α-SKEW π-ARMENDARIZ RING FOR IMPROVING SECURE ALGEBRAIC ZERO KNOWLEDGE CRYPTOSYSTEM

[1]AREEJ M. ABDULDAIM

[1]University of Technology, Applied Sciences Department, Mathematics and Computer Applications

Baghdad, Iraq

E-mail: [1]areejmussab@gmail.com

ABSTRACT

A zero knowledge proof is a form of an authentication technique that gives no data more than the authenticity allowed to mark a being. Without transit any data about the password to the other trusted tip, the password must be known by the first party and he must prove that. The proposed scheme is considered as a method for preventing a password over a particular network that is capable of being detected by a third party. Factorization and discrete logarithm problems (which are hard mathematical problems) are adopted in several public-key cryptosystems. Nowadays, several cryptographic protocols have been improved with respect to noncommutative algebraic frameworks like authentication and encryption-decryption methods. They are proven to be efficient in corresponding to their commutative case. Under this study, proof on a novel zero knowledge is based typically on $\boldsymbol{\alpha}$-skew $\boldsymbol{\pi}$-Armendariz rings is proposed. The algebraic structure ($\boldsymbol{\alpha}$-skew $\boldsymbol{\pi}$-Armendariz ring) is the heart of this method. Unlike methods raised previously for the zero knowledge proof, this work is searching to construct an algebraic scope of the zero knowledge proof depending upon the constraint in the definition of the mentioned ring.

Keywords: *α-Skew π-Armendariz Ring, Zero Knowledge Proof, Algebraic Structure, Authentication, Cryptosystem.*

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 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 element is 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.

In this paper, associative rings are considered with identity unless otherwise mentioned. Authentication protocols that count on some algebraic structures attracted the interest of a lot of authors so many modern authentication schemes have been introduced on groups, rings and algebras such as; quaternion algebra and endomorphism rings as in [16].

Let $\mathfrak{R}$ be considered a ring, which is the set of the entire polynomials in the indeterminate χ with regard to an endomorphism α of $\mathfrak{R}$ is said to be the skew polynomial ring and expressed as $\mathfrak{R}[\chi,\alpha]$, where $\chi r = \alpha(r)\chi$ for all $r \in R$. The prime radical of $\mathfrak{R}$ is denoted by $P(\mathfrak{R})$ (the intersection of all prime ideals) and $\aleph(\mathfrak{R})$ is denoted the set of all nilpotent elements in $\mathfrak{R}$. Finally, $\mathbb{Z}$ represents the ring of integers.

A ring $\mathfrak{R}$ is called reduced if the only nilpotent element in $\mathfrak{R}$ is zero. In other words, \r $^2 = 0$ implies $r = 0$ for any $r \in R$ [17]. Due to Rege and Chhawchharia in 1997 [18], a ring R is called an Armendariz if for any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i\chi$, $\psi(\chi) = \sum_{j=0}^{n} b_j\chi$ in $\mathfrak{R}[\chi]$, such that; $\varphi(\chi)\psi(\chi) = 0$, then $a_i b_j = 0$ for all i, j. Also, it is showed in [18] that each reduced ring is Armendariz. Hong et al. [19] introduced the notion of Armendariz rings as a generalization to the concept of α-skew Armendariz. Thereafter, the notion of α-skew π-Armendariz rings is introduced to generalize the notion of α-skew Armendariz rings [20]. A ring $\mathfrak{R}$ is denoted by α-skew π-Armendariz if for every two polynomials $\vartheta(\chi) = \sum_{i=0}^{m} a_i\chi^i$, $\phi(\chi) = \sum_{j=0}^{n} b_j\chi^j \in \mathfrak{R}[\chi,\alpha]$, such that, $\vartheta(\chi)\phi(\chi) \in \aleph(\mathfrak{R}[\chi,\alpha])$ then $a_i\alpha^i(b_j) \in \aleph(\mathfrak{R})$ for each i, j.

The remaining parts of this study are ordered as the following. Section II is dedicated entirely to give mathematical preliminaries of the notion of α-skew π-Armendariz rings. Section III summarizes some reviews and related works of the principal zero-knowledge protocol in general. Section IV introduced the algebraic structure for zero knowledge Proof and divides into two subsections; in the first one a detailed algorithm of the algebraic structure for zero-knowledge proof with the underlying α-skew π-Armendariz rings is given, and in the second subsection the zero knowledgeness of the algebraic zero knowledge proof is investigated with various analysis. The discussion and the conclusion are given in Section V and Section VI respectively.

2. THE ALGEBRAIC STRUCTURE OF α-SKEW π-ARMENDARIZ RING

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

2.1 Definition:

A ring $\mathfrak{R}$ is α-skew π-Armendariz if for $\vartheta(\chi) = \sum_{i=0}^{m} a_i\chi^i$, $\phi(\chi) = \sum_{j=0}^{n} b_j\chi^j \in \mathfrak{R}[\chi,\alpha]$ such that $\vartheta(\chi)\phi(\chi) \in \aleph(\mathfrak{R}[\chi,\alpha])$ implies $a_i\alpha^i(b_j) \in \aleph(\mathfrak{R})$ for each i, j.

Let $\mathfrak{R}$ be a ring. For any integer $n \geq 2$, consider $\mathcal{M}_n(\mathfrak{R})$ be the $n \times n$ matrix ring and $T_n(\mathfrak{R})$ be the $n \times n$ triangular matrix ring primarily over a ring $\mathfrak{R}$. Let $\alpha: \mathfrak{R} \to \mathfrak{R}$ be a ring endomorphism. For any $A = (a_{i,j}) \in \mathcal{M}_n(\mathfrak{R})$, we define $\bar{\alpha}: \mathcal{M}_n(\mathfrak{R}) \to \mathcal{M}_n(\mathfrak{R})$ by $\bar{\alpha}\left((a_{i,j})_{n\times n}\right) = (\alpha(a_{i,j}))_{n\times n}$, and hence $\bar{\alpha}$ is a ring endomorphism of the particular ring $\mathcal{M}_n(\mathfrak{R})$.

Therefore, the following theorem specifies an equivalent property of the α-skew π-Armendariz notion:

2.2 Theorem [19, Theorem 2.2.1]:

Let α be an endomorphism of the ring $\mathfrak{R}$ and $\bar{\alpha}$ be a ring endomorphism of $\mathcal{M}_n(\mathfrak{R})$. The conditions below are equivalent in particular:

1) $\mathfrak{R}$ is an α-skew π-Armendariz ring.
2) For any positive integer n, $T_n(\mathfrak{R})$ is an $\bar{\alpha}$-skew π-Armendariz ring.

2.3 Example:

Let $\mathfrak{R}$ be a reduced ring,

$$\mathcal{M}_4 = \left\{ \left. \begin{pmatrix} a & a_{12} & a_{13} & a_{14} \\ 0 & a & a_{23} & a_{24} \\ 0 & 0 & a & a_{34} \\ 0 & 0 & 0 & a \end{pmatrix} \right| a, a_{ij} \in \mathfrak{R} \right\}.$$

Then $\mathcal{M}_4$ is $\bar{\alpha}$-skew π-Armendariz by Theorem 2.2.

2.4 Example:

Let $\mathfrak{R}$ be a ring and $\mathcal{M}_2(\mathfrak{R})$ 2×2 matrix ring over $\mathfrak{R}$ with usual matrix operations. Let $\mathcal{F}$ be a ring such that

$$\mathcal{F} = \left\{\begin{pmatrix} \mathcal{A} & \mathcal{B} \\ 0 & \mathcal{C} \end{pmatrix} | \mathcal{A},\mathcal{B},\mathcal{C}\in \mathcal{M}_2(\Re)\right\}.$$

Define the endomorphism $\alpha:\mathcal{F} \to \mathcal{F}$ by

$$\alpha\left(\begin{pmatrix} \mathcal{A} & \mathcal{B} \\ 0 & \mathcal{C} \end{pmatrix}\right) = \begin{pmatrix} \mathcal{A} & -\mathcal{B} \\ 0 & \mathcal{C} \end{pmatrix} \text{ for any } \begin{pmatrix} \mathcal{A} & \mathcal{B} \\ 0 & \mathcal{C} \end{pmatrix} \in \mathcal{F}.$$

The ring $\mathcal{F}$ is not α-skew π-Armendariz; because if $\vartheta(\chi)$ and $\phi(\chi) \in \mathcal{F}[\chi;\alpha]$ such that

$$\vartheta(\chi) = \begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{pmatrix} + \begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \end{pmatrix}\chi,$$

$$\phi(\chi) = \begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \end{pmatrix} + \begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{pmatrix}\chi$$

then

$$\vartheta(\chi)\phi(\chi) = \begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{pmatrix},$$

which means that $\vartheta(\chi)\phi(\chi) = 0 \in \aleph(\mathcal{F}[\chi;\alpha])$.
Now, we claim that $a_1\alpha(b_0) \notin \aleph(\mathcal{F})$

$$\left[\begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \end{pmatrix} \alpha\left(\begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \end{pmatrix}\right)\right]^n$$

$$= \left[\begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \end{pmatrix}\begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \end{pmatrix}\right]^n$$

$$= \begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} \end{pmatrix}^n$$

The latest term will never be zero whatever n is.
Therefore,

$$\begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \end{pmatrix} \alpha\left(\begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \end{pmatrix}\right) \notin \aleph(\mathcal{F})$$

which implies that $\mathcal{F}$ is not α-skew π-Armendariz ring.

2.5 Example:

Let $\Re = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, where $\mathbb{Z}_2$ is the integers modulo 2's ring. Let $\alpha: \Re \to \Re$ be the endomorphism α that determined by $\alpha((a,b)) = (b,a)$. Let $\vartheta(\chi)$, $\phi(\chi) \in \Re[\chi,\alpha]$, such that,

$$\vartheta(\chi) = (0,1) - (0,1)\chi,$$

and

$$\phi(\chi) = (1,0) + (0,1)\chi$$

this gives

$$\vartheta(\chi)\phi(\chi) = ((0,1)(1,0) + (0,1)(0,1)\chi - (0,1)x(1,0) - (0,1)\chi(0,1)\chi)$$
$$= ((0,0) + (0,1)\chi - (0,1)(0,1)\chi - (0,1)(1,0)\chi^2)$$
$$= ((0,0) + (0,1)\chi - (0,1)\chi - (0,0)\chi^2)$$
$$= 0 \in \aleph(\Re[\chi,\alpha]),$$

But

$$(0,1)(0,1) = (0,1) \notin \aleph(\Re).$$

So $\Re$ is not α-skew π-Armendariz rings.

3. THE PIONEER ZERO KNOWLEDGE PROTOCOL

Wide investigations regarding ZKP have been studied. There are proofs usually viewed (especially by scientists) based on a static mathematical object [21]:

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 perpetrate 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 prover 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. ALGEBRAIC STRUCTURE FOR ZERO KNOWLEDGE PROOF WITH THE UNDERLYING α-SKEW π-ARMENDARIZ RING

4.1 Algorithm

The identification scheme includes initial setup, key generation, and authentication. The algebraic ZKP algorithm includes the following fundamental proceedings: considering that V is the verifier and P is the prover.

P the prover would like to show V the verifier that a secret polynomial $\vartheta(\chi) \in \mathfrak{R}[\chi,\alpha]$ has coefficients belong to an α-skew π-Armendariz ring $\mathfrak{R}$. The secret polynomial is protected by P and will never be declared. Each of P and V knows the ring $\mathfrak{R}$, and it is α-skew π-Armendariz.

For every two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i\chi^i$, $\psi(\chi) = \sum_{j=0}^{n} b_j\chi^j \in \mathfrak{R}[\chi,\alpha]$, P calculates the multiplication of $\varphi(\chi)$ and $\psi(\chi)$ such that, $\varphi(\chi)\psi(\chi) \in \aleph(\mathfrak{R}[\chi,\alpha])$ and publishes her public key, the set $P_{coef.} = \{a_i\alpha^i(b_j) | 0 \le i \le m \text{ and } 0 \le j \le n\}$ in order to make V knows that every element in the set $P_{coef.}$ is nilpotent such that the secret polynomial $\varphi(\chi)$ is not used as P’s private key. This polynomial is protected by the P and will not ever be declared.

Step 1: P selects an endomorphism $\alpha: \mathfrak{R} \to \mathfrak{R}$ and $\varphi(\chi)$, $\psi(\chi)$ $\in \mathfrak{R}[\chi,\alpha]$ such that, $\varphi(\chi)\psi(\chi) \in \aleph(\mathfrak{R}[\chi,\alpha])$, where

$$\begin{aligned}\varphi(\chi)\psi(\chi) = {} & a_0b_0 + a_0b_1\chi + a_0b_2\chi^2 + a_0b_3\chi^3 \\ & + \cdots + a_0b_n\chi^n \\ & +a_1\alpha(b_0)\chi + a_1\alpha^1(b_1)\chi^2 + a_1\alpha^1(b_2)\chi^3 \\ & + a_1\alpha^1(b_3)\chi^4 + \cdots \\ & + a_1\alpha^1(b_n)\chi^{n+1} \\ & +a_2\alpha^2(b_0)\chi^2 + a_2\alpha^2(b_1)\chi^2\chi + a_2\alpha^2(b_2)\chi^2\chi^2 \\ & + a_2\alpha^2(b_3)\chi^2\chi^3 + \cdots \\ & + a_2\alpha^2(b_n)\chi^2\chi^n \\ & +a_3\alpha^3(b_0)\chi^3 + a_3\alpha^3(b_1)\chi^3\chi + a_3\alpha^3(b_2)\chi^3\chi^2 \\ & + a_3\alpha^3(b_3)\chi^3\chi^3 + \cdots \\ & + a_3\alpha^3(b_n)\chi^3\chi^n \\ & +\cdots \\ & +a_m\alpha^m(b_0)\chi^m + a_m\alpha^m(b_1)\chi^m\chi \\ & + a_m\alpha^m(b_2)\chi^m\chi^2 \\ & + a_m\alpha^m(b_3)\chi^m\chi^3 + \cdots \\ & + a_m\alpha^m(b_n)\chi^m\chi^n\end{aligned}$$

and V transmits the set

$$P_{coef.} = \{a_i\alpha^i(b_j) | 0 \le i \le m \text{ and } 0 \le j \le n\}.$$

Step 2: V selects at random $r = 0$ or 1 and sends it for P.

Step 3: To every i, j, P obtains $k_{ij} \in \mathbb{Z}^+$, such that, $(a_i\alpha^i(b_j))^{k_{ij}} = 0$, k_{ij} relying upon i, j and send V $k_{ij} - r$ as a power of $a_i\alpha^i(b_j)$.

Step 4: V confirms:

1- If $r = 0$, then V confirms that $(a_i\alpha^i(b_j))^{k_{ij}-r} = 0$ (the reason is V knows that $\mathfrak{R}$ is α-skew π-Armendariz ring $\& r = 0$) which means that $a_i\alpha^i(b_j)$ is a nilpotent element.
2- If $r = 1$, it is definitely V confirms that $(a_i\alpha^i(b_j))^{k_{ij}-r} \neq 0$ (this means that $a_ib_j \notin \aleph(\mathfrak{R})$ which represents a contradiction the fact that A is α-skew π-Armendariz ring).

Step 5: Iterate the previous proceedings ρ times, where ρ is the polynomials number of $\psi(\chi) \in \mathfrak{R}[\chi,\alpha]$, such that, $\varphi(\chi)\psi(\chi) \in \aleph(\mathfrak{R}[\chi,\alpha])$. For obtaining ρ, the degree of $\psi(\chi)$, k should be specified and it must be large enough.

4.2 Example

Let

$$\mathfrak{R}_4 = \left\{ \begin{pmatrix} r & r_{12} & r_{13} & r_{14} \\ 0 & r & r_{23} & r_{24} \\ 0 & 0 & r & r_{34} \\ 0 & 0 & 0 & r \end{pmatrix} \middle| r, r_{i,j} \in \mathbb{Z} \,\&\, i,j = 1,2,3,4 \right\} \in \mathcal{M}_4(\mathbb{Z})$$

where $\mathbb{Z}$ is the set of integers. Hence $\mathfrak{R}_4$ is $\bar{\alpha}$-skew π-Armendariz by Theorem 3.2. For any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i\chi^i, \psi(\chi) = \sum_{j=0}^{n} b_j\chi^j \in \mathfrak{R}_4[\chi,\bar{\alpha}]$, such that $\varphi(\chi)\psi(\chi) \in \aleph(\mathfrak{R}_4[\chi,\bar{\alpha}])$ we have that $a_i\bar{\alpha}^i(b_j) \in \aleph(\mathfrak{R}_4)$.

Step 1: P chooses:

1- $\alpha: \mathfrak{R}_4 \to \mathfrak{R}_4$ that is defined by $\alpha(r) = r$. Then $\bar{\alpha}: \mathcal{M}_4(\mathbb{Z}) \to \mathcal{M}_4(\mathbb{Z})$ becomes

$$\bar{\alpha}\left(\begin{pmatrix} r & r_{12} & r_{13} & r_{14} \\ 0 & r & r_{23} & r_{24} \\ 0 & 0 & r & r_{34} \\ 0 & 0 & 0 & r \end{pmatrix}\right) = \left(\begin{pmatrix} \alpha(r) & \alpha(r_{12}) & \alpha(r_{13}) & \alpha(r_{14}) \\ 0 & \alpha(r) & \alpha(r_{23}) & \alpha(r_{24}) \\ 0 & 0 & \alpha(r) & \alpha(r_{34}) \\ 0 & 0 & 0 & \alpha(r) \end{pmatrix}\right)$$

2- $\varphi(\chi) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}\chi \in \mathfrak{R}_4[\chi, \bar{\alpha}]$

($\varphi(\chi)$ represents the secret)

3- $\psi(\chi) = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}\chi \in \mathfrak{R}_4[\chi, \bar{\alpha}]$

Thus

$$a_0 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \ a_1 = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$b_0 = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad b_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

are the coefficients of $\varphi(\chi)$ and $\psi(\chi)$. 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,

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

which means that

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

$$+ \begin{pmatrix} 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}\chi^2$$

$\in \aleph(\mathfrak{R}_4[\chi, \bar{\alpha}])$

then P sends V the set $P_{coef.} = \{a_i\bar{\alpha}^i(b_j) | 0 \leq i \leq 1 \text{ and } 0 \leq j \leq 1\} =$

$\{a_0b_0, a_0b_1, a_1b_0, a_1b_1\} =$

$$\left\{\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}\right\}$$

Step 2: V selects at random $r = 0$ or 1 and transmits it to P.

Step 3: To every element belongs to the following set: $P_{coef.} = \{a_i\bar{\alpha}^i(b_j) | 0 \leq i \leq 1 \text{ and } 0 \leq j \leq 1\}$, P find

i- $k_{00} = 2 \in \mathbb{Z}^+$, such that,

$$(a_0\bar{\alpha}^0(b_0))^{k_{00}} = (a_0b_0)^2 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^2 = 0,$$

P transmits V $k_{00} = 2$ to confirm $(a_0\bar{\alpha}^0(b_0))^{k_{00}-r}$.

ii- $k_{01} = 2 \in \mathbb{Z}^+$ such that,

$$(a_0\bar{\alpha}^0(b_1))^{k_{01}} = (a_0b_1)^2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^2 = 0,$$

P transmits V $k_{01} = 2$ to confirm $(a_0\bar{\alpha}^0(b_1))^{k_{01}-r}$.

iii- $k_{10} = 3 \in \mathbb{Z}^+$ such that,

$$(a_1\bar{\alpha}^1(b_0))^{k_{10}} = (a_1b_0)^3 = \begin{pmatrix} 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}^3 = 0,$$

P transmits V $k_{10} = 3$ to confirm $(a_1\bar{\alpha}^1(b_0))^{k_{10}-r}$.

iv- $k_{11} = 2 \in \mathbb{Z}^+$ such that,

$$(a_1\bar{\alpha}^1(b_1))^{k_{11}} = (a_1b_1)^2 = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^2 = 0,$$

P transmits Vic $k_{10} = 3$ to confirm $(a_1\bar{\alpha}^1(b_1))^{k_{10}-r}$.

Step 4:

i- If $r = 0$, so V confirms that

$$(a_0\bar{\alpha}^0(b_0))^{k_{00}-r} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^{k_{00}-r} = 0$$

(the reason is V knows that $\mathfrak{R}_4$ is $\bar{\alpha}$-skew π-Armendariz ring & $r = 0$).

If $r = 1$, so V confirms that

$$(a_0\bar{\alpha}^0(b_0))^{k_{00}-r} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^{k_{00}-r} \neq 0$$

(This means that $\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \notin \aleph(\mathfrak{R}_4)$ which represents a contradiction to the fact that $\mathfrak{R}_4$ is $\bar{\alpha}$-skew π-Armendariz ring).

ii- If $r = 0$, so V confirms that

$$(a_0\bar{\alpha}^0(b_1))^{k_{01}-r} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^{k_{01}-r} = 0$$

(the reason is V knows that $\mathfrak{R}_4$ is $\bar{\alpha}$-skew π-Armendariz ring & $r = 0$).

If $r = 1$, so V confirms that

$$(a_0\bar{\alpha}^0(b_1))^{k_{00}-r} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^{k_{01}-r} \neq 0$$

(This means that $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \notin \aleph(\mathfrak{R}_4)$ which represents a contradiction to the fact that $\mathfrak{R}_4$ is $\bar{\alpha}$-skew π-Armendariz ring).

iii- If $r = 0$, so V confirms that

$$(a_1\bar{\alpha}^1(b_0))^{k_{10}-r} = \begin{pmatrix} 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}^{k_{10}-r} = 0$$

(the reason is V knows that $\mathfrak{R}_4$ is $\bar{\alpha}$-skew π-Armendariz ring & $r = 0$).

If $r = 1$, so V confirms that

$$(a_1\bar{\alpha}^1(b_0))^{k_{10}-r} = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^{k_{10}-r} \neq 0$$

(This means that $\begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \notin \aleph(\mathfrak{R}_4)$ which represents a contradiction to the fact that $\mathfrak{R}_4$ $\bar{\alpha}$-skew is π-Armendariz ring).

iv- If $r = 0$, so Vic confirms that

$$(a_1\bar{\alpha}^1(b_1))^{k_{11}-r} = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^{k_{11}-r} = 0$$

(the reason is V knows that $\mathfrak{R}_4$ is $\bar{\alpha}$-skew π-Armendariz ring & $r = 0$).

If $r = 1$, so V confirms that

$$(a_1\bar{\alpha}^1(b_1))^{k_{11}-r} = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}^{k_{11}-r} \neq 0$$

(This means that $\begin{pmatrix}0&0&0&2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \notin \aleph(\Re_4)$ which represents a contradiction to the fact that $\Re_4$ is $\bar{\alpha}$-skew π-Armendariz ring).

Step 5: Iterate the previous proceedings ρ times, where μ is the polynomials number $\psi(\chi) \in \Re[\chi, \bar{\alpha}]$, such that, $\varphi(\chi)\psi(\chi) \in \aleph(\Re[\chi, \bar{\alpha}])$. To obtain ρ, the degree of $\psi(\chi)$, k should be specified and it must be large enough.

Finite fields are the essence of the public communal encryption schemes. Powerless encryption features resulted from a non-prime modular number, so zero-divisors becomes with order less than others, for this reason, finite fields always required.

4.3 The Zero Knowledge Property of the Algebraic Cryptosystem

Under this section, the proof of knowledge scheme is then based on α-skew π-Armendariz rings are detailed. Generally, Zero Knowledge Proofs are typically not considered as proofs existing in the mathematical sense of its term, due to the fact that there are a few little probabilities (known as the soundness error) that a particular cheating prover will be capable of convincing the verifier of a particular false statement. In any case, some standard techniques exist to increment the soundness error to any type of arbitrarily small value. Therefore, three different core requirements exist in the zero-knowledge proofs as shown below:

Completeness: The verifier can be convinced by a prover, this is true statements
Apparently, our protocol is simply complete. If $\vartheta(\chi) = \sum_{i=0}^{m} a_i \chi^i$, $\phi(\chi) = \sum_{j=0}^{n} b_j \chi^j \in \Re[\chi, \alpha]$, such that $\vartheta(\chi)\phi(\chi) \in \aleph(\Re[\chi, \alpha])$, then $a_i \alpha^i(b_j) \in \aleph(\Re)$. Furthermore, the prover who knows the secret polynomial $\vartheta(\chi)$ can easily check if each $a_i \alpha^i(b_j)$ is nilpotent or not. So, the prover has the capacity to provide an answer to the two possible challenges, $r \in \{0,1\}$ having 100% a probability to convince the verifier in particular.

Soundness: A prover is capable of convincing the verifier (regardless of a case whereby the prover tends to cheats and then deviates strongly from the protocol), this is false statements.
Meanwhile, our protocol is considered sound based on the fact that 50 percent privilege of getting a cheating prover to exist. If $\vartheta(\chi)\phi(\chi) \in \aleph(\Re[\chi, \alpha])$, such that $a_i \alpha^i(b_j) \notin \aleph(\Re)$, then $\Re$ cannot be a α-skew π-Armendariz ring. So, if the verifier picks r, such that, $a_i \alpha^i(b_j) \notin \aleph(\Re)$, at such point, the prover is unable to proffer solutions to the challenge. For our opportunity of getting a tricking prover to be increased, the response and challenge protocol can be repeated. The protocol to carry out n repetitions can be modified for the particular $\vartheta(\chi)$ but different $\phi(\chi)$. Under individual interaction, there is a 50 percent chance to catch the cheating prover, thus, a decrease in the entire risk of cheating occurs to about 2^{-n}.

Zero Knowledge Property: There is nothing for the verifier to learn from the interaction aside if the statement is considered true. In a case whereby the statement is proven true, there will be no cheating verifier to learn anything, but the truth of the statement. The answers of Peggy cannot uncover the original secret polynomial $\varphi(\chi)$. Each round, Vic will learn only the set $P_{coef.} = \{a_i \alpha^i(b_j) | 0 \le i \le m \; and \; 0 \le j \le n\}$ with each element of $P_{coef.}$ is nilpotent or not. He needs all a_i to discover the secret polynomial, therefore, the information stays unknown as far as Peggy has the ability to choose distinctly $\psi(\chi)$ and generate $a_i \alpha^i(b_j)$ at each round. In a case whereby Peggy is unaware of a secret polynomial $\varphi(\chi)$, however, in a way, is aware in advance what Vic would inquire to see an individual round, at such point, she can probably cheat. A typical example is if Peggy was earlier informed that Vic would ask if she could view the secret polynomial $\varphi(\chi)$, then she could choose distinctly $\psi(\chi)$ and generate $a_i \alpha^i(b_j)$ specifically for an unrelated polynomial. In the same vein, if Peggy has been earlier informed that Vic would ask to view the main isomorphism, at that point she can probably simply choose distinctly $\psi(\chi)$ and generate the set $P_{coef.} = \{a_i \alpha^i(b_j) | 0 \le i \le m \; and \; 0 \le j \le n\}$. Vic can probably stimulate the entire protocol on his own (without the help of Peggy) since he is aware of what he intends to see. Therefore, Vic gets no information regarding the secret polynomial $\varphi(\chi)$ from the information revealed in each round.

5. DISCUSSION

The proposed ZKP based on α-skew π-Armendariz rings comprises of two different parties, including Peggy and Vic. Peggy attempts to confirm her identity to Vic without informing her of any secret data $\varphi(\chi)$. So she obtains a public key $\varphi(\chi)\psi(\chi) \in \Re[\chi,\alpha]$, selecting the polynomial $\psi(\chi)$ and transmits the set $P_{coef.} = \{a_i\alpha^i(b_j)|0 \le i \le m \; and \; 0 \le j \le n\}$ to Vic. In parallel, Vic does the same steps and transmits his public key $r = 0$ or 1 to Peggy. Next, Peggy utilizes the α-skew π-Armendariz feature of $\Re$ and her private key $\varphi(\chi)$ to calculate the set $P_{coef.} = \{a_i\alpha^i(b_j)|0 \le i \le m \; and \; 0 \le j \le n\}$, and transmits it to Vic. To confirm Peggy's key, Vic requires to calculate $(a_i\alpha^i(b_j))^{k_{ij}-r}$. If $(a_i\alpha^i(b_j))^{k_{ij}-r}$=0, so Vic has the ability to convince that Peggy is aware of the secret, while the authentication procedure is succeeded. Attempting to obtain the private keys, this requires to obtain the matrices whose multiplication is specified, which is arithmetically not possible. This will eliminate attacks against private key amounts. In a case whereby the number of bits is n, at that point, there are about 2^n possibilities for each $a_i\alpha^i(b_j)$ and n values. Under such circumstances, when the length of these keys is very long, then the despotic force attack would not work.

6. COMPARISON

According to the structure of the Algebraic zero knowledge Protocol, three properties are adopted for comparison: First: Strength of the protocol, Second: Security of the protocol, Third: Quickness of the protocol. Table 1 describes a comparison of the proposed Algebraic Zero Knowledge protocol with some of the previous protocols.

Zero Knowledge protocol	Strength	Security	Quickness
Fiat –Shamir	Integer factorization	Not secure	Lower
Guillou-Integer	Integer factorization	Not secure	Low
Fiege-Fiat-Shamir	Integer factorization	Not secure	Low
Schnorr	Discrete logarithm problem	Secure	Fast
Algebraic Zero Knowledge	α- skew π-McCoy rings	Secure	Fast

7. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Basically, a modern algebraic system has been introduced in this paper, it relies upon the algebraic framework for the α-skew π-Armendariz rings. In addition, the achievements of this work are to show and prove that a complete zero knowledge cryptosystem has been built successfully based on the new mathematical notion α- skew π-McCoy. This cryptosystem will be regarded as an improvement depending on the increase of its security using the new type of rings.

The fact that the security of the proposed algebraic cryptographic systems is also taken into consideration in this work, which based on noncommutative 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.

These kinds of cryptosystems open the way to future research algebraic directions of an arithmetic nature whose effect is effective when finite fields are adopted as the basic rings. Many related and closed connotations to α-skew π-Armendariz rings attracted the attention of many authors, some of them are the concepts of McCoy ring, π-McCoy rings and α- skew π-McCoy rings [21].

REFERENCES:

[1] S. Sarairah, J. Al-Sarairah, Y. Al-Sbou, and M. Sarairah, "A Hybrid Text-Image Security Technique", *Journal of Theoretical and Applied Information Technology*, Vol.96, No 09, 2018, p. 2414- 2422.

[2] A. Kumar, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", *Journal of Computer Engineering*, vol. 18, no. 1, 2016, p. 39-43.

[3] D. Rachmawati, F. Pratiwi, and S. M. Hardi, "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*, Vol.97. No 11, 2019,p. 3003-3013.

[4] S. Goldwasser, S. Micali, and C.Rckoff, "The Knowledge Complexity of Interactive Proof Systems", *SIAM Journal of Computing*, vol. 18, 1989, pp.186-208.

[5] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or All Languages in NP Have Zero-Knowledge Proof Systems", *Journal of the ACM*, Vol 38, No. 1, 1991, pp. 691-729.

[6] A. Fiat, and A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problem", *Crypto 86*, vol. 263, 1987, pp.186-189.

[7] S. Micali, and A. Shamir, "An Improvement of the Fiat-Shamir Identification and Signature Scheme", *Crypto 88*, vol. 403,1988, pp.244-250.

[8] U. Fiege, A. Fiat, and A. Shamir, "Zero Knowledge Proof of Identity", *Proc. of 19th STOC*, 1987, pp. 210-217.

[9] L.C Guillou, and J.J Quisquater, "A Paradoxical Identity-Based Signature Resulting From Zero Knowledge", *Crypto 88*, vol.403, 1988., pp. 216-231

[10] S. Goldwasser, and Y. T. Kalai, "On the (In)security of the Fiat-Shamir Paradigm", *FOCS*, vol. 38, no. 1, 1991, pp. 691-729.

[11] N. T. Courtois, "Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank", *Asiacryp*, vol. 2248, 2001, pp. 402-411.

[12] C. Wolf, "Zero-Knowledge and Multivariate Quadratic Equations", *Workshop on Coding and Cryptography*, 2004.

[13] O. Goldreich and Y. Oren, "Definitions and Properties of Zero-Knowledge Proof Systems", *Journal of Cryptology*, vol. 7, no. 1, 1994, pp. 1-32.

[14] D. Rachmawati, and M. A. Budiman, "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*, Vol.96. No 17, 2018, p. 5663- 5673.

[15] V. S. D. Gaikwad, "An Analysis upon Basic Fundamental Application of Ring Theory", *Journal of Advances and Scholarly Researches in Allied Education,* Vol. 13, No. 2, 2017, p. 217-223.

[16] M. R. Valluri, "Authentication Schemes Using Polynomials Over Non-Commutative Rings", *International Journal on Cryptography and Information Security*, vol. 2, no. 4, 2012, p. 51-58.

[17] E. Armendariz, "A note on extensions of Baer and P.P. –rings", *Journal of Austral. Math. Soc*, vol. 18, 1974, pp. 470-473.

[18] M.B. Rege, and S. Chhawchharia, "Armendariz Rings", *Proc. Japan Acad. (Ser. A)*, vol. 73, 1997, pp. 14-17.

[19] C. Y. Hong, N. K. Kim and T. K. Kwak, "On Skew Armendariz Rings", *Communications in Algebra*, vol. 31, no. 1, 2003, pp. 103-122.

[20] A. M. Abduldaim and A. M. Ajaj, "A new paradigm of the zero-knowledge authentication protocol basedπ-Armendariz rings," *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, Baghdad, 2017, pp. 97-104.

[21] A. M. Abduldaim, and S. Chen, "α -Skew π -McCoy Rings", *J. App. Math.*, vol.2013, (Article ID 309392) , 2013, 7 pages.