α-Skew π-Armendariz Rings

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

Ahmed M. Ajaj
Department of Applied Sciences
University of Technology
Baghdad, Iraq
ahmed1985_mahmood@yahoo.com

***Abstract*—In this article we introduce a new concept called α-skew π-Armendariz rings (α-Sπ-AR)as a generalization of the notion of α -skew Armendariz rings.Another important goal behind studying this class of rings is to employ it in order to design a modern algorithm of an identification scheme according to the evolution of using modern algebra in the applications of the field of cryptography.We investigate general properties of this concept and give examples for illustration. Furthermore, this paperstudy the relationship between this concept and some previous notions related to α-skew Armendariz rings. It clearly presents that every weak α-skew Armendariz ring is α-skew π-Armendariz (α-Sπ-AR). Also, thisarticle showsthat the concepts ofα-skew Armendariz rings and α-skew π- Armendariz rings are equivalent in case R is 2-primal and semiprime ring.Moreover, this paper proves for a semicommutativeα-compatible ringR that if R[x; α] is nil-Armendariz, thenR is an α-Sπ-AR. In addition, if R is an α-Sπ-AR, 2-primal and semiprime ring, then N(R[x; α]) = N(R)[x; α]. Finally, we look forwardthat α-skew π-Armendariz rings (α-Sπ-AR)be more effect (due to their properties) in the field of cryptography than π-Armendariz rings, weak Armendariz rings and others.For these properties and characterizations of the introduced concept α -S π -AR, we aspire to design a novel algorithm of an identification scheme.**

***Keywords*— α-skew π-Armendariz rings, α-skew Armendariz rings, 2-primel rings, semiprime rings, (α, δ)- compatible rings.**

I. INTRODUCTION

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. Recently, the evolution of using the abstractions occurred as a result of the expansion of employing modern algebra in the applications of the field of cryptography. In the current time, a lot of algebraic cryptosystem schemes depend on non-commutative algebraic concepts such as; authentication, key exchange, and encryption-decryption processes are arose.

Throughout this paper we refer R to an associative ring with identity and α is a ring endomorphism of R. The ring $R[x;\alpha]$ is known as a skew polynomial ring whose elements are the polynomials over R, the addition is defined as is customary and the multiplication is defined taking into account the relation $xr = \alpha(r)x$ for any $r \in R$. The set of all nilpotent elements of R will be denote by $N(R)$. The concept of Armendariz rings arose in 1997 by Rege and Chhawchharia [1] as a generalization of reduced rings (i.e., a ring without nonzero nilpotent elements). A ring R is said to be Armendariz if for any two polynomials $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{j=0}^{n} b_j x^j \in R[x]$ satisfy $f(x)g(x) = 0$, then $a_i b_j = 0$ for each $0 \le i \le m$ and $0 \le j \le n$. Hong et al. [2]introduced the notion of α-skew Armendariz rings to be a new generalization of the conceptsα-rigid rings and Armendariz rings. A ring R is said to be α-skew Armendariz if for an endomorphism α of R any two polynomials $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{j=0}^{n} b_j x^j \in R[x;\alpha]$ satisfy $f(x)g(x) = 0$ then $a_i \alpha^i(b_i) = 0$ for each $0 \le i \le m$ and $0 \le j \le n$. Hence, every Armendariz ring is an I_R-skew Armendariz ring such that I_R is an identity endomorphism of R and consequently reduced rings impliesI_R-skew Armendariz rings. Whilst, it is possible to find an I_R-skew Armendariz ring R which is not I_R-rigid, thismeans that$R$ is not reduced ring. Moreover,any subring of an α-skew Armendariz ring is α-skewArmendariz [2].

Many generalizations of the notion of Armendariz rings arose in several trends; one of them is the concept weak Armendariz rings introduced by Liu and Zhao [3]. A ring is called weak Armendariz if whenever any two polynomials $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ in $R[x]$, satisfy $f(x)g(x) = 0$, then $a_i b_j \in N(R)$ for all i and j. Zhang and Chen [4] introduced a new generalization of weak Armendariz rings. A ring R is called weak α -skew Armendariz if for $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ in $R[x;\alpha]$, satisfy $f(x)g(x) = 0$, then $a_i \alpha^i(b_j) \in N(R)$ for all i and j. An application of the concept weak Armendariz ring can be found in [5].On the other hand, Huh et al. [6] studied a generalization of Armendariz rings, which is known asπ-Armendariz rings. A ring R is said to be a π -Armendariz ring provided that whenever $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{j=0}^{n} b_j x^j \in R[x]$ satisfy $f(x)g(x) \in N(R[x])$, then $a_i b_j \in N(R)$. According to [6], each 2-primal ring is π-Armendariz, this gives that π-Armendariz rings are a common generalization of 2-primal rings and Armendariz rings. This class of rings has been used in the application of designing a new paradigm of the zero-knowledge authentication protocol [7] and [8].All of the above motivate us to introduce the concept of α-skew π-Armendariz rings.

IJARE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

In this paper, we introduce the concept of α-skew π-Armendariz rings by combining between the concept of α-skew Armendariz rings and the concept of π-Armendariz rings.

The paper will show that the notion of α-skew π-Armendariz rings generalize that of α-skew Armendariz rings introduced by Hong et al. [2]. We study α-skew π-Armendariz of different kinds of rings. Consequently, some known results are obtained as special cases and new families of α-skew Armendariz rings are presented. Finally, the paper show that if R is a 2-primal semiprime ring, then R is an α-skew π-Armendariz ring iff R is α-skew Armendariz, and if R is an α-skew π-Armendariz, 2-primal and semiprime ring, then $N(R[x;\alpha]) = N(R)[x;\alpha]$.

The rest of this paper is organized as follows. Section II is devoted to give the new definition, some properties, examples and some general results. The conclusion and future work are given in Section III.

Not that we will denote the expression "skew (π-) Armendariz rings" by SAR (Sπ-AR).

II. DEFINITION AND GENERAL RESULTS OF α-SKEW π-ARMENDARIZ RINGS

Motivating by [2, 9, 10], in this section we introduce the concept of α-Sπ-AR and study some properties of this new class of rings.

A. Definition

Let α be an endomorphism of a ring R. A ring R is called α-skew π-Armendariz (for shortness α-S π-AR) if two polynomials $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j \in R[x;\alpha]$ such that $f(x)g(x) \in N(R[x;\alpha])$, then $a_i\alpha^i(b_i) \in N(R)$ for each $0 \le i \le m$, $0 \le j \le n$.

It is known that every Armendariz and π-Armendariz ring is id_R-Sπ-AR, where id_R is the identity endomorphism of R.

Huh et. al. in [6] proved that every subring of (π-)Armendariz rings are (π-)Armendariz. In case of α-Sπ-AR we need a restriction on the subring to inherit α-Sπ-AR property. It is well known that a subring S of a ring R is said to be invariant if $\alpha(S) \subseteq S$ for each endomorphism α of R. In particular, R is an invariant subring of $R[x,\alpha]$. For more detailed examples of the application of the mentioned notions in the field of cryptography see [5, 7, 8].

B. Proposition

Every invariant subring of an α-Sπ-AR is α-Sπ-AR.

Proof: Let S be a subring of an α-Sπ-ARR, then for any two polynomials $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{j=0}^{n} b_j x^j \in R[x;\alpha]$ satisfy $f(x)g(x) \in N(R[x;\alpha])$ implies $a_i\alpha^i(b_i) \in N(R)$ for each $0 \le i \le m$ and $0 \le j \le n$. Suppose that $p(x)q(x) \in N(S[x;\alpha])$ where $p(x) = \sum_{i=0}^{m} a_i x^i$ and $q(x) = \sum_{j=0}^{n} b_j x^j \in S[x;\alpha] \subseteq R[x;\alpha]$, hence $p(x)q(x) \in N(S[x;\alpha]) \subseteq N(R[x;\alpha])$. Since $a_i\alpha^i(b_j) \in N(R)$, then there is a positive integer k such that $(a_i\alpha^i(b_j))^k = 0$, but $a_i\alpha^i(b_j) \in S$ (because S is an invariant subring of R) which implies that $a_i\alpha^i(b_j) \in N(S)$. Therefore S is α-Sπ-AR.

Next we show that the concept of α-Sπ-AR represents a generalization of the α-SAR.

C. Proposition

Every α-SAR is α-Sπ-AR.

Proof: Assume that R is an α-SAR, then $f(x)g(x) = 0$ implies $a_i\alpha^i(b_j) = 0$, where $f(x), g(x) \in R[x;\alpha]$. Suppose that $f(x)g(x) \in N(R[x;\alpha])$, we have to prove that $a_i\alpha^i(b_j) \in N(R)$. Since R is α-SAR, then $a_i\alpha^i(b_j) = 0 \in N(R)$, therefore R is α-Sπ-AR.

It is known that every Armendariz rings and weak Armendariz rings is weak α-SAR [4]. In the following result we present the relationship between the notion of weak α-skew Armendariz rings and the notion of α-Sπ-AR.

D. Proposition

Every weak α-Sπ-AR is α-Sπ-AR.

Proof: Assume that R is weak α-SAR, so for each $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j \in R[x;\alpha]$ such that $f(x)g(x) = 0$ implies $a_i\alpha^i(b_j) \in N(R)$. Now, suppose that $f(x)g(x) \in N(R[x;\alpha])$, thus we have to prove that $a_i\alpha^i(b_j) \in N(R)$ for each i, j which is already satisfied because R is weak α-SAR. Therefore R is α-Sπ-AR.

Next we found conditions such that the converse of *Proposition D* is true.

E. Proposition

If R is an α-Sπ-AR and $R[x;\alpha]$is 2-primel semiprime ring, then R is weak α-SAR.

Proof: Assume that $f(x)g(x) = 0$ we claim $a_i\alpha^i(b_j) \in N(R)$. Since R is α-Sπ-AR, then $f(x)g(x) \in N(R[x;\alpha])$ since $R[x;\alpha]$ 2-primel semiprime we have $f(x)g(x) = 0$ so R is weak α-SAR.

F. Remark

Let α be an endomorphism of a ring R and let $M_n(R)$ be the n by n full matrix ring over R. Define an endomorphism $\bar{\alpha}: M_n(R) \to M_n(R)$ by $\bar{\alpha}((a_{ij})) = (\alpha(a_{ij}))$. It is well known that the restriction $\bar{\alpha}|T_n(R)$ of $\bar{\alpha}$ to $T_n(R)$ is an endomorphism of$T_n(R)$ where $T_n(R)$ is the $n \times n$upper triangularmatrix ring over$R$. There is no deferent if we also define$\bar{\alpha}|T_n(R)$ by $\bar{\alpha}$.

In the following result we give a new characterization α-Sπ-AR.

G. Theorem

Let α be an endomorphism of R. Then the following conditions are equivalent:

1) R is an α-Sπ-AR.
2) For any positive integer n, $T_n(R)$ is an $\bar{\alpha}$-Sπ-AR.

Proof: (1) $\Rightarrow$ (2) let $T_n(R)$ is a $\bar{\alpha}$-Sπ-AR, then$R$ is an α-Sπ-AR. Note that $T_n(R)[x;\bar{\alpha}] \cong T_n(R[x;\alpha])$. Let $f(x) = \sum_{i=0}^{p} A_i x^i$, $g(x) = \sum_{j=0}^{q} B_j x^j$ to beelements of $T_n(R)[x;\bar{\alpha}]$, $f(x)g(x) \in N(T_n(R)[x;\bar{\alpha}])$.

Let,

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

$$A_i = \begin{pmatrix} a_{11}^{(i)} & a_{12}^{(i)} & a_{13}^{(i)} & \cdots & a_{1n}^{(i)} \\ 0 & a_{22}^{(i)} & a_{23}^{(i)} & \cdots & a_{2n}^{(i)} \\ 0 & 0 & a_{33}^{(i)} & \cdots & a_{3n}^{(i)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn}^{(i)} \end{pmatrix}$$

and

$$B_j = \begin{pmatrix} b_{11}^{(j)} & b_{12}^{(j)} & b_{13}^{(j)} & \cdots & b_{1n}^{(j)} \\ 0 & b_{22}^{(j)} & b_{23}^{(j)} & \cdots & b_{2n}^{(j)} \\ 0 & 0 & b_{33}^{(j)} & \cdots & b_{3n}^{(j)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b_{nn}^{(j)} \end{pmatrix}$$

For $0 \le i \le p$ and $0 \le j \le q$. Then $f_s(x) = \sum_{i=0}^{p} a_{ss}^{(i)} x^i$ and $g_s(x) = \sum_{j=0}^{q} b_{ss}^{(j)} x^j \in N(R[x;\alpha])$ and $f_s(x)g_s(x) \in N(R[x;\alpha])$ for each $1 \le s \le n$. Since R is α-Sπ-AR, there exists some positive integer $m_{ijs} \in \mathbb{N}$ gives $\left(a_{ss}^i \alpha^i(b_{ss}^j)\right)^{m_{ijs}} = 0$for any$s, i$ and j.

Let $m_{ij} = \max\{m_{ij1}, m_{ij2}, \dots, m_{ijn}\}$. Thus

$$\left(A_i \bar{\alpha}^i(B_j)\right)^{m_{ij}} = \begin{pmatrix} a_{11}^i \alpha^i(b_{11}^j) & * & * & \cdots & * \\ 0 & a_{22}^i \alpha^i(b_{22}^j) & * & \cdots & * \\ 0 & 0 & a_{33}^i \alpha^i(b_{33}^j) & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn}^i \alpha^i(b_{nn}^j) \end{pmatrix}^{m_{ij}}$$

$$= \begin{pmatrix} 0 & * & * & \cdots & * \\ 0 & 0 & * & \cdots & * \\ 0 & 0 & 0 & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Thus $((A_i \bar{\alpha}^i(B_j))^{m_{ij}})^n = 0$. This means that $T_n(R)$ is a $\bar{\alpha}$-Sπ-AR. (2) $\Longrightarrow$(1) as all subring of a α-Sπ-AR is also α-Sπ-AR.

According to Hong et. al. and Krempa [11, 12], an endomorphism α of a ring R is said to be rigid if $a\alpha(a) = 0$implies $a = 0$for $a \in R$. A ring R is said to be an α-rigid if there exists a rigid endomorphism α of R. Note that any rigid endomorphism of a ring is a monomorphism, and α-rigid rings are reduced rings by [13]. Following [2], every α-rigid ring is an α-SARwhile the converse does not hold. The following example shows that the converse of *Proposition C* is not true in general:

H. Example

Ifα is an R-endomorphism and $R$is an α-rigid ring.Let

$$S_4 = \left\{ \begin{pmatrix} a & a_{12} & a_{13} & a_{14} \\ 0 & a & a_{23} & a_{24} \\ 0 & 0 & a & a_{34} \\ 0 & 0 & 0 & a \end{pmatrix} \middle| a, a_{ij} \in R \right\}.$$

Since S_4 is weak $\bar{\alpha}$-α-SAR[4, Example 2.6], hence S_4 is $\bar{\alpha}$-Sπ-AR by *Proposition D*, but S_4 is not $\bar{\alpha}$-α-SAR [2, Example11].

Kim [14, Example 3] proved that S_4 is not Armendariz ring and we mentioned earlier that every Armendariz ring is I_R-Sπ-AR. However, the concepts of Armendariz rings α-Sπ-ARare different as shown in the following:

I. Example

Let$R$ be an α-rigid ring and let

$$S_4 = \left\{ \begin{pmatrix} a & a_{12} & a_{13} & a_{14} \\ 0 & a & a_{23} & a_{24} \\ 0 & 0 & a & a_{34} \\ 0 & 0 & 0 & a \end{pmatrix} \middle| a, a_{ij} \in R \right\}.$$

Since S_4 is weak $\bar{\alpha}$-SAR, then S_4 is $\bar{\alpha}$-Sπ-AR by *Proposition D*.

Armendariz in [15, lemma 1] proved that any reduced ring satisfy the definition of Armendariz rings. In the next example we give an Armendariz ring which is not α-Sπ-AR, also see [16]:

J. Example

Set$\mathbb{Z}_2$to be the ring of integers mod 2, suppose that $R = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ with usual addition and multiplication. R is a commutative and reduced ring. Now let $\alpha: R \to R$ be determined by $\alpha\big((a,b)\big) = (b,a)$. R is not α-Sπ-AR for if $f(x) = (1,0) - (1,0)x, \quad g(x) = (0,1) + (1,0)x \in R[x;\alpha]$

we have

$$\begin{aligned} f(x)g(x) &= (1,0)(0,1) + (1,0)(1,0)x - (1,0)x(0,1) \\ &\quad - (1,0)x(1,0)x \\ &= (0,0) + (1,0)x - (1,0)\alpha(0,1)x - (1,0)\alpha(1,0)x^2 \\ &= (0,0) + (1,0)x - (1,0)(1,0)x - (1,0)(0,1)x^2 \\ &= (0,0) + (1,0)x - (1,0)x - (0,0)x^2 \\ &= (0,0) \in N(R[x;\alpha]) \end{aligned}$$

but

$$(1,0)\alpha((0,1)) = (1,0) \notin N(R)$$

Thus$R$ is not α-Sπ-AR.

Birkenmeier et al. [9] called a ring R 2-primal if $P(R) = N(N)$. Note that a 2-primal ring is reduced and a ring R is 2-primal if and only if $R/P(x)$ is reduced. Huh [6] proved that every 2-primal ring is π-Armendariz. This fact inspires that every 2-primal ring may be also α-Sπ-AR. But the following example eliminates the possibility.

K. Example

Let $\mathbb{Z}_2$ be the ring of integers modulo 2, suppose that $R = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ with usual addition and multiplication. R is a commutative and reduced ring, then R is Armendariz rings. Now let $\alpha: R \to R$ be determined by $\alpha\big((a,b)\big) = (b,a)$. With $(R) = \{(0,0)\}$, which implies that R is 2-primal ring. But R is not α-Sπ-AR as in *Example J*.

IJARE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

Now it is convenient to give appropriate qualifications such that the converse of *Proposition C* becomes true.

L. Proposition

Let R be a 2-primal semiprime ring. R is α-Sπ-AR iff R is α-SAR.

Proof: We suppose $f(x)g(x) = 0$ implies $a_i\alpha^i(b_j) = 0$. Since R is α-Sπ-AR, then $a_i\alpha^i(b) \in N(R)$ and since R is 2-primal semiprime ring, then $N(R) = P(R) = 0$ and we have $a_i\alpha^i(b) = 0$, so R is α-SAR.

Next we show that α-Sπ-AR and semeprime rings are different concepts as shown in the following two examples:

M. Example

Set $\mathbb{Z}_2$ be the ring of integers mod 2, suppose that $R = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ with usual addition and multiplication. R is a commutative and reduced ring, then R is 2-primal with $N(R) = 0$ which implies that R is semiprime ring. However R is not α-Sπ-ARas shown in *Example J*.

N. Example

Let R be the following ring:

$$R = \left\{ \begin{pmatrix} a & t \\ 0 & a \end{pmatrix} | a \in \mathbb{Z}, t \in \mathbb{Q} \right\}$$

where $\mathbb{Z}$ is the set of all integers and $\mathbb{Q}$ is the set of all rational numbers. Let σ be an automorphism defined by $\sigma\left(\begin{pmatrix} a & t \\ 0 & a \end{pmatrix}\right) = \begin{pmatrix} a & \frac{t}{2} \\ 0 & a \end{pmatrix}$. Then R is α-SAR [2] and hence $R\alpha$-Sπ-AR, but R is not semiprime [17].

Due to Antoine [18, Corollary 5.3], if R is an Armendariz ring then $N(R[x]) = N(R)[x]$. In addition, the following result given by Ouyang and Birkenmeier [19]:

O. Corollary

Let R be an $(\alpha;\delta)$-compatible 2-primal. Then we have the following:

(1) $N(R[x;\alpha;\delta])$ is an ideal.

(2) $N(R[x;\alpha;\delta]) = N(R)[x;\alpha;\delta]$

In particular, if R is an α-compatible ring, then $N(R[x;\alpha])$ is an ideal and $N(R[x;\alpha]) = N(R)[x;\alpha]$

In case of α-Sπ-AR, we have the following:

P. Theorem

If R is an α-Sπ-AR, 2-primal and semiprime ring, then $N(R[x;\alpha]) = N(R)[x;\alpha]$.

Proof: To prove that $N(R)[x;\alpha] \subseteq N(R[x;\alpha])$, let $f(x) = \sum_{i=0}^{m} a_i x^i \in N(R)[x;\alpha]$, and let $t > 1, a_i^t = 0$, each $i = 0, \dots, m$. We suppose $f^{(m+1)t}(x) = 0$. We can write the coefficients of $f^{(m+1)t}(x)$ as sums of terms of $(m+1)t$ in the $\alpha^l(a_i)$'s. Consider one of these, as follows:

$$a_{i_1}\alpha^{i_1}(a_{i_2})\alpha^{i_1+i_2}(a_{i_3}) \dots \alpha^{i_1+\cdots+i_{(m+1)t-1}}\left(a_{i_{(m+1)t}}\right) \quad 0 \le i_u \le m. \quad \dots\dots\dots\dots \quad (1)$$

It must contain at least t occurrences of some a_j, for some $0 \le j \le m$. Suppose $a_{i_{r_1}} = \cdots = a_{i_{r_t}} = a_j$, for some $1 \le r_1 < \cdots < r_t \le (m+1)t$. Let

$$p_{i_s}(x) = 1 - a_{i_s}x,$$
$$q_{i_s}(x) = 1 + a_{i_s}x + a_{i_s}\alpha(a_{i_s})x^2 + \cdots + a_{i_s}\alpha(a_{i_s}) \dots \alpha^{t-2}(a_{i_s})x^{t-1}$$

By polynomials $R[x;\alpha]$, for each $i_s \notin \{i_{r_t}, \dots, i_{r_t}\}$. $a_{i_s}^t = 0, p_{i_s}(x)q_{i_s}(x) = 1$, for each i_s. *Let* $\alpha(o(x)) = \sum_{i=0}^{u} \alpha(v_i)x^i$, for any $o(x) = \sum_{i=0}^{u}(v_i)x^i \in R[x;\alpha]$. Now, by replacing all a_{i_s} by the product $p_{i_s}(x)q_{i_s}(x)$ *in Eq. (1),* and considering the fact $a_j^t = 0$, we have that

$$p_{i_1}q_{i_1} \dots \alpha^{i_1+\cdots+i_{r_1-1}}(a_j) \dots \alpha^{i_1+\cdots+i_{r_t-1}}(a_j) \dots \alpha^l\left(p_{i_{r_{(m+1)t}}}\right)$$
$$\alpha^l\left(q_{i_{r_{(m+1)t}}}\right) = 0,$$

Where $l = i_1 + \cdots + i_{(m+1)t-1}$. Thus $a_{i_1}\alpha^{i_1}(a_{i_2})\alpha^{i_1+i_2}(a_{i_3}) \dots \alpha^l\left(a_{i_{(m+1)t}}\right) = 0$ which implies that $f^{(m+1)t}(x) = 0$ which means that $f(x) \in N(R[x;\alpha])$.

Lunqun et al. [10] introduced the concept of skew π-Armendariz rings. A ring R is called skew π-Armendariz (Sπ-AR) if $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{j=0}^{m} b_j x^j \in R[x;\alpha,\delta], f(x)g(x) \in N(R[x;\alpha,\delta])$ implies $a_i b_j \in N(R)$ for all i, j. Authors showed that every π-Armendariz ring is Sπ-ARby [10], where $\alpha = id_R$ and δ is zero mapping. The following example provides a non-Sπ-AR.

Q. Example

Let R be a ring and let $J = Mat_2(R)$ and let

$$f(x) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}x \quad , \quad g(x) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}x$$

be two polynomials in $J[x; id_J]$. Then $f(x)g(x) = 0 \in N(J[x; id_J, 0])$.

But

$$\begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} \notin N(R).$$

Thus J is not Sπ-AR.

The following result shows that our definition α-Sπ-ARrings represents a generalization of a Sπ-AR.

R. Proposition

Each Sπ-ARis α-Sπ-AR.

Proof: Let R be a Sπ-ARand let $f(x) = \sum_{i=0}^{m} a_i x^i, g(x) = \sum_{j=0}^{n} b_j x^j \in R[x;\alpha,0]$ with $f(x)g(x) \in N(R[x;\alpha,0])$. Note that $a_i b_j \in N(R)$ for each i and j. We claim that $a_i\alpha^i(b_j) \in N(R)$ each i, j. Now

$$f(x)g(x) = a_0(b_0 + b_1x + \cdots + b_nx^n) + (a_1x + \cdots + a_mx^m)(b_0 + b_1x + \cdots + b_nx^n$$
$$= (a_1x + \cdots + a_mx^m)(b_0 + b_1x + \cdots + b_nx^n)$$

because $a_0 b_j \in N(R)$ for all $0 \le j \le n$, so we get

$$= (a_1 + a_2x + \cdots + a_mx^{m-1})x(b_0 + b_1x + \cdots + b_nx^n)$$

IJARE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

$$= (a_1 + a_2x + \cdots + a_mx^{m-1})(\alpha(b_0)x + \alpha(b_1)x^2 + \cdots + \alpha(b_n)x^{n+1}.$$

Put

$f_1(x) = a_1 + a_2x + \cdots + a_mx^{m-1}$ and $g_1(x) = \alpha(b_0)x + \alpha(b_1)x^2 + \cdots + \alpha(b_n)x^{n+1}$.

Then $f_1(x)g_1(x) \in N(R[x;\alpha])$ implies $a_i\alpha(b_j) \in N(R)$ all $1 \le i \le m,\ 0 \le j \le n$ where R is Sπ-AR. Hence,

$$f_1(x)g_1(x) = a_1(\alpha((b_0)x + \alpha(b_1)x^2 + \cdots + \alpha(b_n)x^{n+1} + (a_2x + \cdots + a_mx^{m-1})(\alpha(b_0)x + \alpha(b_1)x^2 + \cdots + \alpha(b_n)x^{n+1})$$

$$= (a_2x + \cdots + a_mx^{m-1})(\alpha(b_0)x + \alpha(b_1)x^2 + \cdots + \alpha(b_n)x^{n+1})$$

$$= (a_2 + a_3x + \cdots + a_mx^{m-2})(\alpha^2(b_0)x^2 + \alpha^2(b_1)x^3 + \cdots + \alpha^2(b_n)x^{n+2}).$$

Put

$f_2(x) = a_2 + a_3x + \cdots + a_mx^{m-2}$ and $g_2(x) = \alpha^2(b_0)x^2 + \alpha^2(b_1)x^3 + \cdots + \alpha^2(b_n)x^{n+2}$.

Then $f_2(x)g_2(x) \in N(R[x;\alpha])$ implies $a_i\alpha^2(b_j) \in N(R)$ each $2 \le i \le m$ and $0 \le j \le n$ where R is Sπ-AR. Continuing this process, we get that $a_i\alpha^i(b_j) \in N(R)$ for each $2 \le i \le m$, $0 \le j \le n$. Thus, R is α-Sπ-AR.

Note that if $\alpha = id_R$, then the concept of Sπ-AR is equivalent to the concept of α-Sπ-AR. But if $\alpha \neq id_R$, then the converse is not true in general.

The relationship betweenα-Sπ-ARand nil-Armendariz rings [20] will be shown in the following example:

A. Example

Let $\mathbb{Z}_2$ be the ring of integers modulo 2, suppose that $R = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ with the usual addition and multiplication. Then R is reduced, hence R is Armendariz. Consequently R is nil-Armendariz, by [20]. But R is notα-Sπ-ARas in *Example J*.

Recall that a ring R is called semicommutative if for any $a, b \in R, ab = 0$ implies $aRb = 0$. Liang et. al. [21] introduced the concept of α-condition, a ring R is said to satisfy α-condition whenever $ab = 0$ if and only if $a\alpha(b) = 0$ for each $a, b \in R$.

The following needed Lemma appears in [22]:

B. Lemma

Let α be an endomorphism of a semicommutative ring R. If R satisfies α-condation, then $N(R[x;\alpha]) = N(R)[x;\alpha]$.

Next we study the relationship between the concept of nil-Armendariz rings and the concept of α-Sπ-AR.

C. Theorem

Let R be a semicommutative α-compatible ring if $R[x;\alpha]$ is nil-Armendariz, then R is an α-Sπ-AR.

Proof: Assume that $f(x) = \sum_{i=0}^{m} a_ix^i$ and $g(x) = \sum_{j=0}^{n} b_jx^j \in R[x;\alpha]$ with $f(x)g(x) \in N(R)[x;\alpha] = N(R[x;\alpha])$. By lemma 3.5 we have to prove that $a_i\alpha^i(b_j) \in N(R)$. Then we have

$$c_k = a_0b_k + a_1\alpha(b_{k-1}) + \cdots + a_k\alpha^k(b_0) \in N(R),$$

All $0 \le k \le m + n$ where c_k is the coefficients of $f(x)g(x)$. Now, let

$$F(y) = a_0 + (a_1x)y + (a_2x^2)y^2 + \cdots + (a_mx^m)y^m,$$

$$G(y) = b_0 + (b_1x)y + (b_2x^2)y^2 + \cdots + (b_nx^n)y^n$$

By polynomials in $R[x;\alpha][y]$. Also we have

$$F(y)G(y) = \sum_{k=0}^{m+n} (c_kx^k)y^k$$

Therefore

$$c_kx^k \in N(R[x;\alpha]),$$

All $0 \le k \le m + n$, since $c_k \in N(R)$ and R is α-compatible. So $a_ix^ib_jx^j \in N(R[x;\alpha])$, for each $0 \le i \le m, 0 \le j \le n$, where $R[x;\alpha]$ is nil-Armendariz. Hence $a_i\alpha^i(b_j)x^{i+j} \in N(R[x;\alpha])$ and so $a_i\alpha^i(b_j) \in N(R)$. Hence R is α-Sπ-AR.

III. CONCLUSION AND FUTURE WORK

This work introduced a new generalization of the concept of α-SAR rings which is called α-Sπ-AR. The main important result proved that a ring$R$ is an α-Sπ-ARif and only if for any positive integer n, the ring $T_n(R)$ is $\bar{\alpha}$-S π-AR. This characterization will enable us to find a large number of numerical examples in order to use in the application fields.

For the given proved properties and characterizations of the introduced concept α-Sπ-AR, we can design a novel algorithm of an identification scheme. To simulate this algorithm, we have to use a numerical example to explain the details. Moreover,we anticipate that the complexity will be increased depending on this type of rings.

REFERENCES

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

[2] C.Y. Hong, N. K. Kim and T. K. Kwak, On Skew Armendariz Rings, *Communications in Algebra*, 31 (2003), 103-122.

[3] Z. Liu and R. Zhao, On weak Armendariz rings,*Communications in Algebra*, 34 (2006), 2607-2616.

[4] C. Zhang and J. Chen, Weak α-Skew Armendariz Rings,*J. Korean Math. Soc.*,47 (2010), 455-466.

[5] A.M. Abduldaim, Weak Armendariz Zero Knowledge Cryptosyste, *Journal of Al-Qadisyah for Computer Science and Mathematics*, 9 (2017), 2, 1 - 6.

[6] C. Huh, C. I. Lee, K. S. Park and S. J. Ryu, On π-Armendariz Ring, *Bull. Korean Math. Soc.*,44 (2007), 641-649.

[7] A.M. Abduldaim and A.M. Ajaj, A new paradigm of the zero-knowledge authentication protocol based π-Armendariz ring, *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad, Iraq*, 2017, 97-104. doi: 10.1109/NTICT.2017.797614.

IJARE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

[8] A. M. Abduldaim, N. Al-Saidi, "Generalized π-Armendariz Authentication Cryptosystem," World Academy of Science, Engineering and Technology, International Science Index 129, *International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering*, vol.11, no. 9, pp: 393 – 398, 2017.

[9] G.F. Birkenmeier, H.E. Heatherly and E. K. Lee, Completely prime ideals and associated radicals, *in (eds. S. K. Jain, S. T. Rizvi) Ring Theory (Granville, OH, 1992), World Scientific, Singapore and River Edge*, *MR 96e:16025*, 373 (1993), 102 - 129.

[10] O. Lunqun, L. Jinwang and X. Yueming, Ore Extensions of Skew π -Armendariz Rings, *Bulletin of the Iranian Mathematical Society*, 39 (2013), 255 - 368.

[11] J. Krempa, Some examples of reduced rings, *Algebra Colloq*.,3 (1996), 289-300.

[12] C.Y. Hong, T.K. Kwak and S.T. Rizvi, Rigid ideals and radicals of Ore extensions, *Algebra Colloq.*,12 (2005), 399-412.

[13] Y. Chan, K. Nam and K. Tai, Ore extensions of Baer and p.p.-rings, *J. Pure Appl. Algebra*, 151 (2000), 215-226.

[14] N. K. Kim, Armendariz Rings and Reduced Rings,*Journal of Algebra,* 223 (2000), 477-488.

[15] E. Armendariz, A note on extensions of Baer and P.P. -rings, *Journal of Austral. Math. Soc*, 18(1974), 470-473.

[16] A. M. Abduldaim and A. M. Ajaj, Examples of α-Skewπ-Armendariz Rings, *Iraqi Journal of Science*, 2017, Vol. 58, No.1C, pp: 482-489.

[17] C. Hong, N. Kim and Y. Lee, Skew Polynomial Rings over Semiprime Rings, *J. Korean Math. Soc.,*47 (2010), 879 - 897.

[18] R. Antoine, Nilpotent Elements and Armendariz Rings, *Journal of Algebra*319 (2008), 3128 - 3140.

[19] L. Ouyang and G. F. Birkenmeier, Weak Annihilator over Extension Rings, *Bull. Malays. Math. Sci. Soc.*, 35(2012), 345 - 357.

[20] R. Antoine, "Nilpotent elements and Armendariz Rings", *Journal of Algebra*, Vol.319,pp: 3128-3140, 2008.

[21] L. Liang, L. Wang and Z. Liu, On a Generalization of Semicommutative Rings, *Taiwanese Journal of Mathematics*, 11(2007), 1359 - 1368.

[22] W. Chen, On Nil-semicommutative Rings,*Thai Journal of Mathematics*,9(2011),39-47.

IJARE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)