International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:11, No:9, 2017

Generalized π-Armendariz Authentication Cryptosystem

Areej M. Abduldaim, Nadia M. G. Al-Saidi

Abstract**—**Algebra is one of the important fields of mathematics. It concerns with the study and manipulation of mathematical symbols. It also concerns with the study of abstractions such as groups, rings, and fields. Due to the development of these abstractions, it is extended to consider other structures, such as vectors, matrices, and polynomials, which are non-numerical objects. Computer algebra is the implementation of algebraic methods as algorithms and computer programs. Recently, many algebraic cryptosystem protocols are based on non-commutative algebraic structures, such as authentication, key exchange, and encryption-decryption processes are adopted. Cryptography is the science that aimed at sending the information through public channels in such a way that only an authorized recipient can read it. Ring theory is the most attractive category of algebra in the area of cryptography. In this paper, we employ the algebraic structure called skew $\boldsymbol{\pi}$-Armendariz rings to design a neoteric algorithm for zero knowledge proof. The proposed protocol is established and illustrated through numerical example, and its soundness and completeness are proved.

Keywords**—**Cryptosystem, identification, skew $\boldsymbol{\pi}$-Armendariz rings, skew polynomial rings, zero knowledge protocol.

I. Introduction

WITH the development of communication in the last several decades, applications that involve abstract algebra have become increasingly important. Ring theory occupies a central role in the subject of abstract algebra, and the importance of its applications such as coding theory and cryptography has grown significantly. In particular, it is efficient in the detection of errors in identification codes. The purpose of cryptography is to send messages through a channel such that only the purposed recipient of the message can read it. Furthermore, the recipient always requires some guarantees that the message is genuine, when a message is received. This means that the massage has not been sent by anyone who is trying to trick the recipient. Currently cryptography is a significant subject for abstract algebra and number theory. Factorization and discrete logarithm problems (which is hard mathematical problems) are adopted in several public key cryptosystems, such as RSA, ElGamal cryptosystem, and ECC.

Zero-knowledge proofs were first devised as an idea in 1985 by Shafi et al. [1]. This paper gives a description of the concept of knowledge complexity, a measurement of the amount of knowledge about the evidence sent from the prover to the verifier. Zero knowledge protocols idea was established by authentication schemes in which one party needs to prove his/her identity to the other party through some confidential information but he/she does not wish the other party to know any information of the confidential facts. Courtois has introduced in [2] a new zero knowledge proof which is depended on the NP-complete problem that is named MinRank. Wolf has presented in [3] the zero knowledge protocols which are used to fix authentication problems. All the previous studies are applied on a finite field, so using a new algebraic structure on the polynomial rings is considered as a new challenge in modern cryptosystems. Nowadays, several cryptographic protocols have been developed based on non-commutative algebraic structure, such as authentication, key exchange, and encryption-decryption processes. They are proven to be efficient in corresponding to their commutative case. On the other hand, throughout this paper, the associative rings with identity are considered unless otherwise mentioned. Many authors have expressed their interest of authentication protocols that depends on some algebraic structures as in [4] and some promising authentication schemes have been proposed on rings and algebras such as; endomorphism rings and quaternion algebra.

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

A ring $\mathfrak{R}$ is said to be reduced if there are no nonzero nilpotent elements belonging to $\mathfrak{R}$. In the other words, $r^{2} = 0$ implies $r = 0$ for any $r \in R$ [5]. Due to Rege and Chhawchharia in 1997 [6], 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 $a_ib_j = 0$ for all i, j. Also, it is showed in [6] that every reduced ring is Armendariz. The concept of Armendariz rings is generalized to the concept of α-skew Armendariz by Hong et al. [7]. A ring $\mathfrak{R}$ is said to be skew π-Armendariz if for any two polynomials $\vartheta(\chi) = \sum_{i=0}^{m} a_i\chi^i$, $\phi(\chi) = \sum_{j=0}^{n} b_j\chi^j \in \mathfrak{R}[\chi,\alpha,\delta]$, such that, $\vartheta(\chi)\phi(\chi) \in \aleph(\mathfrak{R}[\chi,\alpha,\delta])$ implies $a_ib_j \in \aleph(\mathfrak{R})$ for each i, j [8].

The rest of this paper is organized as follows. Section II is devoted entirely to give mathematical preliminaries of the concept of skew π-Armendariz rings. Section III summarizes

Areej M. Abduldaim is with the Department of Applied Sciences, University of Technology, Baghdad, CO 10001 Iraq (phone: +9647707892924; e-mail: areejmussab@gmail.com).

Nadia M. G. Al-Saidi is with the Department of Applied Sciences, University of Technology, Baghdad, CO 10001 Iraq (e-mail: nadiamg08@gmail.com).

some reviews and related works of the original 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 skew π-armendariz rings is given, and in the second subsection, the zero knowledge of the algebraic zero knowledge proof is investigated with some analysis. The discussion and the conclusion are given in Sections V and VI, respectively.

It is worth mentioning that there are many concepts related and closed to the concept of skew π-Armendariz rings, some of them are the notion of McCoy rings and its generalizations: π-McCoy rings and α- skew π-McCoy rings [9]-[13].

II. Preliminaries: Mathematical of the Algebraic Structure skew π-Armendariz rings

To construct a stubborn problem, the condition of skew π-Armendariz rings, and the properties of the polynomial ring related to this kind of rings should be integrated with the principals of the zero knowledge protocol to achieve our goal. Next, we recall the definition and some fundamental basics and properties of skew π-Armendariz rings, which are necessary in the rest of this work.

A. Definition

A ring $\mathfrak{R}$ is skew π-Armendariz if for $\vartheta(\chi)=\sum_{i=0}^{m} a_i\chi^i$, $\phi(\chi)=\sum_{j=0}^{n} b_j\chi^j \in \mathfrak{R}[\chi,\alpha,\delta]$ such that $\vartheta(\chi)\phi(\chi)\in \aleph(\mathfrak{R}[\chi,\alpha,\delta])$ implies $a_ib_j\in\aleph(\mathfrak{R})$ 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 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 ring $\mathcal{M}_n(\mathfrak{R})$. The following theorem gives some characterizations of skew π-Armendariz rings [8]:

B. Theorem

Let α be an endomorphism of the ring $\mathfrak{R}$. Then, the following conditions are equivalent:

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

C. Example

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

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

Then, $\mathcal{M}_4$ is skew π-Armendariz by Theorem B.

D. 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

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

Define the endomorphism $\alpha:\mathcal{F}\to\mathcal{F}$ by $\alpha\left(\begin{pmatrix} A & \mathcal{B}\\ 0 & C\end{pmatrix}\right)=\begin{pmatrix} A & -\mathcal{B}\\ 0 & C\end{pmatrix}$ for any $\begin{pmatrix} A & \mathcal{B}\\ 0 & C\end{pmatrix}\in\mathcal{F}$. The ring $\mathcal{F}$ is not 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 $a_1b_0\notin\aleph(\mathcal{F})$

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

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

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

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

III. the Original Zero Knowledge Protocol

Many theories have been written extensively about zero knowledge proofs. However, the information available is not much practical in spite of many applications that use the zero knowledge technique. Proofs are often seen (by scientists) as a static mathematical object. A zero knowledge protocol is a proof system by which one party (known the prover) tries to convince another party (known the verifier) that the hidden secret is true. The following names appear in the zero knowledge protocols [14], [15]:

Peggy the Prover: Peggy hides a secret σ, and she has to prove to Vic that she knows it, but without disclosing the secret σ itself to Vic.

Victor (Vic) the Verifier: Vic requests Peggy to answer a group of questions to check that Peggy truly knows the secret σ or not. Vic will not know anything about the secret itself, even if he cheats or does not commit to the protocol.

Eave the Eavesdropper: Eave is the entity who is listening to the discussion between Peggy and Vic. A secure zero knowledge protocol guarantees that no third entity is able to know about the secret σ .

An interactive proof system for a set Σ is a two-parity game between a prover and a verifier and it satisfies two properties:

- Completeness: Peggy has very high probability of convincing Vic if she knows σ ∈Σ,
- Soundness: Peggy has very low probability to fool Vic if she does not know σ .
- Zero Knowledge property: ZK Protocols having some special features; the verifier cannot know anything from the protocol. The verifier cannot deceive the prover, he cannot claim to be the prover to any third entity and the prover cannot deceive the verifier.

IV. Algebraic Structure for Zero Knowledge Proof with the Underlying Skew π-Armendariz Rings

A. Algorithm

The identification scheme includes initial setup, key generation and authentication. The algebraic zero knowledge proof algorithm contains the following main steps: Peggy is the prover and Vic is the verifier.

Peggy, the prover, would like to show Vic, the verifier, that a secret polynomial $\vartheta(\chi) \in \mathfrak{R}[\chi, \alpha, \delta]$ has coefficients belonging to a skew π-Armendariz ring $\mathfrak{R}$. This polynomial is kept by the prover and never shared. Both of the prover and the verifier know the ring $\mathfrak{R}$, and it is skew π-Armendariz.

For any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i \chi^i$, $\psi(\chi) = \sum_{j=0}^{n} b_j \chi^j \in \mathfrak{R}[\chi, \alpha, \delta]$, Peggy the prover computes the product of $\varphi(\chi)$ and $\psi(\chi)$ such that, $\varphi(\chi)\psi(\chi) \in \aleph(\mathfrak{R}[\chi, \alpha, \delta])$ and publishes her public key, the set $P_{coef.} = \{a_i b_j | 0 \leq i \leq m \text{ and } 0 \leq j \leq n\}$ to show Vic that each element of the set $P_{coef.}$ is nilpotent without sharing the secret polynomial $\varphi(\chi)$ as Peggy's private key. This polynomial is kept by the prover and never shared.

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

$$\begin{aligned}
\varphi(\chi)\psi(\chi) = {} & a_0 b_0 + a_0 b_1 \chi + a_0 b_2 \chi^2 + a_0 b_3 \chi^3 + \cdots \\
& + a_0 b_n \chi^n \\
& + a_1 \alpha(b_0)\chi + a_1 \alpha^1(b_1)\chi^2 + a_1 \alpha^1(b_2)\chi^3 + a_1 \alpha^1(b_3)\chi^4 + \cdots \\
& + a_1 \alpha^1(b_n)\chi^{n+1} \\
& + a_2 \alpha^2(b_0)\chi^2 + a_2 \alpha^2(b_1)\chi^2\chi + a_2 \alpha^2(b_2)\chi^2\chi^2 \\
& + a_2 \alpha^2(b_3)\chi^2\chi^3 + \cdots + a_2 \alpha^2(b_n)\chi^2\chi^n \\
& + a_3 \alpha^3(b_0)\chi^3 + a_3 \alpha^3(b_1)\chi^3\chi + a_3 \alpha^3(b_2)\chi^3\chi^2 \\
& + a_3 \alpha^3(b_3)\chi^3\chi^3 + \cdots + a_3 \alpha^3(b_n)\chi^3\chi^n \\
& + \cdots \\
& + a_m \alpha^m(b_0)\chi^m + a_m \alpha^m(b_1)\chi^m\chi + a_m \alpha^m(b_2)\chi^m\chi^2 \\
& + a_m \alpha^m(b_3)\chi^m\chi^3 + \cdots + a_m \alpha^m(b_n)\chi^m\chi^n
\end{aligned}$$

and sends Vic the set

$$P_{coef.} = \{a_i b_j | 0 \leq i \leq m \text{ and } 0 \leq j \leq n\}.$$

Step 2. Vic chooses randomly $r = 0$ or 1 and sends it to Peggy.

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

Step 4. Vic checks that:

if $r = 0$, then Vic checks that $(a_i b_j)^{k_{ij}-r} = 0$ (because Vic knows that $\mathfrak{R}$ is skew π-Armendariz ring & $r = 0$) which means that $a_i b_j$ is nilpotent element.

if $r = 1$, it is definitely Vic checks that $(a_i b_j)^{k_{ij}-r} \neq 0$ (this means that $a_i b_j \notin \aleph(\mathfrak{R})$ which contradicts the fact that A is skew π-Armendariz ring).

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

B. 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 skew π-Armendariz by Theorem B. 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 $a_i b_j \in \aleph(\mathfrak{R}_4)$.

Step 1. Peggy 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,

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

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

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

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

Now,

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

which means that

$$\varphi(\chi)\psi(\chi)=\begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}+\begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\chi$$
$$+\begin{pmatrix}0&0&0&-2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}+\begin{pmatrix}0&0&0&2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\chi^2\in\aleph(\Re_4[\chi,\bar{\alpha}])$$

then Peggy sends Vic the set $P_{coef.}=\{a_ib_j|0\le i\le 1\text{ and }0\le j\le 1\}=$

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

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

Step 2. Vic chooses randomly $r=0$ or 1 and sends it to Peggy.

Step 3. For each element of the set

$P_{coef.}=\{a_ib_j|0\le i\le 1\text{ and }0\le j\le 1\}$, Peggy finds

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

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

Peggy sends Vic $k_{00}=2$ to check$(a_0b_0)^{k_{00}-r}$.

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

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

Peggy sends Vic $k_{01}=2$ to check $(a_0b_1)^{k_{01}-r}$.

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

$$(a_1b_0)^{k_{10}}=(a_1b_0)^3=\begin{pmatrix}0&0&0&-2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^3=0,$$

Peggy sends Vic $k_{10}=3$ to check $(a_1b_0)^{k_{10}-r}$.

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

$$(a_1b_1)^{k_{11}}=(a_1b_1)^2=\begin{pmatrix}0&0&0&2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^2=0,$$

Peggy sends Vic $k_{10}=3$ to check $(a_1b_1)^{k_{10}-r}$.

Step 4.

i. If $r=0$, then Vic checks that

$$(a_0b_0)^{k_{00}-r}=\begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{00}-r}=0$$

(because Vic knows that $\Re_4$ is skew π-Armendariz ring & $r=0$).

If $r=1$, then Vic checks that

$$(a_0b_0)^{k_{00}-r}=\begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{00}-r}\neq 0$$

(This means that $\begin{pmatrix}0&0&-1&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\notin\aleph(\Re_4)$, which contradicts the fact that $\Re_4$ is skew π-Armendariz ring).

ii. If $r=0$, then Vic checks that

$$(a_0b_1)^{k_{01}-r}=\begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{01}-r}=0$$

(because Vic knows that $\Re_4$ is skew π-Armendariz ring & $r=0$).

If $r=1$, then Vic checks that

$$(a_0b_1)^{k_{00}-r}=\begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{01}-r}\neq 0$$

(This means that $\begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\notin\aleph(\Re_4)$, which contradicts the fact that $\mathfrak{R}_4$ is skew π-Armendariz ring).

iii. If $r = 0$, then Vic checks that

$$(a_1b_0)^{k_{10}-r} = \begin{pmatrix}0&0&0&-2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{10}-r} = 0$$

(because Vic knows that $\mathfrak{R}_4$ is skew π-Armendariz ring & $r = 0$).

If $r = 1$, then Vic checks that

$$(a_1b_0)^{k_{10}-r} = \begin{pmatrix}0&0&0&-2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{10}-r} \neq 0$$

(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 contradicts the fact that $\mathfrak{R}_4$ skew is π-Armendariz ring).

iv. If $r = 0$, then Vic checks that

$$(a_1b_1)^{k_{11}-r} = \begin{pmatrix}0&0&0&2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{11}-r} = 0$$

(because Vic knows that $\mathfrak{R}_4$ is skew π-Armendariz ring & $r = 0$).

If $r = 1$, then Vic checks that $(a_1b_1)^{k_{11}-r} = \begin{pmatrix}0&0&0&2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{11}-r} \neq 0$ (This means that $\begin{pmatrix}0&0&0&2\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \notin \aleph(\mathfrak{R}_4)$, which contradicts the fact that $\mathfrak{R}_4$ is skew π-Armendariz ring).

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

V. The Zero Knowledgeness of the Skew π-Armendariz Zero Knowledge Protocol

In this section, the proof of knowledge scheme, based on α-skew π-Armendariz rings, is detailed. Zero knowledge proofs are not proofs in the mathematical meaning of the expression, since there is some soundness error when a deceit prover will be able to trick the verifier of a non-true statement. Nevertheless, there are standard techniques to reduce the soundness error for some small value. Thus, there are three core requirements in zero knowledge proofs:

Completeness: A prover can convince the verifier, this is true statements.

It is simple to see that our protocol is complete. If $\vartheta(\chi) = \sum_{i=0}^{m} a_i\chi^i$, $\phi(\chi) = \sum_{j=0}^{n} b_j\chi^j \in \mathfrak{R}[\chi, \alpha]$, such that $\vartheta(\chi)\phi(\chi) \in \aleph(\mathfrak{R}[\chi, \alpha])$, then $a_ib_j \in \aleph(\mathfrak{R})$. Furthermore, the prover who knows the secret polynomial $\vartheta(\chi)$ can easily check if each a_ib_j is nilpotent or not. So, the prover can answer both of the possible challenges $r \in \{0,1\}$ and has 100% probability of convincing the verifier.

Soundness: A prover cannot convince the verifier (even if the prover cheats and deviates from the protocol), this is false statements.

Our protocol is sound in the sense that there is 50% chance of catching a cheating prover. If $\vartheta(\chi)\phi(\chi) \in \aleph(\mathfrak{R}[\chi, \alpha])$, such that $a_ib_j \notin \aleph(\mathfrak{R})$, then $\mathfrak{R}$ cannot be skew π-Armendariz ring. So, if the verifier picks r, such that, $a_ib_j \notin \aleph(\mathfrak{R})$, then the prover cannot answer the challenge. To increase our chance of catching a cheating prover, we can repeat the challenge and response protocol. We modify the protocol to perform n repetitions for the same $\vartheta(\chi)$ but different $\phi(\chi)$. In each interaction, we have 50% chance of catching the cheating prover, so overall the risk of cheating is reduced to 2^{-n}.

Zero knowledge property: The verifier will not learn anything from the interaction apart from the fact that the statement is true. If the statement is true, no cheating verifier can learn anything other than the truth of this statement.

Peggy's answers do not reveal the original secret polynomial $\varphi(\chi)$. Each round, Vic will learn only the set $P_{coef.} = \{a_ib_j | 0 \leq i \leq m\ and\ 0 \leq j \leq n\}$ with each element of $P_{coef.}$ is nilpotent or not. He needs all a_i to discover the secret polynomial, so the information remains unknown as long as Peggy can choose distinct $\psi(\chi)$ and generate a_ib_j every round. If Peggy does not know of a secret polynomial $\varphi(\chi)$, but somehow knew in advance what Vic would ask to see each round, then she could cheat. For example, if Peggy knew ahead of time that Vic would ask to see the secret polynomial $\varphi(\chi)$, then she could choose distinct $\psi(\chi)$ and generate a_ib_j for an unrelated polynomial. Similarly, if Peggy knew in advance that Vic would ask to see the isomorphism, then she could simply choose distinct $\psi(\chi)$ and generate the set $P_{coef.} = \{a_ib_j | 0 \leq i \leq m\ and\ 0 \leq j \leq n\}$. Vic could simulate the protocol by himself (without Peggy), because he knows what he will ask to see. Therefore, Vic gains no information about the secret polynomial $\varphi(\chi)$ from the information revealed in each round.

VI. Discussion

The proposed zero knowledge protocol based on skew π-Armendariz rings involves two parties, Peggy and Vic. Peggy tries to prove her identity to Vic without telling her private information $\varphi(\chi)$. Then she generates a public key $\varphi(\chi)\psi(\chi) \in \mathfrak{R}[\chi, \alpha]$, choosing the polynomial $\psi(\chi)$ and sends the set $P_{coef.} = \{a_ib_j | 0 \leq i \leq m\ and\ 0 \leq j \leq n\}$ to Vic. On the other hand, Vic does the same strategy, and sent his public key $r = 0$ or 1 to Peggy. Now, Peggy uses the skew π-Armendariz property of $\mathfrak{R}$ and her private key $\varphi(\chi)$ to compute the set $P_{coef.} = \{a_ib_j | 0 \leq i \leq m\ and\ 0 \leq j \leq n\}$, and sends it to Vic. To verify Peggy's secret, Vic needs to compute $(a_ib_j)^{k_{ij}-r}$. If $(a_ib_j)^{k_{ij}-r}$=0, then Vic can convince that Peggy knows the secret, and the authentication process is succeeded. Trying to find the private keys, this involves us to find the matrices whose product is given, which is computationally infeasible. This will prevent attacks on private key values. If the number of bits is n, then there are 2^n possibilities for every value of $a_i b_j$ and n. In this case, the brute force attack does not work when the length of these keys is as long as possible.

VII. Conclusion

A novel algebraic protocol is proposed in this paper to be used in zero knowledge systems and it depends on the algebraic structure of skew π-Armendariz rings. Another important fact that we have considered is the security of algebraic cryptography systems, which is based on noncommutative rings to ensure that it cannot be solved in practical amount of time. Consequently, several familiar attacks are unsuccessful to solve the nonlinear systems and discover the inaccurate secret key factor from the known public key. Although it is theoretically potential, it is arithmetically not workable. Even if it is theoretically possible, it is computationally not feasible.

References

[1] S. Goldwasser, S. Micali, and C.Rckoff, "The knowledge complexity of interactive proof systems," *SIAM Journal of Computing*, vol. 18, pp.186-208, 1989.

[2] N. T. Courtois, "Efficient zero-knowledge authentication based on a linear algebra problem minrank," *Asiacrypt 2001*, vol. 22, no. 48, pp. 402-411, 2001.

[3] C. Wolf, "Zero-knowledge and multivariate quadratic equations," *Workshop on Coding and Cryptography*, 2004.

[4] M. R. Valluri, "Authentication schemes using polynomials over non-commutative rings," *International Journal on Cryptography and Information Security*, vol.2, no.4, 51-58, 2012

[5] E. Armendariz, "A note on extensions of baer and p.p. –rings", *Journal of Austral. Math. Soc*, vol.18, pp: 470-473, 1974.

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

[7] C. Y. Hong, N. K. Kim and T. K. Kwak, "On skew armendariz rings," *Communications in Algebra*, vol. 31, no. 1, pp: 103-122, 2003.

[8] O. Lunqun_, L. Jinwang and X. Yueming, "Ore extensions of skew π - Armendariz rings", *Bulletin of the Iranian Mathematical Society* vol. 39 no. 2, pp 355-368, 2013.

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

[10] A. M. Abduldaim and A. M. Ajaj, "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, 2017, pp 112-117.

[11] A. M. Abduldaim, "Weak Armendariz Zero Knowledge Cryptosystem," Journal of Al-Qadisiyah for Computer Science and Mathematics, vol. 9, no. 2, pp. 1-6, 2017.

[12] A. M. Abduldaim and R. M. Abidali, "π-Armendariz Rings and Related Concepts," Baghdad Science Journal, vol. 13, no. 4, pp. 853-861, 2016.

[13] A. M. Abduldaim and A. M. Ajaj, "Examples of α-Skew π-Armendariz Rings," Iraqi Journal of Science (Baghdad University), vol. 58, no. 1C, pp. 482-489, 2017.

[14] O. Goldreich and Y. Oren, "Definitions and properties of zero-knowledge proof systems," Journal of Cryptology, vol. 7, no. 1, pp. 1-32, 1994.

[15] A. Piva, "On the integration between digital watermarking and cryptography," European Association for Signal Processing (EURASIP) NewsLetter, vol. 16, no. 4, pp. 2-14, 2005.

Areej M. Abduldaim was born in Iraq, 1973. She received the B.Sc. degree in mathematics from Al-Mustansiryah University, Baghdad, Iraq, 1995, the M.Sc. degree in mathematics from Al-Mustansiryah University, Baghdad, Iraq, 1999, and the Ph.D. degree in mathematics from Harbin Institute of technology, Harbin, Heilongjiang, China, 2014.

She joined the Department of Applied Sciences, University of Technology-Baghdad-Iraq, as an academic staff member in 1999. She has numerous technical papers since 1999 in several journals that have Thomson Reuters rating, Scopus rating, etc. Her research interests include: Abstract Algebra, Image Processing and Cryptography.

Nadia M. G. Al-Saidi is a professor in the Department of Applied Sciences, University of Technology-Baghdad-Iraq. She completed her Bachelor of Science and Master of Science degrees in applied mathematics, from Department of Applied Sciences-University of Technology, Baghdad, Iraq, in 1989, and 1995, respectively. She received her Ph.D degree in mathematics and computer application sciences from Al-Nahrien University, Baghdad, Iraq 2003. She joined the Institute for Mathematical Research (INSPEM), University Putra Malaysia (UPM) as a post doctorate researcher from 2008-2010 with the research project "fractals in Cryptography".

In 1989 she joined the Department of Applied Sciences, University of Technology, as an academic staff member.

Prof. Dr. Nadia is the author of numerous technical papers since 1994, her research interests include: Cryptography, Fractal geometry, Chaos theory, Graph theory.