symmetry

MDPI

Article

Asymmetric Cryptosystem on Matrix Algebra Over a Chain Ring

Muzna Yumman [1], Tariq Shah [1] and Iqtadar Hussain [2,*]

[1] Department of Mathematics, Quaid-i-Azam University, Islamabad 44000, Pakistan; myumman@math.qau.edu.pk (M.Y.); stariqshah@qau.edu.pk (T.S.)
[2] Department of Mathematics, Statistics and Physics, Qatar University, Doha 2713, Qatar
* Correspondence: iqtadarqau@qu.edu.qa

Abstract: The revolutionary idea of asymmetric cryptography brings a fundamental change to our modern communication system. However, advances in quantum computers endanger the security of many asymmetric cryptosystems based on the hardness of factoring and discrete logarithm, while the complexity of the quantum algorithm makes it hard to implement in many applications. In this respect, novel asymmetric cryptosystems based on matrices over residue rings are in practice. In this article, a novel approach is introduced. Despite the matrix algebra $M(k,\mathbb{Z}_n)$, the matrix algebra $M(k,R'_n)$, $R'_n = \frac{\mathbb{Z}_2[w]}{\langle w^n-1\rangle}$ as the chain ring is considered. In this technique, instead of exponentiation, the inner product automorphisms the use for key generation. The chain ring provides computational complexity to its algorithm, which improves the strength of the cryptosystem. However, the residue ring endangers the security of the original cryptosystem, while it is hard to break using R'_n. The structure of the chain ring deals with the binary field $\mathbb{Z}_2$, which simplifies its calculation and makes it capable of efficient execution in various applications.

Keywords: asymmetric cryptosystems; chain ring; general linear group

Citation: Yumman, M.; Shah, T.; Hussain, I. Asymmetric Cryptosystem on Matrix Algebra over a Chain Ring. *Symmetry* **2021**, *13*, 45. https://doi.org/10.3390/sym13010045

Received: 13 May 2020
Accepted: 2 June 2020
Published: 30 December 2020

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Internet and network applications have become the basic necessity of the modern world. Cryptography techniques provide security for these applications. Cryptography is the deliberate attempt to scramble information so that adversaries fail to access secret data. Symmetric cryptography mainly focuses on private-key encryption. The key-distribution and key-management problems make it futile for today's world. A new approach is required to overcome these problems. Asymmetric cryptography provides a solution. Moreover, it gives a new direction to cryptography. The idea of key exchange protocol was initiated by Merkle, Differ, and Hellman [1] in the mid-1970s. One of the earliest asymmetric cryptosystems is the famous RSA. Later on, many more asymmetric algorithms were introduced, such as ElGamal and ECC [2,3], which were based on the complexity of the integer factorization problem. It was further modified by different cryptologists in [4–6]. The elliptic curve discrete logarithm problem (ECDLP) has been a prominently researched area, still under the analysis of many cryptographers [7,8].

Data confidentiality, integrity, and authenticity are the fundamental protection goals of cryptography. Hash functions and digital signatures improve message integrity and make it more authentic [9,10]. Nowadays, a critical problem that classical and modern cryptography fails to address is long term security. Quantum cryptography can resolve this problem as it is based on the law of quantum physics, which is valid forever [11,12]. The complexity of the quantum algorithm makes it difficult to be implemented in various applications. In this respect, asymmetric cryptosystems based on matrix algebra over residue ring have been studied for the last decade.

The main focus of this work is to ensure an improvement in Khan et al.'s [13] proposed scheme, based on a commutative subgroup of the $GL(2, \mathbb{Z}_n)$. Our goal is to increase the security of the algorithms by using a unique algebraic structure of the local chain ring $R'_n = \frac{\mathbb{Z}_2[w]}{\langle w^n - 1\rangle}$ and generalizing both the cryptosystems given in [13]. However, the local ring $\mathbb{Z}_n$ of integer modulo n makes both cryptosystems insecure in the sense that an attacker that is efficient in solving linear equations in $\mathbb{Z}_n$ can easily break both schemes in a very limited period. In 2016, Jianwei Jia et al. [14] worked on schemes given in [13]; they conducted a detailed analysis of structural attack and deduced that both cryptosystems were breakable. In this article, we propose new asymmetric cryptosystems that are based on the abelian subgroup of the general linear group $GL(k, R'_n)$, as done for Cryptosystem 1 over residue ring in [15]. Chain ring R'_n has a special structure of polynomials; the coefficients of a polynomial are from $\mathbb{Z}_2$ which make its calculations easy but unfeasible for the attacker to decrypt it.

The rest of the article comprises as follows. In Section 2, we briefly define the chain ring. The details of the proposed scheme are given in Section 3, and then it is verified with an example in Section 4. Finally, some attacks are discussed in the security analysis in Section 5, and a conclusion is drawn in the end.

2. Chain Ring

Chain ring R is a commutative ring, with identity having the property that under inclusion, each of its ideals forms a chain. More precisely, it is a finite local ring with radical M of R as a principal ideal. Roughly speaking, it is an extension over the Galois ring $GR(q, h) = \frac{\mathbb{Z}_q[w]}{\langle g(w)\rangle}$, where $q = p^m$, such that p is a prime, $m, h > 0$, and $g(w) \in \mathbb{Z}_q[w]$ is a basic irreducible polynomial of degree h. The cardinality of the Galois ring is p^{mh}. Now, if M is a maximal ideal of R, then $\frac{R}{M}$ is residue field which is the Galois extension field $GF(p^h)$.

The finite chain ring is quotient ring $\frac{GF(p^h)[w]}{\langle w^n - 1\rangle} = \frac{\mathbb{F}_{p^h}[w]}{\langle w^n - 1\rangle} = \sum_0^{n-1} w^n \mathbb{F}_{p^h}$, where $\mathbb{F}_{p^h}[w]$ is Euclidean domain and $w^n = 1, n \geq 2$, whereas one of the special class of finite chain ring is quotient ring $R'_n = \frac{GF(2)[w]}{\langle w^n - 1\rangle} = \frac{\mathbb{F}_2[w]}{\langle w^n - 1\rangle} = \sum_0^{n-1} w^n \mathbb{F}_2$. The cardinality of R'_n is 2^n. Elements of this class of chain ring are invertible if the sum of the coefficient of the element $\sum_0^{n-1} b_n w^n \in R'_n$ is non-zero, $i.e.$, $\sum_0^{n-1} b_n \neq 0$, where $b_n \in \mathbb{F}_2$. The group of invertible elements of R'_n is denoted as ${R'_n}^*$. In particular, take $n = 8$, so the finite chain ring will be ${R_8}' = \frac{\mathbb{F}_2[w]}{\langle w^8 - 1\rangle} = \sum_0^7 w^n\, \mathbb{F}_2$, where $w^8 = 1$. The number of elements in this chain ring and its unit elements is

$$r = |{R_8}'| = 2^8 = 256, \text{ and } |{R'_8}^*| = \phi(r) = 2^{8-1}(2-1) = 128.$$

3. Proposed Cryptosystems

In the proposed asymmetric cryptosystems, the subgroup of $GL(k, R'_n)$ is the aim of the study, while in the original cryptosystems, the subgroup of $GL(2, \mathbb{Z}_n)$ was under discussion. Hence, the proposed algorithm is a generalization of original cryptosystems, while the finite chain ring is used instead of a residue ring. We will discover later that this modification increases in the computational complexity of the proposed cryptosystem.

Let Q be the subgroup of $GL(k, R'_n)$. It can be easily proved that Q is an abelian subgroup of $GL(k, R'_n)$.

Proposition 1. *Let $M(k, R'_n)$ be the ring of matrices and $GL(k, R'_n)$ its general linear group. Then,*

$$Q=\left\{\begin{bmatrix} \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \acute{x}_4 & \cdots & \acute{x}_k \\ 0 & \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \cdots & \acute{x}_{k-1} \\ 0 & 0 & \acute{x}_1 & \acute{x}_2 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \acute{x}_3 \\ 0 & 0 & 0 & \ldots & \acute{x}_1 & \acute{x}_2 \\ 0 & 0 & 0 & \ldots & 0 & \acute{x}_1 \end{bmatrix} \,\middle|\, \acute{x}_1 \in R_n'^{*}, \acute{x}_i \in R_n', i=2,3,\ldots,k \text{ and } det\ Q \in R_n'^{*}\right\}$$

is an abelian subgroup of $GL(k,R_n')$.

Proof of Proposition 1.

1. Let $Q_1, Q_2 \in Q$.

$$Q_1=\begin{bmatrix} \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \acute{x}_4 & \cdots & \acute{x}_k \\ 0 & \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \cdots & \acute{x}_{k-1} \\ 0 & 0 & \acute{x}_1 & \acute{x}_2 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \acute{x}_3 \\ 0 & 0 & 0 & \cdots & \acute{x}_1 & \acute{x}_2 \\ 0 & 0 & 0 & \cdots & 0 & \acute{x}_1 \end{bmatrix}, Q_2=\begin{bmatrix} \acute{y}_1 & \acute{y}_2 & \acute{y}_3 & \acute{y}_4 & \cdots & \acute{y}_k \\ 0 & \acute{y}_1 & \acute{y}_2 & \acute{y}_3 & \cdots & \acute{y}_{k-1} \\ 0 & 0 & \acute{y}_1 & \acute{y}_2 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \acute{y}_3 \\ 0 & 0 & 0 & \cdots & \acute{y}_1 & \acute{y}_2 \\ 0 & 0 & 0 & \cdots & 0 & \acute{y}_1 \end{bmatrix}$$

Then, $Q_1Q_2=\begin{bmatrix} \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \acute{x}_4 & \cdots & \acute{x}_k \\ 0 & \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \cdots & \acute{x}_{k-1} \\ 0 & 0 & \acute{x}_1 & \acute{x}_2 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \acute{x}_3 \\ 0 & 0 & 0 & \cdots & \acute{x}_1 & \acute{x}_2 \\ 0 & 0 & 0 & \cdots & 0 & \acute{x}_1 \end{bmatrix}\begin{bmatrix} \acute{y}_1 & \acute{y}_2 & \acute{y}_3 & \acute{y}_4 & \cdots & \acute{y}_k \\ 0 & \acute{y}_1 & \acute{y}_2 & \acute{y}_3 & \cdots & \acute{y}_{k-1} \\ 0 & 0 & \acute{y}_1 & \acute{y}_2 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \acute{y}_3 \\ 0 & 0 & 0 & \cdots & \acute{y}_1 & \acute{y}_2 \\ 0 & 0 & 0 & \cdots & 0 & \acute{y}_1 \end{bmatrix}$

$$=\begin{bmatrix} \acute{x}_1\acute{y}_1 & \acute{x}_1\acute{y}_2+\acute{x}_2\acute{y}_1 & \acute{x}_1\acute{y}_3+\acute{x}_2\acute{y}_2+\acute{x}_3\acute{y}_1 & \cdots & \acute{x}_1\acute{y}_k+\acute{x}_2\acute{y}_{k-1}+\cdots+\acute{x}_{k-1}\acute{y}_2+\acute{x}_k\acute{y}_1 \\ 0 & \acute{x}_1\acute{y}_1 & \acute{x}_1\acute{y}_2+\acute{x}_2\acute{y}_1 & \cdots & \acute{x}_1\acute{y}_{k-1}+\acute{x}_2\acute{y}_{k-2}+\cdots+\acute{x}_{k-2}\acute{y}_2+\acute{x}_k\acute{y}_{k-1} \\ 0 & 0 & \acute{x}_1\acute{y}_1 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \acute{x}_1\acute{y}_3+\acute{x}_2\acute{y}_2+\acute{x}_3\acute{y}_1 \\ 0 & 0 & \cdots & \acute{x}_1\acute{y}_1 & \acute{x}_1\acute{y}_2+\acute{x}_2\acute{y}_1 \\ 0 & 0 & \cdots & 0 & \acute{x}_1\acute{y}_1 \end{bmatrix}$$

Since $det(Q_1)=\acute{x}_1^k \neq 0, det(Q_2)=\acute{y}_1^k \neq 0$, therefore, $det(Q_1Q_2)=\acute{x}_1^k\acute{y}_1^k \neq 0$ implies $Q_1Q_2 \in Q$.

2. Let $Q_1 \in Q$, and $det(Q_1)=\acute{x}_1^k \neq 0$. Then,

$$Q_1{}^{-1}=\begin{bmatrix} \acute{x}_1^{-1} & \acute{x}_1^{-2}\acute{x}_2 & \acute{x}_1^{-3}\acute{x}_2^2+\acute{x}_1^{-2}\acute{x}_3 & \cdots & \acute{x}_k\acute{x}_1^{-2}+\cdots+\acute{x}_1^{-k}\acute{x}_2^{k-1} \\ 0 & \acute{x}_1^{-1} & \acute{x}_1^{-2}\acute{x}_2 & \cdots & \vdots \\ 0 & 0 & \acute{x}_1^{-1} & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \acute{x}_1^{-3}\acute{x}_2^2+\acute{x}_1^{-2}\acute{x}_3 \\ 0 & 0 & \cdots & \acute{x}_1^{-1} & \acute{x}_1^{-2}\acute{x}_2 \\ 0 & 0 & \cdots & 0 & \acute{x}_1^{-1} \end{bmatrix}$$

Since $det\left(Q_1{}^{-1}\right)=\acute{x}_1^{-k} \neq 0$, therefore $Q_1{}^{-1} \in Q$.

3. Let $Q_1, Q_2 \in Q$. Then,

$$Q_1Q_2=\begin{bmatrix} \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \acute{x}_4 & \cdots & \acute{x}_k \\ 0 & \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \cdots & \acute{x}_{k-1} \\ 0 & 0 & \acute{x}_1 & \acute{x}_2 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \acute{x}_3 \\ 0 & 0 & 0 & \cdots & \acute{x}_1 & \acute{x}_2 \\ 0 & 0 & 0 & \cdots & 0 & \acute{x}_1 \end{bmatrix}\begin{bmatrix} \acute{y}_1 & \acute{y}_2 & \acute{y}_3 & \acute{y}_4 & \cdots & \acute{y}_k \\ 0 & \acute{y}_1 & \acute{y}_2 & \acute{y}_3 & \cdots & \acute{y}_{k-1} \\ 0 & 0 & \acute{y}_1 & \acute{y}_2 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \acute{y}_3 \\ 0 & 0 & 0 & \cdots & \acute{y}_1 & \acute{y}_2 \\ 0 & 0 & 0 & \cdots & 0 & \acute{y}_1 \end{bmatrix}$$

$$=\begin{bmatrix} \acute{x}_1\acute{y}_1 & \acute{x}_1\acute{y}_2+\acute{x}_2\acute{y}_1 & \acute{x}_1\acute{y}_3+\acute{x}_2\acute{y}_2+\acute{x}_3\acute{y}_1 & \cdots & \acute{x}_1\acute{y}_k+\acute{x}_2\acute{y}_{k-1}+\cdots+\acute{x}_{k-1}\acute{y}_2+\acute{x}_k\acute{y}_1 \\ 0 & \acute{x}_1\acute{y}_1 & \acute{x}_1\acute{y}_2+\acute{x}_2\acute{y}_1 & \cdots & \acute{x}_1\acute{y}_{k-1}+\acute{x}_2\acute{y}_{k-2}+\cdots+\acute{x}_{k-2}\acute{y}_2+\acute{x}_k\acute{y}_{k-1} \\ 0 & 0 & \acute{x}_1\acute{y}_1 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \acute{x}_1\acute{y}_3+\acute{x}_2\acute{y}_2+\acute{x}_3\acute{y}_1 \\ 0 & 0 & \cdots & \acute{x}_1\acute{y}_1 & \acute{x}_1\acute{y}_2+\acute{x}_2\acute{y}_1 \\ 0 & 0 & \cdots & 0 & \acute{x}_1\acute{y}_1 \end{bmatrix}$$

$$=\begin{bmatrix} \acute{y}_1\acute{x}_1 & \acute{y}_2\acute{x}_1+\acute{y}_1\acute{x}_2 & \acute{y}_3\acute{x}_1+\acute{y}_2\acute{x}_2+\acute{y}_1\acute{x}_3 & \cdots & \acute{y}_k\acute{x}_1+\acute{y}_{k-1}\acute{x}_2+\cdots+\acute{y}_2\acute{x}_{k-1}+\acute{y}_1\acute{x}_k \\ 0 & \acute{y}_1\acute{x}_1 & \acute{y}_2\acute{x}_1+\acute{y}_1\acute{x}_2 & \cdots & \acute{y}_{k-1}\acute{x}_1+\acute{y}_{k-2}\acute{x}_2+\cdots+\acute{y}_2\acute{x}_{k-2}+\acute{y}_{k-1}\acute{x}_k \\ 0 & 0 & \acute{y}_1\acute{x}_1 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \acute{y}_3\acute{x}_1+\acute{y}_2\acute{x}_2+\acute{y}_1\acute{x}_3 \\ 0 & 0 & \cdots & \acute{y}_1\acute{x}_1 & \acute{y}_2\acute{x}_1+\acute{y}_1\acute{x}_2 \\ 0 & 0 & \cdots & 0 & \acute{y}_1\acute{x}_1 \end{bmatrix}$$

$$=\begin{bmatrix} y_1 & y_2 & y_3 & y_4 & \cdots & y_k \\ 0 & y_1 & y_2 & y_3 & \cdots & y_{k-1} \\ 0 & 0 & y_1 & y_2 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & y_3 \\ 0 & 0 & 0 & \cdots & y_1 & y_2 \\ 0 & 0 & 0 & \cdots & 0 & y_1 \end{bmatrix}\begin{bmatrix} \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \acute{x}_4 & \cdots & \acute{x}_k \\ 0 & \acute{x}_1 & \acute{x}_2 & \acute{x}_3 & \cdots & \acute{x}_{k-1} \\ 0 & 0 & \acute{x}_1 & \acute{x}_2 & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \acute{x}_3 \\ 0 & 0 & 0 & \cdots & \acute{x}_1 & \acute{x}_2 \\ 0 & 0 & 0 & \cdots & 0 & \acute{x}_1 \end{bmatrix}=Q_2Q_1$$

Hence it is proved that Q is an abelian subgroup of $GL\ (k, R_n')$. □

The probability P' that any matrix $N \in GL(k, R_n')$ but does not exist in Q is

$$P' = 1 - \frac{\phi(r)}{r}\text{ , where } r = |{R_n}'|$$

The following is the main scheme proposed in this article. Now we discuss Cryptosystems 1 and 2 in detail.

Cryptsystem 1

Key Generation

1. Choose fixed prime number $z = 2$ and random number n such that $r = z^n$, $n \geq 2$.

2. Select random elements $x_1 \in {R_n'}^*$ and $x_i \in R_n'$, where $i = 2,3,\dots,k$.

3. Construct two matrices from these elements, such that $L, M \in Q$ with $L \neq M$. If either matrix is not in Q then repeat Step 2.

4. Define α, β two commutative inner product automorphisms of $M_k({R_n}')$.

$$\alpha: A \to L^{-1}AL,\ \ \beta: A \to M^{-1}AM,\ \ \forall\ A\ \in M_k({R_n}')$$

5. Compute another automorphism of $M_k({R_n}')$ by taking the composition of the above two automorphisms,

$$\gamma = \alpha^2\beta, \omega = \beta^2\alpha$$

$$\gamma: A \to (L^2M)^{-1}A(L^2M),\ \ \omega: A \to (LM^2)^{-1}A(LM^2),\ \ \forall\ A\ \in M_k({R_n}')$$

Since α and β commute, therefore γ and ω also commute, and we have

$$\gamma = \alpha\beta^{-1}\omega, \omega\ = \alpha^{-1}\beta\gamma$$

Choose a random matrix $T \in GL(k, {R_n}')$ such that T does not belong to Q, and then calculate the public key $\left(r, \gamma(T), \omega(T^{-1})\right)$ and the private key (L, M).

Encryption

1. Choose the plaintext $m \in M_k({R_n}')$.

2. Now for each m, choose a unique random matrix $Z^m \in Q$.

3. Define commutative inner product automorphism $\delta: A \to (Z^m)^{-1}A(Z^m)$, $\forall A \in M_k(R'_n)$.

4. Calculate matrices $\delta(\gamma(T))$, $\delta(\omega(T^{-1}))$, and $m\delta(\gamma(T))$.

5. Choose a random unit element $u \in {R'_n}^*$ and calculate the ciphertext,

$$K = (K_1, K_2) = \left(u\delta(\omega(T^{-1})), u^{-1}m\delta(\gamma(T))\right)$$

Decryption

Compute the plaintext matrix $m = K_2\alpha\,\beta^{-1}(K_1)$.

Cryptsystem 2

Key Generation

1. Choose fixed prime number $z = 2$ and a random number n such that $r = z^n, n \geq 2$.

2. Select any random matrix $A \in GL(k, R'_n)$ such that $detA \in {R'_n}^*$.

3. Now compute the matrices $L = A^2, M = A^3, L^2M$, and LM^2.

4. Choose a random matrix $T \in GL(k, R'_n)$. Define α, β two commutative inner product automorphisms of $M_k(R_n{}')$, $\alpha: A \to L^{-1}AL$ and $\beta: A \to M^{-1}AM$, where $A \in M_k(R'_n)$.

5. Define other automorphisms γ & ω,

$$\gamma = \alpha^2\beta, \omega = \alpha\beta^2$$

$$\gamma: A \to (L^2M)^{-1}A(L^2M), \ \ \omega: A \to (LM^2)^{-1}A(LM^2), \ \ \forall A \in M_k(R'_n).$$

Since α and β commute, therefore γ and ω also commute, and we have

$$\gamma = \alpha\beta^{-1}\omega, \omega = \alpha^{-1}\beta\gamma$$

Calculate the public key $(r, LM, \gamma(T), \omega(T^{-1}))$ and the private key (L, M).

Encryption

1. Choose the plaintext $m \in M_k(R'_n)$.

2. Now for each m, choose an arbitrary integer $f \geq 2$, such that $V = (LM)^f$.

3. Define automorphism $\delta: A \to (V)^{-1}A(V)$, where $A \in M_k(R'_n)$.

4. Calculate the matrices $\left(\delta(\gamma(T)), \delta(\omega(T^{-1}))\right)$.

5. Choose a random unit element $u \in {R'_n}^*$ and calculate the ciphertext

$$K = (K_1, K_2) = \left(u\delta(\omega(T^{-1})), u^{-1}m\delta(\gamma(T))\right).$$

Decryption

Compute the plaintext matrix $m = K_2\alpha\beta^{-1}(K_1)$.

4. Illustration

Cryptsystem 1

Key generation

1. Select random integer $k = 3$, $n = 8$ and fixed number $z = 2$ such that $r = 2^8 = 256$.

2. Choose random elements $1, w^2 + w + 1 \in {R'_8}^*$ (diagonal entries of upper triangular matrices L and M) and $w + 1, w^2, w, w^2 + 1 \in R'_8$ (rest of entries of matrices).

3. Now the matrices $L, M \in Q$ with $L \neq M$.

$$L = \begin{pmatrix} 1 & w+1 & w^2 \\ 0 & 1 & w+1 \\ 0 & 0 & 1 \end{pmatrix}, M = \begin{pmatrix} w^2+w+1 & w & w^2+1 \\ 0 & w^2+w+1 & w \\ 0 & 0 & w^2+w+1 \end{pmatrix}$$

4. Define two inner product automorphisms α and β of $M_3(R'_8)$,

$$\alpha: A \to L^{-1}AL, \beta: A \to M^{-1}AM, \qquad \forall A \in M_3(R'_8)$$

5. Now define other automorphisms γ & ω of $M_3(R'_8)$,

$$\gamma = \alpha^2\beta, \omega = \beta^2\alpha$$

$$\gamma: A \rightarrow (L^2M)^{-1}A(L^2M), \omega: A \rightarrow (LM^2)^{-1}A(LM^2)$$

6. Select a random invertible matrix $T \in Q \leq GL(3, R'_8)$,

$$T = \begin{pmatrix} 1 & w & w^2+1 \\ w^2 & w+1 & w^3 \\ w^3+1 & w^2+w & w \end{pmatrix}$$

7. Calculate the matrices, $\big(\gamma(T), \omega(T^{-1})\big) = \big((L^2M)^{-1}(T)(L^2M), (LM^2)^{-1}(T^{-1})(LM^2)\big)$

$$\left(\begin{pmatrix} w^7+w^6+w^5+w^4+w^3+1 & w^7+w^6+w^3+w^2+1 & w^6+w^5+w^4+w^3+w^2+w+1 \\ w & w^7+w^5+w^4+w^2+w & w^5+w^3 \\ w^3+1 & 0 & w^6+w^3+w^2+w+1 \end{pmatrix}, \begin{pmatrix} w^7+w^2 & w^7+w^5+w^4 & w^6+w^5+w^4+w^3+w^2+w+1 \\ w^6+w^3+w^2 & w^7 & w^7+w^6+w^3+w^2+1 \\ w^7+w^5+w^4+w & w^7+w^3 & w^5+w^4+w^3+w^2+w \end{pmatrix}\right)$$

8. The public key is $\big(256, \gamma(T), \omega(T^{-1})\big)$ and the private key is $(L\ , M)$.

Encryption

1. Choose the plaintext $m \in M_3(R'_8)$

$$m = \begin{pmatrix} 1 & w & w^2 \\ w^3 & w^2+1 & w \\ w^2 & 1 & w+1 \end{pmatrix}$$

2. For each plaintext m, choose a unique matrix $Z^m = \begin{pmatrix} w & w+1 & w^2 \\ 0 & w & w+1 \\ 0 & 0 & w \end{pmatrix} \in Q$.

3. Define automorphism

$$\delta: A \rightarrow (Z^m)^{-1}A(Z^m), \quad \forall\, A \in M_3(R'_8)$$

4. Calculate $\Big(\delta\big(\gamma(T)\big), \delta\big(\,\omega(T^{-1})\big)\Big)$

$$\left(\begin{pmatrix} w^7+w^5+w+1 & w^6+w^4+w & w^5+w^4+w^2+w \\ w^7+w^3+w^2+w+1 & w^7+w^6+w^5+w^4+w^3+w^2+w & w^5+w^4+w \\ w^3+1 & w^7+w^3+w^2+1 & w^6+w^4+w^3+w^2+1 \end{pmatrix}, \begin{pmatrix} w^7+w^4+w^2+1 & w^7+w^4+w^2 & w^7+w^4+w^3+w^2 \\ w^7+w^5+w^2+w+1 & w^5+w^4+w^3 & w^7+w^6+w^3+1 \\ w^7+w^5+w^4+w & w^6+w^5+w+1 & w^7+w^4+w^2+w+1 \end{pmatrix}\right)$$

5. Now choose a unit element $u = 1 + w + w^2$ and calculate the ciphertext

$$K = (K_1, K_2) = \Big(u\delta\big(\,\omega(T^{-1})\big), u^{-1}m\delta\big(\gamma(T)\big)\Big)$$

$$\left(\begin{pmatrix} w^7+w^6+w^5+w^3 & w^7+w^6+w^5+w^3+w^2+w+1 & w^7+w^6+w^4+w^2+w+1 \\ w^6+w^5+w^4+w^2+w & w^7+w^5+w^3 & w^6+w^5+w^4+w^3+w^2+1 \\ w^4+w^3+w^2+1 & w^5+w^3 & w^7+w^6+w^5+w^2+w \end{pmatrix}, \begin{pmatrix} w^7+w^2+1 & w^5+w^4+w+1 & w^7+w^6+w^4+w^2+w+1 \\ w^7+w^6+w^5+w^2 & w^5+w^4+w^2 & w^7+w^6+w^5+w^4+w^3+w^2+1 \\ w^7+w^5+w^4+w+1 & w^6+w^5 & w^7+w^6+w^4+w^3+1 \end{pmatrix}\right)$$

Decryption

Compute the plaintext matrix $m = K_2\alpha\beta^{-1}(K_1) = \begin{pmatrix} 1 & w & w^2 \\ w^3 & w^2+1 & w \\ w^2 & 1 & w+1 \end{pmatrix}$

Cryptosystem 2

Key generation

1. Select a random number $k = 3, n = 8$, and fixed number $z = 2$ such that $r = 2^8 = 256$.

2. Choose a random matrix $A \in GL(3, R'_8)$ such that $detA \in {R'_8}^*$.

$$A = \begin{pmatrix} 1 & w & w^2+1 \\ w^2 & w+1 & w^3 \\ w^3+1 & w^2+w & w \end{pmatrix}$$

3. Calculate

$$L = A^2 = \begin{pmatrix} w^5+w^2 & w^4+w^3+w & w^4+w^3+w^2+w+1 \\ w^6 & w^5+w^4+w^3+w^2+1 & w^4+w^3+w^2 \\ w+1 & w^4+w^2 & w^4+w^3+1 \end{pmatrix}$$

$$M = A^3 = \begin{pmatrix} w^7+w^5+w^3+w+1 & w^5+w^2 & w^6+w^4+w^3+w \\ w^6+w^3 & w^7+w^3+w^2+w+1 & w^7+w^4 \\ w^7+w & w^6+w^5+w^3+w^2 & w^7+w^4+w^3+w^2+1 \end{pmatrix}$$

4. Choose a random invertible matrix $T \in GL(3, R'_8)$.

$$T = \begin{pmatrix} 1 & w & w^2 \\ w^3 & w^2+1 & w \\ w^2 & 1 & w+1 \end{pmatrix}$$

5. Define α, β inner product automorphisms of $M_3(R'_8)$ as

$$\alpha: A \to L^{-1}AL, \ \ \beta: A \to M^{-1}AM, \ \ \forall\, A \in M_3(R'_8)$$

6. Define other automorphisms γ and ω,

$$\gamma = \alpha^2\beta, \omega = \alpha\beta^2$$

$$\gamma: A \to (LM^2)^{-1}A(L^2M), \ \ \omega: A \to (LM^2)^{-1}A(LM^2), \forall A \in M_3(R'_8).$$

7. Calculate

$$\gamma(T) = (L^2M)^{-1}T(L^2M)$$
$$= \begin{pmatrix} w^7+w^6+w^4 & w^6+w^2+w+1 & w^7+w^5+w^4+1 \\ w^4+w^3+w^2+w+1 & w^5+w^3+w & w^4+w \\ w^6+w^5+w^3+w^2 & w^7+w^6+w^5+w^4+w^3+w+1 & w^7+w^6+w^5+w^4+w^3+w^2+1 \end{pmatrix}$$

$$\omega(T^{-1}) = (LM^2)^{-1}(T)^{-1}(LM^2)$$
$$= \begin{pmatrix} w^7+w^6+w^5+w^3+w^2+1 & w^4+w^2 & w^6+w^4+w^2 \\ w^7+w^6+w^2 & w^6+w^5+w^3 & w^7+w^6+w^3 \\ w^6+w^4+w^2+w & w^6+w^5+w & w^7+w^5+w^4+1 \end{pmatrix}$$

$$LM = \begin{pmatrix} w^5+w^4+w^3+w^2 & w^5+w^3+w^2+w+1 & w^6+w^5+w^3+w+1 \\ w^6+w^5+w^4+w^3+w & w^7+w^6+w^4+w^3+1 & w^7+w^4+w^3 \\ w^7+w^6+w^5+w^2+w+1 & w^6+w^5+w+1 & w^3+w^2+1 \end{pmatrix}$$

8. The public key is $\big(256, LM, \gamma(T), \omega(T^{-1})\big)$ and the private key is (L, M).

Encryption

1. Select the plaintext $m \in M_3(R'_8)$

$$m = \begin{pmatrix} w & w^7 & 1 \\ w^2+1 & w^2 & w^5 \\ w^3 & 1 & w+1 \end{pmatrix}$$

2. Select unique random number $f = 2$, for each plaintext m and then compute matrix $V = (LM)^2$,

$$\begin{pmatrix} w^7+w^5+w^4+w^3+w^2 & w^5 & w^7+w^5+w^3+w^2 \\ w^7+w^6+w^3+w^2+1 & w^6+w^5+w^4+w^2+w+1 & w^3+w^2+1 \\ w^5+w^4+w^3+w & w^7+w^5+w^2+w & w^7+w^6+w^4+w^3+w^2+w+1 \end{pmatrix}$$

3. Define automorphism $\delta: A \to (V)^{-1}(A)(V), \forall\, A \in M_3(R'_8)$.

4. Compute the matrices $\Big(\delta\big(\gamma\,(T)\big), \delta(\omega(T^{-1}))\Big)$

$$\left(\begin{matrix} \begin{pmatrix} w^7+w^5+w^4 & w^7+w^4+1 & w^6+w^4+w^3+w^2+1 \\ w^7+w^6+w^5+w^3 & w^7+w^6+w+1 & w^6+w+1 \\ w^6+w^5+w^4 & w^6+w^2 & w^6+w^5+w^4+w^2 \end{pmatrix}, \\ \begin{pmatrix} w^6+w^5+w^4+w^3+1 & w^4 & w^7+w^6+w^5+w+1 \\ w^7+w^2+1 & w^2 & w^4+w^3+w^2+w \\ w^6+w^5+w^2+w+1 & w^5+w^3+w+1 & w^6+w^3+1 \end{pmatrix} \end{matrix}\right)$$

5. Now choose a unit element $u = 1 + w + w^2$ and calculate the ciphertext

$$K = (K_1, K_2) = \left(u\delta\left(\ \omega(T^{-1})\right), u^{-1}m\delta\left(\gamma(T)\right)\right)$$

$$\left(\begin{pmatrix} w^6 + w^5 + w^3 + w^2 + w & w^6 + w^5 + w^4 & w^7 + w^5 + w^3 + w + 1 \\ w^7 + w^4 + w^3 & w^4 + w^3 + w^2 & w^6 + w^4 + w^3 + w \\ w^5 + w^4 + w^2 & w^7 + w^6 + w^4 + 1 & w^7 + w^6 + w^5 + w^4 + w^3 + w^2 + w \end{pmatrix}, \begin{pmatrix} w^4 + w^2 + w + 1 & w^7 + w^6 + w^5 + w^3 + w^2 & w^7 + w^6 + w^3 + w^2 + w + 1 \\ w^5 + w^3 + 1 & w^7 + w^6 + w^2 + w & w^7 + w^6 + w^5 + w + 1 \\ w^7 + w^4 + w & w^7 & w^7 + w^6 + w^4 + 1 \end{pmatrix}\right)$$

Decryption

1. Compute the plaintext matrix

$$m = K_2\alpha\beta^{-1}(K_1) = \begin{pmatrix} w & w^7 & 1 \\ w^2 + 1 & w^2 & w^5 \\ w^3 & 1 & w + 1 \end{pmatrix}.$$

Theorem 1. *The algorithm of Cryptosystems 1 and 2 are accurate.*

Proof of Theorem 1. Since automorphisms in the proposed cryptosystems remain the same, so its proof is similar to the original scheme. The commutative inner automorphisms are defined in this article $\alpha: A \to L^{-1}AL$, $\beta: A \to M^{-1}AM$, $\forall\ A \in M(k, R'_n)$, and another automorphism of $M(k, R'_n)$ by taking the composition of above two automorphisms $\gamma = \alpha^2\beta: A \to (L^2M)^{-1}A(L^2M)$, $\omega = \beta^2\alpha: A \to (LM^2)^{-1}A(LM^2)$. Since α and β commute, therefore γ and ω also commute, and we have $\gamma = \alpha\beta^{-1}\omega$, $\omega\ = \alpha^{-1}\beta\gamma$

$$K_2\alpha\beta^{-1}(K_1) = \left(um\delta\left(\gamma\ (T)\right)\right)\left(\alpha\beta^{-1}\left(u^{-1}\delta\left(\omega(T^{-1})\right)\right)\right)$$

$$= \left(uu^{-1}m\delta\left(\gamma\ (T)\right)\right)\left(\left(\delta\left(\alpha\beta^{-1}\left(\omega(T^{-1})\right)\right)\right)\right)$$

$$= \left(m\delta\left(\gamma(T)\right)\right)\left(\left(\delta\left(\gamma(T^{-1})\right)\right)\right), \quad uu^{-1} = 1$$

$$= \left(m\delta\left(\gamma(TT^{-1})\right)\right)$$

$$= \left(m\delta\left(\gamma(I)\right)\right)\ = \left(m\delta(I)\right)\ = m(I) = m$$

□

Now, we illustrate the comparison of proposed and original schemes in Table 1. This demonstrates that we compute different public keys from the same private keys in both algebraic structures. Further detail is given in the security analysis section. (Note that we can convert elements from R'_8 to $\mathbb{Z}_{256}$ and vice versa).

Table 1. Comparison of the proposed scheme and the original scheme.

	Comparison of Proposed Scheme Original Scheme	
	Proposed Scheme	**Original Scheme**
Local Ring	R'_8	$\mathbb{Z}_{256}$
Operation	Polynomial addition and multiplication s.t $w^{8n} = 1, w^{9n} = w, w^{10n} = w^2, w^{11n} = w^3, w^{12n} = w^4, w^{13n} = w^5, w^{14n} = w^6, w^{15n} = w^7, n \in N$	Modulo addition and multiplication
Non-Commutative Group	$GL(3, R'_8)$	$GL(3, \mathbb{Z}_{256})$
	Cryptsystem 1	
Public-Key	$L = \begin{pmatrix} 1 & 1+w & w^2 \\ 0 & 1 & 1+w \\ 0 & 0 & 1 \end{pmatrix}, M = \begin{pmatrix} 1+w+w^2 & w & 1+w^2 \\ 0 & 1+w+w^2 & w \\ 0 & 0 & 1+w+w^2 \end{pmatrix}$	$L = \begin{pmatrix} 1 & 3 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix},$ $M = \begin{pmatrix} 7 & 2 & 5 \\ 0 & 7 & 2 \\ 0 & 0 & 7 \end{pmatrix}$
Private-Key	$\left(256, \gamma(T), \omega(T^{-1})\right)$	$\left(256, \gamma(T), \omega(T^{-1})\right)$

	$\left\{\begin{matrix} 256, \\ \begin{pmatrix} w^7+w^6+w^5+w^4+w^3+1 & w^7+w^6+w^3+w^2+1 & w^6+w^5+w^4+w^3+w^2+w+1 \\ w & w^7+w^5+w^4+w^2+w & w^5+w^3 \\ w^3+1 & 0 & w^6+w^3+w^2+w+1 \end{pmatrix} \\ \begin{pmatrix} w^7+w^2 & w^7+w^5+w^4 & w^6+w^5+w^4+w^3+w^2+w+1 \\ w^6+w^3+w^2 & w^7 & w^7+w^6+w^3+w^2+1 \\ w^7+w^5+w^4+w & w^7+w^3 & w^5+w^4+w^3+w^2+w \end{pmatrix} \end{matrix}\right\}$	$\left\{\begin{matrix} 256, \\ \begin{pmatrix} 73 & 202 & 133 \\ 240 & 11 & 156 \\ 9 & 26 & 178 \end{pmatrix} \\ \begin{pmatrix} 95 & 166 & 87 \\ 187 & 252 & 96 \\ 155 & 153 & 207 \end{pmatrix} \end{matrix}\right\}$
	Cryptsystem 2	
Public-Key	$A=\begin{pmatrix} 1 & w & w^2+1 \\ w^2 & w+1 & w^3 \\ w^3+1 & w^2+w & w \end{pmatrix}$ $L=\begin{pmatrix} w^5+w^2 & w^4+w^3+w & w^4+w^3+w^2+w+1 \\ w^6 & w^5+w^4+w^3+w^2+1 & w^4+w^3+w^2 \\ w+1 & w^4+w^2 & w^4+w^3+1 \end{pmatrix}$ $M=\begin{pmatrix} w^7+w^5+w^3+w+1 & w^5+w^2 & w^6+w^4+w^3+w \\ w^6+w^3 & w^7+w^3+w^2+w+1 & w^7+w^4 \\ w^7+w & w^6+w^5+w^3+w^2 & w^7+w^4+w^3+w^2+1 \end{pmatrix}$	$A=\begin{pmatrix} 1 & 2 & 5 \\ 4 & 3 & 8 \\ 9 & 6 & 2 \end{pmatrix},$ $L=\begin{pmatrix} 54 & 38 & 31 \\ 88 & 65 & 60 \\ 51 & 48 & 97 \end{pmatrix}$ $M=\begin{pmatrix} 229 & 152 & 124 \\ 120 & 219 & 56 \\ 92 & 60 & 65 \end{pmatrix}$
Private-Key	$(256,\gamma(T),\omega(T^{-1}),LM)$ $\left\{\begin{matrix} 256, \\ \begin{pmatrix} w^7+w^6+w^4 & w^6+w^2+w+1 & w^7+w^5+w^4+1 \\ w^4+w^3+w^2+w+1 & w^5+w^3+w & w^4+w \\ w^6+w^5+w^3+w^2 & w^7+w^6+w^5+w^4+w^3+w+1 & w^7+w^6+w^5+w^4+w^3+w^2+1 \end{pmatrix}, \\ \begin{pmatrix} w^7+w^6+w^5+w^3+w^2+1 & w^4+w^2 & w^6+w^4+w^2 \\ w^7+w^6+w^2 & w^6+w^5+w^3 & w^7+w^6+w^3 \\ w^6+w^4+w^2+w & w^6+w^5+w & w^7+w^5+w^4+1 \end{pmatrix}, \\ \begin{pmatrix} w^5+w^4+w^3+w^2 & w^5+w^3+w^2+w+1 & w^6+w^5+w^3+w+1 \\ w^6+w^5+w^4+w^3+w & w^7+w^6+w^4+w^3+1 & w^7+w^4+w^3 \\ w^7+w^6+w^5+w^2+w+1 & w^6+w^5+w+1 & w^3+w^2+1 \end{pmatrix} \end{matrix}\right\}$	$(256,\gamma(T),\omega(T^{-1}),LM)$ $\left\{\begin{matrix} 256, \\ \begin{pmatrix} 123 & 21 & 104 \\ 6 & 133 & 180 \\ 126 & 53 & 9 \end{pmatrix}, \\ \begin{pmatrix} 29 & 37 & 156 \\ 50 & 7 & 94 \\ 52 & 52 & 117 \end{pmatrix}, \\ \begin{pmatrix} 66 & 214 & 87 \\ 192 & 235 & 20 \\ 251 & 20 & 213 \end{pmatrix} \end{matrix}\right\}$

5. Security Analysis of the Proposed Cryptosystem

The essence of every cryptosystem lies in its security. So, to find the efficiency of any cryptosystem, security analysis plays a fundamental role in this aspect. Now we discuss some attacks. The proposed scheme has the potential to resist these attacks effectively.

5.1. Ciphertext-Only Attack

Suppose $(r,\gamma(T),\omega(T^{-1}),\ K_1,K_2)$ information is known to the adversary, and he wants to compute the message m by using a ciphertext-only attack, as done by Jianwei Jia et al. [14] for $\mathbb{Z}_n$. First of all, the attacker finds out the invertible element $u\in R_n'^{*}$ by $\det(\ K_1)=(u)^2 det\left(\omega(T^{-1})\right),\ \forall K_1$ (Note inverse of R_n' is hard to compute as compare with $\mathbb{Z}_n$, since the square root of polynomials makes this step laborious for the attacker). Now, the cryptanalyst solves the system of homogeneous linear equations,

$$(Z^m)K_1=u\omega(T^{-1})(Z^m) \tag{1}$$

After solving the system of Equation (1), he can compute the unknown matrix $Z^m=Z_o^m$ for each $u=u_0$. Finally, he solves the system (2) and decrypts the corresponding message $m=m_o$.

$$m_0=u_0K_2(Z_o^m)^{-1}\gamma(T)^{-1}Z_o^m \tag{2}$$

(Note that here, the systems consist of the polynomial matrices from $GL(k,R_n')$ since equations have become nonlinear, so it becomes hard to find an unknown matrix Z_o^m for a large value of k. However, the attacker can easily compute this system in $\mathbb{Z}_n$. On the other hand, if an attacker tries to compute the system in $\mathbb{Z}_n$ by converting the given information from R_n' to $\mathbb{Z}_n$, it does not work because the public key generated in both cryptosystems differ and the attacker fails to compute m as demonstrate in comparison Table 1 for R_8' and $\mathbb{Z}_{256}$).

The cryptanalyst gets $\phi(r)r^{k-1}$ possibilities of Z^m since he has $\phi(r)$ possibilities of diagonal entry and r^{k-1} possibilities rest of upper diagonal entries of Z^m. Hence, it is clear that it becomes infeasible for the attacker to decrypt the plaintext for a large value of r and k.

5.2. Known-Plaintext Attack

In this case, the adversary gets access to some of the plaintext m and its ciphertext K. He fails to reveal any information about the key. Because for each plaintext m, we choose a unique matrix Z^m, the cryptanalyst wants to find out all pairs (m, Z^m), but, in this case, he cannot find a new pair from the known information. Hence the attacker is not able to retrieve any information and is incapable of this attack.

5.3. Chosen-Ciphertext Attack and its Prevention

Suppose Alice wants to send a message m to Bob. She decrypts the message m and finds the ciphertext $K = (K_1, K_2)$. The attacker intercepts during the communication and gets access to ciphertext K. He selects a random matrix $\ddot{m} \in GL(k, R'_n)$ and sends $K^* = (K_1, \ddot{m}\, K_2)$ to Bob. Now Bob deciphers the false ciphertext K^* and computes a new plaintext $m^* = mK^*$. The cryptanalyst uses this information and finds the original message m successfully.

$$(\ddot{m}\ )^{-1}(\ddot{m}\, m) = m$$

To protect the cryptosystem from this type of attack, one must replace the one-sided ciphertext with the two-sided ciphertext text. Now replace the ciphertext,

$K_1 = u(Z^m)^{-1}\big(\omega(T^{-1})\big)Z^m$, $K_2 = (u^{-1})^2(Z^m)^{-1}\big(\gamma(T)\big)Z^m \quad (m)\ (Z^m)^{-1}\big(\gamma(T)\big)Z^m$. In this case, one can decrypt the message by calculating $m = \alpha\beta^{-1}(K_1)K_2\alpha\beta^{-1}(K_1)$ since the matrices Z^m and m do not commute in general. Hence this attack is inefficient in this scenario.

6. Conclusions

In this article, asymmetric cryptosystems of [13] have been generalized and the residue ring has been replaced by a finite chain ring. The local ring $\mathbb{Z}_n$ resulted in the insecurity of the cryptosystem, as inferred by Jianwei Jia et al. [14] in their cryptoanalysis of the original scheme. It can be anticipated that the security of the proposed algorithm increased compared to the original one for various attacks. The finite local ring R'_n enhances the complexity of algorithms in a way that it becomes laborious for the attacker to decrypt it. Hence, it maximizes the computational security of the cryptosystem. The chain ring has the potential to resist the attacks and both cryptosystems are invulnerable in a sense that attackers unable to solve the system of equation in R'_n for large values of n and k. The use of a binary field in the local ring R'_n avoids the exponentiation approach, which makes it efficient to use in various applications.

Author Contributions: Conceptualization, M.Y., T.S. and I.H.; methodology, M.Y., T.S. and I.H.; software, M.Y., T.S. and I.H.; validation, M.Y., T.S. and I.H.; formal analysis, M.Y., T.S. and I.H.; investigation, M.Y., T.S. and I.H.; resources, M.Y., T.S. and I.H.; data curation, M.Y., T.S. and I.H.; writing—original draft preparation, M.Y., T.S. and I.H.; writing—review and editing, M.Y., T.S. and I.H.; visualization, M.Y., T.S. and I.H.; supervision, T.S.; project administration, T.S.; funding acquisition, I.H. All authors have read and agreed to the published version of the manuscript.

Funding: The publication of this article was funded by the Qatar National Library.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654.
2. Elgamal, T. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472.
3. Kumar, M.; Gupta, P. Cryptographic schemes based on elliptic curves over the ring Zp. *Appl. Math.* ***2016***, *7*, 304–312.
4. Islam, M.; Islam, M.; Islam, N.; Shabnam, B. A modified and secured RSA public key cryptosystem based on "n" prime numbers. *J. Comput. Commun*. **2018**, *6*, 78–90.

5. Pradhan, S.; Sharma, B. An efficient RSA cryptosystem with BM-PRIME method. *Int. J. Inf. Netw. Secur.* **2012**, *2*, doi:10.11591/ijins.v2i1.1718.
6. Lüy, E.; Karatas, Z.; Ergin, H. Comment on "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)". *J. Inf. Secur. Appl.* **2016**, *30*, 1–2.
7. Muzereau, A.; Smart, N.; Vercauteren, F. The equivalence between the DHP and DLP for elliptic curves used in practical applications. *Lms J. Comput. Math.* **2004**, *7*, 50–72.
8. Bernstein, D.J.; Lange, T. SafeCurves: Choosing Safe Curves for Elliptic-Curve Cryptography. Available online: https://safecurves.cr.yp.to (accessed on 12 May 2020).
9. Zhu, Z.; Yao, G. New digital signature scheme based on discrete logarithm. *J. Comput. Appl.* **2009**, *29*, 2342–2343.
10. Patel, P. Secure digital signature schemes based on hash functions. *Int. J. Comput. Eng. Sci.* **2015**, *1*, 27, doi:10.26472/ijces.v1i1.18.
11. Bennett, C.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2011**, doi:10.1016/j.tcs.2011.08.039.
12. Braun, J.; Buchmann, J.; Mullan, C.; Wiesmaier, A. Long term confidentiality: A survey. *Des. Codes Cryptogr.* **2012**, *71*, 459–478.
13. Khan, M.; Shah, T. A novel cryptosystem based on general linear group. *3D Res.* **2014**, *6*, 2, doi:10.1007/s13319-014-0035-2.
14. Jia, J.; Liu, J.; Zhang, H. Cryptanalysis of cryptosystems based on general linear group. *China Commun.* **2016**, *13*, 217–224.
15. Karatas, Z.; Luy, E.; Gonen, B. Public key cryptosystem based on matrices. *Int. J. Comput. Appl.* **2019**, *182*, 47–50.