{i,j} \in \mathbb{Z}, \forall i,j = 1,2,...,n \right\} \tag{5}$$

To ensure that the bases B and H are spanning the same lattice (i.e $L(B) = L(H)$), the matrix W is required to be a unimodular matrix with $det(U) = \pm 1$.

The desired properties for the public and private basis are as the following:

1. Both H and R
   a) Two different bases span the same lattice L, i.e., $\mathscr{L}(R) = L = \mathscr{L}(H)$.
   b) To be a lattice basis, both matrices H and R must satisfy the following conditions:
   i. The vectors $\{\vec{h}_1,\vec{h}_2,...,\vec{h}_n\}$ and $\{\vec{r}_1,\vec{r}_2,...,\vec{r}_n\}$ are linearly independent, where the only solution for the following equations
   $$\alpha_1\vec{h}_1 + \alpha_2\vec{h}_2 + ... + \alpha_n\vec{h}_n = \vec{0} \tag{6}$$
   and
   $$\beta_1\vec{r}_1 + \beta_2\vec{r}_2 + ... + \beta_n\vec{r}_n = \vec{0} \tag{7}$$
   are the trivial solutions, i.e., $\alpha_i = 0$ and $\beta_i = 0\ \forall, i = 1,2,...,n$.
   ii. The vectors $\{\vec{h}_1,\vec{h}_2,...,\vec{h}_n\}$ and $\{\vec{r}_1,\vec{r}_2,...,\vec{r}_n\}$ span the whole space $\mathbb{Z}$, i.e.,
   $$span\{\vec{h}_1,\vec{h}_2,...,\vec{h}_n\} = \mathbb{Z} \tag{8}$$
   and
   $$span\{\vec{r}_1,\vec{r}_2,...,\vec{r}_n\} = \mathbb{Z} \tag{9}$$
   c) Since both H and R are spanning the same lattice L, these bases have the same determinant, i.e., $det(H) = det(R)$.
   d) Both H and R are mathematically related by unimodular matrix U, as $R = UH$.
2. The public basis H
   The column vectors $\{\vec{h}_1,\vec{h}_2,...,\vec{h}_n\}$ are long vectors from the origin and highly nonorthogonal vectors where the Hadamard ratio of the matrix H is far from 1 and closer to 0.
3. The private basis R
   a) The column vectors $\{\vec{r}_1,\vec{r}_2,...,\vec{r}_n\}$ are short vectors from the origin and reasonably orthogonal vectors where the Hadamard ratio of the matrix R is far from 0 and closer to 1.
   b) The rounding vector $\lfloor R\vec{e} \rceil = \vec{0}$ to ensure the decryption process succeeds.

Proposition 3.2. *[19] Let $B,H \in \mathbb{R}^{n\times n}$ be nonsingular square matrices such that $B = HW$, where B is a basis for lattice $L(B)$, H is a basis for lattice $L(H)$. If W is a unimodular matrix, then $L(B) = L(H)$ where $W \in \mathbb{Z}^{n\times n}$.*

3.1. GGH Scheme algorithm using hourglass matrix

The algorithm of the GGH Scheme by using hourglass matrix is as follows:

1. Key Generation by Alice (recipient)
   - Sets the security parameters $n,\sigma \in N$ where n is an even number.
   - Generates a non-singular $n \times n$ -matrix R with the following properties:
     a) Represent the matrix R as
     $$R = [\vec{r}_1\ \vec{r}_2\ ...\ \vec{r}_n] \tag{10}$$
     where the vectors $\vec{r}_i \in \mathbb{Z}$ are the columns of R. These vectors are required to be linearly independent.

b) Compute the Hadamard ratio of the matrix R as

$$\mathscr{H}(R) = \left(\frac{|det(R)|}{\prod_{i=1}^{n} \|\vec{r}_i\|} \right)^{\frac{1}{n}} \tag{11}$$

where $\|\vec{r}_i\|$ is the Euclidean norm of the vectors $\vec{r}_i$. The Hadamard ratio is required to measure the orthogonality of the vectors $\vec{r}_i$. The closure the Hadamard ratio to 1, the more orthogonal the vectors $\vec{r}_i$ are. We accept R to be the private basis if

$$\mathscr{H}(R) \in [0.7, 1) \tag{12}$$

to make sure that the private basis R is a reasonably orthogonal basis.

- Computes the factorization of the matrix R as follows

$$R = UH$$

where $U \in \mathbb{Z}^{n\times n}$ is a unimodular matrix with $det(U) = \pm 1$ and $H \in \mathbb{Z}^{n\times n}$ is an Hourglass matrix. For the Hourglass matrix H,

a) Represent the matrix H as

$$H = [\vec{h}_1 \ \vec{h}_2 \ ... \ \vec{h}_n] \tag{13}$$

where the vectors $\vec{h}_i \in \mathbb{Z}^n$ are the columns of H. These vectors are required to be linearly independent.

b) Since H and R are related by a unimodular matrix U as $R = UH$, then

$$det(UH) = det(R) = \pm det(H) \tag{14}$$

c) Compute the Hadamard ratio of the matrix H as

$$\mathscr{H}(H) = \left(\frac{|det(H)|}{\prod_{i=1}^{n} \|\vec{h}_i\|} \right)^{\frac{1}{n}} \tag{15}$$

where $\|\vec{h}_i\|$ is the Euclidean norm of the vectors $\vec{h}_i$. The closure of the Hadamard ratio to 0, the more highly non-orthogonal the vectors $\vec{h}_i$ are. We accept H to be the public basis if

$$\mathscr{H}(H) \in (0, 0.3] \tag{16}$$

to make sure that the public basis H is a highly non-orthogonal basis.

- Keeps the matrix R as her private basis and U as her private matrix.
- Sends the Hourglass matrix H as her public basis to Bob together with her security parameters $n, \sigma \in N$.

2. Encryption by Bob (sender)
   - Sets the message as $\vec{m} = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix} \in \mathbb{Z}^n$
   - Generates the error vector as $\vec{e} = \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix}$ where $e_i \in \{\pm\sigma\}$
   - Encrypts the message $\vec{m}$ as follows

$$\vec{c} = H\vec{m} + \vec{e} \tag{17}$$

   where $\vec{c} \in \mathbb{Z}^n$ is the ciphertext vector.
   - Sends the ciphertext $\vec{c}$ to Alice.
3. Decryption by Alice (recipient)
   - Computes a vector $T \in \mathbb{R}^n$ as follows

$$T = R^{-1}\vec{c} \tag{18}$$

   - Rounds each entry of the matrix T to the nearest integer, i.e., $\lfloor t_i \rceil \in \mathbb{Z}$ where $t_i \in T$ for all $i = 1, 2, ..., n$.
   - Decrypts the ciphertext as follows

$$\vec{M} = U\lfloor T \rceil \tag{19}$$

   where $\lfloor T \rceil$ is a matrix T with rounded entries. Decryption succeeds if

$$\vec{M} = \vec{m} \tag{20}$$

Now, consider the following scenario. Suppose that Bob wants to send a secret message to Alice. As the recipient, Alice generates the private basis R as a good basis. Then, she derived the public basis H as $R = UH$. The public basis H is accepted if the basis H is a highly non-orthogonal basis. Otherwise, the key generation process will be re-initiated. Once the proper bases R and H are completely generated, Alice sends the public basis H, the security parameter $\{n, \alpha\}$ to Bob and keeps the other basis and parameters secret. Upon receiving the information from Alice, Bob encoded his secret message in a vector $\vec{m} \in \mathbb{Z}^n$. Then, he generates the error vector $\vec{e} \in \{-\alpha, \alpha\}^n$ and then proceeds to the encryption process which is done as $\vec{c} = H\vec{m} + \vec{e}$. The ciphertext $\vec{c} \in \mathbb{Z}^n$ is then sent to Alice. Upon receiving $\vec{c}$ from Bob, Alice proceed with the decryption process which can be done by solving the underlying CVP instance using Babai's round-off method. She computes $\vec{m} = U\lfloor R^{-1}\vec{c} \rceil$.

Proposition 3.3. *Suitability of hourglass matrix in GGH scheme is attainable if the encrypted message M is successfully decrypted to message m, such that*

$$\vec{M} = \vec{m}.$$

Proof. Since $R = UH$, then $U = H^{-1}R$.
Thus,

$$\begin{aligned} \vec{M} &= U\lfloor T \rceil \\ &= U\lfloor R^{-1}\vec{c} \rceil \end{aligned}$$

$$
\begin{aligned}
&= U\lfloor R^{-1}(H\vec{m}+\vec{e})\rceil \\
&= U\lfloor R^{-1}H\vec{m}+R^{-1}\vec{e}\rceil \\
&= \lfloor UR^{-1}H\vec{m}+UR^{-1}\vec{e}\rceil \\
&= \lfloor H^{-1}RR^{-1}H\vec{m}+UR^{-1}\vec{e}\rceil \\
&= \lfloor \vec{m}+UR^{-1}\vec{e}\rceil \\
&= \lfloor \vec{m}\rceil + \lfloor UR^{-1}\vec{e}\rceil .
\end{aligned}
$$

Since $\vec{m} \in \mathbb{Z}^n$, $\lfloor m\rceil = m$. For the decryption to succeed, the rounding vector is required to be $\lfloor R^{-1}\vec{e}\rceil = \vec{0}$. Therefore,

$$\vec{M} = \vec{m} + U\lfloor R^{-1}\vec{e}\rceil$$

If all the entries of the rounding vector $\lfloor R^{-1}\vec{e}\rceil$ are smaller than $\frac{1}{2}$, then we have $\lfloor R^{-1}\vec{e}\rceil = \vec{0}$. Therefore, we have

$$\vec{M} = \vec{m} + U\vec{0}$$

$$\vec{M} = \vec{m}$$

□

3.2. A numerical example of hourglass matrix in GGH scheme

We consider a numerical example of 4×4 hourglass matrix in GGH scheme. Let R, U, H be the hourglass matrix, unimodular matrix, nonsingular matrix, error, and encrypted message to be sent from Alice to Bob, and e, m are vectors.

$$H = \begin{bmatrix} 143 & 123 & -211 & 103 \\ 0 & -14 & 33 & 0 \\ 0 & -14 & -124 & 0 \\ -211 & -14 & -122 & 213 \end{bmatrix}, \qquad \vec{m} = \begin{bmatrix} 5 \\ 6 \\ 7 \\ 8 \end{bmatrix}, \qquad \vec{e} = \begin{bmatrix} -3 \\ 3 \\ -3 \\ -3 \end{bmatrix}.$$

Then $det(H) = 114,718,016$ and the Hadamard ratio of H is 0.4495. Then U is given as

$$U = \begin{bmatrix} -1 & 2 & 1 & -2 \\ 2 & -1 & 1 & 2 \\ 1 & -1 & 1 & 2 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

where $det(U) = 1$. Thus, R is computed as

$$R = H \cdot U = \begin{bmatrix} -5 & 477 & 158 & -565 \\ 5 & -19 & 19 & 38 \\ -152 & 138 & -138 & -276 \\ 274 & -73 & -134 & -63 \end{bmatrix}$$

Vividly, $det(R) = 114,718,016$. Thus, the Hadamard ration of R is 0.2606. Now compute H^{-1} as

$$H^{-1} = \begin{bmatrix} 0.00408 & 0.033828 & 0.004000 & -0.001973 \\ 0 & -0.056415 & -0.015014 & 0 \\ 0 & 0.006370 & -0.006370 & 0 \\ 0.00404 & 0.033451 & -0.000673 & 0.002740 \end{bmatrix}$$

and

$$H^{-1} \cdot e = \begin{bmatrix} -0.107163 \\ 0.214286 \\ 0 \\ -0.077988 \end{bmatrix}$$

The round-off $\lfloor H^{-1} \cdot e\rceil$ gives a zero vector, $\vec{0} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$. The message m sent by Alice to Bob be

$$m = \begin{bmatrix} 5 \\ 6 \\ 7 \\ 8 \end{bmatrix}$$

$$R \cdot m = \begin{bmatrix} -577 \\ 348 \\ -3106 \\ -510 \end{bmatrix}$$

$$c = R \cdot m + e = \begin{bmatrix} -574 \\ 345 \\ -3109 \\ -507 \end{bmatrix}$$

$$T = H^{-1}c = \begin{bmatrix} -2.107163 \\ 27.214286 \\ 22.000000 \\ 9.922012 \end{bmatrix}$$

The round-off $\lfloor T\rceil$ to nearest integers gives

$$\lfloor T\rceil = \begin{bmatrix} -2 \\ 27 \\ 22 \\ 10 \end{bmatrix}$$

$$H\lfloor T\rceil = \begin{bmatrix} -577 \\ 348 \\ -3106 \\ -510 \end{bmatrix}$$

The decryption M is

$$M = R^{-1}HT = \begin{bmatrix} 4.9999999994 \\ 5.9999999780 \\ 6.9999999926 \\ 8.0000000102 \end{bmatrix}$$

The round-off decrypted message $\lfloor M\rceil$ by Bob is

$$\lfloor M\rceil = \begin{bmatrix} 5 \\ 6 \\ 7 \\ 8 \end{bmatrix}$$

Hence, $\vec{M} - \vec{m} = \vec{0}$.

4. Conclusion

The advantage of the hourglass matrix as a public key has been explored in the encryption scheme to enhance the efficiency of the GGH. The orthogonal columns of hourglass matrix keep the GGH encryption scheme efficient and practical by reducing the number of non-zero elements on the public basis while maintaining all the required properties of the public basis, especially the linear independency and orthogonality properties. With better security and efficiency, the scheme is expected to be highly competitive in the post-quantum era. Due to the simplicity and practicality that can be offered by the scheme, it may be widely adopted for providing security in devices with small computing capacity.

References

[1] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, John Wiley and Sons, 2007.

[2] C. Meshram, "An efficient id-based cryptographic encryption based on discrete logarithm problem and integer factorization problem", Information Processing Letters **115** (2015) 351â358. doi:https://doi.org/10.1016/j.ipl.2014.10.007.

[3] K. S. McCurley, "The discrete logarithm problem", Proceedings of Symposia in Applied Math **42** (1990) 49.

[4] S. F. Tzeng & M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", Computer Standards & Interfaces **26** (2004) 61. doi:https://doi.org/10.1016/S0920-5489(03)00069-2.

[5] P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, Ieee, 1994, pp. 124â134. doi:https://doi.org/10.1109/SFCS.1994.365700.

[6] P. E. Black, D. R. Kuhn & C. J. Williams, "Quantum Computing and Communication", 56 (2002) 189. doi:https://doi.org/10.1016/S0065-2458(02)80007-9.

[7] K. Balasubramanian & M. Rajakani, *Problems in cryptography and cryptanalysis* Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government, IGI Global, 2021, pp. 837â853. doi:https://doi.org/10.4018/978-1-7998-5351-0.ch048.

[8] A. Ekert & R. Jozsa, "Quantum computation and shorâs factoring algorithm", Reviews of Modern Physics **68** (1996) 733. doi:https://doi.org/10.1103/RevModPhys.68.733.

[9] M. Bunder, A. Nitaj, W. Susilo & J. Tonien, *A new attack on three variants of the rsa cryptosystem* in: Australasian Conference on Information Security and Privacy, Springer, 2016, pp. 258â268. doi:https://doi.org/10.1007/978-3-319-40367-016.

[10] A. Mandangan, H. Kamarulhaili & M. Asbullah, "On the smallest-basis problem underlying the GGH lattice-based cryptosystem", Malaysian Journal of Mathematical Sciences **13** (2019) 1.

[11] O. Goldreich, S. Goldwasser & S. Halevi, *Public-key cryptosystems from lattice reduction problems*, Annual International Cryptology Conference, Springer, 1996, pp. 112-131.

[12] D. Micciancio & O. Regev, *Lattice-based cryptography*, Post-quantum cryptography, Springer, 2009, pp. 147â191. doi:https://doi.org/10.1007/978-3-540-88702-75.

[13] P. Nguyen, *Cryptanalysis of the goldreich-goldwasser-halevi cryptosystem from crypto'97*, Annual International Cryptology Conference, Springer, 1999, pp. 288â304.

[14] D. Micciancio, *Improving lattice based cryptosystems using the hermite normal form*, International Cryptography and Lattices Conference, Springer, 2001, pp. 126. doi:https://doi.org/10.1007/3-540-44670-211.

[15] S. Osikoya & E. Adeyefa, "Jensen-based new cryptographic scheme", Journal of the Nigerian Society of Physical Sciences **4** (2022) 49. doi:https://doi.org/10.46481/jnsps.2022.325.

[16] S. Ludwig, W. Kalfa, File system encryption with integrated user management, ACM SIGOPS Operating Systems Review 35 (2001) 88. doi:https://doi.org/10.1145/506084.506092.

[17] M. A. Asbullah & M. R. K. Ariffin, "Design of rabin-like cryptosystem without decryption failure", Malaysian Journal of Mathematical Sciences 10 (2016) 1.

[18] O. Babarinsa & H. Kamarulhaili, *Quadrant interlocking factorization of hourglass matrix*, AIP Conference Proceedings of the 25th National Symposium on Mathematical Sciences, Vol. 1974, AIP Publishing, 2018. pp. 030009:1â9. doi:https://doi.org/10.1063/1.5041653.

[19] O. Babarinsa, M. Arif, H. Kamarulhaili, "Potential applications of hourglass matrix and its quadrant interlocking factorization", ASM Science Journal **12** (2019) 72.

[20] O. Babarinsa, H. Kamarulhaili, Mixed energy of a mixed hourglass graph, Communications in Mathematics and Applications **10** (2019) 45. doi:https://doi.org/10.26713/cma.v10i1.1143.

[21] O. Babarinsa & H. Kamarulhaili, *Mixed hourglass graph*, AIP Conference Proceedings, Vol. 2184, AIP Publishing LLC, 2019, pp. 020003. doi:https://doi.org/10.1063/1.5136357.

[22] J. Hoffstein, J. Pipher, J. H. Silverman, J. H. Silverman, *An introduction to mathematical cryptography*, Vol. 1, Springer, 2008.

[23] A. Nitaj, M. R. K. Ariffin, D. I. Nassr & H. M. Bahig, *New attacks on the rsa cryptosystem*, International Conference on Cryptology in Africa, Springer, 2014, pp. 178â198. doi:https://10.1007/978-3-319-06734-612.

[24] O. Babarinsa, "Graph theory: A lost component for development in Nigeria", Journal of the Nigerian Society of Physical Sciences 4 (2022) 844. doi:https://doi.org/10.46481/jnsps.2022.844.