Algebraic Verification Algorithm

Areej M. Abduldaim
Department of Applied Sciences
University of Technology
Baghdad, Iraq
areejmussab@gmail.com

***Abstract*—Authentication over insecure public networks or with untrusted servers raises more concerns in privacy and security.Modern algebra is one of the significantfields of mathematics. It is a combination of techniques used for a variety of applications including the process of the manipulation of the mathematical categories. In addition,modern algebra deals in depth with the study of abstractions such as groups, rings and fields,the main objective of this article is to provide a novel algebraic verification protocol using ring theory. The protocol is blind, meaning that it detects only the identity, and no additional information will be known anything about the prover (the biometric) to the authenticating server or vice-versa. More officially a blind authentication scheme is a cryptographic protocol that comprises of two parties, a user (the prover) that wants to achieve having signs on her messages, and a signer (the verifier) that is in ownership of his secret signing key. In this paper, we employ the algebraic structure called central 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.This method gave two important properties for the central Armendariz zero knowledge protocol compared with other known protocols.**

***Keywords*—Central Armendariz rings, Authentication, Zero Knowledge Protocol, Cryptography, Polynomial Ring**

I. INTRODUCTION

Zero knowledge protocol is one of the cornerstones of modern cryptography, in which one party can confirm whether or not a statement is true without detecting any other data about the statement. Zero knowledge authentication protocol is a practical application of the concept of a zero knowledge proof. This type of proof is particularly useful in the context of remote authentication because of the hazard of disclosure through the insecure transition medium.

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 aim of cryptography is to send messages across a channel so that only the intended recipient of the message can read it. In addition, when a message is received, the recipient usually requires some assurance that the message is authentic; that is, it has not been sent by someone who is trying to deceive the recipient. Modern cryptography is heavily dependent on 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 by Goldwasser et al. [1]. This paper conceived the concept of knowledge complexity, a measurement of the amount of knowledge about the proof transferred from the prover to the verifier. The idea of zero-knowledge proofs has been motivated by authentication systems where one party wants to prove its identity to a second party via some secret information (such as a password) but doesn't want the second party to learn anything about this secret. 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 considers 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 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 in the form $a_0 + a_1\chi + a_2\chi^2 + \cdots + a_m\chi^m$, where m can be any nonnegative integer and the coefficients $a_0, a_1, a_2, \cdots, a_m$ are all in $\mathcal{R}$. The set of all central elements in $\mathcal{R}$ can be denoted by $C(\mathcal{R})$.

A ring $\mathcal{R}$ is said to be reducedif there is no nonzero nilpotent elements belong to $\mathcal{R}$. For any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i\chi$, $\psi(\chi) = \sum_{j=0}^{n} b_j\chi$in $\mathcal{R}[\chi]$, Armendariz [4] proved that if $\mathcal{R}$ is a reduced ring such that $\varphi(\chi)\psi(\chi) = 0$, then $a_ib_j = 0$ for all i,j. Any ring, which may not be reduced, and satisfy Armendariz's condition, is said to be Armendariz by Rege et al. [5]. Moreover, every reduced ring is Armendariz. Thereafter, Agayevet. al. in [6] introduced the concept of central Armendariz rings such that, every Armendariz ring is central Armendariz. In other words, the class of central Armendariz rings regards as generalization of the class of Armendariz rings. A ring $\mathcal{R}$ is central Armendariz if for any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i\chi^i$ and $\psi(\chi) = \sum_{j=0}^{n} b_j\chi^j$ in $\mathcal{R}[\chi]$ provided that $\varphi(\chi)\psi(\chi) = 0$ implies $a_ib_j \in C(\mathcal{R})$ for each $0 \le i \le m$and $0 \le j \le n$. In this paper is organized as follows. Part II is devoted to review the original

zero knowledge protocol in details. Part III summarizes some mathematical preliminaries of the central Armendariz rings. Part IV presents the proposed Algebraic Zero Knowledge Protocol based on the central Armendariz rings with a simulation example. The advantages of the proposed algorithm and the procedure analysis are established in part V. Finally, the conclusion is given in part VI.

It is worth to mention that there are many concepts related and closed to the concept of the central Armendariz rings. One of them is the McCoy rings and its generalizations the π-McCoy rings and π-skew π-McCoy rings [7-9]. On the other hand, there are several applications of the series of Armendariz rings in zero knowledge cryptosystems [10, 12].

II. THE ZERO KNOWLEDGE PROTOCOL

A lot of theories have been written extensively about zero knowledge proofs. However, the information available is not much practical in spite of many applications based on 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 namesappear in zero-knowledge protocols [13]:

Peggy the Prover: Peggy hides a secret $\mathbb{S}$ that she has to prove to Vic, but without disclosing the secret $\mathbb{S}$ itself to Vic.

Victor the Verifier: Vic requests Peggy to answer a group of questions, to check that Peggy truly knows the secret $\mathbb{S}$ 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 listening to the discussion between Peggy and Vic. A secure zero knowledge protocol also guarantees that no third entity can know about the secret $\mathbb{S}$.

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

Completeness: Peggy has very high probability of convincing Victor if she knows $\mathbb{S} \in S$,

Soundness: Peggy has very low probability to fool Victor if she does not know $\mathbb{S}$.

Zero-knowledge protocols having some specific features like: (1) The verifier cannot know anything from the protocol, (2) The verifier cannot deceive the prover, (3) The verifier cannot have claimed to be the prover to any third entity and the prover cannot deceive the verifier.

III. CENTRAL ARMENDARIZRINGS

To construct a stubborn problem we would like to integrate the condition of central Armendariz rings and the properties of the polynomial ring related to this kind of rings with the principals of the zero knowledge protocol to achieve our goal.

Now, we recall the definition and some fundamental basics and properties of central Armendariz rings which are necessary in the rest of this work.

A. Definition

A ring $\mathcal{R}$ is central Armendariz if for $\varphi(\chi) = \sum_{i=0}^{m} a_i \chi^i$, $\psi(\chi) = \sum_{j=0}^{n} b_j \chi^j \in \mathcal{R}[\chi]$ such that, $\varphi(\chi)\psi(\chi) = 0$, then $a_i b_j \in C(\mathcal{R})$ for all i, j. [6]

It is clear that every Armendariz ring is central Armendariz but the converse may not be true in general. In 2017, Chen [14] proved that the ring $R[x]/(x^2)$ is central Armendariz but not central reduced.

Let $UTM_n(\mathcal{R})$ be the $n \times n$ upper triangular matrix ring over a ring $\mathcal{R}$, and k be a natural number smaller than n. Say $UTM_n^k(\mathcal{R})\{\sum_{i=j}^{n}\sum_{j=1}^{k} a_j e_{(i-j+1)i} + \sum_{i=j}^{n-k}\sum_{j=1}^{n-k} r_{ij} e_{j(k+i)} : a_j, r_{ij} \in \mathcal{R}\}$, where e_{ij}'s are matrix units. Elements of $UTM_n^k(\mathcal{R})$are in the form $\begin{pmatrix} x_1 & x_2 & \cdots & x_k \cdots a_{1(k+1)} \\ 0 & x_1 & & \cdots \quad a_{2n} \\ \vdots & \vdots & & \ddots \quad \vdots \\ 0 & 0 & & \cdots \quad \alpha \end{pmatrix}$ where $x_i, a_{js} \in \mathcal{R}, 1 \le i \le k, 1 \le j \le n-k$ and $k+1 \le s \le n$.

The following theorem gives some characterizations of central Armendariz rings:

B. Theorem

Let $\mathcal{R}$ be a ring, $n \ge 3$ be a natural number and $k = \left[\frac{n}{2}\right]$.The following conditions are equivalent:

(1) $\mathcal{R}$ is reduced ring;

(2) $UTM_n^k(\mathcal{R})$ is an Armendariz ring;

(3) $UTM_n^{n-2}(\mathcal{R})$is a central Armendariz ring.

A ring $\mathcal{R}$ is said to be abelian if every idempotent of it belong to the $C(\mathcal{R})$. It is clear that every central Armendariz ring is abelian but the converse is not true in general.

IV. THE PROPOSED ALGEBRAIC VERIFICATION ALGORITHM

Initial Setup: Assume that $\mathcal{R}$ is central Armendariz 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 central Armendariz.

Key Generation: For any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i \chi^i$, $\psi(\chi) = \sum_{j=0}^{n} b_j \chi^j \in \mathcal{R}[\chi]$, Peggy the prover computes the product of $\varphi(\chi)$ and $\psi(\chi)$, such that, $\varphi(\chi)\psi(\chi) = 0$ and publishes her public key, the set $P_{coef.} = \{a_i b_j | 0 \le i \le m \text{ and } 0 \le j \le n\}$ to show Vic the verifier that each element of the set $P_{coef.}$ is central 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 (χ) , $\psi(\chi) \in \mathcal{R}[\chi]$ such that $\varphi(\chi)\psi(\chi) = 0$ and sends Vic the set

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

Authentication: To start authentication

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

Step 3: For each i, j, and for each $c \in R$ Peggy finds $k_{ij} \in \mathbb{Z}^+$, such that $[a_i b_j, c] = rk_{ij} + k_{ij}$, where $k_{ij} = a_i b_j c - c a_i b_j$ and send Vic $rk_{ij} + k_{ij}$ as a value of $[a_i b_j, c]$.

Step 4: Vic checks that:
If $r = 0$, then Vic checks that $[a_i b_j, c] = rk_{ij} + k_{ij}$ (because Vic knows that $\mathcal{R}$ is central Armendariz ring & $r = 0$),

i- If $k_{ij} = 0$, then $[a_i b_j, c] = 0$, for all $c \in R$ and this means that $a_i b_j$ is central element.

ii- If $k_{ij} \neq 0$, then $[a_i b_j, c] \neq 0$ this means that $a_i b_j$ cannot commute with every element of R. Hence $a_i b_j$ is not central element.

If $r = 1$, then

i- If $k_{ij} = 0$, then $[a_i b_j, c] = 0$, for all $c \in R$ and this means that $a_i b_j$ is central element.

ii- If $k_{ij} \neq 0$, it is definitely Vic checks that $[a_i b_j, c] \neq 0$ (this means that $a_i b_j \notin C(\mathcal{R})$ which contradicts the fact that $\mathcal{R}$ is central Armendariz ring).

Step 5: Repeat the above steps μ times, where μ is the number of polynomials $\psi(\chi) \in \mathcal{R}[\chi]$ such that $\varphi(\chi)\psi(\chi) = 0$. To find μ, we should first determine the degree of $\psi(\chi)$, k, which must be large enough.

A. Example

Define

$$T_4^2 = \left\{ \begin{pmatrix} x_1 & x_2 & a_{13} & a_{14} \\ 0 & x_1 & x_2 & a_{24} \\ 0 & 0 & x_1 & x_2 \\ 0 & 0 & 0 & x_1 \end{pmatrix} \middle| x_i, a_{ij} \in \mathbb{Z}_5 \& \, i, j = 1,2,3,4 \right\} \in UTM_n^k(\mathcal{R})(\mathbb{Z}_5)$$

where $\mathbb{Z}_5$ is the ring of integers modulo 5, $\mathbb{Z}_5$ is reduced ring. Hence, T_4^2 is central Armendariz by *Theorem* for any two polynomials $\varphi(\chi) = \sum_{i=0}^{m} a_i \chi^i, \psi(\chi) = \sum_{j=0}^{n} b_j \chi^j \in T_4^2[\chi]$, such that $\varphi(\chi)\psi(\chi) = 0$ we have that $a_i b_j \in C(T_4^2)$.

Step 1: Peggy chooses $\varphi(\chi) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \chi \in T_4^2[\chi]$ as a private key and kept it, and

$\psi(\chi) = \begin{pmatrix} 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \chi \in T_4^2[\chi]$ where

$$a_0 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; a_1 = \begin{pmatrix} 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$b_0 = \begin{pmatrix} 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; b_1 = \begin{pmatrix} 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

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

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

and then Peggy sends Vic the set
$P_{coef.} = \{a_i b_j | 0 \leq i \leq 1 \text{ and } 0 \leq j \leq 1\} = \{a_0 b_0, a_0 b_1, a_1 b_0, a_1 b_1\}$

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

Step 3: For each i, j, and for each $c \in R$ Peggy finds $k_{ij} \in \mathbb{Z}^+$, such that $[a_i b_j, c] = rk_{ij} + k_{ij}$, where $k_{ij} = a_i b_j c - c a_i b_j$ and send Vic the value of $[a_i b_j, c]$.

For each element of the set
$P_{coef.} = \{a_i b_j | 0 \leq i \leq 1 \text{ and } 0 \leq j \leq 1\}$ Peggy found
$\forall c = \begin{pmatrix} c_1 & c_2 & d_{13} & d_{14} \\ 0 & c_1 & c_2 & d_{24} \\ 0 & 0 & c_1 & c_2 \\ 0 & 0 & 0 & c_1 \end{pmatrix} \in T_4^2$ we have that

(i) $[a_0 b_0, c] = a_0 b_0 c - c a_0 b_0 = k_{00} =$

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} c_1 & c_2 & d_{13} & d_{14} \\ 0 & c_1 & c_2 & d_{24} \\ 0 & 0 & c_1 & c_2 \\ 0 & 0 & 0 & c_1 \end{pmatrix} - \begin{pmatrix} c_1 & c_2 & d_{13} & d_{14} \\ 0 & c_1 & c_2 & d_{24} \\ 0 & 0 & c_1 & c_2 \\ 0 & 0 & 0 & c_1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = 0.$$

(ii) $[a_0 b_1, c] = a_0 b_1 c - c a_0 b_1 = k_{01} = 0$

(iii) $[a_1 b_0, c] = a_1 b_0 c - c a_1 b_0 = k_{10} = 0$

(iv) $[a_1 b_1, c] = a_1 b_1 c - c a_1 b_1 = k_{11} = 0$

Step 4: Vic checks that:

(i) If $r = 0$, then Vic checks that $[a_0b_0, c] = a_0b_0c - ca_0b_0 = rk_{00} + k_{00}$ (because Vic knows that $\mathcal{R}$ is central Armendariz ring & $r = 0$),

a- If $k_{00} = 0$, then $[a_0b_0, c] = 0$, for all $c \in R$ and this means that a_0b_0 is central element.

b- If $k_{00} \neq 0$, then$[a_0b_0, c] \neq 0$ this means that a_0b_0 cannot commute with every element of R. Hence a_0b_0 is not central element.

If $r = 1$, then

a- If $k_{00} = 0$, then $[a_0b_0, c] = 0$, for all $c \in R$ and this means that a_ib_j is central element.

b- If $k_{00} \neq 0$, it is definitely Vic checks that $[a_0b_0, c] \neq 0$ (this means that $a_0b_0 \notin C(\mathcal{R})$ which contradicts the fact that $\mathcal{R}$ is central Armendariz ring).

(ii) If $r = 0$, then Vic checks that $[a_0b_1, c] = a_0b_1c - ca_0b_1 = rk_{01} + k_{01}$ (because Vic knows that $\mathcal{R}$ is central Armendariz ring & $r = 0$),

a- If $k_{01} = 0$, then $[a_0b_1, c] = 0$, for all $c \in R$ and this means that a_0b_1 is central element.

b- If $k_{01} \neq 0$, then$[a_0b_1, c] \neq 0$ this means that a_0b_1 cannot commute with every element of R. Hence $a_0b_1$is not central element.

If $r = 1$, then

a- If $k_{01} = 0$, then $[a_0b_1, c] = 0$, for all $c \in R$ and this means that a_0b_1 is central element.

b- If $k_{01} \neq 0$, it is definitely Vic checks that $[a_0b_1, c] \neq 0$ (this means that $a_0b_1 \notin C(\mathcal{R})$ which contradicts the fact that $\mathcal{R}$ is central Armendariz ring).

(iii) If $r = 0$, then Vic checks that $[a_1b_0, c] = a_1b_0c - ca_1b_0 = rk_{10} + k_{10}$ (because Vic knows that $\mathcal{R}$ is central Armendariz ring & $r = 0$),

a- If $k_{10} = 0$, then $[a_1b_0, c] = 0$, for all $c \in R$ and this means that a_1b_0 is central element.

b- If $k_{10} \neq 0$, then$[a_1b_0, c] \neq 0$ this means that a_1b_0 cannot commute with every element of R. Hence $a_1b_0$is not central element.

If $r = 1$, then

a- If $k_{10} = 0$, then $[a_1b_0, c] = 0$, for all $c \in R$ and this means that a_1b_0 is central element.

b- If $k_{10} \neq 0$, it is definitely Vic checks that $[a_1b_0, c] \neq 0$ (this means that $a_1b_0 \notin C(\mathcal{R})$ which contradicts the fact that $\mathcal{R}$ is central Armendariz ring).

(iv) If $r = 0$, then Vic checks that $[a_1b_1, c] = a_1b_1c - ca_1b_1 = rk_{11} + k_{11}$ (because Vic knows that $\mathcal{R}$ is central Armendariz ring & $r = 0$),

a- If $k_{11} = 0$, then $[a_1b_1, c] = 0$, for all $c \in R$ and this means that a_1b_1 is central element.

b- If $k_{11} \neq 0$, then$[a_1b_1, c] \neq 0$ this means that a_1b_1 cannot commute with every element of R. Hence $a_1b_1$is not central element.

If $r = 1$, then

a- If $k_{11} = 0$, then $[a_1b_1, c] = 0$, for all $c \in R$ and this means that a_1b_1 is central element.

b- If $k_{11} \neq 0$, it is definitely Vic checks that $[a_1b_1, c] \neq 0$ (this means that $a_1b_1 \notin C(\mathcal{R})$ which contradicts the fact that $\mathcal{R}$ is central Armendariz ring).

Step 5: Repeat the above steps μ times, where μ is the number of polynomials $\psi(\chi) \in \mathcal{R}[\chi]$ such that $\varphi(\chi)\psi(\chi) = 0$. To find, μ we should first determine the degree k of $\psi(\chi)$ which should be large enough.

V. THE ADVANTAGES OF THE PROPOSED ALGORITHM:PROCEDURE ANALYSIS

In this section, we prove some properties that the central Armendariz zero knowledge protocol satisfied. First we focus on the *Confidentiality* which is guaranteed by the randomly selection of the polynomial $\psi(\chi)$. On the other hand the *Mutual Authentication* ensured by $rk_{ij} + k_{ij}$ which is based on $a_ib_j \in C(R)$and the zero knowledge proof stationed on central Armendariz ring. Regarding to the **Efficiency**of the introduced algorithm and because it only uses addition, multiplication, and exponents, this process is effective enough. Finally, the *Secrecy* is infeasibleto specify the secret polynomial $\varphi(\chi)$ is satisfied because it due to the difficulty in finding$a_i \forall i$ for all random $\psi(\chi)$.

There are three essential features that central Armendariz zero knowledge proof should be satisfied, they are as follows:

Completeness: For true statements, a prover can convince the verifier.

The prover can answer both of the possible challenges $r \in \{0,1\}$ and has 100% probability of convincing the verifier. So, the proposed protocol is complete.

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

If the verifier picks r, such that, $a_ib_j \notin C(\mathcal{R})$, 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 $\varphi(\chi)$ but different $\psi(\chi)$. In each interaction, we have 50% chance of catching the cheating prover, so overall the risk of cheating is reduced to 2^{-n}. So, the proposed protocol is sound.

Zero KnowledgeProperty: The verifier will not learn anything from the interaction apart from the fact that the statement is true.

Peggy's answers do not disclose the original secret polynomial $\varphi(\chi)$. Each round, Vic will impart only the set $P_{coef.} = \{a_ib_j | 0 \leq i \leq m \text{ and } 0 \leq j \leq n\}$ with each

element of $coef(P)$ is central or not. The verifier needs all a_i to discover the secret polynomial, so, the information remains unclear as long as Peggy can choose distinct $\psi(\chi)$ and generate $a_i b_j$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. Similarly, if Peggy knew in advance that Vic would ask to see the secret polynomial, then she could simply choose distinct $\psi(\chi)$ and generate the set $P_{coef.}$,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. CONCLUSION

The new approach based on the algebraic structure of central Armendariz rings is proposed to show that, the zero knowledge protocols doesn't restricted to specific cases. We used central Armendariz rings to prove that the scheme represent a zero knowledge protocol. Central Armendarizzero knowledge protocol can be used as a method for authentication.

The most important feature of central Armendariz ZKP among other is its high confidentiality. In order to achieve the best possible protocol, we followed the tactic of the straightforward computations with an unusual underlying algebraic ring. This method gave two important properties for the central Armendariz zero knowledge protocol compared with other known protocols: completeness and soundness. According to the structure of the algebraic zero knowledge protocol; four properties are adopted for comparison: The Confidentiality, MutualAuthentication, Efficiency and Secrecy of the protocol.

REFERENCES

[1] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," SIAM J. COMPUT. Vol. 18, No. 1, pp. 186-208, February 1989.

[2] N. T. Courtois, "Efficient zero-knowledge authentication based on a linear algebra problem minrank," Asiacrypt 2001, vol.2248, pp.402-411, 2001.

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

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

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

[6] N. Agayev, G. Güngöroğlu, A. Harmanci and S. Halıcıoğlu, "Central Armendariz rings," Bulletin of the Malaysian Mathematical Sciences Society, vol. 34, no. 1, pp:137-145, 2011.

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

[8] A. M. Abduldaim and R. M. Abidali, "π-Armendariz rings and related concepts," Baghdad Science Journal, vol. 13, no. 4, pp. 853-861, 2016.

[9] 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.

[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, pp 112-117, 2017.

[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] Areej M. Abduldaim and Nadia M. G. Al-Saidi, Generalized π-Armendariz Authentication Cryptosystem, World Academy of Science, Engineering and Technology, International Journal of Mathematical and Computational Sciences, Vol:11, No:9, 2017.

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

[14] W. Chen, Further results on central Armendariz rings, Journal of Algebra and Its Applications, Vol. 16, No. 2 (2017) 1750194 (12 pages).