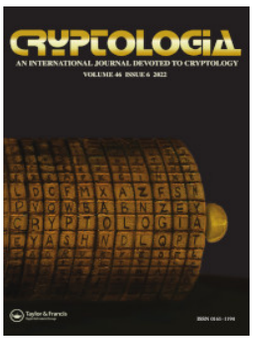

Cryptologia

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ucry20

Construction of cryptographically strong S-boxes from ternary quasigroups of order 4

Dimpy Chauhan, Indivar Gupta, P. R. Mishra & Rashmi Verma

To cite this article: Dimpy Chauhan, Indivar Gupta, P. R. Mishra & Rashmi Verma (2022) Construction of cryptographically strong S-boxes from ternary quasigroups of order 4, Cryptologia, 46:6, 525-551, DOI: 10.1080/01611194.2021.1934915

To link to this article: https://doi.org/10.1080/01611194.2021.1934915

CRYPTOLOGIA
2022, VOL. 46, NO. 6, 525–551
https://doi.org/10.1080/01611194.2021.1934915

Taylor & Francis
Taylor & Francis Group

Construction of cryptographically strong S-boxes from ternary quasigroups of order 4

Dimpy Chauhan, Indivar Gupta, P. R. Mishra, and Rashmi Verma

ABSTRACT
The security of block ciphers solely depends on the S-boxes used in their design. Hence, for a secure block cipher, S-boxes should be chosen very thoughtfully. *n*-ary quasigroups of different orders and for different values of *n* are being used to design various cryptographic primitives. In the literature, many algorithms based on the quasigroups have been proposed for the generation of S-boxes of order 4. However, in this article, we propose a general method for the construction of symmetric S-boxes of even order using ternary quasigroups of order 4 with certain properties. These S-boxes give strong resistance against linear, differential, algebraic, and DPA attacks and hence provide good cryptographic properties.

KEYWORDS
algebraic normal form; Latin cube; left and right e-transformation; n-ary quasigroup; S-box

1. Introduction

The structure, properties, and existence of a large number of *n*-ary quasigroups of certain order enable them to be applied in cryptology to design various cryptographic primitives, namely block ciphers, stream ciphers, S-boxes, message authentication codes, quasigroup-based secret sharing schemes, hash functions, etc. In almost all modern block ciphers, S-boxes play a vital role in the design of cryptosystems as well as in security. They are the only nonlinear part of the block cipher in the two main round functions, namely Feistel networks and substitution/permutation networks. Thus, in order to make the cipher secure against various types of attacks, S-boxes should be chosen very carefully.

There are two main kinds of attacks on block ciphers. One kind of attack depends on the cryptographic properties like S-boxes involved in designing the cryptosystem, whereas another kind of attack depends on the analysis of the leakages in hardware (also known as side channel analysis). Linear cryptanalysis (Matsui 1993) and differential cryptanalysis (Biham and Shamir 1991) are the mainly used attacks against block ciphers. In order to protect the block cipher against these attacks, S-boxes are designed in a way to satisfy certain cryptographic criteria like balancedness, high

CONTACT Dimpy Chauhan dimpychauhan21jan@gmail.com Department of Mathematics, University of Delhi, Delhi 110007, India

algebraic degree, high nonlinearity, etc. In the side channel analysis, sensitive information such as the power consumption or the timing of operations can be obtained (as the electronic components are not usually perfectly temper proof). Among all the side channel attacks, the differential power analysis (DPA) is one of the most powerful attacks against iterated block ciphers. To quantify the resistance of an S-box to DPA attacks, the transparency order (TO) of an S-box has been introduced in Prouff (2005). In order to have resistance against DPA attacks, the TO of an S-box must be as low as possible. An S-box with a smaller TO is more resistant to DPA attacks.

To the best of our knowledge, all the articles available in the literature for the construction of S-boxes based on quasigroup or ternary quasigroup are for the generation of optimal 4×4-bit S-boxes only (Mihajloska and Gligoroski 2012; Yu and Xu 2017). In our article, we give a general method to construct cryptographically strong symmetric S-boxes of even order from ternary quasigroup of order 4 and such S-boxes shall be called TQ-S-boxes. Using this method we generate 4×4, 6×6 and 8×8-bit nonlinear cryptographically strong TQ-S-boxes and analyse each of them. We also discuss comparative analysis with the existing methods for the generation of S-boxes and show that our method is better.

The article has the following structure: in Section 2, we give some definitions and discuss a classification of ternary quasigroups of order 4. Section 3 illustrates a detailed review of cryptographic properties of S-boxes and some of the important criteria for cryptographically strong S-boxes. In Section 4, we propose an algorithm to generate cryptographically strong TQ-S-boxes. We then give an experimental verification and cryptographic analysis of the 4×4, 6×6, and 8×8-bit TQ-S-boxes generated from the algorithm in Section 5. Section 6 discusses a comparison with the old methods. Finally, Section 7 concludes this article.

2. Preliminaries

In this section, we discuss some basic mathematical background needed for the understanding of concepts of the article.

Definition 1 (Belousov 1972). Let Q be a nonempty set. An n-ary groupoid (Q, f) with n-ary operation f is said to be an n-ary quasigroup if in the equality $f(x_1, x_2, \ldots, x_n) = x_{n+1}$ on knowing any n elements of the set $\{x_1, x_2, \ldots, x_n, x_{n+1}\}$ uniquely specifies the remaining one element.

Note: Taking $n = 2$ and 3 in Definition 1, we get 2-ary and 3-ary quasigroups, which are also known as binary quasigroup (or quasigroup) and ternary quasigroup, respectively. A ternary quasigroup may also be defined as follows:

Definition 2 (Lyu and Xu 2015). Let Q be a nonempty set. A ternary groupoid (Q, f) is called a ternary quasigroup if there exist unique solutions $x, y, z \in Q$ of the equations $f(x, a, b) = c, f(a, y, b) = c$ and $f(a, b, z) = c$ for all $a, b, c \in Q$.

Let $\mathbb{F}_2$ denotes a Galois field with two elements. A map $f : \mathbb{F}_2^k \to \mathbb{F}_2^t$ is known as a *vector valued Boolean function or Boolean map*. Any such function can be written as t k-ary *Boolean functions* (which are nothing but functions $f_i : \mathbb{F}_2^k \to \mathbb{F}_2$) as follows:

$$f(x_1, ..., x_k) = (f_1(x_1, ..., x_k), f_2(x_1, ..., x_k), ..., f_t(x_1, ..., x_k)).$$

The Boolean functions $f_1, f_2, ..., f_t$ are called *coordinate functions of f* and the Boolean functions obtained by their nonzero $\mathbb{F}_2$ linear combinations are called *component functions of f*. Clearly, every coordinate function is a component function.

Every Boolean function in k variables $f_i(x_1, x_2, ..., x_k)$ can uniquely be represented in algebraic normal form (ANF) as:

$$f_i(x_1, x_2, ..., x_k) = \sum_{I \subseteq \{1, 2, ..., k\}} \alpha_I \left(\prod_{i \in I} x_i \right)$$

where the addition and multiplication are over $\mathbb{F}_2$ and the coefficients $\alpha_I \in \mathbb{F}_2$. This representation gives the algebraic degree of the Boolean map, which is the maximum of the degrees of its coordinate functions, i.e.,

$$\deg(f) = \max\{\deg(f_i) | i \in \{1, ..., t\}\}. \tag{1}$$

Let $Q = \mathbb{F}_2^d$ and (Q, f) be a ternary quasigroup. Then function f is a Boolean map $f : \mathbb{F}_2^{3d} \to \mathbb{F}_2^d$. For every element $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathbb{F}_2^{3d}$ and $\mathbf{w} \in \mathbb{F}_2^d$, the function $f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathbf{w}$ can be represented in binary as:

$$\begin{aligned} f(x_1, ..., x_d, y_1, ..., y_d, z_1, ..., z_d) \quad &= (f_1(x_1, ..., x_d, y_1, ..., y_d, z_1, ..., z_d), ..., \\ &\quad f_d(x_1, ..., x_d, y_1, ..., y_d, z_1, ..., z_d)), \end{aligned}$$

where $(x_1, ..., x_d), (y_1, ..., y_d)$ and $(z_1, ..., z_d)$ are the binary representation of $\mathbf{x}, \mathbf{y}$, and $\mathbf{z}$, respectively, and the Boolean functions $f_i : \mathbb{F}_2^{3d} \to \mathbb{F}_2, 1 \leqslant i \leqslant d$ are the corresponding coordinate functions of f (i.e., the binary representation of $\mathbf{w}$). The algebraic degree of the ternary quasigroup (Q, f) is the algebraic degree of the Boolean map f, which can be found using Equation (1). The function f can be viewed as a $3d \times d$-bit S-box.

Let Q be a finite set with cardinality m. A *Latin square* L on Q is a square matrix of order m with elements from Q such that, within any row or column of the matrix, no element occurs twice. And a *Latin cube* L on Q of order m is a 3-dimensional array with elements from Q such that each 1-dimensional sub-array contains each element of Q exactly once.

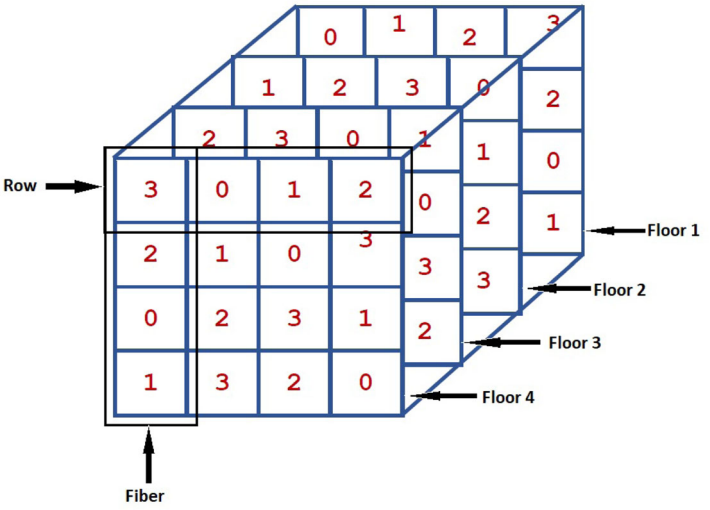

Figure 1. Latin cube.

Latin squares and Latin cubes are the equivalent combinatorial structures of quasigroups and ternary quasigroups, respectively.

Let L be a Latin cube whose elements and indices are from Q. Let $L(i,j,k)$ denotes the element of L at the cell (i, j, k). The ternary operation f on Q is defined as $f(x,y,z) = L(x,y,z)$, for all $x,y,z \in Q$. The pair (Q, f) is a ternary quasigroup on Q. In this article, we use Latin cube and ternary quasigroup interchangeably.

In a Latin cube, a 1-dimensional sub-array in which only the first (respectively second, third) coordinate varies is known as a fibre (respectively row, column). The Latin square obtained by fixing the first (respectively second, third) coordinate of the Latin cube is called a layer (respectively slice, floor). As in a layer only the second and third coordinate changes, hence it comprises rows and columns. Similarly, a slice comprises columns and fibres, and a floor comprises fibres and rows (Lyu and Xu 2015; Yu and Xu 2017). Figure 1 shows graphically the 4 floors of a Latin cube of order 4.

Here in this article, we will work with ternary quasigroups of order 4. So we take $Q = \mathbb{F}_2^2$ throughout the article. A ternary quasigroup of order 4 is called *pure nonlinear* if all the 3 component functions (i.e., f_1, f_2 and $f_1 \oplus f_2$) of f are nonlinear.

Definition 3 (Yu and Xu 2017). Let C_1 be a Latin cube of order 4 with floors f_0, f_1, f_2, f_3. Let α be a permutation on set $\{0,1,2,3\}$. A Latin cube C_2 with floors $f_{\alpha(0)}, f_{\alpha(1)}, f_{\alpha(2)}, f_{\alpha(3)}$ is called a *floor isomorphism* of C_1. The orbits of floor isomorphism are called the floor isomorphism classes, where the orbit is the set of all floor isomorphisms to which a floor can be moved through the permutation α.

Table 1. Criteria for cryptographically strong S-boxes.

Order	Non-linearity	Differential uniformity	Degree
4×4	$\mathcal{N}_s = 4$	$\text{Diff}(S) = 4$	$\deg(S) = 3$
6×6	$12 \leqslant \mathcal{N}_s \leqslant 24$	$2 \leqslant \text{Diff}(S) \leqslant 10$	$\deg(S) = 5$
$2k \times 2k$	$2^{2k-1} - 2^{k+1} - 2^k \leqslant \mathcal{N}_s \leqslant 2^{2k-1} - 2^k$	$2 \leqslant \text{Diff}(S) \leqslant 4k-2$	$\deg(S) = 2k-1$

There are 55,296 Latin cubes of order 4 (Mullen and Weber 1980), which, according to Definition 3, is further divided in 2304(= 55296/4!) floor isomorphism classes. If the elements on the top left corner of four floors of a Latin cube are in order, 0, 1, 2, 3, then the Latin cube is called *floor standard*. There is only one floor standard in each floor isomorphism class, which is called *representative of the class*. Hence, there are a total of 2,304 representatives of Latin cubes of order 4 ordered lexicographically as $L_1, L_2, \ldots, L_{2304}$ (Yu and Xu 2017). Only 648 of these representatives are pure nonlinear, whose indices are listed in Table 1 of Yu and Xu (2017).

For the construction of cryptographically strong TQ-S-boxes, we will only use these 648 pure nonlinear representatives in the Section 4.

Example 1. Consider a ternary quasigroup (Q, f) of order 4 (Latin cube L_{241} in lexicographical order) with the following four floors as shown in the Figure 2:

The function f is a Boolean map $f : \mathbb{F}_2^6 \to \mathbb{F}_2^2$ and hence acts as a 6×2-bit S-box. In other words, a ternary quasigroup of order 4 can be considered as a 6×2-bit S-box. Moreover, if, $\mathbf{x} = (0, 1; 0, 0; 1, 1)$, which is $(1, 0, 3)$ over Q is an input to the S-box, then the output is computed as $f(1, 0, 3) = L(1, 0, 3) = 2$, which is (1,0) in binary.

The ANF of this function f is as follows:

$$\begin{aligned} f(x_1, x_2; y_1, y_2; z_1, z_2) &= (f_1(x_1, x_2; y_1, y_2; z_1, z_2), f_2(x_1, x_2; y_1, y_2; z_1, z_2)) \\ &= (x_1 + y_2 + z_1 + x_1z_1 + x_1y_2z_1 + x_2z_1 + y_1z_1 + y_2z_1 + x_1z_2 + x_1y_2z_2 + x_2z_2 \\ &\quad + y_1z_2 + y_2z_2, x_1y_2 + x_2 + y_1 + x_1z_1 + x_1y_2z_1 + x_2z_1 + y_1z_1 + y_2z_1 + z_2 + \\ &\quad x_1z_2 + x_1y_2z_2 + x_2z_2 + y_1z_2 + y_2z_2). \end{aligned}$$

The algebraic degree of f is 3 (maximum of the degree of f_1, f_2). In this example, all the 3 component functions f_1, f_2, and $f_1 \oplus f_2$ are nonlinear; hence, (Q, f) is a pure nonlinear ternary quasigroup.

3. S-Boxes and their cryptographic properties

An $n \times m$ S-box is nothing but a map $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, where $\mathbb{F}_2$ is the Galois field with two elements. An $n \times m$ S-box transforms an n bit value to an m bit value. S-boxes are used to infuse nonlinearity into cryptographic designs. Given a vector $\mathbf{b} \in \mathbb{F}_2^m \backslash \{0\}$, the Boolean function $S_\mathbf{b} : \mathbb{F}_2^n \to \mathbb{F}_2$

0	1	2	3
2	3	1	0
1	0	3	2
3	2	0	1

1	3	0	2
0	2	3	1
3	1	2	0
2	0	1	3

2	0	3	1
3	1	0	2
0	2	1	3
1	3	2	0

3	2	1	0
1	0	2	3
2	3	0	1
0	1	3	2

Figure 2. The four floors of the Latin cube L_{241}.

defined as $S_{\mathbf{b}}(x) = \langle \mathbf{b}, S(\mathbf{x}) \rangle$, is a component function of S. There is 1-1 correspondence between values of $\mathbf{b}$ and the component function of S. The cryptographic properties of an S-box are defined in terms of its component functions. We describe some important cryptographic properties required for our discussion.

Using Equation (1), the *algebraic degree* of S can be given as:

$$\deg(S) = \max_{\mathbf{b} \in \mathbb{F}_2^m \setminus \{0\}} \deg(S_{\mathbf{b}}).$$

A criterion for designing a good S-box is to have the highest possible algebraic degree (Carlet 2010; Leander and Poschmann 2007). It can be seen that the algebraic degree of any invertible map on $\mathbb{F}_2^n$ must be less or equal to $n-1$ [Proposition 2, Carlet 2010].

Let $\mathcal{F}_n$ be the set of all Boolean functions in n variables, $\mathcal{L}_n \subset \mathcal{F}_n$ be the set of linear ones, and $\mathcal{A}_n \subset \mathcal{F}_n$ be the set of affine ones. We have $\mathcal{L}_n \subset \mathcal{A}_n \subset \mathcal{F}_n$.

A Boolean function is said to be *balanced* if its truth table has an equal number of zeroes and ones. And an S-box is balanced if all of its nontrivial component functions are balanced. Equivalently, an $n \times m$ S-box S is said to be balanced if every $\mathbf{y} \in \mathbb{F}_2^m$ has 2^{n-m} pre-images by S. This is one of the criteria that a good S-box should satisfy.

Let $f(\mathbf{x}), g(\mathbf{x}) \in \mathcal{F}_n$, then the correlation coefficient of these functions is defined as:

$$\begin{aligned} C(f,g) &= \frac{1}{2^n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) + g(\mathbf{x})} \\ &= \frac{1}{2^n} \#\{\mathbf{x} \in \mathbb{F}_2^n | f(\mathbf{x}) = g(\mathbf{x})\} - \#\{\mathbf{x} \in \mathbb{F}_2^n | f(\mathbf{x}) \neq g(\mathbf{x})\}. \end{aligned}$$

The correlation coefficient of those Boolean functions whose output bits are statistically independent is equal to zero. Let $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$. The *Walsh transform* of S is the Walsh transform of the component function $S_{\mathbf{b}}$, $\mathbf{b} \in \mathbb{F}_2^m$ and is defined as:

$$W_{S_{\mathbf{b}}}(\mathbf{a}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{S_{\mathbf{b}}(\mathbf{x}) + \langle \mathbf{a}, \mathbf{x} \rangle} = 2^n C(S_{\mathbf{b}}, L_{\mathbf{a}})$$

where $L_{\mathbf{a}}(\mathbf{x}) = \langle \mathbf{a}, \mathbf{x} \rangle = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$ is a linear function with $\mathbf{a}$

as coefficient vector. The *autocorrelation transform* of a Boolean function $f \in \mathcal{F}_n$ with respect to $\mathbf{a} \in \mathbb{F}_2^n$ is defined as $\mathcal{A}_f(\mathbf{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})+f(\mathbf{x}\oplus\mathbf{a})}$. And the *cross-correlation spectrum* between two Boolean functions $f, g \in \mathcal{F}_n$ is defined as:

$$\mathcal{C}_{f,g}(\mathbf{a}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})+g(\mathbf{x}\oplus\mathbf{a})}$$

for every $\mathbf{a} \in \mathbb{F}_2^n$.

The *linearity* of S is the maximum linearity of its component functions and is defined as:

$$\mathrm{Lin}(S) = \max_{\mathbf{b}\in\mathbb{F}_2^m\setminus\{0\}} \mathrm{Lin}(S_\mathbf{b}) = \max_{\mathbf{a}\in\mathbb{F}_2^n,\, \mathbf{b}\in\mathbb{F}_2^m\setminus\{0\}} |W_{S_\mathbf{b}}(\mathbf{a})|.$$

The linearity of an S-box measures resistance against linear cryptanalysis. The smaller the linearity is, the more secure the S-box is against linear attack (Leander and Poschmann 2007). For even n, the smallest known linearity of a bijection on $\mathbb{F}_2^n$ is $2^{\frac{n}{2}+1}$ (Chabaud and Vaudenay 1995).

The *nonlinearity* of an S-box is the minimum nonlinearity of its component functions and can also be defined as:

$$\mathcal{N}_s = \min_{\mathbf{b}\in\mathbb{F}_2^m\setminus\{0\}} \mathcal{N}_{S_\mathbf{b}} = 2^{n-1} - \frac{1}{2} \max_{\mathbf{a}\in\mathbb{F}_2^n,\, \mathbf{b}\in\mathbb{F}_2^m\setminus\{0\}} |W_{S_\mathbf{b}}(\mathbf{a})| = 2^{n-1} - \frac{1}{2}\mathrm{Lin}(S).$$

The degree and the nonlinearity of an S-box quantify the level of confusion brought into the system by the function. To prevent the linear attack, the nonlinearity of cryptographic functions used in block ciphers must be high (Carlet 2010). The larger the nonlinearity is, the more secure the S-box is against linear attack. The nonlinearity of an S-box cannot be more than $2^{n-1} - 2^{\frac{n}{2}-1}$ and, if n is even and $m \leqslant \frac{n}{2}$, then the function that achieves this upper bound is called bent function.

In Biham and Shamir (1991), Biham and Shamir invented the concept of differential cryptanalysis. A cipher is vulnerable to a differential attack if the output differences can be guessed by an attacker with high probability. From the designer's point of view, a block cipher should be designed in such a way that, for any given nonzero input difference, there should not occur a fixed output difference with high probability. The *differential uniformity* of S can also be defined as:

$$\mathrm{Diff}(S) = \max_{\mathbf{a}\in\mathbb{F}_2^n\setminus\{0\},\, \mathbf{b}\in\mathbb{F}_2^m} \#\{\mathbf{x} \in \mathbb{F}_2^n : S(\mathbf{x}\oplus\mathbf{a})\oplus S(\mathbf{x}) = \mathbf{b}\}.$$

For a given fixed nonzero input difference $\mathbf{a}$, the differential uniformity of S is the maximum of the number of message pairs $(\mathbf{x}, \mathbf{x}+\mathbf{a})$ with the fixed output difference $\mathbf{b}$ after applying the S-box. $\mathrm{Diff}(S)$ of an S-box is used to measure the resistance against differential cryptanalysis. The smaller the

$\mathrm{Diff}(S)$ is, the more secure the S-box against the differential cryptanalysis. Clearly, $\mathrm{Diff}(S) \geq 2$ for any $n \times n$ S-box and the permutations for which the lower bound is attained are known as *almost perfect no-linear* (APN) permutations. It has been conjectured that $\mathrm{Diff}(S) \geq 4$ for any $n \times n$ bijective S-box (n even) (Leander and Poschmann 2007). Dillon (2009) disproved this by showing an APN permutation of order 6 has $\mathrm{Diff}(S) = 2$ (Browning, et al. 2010), which is the only even order APN permutation till now.

The reader may refer to Wu and Feng (2016) for a detailed study on S-boxes.

To quantify the resistance of an S-box to DPA attacks, the notion of transparency order (TO) of an S-box has been introduced in Prouff (2005). It measures the resistance of S-boxes against multi-bit DPA attack in Hamming weight model. From the DPA attack's point of view, the bent functions are the weakest possible functions. Hence, bent functions are never used as cryptographic primitives. It has been established that it is not possible to design a function that optimally can resist linear, differential, and DPA attacks. In Prouff (2005), it has been shown that the function satisfying propagation criteria of order k does not have a good transparency order for a large value of k. It may further be noted that this value of k may not necessarily be optimal. Based on differential traces, DPA attacks provide the attacker various kinds of distinguishers to recover the secret key $\dot{\boldsymbol{K}}$. When the hypothesis key is equal to the correct key $\dot{\boldsymbol{K}}$ then the distinguishers take the maximum value. It is difficult for an attacker to identify the correct secret key when the difference between the score of the distinguisher for the correct key is small. The Hamming weight model assumes that the information in the form $T_{\dot{\boldsymbol{K}}}(\mathbf{x}) = H(F(\mathbf{x} \oplus \dot{\boldsymbol{K}}) \oplus \boldsymbol{\beta}) + \omega$ leaks by cryptographic device, where $\mathbf{x}, \dot{\boldsymbol{K}}$ and ω respectively denote the public data, the secret key, and an independent noise. The transparency order of an S-box not only depends on the algebraic properties of the S-box but also on the register initial state $\boldsymbol{\beta}$, which is, by assumption, constant for some platforms. Smaller TO of an S-box gives more resistance against DPA attacks. Under certain assumptions, TO of an $n \times m$ S-box $F = (F_1, F_2, \ldots, F_m)$ is as follows:

$$\mathrm{TO}(F) = \max_{\boldsymbol{\beta} \in \mathbb{F}_2^m} \left(|m - 2H(\boldsymbol{\beta})| - \frac{1}{2^{2n} - 2^n} \sum_{\mathbf{a} \in \mathbb{F}_2^{n^*}} \left| \sum_{i=1}^{m} (-1)^{\beta_i} \mathcal{A}_{F_i}(\mathbf{a}) \right| \right). \tag{2}$$

Later, Chakraborty et al. (2017) introduced the notion of modified transparency order (MTO). The authors explained the assumption that the coordinates of an S-box are uncorrelated with each other on which TO is based on cannot holds in real-world S-boxes like AES S-box. This leads to the

generation of MTO. It is more useful than TO to quantify the DPA resistance of S-box and is defined as:

$$\mathrm{MTO}(F) = \max_{\boldsymbol{\beta}\in\mathbb{F}_2^m}\left(m - \frac{1}{2^{2n}-2^n}\sum_{\mathbf{a}\in\mathbb{F}_2^{n^*}}\sum_{j=1}^{m}\left|\sum_{i=1}^{m}(-1)^{\beta_i\oplus\beta_j}\mathcal{C}_{F_i,F_j}(\mathbf{a})\right|\right). \tag{3}$$

4. Construction of cryptographically strong TQ-S-boxes

First, we define the term cryptographically strong S-boxes. Cryptographically strong S-boxes are those S-boxes that give strong resistance against linear, differential, algebraic, and DPA attacks.

This article aims to generate $2k \times 2k$-bit cryptographically strong TQ-S-boxes from ternary quasigroup Q of order 4, where k is the size of the input string formed by the elements of Q. In this section, we propose an algorithm to construct cryptographically strong S-boxes by using 648 pure nonlinear ternary quasigroups representative (Latin cubes representative) of order 4.

In Lyu and Xu (2015), an e-transformation based on the ternary quasigroup has been defined. It can be written as:

Definition 4. Let (Q, f) be a finite ternary quasigroup with $|Q| \geq 2$. Let $n \geq 2$ be a positive integer. For all ordered pairs $(\alpha, \beta) \in Q \times Q$, the function $L_{f,(\alpha,\beta)} : Q^n \to Q^n$ is defined as follows:

$$L_{f,(\alpha,\beta)}(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \Longleftrightarrow y_i = \begin{cases} f(\alpha, \beta, x_1), i = 1 \\ f(\beta, y_1, x_2), i = 2 \\ f(y_{i-2}, y_{i-1}, x_i), 3 \leqslant i \leqslant n \end{cases} \tag{4}$$

The function $L_{f,(\alpha,\beta)}$ is called an e-transformation of Q^n based on the ternary quasigroup (Q, f) with leader pair (α, β).

We denote this transformation as left e-transformation. In Lyu and Xu (2015), it has been proved that $L_{f,(\alpha,\beta)}$ is bijective.

Below we have defined right e-transformation. These two transformations are used in our algorithm for the construction of cryptographically strong TQ-S-boxes. They are the building blocks of our S-box design.

Definition 5. Let (Q, f) be a finite ternary quasigroup with $|Q| \geq 2$. Let $n \geq 2$ be a positive integer. For all ordered pairs $(\alpha, \beta) \in Q \times Q$, we define a function $R_{f,(\alpha,\beta)} : Q^n \to Q^n$ as follows:

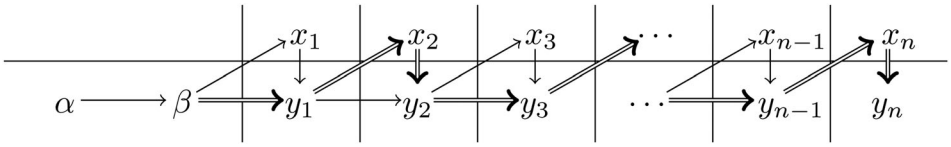

Figure 3. Graphical representation of $L_{f,(\alpha,\beta)}$.

$$R_{f,(\alpha,\beta)}(x_1,x_2,\ldots,x_n)=(y_1,y_2,\ldots,y_n)\iff y_i=\begin{cases}f(\alpha,\beta,x_n), i=n\\ f(\beta,y_n,x_{n-1}), i=n-1\\ f(y_{i+2},y_{i+1},x_i), n-2\geq i\geq 1.\end{cases} \tag{5}$$

The function $R_{f,(\alpha,\beta)}$ is called right e-transformation of Q^n based on the ternary quasigroup (Q, f) with leader pair (α, β).

The graphical representation of $L_{f,(\alpha,\beta)}$ and $R_{f,(\alpha,\beta)}$ with even n are, respectively, shown in Figures 3 and 4.

Theorem 1. *The right e-transformation $R_{f,(\alpha,\beta)}$ in Definition 5 is bijective on Q^n.*

Proof. It is enough to prove that $R_{f,(\alpha,\beta)}$ is an injective function (because Q is finite). For this, we will show that if $(x_1,x_2,\ldots,x_n)$ and $(x'_1,x'_2,\ldots,x'_n)\in Q^n$ be such that $R_{f,(\alpha,\beta)}(x_1,x_2,\ldots,x_n)=R_{f,(\alpha,\beta)}(x'_1,x'_2,\ldots,x'_n)$ then $(x_1,x_2,\ldots,x_n)=(x'_1,x'_2,\ldots,x'_n)$.

Let $R_{f,(\alpha,\beta)}(x_1,x_2,\ldots,x_n)=(y_1,y_2,\ldots,y_n)$, where $y_n=f(\alpha,\beta,x_n)$, $y_{n-1}=f(\beta,y_n,x_{n-1})$, $y_i=f(y_{i+2},y_{i+1},x_i)$ for $n-2\geq i\geq 1$ and $R_{f,(\alpha,\beta)}(x'_1,x'_2,\ldots,x'_v)=(y'_1,y'_2,\ldots,y'_v)$, where $y'_n=f(\alpha,\beta,x'_n), y'_{n-1}=f(\beta,y'_n,x'_{n-1})$, $y'_i=f(y'_{i+2},y'_{i+1},x'_i)$ for $n-2\geq i\geq 1$.

We have $y_n=y'_n$, i.e. $f(\alpha,\beta,x_n)=f(\alpha,\beta,x'_n)$. Hence, by the uniqueness property of the ternary quasigroup described in Definition 2, $x_n=x'_n$. In the similar way $y_n=y'_n$ and $y_{n-1}=y'_{n-1}$ gives $x_{n-1}=x'_{n-1}$. From $y_n=y'_n, y_{n-1}=y'_{n-1}$, and $y_k=y'_k$, i.e., $f(y_{k+2},y_{k+1},x_k)=f(y'_{k+2},y'_{k+1},x'_k)$, we get $x_k=x'_k$ $k=n-2,\ldots,2,1$ for $k=n-2,\ldots,2,1$ (because of uniqueness property). Hence, $R_{f,(\alpha,\beta)}$ is injective. □

Let (Q, f) be a finite ternary quasigroup. Let $L_{f,(\alpha_i,\beta_i)}$ and $R_{f,(\alpha_i,\beta_i)}$ $(i=1,2,\ldots,k)$ be transformations as defined in Equations (4) and (5) with leader pairs $(\alpha_1,\beta_1),(\alpha_2,\beta_2),\ldots,(\alpha_k,\beta_k)\in Q\times Q$. For i $\in$ {1, 2, … , k} and $t_i\in\mathbb{F}_2$, let

$$T_{t_i,f,(\alpha_i,\beta_i)}=\begin{cases}L_{f,(\alpha_i,\beta_i)}, & \text{if } t_i=0\\ R_{f,(\alpha_i,\beta_i)}, & \text{if } t_i=1.\end{cases}$$

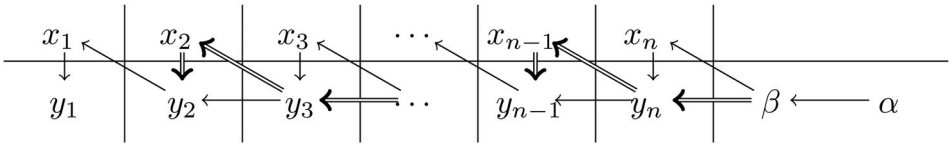

Figure 4. Graphical representation of $R_{f,(\alpha,\beta)}$.

The transformations L, R, and T are defined on Q^n as follows:

$$L = L^{(k)}_{(\alpha_k,\beta_k),(\alpha_{k-1},\beta_{k-1}),\ldots,(\alpha_1,\beta_1)} = L_{f,(\alpha_k,\beta_k)} \circ L_{f,(\alpha_{k-1},\beta_{k-1})} \circ \cdots \circ L_{f,(\alpha_1,\beta_1)}, \quad (6)$$

$$R = R^{(k)}_{(\alpha_k,\beta_k),(\alpha_{k-1},\beta_{k-1}),\ldots,(\alpha_1,\beta_1)} = R_{f,(\alpha_k,\beta_k)} \circ R_{f,(\alpha_{k-1},\beta_{k-1})} \circ \cdots \circ R_{f,(\alpha_1,\beta_1)}, \quad (7)$$

$$T = T^{(k)}_{(\alpha_k,\beta_k),(\alpha_{k-1},\beta_{k-1}),\ldots,(\alpha_1,\beta_1)} = T_{t_k,f,(\alpha_k,\beta_k)} \circ T_{t_{k-1},f,(\alpha_{k-1},\beta_{k-1})} \circ \cdots \circ T_{t_1,f,(\alpha_1,\beta_1)}, \quad (8)$$

where $\circ$ is the usual composition function.

The composition of bijective functions is bijective. Hence, from Theorem 1, we get the transformations L, R, and T as defined above are bijective. We have the following corollary:

Corollary 1.1. *The transformations L, R, and T defined in Equations (6, 7) and (8) are bijective on* Q^n.

Before going to the algorithm for the construction of cryptographically strong (C.S.) TQ-S-boxes, we describe criteria for a $2k \times 2k$-bit cryptographically strong TQ-S-box. For C.S. TQ-S-boxes we have set criteria on their cryptographic properties. The criteria comprise three functions, namely nonlinearity, differential uniformity, and algebraic degree. Table 1 shows the criteria for 4, 6, and $2k$ ($k \geq 4$) order S-boxes, which are based on the following observations.

As discussed in Section 3, the resistance against linear and differential cryptanalysis is the basic requirement for an S-box and hence for secure block cipher. In Nyberg (1991), Nyberg showed that there is no bent function on $\mathbb{F}_2^n$ for any $n \in \mathbb{N}$. Hence, in any bijective n-bit S-box, $\mathcal{N}_s \leqslant 2^{n-1} - 2^{\frac{n}{2}}$. We have discussed in the previous section that the nonlinearity of an S-box quantifies the level of confusion and prevents linear attack. The nonlinearity of an S-box must be as high as possible. Therefore, the nonlinearities in the criteria are, respectively, taken as $\mathcal{N}_s = 4, 12 \leqslant \mathcal{N}_s \leqslant 24$, and $2^{2k-1} - 2^{k+1} - 2^k \leqslant \mathcal{N}_s \leqslant 2^{2k-1} - 2^k$ for 4, 6, and $2k$-bit ($k \geq 4$) S-boxes. For any S-box, we have $\mathrm{Diff}(S) \geq 2$, but there is no 4-bit S-box having $\mathrm{Diff}(S) = 2$. This is because it has been proven that there is no APN permutation on $\mathbb{F}_2^4$. Also, $\mathrm{Diff}(S)$ is always even, hence any 4-bit S-box must have $\mathrm{Diff}(S) \geq 4$, As discussed earlier, the differential uniformity of an S-box must be as small as possible to protect it against differential cryptanalysis. Hence, we took $\mathrm{Diff}(S) = 4, 2 \leqslant \mathrm{Diff}(S) \leqslant 10$, and

$2 \leqslant \mathrm{Diff}(S) \leqslant 4k-2$, respectively, as third conditions in the Table (as there exist 4-bit S-box with $\mathrm{Diff}(S) = 4$ and 6-bit S-box with $\mathrm{Diff}(S) = 2$). As discussed in the previous section, the algebraic degree of any bijective map on $\mathbb{F}_2^n$ must be less than or equal to $n-1$. Hence, we have taken $\deg(S) = n-1$ for $n \times n$-bit S-boxes.

We now propose an algorithm for the construction of cryptographically strong TQ-S-boxes of even order using ternary quasigroups of order 4 (over $Q = \mathbb{F}_2^2$). In this algorithm, out of 2,304 representatives of Latin cubes of order 4, we only use 648 pure nonlinear representatives in the construction. Let I denote the indices of these pure nonlinear representatives (listed in Table 1 of Yu and Xu (2017)), i.e. $I = \{i : L_i$ is pure nonlinear representative$\}$.

We take three positive integers k (the size of the input string), r (the number of rounds), and m (the number of leader pairs) such that $r \geq 4$ and even, and $m \leqslant r$. For each pure nonlinear ternary quasigroup representative L_i, $i \in I$, we choose m leader pairs $(\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_m, \beta_m)$ from $Q \times Q$. If $m < r$, then we pick $s_1, s_2, \ldots, s_{r-m}$, a sequence of length $(r-m)$ from $\{1, 2, \ldots, m\}$. We finally have r leader pairs $(\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m), (\alpha_{m+1}, \beta_{m+1}) = (\alpha_{s_1}, \beta_{s_1}), (\alpha_{m+2}, \beta_{m+2}) = (\alpha_{s_2}, \beta_{s_2}), \ldots, (\alpha_r, \beta_r) = (\alpha_{s_{r-m}}, \beta_{s_{r-m}})$. Using these leader pairs, we construct an S-box S: $\mathbb{F}_2^{2k} \to \mathbb{F}_2^{2k}$ as:

$$S = T_{1,f,(\alpha_r,\beta_r)} \circ \cdots \circ T_{1,f,(\alpha_2,\beta_2)} \circ T_{0,f,(\alpha_1,\beta_1)},$$

where each transformation is taken with respect to L_i. Then the criteria in Table 1 are checked for the constructed S-box. If the S-box satisfies the criteria, then we put it in the set $\mathcal{C}$ of C.S. TQ-S-boxes. At the end, we get a set $\mathcal{C}$ containing cryptographically strong $2k \times 2k$-bit TQ-S-boxes.

Algorithm 1 precisely describes the construction of cryptographically strong TQ-S-boxes in the form of pseudo-code. We noticed that the TQ-S-boxes obtained by using odd or less than 4 rounds are weaker. So in the Algorithm, we have taken at least 4 and even numbers of rounds. We show in the next section that the S-boxes so generated also have good resistance to the DPA attack. The obtained set $\mathcal{C}$ can be analysed for various cryptographic properties and can be used for many purposes, like designing lightweight block ciphers and hash functions.

Algorithm 1 Construction of cryptographically strong TQ-S-boxes

Inputs:

1. $k-$ the size of the input string (formed by the elements of Q)
2. $r-$ the number of rounds ($r \geq 4$, even)
3. $m-$ the number of leader pairs ($m \leqslant r$)
4. $S = s_1, s_2, \ldots, s_{r-m}$, a sequence of length $r-m$ from $\{1, 2, \ldots, m\}$

5. The pre-computed set $I = \{i | L_i$ is a pure nonlinear ternary quasigroup representative$\}$

Outputs:

1. u- the number of cryptographically strong $2k \times 2k$-bit TQ-S-boxes generated
2. A set $\mathcal{C}$ of u cryptographically strong $2k \times 2k$-bit TQ-S-boxes. $\mathcal{C} = \{S_1, S_2, ..., S_u\}$.

1: **function** Gen_CS_SB(k, r, m, S, I)
2: $u := 0$
3: $\mathcal{C} := \emptyset$
4: **for** $i \in I$ **do**
5: $M := \{(\alpha_1, \beta_1), (\alpha_2, \beta_2), ..., (\alpha_m, \beta_m) | \alpha_i, \beta_i \in Q, \forall 1 \leqslant i \leqslant m\}$
6: **while** $M \neq \emptyset$ **do**
7: pick $\{(\alpha_1, \beta_1), (\alpha_2, \beta_2), ..., (\alpha_m, \beta_m)\} \in M$
8: **for** $\mathbf{x} \in \mathbb{F}_2^{2k}$ **do**
9: $\mathbf{y} := \mathbf{x}$
10: **for** $j = 1$ to m **do**
11: $t \equiv (j-1) \bmod 2$
12: $\mathbf{y} := T_{t,f,(\alpha_j,\beta_j)}(\mathbf{y})$ ▷ $T_{t,f,(\alpha_j,\beta_j)}$ is taken w.r.t L_i.
13: **end for**
14: **for** $j = 1$ to $r - m$ **do**
15: $t \equiv (m + j - 1) \bmod 2$
16: $\mathbf{y} := T_{t,f,(\alpha_{s_j},\beta_{s_j})}(\mathbf{y})$ ▷ $T_{t,f,(\alpha_{s_j},\beta_{s_j})}$ is taken w.r.t L_i.
17: **end for**
18: Set $S_u(\mathbf{x}) := \mathbf{y}$
19: **end for**
20: **if** S_u satisfies the criteria in Table 1 **then**
21: $\mathcal{C} := \mathcal{C} \cup \{S_u\}$
22: $u := u + 1$
23: **end if**
24: $M := M \backslash \{(\alpha_1, \beta_1), (\alpha_2, \beta_2), ..., (\alpha_m, \beta_m)\}$
25: **end while**
26: **end for**
27: **return** $(u, \mathcal{C})$
28: **end function**

Below we have given an example to explain the working of the algorithm for $k = 2$, $r = 4$ and $m = 4$. In this example, we have constructed one 4×4-bit cryptographically strong TQ-S-box.

Table 2. TQ-S-box in its hexadecimal notation.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(\mathbf{x})$	1	2	F	3	D	A	E	9	0	4	C	8	5	6	7	B

Example 2. Consider pure nonlinear representative L_{241} (as shown in Example 1). Let $(0,2),(3,1),(1,1),(1,0)$ be 4 leader pairs used in 4 rounds. Then, from the algorithm, a 4×4 TQ-S-box is obtained in the following way.

Let f be the corresponding ternary operation associated with L_{241}. We take input one by one (in lexicographical order) and obtain output as follows:

For input $0=(0,0)\in Q\times Q$:

Round 1: $L_{f,(0,2)}(0,0)=(a_1,a_2)$, where $a_1=f(0,2,0)=2, a_2=f(2,2,0)=3$. Therefore, $L_{f,(0,2)}(0,0)=(2,3)$.

Round 2: $R_{f,(3,1)}(2,3)=(b_1,b_2)$, where $b_2=f(3,1,3)=1, b_1=f(1,1,2)=1$. Therefore, $R_{f,(3,1)}(2,3)=(1,1)$.

Round 3: $L_{f,(1,1)}(1,1)=(c_1,c_2)$, where $c_1=f(1,1,1)=2, c_2=f(1,2,1)=3$. Therefore, $L_{f,(0,2)}(0,0)=(2,3)$.

Round 4: $R_{f,(1,0)}(2,3)=(d_1,d_2)$, where $d_2=f(1,0,3)=1, d_1=f(0,1,2)=0$. Therefore, $R_{f,(1,0)}(2,3)=(0,1)$.

The output (0, 1) of the last round (4th) is the final output of (0, 0). In hexadecimal, (0, 1) is 1. Hence, $S(0)=1$.

For input $1=(0,1)\in Q\times Q$:

Round 1: $L_{f,(0,2)}(0,1)=(a_1,a_2)$, where $a_1=f(0,2,0)=2, a_2=f(2,2,1)=2$. Therefore, $L_{f,(0,2)}(0,1)=(2,2)$.

Round 2: $R_{f,(3,1)}(2,2)=(b_1,b_2)$, where $b_2=f(3,1,2)=3, b_1=f(1,3,2)=2$. Therefore, $R_{f,(3,1)}(2,3)=(2,3)$.

Round 3: $L_{f,(1,1)}(2,3)=(c_1,c_2)$, where $c_1=f(1,1,2)=1, c_2=f(1,1,3)=0$. Therefore, $L_{f,(0,2)}(0,0)=(1,0)$.

Round 4: $R_{f,(1,0)}(1,0)=(d_1,d_2)$, where $d_2=f(1,0,0)=2, d_1=f(0,2,1)=0$. Therefore, $R_{f,(1,0)}(2,3)=(0,2)$.

The output (0, 2) of the last round (4th) is the final output (0, 1). In hexadecimal, (0, 2) is 2. Hence, $S(1)=2$.

Continuing in a similar fashion, we obtain the TQ-S-box as shown in Table 2.

The obtained TQ-S-box has the following properties:

1. Balanced,
2. Nonlinearity $=4$,
3. Differential uniformity $=4$,
4. Degree $=3$.

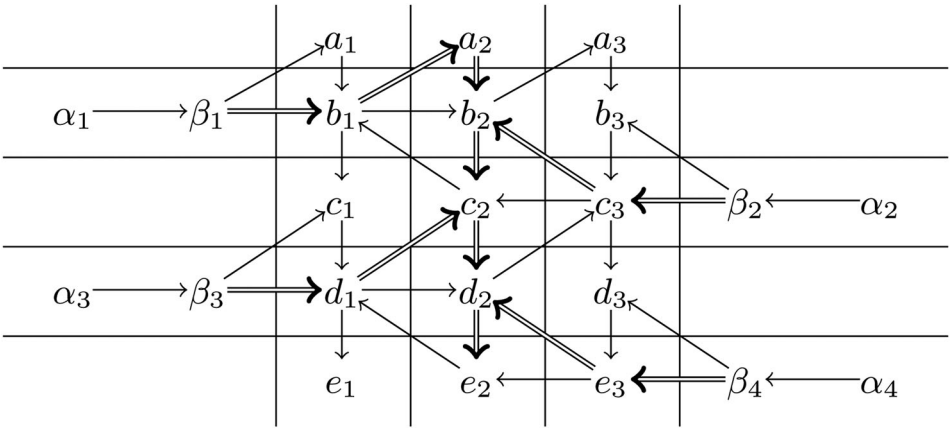

Figure 5. Graphical representation of 4 rounds construction of 6-bit TQ-S-box from leaders $(\alpha_1, \beta_1), (\alpha_2, \beta_2), (\alpha_3, \beta_3)$, and$(\alpha_4, \beta_4)$.

Hence, this S-box is satisfying the criteria for a cryptographically strong S-box as defined in Table 1.

From the algorithm, 65,536 TQ-S-boxes of order 4 get constructed from ternary quasigroup L_{241} with $r = 4$ and $m = 4$, out of which 4,096 satisfy the criteria for cryptographically strong TQ-S-boxes.

Note: In the above example, for the given leader pairs and 4 rounds, the TQ-S-box $S : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ can also be written as a composition of left and right e-transformations defined in Equations (4) and (5) as follows:

$$S = S^{(4)}_{(0,2),(3,1),(1,1),(1,0)} = R_{f,(1,0)} \circ L_{f,(1,1)} \circ R_{f,(3,1)} \circ L_{f,(0,2)}.$$

In general, consider a ternary quasigroup (Q, f). Let r be the number of rounds. Then, for leader pairs $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \ldots, (\alpha_r, \beta_r)$, the TQ-S-box defined in the algorithm is a function $S : \mathbb{F}_2^{2k} \to \mathbb{F}_2^{2k}$ and can also be written as a composition of left and right e-transformations as follows:

$$S = S^{(r)}_{(\alpha_r,\beta_r),(\alpha_{r-1},\beta_{r-1}),\ldots,(\alpha_1,\beta_1)} = R_{f,(\alpha_r,\beta_r)} \circ L_{f,(\alpha_{r-1},\beta_{r-1})} \circ \cdots \circ L_{f,(\alpha_1,\beta_1)}. \quad (9)$$

Corollary 1.2. *All the TQ-S-boxes generated through the algorithm are balanced.*

Proof. In view of representation (9) and Corollary 1.1, all the TQ-S-boxes generated are bijective. Also, in symmetric S-boxes, bijective implies balancedness. Therefore, all the TQ-S-boxes generated through the algorithm are balanced. □

From the above result, it can be concluded that there is no need to check the balancedness in the algorithm.

Figure 5 graphically represents 4 rounds of the algorithm for 6-bit input. The j-th row in the figure starts with leader pair (α_j, β_j), for $j = 1, 2, 3, 4$ and bijectively transforms 6-bit input into 6-bit output. The output of each round becomes the input of the next round. Left and right e-transformations are used alternatively in each subsequent round. The 6-bit output obtained in the last round is the final output.

Theorem 2. *None of the TQ-S-boxes constructed through the algorithm is linear.*

Proof. Consider a pure nonlinear ternary quasigroup (Q, f) of order 2^2. Then, for any $x, y, z, w \in Q, f(x, y, z) = w$ can be written as:

$$f(x, y, z) = (f_0(x, y, z), f_1(x, y, z)),$$

where the Boolean functions $f_0 : \mathbb{F}_2^6 \to \mathbb{F}_2$ and $f_1 : \mathbb{F}_2^6 \to \mathbb{F}_2$ are the coordinate functions of f (i.e., the binary representation of w). Let, for all leader pairs$(\alpha, \beta) \in Q \times Q$, left and right e-transformations $L_{f,(\alpha,\beta)}$ and $R_{f,(\alpha,\beta)}$ on Q^k are as given in Equations (4) and (5), respectively. Now in order to prove the constructed TQ-S-boxes are nonlinear, it is enough to prove that at least one component function of it has degree greater than 1. We will prove this by induction on the number of rounds taken for the construction of TQ-S-boxes because the number of rounds in the algorithm is greater than or equal to 4 and even. Hence, we will first prove the result for 4 rounds.

Let k be the size of the input string in the algorithm. We start the first round with leader pair, say $(\alpha_1, \beta_1) \in Q^2$ and input $(a_1, a_2, ..., a_k) \in Q^k$. On application of left e-transformation, we get $L_{f,(\alpha_1,\beta_1)}(a_1, a_2, ..., a_k) = (b_1, b_2, ..., b_k)$ as output of the first round, where $b_1 = f(\alpha_1, \beta_1, a_1), b_2 = f(\beta_1, b_1, a_2)$, and $b_i = f(b_{i-2}, b_{i-1}, a_i) \ \forall \ i = 3, 4, ..., k$. Hence, the second round starts with leader pair (α_2, β_2) (say) and input $(b_1, b_2, ..., b_k)$. After applying right e-transformation, we get the output $R_{f,(\alpha_2,\beta_2)}(b_1, b_2, ..., b_k) = (c_1, c_2, ..., c_k)$, where $c_k = f(\alpha_2, \beta_2, b_k), c_{k-1} = f(\beta_2, c_k, b_{k-1})$ and $c_i = f(c_{i+2}, c_{i+1}, b_i) \ \forall \ i = k-2, ..., 2, 1$. Now the output of the third round is computed using leader pair (α_3, β_3) (say) and input $(c_1, c_2, ..., c_k)$. Hence, the output of the third round will be $L_{f,(\alpha_3,\beta_3)}(c_1, c_2, ..., c_k) = (d_1, d_2, ..., d_k)$, where $d_1 = f(\alpha_3, \beta_3, c_1), d_2 = f(\beta_3, d_1, c_2)$ and $d_i = f(d_{i-2}, d_{i-1}, c_i) \ \forall \ i = 3, 4, ..., k$. In the fourth round, we have leader pair (α_4, β_4) (say) and input $(d_1, d_2, ..., d_k)$. The output of the forth round is computed as $R_{f,(\alpha_4,\beta_4)}(d_1, d_2, ..., d_k) = (e_1, e_2, ..., e_k)$, where $e_k = f(\alpha_4, \beta_4, d_k), e_{k-1} = f(\beta_4, e_k, d_{k-1})$, and $e_i = f(e_{i+2}, e_{i+1}, d_i) \ \forall \ i = k-2, ..., 2, 1$. Therefore, after 4 rounds, we get the TQ-S-box as a function $S : \mathbb{F}_2^{2k} \to \mathbb{F}_2^{2k}$ and is given by:

$$\begin{aligned} S(a_1, a_2, ..., a_k) &= R_{f,(\alpha_4,\beta_4)} \circ L_{f,(\alpha_3,\beta_3)} \circ R_{f,(\alpha_2,\beta_2)} \circ L_{f,(\alpha_1,\beta_1)}(a_1, a_2, ..., a_k) \\ &= (e_1, e_2, ..., e_k), \end{aligned}$$

where $e_1, e_2, ..., e_k$ are defined as above. For any vector $u \in \mathbb{F}_2^{2k} \backslash \{0\}$, the component function of S corresponding to u is a Boolean function $S_u : \mathbb{F}_2^{2k} \to \mathbb{F}_2$ such that $S_u(x) = \langle u, S(x) \rangle \forall x \in \mathbb{F}_2^{2k}$. Let (e_i', e_i'') be the binary representation of e_i, for $i = 1, 2, ..., k$ (as $e_i \in Q = \mathbb{F}_2^2$). Let us take $u = (1, \underbrace{0, 0, ..., 0}_{2k-1})$ and $v = (0, 1, \underbrace{0, 0, ..., 0}_{2k-2})$ (in binary). Therefore, $S_u(x) = e_1' = f_0(e_3, e_2, d_1)$ and $S_v(x) = e_1'' = f_1(e_3, e_2, d_1)$. Because (Q, f) is a pure nonlinear ternary quasigroup, it implies all of the 3 component functions of f are nonlinear, i.e., of degree > 1, and also e_3, e_2, and d_1 are functions of $a_1, a_2, ..., a_k$. Thus, at least one of $S_u(x)$ and $S_v(x)$ has degree greater than 1. We have $\deg(S) = \max_{b \in \mathbb{F}_2^{2k} \backslash \{0\}} \deg(S_b)$ and there exists at least one component function with degree > 1. Therefore, $\deg(S) > 1$. Hence, all the TQ-S-boxes constructed from 4 rounds are nonlinear.

Suppose none of the TQ-S-boxes constructed from r rounds ($r \geqslant 4$, even) is linear. We will prove the result for $(r + 2)$ rounds. Let a TQ-S-box obtained after r rounds be $S^{(1)}(a_1, a_2, ..., a_k) = (b_1, b_2, ..., b_k)$. Hence, the TQ-S-box $S^{(1)}$ is nonlinear and has at least one component function having degree greater than 1. The output of $(r + 1)^{\text{th}}$ round is obtained on application of left e-transformation on $(b_1, b_2, ..., b_k)$ with leader pair (α_1, β_1) (say). Therefore, we get $L_{f,(\alpha_1,\beta_1)}(b_1, b_2, ..., b_k) = (c_1, c_2, ..., c_k)$, where $c_1 = f(\alpha_1, \beta_1, b_1), c_2 = f(\beta_1, c_1, b_2)$ and $c_i = f(c_{i-2}, c_{i-1}, b_i)\ \forall\ i = 3, 4, ..., k$, which will be the input of the next $(r + 2)^{\text{th}}$ round. Hence, on applying right e-transformation with leader pair, say (α_2, β_2), we get the output $R_{f,(\alpha_2,\beta_2)}(c_1, c_2, ..., c_k) = (d_1, d_2, ..., d_k)$, where $d_k = f(\alpha_2, \beta_2, c_k), d_{k-1} = f(\beta_2, d_k, c_{k-1})$ and $d_i = f(d_{i+2}, d_{i+1}, c_i)\ \forall\ i = k-2, ..., 2, 1$. The TQ-S-box obtained after $(r + 2)$ rounds is given by:

$$S(a_1, a_2, ..., a_k) = R_{f,(\alpha_2,\beta_2)} \circ L_{f,(\alpha_1,\beta_1)} \circ S^{(1)}(a_1, a_2, ..., a_k) = (d_1, d_2, ..., d_k)$$

Let (d_i', d_i'') be the binary representation of d_i, for $i = 0, 1...., k$. Let us take $u = (1, 0, ..., 0)$ and $v = (0, 1, 0, ..., 0) \in \mathbb{F}_2^{2k} \backslash \{0\}$. Therefore, $S_u(x) = d_1' = f_0(d_3, d_2, c_1)$ and $S_v(x) = d_1'' = f_1(d_3, d_2, c_1)$. Hence, from the given hypothesis and because (Q, f) is a pure nonlinear ternary quasigroup, we get at least one of $S_u(x)$ and $S_v(x)$ has degree greater than 1. We have $\deg(S) = \max_{b \in \mathbb{F}_2^m \backslash \{0\}} \deg(S_b)$ and there exists at least one component function with degree > 1. Therefore, $\deg(S) > 1$. Hence all the TQ-S-boxes constructed from $(r + 2)$ rounds are nonlinear.

Hence, by the principle of mathematical induction, none of the TQ-S-boxes constructed through the algorithm is linear. □

5. Experimental verification and cryptographic analysis

In this section, we will do an analysis on the TQ-S-boxes that are generated for $k = 2$, 3, and 4 from the algorithm described in the previous section. For $k = 2$, 3, and 4, we, respectively, get $4 \times 4, 6 \times 6,$ and 8×8-bit TQ-S-boxes. Now we discuss them one after the other.

5.1. 4 × 4 TQ-S-boxes

If $k = 2$ in the algorithm, we get cryptographically strong 4×4-bit TQ-S-boxes. The number of TQ-S-boxes so generated depends on the number of leader pairs, i.e., m. Here in our analysis, we have considered two cases: first when the number of leaders is 2 and second when they are 4 in number, both for 4 rounds.

Case I: If $r = 4$ and $m = 2$, i.e, 4 rounds and 2 leaders.

The number of leaders is 2. Then we further have 4 subcases, according to the pair of leaders taken for the 3rd and 4th rounds. The leader pairs for the 3rd and 4th rounds are taken from the initially chosen 2 leaders and this can be done in 16×16 ways. Because only pure nonlinear representatives are used in the TQ-S-box construction, and they are 648 in number. Therefore, $648 \times 16 \times 16 = 165{,}888$, are the total number of 4×4 TQ-S-boxes gets generated through the algorithm. Let (α_j, β_j) denotes the leader at the j-*th* round for $j = 1, 2, 3, 4,$ then the 4 subcases are as follows:

1. $(\alpha_3, \beta_3) = (\alpha_4, \beta_4) = (\alpha_2, \beta_2)$: When the leader pairs taken for both 3rd and 4th rounds are equal to the 2nd leader.
2. $(\alpha_3, \beta_3) = (\alpha_4, \beta_4) = (\alpha_1, \beta_1)$: When the leader pairs taken for both 3rd and 4th rounds are equal to the 1st leader.
3. $(\alpha_3, \beta_3) = (\alpha_1, \beta_1), (\alpha_4, \beta_4) = (\alpha_2, \beta_2)$: When the leader pair taken for the 3rd round is equal to the 1st leader and for the 4th round, the 2nd one is taken.
4. $(\alpha_3, \beta_3) = (\alpha_2, \beta_2), (\alpha_4 \beta_4) = (\alpha_1, \beta_1)$: When the leader pair taken for the 3rd round is equal to the 2nd leader and for the 4th round, the 1st one is taken.

In each of these subcases, the filter function is applied on 165,888 generated S-boxes to obtain cryptographically strong TQ-S-boxes of order 4.

Case II: If $r = 4$ and $m = 4$, i.e., 4 rounds and 4 leaders.

Four leaders are taken from the set of all possible leader pairs and this can be done in $16 \times 16 \times 16 \times 16 = 65536$ number of ways. Hence, from 648 pure nonlinear representatives $648 \times 65{,}536 = 4{,}2467{,}328$ number of 4×4 TQ-S-boxes get generated. The filter function is applied on the generated S-boxes to obtain cryptographically strong TQ-S-boxes of order 4 and

Table 3. Distribution of 4×4 TQ-S-boxes.

Case	Subcase	$\mathcal{N}_s = 4$		Diff$(S) = 4$		deg$(S) = 3$		C.S. TQ-S-boxes	
		n	%	*n*	%	*n*	%	*n*	%
I.	1.	45,312	27.31	39,168	23.61	135,168	81.48	39,168	23.61
	2.	37,248	22.45	19,008	11.46	135,360	81.60	19,008	11.46
	3.	35,520	21.41	28,992	17.48	145,344	87.62	28,992	17.48
	4.	47,040	28.36	28,416	17.13	135,360	81.60	28,416	17.13
II.		9,080,832	21.38	4,399,104	10.36	35,807,232	84.32	4,399,104	10.36

these are 4,399,104 in number. Hence, 10.359% of the TQ-S-boxes so obtained are cryptographically strong.

The total number of cryptographically strong 4×4 TQ-S-boxes and a distribution of the total obtained TQ-S-boxes in both the cases discussed above are shown in Table 3.

One of the C.S. 4×4 TQ-S-boxes obtained in case II is shown in Example 2.

We have analysed the modified transparency order (MTO) (Chakraborty et al. 2017) of the C.S. TQ-S-boxes obtained from all the 4 subcases of the case I and case II. The data obtained in the 4 subcases of case I are graphically shown in the form of a histogram in Figure 6. The values of modified transparency order of all the obtained 4×4 C.S. TQ-S-boxes range from 2.233333 to 2.800000 in all 4 subcases of case I. And the minimum and maximum MTO of all the obtained C.S. TQ-S-boxes in case II are respectively 2.033333 and 2.800000.

It has been shown in Duan et al. (2016) and Zhang et al. (2010) that the ultra-light block cipher PRESENT (Bogdanov et al. 2007) is not resistant to DPA attacks. As we know, the lesser the MTO of an S-box the more secure the S-box is against DPA attacks. So in order to have resistance against DPA attacks, one should have an S-box with MTO as low as possible. It can be checked that the MTO of the S-box used in PRESENT cipher is 2.466667. So it can be replaced by some suitably chosen S-box with lesser MTO. Table 4 shows the number of C.S. TQ-S-boxes obtained through our algorithm having MTO less than the S-box in PRESENT cipher (for the 2 cases). These TQ-S-boxes have more resistance against DPA attacks, hence, can be used in PRESENT cipher.

5.2. 6 × 6 TQ-S-boxes

If $k = 3$ in the algorithm we get cryptographically strong 6×6-bit TQ-S-boxes. The number of TQ-S-boxes generated depends on the number of leader pairs, i.e., m. We have considered the same two cases as discussed above and study the cryptographic properties of the generated TQ-S-boxes.

Case I: If $r = 4$ and $m = 2$, i.e., 4 rounds and 2 leaders.

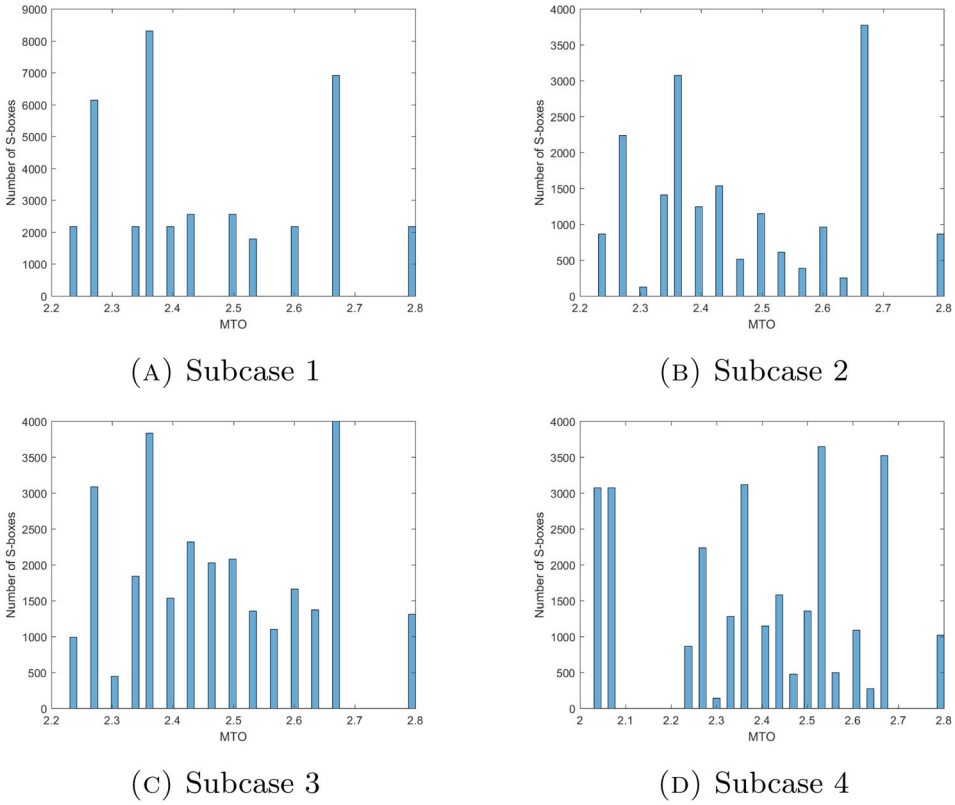

Figure 6. Graphical representation of MTO of C.S. TQ-S-boxes of order 4 obtained from case I.

Table 4. C.S. TQ-S-boxes having MTO less than the S-box in PRESENT.

Case	Subcase	C.S. TQ-S-boxes	MTO less than PRESENT	
			n	%
I.	1.	39,168	23,552	60.013
	2.	19,008	10,496	55.219
	3.	28,992	14,064	48.510
	4.	28,416	16,528	58.164
II.		4,399,104	2,096,128	47.649

There are in total $648 \times 16 \times 16 = 165{,}888$ 6×6 TQ-S-boxes that get generated through the algorithm. Let (α_j, β_j) denotes the leader at the j-th round for $j = 1, 2, 3, 4$, then we have the same 4 subcases as discussed for the 4×4 TQ-S-boxes. In each of the 4 subcases, the filter function is applied on the generated S-boxes to obtain cryptographically strong TQ-S-boxes of order 6.

Case II: If $r = 4$ and $m = 4$, i.e., 4 rounds and 4 leaders.

Four leaders are taken from the set of all possible leader pairs and this can be done in $16 \times 16 \times 16 \times 16 = 65536$ number of ways. Hence, from 648 pure nonlinear representatives, $648 \times 65{,}536 = 4{,}2467{,}328$ number of 6×6 TQ-S-boxes get generated. The filter function is applied on these

Table 5. Distribution of 6×6 TQ-S-boxes.

Case	Subcase	$12 \leqslant \mathcal{N}_s \leqslant 24$		$2 \leqslant \text{Diff}(S) \leqslant 10$		$\deg(S) = 5$		C.S. TQ-S-boxes	
		n	%	*n*	%	*n*	%	*n*	%
I.	1.	160,896	96.99	110,256	66.46	164,928	99.42	110,064	66.35
	2.	162,084	97.71	109,416	65.96	165,528	99.78	109,362	65.93
	3.	160,938	97.02	109,296	65.89	165,480	99.75	108,642	65.49
	4.	161,334	97.25	106,890	64.44	165,336	99.67	106,764	64.36
II.		41,660,976	98.10	28,402,416	66.88	42,408,576	99.86	28,303,152	66.65

S-boxes to obtain cryptographically strong TQ-S-boxes of order 6 and these are 28,303,152 in number. Hence, 66.65% of the TQ-S-boxes so obtained are cryptographically strong.

The total number of cryptographically strong TQ-S-boxes and a distribution of the total obtained TQ-S-boxes in both the cases discussed above are shown in Table 5. From the table, it can be said that, in both cases, almost all the TQ-S-boxes obtained through our algorithm have algebraic degree 5.

One of the C.S. 6×6 TQ-S-boxes obtained from the algorithm is given in Table 6. In this table, column determines 3 least significant bits and row determines 3 most significant bits. For example, the entry $0c$ in the table, at the intersection of 100 row and 001 column, is the output of 100001. This S-box has been obtained from ternary quasigroup L_{33} (in lexicographical order) and leader pairs $(0,0),(0,3),(0,2),(1,3)$. It has nonlinearity$= 20$, differential uniformity $= 6$, and degree$= 5$.

Now after the analysis of the modified transparency order of the C.S. TQ-S-boxes obtained from all the 4 subcases of the case I and case II. The maximum and minimum values of MTO of all the C.S. 6×6 TQ-S-boxes obtained in 4 subcases of case I as well as for case II are shown in Table 7.

5.3. 8×8 TQ-S-boxes

If $k = 4$ in the algorithm, we get cryptographically strong 8×8-bit TQ-S-boxes. Here also we discuss the same two cases and study the cryptographic properties of the generated TQ-S-boxes.

Case I: If $r = 4$ and $m = 2$, i.e., 4 rounds and 2 leaders.

There are in total $648 \times 16 \times 16 = 165{,}888$ 8×8 TQ-S-boxes that get generated. Let (α_j, β_j) denotes the leader at the j-th round for $j = 1, 2, 3, 4$, then we have the same 4 subcases as discussed for the 4×4 TQ-S-boxes. In each of the 4 subcases, the filter function is applied on the generated S-boxes to obtain cryptographically strong TQ-S-boxes of order 8.

Case II: If $r = 4$ and $m = 4$, i.e., 4 rounds and 4 leaders.

Four leaders are taken from the set of all possible leader pairs. Then there are, in total, $648 \times 16 \times 16 \times 16 \times 16 = 42{,}467{,}328$ number of 8×8 TQ-S-boxes generated. The filter function is applied on these S-boxes to obtain cryptographically strong TQ-S-boxes of order 8.

Table 6. Example of C.S. 6×6 TQ-S-box in its hexadecimal notation.

	000	001	010	011	100	101	110	111
000	14	1*b*	32	0*e*	11	2*c*	38	0*f*
001	17	03	3*b*	2*f*	04	23	1*e*	39
010	2*e*	2*b*	31	29	3*c*	3*f*	37	3*a*
011	26	33	05	20	2*a*	12	0*a*	28
100	00	0*c*	1*a*	35	08	34	1*f*	16
101	13	02	18	30	19	25	27	1*d*
110	1*c*	07	10	09	06	3*e*	01	22
111	0*b*	0*d*	3*d*	2*d*	36	24	21	15

Table 7. MTO of C.S. 6×6 TQ-S-boxes.

Case	Subcase	MTO values	
		Min	Max
I.	1.	4.277778	4.708333
	2.	4.277778	4.700397
	3.	4.134921	4.716270
	4.	4.277778	4.722222
II.		4.13492	4.74802

Table 8. Distribution of 8×8 TQ-S-boxes.

Case	Subcase	$80 \leqslant \mathcal{N}_s \leqslant 112$		$2 \leqslant \text{Diff}(S) \leqslant 14$		$\deg(S) = 7$		C.S. TQ-S-boxes	
		n	%	*n*	%	*n*	%	*n*	%
I.	1.	151,824	91.52	114,000	68.72	165,888	100	109,632	66.09
	2.	152,340	91.83	108,096	65.16	165,888	100	104,028	62.71
	3.	154,050	92.86	111,006	66.92	165,888	100	106,686	64.31
	4.	153,720	92.66	114,174	68.83	165,888	100	110,100	66.37
II.		34,107,504	80.31	28,964,784	68.20	42,467,328	100	27,861,360	65.61

Table 9. Example of C.S. 8×8 TQ-S-box in its hexadecimal notation.

	00	01	02	03	04	05	06	07	08	09	0*a*	0*b*	0*c*	0*d*	0*e*	0*f*
00	76	*a*5	*ff*	*c*3	48	*db*	*f*0	9*c*	39	13	1*b*	*c*9	9*b*	70	*e*8	*d*1
10	7*a*	1*f*	52	*d*0	77	15	*ab*	*f*5	*a*8	*f*6	*e*0	*e*7	2*e*	*ef*	*f*4	41
20	5*e*	42	91	35	36	9*e*	10	*bb*	*d*6	4*d*	*b*5	*c*6	11	7*c*	*d*9	84
30	*df*	17	95	28	6*c*	6*b*	*a*2	*fe*	50	5*f*	71	*ee*	*b*8	*ae*	*ea*	3*d*
40	20	67	68	74	*f*8	*a*0	55	8*e*	*a*6	*b*3	75	60	*a*1	*f*2	4*c*	*ec*
50	*cf*	22	2*a*	*e*9	9*f*	65	3*b*	*cb*	69	49	*de*	96	25	6*e*	8*f*	54
60	3*e*	8*d*	90	81	*e*1	*d*8	*ad*	40	*fb*	*f*9	37	*b*2	*cc*	*b*0	51	*e*5
70	43	*b*6	47	*e*6	82	*bf*	05	*be*	9*a*	58	*bc*	*eb*	7*e*	87	7*b*	5*b*
80	*f*3	*d*3	0*b*	1*e*	0*d*	57	*d*4	6*a*	78	59	44	1*a*	*ca*	9*d*	64	09
90	4*e*	*c*1	30	*ac*	83	6*d*	*a*4	5*d*	2*d*	53	*c*4	03	*e*4	1*c*	99	*ed*
a0	*d*5	85	*d*7	33	7*d*	*e*3	*aa*	3*f*	23	73	*da*	*bd*	*dc*	*cd*	*f*7	*a*3
b0	*c*0	2*b*	*fa*	14	56	34	94	12	*b*4	4*a*	5*a*	*c*2	8*a*	92	1*d*	3*a*
c0	27	*dd*	8*c*	89	0*f*	80	*ce*	*e*2	*fd*	72	08	61	5*c*	06	38	88
d0	07	*a*7	46	3*c*	4*f*	02	66	45	*c*5	*b*1	04	*c*8	7*f*	19	63	*c*7
e0	6*f*	*ba*	*b*7	29	*d*2	16	8*b*	18	62	24	*af*	4*b*	*fc*	98	*a*9	2*f*
f0	93	32	0*c*	*b*9	21	00	97	01	86	79	26	*f*1	31	0*a*	0*e*	2*c*

The total number of cryptographically strong TQ-S-boxes and a distribution of the total obtained TQ-S-boxes in both the cases discussed above are shown in Table 8. From the table, it can be said that, in both the cases, all the TQ-S-boxes obtained through our algorithm have algebraic degree 7.

One of the C.S. 8×8 TQ-S-boxes obtained from the algorithm is given in Table 9. In the table, if the input is 8*a*, then the most significant nibble

Table 10. MTO of C.S. 8×8 TQ-S-boxes.

Case	Subcase	MTO values	
		Min	Max
I.	1.	6.79755	6.91863
	2.	6.75221	6.92243
	3.	6.76728	6.92402
	4.	6.78689	6.92463

is 8 and the least significant nibble is a. This S-box has been obtained from ternary quasigroup L_{33} (in lexicographical order) and leader pairs $(0,2),(0,2),(2,3),(2,3)$. The S-box has nonlinearity$=98$, differential uniformity$=10$, and degree$=7$.

We have analysed the modified transparency order of the C.S. TQ-S-boxes obtained from all the 4 subcases of the case I. The maximum and minimum values of MTO of all the 8×8 TQ-S-boxes obtained in 4 subcases of case I are shown in Table 10.

The block cipher advanced encryption standard (AES) (National Institute of Standards and Technology 2001) is not resistant to DPA attacks (Yonli 2019; Yu et al. 2008). The lesser the MTO is, the more resistant the S-box is against DPA attacks. It can be checked that the MTO of the S-box used in AES is 6.91605 (Chakraborty et al. 2017). Table 11 shows the number of C.S. TQ-S-boxes obtained through our algorithm having MTO less than the S-box in AES cipher. These S-boxes have better resistance against the DPA attacks.

6. Comparative study and analysis

We have done a comparative study of 4-, 6-, and 8-order S-boxes constructed from our algorithm in case I (discussed in Section 5) with the S-boxes constructed from the previous methods (Mihajloska and Gligoroski 2012; Yu and Xu 2017) (known to us). Our algorithm is a generalised method for the construction of C.S. S-boxes of even order as well as gives S-boxes with better cryptographic properties.

We have compared the cryptographic properties of S-boxes obtained from our method to that obtained from the method proposed in Mihajloska and Gligoroski (2012). In our comparison, we have checked the percentage of S-boxes of order 4, 6, and 8, obtained in case I, satisfying the criteria given in Table 1. Figures 7–9, respectively, show the comparison of the 4×4, 6×6, and 8×8 S-boxes obtained through the 2 methods. In these Figures, we have denoted our method as "new" and the method in Mihajloska and Gligoroski (2012) as "old." To obtain 6- and 8-order S-boxes, we have extended the algorithm for the construction of S-boxes in Mihajloska and Gligoroski (2012). We have found that it performs worst for the 6- and 8-order, as none of the obtained S-boxes is C.S. (this can be

Table 11. C.S. TQ-S-boxes having MTO less than the S-box in AES.

Case	Subcase	C.S. TQ-S-boxes	MTO less than PRESENT	
			n	%
I.	1.	109,632	109,616	99.985
	2.	104,028	104,018	99.990
	3.	106,686	106,678	99.993
	4.	110,100	110,090	99.991

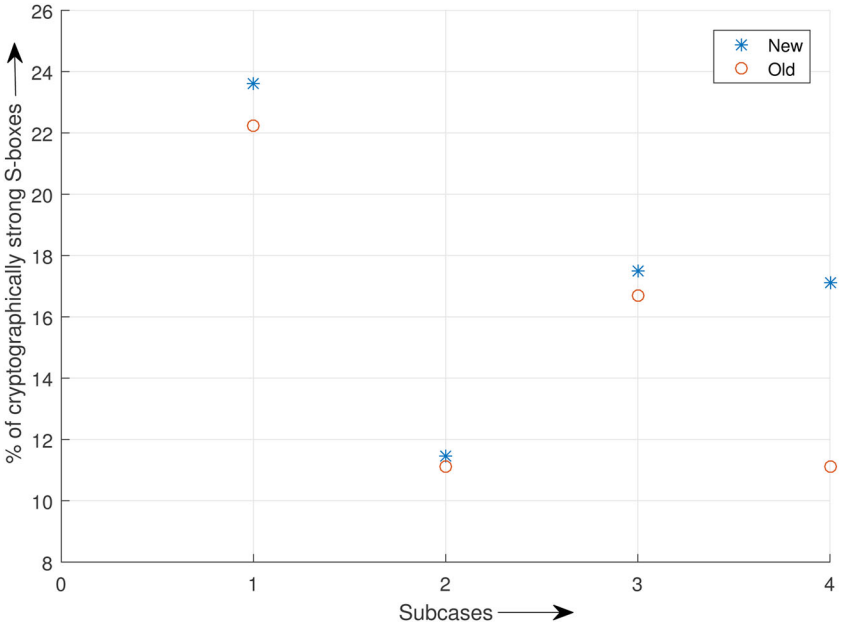

Figure 7. Comparison on the 4×4 C.S. S-boxes.

seen from Figures 8 and 9). Also, the S-boxes obtained through our algorithm have relatively less minimum MTO.

In Yu and Xu (2017), only 1,008 from the total 15,552 S-boxes of order 4 are C.S, which is just 6.48%. This also gives relatively lesser C.S. S-boxes.

7. Conclusions and future work

In this article, first we described some concepts required for the understanding of the article, including some important cryptographic properties of S-boxes. Then we have proposed an algorithm to construct cryptographically strong symmetric S-boxes of even order using ternary quasigroups of order 4. Finally, experimental verification and cryptographic analysis of the obtained 4×4, 6×6, and 8×8 TQ-S-boxes have been discussed. And hence a comparison of these with earlier proposed methods and randomly generated S-boxes is given. The obtained cryptographically strong TQ-S-boxes can be used in the design of lightweight block ciphers and hash functions.

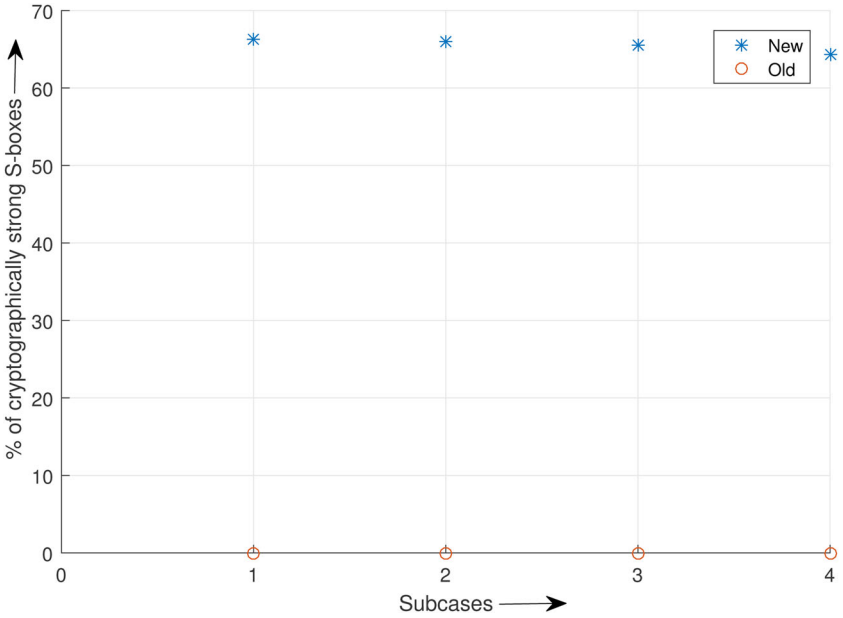

Figure 8. Comparison on the 6×6 S-boxes.

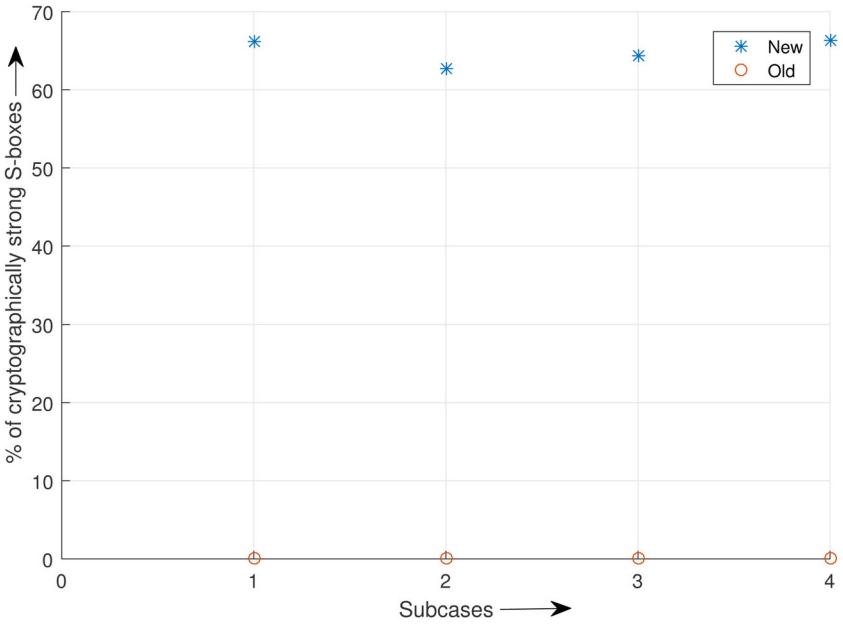

Figure 9. Comparison on the 8×8 S-boxes.

The reader may analyse TQ-S-boxes obtained from our algorithm for a higher number of rounds or/and a different number of leader pairs. Also, TQ-S-boxes of larger orders can be analysed. The reader may study cryptographic properties of the obtained TQ-S-boxes other than those discussed in the article.

This work may naturally be extended to generate more different order S-boxes like that of 6×4-bit cryptographically strong S-boxes.

About the Authors

Dimpy Chauhan is a research scholar at the Department of Mathematics, University of Delhi, India. She has received her Masters in Mathematics from Panjab University, India. Her research interests are in algebra and its applications, especially cryptography and coding theory.

Indivar Gupta is a senior scientist in Scientific Analysis Group, DRDO, Delhi, India. He completed his Ph.D. from the IIT Delhi, India. His areas of research include computational algebra, number theory, cryptography, information security, and high-performance computing.

P. R. Mishra is a senior scientist in Scientific Analysis Group, DRDO, Delhi, India. He obtained his Ph.D. in number theory from Banaras Hindu University, Varanasi, India. His main research interests are cryptography and number theory.

Rashmi Verma is an assistant professor at the Department of Mathematics, Mata Sundri College for Women, University of Delhi, India. She completed her M.Phil. and Ph.D. from the Department of Mathematics, University of Delhi, India. Her research interests is algebraic coding theory.

Acknowledgments

The authors would like to thank the anonymous referees for their extensive comments on the revision of the manuscript, which really improved the quality of the article.

Funding

The research of the first author is supported by University Grants Commission (UGC), Government of India, with reference no.: 20/12/2015(ii)EU-V.

References

Belousov, V. D. 1972. n-Ary quasigroups (Russian). *Izdat.* "Stiinca," Kishinev, 227.

Biham, E., and A. Shamir. 1991. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology* 4 (1):3–72. doi: 10.1007/BF00630563.

Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C. 2007. PRESENT: An ultra-lightweight block cipher. In *Proceedings of CHES 2007. Lecture notes in computer science*, ed. P. Paillier, I. Verbauwhede vol. 4727. pp. 450-66. Berlin: Springer. doi: 10.1007/978-3-540-74735-2-31.

Browning, K. A., J. F. Dillon, M.T. McQuistan, A.J. Wolfe. 2010. An APN permutation in dimension six. In *Finite fields: Theory and applications*, ed. G. McGuire, G. L. Mullen, D. Panario, and I. E. Shparlinski, *Contemporary mathematics*, vol. 518, 33–42. Providence, RI: American Mathematical Society.

Carlet, C. 2010. Boolean functions for cryptography and error correcting codes. In *Chapter of the monography Boolean models and methods in mathematics, computer science, and engineering*, ed. Y. Crama and P. Hammer, 257–397. Cambridge: Cambridge University Press.

Chabaud, F., and S. Vaudenay. 1995. Links between differential and linear cryptanalysis. In *Advances in cryptology—EUROCRYPT '94 (Perugia). Lecture notes in computer science*, vol. 950, 356–65. Berlin: Springer.

Chakraborty, K., S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay, and E. Prouff. 2017. Redefining the transparency order. *Designs, Codes and Cryptography* 82 (1–2): 95–115. doi: 10.1007/s10623-016-0250-3.

Duan, X., Q. Cui, S. Wang, H. Fang, and G. She. 2016. Differential power analysis attack and efficient countermeasures on PRESENT. 8th IEEE International Conference on Communication Software and Networks (ICCSN), Beijing, 8–12.

Leander, G., and A. Poschmann. (2007) On the classification of 4 bit S-boxes. In *Arithmetic of finite fields. Lecture notes in computer science*, Carlet C., Sunar B. (eds) vol. 4547, 159–76. Berlin: Springer.

Lyu, S., and Y. Xu. 2015. String transformation based on 3-quasigroups. *Journal of Computational Information Systems* 11 (19):6989–7000.

Matsui, M. 1993. Linear cryptanalysis method for DES cipher. In *EUROCRYPT '93*. Vol. 765 of *LNCS*, ed. T. Helleseth, 386–97. Berlin, Heidelberg: Springer.

Mihajloska, H., and D. Gligoroski. 2012. Construction of optimal 4-bit S-boxes by quasigroups of order 4. Proceedings of SECURWARE 2012: The Sixth International Conference on Emerging Security Information, Systems and Technologies, Rome, Italy, 163–8. IARIA.

Mullen, G. L., and R. E. Weber. 1980. Latin cubes of order $\leqslant 5$. *Discrete Mathematics* 32 (3):291–7.

National Institute of Standards and Technology. 2001. Advanced Encryption Standard (AES) (FIPS PUB 197). National Institute of Standards and Technology. Federal Information Processing Standards Publication 197 (FIPS 197), November 2001.

Nyberg, K. 1991. Perfect non-linear S-boxes. In *Advances in cryptology—EUROCRYPT 91 (Brighton 1991). Lecture notes in computer science*, Davies D.W. ed. vol. 547, 378–86. Berlin: Springer.

Prouff, E. 2005. DPA attacks and S-boxes. In *Fast software encryption – FSE 2005*. Vol. 3557 of *Lecture notes in computer science*, ed. H. Handschuh and H. Gilbert, 424–42. New York: Springer.

Wu, C.-K., and D. Feng. 2016. *Boolean functions and their applications in cryptography. Advances in computer science and technology*. Heidelberg: Springer.

Yonli, M. 2019. A comparison of single-bit and multi-bit DPA for attacking AES128 on an ATmega328P. *IACR Cryptology ePrint Archive* 2019:899.

Yu, H., Z. Xue-Cheng, L. Zheng-Lin, and C. Yi-Cheng. 2008. The research of DPA attacks against AES implementations. *The Journal of China Universities of Posts and Telecommunications* 15 (4):101–6. doi: 10.1016/S1005-8885(08)60412-4.

Yu, Z., and Y. Xu. 2017. Optimal S-boxes based on 3-quasigroups of order 4. 6th International Conference on Advanced Materials and Computer Science (ICAMCS 2017), 114–21. Clausius Scientific Press (CSP).

Zhang, J., D. Gu, Z. Guo, and L. Zhang. 2010. Differential power cryptanalysis attacks against PRESENT implementation. IEEE 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, V6-61–V6-65.