π-McCOY RINGS AS A BASIS OF A ZERO KNOWLEDGE CRYPTOSYSTEM

Areej M. Abduldaim
University of Technology, Applied Sciences Department, Mathematics and Computer Applications, Baghdad, Iraq
E-mail: areejmussab@gmail.com

***ABSTRACT**: In this paper, a novel approach for conveying abstract algebra, that represented by ring theory and algebraic structures, to cryptography is proposed. The zero-knowledge proof is an interactive cryptosystem used for identification. Ring theory, through the algebraic structure π-McCoy rings, is taken into consideration to construct a new algorithm for the zero-knowledge proof used a secret polynomial and specific parameters that achieve some conditions based on satisfying if the notion of π-McCoy rings and some characterizations. The aim is to introduce a modern algorithm with a key polynomial whose coefficients are in a π-McCoy ring and this polynomial is protected by the prover. In fact, the π-McCoy zero-knowledge scheme does not detect the original secret polynomial. This scheme is particularly useful in cryptographic applications, such as digital signature and key agreement.*

Keywords: *π-McCoy rings, zero-knowledge proof, polynomial rings, identification, nilpotent polynomial.*

1. INTRODUCTION

Cryptography is the art and science of keeping messages secure by converting them from one form to another. Several cryptography algorithms such as Advanced Encryption Standard (AES), DES, and International Data Encryption Algorithm (IDEA) were implemented for data encryption. These algorithms are suitable for encryption of the least amount of data however they are not suitable when the data to be encrypted is huge. That is because these algorithms need large computation times and therefore super-fast processing machines. [1]

Cryptography is the study of mathematical techniques related to information security aspects such as confidentiality, data integrity, and authentication [2]. The advantage of steganography over cryptography is that its messages do not attract other people's attention. The core message is retained, only in its delivery obscured or hidden in various ways. So only the legitimate recipient can know the core message [3].

Cryptography is divided into two, namely symmetrical and asymmetrical. Symmetric cryptography has the same key in the encryption and decryption process, so the security of this key symmetry system lies in the secrecy of the key. Examples of symmetrical algorithms are Permutation Cipher, Substitute Cipher, Hill Cipher, OTP, RC6, Twofish, Magenta, FEAL, SAFER, LOCI, CAST, Rijndael (AES), Blowfish, GOST, A5, Kasumi, DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm). Asymmetric cryptography has two keys in the process of encryption and decryption, where the encryption key is public (public key), and the decryption key is confidential (private key). Examples of well-known asymmetrical algorithms are RSA (Rivest Shamir Adleman), ECC (Elliptic Curve Cryptography and ElGamal) [3].

The zero-knowledge (ZK) scheme is a process utilized for authentication problems. Basically, the first tip has to prove knowing the true password without transit any data about that password to the trusted second tip. This is a method to avert transiting data over network channels that can be detected by the third tip. Through an overview of authentication-schemes turns out to be the one who gave for the first time the zero-knowledge proof (ZKP) was Goldwasser et al. [4] in 1985. In [5], Goldreich *et al*. the scheme of ZKM has been given because of the wide applications of the zero-knowledge.

Micali in [6] and Shamir in [7] show up an improvement to this protocol that reduces the complexity of the verifier to less than about two different modular multiplications and makes the prover's complexity steady. The notion of interactive proofs of assertions was introduced by Fiege et al. [8] to interactive proofs of knowledge.

The identification scheme, Guillou Quisquater (GQ) [9] is regarded as an expansion to Fiat-Shamir protocol, that decreases some memory requirements and exchanged messages for secret keys. Additionally, the GQ scheme is considered as RSA scheme expansion, which reduces the number of necessary runs to just 1, while the security of this scheme is relying on RSA cryptosystem robustness. The possibility of forged the signature that is relying on (Fiege) Fiat-Shamir was demonstrated by Goldwasser and Kalai [10]. On the other hand, a good ZKP relying on the NP-complete case has been introduced in [11] by Courtois and named as MinRank. Furthermore, to solve authentication problems zero-knowledge schemes can be utilized as presented Wolf in [12]. Zero-knowledge proofs are of wide applicability in the field of cryptographic protocols, Oren in [13] investigated some aspects of these systems. Oren presented new definitions of zero-knowledge, discuss their importance and investigated their relative power. Furthermore, Oren demonstrated that certain properties are essential to zero knowledge of interactive proofs. The class of symmetric algorithms includes the algorithms used in the three-pass protocol that follows the commutative-encryption system. Rachmawati *et al.* [14], take an unconventional approach: instead of using a symmetric algorithm, we use RSA, an asymmetric algorithm, in the three-pass protocol.

All the past research were studied on a finite field, thus, making use of a modern algebraic framework based on rings of polynomial regards a promising challenge in cryptography. In mathematics, a ring is an algebraic framework in which an abelian group together with addition and multiplication such that multiplication distributes over addition. In fact, the ring presuppositions demand that: 1- addition is a commutative operation, 2- addition and multiplication are associative

operations, 3- the multiplication operation distributes over addition operation, 4- each element in the group has an inverse under addition operation, and finally, 5- there exists an identity under addition operation. The set of integers is a familiar example of a ring under the ordinary addition and multiplication operations [15].

Ring theory is the branch of mathematics that studies rings. The properties of the mathematical structures like polynomials and integers are studied by ring theory. The ubiquity of rings makes them a central organizing principle of contemporary mathematics [15].

Ring theory is used all over the place in computer science, from databases to machine learning to formal language theory to image processing. Basically, the algebraic structures are useful for understanding how one can transform a situation given various degrees of freedom, and as this is a fundamental type of question, these structures end up being essential. Mathematical procedures on rings can be conveyed in an ordinary method to mathematical procedures of matrices and vectors created in new categories. This method needs to utilize the natural addition operation, subtraction operation, multiplication operation, powers operation, and transposition of matrices. hence, it is well known that every field is a ring but the converse is not true in general, this means that not every ring is a field, such as the ring of integers and different rings of polynomials (polynomial rings over the field of rational numbers Q[x], polynomial rings over the field of real numbers R[x], polynomial rings over the field of complex numbers C[x] or polynomial rings of integral coefficients Z[x]). Mathematical calculations used in these rings are natural operations. The zero elements are 0 and the identity of the multiplication operation is 1. In addition, Zm (residue classes modulo m) forms a ring, so a residue class ring is truly a ring. Ring Theory has been well-used in cryptography and many other computer vision tasks.

During this work, the associative rings with identity are considered to use unless otherwise mentioned. Let $\mathcal{R}$ be a ring, the set of all polynomials in the indeterminate χ, is called the polynomial ring and denoted by $\mathcal{R}[\chi]$. Any element belongs to $\mathcal{R}[\chi]$ is of the form $\varphi(\chi) = a_0 + a_1\chi + a_2\chi^2 + \cdots + a_m\chi^m$, where m can be any nonnegative integer and the coefficients $a_0, a_1, a_2, \cdots, a_m$ are all in $\mathcal{R}$. Let $\mathcal{M}_n(\mathcal{R})$ be the $n \times n$ matrix ring over $\mathcal{R}$. The prime radical of $\mathcal{R}$ (which is the intersection of all prime ideals) can be denoted by $\mathcal{P}(\mathcal{R})$. The set of all nilpotent elements in $\mathcal{R}$ can be denoted by $\aleph(\mathcal{R})$. Finally, set $\mathbb{Z}$ is the ring of integers.

Following Nielsen [16], a ring $\mathcal{R}$ is said to be right McCoy if for any two polynomials $\varphi(\chi)$ and $\psi(\chi) \in \mathcal{R}[\chi] \setminus \{0\}$ such that $\varphi(\chi)\,\psi(\chi) = 0$, then there exists $r \in \mathcal{R} \setminus \{0\}$ satisfies $\varphi(\chi)r = 0$. A left McCoy ring is defined similarly. If a ring is both right and left McCoy, then it is called McCoy ring. Commutative rings are McCoy [16]. Young et al. [17] introduced the concept of π-McCoy rings. For any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i\chi$, $\psi(\chi) = \sum_{j=0}^{n} b_j\chi$ in $\mathcal{R}[\chi]$, a ring R is said to be π-McCoy if whenever $\varphi(\chi)\,\psi(\chi) \in \aleph(\mathcal{R}[\chi])$, then $\varphi(\chi)\varsigma \in \aleph(\mathcal{R}[\chi])$ for some $\varsigma \in \mathcal{R} \setminus \{0\}$, where $\varphi(\chi)$ and $\psi(\chi)$ are in $\mathcal{R}[\chi] \setminus \{0\}$. Motivated by all of the above, in this paper, we introduced a new algorithm for the zero-knowledge protocol using the notion of π-McCoy rings. Starting with an initial setup in which we fix $\mathcal{R}$ to be a π-McCoy ring and choose the secret polynomial to create the key. The authentication process depends on a test (a symbolic dialogue) between the prover Piper and the verifier Vali, through it Vali can decide whether Piper has the secret or not.

The rest of this paper is organized as follows. Section 2 is devoted to recalling some mathematical preliminaries of π-McCoy rings. In Section 3, we summarize information about the original zero-knowledge protocol. Section 4 presents the proposed π-McCoy zero-knowledge algorithm. The analysis of this protocol is put forward in section 5. In the end, the conclusion is given in Section 6.

It is worth noting that there are several notions concerning and nearby to the concept of the π-McCoy rings. The first one is the Armendariz rings and its generalizations in addition to α- skew π-McCoy rings [18-20]. On the other hand, there are several applications of the series of Armendariz rings in zero-knowledge cryptosystems [21, 22].

2. MATHEMATICAL PRELIMINARIES OF π-McCOY RINGS

In this section, we will provide the reader with known and basic important information that will be used in the rest of this paper.

2.1 Definition [17]

To construct a robust scheme, the properties of the polynomial ring concerning this type of rings and the condition of π-McCoy rings should be integrated with the fundamentals of the zero-knowledge to reach the aim that we seek. The definition of π-McCoy rings is recalled in addition to some basics and properties which are necessary for the rest of the paper are given.

A ring R is said to be π-McCoy if whenever $\varphi(\chi)\,\psi(\chi) \in \aleph(\mathcal{R}[\chi])$, then $\varphi(\chi)\varsigma \in \aleph(\mathcal{R}[\chi])$ for some $\varsigma \in \mathcal{R} \setminus \{0\}$, where $\varphi(\chi)$ and $\psi(\chi)$ are in $\mathcal{R}[\chi] \setminus \{0\}$.

Let $\mathcal{R}$ be any ring. For any integer $n \geq 2$, consider $\mathcal{M}_n(\mathcal{R})$ be the $n \times n$ matrix ring. Let $U_n(\mathcal{R})$ and $L_n(\mathcal{R})$ be the $n \times n$ upper and lower triangular matrix ring over a ring $\mathcal{R}$. The following Lemma is given in [17, Lemma 1.2].

2.2 Lemma [17]

1- For any ring $\mathcal{R}$, if there exists an ideal $(\neq 0)I \subseteq \mathcal{R}$ with $I[\chi] \subseteq \aleph(\mathcal{R}[\chi])$, then $\mathcal{R}$ is π-McCoy.

2- If $\mathcal{R}$ is a non-semiprime ring, then $\mathcal{R}$ is π-McCoy.

3- For any ring $\mathcal{R}$ such that there exists a nonzero nilpotent ideal in $\mathcal{R}$, then the ring $\mathcal{M}_n(\mathcal{R})$ (n≥1) is π-McCoy.

4- For any ring $\mathcal{R}$ the rings $U_n(\mathcal{R})$ and $L_n(\mathcal{R})$ are π-McCoy where $n \geq 2$.

5- For any two rings $\mathcal{R}$ and $\mathcal{S}$, a bimodule ${}_{\mathcal{R}}\mathcal{M}_{\mathcal{S}} \begin{pmatrix} \mathcal{R} & \mathcal{M} \\ 0 & \mathcal{S} \end{pmatrix}$ and ${}_{\mathcal{R}}\mathcal{M}_{\mathcal{S}} \begin{pmatrix} \mathcal{R} & 0 \\ \mathcal{M} & \mathcal{S} \end{pmatrix}$ resp. are π-McCoy.

6- For any ring $\mathcal{R}$ and any positive integer n, we have that $\mathcal{R}[\chi]/(\chi^n)$ is a π-McCoy ring where (χ^n) is a principal ideal.

7- For any ring $\mathcal{R}$ and a central element $0 \neq a \in \mathcal{N}(\mathcal{R})$, the ring $\mathcal{M}_n(\mathcal{R})$ is π-McCoy.

2.3 Remarks

1- For any reduced ring $\mathcal{R}$, the full matrix ring $n \times n$ over $\mathcal{R}$ is not π-McCoy where $n \geq 2$ [17].

2- The ring $\mathcal{M}_n(Zm^2)$ is π-McCoy by *Lemma 2.2* (7) where $m \geq 2$ is an integer. Despite, there exist non-π-McCoy matrix rings (for example $\mathcal{M}_n(Zp)$, p is prime) by 1 above.

3. THE FIRST ZERO KNOWLEDGE PROTOCOL

Wide investigations regarding ZKP have been studied. There are proofs usually viewed (especially by scientists) based on a static mathematical object.

The Prover Peggy (P): P conceals a secret σ, P has to prove that she knows σ without divulging σ itself.

The Verifier Victor (V): P will be asked certain questions by V to be sure that P truly knows σ or not. At the same time, V suppose to be know everything about σ, even in a case whereby that he deceives or intent not to perpetuate to the system itself.

The Eavesdropper Eave: Basically, the tip who eavesdropping to the conversation amidst P and V is called Eave (E). A safe ZKP ensures that no other tip can possibly know any information about σ.

Meanwhile, an interactive proof system specifically a set Σ is considered as a two valency match existing amidst a verifier and a proover and it fulfills two different attributes:

1. The Completeness: P owns a very big chance of persuasive V if she could find out σ ∈Σ,

2. The Soundness: Peggy owns a very minimum probability to fool Vic in case she's not aware of σ.

Zero-Knowledge Property: There are many advantages can be characterizing ZKP; V is not able to know anything from the protocol. V is not able to deceive the P, V is not able to claim to be the P to any other tip and the P is not able to deceive the V.

4. THE PROPOSED ALGORITHM FOR THE ZERO KNOWLEDGE PROOF THROUGH π-McCOY RINGS

In this section, *the* π-McCoy zero-knowledge algorithm is given started with the initial setup in which we fix $\mathcal{R}$ to be a π-McCoy ring and set the secret polynomial to create a key. The authentication process depends on a test (a symbolic dialogue) between the prover Piper and the verifier Vali, through it Vali can decide whether Piper really has the secret or not.

4.1 The Algorithm

Suppose that $\mathcal{R}$ is a π-McCoy ring and $\mathcal{R}$ is the underlying work fundamental infrastructure where $\mathcal{R}[\chi]$ is the polynomial ring over $\mathcal{R}$. Both of the prover and the verifier know that the ring $\mathcal{R}$ is π-McCoy.

For any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i\chi^i$, $\psi(\chi) = \sum_{j=0}^{n} b_j\chi^j \in \mathcal{R}[\chi]$, Piper the prover computes the product of $\varphi(\chi)$ and $\psi(\chi)$, such that, $\varphi(\chi)\varsigma \in \aleph(\mathcal{R}[\chi])$ for some $\varsigma \in \mathcal{R} \setminus \{0\}$ and publishes her public key, the set $\varphi\varsigma_{coef.} = \{a_i\varsigma | 0 \leq i \leq m \text{ and } \varsigma \in \mathcal{R}\}$ to show Vali the verifier that each element of the set $\varphi\varsigma_{coef.}$ is nilpotent without sharing the secret polynomial $\varphi(\chi)$ as Piper private key. This polynomial is kept by the prover and never shared.

Step 1: Piper chooses (χ) , $\psi(\chi) \in \mathcal{R}[\chi]$ and $\varsigma \in \mathcal{R}$ such that $\varphi(\chi)\psi(\chi) \in \aleph(\mathcal{R}[\chi])$ where $\varphi(\chi)\varsigma = \{a_i\varsigma | 0 \leq i \leq m \; and \; \varsigma \in \mathcal{R}\}$ and sends Vali the set $\varphi\varsigma_{coef.} = \{a_i\varsigma | 0 \leq i \leq m \text{ and } \varsigma \in \mathcal{R}\}$.

Step 2: Vali chooses randomly $r = 0$ or 1 and sends it to Piper.

Step 3: For each i, Piper finds $k_i \in \mathbb{Z}^+$, such that $(a_i\varsigma)^{k_i} = 0$, k_{ij} depends on i and send Vali $k_i - r$ as a power of $a_i\varsigma$.

Step 4: Vali checks that:

f $r = 0$, then Vali checks that $(a_i\varsigma)^{k_i - r} = 0$ (because Vali knows that $\mathcal{R}$ is π-McCoy ring & $r = 0$), which means that $a_i\varsigma$ is a nilpotent element.

If $r = 1$, it is definitely Vali checks that $(a_i\varsigma)^{k_i - r} \neq 0$ (this means that $a_i\varsigma \notin \aleph(\mathcal{R})$ which contradicts the fact that $\mathcal{R}$ is π-McCoy ring).

The verifier accepts the proof if $(a_i\varsigma)^{k_i - r} = 0$ and rejects it if $(a_i\varsigma)^{k_i - r} \neq 0$.

Step 5: Repeat the above steps λ times, where λ is the number of polynomials $\varsigma \in \mathcal{R}$ such that $\varphi(\chi)\psi(\chi) \in \aleph(\mathcal{R}[\chi])$. To find λ, we should first determine the degree k of $\psi(\chi)$ which should be large enough.

4.2 Example

Let

$$\mathcal{R}_4 = \left\{ \begin{pmatrix} z_{11} & z_{12} & z_{13} & z_{14} \\ 0 & z_{22} & z_{23} & z_{24} \\ 0 & 0 & z_{33} & z_{34} \\ 0 & 0 & 0 & z_{44} \end{pmatrix} \middle| \begin{matrix} z_{ij} \in \mathbb{Z}_{16} \\ i,j = 1,2,3,4 \end{matrix} \right\} \in U_4(\mathbb{Z}_{16})$$

where $\mathbb{Z}_{16}$ is the ring of integers mod 16. The ring $\mathcal{R}_4$ is π-McCoy by *Remark C*. For any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i\chi^i, \psi(\chi) = \sum_{j=0}^{n} b_j\chi^j \in \mathcal{R}_4[\chi]$, such that $\varphi(\chi)\psi(\chi) \in \aleph(\mathcal{R}_4[\chi])$ we have that $a_i\varsigma \in \aleph(\mathcal{R}_4)$ for some $\varsigma \in \mathcal{R} \setminus \{0\}$.

Step 1: Piper chooses $\varphi(\chi) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}\chi \in \mathcal{R}_4[\chi]$ as a private key and kept it, and $\psi(\chi) = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}\chi \in \mathcal{R}_4[\chi]$ where,

$a_0 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, $a_1 = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, are the coefficients of $\varphi(\chi)$. Therefore,

$$\varphi(\chi)\psi(\chi) = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}\chi + \begin{pmatrix} 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}\chi + \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}\chi^2.$$

Now

$$(\varphi(\chi)\psi(\chi))^2 = \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} + \begin{pmatrix}0&0&0&-1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\chi + \begin{pmatrix}0&0&0&-2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\chi^2 + \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\chi^3 + \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\chi^4$$

$(\varphi(\chi)\psi(\chi))^3 = \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$, which means that

$$\varphi(\chi)\psi(\chi) = \begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} + \begin{pmatrix}0&1&-1&2\\0&0&0&-1\\0&0&0&1\\0&0&0&0\end{pmatrix}\chi + \begin{pmatrix}0&0&0&2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\chi^2 \in \aleph(\mathcal{R}_4[\chi])$$

Now, Piper chooses $\varsigma = \begin{pmatrix}0&0&1&0\\0&0&1&0\\0&0&-1&0\\0&0&0&0\end{pmatrix}$ such that, $a_i\varsigma \in \aleph(\mathcal{R}_4)$. After there, Piper sends Vali the set

$\varphi\varsigma_{coef.} = \{a_i\varsigma | 0 \le i \le m \text{ and } \varsigma \in \mathcal{R}\} = \{a_0\varsigma, a_1\varsigma\} = \left\{\begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}, \begin{pmatrix}0&0&-2&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\right\}$.

Step 2: Vali chooses randomly $r = 0$ or 1 and sends it to Piper.

Step 3: For each element of the set $\varphi\varsigma_{coef.} = \{a_i\varsigma | 0 \le i \le m \text{ and } \varsigma \in \mathcal{R}\}$ Piper found

i- $k_0 = 2 \in \mathbb{Z}^+$ such that, $(a_0\varsigma)^{k_0} = (a_0\varsigma)^2 = \begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^2 = 0$, Piper sends Vali $k_0 = 2$ to check $(a_0\varsigma)^{k_0 - r}$.

ii- $k_1 = 2 \in \mathbb{Z}^+$ such that $(a_1\varsigma)^{k_1} = (a_1\varsigma)^2 = \begin{pmatrix}0&0&-2&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^2 = 0$, Piper sends Vali $k_1 = 2$ to check $(a_1\varsigma)^{k_1 - r}$.

Step 4:

i- If $r = 0$, then Vali checks that $(a_0\varsigma)^{k_0 - r} = \begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_0 - r} = 0$ (because Vali knows that $\mathcal{R}_4$ is π-McCoy ring & $r = 0$). Hence Vali accepts the proof.

If $r = 1$, then Vali checks that $(a_0\varsigma)^{k_0 - r} = \begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_0 - r} \neq 0$ (this means that $\begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \notin \aleph(\mathcal{R}_4)$, which contradicts the fact that $\mathcal{R}_4$ is a π-McCoy ring). Hence Vali reject the proof.

ii- If $r = 0$, then Vali checks that $(a_1\varsigma)^{k_1 - r} = \begin{pmatrix}0&0&-2&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_1 - r} = 0$ (because Vali knows that $\mathcal{R}_4$ is π-McCoy ring & $r = 0$). Hence Vali accepts the proof.

If $r = 1$, it is definitely Vali checks that $(a_1\varsigma)^{k_1 - r} = \begin{pmatrix}0&0&-2&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_1 - r} \neq 0$ (this means that $\begin{pmatrix}0&0&-2&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \notin \aleph(\mathcal{R}_4)$ which contradicts the fact that $\mathcal{R}_4$ is π-McCoy ring). Hence Vali rejects the proof.

Step 5: Repeat the above steps λ times, where λ is the number of polynomials $\psi(\chi) \in \mathcal{R}[\chi]$ such that $\varphi(\chi)\psi(\chi) \in \aleph(\mathcal{R}[\chi])$. To find, λ we should first determine the degree k of $\psi(\chi)$ which should be large enough.

5. ANALYSIS OF THE π-MCCOY ZERO KNOWLEDGE PROTOCOL

In this section, we show some properties that the π-McCoy zero-knowledge protocol satisfied:

1- Confidentiality: An attacker cannot know the coefficients of the polynomial $\varphi(\chi)$ or $\psi(\chi)$ even if the set $\varphi\varsigma_{coef.} = \{a_i\varsigma | 0 \le i \le m \text{ and } \varsigma \in \mathcal{R}\}$ is exposed, confidentiality is ensured by the random selection of the polynomial $\psi(\chi)$.

2- Reciprocal Authentication: Reciprocal authentication is ensured by $k_i - r$, which is based on $a_i\varsigma \in \aleph(\mathcal{R})$ and zero-knowledge proof, which in turn is based on a π-McCoy ring.

3- Efficiency: The introduced algorithm is very effective ecause it only utilizes addition, multiplication, and exponents.

4- Secrecy: It is computationally impossible to find a_i $\forall i$ for all random $\psi(\chi)$ and hence it is infeasible to find the secret polynomial $\varphi(\chi)$.

6. CONCLUSION

Basically, a modern algebraic system has been introduced in this paper, it relies upon the algebraic framework for the π-

McCoy rings. The fact that the security of the proposed algebraic cryptographic systems has also been taken into consideration in this work, which is based on non-commutative rings to make sure that it is impossible to have the nonlinear systems solved and discover the general privet key factor typically from the provided public one. Even in the case where it is theoretically possible, it is then computationally unfeasible. Moreover, the proposed cryptosystem regards a new promising algebraic method depending on rings.

REFERENCES

1. Sarairah, S., Al-Sarairah, J., Al-Sbou, Y. and Sarairah, M., "A Hybrid Text-Image Security Technique", *Journal of Theoretical and Applied Information Technology*, **96**(09): 2414- 2422(2018).
2. Kumar, A., "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", *Journal of Computer Engineering*, **18**(1): 39-43(2016).
3. Rachmawati, D., Pratiwi, F. and Hardi, S. M., "Improving Audio Files Security By Using Rivest Shamir Adleman Algorithm and Modified Least Significant Bit on the Red Channel Method", *Journal of Theoretical and Applied Information Technology*, **97**(11): 3003-3013(2019).
4. Goldwasser, S., Micali, S. and Rckoff, C., "The Knowledge Complexity of Interactive Proof Systems", *SIAM Journal of Computing*, **18**: 186-208(1989).
5. Goldreich, O., Micali, S. and Wigderson, A., "Proofs that yield nothing but their validity or All Languages in NP Have Zero-Knowledge Proof Systems", *Journal of the ACM*, **38**(1): 691-729(1991).
6. Fiat, A., and Shamir, A., "How to Prove Yourself: Practical Solutions to Identification and Signature Problem", *Crypto 86*, **263**:, 186-189(1987).
7. Micali, S., and Shamir, A., "An Improvement of the Fiat-Shamir Identification and Signature Scheme", *Crypto 88*, **403**: 244-250(1988).
8. Fiege, U., Fiat, A. and Shamir, A., "Zero Knowledge Proof of Identity", *Proc. of 19th STOC*, 210-217 (1987).
9. Guillou, L.C and Quisquater, J.J, "A Paradoxical Identity-Based Signature Resulting From Zero Knowledge", *Crypto 88*, **403**: 216-231(1988).
10. Goldwasser, S. and Kalai, Y. T. , "On the (In)security of the Fiat-Shamir Paradigm", *FOCS*, **38**(1): 691-729(1991).
11. Courtois, N. T., "Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank", *Asiacryp*, **2248**: 402-411(2001).
12. Wolf, C., "Zero-Knowledge and Multivariate Quadratic Equations*", Workshop on Coding and Cryptography*, (2004).
13. Goldreich, O. and Oren, Y., "Definitions and Properties of Zero-Knowledge Proof Systems", *Journal of Cryptology*, **7**(1): 1-32(1994).
14. Rachmawati, D., and Budiman, M. A., "Using The RSA As As an Asymmetric Non-Public Key Encryption Algorithm in The Shamir Three-pass Protocol", *Journal of Theoretical and Applied Information Technology*, **96**(17): 5663- 5673(2018).
15. Gaikwad, V. S. D. , "An Analysis upon Basic Fundamental Application of Ring Theory", *Journal of Advances and Scholarly Researches in Allied Education*, **13**(2): . 217-223(2017).
16. Nielsen, P. P., "Semi-commutativity and the McCoy condition," *J. Algebra*, **298**(1): 134–141(2006).
17. Jeon, Y. C., Kim, H. K. , Kim, N. K. , Kwak, T. K., Lee, Y., and Yeo, D. E., "On A Generalization of The McCoy Condition," *J. Korean Math. Soc.*, **47**(6): 1269–1282(2010).
18. Abduldaim, A. M. and Chen, S., "α -Skew π -McCoy Rings," *J. App. Math.*, **2013**: 7 pages(2013).
19. Abduldaim, A. M. and Abidali, R. M., "π-Armendariz rings and related concepts," *Baghdad Science Journal*, **13**(4): 853-861(2016).
20. Abduldaim, A. M. and Ajaj, A. M., "Examples of α-skew π-Armendariz rings*," Iraqi Journal of Science (Baghdad University)*, **58**(1C): 482-489(2017).
21. Abduldaim, A.M. and Ajaj, A.M., "A new paradigm of the zero-knowledge authentication protocol based π-Armendariz rings," *in Proc. IEEE International Conference on New Trends in Information & Communications Technology Applications, Baghdad*, 112-117(2017).
22. Abduldaim, A. M., "Weak Armendariz Zero Knowledge Cryptosystem," *Journal of Al-Qadisiyah for Computer Science and Mathematics*, **9**(2): 1-6(2017).