Comp. Appl. Math. (2017) 36:843–857
DOI 10.1007/s40314-015-0265-9

Design of new 4 × 4 S-box from finite commutative chain rings

Tariq Shah[1] · **Saira Jahangir**[1] · **Antonio Aparecido de Andrade**[2]

Received: 4 February 2015 / Accepted: 18 July 2015 / Published online: 9 August 2015

Abstract Substitution boxes (S-boxes) are the fundamental mechanisms in symmetric key cryptosystems. These S-boxes guarantee that the cryptosystem is cryptographically secure and make them nonlinear. The S-boxes used in conventional and modern cryptography are mostly constructed over finite Galois field extensions of binary Field $\mathbb{F}_2$. We have presented a novel construction scheme of S-boxes which is based on the elements of subgroups of multiplicative groups of units of the commutative finite chain rings of type $\frac{\mathbb{F}_2[u]}{\langle u^k \rangle}$, where $2 \leq k \leq 8$. Majority logic criterion (MLC) is applied on the apprehended S-boxes owing to, checked their strength.

Keywords S-box · Finite chain ring · Unit elements · Subgroup of order 16 · Majority logic criterion

Mathematics Subject Classification 34H10 · 74H65 · 90B06

Communicated by Antonio José Silva Neto.

This work was partially supported by Fapesp 2013/25977-7.

✉ Antonio Aparecido de Andrade
andrade@ibilce.unesp.br

Tariq Shah
stariqshah@gmail.com

Saira Jahangir
saira156@gmail.com

[1] Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

[2] Department of Mathematics, São Paulo State University, São José do Rio Preto, São Paulo, Brazil

1 Introduction

Throughout we consider the ring associative, commutative and with identity. A local finite ring $\mathcal{R}$ is a chain ring if and only if the radical $\mathcal{M}$ of $\mathcal{R}$ is a principal ideal, and therefore $\frac{\mathcal{R}}{\mathcal{M}}$ is the residue field. Accordingly the ideals of a chain ring form a chain. Basic examples of such rings having cardinality $q = p^n$, where p is prime and n is a positive integer, are $\mathbb{Z}_q$, the ring of integers modulo q, and the Galois field $GF(q) = \mathbb{F}_q$. Moreover a wide-ranging class of finite chain rings is the Galois rings. The Galois ring $GR(q, r) = \frac{\mathbb{Z}_q[x]}{\langle f(x)\rangle}$, where $f(x) \in \mathbb{Z}_q[x]$ is r degree monic irreducible polynomial modulo q which is also irreducible modulo p, has cardinality q^r. The radical $\mathcal{M}$ is maximal ideal of the ring $\mathcal{R} = GR(q, r)$ consisting of nilpotent elements; however, the residue field $\frac{\mathcal{R}}{\mathcal{M}}$ is the Galois field $GF(q)$. Another class of chain ring is the factor ring $\frac{GF(q)[x]}{\langle x^k\rangle} = \sum_{i=0}^{k-1} x^i GF(q)$. Clark and Liang (1973) associate with each finite chain ring five invariants (integers) and determine (in certain cases) the number of isomorphism classes of rings with given invariants.

Shifting codes symbols from a finite Galois field $GF(q)$ to a finite chain ring defined a new role of maximal cyclic subgroup $\mathcal{G}_s$ of the group of units of a Galois ring $GR(q, r)$ at the place of cyclic Galois group $GF(q)^*$. In this regard, primarily Shankar (1979) gives a construction technique of a BCH code over a local ring $\mathbb{Z}_q$ with the advantage of maximal cyclic subgroup $\mathcal{G}_s$ of the group of units of the Galois extension ring $GR(q, r)$ of the local ring $\mathbb{Z}_q$. In Shankar (1979), she explained the existence of this maximal cyclic subgroup $\mathcal{G}_s$ and it is due to the modulo p reduction map from the ring $\mathbb{Z}_q$ to the prime field $GF(p)$. The focus in Shankar (1979) is to construct a BCH code through the maximal cyclic subgroup $\mathcal{G}_s$. Though, Shanbhag et al. (1996) discuss exponential sums and an upper bound for hybrid sum over the Galois rings by the usage of maximal cyclic subgroups of the groups of units of these Galois rings [see also Cohen and Niederreiter (2009)]. Later, Andrade and Palazzo (1999), with the help of maximal cyclic subgroup $\mathcal{G}_s$ give a construction and decoding schemes of BCH codes over a finite commutative ring. In continuation to Andrade and Palazzo (1999), Shah et al. (2012a, b) discuss a construction and decoding technique over a sequence of BCH codes by means of the chain of maximal cyclic subgroups of the chain of groups of units of Galois rings.

Recently, in coding theory the finite chain rings of type $\frac{\mathbb{F}_q[x]}{\langle x^k\rangle}$ are used for the construction of cyclic codes. Bonnecaze and Udaya (1999) set a trend in coding theory to construct cyclic and self dual codes on the four elements chain ring $\mathbb{F}_2 + u\mathbb{F}_2$. Meanwhile numerous code theorist have used these type of rings to design codes, e.g. in Qian et al. (2006) constacyclic and cyclic codes are constructed over finite chain ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, while the construction of cyclic codes over finite chain rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ is discussed in Abualrub and Saip (2007). The simplex codes over the finite chain ring $\sum_{n=0}^{s} u^n\mathbb{F}_2$ are investigated in Al-Ashker (2005), however simplex codes having symbols from four elements chain ring $\mathbb{F}_2 + u\mathbb{F}_2$ are given in Al-Ashker (2005). The cyclic codes over chain ring $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$ are addressed in Al-Ashker and Hamoudeh (2011), whereas $(1+u)$ constacyclic and cyclic codes over chain ring $\mathbb{F}_2 + u\mathbb{F}_2$ are presented in Qian et al. (2006). While the linear codes over finite chain ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ of constant Lee weight are considered in Naji (2002). Though in more general setting, the cyclic codes over finite chain ring $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$ are introduced in Qian et al. (2005), however, ultimately in almost with complete sense, in Al-Ashker and Chen (2013) cyclic codes of arbitrary length are designed over finite chain ring $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{k-1}\mathbb{F}_q$. Also, on negacyclic and constacyclic codes over finite chain rings is given in Abu Dahrouj (2008).

A usual succession from the theory of single output Boolean function is the extension of that theory to multiple output Boolean functions, together referred as an S-box. The link between the input and the output bits in terms of dimension and exclusivity gives rise to various types of S-boxes. An $n \times m$ S-box is a mapping $\varsigma : \mathbb{F}_2^n \to \mathbb{F}_2^m$ from n input binary bits to m output binary bits, however, respectively there are 2^n and 2^m number of inputs and outputs. Thus, an S-box is simply a set of m single output Boolean functions combined in a fixed order. The dimension of an S-box will have an effect on the distinctness of the output and the input which may influence the properties of S-box. S-box with dimension $n \times m$, where $n < m$, such that the number of input bits are lesser than output bits, then some entries in the S-box must be repeated. While, an $n \times m$ S-box for $n = m$, may either contain distinct entries where each input is mapped to distinct output or repeat some entries of the S-box. The S-boxes which are both injective and surjective are called bijective S-boxes and these are reversible Hussain and Shah (2013).

These S-boxes are the fundamental part in almost all the cryptosystems. The significant portion of the time spent on design and analysis is focused on the S-boxes because it is the only nonlinear part of the algorithm. Thus severe weaknesses in the S-boxes can therefore lead to a cryptosystems which are easily broken. The S-boxes are used as a gauging device to confirm the strength of cryptographic algorithms. Accordingly the construction of S-boxes must be cryptographically strong in order to protect the cryptosystems. Several constructions and criteria are suggested in literature to synthesize S-boxes. The Rijndael Daemen and Rijmen (2000) S-box is based on the mapping $x \to x^{-1}$, where x^{-1} denotes the multiplicative inverse of x in the field $\mathbb{F}_{2^m}$ and there are several methods to calculate multiplicative inverse in the field $\mathbb{F}_{2^8}$. Whereas in Gupta and Sarkar (2005) an algorithm is given by which the calculations of multiplicative inverses in the field $\mathbb{F}_{2^8}$ are reduced to the finding multiplicative inverses in the field $\mathbb{F}_{2^4} = GF(2^4)$. Adams and Tavares (1990) describe a construction technique for the bijective highly nonlinear S-boxes; however, an improved construction method for nonlinear resilient S-boxes is given in Gupta and Sarkar (2005).

In archetypal and modern cryptography S-boxes are typically constructed over finite Galois fields $\mathbb{F}_{2^m}$, for $2 \leq m \leq 8$, such as AES S-box, residue prime S-box Hussain et al. (2011), Gray S-box Tran et al. (2008), APA S-box Cui and Cao (2007), S_8 AES S-box, Skipjack S-box Kim and Phan (2009), Xyi S-box Yi et al. (2002) and perfect nonlinear S-box Nyberg (1991).

Side-channel analysis exploits the information leaked during the computation of a cryptographic algorithm. Threshold implementations are a kind of side-channel attacks counter measures, based on secret sharing schemes and techniques from multiparty computation, accordingly in Bilgin et al. (2012) a procedure is devised by which the Boolean functions are derived for all 3×3 and 4×4 S-boxes. Practically all of services of finite local rings are in the coding theory; however, in this study our aim is to use the finite local rings in cryptography and launch a new construction scheme of S-boxes. Primarily, Shah et al. (2013) has given a construction technique of S-boxes by the use of maximal cyclic subgroups G_3 and G_{15} of groups of units of the Galois rings $GR(2^2, 2)$ and $GR(2^2, 4)$. Whereas, the maximal cyclic subgroups G_3 and G_{15} of orders 3 and 15 are, respectively, isomorphic to the cyclic Galois groups $\mathbb{F}^*_{2^2}$ and $\mathbb{F}^*_{2^4}$. The connection of maximal cyclic subgroup with agreeing cyclic Galois group, which is because of the modulo p reduction map from local ring $\mathbb{Z}_{p^n}$ to its residue field $\mathbb{F}_p$, helps in construction of the S-boxes over maximal cyclic subgroup. S-box constructed in this way, upsurges in complexity of encryption and decryption. In continuation to Shah et al. (2013), this study proposes a novel construction technique of 4×4 S-boxes, which shifts the role of finite Galois fields $\mathbb{F}_{2^k}$, for $2 \leq k \leq 8$ to the finite chain rings $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u_2^{k-1}\mathbb{F}_2$, for $1 \leq k \leq 8$. Regardless of the construction of Shah et al. (2013), advantageously the bits

involved in this new S-boxes construction are consisting on the binary digits. The Majority logic criterion (MLC) is used to measure the effectiveness of newly constructed S-boxes.

Rest of the discussion is systematized as follows. The basic notions in chain rings are presented in Sect. 2. In Sect. 3, we describe the mechanism of designing S-boxes through the multiplicative groups and subgroups of these multiplicative groups of finite chain rings. Section 4, deals with the MLC applied on proposed S-boxes, whereas in Sect. 5, concluding remarks are given.

2 Preliminaries

Let $\mathcal{R}$ be a ring. An element v is unit in $\mathcal{R}$ if there exists an element w in $\mathcal{R}$ such that $vw = 1$, where 1 is the identity of $\mathcal{R}$. Unit elements of a ring form a multiplicative group. A non-zero element a is a zero divisor in $\mathcal{R}$ if there exists a non-zero element b in $\mathcal{R}$ such that $ab = 0$. A nonzero element a is said to be nilpotent element in $\mathcal{R}$ if there exists a positive integer k such that $a^k = 0$. The least positive integer k with this property is known as the nilpotency index a.

A ring $\mathcal{R}$ is local if and only if its all non-unit elements form an additive Abelian group. More unambiguously a local ring $\mathcal{R}$ has a unique maximal ideal $\mathcal{M}$ and the factor ring $\frac{\mathcal{R}}{\mathcal{M}}$ is its residue field.

A local finite ring $\mathcal{R}$ is a chain ring if and only if the radical $\mathcal{M}$ of $\mathcal{R}$ is a principal ideal (consists of all multiples of a fixed element of $\mathcal{R}$ and this fixed element is called the generator of the ideal), and therefore, the factor ring $\frac{\mathcal{R}}{\mathcal{M}}$ is a field. Thus ideals of a chain ring form a chain. The famous examples of such rings are $\mathbb{Z}_{p^n}$, the ring of integers modulo p^n where p is prime, and the Galois field $GF(p^n) = \mathbb{F}_q$ with $q = p^n$ elements. Another large class offinite chain rings is the Galois rings $GR(p^n, r) = \frac{\mathbb{Z}_{p^n}[x]}{\langle f(x)\rangle}$, where $f(x) \in \mathbb{Z}_{p^n}[x]$ is a monic irreducible polynomial of degree r generates the principal ideal $\langle f(x)\rangle$. However $f(x)$ is also irreducible modulo the prime p, i.e., $f(x)$ is the basic irreducible polynomial. Whereas the Galois ring $\mathcal{R} = GR(p^n, r)$ has p^{nr} number of elements and an element $\overline{a}(x)$ in $GR(p^n, r)$ has the representation $\overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_{r-1}x^{r-1}$, where $\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_{r-1} \in \mathbb{Z}_{p^n}$. The radical $\mathcal{M}$ is the set of nilpotent elements of $\mathcal{R}$ and the residue field $\frac{\mathcal{R}}{\mathcal{M}}$ of $\mathcal{R}$ is the Galois extension field $GF(p^r)$. One of the typical class of chain rings is the factor ring $\frac{GF(p^r)[x]}{\langle x^k\rangle}$ of Euclidean domain $GF(p^r)[x]$. The finite chain ring $\frac{GF(p^r)[x]}{\langle x^k\rangle} = \frac{\mathbb{F}_{p^r}[x]}{\langle x^k\rangle}$ has the representation $\mathbb{F}_{p^r} + x\mathbb{F}_{p^r} + \cdots + x^{k-1}\mathbb{F}_{p^r}$.

Let R_k be the representation of finite chain ring $\frac{\mathbb{F}_2[u]}{\langle u^k\rangle} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$. The ring R_k has 2^k number of elements. The element u is the nilpotent element with nilpotency index k, i.e., $u^k = 0$. Thus it follows that $\langle 0\rangle = u^k R_k \subset u^{k-1}R_k \subset \cdots \subset u^2 R_k \subset uR_k \subset R_k$ is the ascending chain of ideals in R_k, and therefore, R_k is a local ring with only maximal ideal uR_k. Whereas, $\frac{R_k}{uR_k} \simeq \mathbb{F}_2$ is the residue field of the chain ring R_k. The ideals $u^i R_k$ and $u^{i+1}R_k$, where $i = 0, 1, 2, \ldots, k-1$, respectively, have the cardinality 2^{k-i} and 2^{k-i+1}. Thus the cardinality of $u^i R_k$ is 2 times the cardinality of $u^{i+1}R_k$.

Amongst the rings of four elements, earlier the Galois field $\mathbb{F}_4$, and later the integers modulo 4 ring $\mathbb{Z}_4$, are frequently used in algebraic coding theory. Recently, Abualrub and Saip (2007) studied cyclic codes of an arbitrary length n over the rings $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, \overline{u} = 1 + u\}$, with $u^2 = 0$, and $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 = \{0, 1, u, u^2, 1 + u, 1 + u^2, u + u^2, 1 + u + u^2\}$, with $u^3 = 0$. However, Al-Ashker and Hamoudeh (2011) extend these results to more general

Table 1 × and + Tables for $\mathbb{F}_2 + u\mathbb{F}_2$

×	0	1	u	$\overline{u}$	+	0	1	$\overline{u}$	u
0	0	0	0	0	0	0	1	$\overline{u}$	u
1	0	1	u	$\overline{u}$	1	1	0	u	$\overline{u}$
u	0	$\overline{u}$	1	u	$\overline{u}$	$\overline{u}$	u	0	1
$\overline{u}$	0	u	u	0	u	u	$\overline{u}$	1	0

rings of the form $R_k = \mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u_2^{k-1}\mathbb{F}_2$, with $u^k = 0$. The ring $\mathbb{F}_2 + u\mathbb{F}_2$ share some good properties of both $\mathbb{Z}_4$ and $\mathbb{F}_4$. The alphabet in the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is given to all binary polynomials in indeterminate u of degree at most 1, and is closed under binary polynomial addition and multiplication modulo u^2. The multiplication and addition tables for the ring $\mathbb{F}_2 + u\mathbb{F}_2$ are given in Table 1. The multiplication table of the ring $\mathbb{F}_2 + u\mathbb{F}_2$ coincides with that of $\mathbb{Z}_4$, when u and $\overline{u}$ are replaced by 2 and 3, respectively. In this sense $\mathbb{F}_2 + u\mathbb{F}_2$ is analogous to $\mathbb{Z}_4$ and here u plays the role of 2. Whereas the addition table is different and is similar to that of the Galois field $\mathbb{F}_4 = \{0, 1, \beta, \beta^2 = 1 + \beta\}$, where $\overline{u}$ and u are replaced by β and β^2, respectively.

3 S-box construction through finite chain rings $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$

The chain ring $R_k = \frac{\mathbb{F}_2[u]}{\langle u^k \rangle} = \mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$ has cardinality 2^k. As u is a nilpotent element with nilpotency index k, it follows that $\langle 0 \rangle = u^k R_k \subset u^{k-1} R_k \subset \cdots \subset uR_k \subset R_k$. Accordingly the residue field of R_k is $\frac{R_k}{uR_k} \simeq \mathbb{F}_2$. The ring R_k shares some properties of the local ring $\mathbb{Z}_{2^k}$ and the Galois field $\mathbb{F}_{2^k}$. More explicitly the multiplication binary operation of R_k coincides with of $\mathbb{Z}_{2^k}$, whereas the addition binary operation is similar to that of $\mathbb{F}_{2^k}$.

A significant S-box with wide-ranging cryptographic features is of ultimate worth for the development of resilient cryptographic system. Constructing cryptographically strong S-boxes is a basic challenge. In this study we propose a method to amalgam an efficient 4 × 4 S-box based on unit elements of the chain rings $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$. For the purpose we fix k to 2, 3, 4, 5, 6, 7 and 8. The 4 × 4 S-box construction steps are given bellow:

1. Table M_{G_k} the multiplicative group of unit elements of the ring R_k.
2. If the cardinality of M_{G_k} is a perfect square and less than or equal to 16 define an inversion map $f : M_{G_k} \to M_{G_k}$ and a linear scalar multiple function $g : M_{G_k} \to M_{G_k}$. Otherwise choose a subgroup H_{G_k} of M_{G_k} of desired size 16 and then define these two bijective maps f and g from H_{G_k} to H_{G_k}. The selection of subgroups and defined maps for each ring are explicitly explained in subsections.
3. Take the composition of the maps f and g.
4. Generate 4 × 4 S-box by arranging them row wise.

3.1 Construction of S-box through multiplicative group of R_3

The chain ring $R_3 = \frac{\mathbb{F}_2[u]}{\langle u^3 \rangle} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ has 8 number of elements. The chain of ideals of this ring is $\langle 0 \rangle = u^3 R_3 \subset u^2 R_3 \subset uR_3 \subset R_3$ and $\frac{R_3}{uR_3} \simeq \mathbb{F}_2$ is its residue field. The multiplication binary operation of R_3 coincides with of $\mathbb{Z}_8$, whereas the addition binary operation is similar to that of $\mathbb{F}_8$ (Table 2).

Table 2 Elements in R_3

Sr. No.	Polynomial	Binary string
1	0	000
2	1	100
3	u	010
4	u^2	001
5	$1+u$	110
6	$1+u^2$	101
7	$u+u^2$	011
8	$1+u+u^2$	111

Table 3 Elements in $(f \circ g)(M_{G_3})$

Sr. No.	Polynomial
$(f \circ g)(2)$	111
$(f \circ g)(5)$	101
$(f \circ g)(6)$	110
$(f \circ g)(8)$	100

Table 4 S-box over $R_3 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$

111	101	110	100
7	5	6	4

The multiplicative group of unit elements of the ring R_3 is

$$M_{G_3} = \left\{1, 1+u, 1+u^2, 1+u+u^2\right\}.$$

Define $f : M_{G_3} \to M_{G_3}$ by $f(a) = a^{-1}$ and $g : M_{G_3} \to M_{G_3}$ by $g(a) = a'a$, where $a' = 1+u$. Thus, $f \circ g(a) = (a'a)^{-1}$ (Tables 3, 4).

3.2 Construction of S-box through multiplicative group of R_4

The chain ring $R_4 = \frac{\mathbb{F}_2[u]}{\langle u^4 \rangle} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ has 16 elements. Its chain of ideals is $\langle 0 \rangle = u^4R_4 \subset u^3R_4 \subset u^2R_4 \subset uR_4 \subset R_4$, whereas the residue field of this ring is $\frac{R_4}{uR_4} \simeq \mathbb{F}_2$. The ring R_4 shares some properties of the local ring $\mathbb{Z}_{16}$ and the Galois field $\mathbb{F}_{16}$. The multiplication and addition binary operations of R_4 coincides with $\mathbb{Z}_{16}$ and $\mathbb{F}_{16}$, respectively (Table 5).

Multiplicative group of unit elements of the ring R_4 is given by

$$M_{G_4} = \left\{1, 1+u, 1+u^2, 1+u^3, 1+u+u^2, 1+u+u^3, 1+u^2+u^3, 1+u+u^2+u^3\right\}.$$

Take a subgroup $H_{G_4} = \{1, 1+u, 1+u^2, 1+u+u^2+u^3\}$ of index 2 of the group M_{G_4} and apply given procedure on subgroup rather than group M_{G_4}. Define $f : H_{G_4} \to H_{G_4}$ by $f(a) = a^{-1}$ and $g : H_{G_4} \to H_{G_4}$ by $g(a) = a'a$, where $a' = 1+u$. Thus, $(f \circ g)(a) = (a'a)^{-1}$. The following Table 6 is of $(f \circ g)(H_{G_4})$ in binary and decimal form, which is in fact the S-box constructed over the chain ring $R_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$.

Table 5 Elements in R_4

Sr. No.	Polynomial	Binary string
1	0	0000
2	1	1000
3	u	0100
4	u^2	0010
5	u^3	0001
6	$1+u$	1100
7	$1+u^2$	1010
8	$1+u^3$	1001
9	$u+u^2$	0110
10	$u+u^3$	0101
11	u^2+u^3	0011
12	$1+u+u^2$	1110
13	$1+u+u^3$	1101
14	$1+u^2+u^3$	1011
15	$u+u^2+u^3$	0111
16	$1+u+u^2+u^3$	1111

Table 6 S-box over $R_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$

1111	1010	1100	1000
15	10	12	8

3.3 Construction of S-box through multiplicative group of R_5

The chain ring $R_5 = \frac{\mathbb{F}_2[u]}{\langle u^5\rangle} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2$ has 32 number of elements. The chain of ideals is $\langle 0\rangle = u^5R_5 \subset u^4R_5 \subset u^3R_5 \subset u^2R_5 \subset uR_5 \subset R_5$ and its residue field is $\frac{R_5}{uR_5} \simeq \mathbb{F}_2$. The multiplication binary operation of R_5 coincides with of $\mathbb{Z}_{2^5}$, whereas the addition binary operation is similar to that of $\mathbb{F}_{2^5}$. Multiplicative group of unit elements of the ring R_5 is given by

$$\begin{aligned} M_{G_5} = \{&1, 1+u, 1+u^2, 1+u^3, 1+u^4, 1+u+u^2, 1+u+u^3, 1+u+u^4,\\ &1+u^2+u^3, 1+u^2+u^4, 1+u^3+u^4, 1+u+u^2+u^3, 1+u+u^2+u^4,\\ &1+u+u^3+u^4, 1+u^2+u^3+u^4, 1+u+u^2+u^3+u^4\}. \end{aligned}$$

Define $f : M_{G_5} \to M_{G_5}$ by $f(a) = a^{-1}$ and $g : M_{G_5} \to M_{G_5}$ by $g(a) = a'a$, where $a' = 1+u$. Thus, $(f \circ g)(a) = (a'a)^{-1}$. The following Table 7 is of $(f \circ g)(H_{G_5})$ in binary and decimal form, which is in fact the S-box constructed over the chain ring $R_5 = \mathbb{F}_2 + u\mathbb{F}_2 + +u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2$.

Table 7 S-box over $R_5 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2$

11111	11110	11010	10011
31	30	26	19
10101	10010	11000	10111
21	18	21	23
11001	10110	11101	11011
25	22	29	27
11100	10100	10001	10000
28	20	17	16

3.4 Construction of S-box through multiplicative group of R_6

The chain ring $R_6 = \frac{\mathbb{F}_2[u]}{\langle u^6\rangle} = \mathbb{F}_2 + u\mathbb{F}_2 + +u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2 + u^5\mathbb{F}_2$ has cardinality 64. As u is a nilpotent element with nilpotency index 6, it follows that $\langle 0\rangle = u^6R_6 \subset u^5R_6 \subset u^4R_6 \subset u^3R_6 \subset u^2R_6 \subset uR_6 \subset R_6$ and the residue field of R_6 is $\frac{R_6}{uR_6} \simeq \mathbb{F}_2$. The addition and multiplication binary operation of R_6 coincides with $\mathbb{F}_{2^6}$ and $\mathbb{Z}_{2^6}$, respectively. Multiplicative group of the ring R_6 is given by

$$\begin{aligned} M_{G_6} = \{&1, 1+u, 1+u^2, 1+u^3, 1+u^4, 1+u^5, 1+u+u^2, 1+u+u^3,\\ &1+u+u^4, 1+u+u^5, 1+u^2+u^3, 1+u^2+u^4, 1+u^2+u^5, 1+u^3+u^4,\\ &1+u^3+u^5, 1+u^4+u^5, 1+u+u^2+u^3, 1+u+u^2+u^4, 1+u+u^2+u^5,\\ &1+u+u^3+u^4, 1+u+u^3+u^5, 1+u+u^4+u^5, 1+u^2+u^3+u^4,\\ &1+u^2+u^3+u^5, 1+u+u^2+u^3+u^4, 1+u+u^2+u^3+u^5,\\ &1+u+u^2+u^4+u^5, 1+u+u^3+u^4+u^5, 1+u^2+u^3+u^4+u^5,\\ &1+u+u^2+u^3+u^4+u^5\}. \end{aligned}$$

The multiplicative subgroup M_{G_6} contains 32 elements, 16 elements of order 8, 8 elements of order 4, 7 elements of order 2 and 1 element of order 1. Since our interest is in the subgroups of cardinality 16, so we combine these cyclic subgroups in such a way that they generate subgroups of order 16.

Remark 3.1 The availability of subgroups of cardinality 16 is as follows:

1. Product of 2 elements of order 4.
2. Product of 2 elements of order 2 and 1 element of order 4.
3. Product of 1 element of order 2 and 1 element of order 2.

In all of the above-mentioned products, intersection of each joining pair or triplet should be just the identity element. We take one of these subgroups, $H_{G_6} = \langle 1+u^2, 1+u^3+u^4, 1+u^3+u^5\rangle$ of cardinality 16 of the multiplicative group M_{G_6}. Define the maps $f : H_{G_6} \to H_{G_6}$ by $f(a) = a^{-1}$ and $g : H_{G_6} \to H_{G_6}$ by $g(a) = a'a$, where $a' = 1+u^4$. Thus, $(g \circ f)(a) = (a'a)^{-1}$. The following Table 8 is of $(f \circ g)(H_{G_6})$ in binary and decimal form, which is in fact the S-box designed over the chain ring R_6.

Table 8 S-box over $R_6 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2 + u^5\mathbb{F}_2$

100010	101000	101010	100100
34	40	42	36
100111	100001	101111	101100
39	33	47	44
101011	100110	100101	100011
43	38	37	35
101101	101110	101001	100000
45	46	41	32

3.5 Construction of S-box through multiplicative group of R_7

The size of chain ring $R_7 = \frac{\mathbb{F}_2[u]}{\langle u^7\rangle} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2 + u^5\mathbb{F}_2 + u^6\mathbb{F}_2$ is 128. The chain of ideals is $\langle 0\rangle = u^7R_7 \subset u^6R_7 \subset u^5R_7 \subset u^4R_7 \subset u^3R_7 \subset u^2R_7 \subset uR_7 \subset R_7$. Accordingly the residue field of R_7 is $\frac{R_7}{uR_7} \simeq \mathbb{F}_2$. The ring R_7 shares some properties of the local ring $\mathbb{Z}_{2^7}$ and the Galois field $\mathbb{F}_{2^7}$. Its multiplicative part is given by

$$\begin{aligned} M_{G_7} = \{&1, 1+u, 1+u^2, 1+u^3, 1+u^4, 1+u^5, 1+u^6, 1+u+u^2, 1+u+u^3,\\ &1+u+u^4, 1+u+u^5, 1+u+u^6, 1+u^2+u^3, 1+u^2+u^4, 1+u^2+u^5,\\ &1+u^2+u^6, 1+u^3+u^4, 1+u^3+u^5, 1+u^3+u^6, 1+u^4+u^5,\\ &1+u^4+u^6, 1+u^5+u^6, 1+u+u^2+u^3, 1+u+u^2+u^4,\\ &1+u+u^2+u^5, 1+u+u^2+u^6, \quad 1+u^2+u^3+u^4, 1+u+u^3+u^4,\\ &1+u+u^3+u^5, 1+u+u^3+u^6, 1+u+u^4+u^5, 1+u+u^4+u^6,\\ &1+u+u^5+u^6, 1+u^2+u^3+u^5, 1+u^2+u^3+u^6, 1+u^2+u^4+u^5,\\ &1+u^2+u^4+u^6, 1+u^2+u^5+u^6, 1+u^3+u^4+u^5, 1+u^3+u^4+u^6,\\ &1+u^3+u^5+u^6, 1+u^4+u^5+u^6, 1+u+u^2+u^3+u^4,\\ &1+u+u^2+u^3+u^5, 1+u+u^2+u^3+u^6, 1+u+u^2+u^4+u^5,\\ &1+u+u^2+u^4+u^6, \quad 1+u+u^2+u^5+u^6, 1+u+u^3+u^4+u^5,\\ &1+u+u^3+u^4+u^6, 1+u+u^3+u^5+u^6, 1+u+u^4+u^5+u^6,\\ &1+u^2+u^3+u^4+u^5, 1+u^2+u^3+u^4+u^6, 1+u^2+u^3+u^5+u^6,\\ &1+u^2+u^4+u^5+u^6, 1+u^3+u^4+u^5+u^6, 1+u+u^2+u^3+u^4+u^5,\\ &1+u+u^2+u^3+u^4+u^6, 1+u+u^2+u^3+u^5+u^6,\\ &1+u+u^2+u^3+u^4+u^5+u^6, 1+u+u^3+u^4+u^5+u^6,\\ &1+u^2+u^3+u^4+u^5+u^6, 1+u+u^2+u^3+u^4+u^5+u^6\}. \end{aligned}$$

The multiplicative subgroup M_{G_7} contains 64 elements, with 32 elements of order 8, 24 elements of order 4, 7 elements of order 2 and 1 element of order 1. Since we require the subgroups of size 16, it follows that we can fulfill our requirement by above explained availability for M_{G_7}. For this purpose we choose a subgroup $H_{G_7} = \langle 1+u^3, 1+u^2+u^3\rangle$ of cardinality 16 of the multiplicative group M_{G_7}. Define the maps $f : H_{G_7} \to H_{G_7}$ by $f(a) = a^{-1}$ and $g : H_{G_7} \to H_{G_7}$ by $g(a) = a'a$, where $a' = 1+u^3$. Thus, $(g \circ f)(a) = (a'a)^{-1}$. The following Table 9 is of $(f \circ g)(H_{G_7})$ in binary and decimal form, which is in fact the S-box constructed over the chain ring $R_7 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2 + u^5\mathbb{F}_2 + u^6\mathbb{F}_2$.

Table 9 S-box over $R_7 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2 + u^5\mathbb{F}_2 + u^6\mathbb{F}_2$

1001001	1000001	1000000	1001000
73	65	64	72
1010110	1001101	1010010	1000101
86	77	82	69
1011101	1011001	1010111	1001100
93	89	87	76
1010011	1011100	1000100	1011000
83	92	76	88

3.6 Construction of S-box through multiplicative group of R_8

The ring $R_8 = \frac{\mathbb{F}_2[u]}{\langle u^8\rangle} = \mathbb{F}_2 + u\mathbb{F}_2 + +u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2 + u^5\mathbb{F}_2 + u^6\mathbb{F}_2 + u^7\mathbb{F}_2$ is a commutative chain ring of 2^8 elements. Since u is nilpotent with nilpotency index 8, it follows that $\langle 0\rangle = u^8R_8 \subset u^7R_8 \subset u^6R_8 \subset u^5R_8 \subset u^4R_8 \subset u^3R_8 \subset u^2R_8 \subset uR_8 \subset R_8$ and $\frac{R_8}{uR_8} \simeq \mathbb{F}_2$ is the residue field of R_8. The ring R_8 shares some properties of the local ring $\mathbb{Z}_{2^8}$ and the Galois field $\mathbb{F}_{2^8}$. The multiplication binary operation of R_8 coincides with of $\mathbb{Z}_{2^8}$, whereas the addition binary operation is similar to that of $\mathbb{F}_{2^8}$. Multiplicative group of the ring R_8 is given by

$$
\begin{aligned}
M_{G_8} = \{&1, 1+u, 1+u^2, 1+u^3, 1+u^4, 1+u^5, 1+u^6, 1+u^7, 1+u+u^2,\\
&1+u+u^3, 1+u+u^4, 1+u+u^5, 1+u+u^6, 1+u+u^7, 1+u^2+u^3,\\
&1+u^2+u^4, 1+u^2+u^5, 1+u^2+u^6, 1+u^2+u^7, 1+u^3+u^4, 1+u^3+u^5,\\
&1+u^3+u^6, 1+u^3+u^7, 1+u^4+u^5, 1+u^4+u^6, 1+u^4+u^7, 1+u^5+u^6,\\
&1+u^5+u^7, 1+u^6+u^7, 1+u+u^2+u^3, 1+u+u^2+u^4, 1+u+u^2+u^5,\\
&1+u+u^2+u^6, 1+u+u^2+u^7, 1+u+u^3+u^4, 1+u+u^3+u^5,\\
&1+u+u^3+u^6, 1+u+u^3+u^7, 1+u+u^4+u^5, 1+u+u^4+u^6,\\
&1+u+u^4+u^7, 1+u+u^5+u^6, 1+u+u^5+u^7, 1+u+u^6+u^7,\\
&1+u^2+u^3+u^4, 1+u^2+u^3+u^5, 1+u^2+u^3+u^6, 1+u^2+u^3+u^7,\\
&1+u^2+u^4+u^5, 1+u^2+u^4+u^6, 1+u^2+u^4+u^7, 1+u^2+u^5+u^6,\\
&1+u^2+u^5+u^7, 1+u^2+u^6+u^7, 1+u^3+u^4+u^5, 1+u^3+u^4+u^6,\\
&1+u^3+u^4+u^7, 1+u^3+u^5+u^6, 1+u^3+u^5+u^7, 1+u^3+u^6+u^7,\\
&1+u^4+u^5+u^6, 1+u^4+u^5+u^7, 1+u^4+u^6+u^7, 1+u^5+u^6+u^7,\\
&1+u+u^2+u^3+u^4, 1+u+u^2+u^3+u^5, 1+u+u^2+u^3+u^6,\\
&1+u+u^2+u^3+u^7, 1+u+u^2+u^4+u^5, 1+u+u^2+u^4+u^6,\\
&1+u+u^2+u^4+u^7, 1+u+u^2+u^5+u^6, 1+u+u^2+u^5+u^7,\\
&1+u+u^2+u^6+u^7, 1+u+u^3+u^4+u^5, 1+u+u^3+u^4+u^6,\\
&1+u+u^3+u^4+u^7, 1+u+u^3+u^5+u^6, 1+u+u^3+u^5+u^7,\\
&1+u+u^3+u^6+u^7, 1+u+u^4+u^5+u^6, 1+u+u^4+u^5+u^7,\\
&1+u+u^4+u^6+u^7, 1+u+u^5+u^6+u^7, 1+u^2+u^3+u^4+u^5,\\
&1+u^2+u^3+u^4+u^6, 1+u^2+u^3+u^4+u^7, 1+u^2+u^3+u^5+u^6,\\
&1+u^2+u^3+u^5+u^7, 1+u^2+u^3+u^6+u^7, 1+u^2+u^4+u^5+u^6,
\end{aligned}
$$

Table 10 S-box over $R_8 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2 + u^5\mathbb{F}_2 + u^6\mathbb{F}_2 + u^7\mathbb{F}_2$

10001010	10011001	10000010	10001000
138	153	130	136
10011011	10101111	10100101	10111010
155	175	165	186
10010010	10110001	10000000	10111010
146	177	128	173
10100111	10111000	10010000	10110011
167	184	143	179

$$1+u^2+u^4+u^5+u^7, 1+u^2+u^4+u^6+u^7, 1+u^2+u^5+u^6+u^7,$$
$$1+u^3+u^4+u^5+u^6, 1+u^3+u^4+u^5+u^7, 1+u^3+u^4+u^6+u^7,$$
$$1+u^3+u^5+u^6+u^7, 1+u^4+u^5+u^6+u^7, 1+u+u^2+u^3+u^4+u^5,$$
$$1+u+u^2+u^3+u^4+u^6, 1+u+u^2+u^3+u^5+u^6,$$
$$1+u+u^2+u^4+u^5+u^6, 1+u+u^3+u^4+u^5+u^6,$$
$$1+u^2+u^3+u^4+u^5+u^6, 1+u+u^2+u^3+u^4+u^7,$$
$$1+u+u^2+u^3+u^5+u^7, 1+u+u^2+u^4+u^5+u^7,$$
$$1+u+u^3+u^4+u^5+u^7, 1+u^2+u^3+u^4+u^5+u^7,$$
$$1+u+u^2+u^3+u^6+u^7, 1+u+u^2+u^4+u^6+u^7,$$
$$1+u+u^3+u^4+u^6+u^7, 1+u^2+u^3+u^4+u^6+u^7,$$
$$1+u+u^2+u^5+u^6+u^7, 1+u+u^3+u^5+u^6+u^7,$$
$$1+u^2+u^3+u^5+u^6+u^7, 1+u+u^4+u^5+u^6+u^7,$$
$$1+u^2+u^4+u^5+u^6+u^7, 1+u^3+u^4+u^5+u^6+u^7,$$

$$1+u+u^2+u^3+u^4+u^5+u^6, 1+u+u^2+u^3+u^4+u^5+u^7,$$
$$1+u+u^2+u^3+u^4+u^6+u^7, 1+u+u^2+u^3+u^5+u^6+u^7,$$
$$1+u+u^2+u^4+u^5+u^6+u^7, 1+u+u^3+u^4+u^5+u^6+u^7,$$
$$1+u^2+u^3+u^4+u^5+u^6+u^7, 1+u+u^2+u^3+u^4+u^5+u^6+u^7\}.$$

The multiplicative group M_{G_8} contains 128 elements, 64 elements of order 8, 48 elements of order 4, 15 elements of order 2 and 1 element of order 1. Ever since we require the subgroups of cardinality 16, therefore we accomplish our constraint by above explained availability for M_{G_6}, and set of all elements of order 2 also generate a subgroup of order 16. We choose a subgroup $H_{G_8} = \langle 1+u^3+u^6, 1+u^2+u^4+u^5+u^7\rangle$ of the group M_{G_8} having cardinality 16. Define the maps $f : H_{G_8} \to H_{G_8}$ by $f(a) = a^{-1}$ and $g : H_{G_8} \to H_{G_8}$ by $g(a) = a'a$, where we take $a' = 1+u^4+u^6$. Thus, $(g \circ f)(a) = (a'a)^{-1}$. The following Table 8 is of $(f \circ g)(H_{G_8})$ in binary and decimal form, which is in fact the S-box designed over the chain ring $R_8 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2 + u^5\mathbb{F}_2 + u^6\mathbb{F}_2 + u^7\mathbb{F}_2$ (Table 10).

We conclude this section by the following Table 11 which shows orders of the unit elements in the chain rings R_8, R_7, R_6, R_5, R_4 and R_3.

Table 11 Orders of elements in M_{G_k}

R_k	Total elements	Elements of M_{G_k}	Order 8	Order 4	Order 2	Order 1
R_8	256	128	64	48	15	1
R_7	128	64	32	24	7	1
R_6	64	32	16	8	7	1
R_5	32	16	8	4	3	1
R_4	16	8		4	3	1
R_3	8	4			3	1

Table 12 S-boxes over $GF(2, 4)$ and $GR(4, 4)$

0	11	12	6
3	8	4	2
1	9	13	15
14	7	10	5

0	67	215	159
25	240	15	16
1	113	116	198
109	45	202	44

3.7 S-Boxes over $GF(2, 4)$ and $GR(4, 4)$

The ring $\mathbb{Z}_4[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_4, n \in \mathbb{Z}^+\}$ is the polynomial ring with one indeterminate x and $\langle f(x)\rangle = \{a(x)f(x) : a(x) \in \mathbb{Z}_4[x]\}$ is a principal ideal generated by basic monic irreducible polynomial $f(x) = x^4 + x + 1$ is basic irreducible over the local rings $\mathbb{Z}_4$ such that by reduction mod 2 map $\overline{f(x)} = x^4 + x + 1$ is irreducible polynomial over $\mathbb{Z}_2$. Thus, $R = \frac{\mathbb{Z}_4[x])}{\langle f(x)\rangle} = \{a_0 + a_1x + a_2x^2 + \cdots + a_3x^3 : a_i \in \mathbb{Z}_4\}$ is the Galois ring extension $GR(4, 4)$ of order 256 with corresponding Galois field extension $\mathbb{K} = \frac{\mathbb{Z}_2[x])}{\langle f(x)\rangle} = GF(2, 4)$ of order 16. The group $\mathbb{K}^* = \mathbb{K}\backslash\{0\}$ becomes the multiplicative group of units of the field $\mathbb{K}$. Now, let $\mathbb{R}^*$ be the multiplicative group of units of the Galois ring R. Thus, the maximal cyclic subgroup G_{15} of R^* is isomorphic to the cyclic Galois group $\mathbb{K}^*$. The following Table 3.6.3 represent the S-boxes obtained through respectively $\mathbb{K}$ and $G_{15} \cup \{0\}$ Shah et al. (2013) (Table 12).

Table 13 MLC of LSBs and MSBs of airplane image by S-boxes R_k, for $5 \le k \le 8$

	Entropy	Correlation	Homogeneity	Contrast	Energy
Plain airplane image	5.4319	0.9532	0.9494	0.2253	0.2430
LSBs of S-box on R_5	5.3797	0.9350	0.9200	0.3007	0.2614
MSBs of S-box on R_5	5.8689	0.8703	0.8486	1.2425	0.1705
LSBs of S-box on R_6	5.2901	0.9367	0.9218	0.2970	0.2654
MSBs of S-box on R_6	5.5856	0.7239	0.8025	1.8846	0.2217
LSBs of S-box on R_7	5.2795	0.9382	0.9260	0.2881	0.2696
MSBs of S-box on R_7	5.9075	0.7910	0.8396	1.3274	0.1862
LSBs of S-box on R_8	5.2844	0.9385	0.9266	0.2873	0.2699
MSBs of S-box on R_8	5.8165	0.7541	0.8400	1.5980	0.1905

Table 14 MLC of LSBs of airplane image by S-boxes on GF(2,4), GR(4,4) and R_k, for $5 \leq k \leq 8$

	Entropy	Correlation	Homogeneity	Contrast	Energy
Plain airplane image	5.4319	0.9532	0.9494	0.2253	0.2430
LSBs of S-box on $GF(2, 4)$	5.5133	0.9390	0.9302	0.2750	0.2712
LSBs of S-box on $GF(4, 4)$	5.4146	0.9358	0.9260	0.2819	0.2668
LSBs of S-box on R_5	5.3797	0.9350	0.9200	0.3007	0.2614
LSBs of S-box on R_6	5.2901	0.9367	0.9218	0.2970	0.2654
LSBs of S-box on R_7	5.2795	0.9382	0.9260	0.2881	0.2696
LSBs of S-box on R_8	5.2844	0.9385	0.9266	0.2873	0.2699

4 Majority logic criterion for the analysis of S-boxes

In Shah et al. (2011) and Hussain et al. (2012), a majority logic criterion (MLC) has been given. This criterion is used to analyze the statistical strength of the S-box in image encryption application. The encryption procedure creates distortions in the image, and the sort of these distortions fixes the strength of the proposed S-boxes. This analysis contains, entropy, correlation, homogeneity, contrast and energy.

The amount of randomness in a system is measured by entropy. In an image the degree of entropy is related to the arrangements of artifacts, which aid the human to perceive the image. Contrast enables the viewer to identify the objects in an image. As the image is encrypted, the amount of randomness increases results in the elevation of contrast level to a very high value. The higher level of contrast in the encrypted image depicts strong encryption. Correlation is an analysis which measures the correlation of a pixel to its neighbor by keeping into consideration the texture of the entire image. The homogeneity analysis measures the closeness of the distribution of elements in the gray level co-occurrence matrix (GLCM) to GLCM diagonal. The GLCM shows the statistics of combinations of pixel brightness values or gray levels in tabular form. In the analysis of energy, we measure the energy of the encrypted images as processed by various S-boxes. This measure gives the sum of square elements in GLCM.

A typical 512 × 512 image of airplane is used for MLC for the S-boxes over chain rings R_k, for $5 \leq k \leq 8$, and the results for both LSBs and MSBs are arranged in the Table 13, spectacle that the proposed S-boxes satisfies all the criteria fit for the standard and can be used for safe communication. In addition, for the sake of comparison the same image of airplane is taken and MLC is operationalized only for LSBs for the S-boxes over $GF(2, 4)$, $GR(4, 4)$ and R_k, for $5 \leq k \leq 8$, LSBs is considered. Thus the Table 14 shows a comparative analysis and reflects the strength of newly constructed S-boxes against the 4 × 4 S-boxes over Galois field $GF(2, 4)$ and the Galois ring $GR(4, 4)$.

5 Conclusion

A novel technique for the construction of substitution boxes over the elements of finite chain rings of a specific type is suggested. The S-boxes are constructed through the 16 order subgroups of the multiplicative groups of units of the chain rings instead of a Galois field $\mathbb{F}_{2^4}$. In designing of 4 × 4 S-boxes, we are able to use chain rings of cardinality 32, 64,

128 and 256, but when Galois field is concerned for this purpose, $\mathbb{F}_{2^4}$ having cardinality 16, can only be use. Furthermore, like Shah et al. (2013) there is no need to use the modulo 2 reduction map, because the elements of chain rings under consideration are already in the form of binary strings. The strength of the proposed S-boxes is verified through MLC and hence this new technique to synthesize S-boxes offers a powerful algebraic complication.

Future directions: since each chain ring R_k might have more than one order sixteen subgroups of its group of unit elements, so, over the chain ring R_k we could generate more S-boxes. Moreover, the chain ring $\sum_{i=0}^{8} u^i \mathbb{F}_2$ could be use for the construction of 8×8 S-boxes.

References

Abualrub T, Saip I (2007) Cyclic coacquired a great consideration in algebraic coding theory over the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Des Codes Cryptogr 42:273–287

Abu Dahrouj FM (2008) Negacyclic and constacyclic codes over finite chain rings. Master of Mathematics Thesis, The Islamic University of Gaza, Gaza

Adams C, Tavares S (1990) The structured design of cryptographically good S-boxes. J Cryptol 3:27–41

Al-Ashker M (2005) Simplex codes over the ring $\sum_{n=0}^{s} u^n \mathbb{F}_2$. Turk J Math 29(3):221–233

Al-Ashker M (2005) Simplex codes over $\mathbb{F}_2 + u\mathbb{F}_2$. Arab J Sci Eng 3:227–285

Al-Ashker M, Hamoudeh M (2011) Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$. Turk J Math 33:737–749

Al-Ashker M, Chen J (2013) Cyclic codes of arbitrary length over $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{k-1}\mathbb{F}_q$. Palistine J Math 2(1):72–80

Andrade AA, Palazzo R Jr (1999) Construction and decoding of BCH codes over finite rings. Linear Algebra Appl 286:69–85

Bilgin B, Nikova S, Nikov V, Rijmen V, Stutz G (2012) Thershold Implementations of all 3×3 S-boxes. In: Cryptographic Hardware and Embedded Systems. Springer, New York, pp 76–91

Bonnecaze A, Udaya P (1999) Cyclic codes and self dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Trans Inf Theory 45:1250–1255

Clark WE, Liang JJ (1973) Enumeration of finite commutative chain rings. J Algebra 27(3):445–453

Cohen S, Niederreiter H (2009) Finite fields and applications. Cambridge University Press, London

Cui L, Cao Y (2007) A new S-box structure named affine-power-affine. Int J Innov Comput I 3(3):45–53

Daemen J, Rijmen V (2000) The block cipher Rijndael. Smart Card Research and Applications, Lecture Notes in Computer Science 1820. Springer, New York, pp 277–284

Gupta KC, Sarkar P (2005) Improved construction of nonlinear resilient S-boxes. IEEE Trans Inf Theory 15(1):339–348

Hou X (2001) Finite commutative chain rings. Finite Fields Appl. 7:382–396

Hussain I, Shah T (2013) Literature survey on nonlinear components and chaotic nonlinear compotents of block cipher. Nonlinear dyn 74:869–904

Hussain I, Shah T, Mahmood H, Gondal MA, Bhatti UY (2011) Some analysis of S-box based on residue of prime number. Proc Pak Acad Sci 48(2):111–115

Hussain I, Shah T, Gondal MA, Mahmood H (2012) Generalized majority logic criterion to analyze the statistical strength of S-boxes. Z Naturforsch A 67a:282–288

Kim J, Phan RCW (2009) Advanced differential-style crypt-analysis of the NSA's skipjack block cipher. Cryptologia 33(3):246–270

Naji A (2002) Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ of constant lee weight. The second conference of the Islamic University on Mathematical Science-Gaza

Nyberg K (1991) Perfect nonlinear S-boxes. In: Advances in cryptology—EUROCRYPT91. Lecture Notes in Computer Science, vol 547. Springer, New York pp 378–386

Qian J, Zhang L, Zhu S (2005) Cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$. IEICE Trans Fundam 3:779–795

Qian J, Zhang L, Zhu S (2006) (1+u) constacyclic and cyclic over $\mathbb{F}_2 + u\mathbb{F}_2$. Appl Math Lett 19(8):820–823

Qian J, Zhang L, Zhu S (2006) Constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. IEICE Trans Fundam 6:1863–1885

Shah T, Hussain I, Gondal MA, Mahmood H (2011) Statistical analysis of S-box in image encryption applications based on majority logic criterion. Inter J Phys Sci 6(16):4110–4127

Shah T, Qamar A, Andrade AA (2012a) Constructions and decoding of a sequence of BCH codes. Math Sci Res J 16(9):234–250

Shah T, Qamar A, Andrade AA (2012b) Construction and decoding of BCH codes over chain of commutative rings. Math Sci 6(51):14

Shah T, Qamar A, Hussain I (2013) Substitution box on maximal cyclic subgroup of units of a Galois ring. Z Naturforsch A 68a:567–572

Shanbhag AG, Kumar PV, Helleseth T (1996) Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation of some q-ary sequences. IEEE Trans Inf Theory IT–42(1):250–254

Shankar P (1979) On BCH codes over arbitrary integer rings. IEEE Trans Inf Theory IT–25(4):480–483

Tran MT, Bui DK, Doung AD (2008) Gray S-box for advanced encryption standard. Inter Conf Comput Intell Secur 1:253–256

Yi X, Cheng SX, You XH, Lam KY (2002) A method for obtaining cryptographically strong 8 × 8 S-boxes. Int Conf Infor Netw Appl 2(3):14–20