On quaternary resilient functions

Conference Paper *in* AIP Conference Proceedings · January 2023

DOI: 10.1063/5.0156723

CITATIONS
0

READS
12

2 authors:

Aboobacker Parammel
govt.Engineering CollegeSreekrishnauram
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

M. Viji
St. Thomas College, Thrissur
10 PUBLICATIONS **5** CITATIONS
SEE PROFILE

RESEARCH ARTICLE | JULY 13 2023

On quaternary resilient functions

Aboobacker Parammel ✉; Viji Maniyil

AIP Conf. Proc. 2829, 050004 (2023)
https://doi.org/10.1063/5.0156723

On Quaternary Resilient Functions

Aboobacker Parammel[1, a)] and Viji Maniyil[2, b)]

[1)]*Govt. Engineering College, Palakkad - 678633, Kerala, India*
[2)]*St. Thomas' College (Autonomous), Thrissur - 680001, Kerala, India*

[a)]*Corresponding author: backer83@gmail.com*
[b)]*vijigeethanjaly@gmail.com*

Abstract. Functions on multiple valued logic are important tools for designing non-binary cryptographic algorithms. Cryptographic characteristics such as correlation immunity and resiliency of Boolean functions are well studied. This paper is on the resiliency of quaternary functions. We provide a method to extract a class quaternary 1-resilient functions in two variables using the group action of the permutation group S_4. Using the resilient functions obtained, based on computational results using python programming language, we conjecture a technique to produce 1-resilient quaternary functions in three variables. We Also discuss orthogonal matrix characterizations of resilient functions on multiple valued logic.

Keywords: Many valued logic; Correlation immunity; Resiliency

INTRODUCTION

Boolean functions play a vital role in designing Block ciphers and stream ciphers [1]. They are the building blocks of the nonlinear component, the substitution box (S box) of a block cipher which makes use of substitution transformations. In block ciphers, the strength of the S box determines the security of the algorithm [2]. If these components are not properly chosen, it renders the cipher weak resistance to various attacks. There are many criteria to measure the quality of Boolean functions, among which non-linearity and resistance against correlation attack are predominant.

Current research are focusing on developing systems and models based on multiple valued logic. Functions on multiple valued logic represent the digital data in a compact form. One of the main benefits of many-valued logic is the ability to optimize or minimize data processing, so it is important to take full advantage of the potential of many-valued logic. There are electronic devices in which models with more than two states (fuzzy logic) are effectively implemented. Multiple valued logic is an alternating solution for many practical problems. It has applications in cryptography, coding theory, signal processing, VLSI IC's, etc. The application of functions on multiple valued logic simplifies the design of position-based cryptographic schemes [3]. In signal processing, multiple-valued logic is convenient in the storage and processing of a huge amount of data encoded in a digital signal, and additionally, numerous strategies implemented in signal processing are geared up sufficient to remedy particular issues confronted in the design of systems based on multiple valued logic [4]. If the signals in an integrated circuit permit to accept four states(quaternary values) instead of only two states(binary values), the problem encountered in some VLSI circuits due to the constraints in the number of connections that can be used within the circuit and that connect the outer world can be solved effectively [5]. Some VLSI ICs are available intended for commercial purpose that has design principle based on quaternary logic.

Various applications of the primitives based on multiple valued logic confirm the need for further research in this direction. A great number of researches are devoted to developing cryptographic characteristics of non-binary functions and cryptographic schemes based on them. The cryptographic algorithm based on three-valued(ternary) logic was proposed by Artem Sokolov et al [6]. The properties such as non-linearity and avalanche criterion of q-valued functions were discussed in [7,8]. As the measure of the input-output correlation of the component q-valued functions, the input-output correlation coefficient ρ_{xy}, x, y=0, 1...$q-1$ and the correlation matrix P_{xy} consisting of the absolute values of the correlation coefficient was introduced in [9].

$$\rho_{xy} = \frac{\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{\sqrt{\frac{1}{n}\sum_{i=1}^{n} {x_i}^2 - \left(\frac{\sum_{i=1}^{n} x_i}{n}\right)^2}\sqrt{\frac{1}{n}\sum_{i=1}^{n} {y_i}^2 - \left(\frac{\sum_{i=1}^{n} y_i}{n}\right)^2}} \tag{1}$$

The correlation attack was coined by Siegethaler in [10] and the original attack was given in [11]. The functions which have resistance against correlation attacks are known as correlation immune functions. The Correlation immunity of order m(m-CI) was studied in [10]. The cryptographic characteristics such as correlation immunity and

International Conference on Recent Advances in Mathematics and Computational Engineering
AIP Conf. Proc. 2829, 050004-1–050004-8; https://doi.org/10.1063/5.0156723
Published by AIP Publishing. 978-0-7354-4574-1/$30.00

resiliency of functions on binary logic were extensively studied in [10, 11]. The extension of the concept to non-binary functions was introduced in [12]. A detailed study of correlation immunity of 3-valued functions and a method to synthesize the complete class of correlation immune ternary functions in two variables was carried out in [13].

This paper elaborates upon the correlation immunity and hence the resiliency of functions on multiple valued logic. Two approaches to defining resiliency are presented. We propose a method to generate a class of resilient quaternary functions of two variables using group action of the permutation group S_4.

PRELIMINARIES

Let $F_q = \{0,1,2,....q-1\}$ be a ring with operations addition modulo q and multiplication modulo q and $V_n = F_q^n$ be the n copies of F_q^n.If q is a prime number then F_q and F_q^n can be considered as a field with q elements and a vector space of dimension n over F_q respectively. An n-variable q-valued function is an arbitrary function from V_n to V_1.One of the method of representing such function is by means of truth table as a string of numbers of F_q of length q^n, f= $\{f(0,0...,0), f(0,0...,1), ..., f(q-1,q-1,...,q-1)\}$. The sign function of q-valued function is, $F = (\omega^{f(0,0,...0)}, ..., \omega^{f(q-1,q-1,...q-1)})$, where ω is the primitive q^{th} root of unity given by $\omega = e^{\frac{2\pi i}{q}}$. The hamming weight or simply weight of an array is the number of non zero values in it. Weight of a vector $u \in V_n$ we denoted by wt(u). Let $x = (x_1, x_2, ..., x_n)$ and $u = (u_1, u_2, ..., u_n)$ be elements of V_n, then its inner product, given by $\langle x,u\rangle = x_1u_1 + x_2u_2 + ... + x_nu_n$ belongs to F_q. In this article,concatenation of x and u is denoted by $x||v$ and it is the array of length equal to the sum of lengths of u and v and is obtained by associating v with u.That is,$x||u$= $(x_1, x_2, ..., x_n, u_1, u_2, ..., u_n)$.

Definition .1 *A q-valued function in n variable is balanced if the 0's, 1's... and $q-1$'s in its truth table are uniformly distributed.*

When $q = 2$,the function is called as Boolean functions.The hamming weight of an array of binary numbers is the number of 1's in it. A Boolean function is balanced when the number of 0's and 1's are equal. Walsh transform has a vital role in the analysis of Boolean function. For any vector $u \in V_n$, the Walsh transform of a Boolean function $f(x)$ is ,

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x)+\langle x,u\rangle} \tag{2}$$

Balancedness of a Boolean function $f(x)$ can also evaluate with help of Walsh transform coefficients.The imbalance is computed as the Walsh transform at $u = 0$. So a Boolean function f in n variable is balanced if $W_f(0) = 2^{n-1}$.

Nonlinearity(NL) is an important characteristic of a cryptographic function that measures the distance of the function from the most approximated linear function. The nonlinearity of Boolean function can be computed using Walsh transform and that of q-valued function can be computed with help of Vilenkin- Chrestenson transform [14],

$$\Phi_f(u) = \sum_{x \in V_n} \omega^{f(x)+\overline{\langle x,u\rangle}} \tag{3}$$

Where $\bar{y}$ we meant by conjugate of the complex number y.

The Vilenkin-Chrestenson transform coefficients(Spectrum) of a q-valued function f can be calculated by using Vilenkin-Chrestenson matrix M_{q^n}, a matrix of order q^n. The coefficients are obtained as a result of multiplication of the function f with the complex conjugate of M_{q^n}.That is,

$$\Phi_f = f.\overline{M_{q^n}} \tag{4}$$

For quaternary functions ($q = 4$)the matrix of order 4^n is obtained by the recurrence relation given in [15],

$$M_{4^{k+1}} = \begin{bmatrix} M_{4^k} & M_{4^k} & M_{4^k} & M_{4^k} \\ M_{4^k} & M_{4^k}+\mathbf{1} & M_{4^k}+\mathbf{2} & M_{4^k}+\mathbf{3} \\ M_{4^k} & M_{4^k}+\mathbf{2} & M_{4^k} & M_{4^k}+\mathbf{2} \\ M_{4^k} & M_{4^k}+\mathbf{3} & M_{4^k}+\mathbf{2} & M_{4^k}+\mathbf{1} \end{bmatrix}, \text{ where } M_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 3 & 2 & 1 \end{bmatrix}$$

For this computation we need to convert the matrix and the function to complex exponential form using the unique transformation,

$$\{0,1,2,3\} \rightarrow \left\{e^{\frac{2\pi i}{4}0}, e^{\frac{2\pi i}{4}1}, e^{\frac{2\pi i}{4}2}, e^{\frac{2\pi i}{4}3}\right\}$$

The digits **p** in the matrix represent square matrix of order 4^k with all entries p and the matrix addition is performed modulo 4.

The nonlinearity is defined as [7] ,

$$N_f = \begin{cases} q^{n-1} - \frac{1}{2} Max_{u \in V_n} |W_f(u)| & if \quad q = 2 \\ q^n - Max_{u \in V_n} |\Phi_f(u)| & if \quad q \geq 3 \end{cases} \tag{5}$$

Definition .2 *(Group action) Let G a group and X be a set.Group action is a mapping from $G \times X$ to X that assign each pair of elements $g \in X$ and $x \in X$ an element in X by a rule denoted by g.x satisfying following axioms,*

i) For every $g \in X$ and $x \in X$, $g.x \in X$.

ii) If $1 \in G$ is the identity,then for every $x \in X$, $1.x = x$.

iii) For every $g,h \in G$ and $x \in X$, $(g.h).x = g.(h.x)$.

Correlation Immunity of Boolean functions

Definition .3 [16] *Let $f(x)$ be a Boolean function and $x_1, x_2, \ldots x_n$ are independent and uniformly distributed random variables, the function $f(x_1, x_2, \ldots x_n)$ is of m^{th} order, $(0 \leq m \leq n)$ correlation immunity if $f(x_1, x_2, \ldots x_n)$ is independent of any set of m of its input variables, $x_1, x_2, \ldots$,and x_n .*

In other words f is of m^{th} order correlation immunity if its probability distribution is unaffected by any set of m input variables.That is, $Pr\left(f(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_m)/x_{i_k} = s_k, 1 \leq k \leq m\right) = Pr\left(f(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_m)\right)$. To define correlation immunity in terms of their sub functions [16],let us recap the definition of the sub-function ,

Definition .4 [16] *A sub-function of a Boolean function f is the function f^I derived from f by inserting constant values 0 or 1 for some of its variables.*

Definition .5 [16] *A Boolean function on V_n is of m^{th} order, $(0 \leq m \leq n)$ correlation immune if any of its sub-function of $n-m$ variable is of weight equal to $wt(f)/2^m$. That is, $wt(f^I) = wt(f)/2^m$.*

The correlation immunity of a Boolean function and its Walsh transform is related as,

Theorem .1 [17] *A Boolean function has correlation immunity of order m if and only if its Walsh transform is zero for all inputs with weight less than or equal to m. ie $W_f(u) = 0$, for $0 \leq wt(u) \leq m$.*

Correlation Immunity of q-valued functions

To define the correlation immunity of a q-valued function, it is required to generalize the concept of sub-function. The sub-function of a q-valued function is,

Definition .6 [13] *A sub-function of a q-valued function $f(x)$ is a function $f^I(x)$ derived from $f(x)$ by inserting constant values from the set $F_q = \{0, 1, \ldots . q-1\}$ for some of its variables.*

The correlation immunity of the ternary function was defined in terms of the imbalance of the function [18] which can be generalized for functions of multiple valued logic as

Definition .7 *The imbalance of the q-valued function is the absolute value of the first coefficient of the Vilenkin-Chrestenson transform. That is , the absolute value of the sum of component-wise product of the function by the sequence* $[e^{i0}, e^{i0}, \ldots\ldots\ldots, e^{i0}]$.

The imbalance can also compute from its truth table representation using the expression given as,

$$\Delta_f = \left| \sum_{k=0}^{q-1} n_k e^{\frac{2\pi i}{q} k} \right| \tag{6}$$

where n_k, k=0, 1, 2,...,$q-1$ are the number of k's in the truth table of the function $f(x)$.

Definition .8 *Let $f(x)$ be a q-valued function in n variables, $f(x)$ has correlation immunity of order m, $0 \leq m \leq n$ if the imbalance of any of its sub-functions f^I obtained by substituting m of its variable with constants from the set F_q is, $\Delta_{f^I} = \Delta_f / q^m$.*

Definition.3 can also be extended for q-valued functions, in such case the random variables take value from the set V_1.

RESILIENT QUATERNARY FUNCTIONS

Quaternary function assume the values in F_4. The elements 0,1,2 and 3 of F_4 can be interpreted as the 4^{th} roots of unity 1, i,-1, and -i respectively.In order to analyse the resiliency we make use imbalance of the functions. The imbalance of the quaternary function $f(x)$ can be computed using eq(6) and it is given by,

$$\Delta_f = |n_0.1 + n_1.i + n_2.-1 + n_3.-i|$$

$$= \sqrt{(n_0 - n_2)^2 + (n_1 - n_3)^2} \tag{7}$$

.
Where n_0, n_1, n_2 and n_3 are respectively the number of 0's, 1's, 2,s and 3's in the truth table of $f(x)$.

Definition .9 *Let $f(x)$ is a 4- valued function on n variable, $f(x)$ is said to have m^{th} order correlation immunity, $0 \leq m \leq n$ if the imbalance of each of its sub-functions f^I of $n-m$ variables is $\Delta_{f^I} = \Delta_f / 4^m$.*

A quaternary function is resilient if it is balanced and correlation immune. That is if it is correlation immune with zero imbalance. The sub-functions satisfy the condition for resiliency only if they are also having zero imbalance. For example, Consider the quaternary function in two variables,

x_1x_2	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
$f(x_1,x_2)$	0	1	2	3	1	2	3	0	2	3	0	1	3	0	1	2

Simply,this function can be represented as f={0123123023013012}.The imbalance of the function is equal to zero. Now let us examine the nature of the sub-functions of f,

$f(0,x_2) = \{f(0,0)f(0,1)f(0,2)f(0,3)\} = \{0123\}$ is one of them. The other sub-functions are, $f(1,x_2) = \{1230\}$, $f(2,x_2) = \{2301\}$, $f(3,x_2) = \{3012\}$, $f(x_1,0) = \{0123\}$, $f(x_1,1) = \{1230\}$, $f(x_1,2) = \{2301\}$, $f(x_1,3) = \{3012\}$.

Clearly, each of the sub-functions of one variable is having zero imbalance and $\Delta_{f^I} = 0 = \frac{\Delta_f}{4^m}$.Thus the function $f(x_1,x_2)$ is a 1-resilient function.

METHOD TO SYNTHESIZE RESILIENT QUATERNARY FUNCTIONS IN TWO VARIABLES

In this section, we present an indigenous method for the construction of 2-variable resilient quaternary functions employing permutation group action on a set consisting of four elements each of which is a string of length 4 whose arguments assume value from the set F_4.For each function obtained the nonlinearity is analyzed.

Consider the set $S = \{\mu_0, \mu_1, \mu_2, \mu_3\}$, where $\mu_0 = (0123), \mu_1 = \mu_0 + I, \mu_2 = \mu_0 + 2I, \mu_3 = \mu_0 + 3I$,where I is a string of length 4 with all its components equal to 1.The addition is performed component wise modulo 4. Now, let us recall the symmetric group $S_4 = \{\gamma_i, i = 1,2.\ldots...4! : \gamma_i$, is a permutation on 4 symbols$\}$. From the group action of the symmetric group S_4 on the set S creates 4! resilient quaternary functions in two variables of length 16 . The algebraic expression of the group action is,

$$\psi : S_4 \times S \to S$$

$$\psi(\gamma_i, \mu_j) = \gamma_i(\mu_j), \qquad i = 1,2,...,24, \quad j = 0,1,2,3. \tag{8}$$

The concatenation $\gamma_i(\mu_0)||\gamma_i(\mu_1)\gamma_i(\mu_2)||\gamma_i(\mu_3)$, i = 1,2,...,24 produces the truth table of the resilient quaternary functions and these functions are,

$f_1 = \{0123123023013012\}$ $f_2 = \{0123123030122301\}$ $f_3 = \{0123301212302301\}$
$f_4 = \{0123230112303012\}$ $f_5 = \{0123301223011230\}$ $f_6 = \{0123230130121230\}$
$f_7 = \{1230012323013012\}$ $f_8 = \{1230230130120123\}$ $f_9 = \{1230301201232301\}$
$f_{10} = \{1230230101233012\}$ $f_{11} = \{1230301223010123\}$ $f_{12} = \{1230012330122301\}$
$f_{13} = \{2301012312303012\}$ $f_{14} = \{2301012312303012\}$ $f_{15} = \{2301123001233012\}$
$f_{16} = \{2301123030120123\}$ $f_{17} = \{2301301201231230\}$ $f_{18} = \{2301301212300123\}$
$f_{19} = \{3012012312302301\}$ $f_{20} = \{3012012323011230\}$ $f_{21} = \{3012123001232301\}$
$f_{22} = \{3012123023010123\}$ $f_{23} = \{3012230101231230\}$ $f_{24} = \{3012230112300123\}$

Using the above 24 resilient functions as the generating function we can derive the class of resilient quaternary function of length $N = 4^2$. Each of the resilient functions produces another 24 resilient quaternary functions by the application of the transformation g from the set of quaternary sequences of length 16 to itself, given by,

$$g(x_1x_2....x_{16}) = (y_1y_2....y_{16}), \qquad where \;\; y_i = \begin{cases} k & if \;\; x_i = l \\ l & if \;\; x_i = k \\ x_i & otherwise \end{cases} \tag{9}$$

By replacing particular values for k and l we get the 24 quaternary resilient functions from each resilient function produced in the last step.The pair of values (k,l) that produce the required functions are (0,1), (0,2), (0,3),(1,2) and (2,3).We verified the resiliency of these functions using a python programming language. Thus, from the method above we could form 144 resilient quaternary functions of length 16 in two variables.

The nonlinearity of the resilient functions obtained are computed using eq(5) with help of python programming language and it is found that 56 of them have nonlinearity NL=8, 72 of them have the value NL= 4.683 and 16 of them have NL=0. The resilient functions with NL=8 are of special importance and they can be used as primitives for various cryptographic applications to attain optimal results.

Based on the computational result on obtained 2-variable 1-resilient functions, we conjecture that,

Conjecture .1 *Let $f_1, f_2, f_3, f_4 : F_{4^2} \to F_4$ are resilient 4-valued functions in two variables, for $x \in F_{4^2}$ the three variable 4-valued function $f : F_{4^3} \to F_4$ defined as,*

$$f(x,x_3) = \begin{cases} f_1(x) & if \;\; x_3 = 0 \\ f_2(x) & if \;\; x_3 = 1 \\ f_3(x) & if \;\; x_3 = 2 \\ f_4(x) & if \;\; x_3 = 3 \end{cases} \tag{10}$$

is a 1-resilient function.

We conformed the resiliency of the functions constructed using python programming language. Some of the functions constructed in this manner might be 2-resilient also. Further research is needed for extracting such functions.

If $f(x)$ is q-valued resilient function,it is balanced.Since a circular shift or scaling by an element co-prime to q does not affect the balancedness the function $f(x)$ and its sub-functions.This fact substantiate the following proposition.

Proposition .1 *Let $f : V_n \to V_1$ be a resilient functions .Then $\{af + bI, a < q, gcd(a,q) = 1, b \in F_q$, where I is a string of length q^n with all its entries 1, are resilient functions.*

The operations specified in proposition .1 are spectral invariant [19].

METHOD FOR ANALYSIS OF RESILIENT FUNCTIONS BASED ON ORTHOGONAL MATRIX

This section is devoted to an analysis of the relation between orthogonal matrix [20] and correlation immunity of q-valued functions.

Definition .10 [20] *An $L \times n$ matrix A over F_q is said to be an (L,n,q,m) orthogonal matrix if for any fixed m columns, each row vector $y \in F_{q^m}$ appears exactly L/q^m times in the matrix consists of these m columns.*

Let $f : V_n \to V_1$ be an n-variable q-valued function. For each $j, 0 \le j \le q-1$ consider the matrix B_j whose rows are the members of the set defined by $W_j = \{x \in F_{q^n} : f(x) = j\}$.Clearly $|W_j| = n_j$, the number of j's in the truth table of $f(x)$. Then B_j is a matrix of order $n_j \times n$. We have, $f(x)$ is m-correlation immune if the number of j's, $0 \le j \le q-1$ in each of the sub-functions obtained by substituting m of its input variable with constants of the set V_1 is equal to $\frac{n_j}{q^m}$.Since in that case,

$$\Delta_{f^I} = \left| \sum_{k=0}^{q-1} \frac{n_k}{q^m} e^{\frac{2\pi i}{q}k} \right| = \frac{1}{q^m} \Delta_f \tag{11}$$

The sub-function is obtained as a result of fixing m input variables and B_j consists of n_j rows, it is true that if we fix m columns of B_j each vector of V_m appears exactly $\frac{n_j}{q^m}$ times.Also, for a balanced function $n_j = q^{n-1}$. From these arguments we can conclude that[see also [20]],

Theorem .2 *An n-variable q-valued function has resiliency of order m if B_j is a (q^{n-1}, n, q, m) orthogonal matrix, $0 \le j \le q-1$.*

Thus, for a resilient resilient function, the matrices $B_j, 0 \le j \le q-1$ contains equal number of rows and if we fix m columns every vectors of V_m appears q^{n-m-1} times.

To illustrate the resiliency of a four-valued function with help of orthogonal matrices, consider a 4-valued function in three variables,

$x_1x_2x_3$	000	001	002	003	010	011	012	013	020	021	022	023	030	031	032	033
$f(x_1,x_2,x_3)$	0	1	2	3	1	2	3	0	2	3	0	1	3	0	1	2

$x_1x_2x_3$	100	101	102	103	110	111	112	113	120	121	122	123	130	131	132	133
$f(x_1,x_2,x_3)$	1	2	3	0	2	3	0	1	3	0	1	2	0	1	2	3

$x_1x_2x_3$	200	201	202	203	210	211	212	213	220	221	222	223	230	231	232	233
$f(x_1,x_2,x_3)$	2	3	0	1	3	0	1	2	0	1	2	3	1	2	3	0

$x_1x_2x_3$	300	301	302	303	310	311	312	313	320	321	322	323	330	331	332	333
$f(x_1,x_2,x_3)$	3	0	1	2	0	1	2	3	1	2	3	0	2	3	0	1

The matrices B_0, B_1, B_2 and B_3 as by the above discussion are,

$$B_0=\begin{bmatrix}0&0&0\\0&1&3\\0&2&2\\0&3&1\\1&0&3\\1&1&2\\1&2&1\\1&3&0\\2&0&2\\2&1&1\\2&2&0\\2&3&3\\3&0&1\\3&1&0\\3&2&3\\3&3&2\end{bmatrix}, B_1=\begin{bmatrix}0&0&1\\0&1&0\\0&2&3\\0&3&2\\1&0&0\\1&1&3\\1&2&2\\1&3&1\\2&0&3\\2&1&2\\2&2&1\\2&3&0\\3&0&2\\3&1&1\\3&2&0\\3&3&3\end{bmatrix}, B_2=\begin{bmatrix}0&0&2\\0&1&1\\0&2&0\\0&3&3\\1&0&1\\1&1&0\\1&2&3\\1&3&2\\2&0&0\\2&1&3\\2&2&2\\2&3&1\\3&0&3\\3&1&2\\3&2&1\\3&3&0\end{bmatrix}, B_3=\begin{bmatrix}0&0&3\\0&1&2\\0&2&1\\0&3&0\\1&0&2\\1&1&1\\1&2&0\\1&3&3\\2&0&1\\2&1&0\\2&2&3\\2&3&2\\3&0&0\\3&1&3\\3&2&2\\3&3&1\end{bmatrix}$$

From the matrices it is clear that $b_0 = b_1 = b_2 = b_3 = 16$ and if we fix any two rows of each of the matrices, every vector $\alpha \in F_{4^2}$ appears exactly $b_j/4^2$ $(= 4^{3-2-1})$ times, $0 \leq j \leq 3$. Thus, the given function is a 2-resilient quaternary function in three variables.

CONCLUSION AND FUTURE WORKS

In this monograph, a class of 1-resilient quaternary functions of two variables is synthesized. We found that there are 144 such functions using the sub-function approach. The orthogonal matrix approach to learn the beauty of the resiliency of the quaternary function is discussed. This will help the cryptographic community for further research on the 2-resiliency of four-valued function in three variables and to find the complete class of such functions. We mentioned a method to find the 1-resilient functions of 3-variable from two-variable resilient functions that can be extended to functions on F_q. Further research is meant to extend the concept of the resiliency of higher order for functions with more variables that will help in designing secure cryptographic algorithms on multiple valued logic.

REFERENCES

1. C.Carlet, Y.Crama and P.Hammer "Boolean functions for cryptography and error-correcting codes", Boolean Methods And Models in Mathematics, Computer Science and Engineering, 257-397 (2010).
2. J. Liu, X. Tong, M. Zhang and Z. Wang, "The Design of S-box Based on Combined Chaotic Map," 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), Shenzhen, China, 350-353 (2020)
3. A.Yu. Bykovsky, "Multiple-valued logic and network in the position based cryptography scheme", Journal of Russian Laser Research, **42(2)**, 618-630 (2021).

4. J. Astola and R. S. Stankovic, "Signal Processing Algorithms and Multiple-Valued Logic Design Methods", 36th International Symposium on Multiple-Valued Logic (ISMVL'06), 16-24 (2006).
5. E.Dubrova, "Multiple-Valued Logic in VLSI: Challenges and Opportunities", Proceedings of NORCHIP'99,(1999).
6. O.N Zhdanov and A.V Sokolov . "Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic", Far East Journal of Electronics and Communications, **16(3)**, 573-58 (2015)
7. A.V Sokolov and O.N Zhdanov, "Avalanche characteristics of cryptographic functions of ternary logic", Radio Electronics, Computer Science, Control **No.4** ,177-185 (2019).
8. A.V. Sokolov, "Constructive method for the synthesis of nonlinear S boxes satisfying the strict avalanche criterion", Radio electronics and Communication Systems, **56(8)**, 415-423 (2013).
9. O.N Zhdanov and A.V Sokolov "Algorithm of construction of optimal according to the criterion of zero correlation nonbinary S-boxes", Problems of Physics, Mathematics, and technics, **3 (24)**, 94-97 (2015).
10. T.Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications", IEEE Transactions Information on Theory,IT, **30(5)**,776–780(1984)
11. T.Siegenthaler,"Decrypting a class of stream ciphers using ciphertext only", IEEE Transactions on Computers,**C-31(1)**, (1985).
12. K.Gopalakrishnan and D.R Stinson , "Three characterizations of non-binary correlation-immune and resilient functions", Designs, Codes and Cryptography, **5**, 241-251 (1995).
13. A. V. Sokolov and O. N. Zhdanov, "Correlation immunity of three-valued logic functions", Journal of Discrete Mathematical Sciences and Cryptography,1-17 (2020).
14. A.M Trakhtman and V.A Trakhtman "Elements of theory of discrete signals on finite intervals", Moscow: Sov. Radio,(1975).
15. Kazakova N and A.V Sokolov, "Spectral and Nonlinear Properties of the Complete Quaternary Code", Conference: Cybersecurity Providing in Information and Telecommunication Systems, (2020)
16. A.A Salnikov and O.A Logachev, "Boolean Functions in Coding Theory & Cryptography", Universities Press (India) Private Limited, ,334 (2017).
17. P.Camion, C.Carlet, P. Charpin, N. Sendrier, "On Correlation-Immune Functions", CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, 86–100 (1991).
18. A.V Sokolov and O.N Zhdanov, "The class of perfect ternary arrays", System analysis and applied information science, **2**, 47-54 (2018).
19. M.M Stancovic,C. Morga Cand R.S Stankovic, "Some spectral invariant operations for multiple-valued functions with homogeneous disjoint products in the polynomial form", Proceedings of 47 the Int. symp.Multiple-valued logic, Federiction NB,Canada.IEEE Press, 61-66 (2017).
20. D Feng,"Over rings Z_N ", Theoretical Computer Science,**226**, 37-43 (1999).