Weak Armendariz Zero Knowledge Cryptosystem

Areej M. Abduldaim

Department of Applied Sciences
University of Technology

areejmussab@gmail.com

Recived : 25\4\2017 Revised : 14\5\2017 Accepted : 29\5\2017

Abstract

Innovative idea using ring theory is raised to build a new algorithm for zero knowledge (ZK) cryptosystem. In this paper we introduce an algorithm for zero knowledge protocol based on a specific kind of rings named weak Armendariz. On the other hand, the aim of this paper focuses on the category of noncommutative algebraic structures to describe a new algebraic scheme of zero knowledge proof using weak Armendariz rings. As a result, we employ for the first time weak Armendariz rings in the science of cryptographic which regards as a new application of this class of rings. Finally, we present a novel idea combining between abstract algebra and cryptography.

Keywords- Zero knowledge protocol, Weak Armendariz rings, Authentication, nilpotent element.

Mathematics subject classification : 22XX .

1. Introduction

Cryptography science is a set of mathematical mechanisms utilized to insure the transmission and save data, and is one of the main gadgets to counteract several menaces. Cryptography is the art of secret writing. It handles many known problems, especially: secrecy; privacy; authentication; passwords; identification and credit cards. The goal of cryptography is to send data through a channel such that only the intended recipient of the message can read it. Authentication provides confidentiality and authenticity confirmations on the data. The zero knowledge protocol is a method used for authentication by which one party allows to cause the second party to believe firmly in the truth of some statement is true, without detecting anything to the second party about the secret statement.

Zero knowledge proof was presented for the first time in 1985 by Goldwasser et al. [1]. Based on the expanded applications of the zero knowledge, Goldreich et al. reflected this protocol in [2].

An amelioration of the proof of zero knowledge, which is discussed by Fiat-Shamir in [3] and Micali-Shamir in [4], leaves the prover's complexity unchanged and reduces the verifier's complexity to less than 2 modular multiplications, however it is still depended on RSA algorithm in spite of it is computationally fast.

Fiege et al. [5] presented the main idea of this type of protocols to become the zero knowledge proof. Guillou-Quisquater (GQ) identification protocol [6] is an expansion to Fiat-Shamir protocol, which minimizes the number of passed messages and memory requirements for secret keys. The GQ protocol is an extension of the RSA scheme which reduces the needed rounds number to 1, and its security based on hardness of RSA cryptosystem. Goldwasser and Kalai [7] showed the possibility that the signature depended on (Fiege) Fiat-Shamir can be forged. Courtois has introduced in [8] a new Zero-knowledge proof which is depended on the NP-complete problem that is named MinRank. Wolf has presented in [9] 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.

Throughout this paper, all rings are associative with identity unless otherwise stated. Let $\mathcal{R}$ be any ring, the set of all polynomials in the indeterminate x, is called the polynomial ring and denoted by $\mathcal{R}[x]$. Any element belong to $\mathcal{R}[\chi]$ is of the form $\varphi(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$, where m can be any nonnegative integer and the coefficients $a_0, a_1, a_2, \cdots, a_m$ are all in $\mathcal{R}$. Let $\mathcal{M}_n(\mathcal{R})$ be the $n \times n$ matrix ring over $\mathcal{R}$ and let $\mathcal{T}_n(\mathcal{R})$ be the $n \times n$ triangular matrix ring over a ring $\mathcal{R}$.

The prime radical of $\mathcal{R}$ (which is the intersection of all prime ideals) can be denoted by $\mathcal{P}(\mathcal{R})$. The set of all nilpotent elements in $\mathcal{R}$ can be denoted by $\mathcal{N}(\mathcal{R})$. Finally, the set $\mathbb{Z}$ is the ring of integers.

A ring $\mathcal{R}$ is said to be reduced if there is no nonzero nilpotent elements belong to $\mathcal{R}$. Armendariz [10] proved that if $\mathcal{R}$ is a reduced ring such that for any two polynomials $\varphi(x) = \sum_{i=0}^{m} a_i x$, $\psi(x) = \sum_{j=0}^{n} b_j x$ in $\mathcal{R}[x]$ satisfy $\varphi(x)\psi(x) = 0$, then $a_i b_j = 0$ for all i, j. Any ring satisfies Armendariz's condition is said to be Armendariz by Rege et al. [11] ($\mathcal{R}$ may not be reduced). Moreover, every reduced ring is Armendariz. Thereafter, Liu and Zhao in [12] introduced the concept of weak Armendariz rings as a generalization of the notion of Armendariz rings. A ring $\mathcal{R}$ is said to be weak Armendariz if whenever polynomials $\varphi(x) = \sum_{i=0}^{m} a_i x^i$, $\psi(x) = \sum_{j=0}^{n} b_j x^j \in \mathcal{R}[x]$ satisfy $\varphi(x)\,\psi(x) = 0$, then $a_i b_j \in \mathcal{N}(\mathcal{R})$. Recently many researchers investigated novel ideas of authentication cryptosystem, in particular the zero knowledge algorithms from the algebraic point of view as in [13], [14] and [15]. Motivated by all of the above, in this paper, we established a new algorithm for the zero knowledge protocol using the class of weak Armendariz rings. In the initialization stage a secret polynomial is chosen to build up the key. A test between the two parties Posy and Vincent is held through the authentication and verification stages by which Vincent conclude if Posy know the secret or not. It is convenient to mention that there is another definition named weak Armendariz ring also given in 2009 by Jeon et al. [16]. A ring R is called weak Armendariz if for given $f(x) = a_0 + a_1 x$ and $g(x) = b_0 + b_1 x \in R[x]$, $f(x)g(x) = 0$ implies that $a_i b_j = 0$ for each i, j. The latest definition is not equivalent to the concept adopted in this paper.

The rest of this paper is organized as follows. Section 2 is devoted to recall some mathematical preliminaries of weak Armendariz rings. In Section 3, we brief the traditional zero knowledge scheme via a classical example. Section 4 shows the established weak Armendariz zero knowledge algorithm. Section 5 dedicates to analyze the weak zero knowledge algorithm. Finally, the conclusion is given in Section 6.

2. Preliminaries:

In this section we give the important and basic definitions, properties and characterizations of weak Armendariz rings that we need to construct the proposed algorithm. We start with the weak Armendariz definition introduced by Liu and Zhao in [12]:

Definition 2.1: A ring $\mathcal{R}$ is said to be weak Armendariz if whenever polynomials $\varphi(x) = \sum_{i=0}^{m} a_i x^i$, $\psi(x) = \sum_{j=0}^{n} b_j x^j \in \mathcal{R}[x]$ satisfy $\varphi(x)\,\psi(x) = 0$, then $a_i b_j \in \mathcal{N}(\mathcal{R})$.

The following proposition gives another characterization of weak Armendariz ring which appears in [12]:

Proposition 2.2: A ring $\mathcal{R}$ is a weak Armendariz ring if and only if, for any n, $\mathcal{T}_n(\mathcal{R})$ is a weak Armendariz ring.

The following example of weak Armendariz rings which is not Armendariz [12].

Example 2.3: Let $\mathcal{S}$ be a weak Armendariz ring. Then

$$\mathcal{R}_4 = \left\{ \begin{pmatrix} a & a_{12} & a_{13} & a_{14} \\ 0 & a & a_{23} & a_{24} \\ 0 & 0 & a & a_{34} \\ 0 & 0 & 0 & a \end{pmatrix} \middle| \, a, a_{i,j} \in \mathcal{S} \,\&\, i, j = 1,2,3,4 \right\}$$

$\in \mathcal{T}_4(\mathcal{S})$ is not Armendariz by Kim and Lee [17, Example 3] when $n \geq 4$, but $\mathcal{R}_4$ is weak Armendariz by Proposition 2.2.

3. Traditional Zero Knowledge Cryptosystem:

The objective of this section is to illustrate the original zero knowledge protocol by presenting the following classical example which is based on the Graph Non-Isomoprphism (zero-knowledge) proof that was presented by Goldreich, Micali and Wigderson in [18].

Posy is color blind. She never knows if her ribbons are identical or not. Vincent, her friend always harasses her by saying that her ribbons are not identical and she should change them. Posy needs to know if Vincent is speaking the truth about her ribbons.

- Vincent gives two ribbons, may be in different colors or not, to Posy such that she is detaining one in each hand.
- Vincent can recognize the ribbons at this stage, but Vincent doesn't tell Posy what is the color of the ribbons in each hand.
- Posy then hides the hands behind her back. Then, she either exchanges the ribbons between her hands or not, with probability 1/2 for each case (**Completeness**). Finally, she shows her hand from behind her back. Now Vincent has to speculate whether she exchanged the ribbons or not.

- By looking at the colors of the ribbons, Vincent can decide exactly if Posy exchanged the ribbons or not. On the other hand, if ribbons have identical colors and consequently cannot be distinguished, then it is impossible that Vincent speculate the correct answer which implies the probability more than 1/2 (which means that Posy is cheating). (**Soundness**)
- If Vincent and Posy repeat this stages t times (for t large enough), then Posy will be convinced if the ribbons are in fact in different colors; because if not, the probability that Vincent has succeeded at specifying all the exchanges or non-exchanges is at most 2^{-t}. (**Complexity)**
- Moreover, the proof is zero knowledge because Posy never discovers which ribbons have what color; in fact, she knows no knowledge about how to recognize the ribbons, but the proof cryptosystem helps her. (**Zero knowledge proof)**

4. Weak Armendariz Zero Knowledge Protocol:

This section is the core of this paper; our target is to put up a new idea by constructing weak Armendariz zero knowledge cryptosystem.

4.1 The Algorithm:

Assume that $\mathcal{R}$ is weak Armendariz ring and $\mathcal{R}$ is the underlying work fundamental infrastructure where $\mathcal{R}[x]$ is the polynomial ring over $\mathcal{R}$. Both of the prover and the verifier know that the ring $\mathcal{R}$ is weak Armendariz.

Step 1: In this step Key Generation can be adopted such that for any two polynomials $\varphi(x) = \sum_{i=0}^{m} a_i x^i$, $\psi(x) = \sum_{j=0}^{n} b_j x^j \in \mathcal{R}[x]$, Posy the prover computes the product of $\varphi(x)$ and $\psi(x)$, such that, $\varphi(x)\psi(x) \in \mathcal{N}(\mathcal{R}[x])$ and publishes her public key, the set $COEF = \{a_i b_j | 0 \le i \le m \text{ and } 0 \le j \le n\}$ to show Vincent the verifier that each element of the set $COEF$ is nilpotent without sharing the secret polynomial $\varphi(x)$ as Posy's private key. This polynomial is kept by the prover and never shared. Posy chooses $\varphi(x)$, $\psi(x) \in \mathcal{R}[x]$ such that $\varphi(x)\psi(x) = 0$ and sends Vincent the set $COEF = \{a_i b_j | 0 \le i \le m \ and \ 0 \le j \le n\}$.

Step 2: This step regards the beginning of the authentication process. Vincent chooses randomly $r = 0$ or 1 and sends it to Posy.

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

Step 4: Vincent checks that:
if $r = 0$, then Vincent checks that $(a_i b_j)^{k_{ij} - r} = 0$ (because Vincent knows that $\mathcal{R}$ is weak Armendariz ring & $r = 0$), which means that $a_i b_j$ is nilpotent element.

if $r = 1$, it is definitely Vincent checks that $(a_i b_j)^{k_{ij} - r} \neq 0$ (this means that $a_i b_j \notin \mathcal{N}(\mathcal{R})$ which contradicts the fact that $\mathcal{R}$ is weak Armendariz ring).

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

Example 4.2: Let $\mathcal{S}$ be a weak Armendariz ring. Then by Example 2.3 the ring

$$\mathcal{R}_4 = \left\{ \begin{pmatrix} a & a_{12} & a_{13} & a_{14} \\ 0 & a & a_{23} & a_{24} \\ 0 & 0 & a & a_{34} \\ 0 & 0 & 0 & a \end{pmatrix} \middle| a, a_{i,j} \in \mathcal{S} \ \& \ i, j = 1,2,3,4 \right\}$$

is weak Armendariz ring. Hence, for any two polynomials $\varphi(x) = \sum_{i=0}^{m} a_i x^i$, $\psi(x) = \sum_{j=0}^{n} b_j x^j \in \mathcal{R}_4[x]$, such that $\varphi(x)\psi(x) = 0$ we have that $a_i b_j \in \mathcal{N}(\mathcal{R}_4)$.

Step 1: Posy chooses $\varphi(x) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} x \in \mathcal{R}_4[x]$ as a private key

and kept it, and

$$\psi(x) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} x \in \mathcal{R}_4[x] \text{ where}$$

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

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

are the coefficients of $\varphi(x)$ and $\psi(x)$. Now, $\varphi(x)\psi(x)$ =0 and then Posy sends Vincent the set $COEF = \{a_i b_j | 0 \le i \le m \text{ and } 0 \le j \le n\} = \{a_0b_0, a_0b_1, a_1b_0, a_1b_1\} =$

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

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

Step 3: For each element of the set $COEF = \{a_i b_j | 0 \le i \le m \text{ and } 0 \le j \le n\}$ Posy found

(i) $k_{00} = 2 \in \mathbb{Z}^+$ such that, $(a_0b_0)^{k_{00}} = (a_0b_0)^2 = \begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^2 = 0,$

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

(ii) $k_{01} = 2 \in \mathbb{Z}^+$ such that $(a_0b_1)^{k_{01}} = (a_0b_1)^2 = \begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^2 = 0,$

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

(iii) $k_{10} = 2 \in \mathbb{Z}^+$ such that $(a_1b_0)^{k_{10}} = (a_1b_0)^2 = \begin{pmatrix}0&0&0&-1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^2 = 0,$

Posy sends Vincent $k_{10} = 2$ to check $(a_1b_0)^{k_{10}-r}$.

(iv) $k_{11} = 1 \in \mathbb{Z}^+$ such that $(a_1b_1)^{k_{11}} = (a_1b_1)^1 = \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^1 = 0,$

Posy sends Vincent $k_{10} = 1$ to check $(a_1b_0)^{k_{10}-r}$.

Step 4:

(i) If $r = 0$, then Vincent checks that $(a_0b_0)^{k_{00}-r} = \begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{00}-r} = 0$ (because Vincent knows that $\mathcal{R}_4$ is weak Armendariz ring & $r = 0$).

If $r = 1$, then Vincent checks that $(a_0b_0)^{k_{00}-r} = \begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{00}-r} \neq 0$ (this means that $\begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \notin \mathcal{N}(\mathcal{R}_4)$, which contradicts the fact that R_4 is weak Armendariz ring).

(ii) If $r = 0$, then Vincent 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 Vincent knows that $\mathcal{R}_4$ is weak Armendariz ring & $r = 0$).

If $r = 1$, it is definitely Vincent checks that $(a_0a_1)^{k_{00}-r} = \begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{01}-r} \neq 0$ (this means that $\begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \notin \mathcal{N}(\mathcal{R}_4)$ which contradicts the fact that $\mathcal{R}_4$ is weak Armendariz ring).

(iii) If $r = 0$, then Vincent checks that $(a_1b_0)^{k_{10}-r} = \begin{pmatrix}0&0&0&-1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{10}-r} = 0$ (because Vincent knows that $\mathcal{R}_4$ is weak Armendariz ring & $r = 0$).

If $r = 1$, it is definitely Vincent checks that $(a_1b_0)^{k_{10}-r} = \begin{pmatrix}0&0&0&-1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{10}-r} \neq 0$ (this means that $\begin{pmatrix}0&0&0&-1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \notin \mathcal{N}(\mathcal{R}_4)$ which contradicts the fact that $\mathcal{R}_4$ is weak Armendariz ring).

(iv) If $r = 0$, then Vincent checks that $(a_1b_1)^{k_{11}-r} = \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{11}-r} = 0$ (because Vincent knows that $\mathcal{R}_4$ is weak Armendariz ring &$r = 0$).

If $r = 1$, it is definitely Vincent checks that $(a_1b_1)^{k_{11}-r} = \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}^{k_{11}-r} \neq 0$ (this means that $\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} \notin \mathcal{N}(\mathcal{R}_4)$ which contradicts the fact that $\mathcal{R}_4$ is weak Armendariz ring).

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

5- Analysis of the Cryptosystem:

Two subscribers join to interact in the creation of the weak Armendariz zero knowledge algorithm, Posy the prover and Vincent the verifier. Posy tries to prove that she has the secret polynomial $\varphi(x)$ to Vincent without telling her private information about $\varphi(x)$. Then she generates a public key $\varphi(x)\psi(x) \in \mathcal{N}(\mathcal{R}[x])$, choosing the polynomial $\psi(x)$ and sends the set $COEF = \{a_i b_j \mid 0 \le i \le m \ and \ 0 \le j \le n\}$ to Vincent. On the other hand, Vincent do the same strategy, and sent his public key $r = 0$ or 1 to Posy. Now, Posy uses the property of the weak Armendariz ring and the private key $\varphi(x)$ to find the set $COEF = \{a_0 b_0,\ a_0 b_1,\ a_0 b_2, \cdots, a_1 b_0,\ a_1 b_1,\ a_1 b_2, \cdots\}$, and sends it to Vincent. To verify Posy's secret, Vincent needs to compute $(a_i b_j)^{k_{ij}-r}$. If $(a_i b_j)^{k_{ij}-r}$=0, then Vincent can convince that Posy knows the secret and the authentication process is succeed. 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.

Consequently, (1) 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 (Completeness). (2) if the verifier picks r, such that, $a_i b_j \notin N(\mathcal{R})$, then the prover cannot answer the challenge. To increase our chance of catching a cheating prover, we can repeat the challenge and response protocol. 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 (Soundness). Finally, (3) from all the analysis above, the verifier will not learn anything from the interaction apart from the fact that the statement is true (Zero Knowledge Property).

6- Conclusion

The new approach based on the algebraic structure weak Armendariz rings is proposed to show that, the zero knowledge protocols doesn't restricted to specific cases. We used weak Armendariz rings to prove that the scheme represent a zero knowledge protocol. Weak Armendariz zero knowledge protocol can be used as a method for authentication. The most important feature of this protocol 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 weak Armendariz zero knowledge protocol compared with other known protocols: completeness and soundness.

REFERENCES

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

[2] Goldreich, Micali and Wigderson Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proof, JACM, July (1991).

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

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

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

[6] L.C Guillou, J.J Quisquater, A Paradoxical Identity-Based Signature Resulting From Zero Knowledge, Crypto 88, vol.403, (1988), pp. 216-231.

[7] S. Goldwasser and Y. T. Kalai, On the (In)security of the Fiat-Shamir Paradigm, FOCS 2003: 102-107, 2003, vol. 38, no. 1, (1991), pp. 691-729.

[8] N. T. Courtois, Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank, Asiacrypt 2001, vol.2248, (2001), pp.402-411.

[9] C. Wolf, Zero-Knowledge and Multivariate Quadratic Equations, Workshop on Coding and Cryptography, (2004).

[10] E. Armendariz, A note on extensions of Baer and P.P. –rings, Journal of Austral. Math. Soc, vol.18, (1974), pp: 470-473.

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

[12] Z. Liu and R. Zhao, On Weak Armendariz Rings, Communications in Algebra, 34, (2006), pp. 2607–2616.

[13] N. M. G. Al-Saidi and M. R. M. Said, Biometric Identification Using Local Iterated Function, The European Physical Journal Special Topics 223 (8), (2014), pp. 1647-1662.

[14] N. M. G. AL-Saidi, M. Said and M. Rushdan, A new idea in zero knowledge protocols based on iterated function systems, World Applied Sciences Journal 15 (3), (2011), pp. 364-371.

[15] A. M. Abduldaim and A. M. Ajaj, A New Paradigm of the Zero Knowledge Authentication Protocol Based π-Armendariz Rings, ", IEEE International Conference on New Trends in Information & Communications Technology Applications (NTICT'2017) 7 - 9 March 2017, pp 112-117.

[16] Y. C. Jeon, H. K. Kim, Y. Lee and J. S. Yoon, On Weak Armendariz Rings, Bull. Korean Math. Soc. 46, No. 1, (2009), pp. 135–146.

[17] Nam Kyun Kim and Yang Lee, Armendariz Rings and Reduced Rings, Journal of Algebra, v. 223, (2000), 477-488.

[18] Goldreich, Micali and Wigderson in, Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proofs, Journal of the ACM, Vol 38, No 1, July (1991), pp. 691-72.

نظام التشفير زيرو نولج ارمندرايز الضعيف

اريج مصعب عبد الدائم
قسم العلوم التطبيقية
الجامعة التكنولوجية
areejmussab@gmail.com

المستخلص :

تم طرح فكرة مبتكرة باستخدام نظرية الحلقات لبناء خوارزمية جديدة لنظام التشفير زيرو نولج. في هذا البحث قدمنا لاول مرة خوارزمية لبروتوكول الزيرو نولج بالاعتماد على نوع خاص من الحلقات يسمى حلقات ارمندرايز الضعيفة. من جهة اخرى، الهدف من هذا البحث هو التركيز على فئة من الهياكل الجبرية الغير ابدالية لوصف مخطط جبري جديد لنظام الزيرو نولج باستخدام حلقات ارمندرايز الضعيفة. كنتيجة لذلك، قمنا بتوضيف حلقات ارمندرايز الضعيفة لاول مرة في علم التشفير والذي يعتبر كتطبيق جديد لهذا الصنف من الحلقات. اخيرا، قدمنا فكرة جديدة تجمع بين الجبر المجرد و علم التشفير.