International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 5, October 2020, pp. 5470~5478
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i5.pp5470-5478

New primitives of controlled elements $F_{2/4}$ for block ciphers

Minh Nguyen Hieu[1], Duy Ho Ngoc[2], Canh Hoang Ngoc[3], Trung Dinh Phuong[4], Manh Tran Cong[5]
[1]Institute of Cryptographic Science and Technology, Vietnam
[2]Cyber Command 86, Vietnam Ministry of Defence, Vietnam
[3]Thuongmai University, Vietnam
[4]Vietnam Government Information Security Committee, Vietnam
[5]Le Quy Don Technical University, Vietnam

Article Info

Article history:

Received Jul 30, 2019
Revised Apr 25, 2020
Accepted May 8, 2020

Keywords:

Cryptography
CSPN
Differential analysis
Fast block cipher
FPGA device

ABSTRACT

This paper develops the cipher design approach based on the use of data-dependent operations (DDOs). A new class of DDO based on the advanced controlled elements (CEs) is introduced, which is proven well suited to hardware implementations for FPGA devices. To increase the hardware implementation efficiency of block ciphers, while using contemporary FPGA devices there is proposed an approach to synthesis of fast block ciphers, which uses the substitution-permutation network constructed on the basis of the controlled elements $F_{2/4}$ implementing the 2□2 substitutions under control of the four-bit vector. There are proposed criteria for selecting elements $F_{2/4}$ and results on investigating their main cryptographic properties. It is designed a new fast 128-bit block cipher MM-128 that uses the elements $F_{2/4}$ as elementary building block. The cipher possesses higher performance and requires less hardware resources for its implementation on the bases of FPGA devices than the known block ciphers. There are presented result on differential analysis of the cipher MM-128.

Corresponding Author:

Canh Hoang Ngoc,
Thuongmai University,
79 Ho Tung Mau, Hanoi, Vietnam.
Email: canhhn@tmu.edu.vn

1. INTRODUCTION

To protect the information in high-speed information and telecommunication systems there is widely used hardware-based encryption, and most widely are used the block ciphers. There are two main variants for hardware implementation: 1) Programmable logic device (PLD); 2) Custom very large integrated circuits (VLSI). First variant is more flexible and faster, as well as economically more advantageous in case of production of comparatively small number of encryption devices. Currently on a mass scale there are available FPGA devices of new generation, which allow essentially improve the performance of information transformation. Earlier in works [1-13] there was developed an approach to the synthesis of fast cipher oriented to efficient hardware implementation, which is based on applying the data-driven operations that are performed with the controlled substitution-permutation networks (CSPNs). The CSPN-based operating blocks are implemented in the form of a multilayer structure, the active layers of which represent cascades of the controlled elements (CEs) with a two-bit input for data. Between two sequential active layers there is located a fixed bit permutation implemented as interlacing wires.

In the known publications there are formulated criteria for selecting the elements $F_{2/1}$ with one-bit control input and the CEs $F_{2/2}$ with two-bit control input [1]. It has been estimated that the implementation of the elements $F_{2/1}$ needs only 50% of the resources of two standard cells of a typical FPGA device and there exist some prerequisites to implement some advanced CEs. The $F_{2/2}$ type CEs controlled with two bits v_1 and

v_2 has been proposed as main building block, while designing the DDO boxes. The $F_{2/2}$ type CEs which provides construction of the CSPNs with high non-linearity and severe avalanche effect. These types of CEs were used for designing fast block ciphers suitable for effective implementation in FPGA devices, typical logic blocks of which contain the 16-bit memory cells.

Currently there are widely available the FPGA devices with 64-bit memory cells. This makes reasonable to use the CEs $F_{2/4}$ with four-bit controlled input for constructing the CSPN-based data-driven operations, replacing the CEs $F_{2/1}$ and $F_{2/2}$ in some given topology of CSPN. Such replacement provides higher non-linearity of the CSPNs containing the given number of the CEs and possibility to improve efficiency of the hardware implementation of block ciphers. Therefore CEs $F_{2/4}$ are proven to be more powerful cryptographic primitives. They potentially support designing more efficient CEs than elements F2/1 and $F_{2/2}$. With the applied advanced DDOs the design of ciphers with less number of rounds is supported, yielding to higher performance/cost ratio.

In this paper we consider the problem of developing criteria for selecting the CEs $F_{2/4}$ well suitable for their use while constructing the CSPNs and in the design of the fast block ciphers oriented to efficient hardware implementation using the FPGA devices Virtex-5, Virtex-6 and Virtex-7 [14]. The rest of the paper is organized as follows: Section 2 introduces the criteria to select CEs $F_{2/4}$ and presents basic cryptographic properties. In Section 3 a new DDO-based cipher, is proposed, well suited to FPGA implementations. FPGA synthesis results and comparisons with other known ciphers are also given. Finally, in Section 4 conclusions is discussed.

2. CRITERIA TO SELECT THE CEs F2/4 AND BASIC CRYPTOGRAPHIC PROPERTIES

2.1. Criteria to select CEs $F_{2/4}$

Controlled element $F_{2/4}$ has a two-bit input and output, and four-bit controlled input. Schematic representation of CEs $F_{2/4}$ is shown in Figure 1(a). By analogy with representation of the elements $F_{2/1}$ and $F_{2/2}$ [1] the CEs $F_{2/4}$ can be conveniently represented in the following variants:

- As a pair of Boolean functions (BF) with six variables as shown in Figure 1(b);
- As an ordered set of sixteen S-boxes of size 2 × 2 one of which is selected depending on the value of the controlled 4-bit vector to perform transformation of the input 2-bit binary vector (x_1, x_2). (The controlled 4-bit vector take on 16 different values $V = (v_1, v_2, v_3, v_4) = (0,0,0,1)$; $(0,0,1,0)$; $(0,0,1,1)$; …; $(1,1,1,1)$, to each of which an elementary S-box operation is to be assigned).

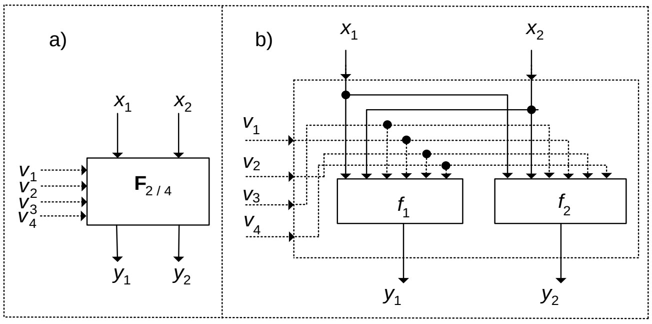

Figure 1. (a) Controlled element $F_{2/4}$, (b) its representation in the form of a pair of boolean functions

The first variant of representation is usually used in hardware implementation of CSPNs and in the investigation of linear properties of CEs and CSPNs. The second variant is used while selecting the CEs by specified criteria [1, 3]. Taking into account the results of the paper [1, 2], the following criteria for selecting concrete variants of the CEs $F_{2/4}$ has been formulated in the case of using the CEs $F_{2/4}$ as elementary building blocks for constructing the CSPNs having higher non-linearity and stronger avalanche effect:

- Criterion 1: Each of two outputs of the block $F_{2/4}$ should be a non-linear BF of six variables: $y_1 = f_1(x_1, x_2, v_1, v_2, v_3, v_4)$ and $y_2 = f_2(x_1, x_2, v_1, v_2, v_3, v_4)$; each of which has a value of non-linearity (NL), close to the maximum possible value of NL for balanced BF of six variables.
- Criterion 2: Each of the sixteen elementary modifications of the block $F_{2/4}$, namely $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, …, $F^{(15)}$ should be bijective transformation $(x_1, x_2) \rightarrow (y_1, y_2)$.
- Criterion 3: Each of the sixteen modifications CEs $F_{2/4}$ should be an involution.

- Criterion 4: The linear combination of two outputs y_1 and y_2, i.e. BF $f_3 = y_1 \oplus y_2$, should have non-linearity close to the non-linearity NL(y_1) and NL(y_2).

These criteria use the notion of the non-linearity (NL) of some BF Φ. The nonlinear is defined as distance from the BF Φ to the set of all affine BF in the same number of variables. Using these criteria, and sorting different variants of CEs $F_{2/4}$, one can find many specific elements of CEs $F_{2/4}$, that are of interest for the use in the design of block ciphers. The computational difficulty of the complete sorting of all possible variants of the CEs $F_{2/4}$ depends on the approach to implement the sorting. We have considered two approaches to this problem, previously used in the papers [1, 2] for sorting the CEs $F_{2/1}$ and $F_{2/2}$. Actually, the following two approaches has been used:

- Sorting all possible pairs of Boolean functions $y_1 = f_1(x_1, x_2, v_1, v_2, v_3, v_4)$ and $y_2 = f_2(x_1, x_2, v_1, v_2, v_3, v_4)$;
- Sorting all possible sets of 16 elementary S-box operations having the size 2 × 2, which are further denoted as modifications $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, ..., $F^{(15)}$ realized by the element $F_{2/4}$.

For first approach, the amount of computation required for the exhaustive search of possible variants CEs $F_{2/4}$, satisfying the specified criteria, is large enough. Indeed, there are 2^{64} of different BF of six variables, therefore it is required to sort $2^{64} \cdot (2^{64} - 1) \approx 3{,}4 \cdot 10^{38}$ different pairs of BF. The number of cases can be significantly reduced taking into account the well known result that each output of the S-box operation is a balanced BF. Thus, it is sufficient to sort all possible pairs of the balanced BF. Number of Balanced BF of n variables equals the number of combinations $C_{2^{n-1}}^{2^n}$, which for n = 6 is approximately equal to $1.83 \cdot 10^{18}$. This gives $3.35 \cdot 10^{18}$ variants that are out of the practical possibility to perform their exhaustive search.

The minimum number of variants of sorting is achieved with the second approach, since in this case, the design of effective CEs $F_{2/4}$ is reduced to the formal choice modifications of $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, …, $F^{(15)}$, each of which is a permutation of size 2×2. Number of substitutions having the size $n \times n$ is defined by $2^n!$, that for n=2 gives $2^2!=4!=24$. Moreover there are 10 variants of such substitutions as shown in Figure 2, satisfying the third criterion. Consequently, the visual design is reduced to the choice of pairs of such modifications and requires an analysis of 10^{16} variants. However, in this case the exhaustive search is applicable only while using large computational resources. For practical application of the CEs $F_{2/4}$, it suffices to find a relatively small number of such elements that represent their main subclasses that satisfy the formulated criteria. Therefore we can apply an exhaustive search for a representative statistical sample of CEs $F_{2/4}$, generating variants of elements $F_{2/4}$ by the equiprobable random sample of 16 modifications $F^{(i)}$, where i = 0, 1, …, 15.

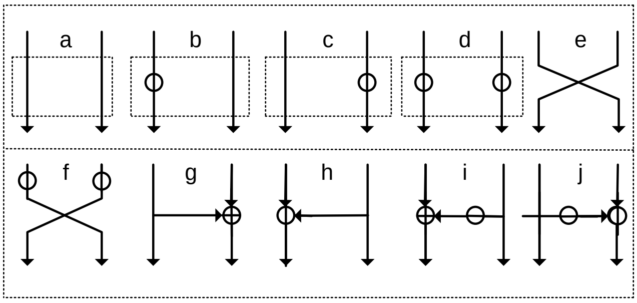

Figure 2. Schematic representation of the various existing transformations $(x_1, x_2) \to (y_1, y_2)$ that are involutions

To analyze the properties of the CEs $F_{2/4}$ defined by a set of the $F^{(i)}$ modifications, where i = 0, 1, …, 15, it is required to obtain the algebraic normal form of the BFs f_1 and f_2 describing the value of the first and second outputs of CEs $F_{2/4}$. Boolean functions f_1 and f_2 can be easily built for the set of sixteen ordered pairs of BF in two variables each of which describes one of sixteen modifications $F^{(i)}$, where i = 0, 1, …, 15, that define some variant of the element $F_{2/4}$. There are 10 various pairs of BF in two variables, which describe the elementary S-boxes that are involutions. Each of the possible 10 pairs of BF in two variables describing the modification of $F^{(i)}$ (i = 0, 1, …, 15), can be easily constructed using their schematic representation shown in Figure 2. Let $\{f_1^1(x_1, x_2), f_2^1(x_1, x_2)\}$ be the pair of BFs describing some given modification $F^{(0)}$ that corresponds to the value $V = (0,0,0,0)$. Let $\{f_1^2(x_1, x_2), f_2^2(x_1, x_2)\}$,

$\{f_1^3(x_1,x_2), f_2^3(x_1,x_2)\}$, …, $\{f_1^{16}(x_1,x_2), f_2^{16}(x_1,x_2)\}$ be the pairs of BFs describing some given modifications $F^{(1)}$, $F^{(2)}$, …, $F^{(15)}$ relating to the following values of the control vector $V = (0,0,0,1)$; $V = (0,0,1,0)$; …; $V = (1,1,1,1)$, respectively. Then the concrete form of two BF realizing CEs $F_{2/4}$, can be obtained from the following two formulas:

$$\begin{aligned}
y_1 = {} & (v_1 \oplus 1)(v_2 \oplus 1)(v_3 \oplus 1)(v_4 \oplus 1) f_1^1(x_1,x_2) \oplus (v_1 \oplus 1)(v_2 \oplus 1)(v_3 \oplus 1)v_4 f_1^2(x_1,x_2) \oplus \\
& \oplus (v_1 \oplus 1)(v_2 \oplus 1)v_3(v_4 \oplus 1) f_1^3(x_1,x_2) \oplus (v_1 \oplus 1)(v_2 \oplus 1)v_3 v_4 f_1^4(x_1,x_2) \oplus \\
& \oplus (v_1 \oplus 1)v_2(v_3 \oplus 1)(v_4 \oplus 1) f_1^5(x_1,x_2) \oplus (v_1 \oplus 1)v_2(v_3 \oplus 1)v_4 f_1^6(x_1,x_2) \oplus \\
& \oplus (v_1 \oplus 1)v_2 v_3(v_4 \oplus 1) f_1^7(x_1,x_2) \oplus (v_1 \oplus 1)v_2 v_3 v_4 f_1^8(x_1,x_2) \oplus \\
& \oplus v_1(v_2 \oplus 1)(v_3 \oplus 1)(v_4 \oplus 1) f_1^9(x_1,x_2) \oplus v_1(v_2 \oplus 1)(v_3 \oplus 1)v_4 f_1^{10}(x_1,x_2) \oplus \\
& \oplus v_1(v_2 \oplus 1)v_3(v_4 \oplus 1) f_1^{11}(x_1,x_2) \oplus v_1(v_2 \oplus 1)v_3 v_4 f_1^{12}(x_1,x_2) \oplus \\
& \oplus v_1 v_2(v_3 \oplus 1)(v_4 \oplus 1) f_1^{13}(x_1,x_2) \oplus v_1 v_2(v_3 \oplus 1)v_4 f_1^{14}(x_1,x_2) \oplus \\
& \oplus v_1 v_2 v_3(v_4 \oplus 1) f_1^{15}(x_1,x_2) \oplus v_1 v_2 v_3 v_4 f_1^{16}(x_1,x_2)
\end{aligned} \tag{1}$$

$$\begin{aligned}
y_2 = {} & (v_1 \oplus 1)(v_2 \oplus 1)(v_3 \oplus 1)(v_4 \oplus 1) f_2^1(x_1,x_2) \oplus (v_1 \oplus 1)(v_2 \oplus 1)(v_3 \oplus 1)v_4 f_2^2(x_1,x_2) \oplus \\
& \oplus (v_1 \oplus 1)(v_2 \oplus 1)v_3(v_4 \oplus 1) f_2^3(x_1,x_2) \oplus (v_1 \oplus 1)(v_2 \oplus 1)v_3 v_4 f_2^4(x_1,x_2) \oplus \\
& \oplus (v_1 \oplus 1)v_2(v_3 \oplus 1)(v_4 \oplus 1) f_2^5(x_1,x_2) \oplus (v_1 \oplus 1)v_2(v_3 \oplus 1)v_4 f_2^6(x_1,x_2) \oplus \\
& \oplus (v_1 \oplus 1)v_2 v_3(v_4 \oplus 1) f_2^7(x_1,x_2) \oplus (v_1 \oplus 1)v_2 v_3 v_4 f_2^8(x_1,x_2) \oplus \\
& \oplus v_1(v_2 \oplus 1)(v_3 \oplus 1)(v_4 \oplus 1) f_2^9(x_1,x_2) \oplus v_1(v_2 \oplus 1)(v_3 \oplus 1)v_4 f_2^{10}(x_1,x_2) \oplus \\
& \oplus v_1(v_2 \oplus 1)v_3(v_4 \oplus 1) f_2^{11}(x_1,x_2) \oplus v_1(v_2 \oplus 1)v_3 v_4 f_2^{12}(x_1,x_2) \oplus \\
& \oplus v_1 v_2(v_3 \oplus 1)(v_4 \oplus 1) f_2^{13}(x_1,x_2) \oplus v_1 v_2(v_3 \oplus 1)v_4 f_2^{14}(x_1,x_2) \oplus \\
& \oplus v_1 v_2 v_3(v_4 \oplus 1) f_2^{15}(x_1,x_2) \oplus v_1 v_2 v_3 v_4 f_2^{16}(x_1,x_2)
\end{aligned} \tag{2}$$

2.2. Basic cryptographic properties

Table 1 shows examples of the sets of the F(i) modifications, which satisfy the non-linearity criteria 1 and 3. It is of interest to study differential characteristics of the CEs F2/4 shown in Figure 2. Next Figure 3 shows the variants of all possible differences related to the F2/4-type CEs. Table 2 presents the results on the investigation of the differential characteristics for CEs F2/4, defined by a set of modifications of № 4 in Table 1.

Table 1. The examples of the sets of the F(i) modifications

№	The value of the non-linearity of BF NL(f_1)- NL(f_2)- NL(f_3)	Set of modifications
1	22-22-22	*a/b/d/e/f/g/h/i/a/b/c/e/f/g/e/j*
2	22-24-22	*a/b/c/e/f/g/h/j/a/d/e/f/g/h/g/i*
3	24-22-22	*a/b/d/e/f/h/i/j/a/b/c/e/g/h/g/j*
4	22-22-24	*a/b/d/e/g/h/i/j/b/d/e/f/g/h/i/g*

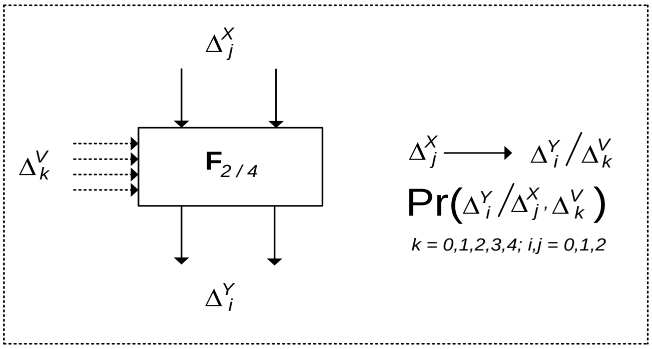
Δ_j^X
Δ_k^V
$F_{2/4}$
Δ_i^Y
$\Delta_j^X \longrightarrow \Delta_i^Y / \Delta_k^V$
$\Pr(\Delta_i^Y / \Delta_j^X, \Delta_k^V)$
k = 0,1,2,3,4; i,j = 0,1,2

Figure 3. Variants of the differences for the CEs $F_{2/4}$

Table 2. Differential characteristics of CEs $F_{2/4}$

i	*j*	*k*	Pr	*i*	*j*	*k*	Pr
0	0	0	1.00	2	1	2	0.242
0	0	1	0.00	2	2	0	0.291
0	0	2	0.00	2	2	1	0.484
0	1	0	0.00	2	2	2	0.225
0	1	1	0.75	3	0	0	0.273
0	1	2	0.25	3	0	1	0.438
0	2	0	0.00	3	0	2	0.289
0	2	1	0.50	3	1	0	0.219
0	2	2	0.50	3	1	1	0.563
1	0	0	0.211	3	1	2	0.219
1	0	1	0.563	3	2	0	0.289
1	0	2	0.227	3	2	1	0.438
1	1	0	0.281	3	2	2	0.273
1	1	1	0.500	4	0	0	0.281
1	1	2	0.219	4	0	1	0.500
1	2	0	0.227	4	0	2	0.219
1	2	1	0.438	4	1	0	0.250
1	2	2	0.336	4	1	1	0.500
2	0	0	0.224	4	1	2	0.250
2	0	1	0.500	4	2	0	0.219
2	0	2	0.276	4	2	1	0.500
2	1	0	0.253	4	2	2	0.281
2	1	1	0.505				

3. 128-BIT BLOCK CIPHER MM-128

3.1. Description of the cipher MM-128

Found variants of the CEs $F_{2/4}$ satisfying the non-linearity criteria can be used for building CSPNs oriented for the use in fast block ciphers. The CEs $F_{2/4}$ relating to variant 4 in Table 1, for which non-linear and differential characteristics are presented in Table 2 and Table 3, have been used to design the block cipher MM-128 representing eight rounds iterative block cipher with 128-bit data blocks. This cipher uses 256-bit secret key $K = (K_1, K_2, K_3, K_4)$, where K_1, K_2, K_3, K_4 are 64-bit subkeys, which are used directly as operands of the transformation operations. The MM-128 uses no precomputing the round keys, therefore it saves high performance of the data encryption even in the case of frequent change of keys. Such property is important for solving some practical problems of information security. The iterated structure of the MM-128 is shown in Figure 4(a), and the structure of transformation rounds is presented in Figure 4(b).

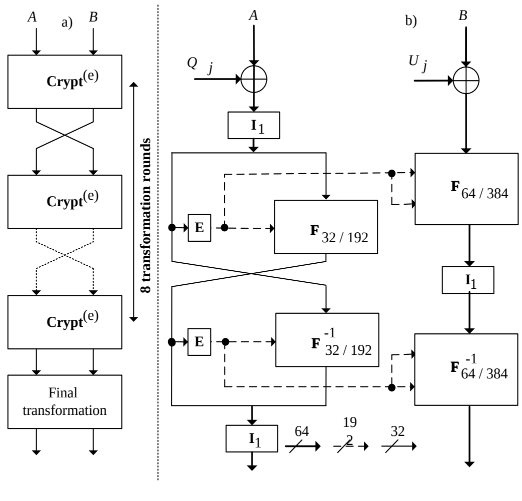

Figure 4. (a) Iterative structure of MM-128, (b) Design of procedure crypt

In general, the encryption procedure of the MM-128 is described as follows: $Y = T^{(e)}(X, K)$, where $X = (A, B)$ is input data block (plaintext), Y is the ciphertext block, $X, Y \in \{0, 1\}^{128}$; $T^{(e)}$ is the transformation function; $e \in \{0, 1\}$ is the parameter that determines the transformation mode: encryption ($e = 0$) or decryption ($e = 1$). The encryption process of MM-128 is described as follows:

- For $j = 1$ to 7 do: $\{(L, R) \leftarrow \mathrm{Crypt}^{(e)}(L, R, Q_j, U_j); (L, R) \leftarrow (R, L)\}$.
- Perform transformation: $(L, R) \leftarrow \mathrm{Crypt}^{(e)}(L, R, Q_8, U_8)$.
- Perform final transformation: $\{(L, R) \leftarrow (L \oplus Q_9, R \oplus U_9)\}$.

Final transformation is performed by performing the XORing the data subblocks with corresponding subkeys. Final transformation is required to provide the identity of encryption and decryption procedures. Due to which the hardware implementation cost of the MM-128 is significantly reduced.

In the left branch of this cipher there are used two CSPNs $F_{32/192}$, $F^{-1}_{32/192}$ operations, where the operation $F_{32/192}$ is a cascade of four CSPNs $F_{8/48}$ as shown in Figure 5, and the operation $F^{-1}_{32/192}$ is a cascade of four CSPNs $F^{-1}_{8/48}$ as shown in Figure 5. In the right branch of the cipher there are used two CSPNs $F_{64/384}$ and $F^{-1}_{64/384}$ operations, where the operation $F_{64/384}$ a cascade of eight CSPNs $F_{8/48}$, and the operation $F^{-1}_{64/384}$ is a cascade of eight CSPNs $F^{-1}_{8/48}$.

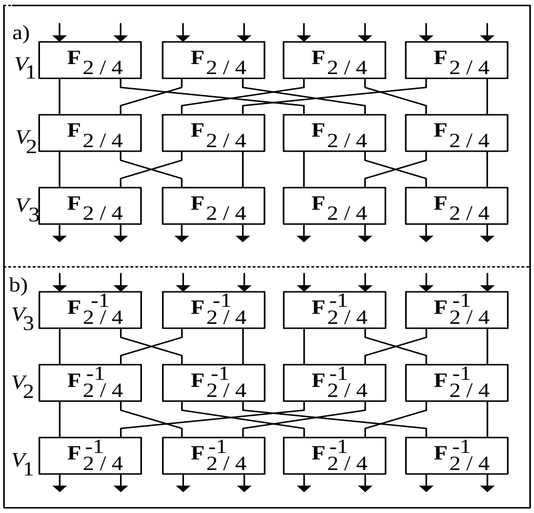
a)
V_1
$\mathbf{F}_{2/4}$ $\mathbf{F}_{2/4}$ $\mathbf{F}_{2/4}$ $\mathbf{F}_{2/4}$
V_2
$\mathbf{F}_{2/4}$ $\mathbf{F}_{2/4}$ $\mathbf{F}_{2/4}$ $\mathbf{F}_{2/4}$
V_3
$\mathbf{F}_{2/4}$ $\mathbf{F}_{2/4}$ $\mathbf{F}_{2/4}$ $\mathbf{F}_{2/4}$
b)
V_3
$\mathbf{F}^{-1}_{2/4}$ $\mathbf{F}^{-1}_{2/4}$ $\mathbf{F}^{-1}_{2/4}$ $\mathbf{F}^{-1}_{2/4}$
V_2
$\mathbf{F}^{-1}_{2/4}$ $\mathbf{F}^{-1}_{2/4}$ $\mathbf{F}^{-1}_{2/4}$ $\mathbf{F}^{-1}_{2/4}$
V_1
$\mathbf{F}^{-1}_{2/4}$ $\mathbf{F}^{-1}_{2/4}$ $\mathbf{F}^{-1}_{2/4}$ $\mathbf{F}^{-1}_{2/4}$

Figure 5. (a) Schematic representation of CSPNs F8/48, (b) F−18/48

The key schedule of the algorithm MM-128 is presented in Table 3. The extension box E is described as follows: $E(X) = (X, X^{<<2}, X^{<<4}, X^{<<6}, X^{<<8}, X^{<<10})$, where $X^{<<b}$ denotes a cyclic rotation of the vector $X = (x_1, ..., x_{32})$ to the left by b bits. The permutation involution I_1 is described as follows:

(1)(2,9)(3,17)(4,25)(5,33)(6,41)(7,49)(8,57)(10)(11,18)(12,26)(13,34)(14,42)
(15,50)(16,58)(19)(20,27)(21,35)(22,43)(23,51)(24,59)(28)(29,36)(30,44)(31,52)
(32,60)(37)(38,45)(39,53)(40,61)(46)(47,54)(48,62)(55)(56,63)(64).

Table 3. Key scheduling in MM-128

$j =$	1	2	3	4	5	6	7	8	9
$Q_j^{(e=0)}$	K_1	K_2	K_3	K_4	K_4	K_1	K_3	K_4	K_1
$U_j^{(e=0)}$	K_3	K_4	K_2	K_1	K_2	K_3	K_2	K_3	K_2
$Q_j^{(e=1)}$	K_1	K_3	K_2	K_3	K_2	K_1	K_2	K_4	K_3
$U_j^{(e=1)}$	K_2	K_4	K_3	K_1	K_4	K_4	K_3	K_2	K_1

3.2. Security estimation of MM-128

Differential analysis of the MM-128 has shown that the differential characteristics [15-20] with a small number of active bits have significantly higher probability compared with the characteristics, which include the differences having larger weight. The greatest probability from the investigated differential characteristics relates to the case of the difference $(\Delta^{L}_{1},0)$ passes through two rounds. Indicated difference passes two rounds of MM-128 with the probability $P(2) < 2^{-44}$ as shown in Figure 6. Experimental studies have shown that the probability of a difference with one active bit after two rounds is $\approx 2^{-47}$. In accordance with the obtained results on investigating the differential characteristics of MM-128 one can concluded that after six rounds of the encryption the MM-128 cipher is indistinguishable from a random transformation with a differential analysis.

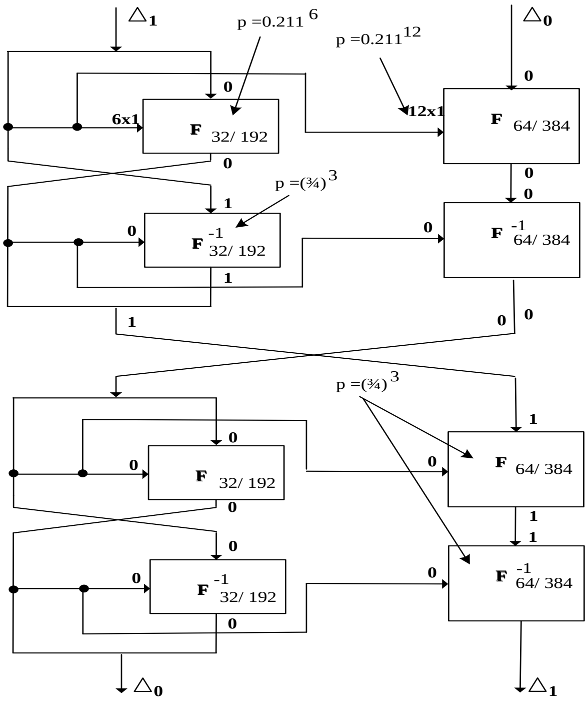

Figure 6. Formation of the two round iterative difference (Δ^L_1, Δ^R_0) with probability $Pr(2) \approx 2^{-44}$

3.3. FPGA synthesis results and comparisons

Cipher MM-128 has a high efficiency of the hardware implementation as compared with the block cipher AES. We have implemented MM-128 using FPGA (Xilinx Virtex-5) and iterative looping architecture. This architecture was chosen for comparative estimation of the effectiveness of the implementation of other well-known ciphers because it is suitable for performing encryption in the cipher block chaining mode that is the most frequently used one. The transition from the electronic codebook mode to Cipher Block Chaining has no effect on the performance of the encryption process in the case of iterative looping architecture, while in the case of pipelined (or partially pipelined) architecture of such transition leads to a notable decrease of the encryption rate.

For execution a comparative analysis of the effectiveness of the hardware implementation of the cipher MM-128, estimated in terms of "performance/cost" [1] there was performed simulation modeling of the hardware implementation of MM-128 and well-known block cipher AES which is currently widely used for information security. From the results shown in Table 4 one can conclude that the developed cipher is much more efficient for the considered hardware implementation in comparison with the advanced encryption standard (AES).

Table 4. FPGA synthesis results and comparisons

Cipher	Design	Frequency (MHz)	Area (CLBs)	Data Rate (Mbps)	Integral efficiency Mbps/#CLBs	Integral efficiency Mbps/# (CLB * GHz)
MM-128 (proposed)	XC5VSX240T	420,2	95	6.723	70,77	168,08
Eagle-128 [3]	XC5VSX240T	92	781	1.177	1,51	16,4
AES [21]	XC5VLX50	339,87	200	4.350	21,75	63,97
AES [22]	XC5VSX240T	233	750	119.300	159,07	681,71
AES [23]	XC5VLX110T	202,26	4448	25.890	5,82	29,1
AES [24]	Virtex7	456	1222	5.300	4,34	9,51
AES [25]	XC6VLX240T	319,29	2964	40.870	13,79	91,12
AES [26]	XC6VLX240T	323,73	168	3.450	20,53	63,43
AES [27]	XC5VLX110T	232,30	1894	29.730	15,70	62,24

4. CONCLUSION

This work focuses on advancing the DDO-based approach to the block cipher design. A new class of the $F_{2/4}$-type CEs have been introduced as cryptographic primitive suitable to the design of the FPGA efficient DDO boxes. Using the CEs $F_{2/4}$ as the main building block is very attractive for designing fast block ciphers suitable for efficient hardware implementation on the base of contemporary FPGA devices (Virtex-5, Virtex-6 and Virtex-7). Their use can substantially increase the efficiency index of the hardware implementation of block ciphers, which is estimated as the ratio "encryption speed per hardware implementation cost". In our estimations the cost of the used hardware resources are measured in number of the required logic blocks of the FPGA devices. The results of the study of non-linearity, differential and linear characteristics of the proposed CE show that the CE has better cryptographic properties than the previously applied CEs $F_{2/1}$ and $F_{2/2}$. Based on the CEs $F_{2/4}$ there were built CSPNs used as transformation operations of new block cipher MM-128 which provides high performance and low cost of the hardware implementation. The performed differential analysis of this 8-round iterative cipher has show that 6 rounds of encryption provide a pseudo-transformation of the input data block. Specifying two additional rounds provides a certain "safety margin" for MM-128 cipher.

ACKNOWLEDGMENTS

This research was funded by the Ministry of Science and Technology (MOST) under grant KC.01.22/16-20.

REFERENCES

[1] N. A. Moldovyan and A. A. Moldovyan, "Data-driven ciphers for fast telecommunication systems," *Auerbach Publications, Talor & Francis Group*, New York, London, 2007.

[2] N. A. Moldovyan, et al., "A class of data-dependent operations," *International Journal of Network Security*, vol. 2, no. 3, pp. 187-204, 2006.

[3] N. A. Moldovyan, et al., "New class of Cryptographic Primitives and Cipher Design for Network Security," *International Journal of Network Security*, vol. 2, no. 2, pp. 114-125, 2006.

[4] N. A. Moldovyan, "On Cipher Design Based on Switchable Controlled Operations," *International Journal of Network Security*, vol. 7, no 3, pp. 404-415, 2008.

[5] N. H. Minh, et al., "Design and estimate of a new fast block cipher for wireless communication devices," in *2008 International Conference on Advanced Technologies for Communications,* pp. 409-412, 2008.

[6] N. H. Minh, et al., "KT-64: A New Block Cipher Suitable to Efficient FPGA Implementation," *International Journal of Computer Science and Network Security,* vol. 10, no. 1, pp. 10-18, 2010.

[7] B. D. Thi, et al., "An Effective and Secure Cipher Based on SDDO," *International Journal of Computer Network and Information Security,* vol. 11, pp. 1-10, 2012.

[8] N. H. Minh, et al., "New SDDO-Based Block Cipher for Wireless Sensor Network Security," *International Journal of Computer Science and Network Security,* vol. 10, no. 3, pp. 54-60, 2010.

[9] B. D. Thi and N. H. Minh, "High-Speed Block Cipher Algorithm Based on Hybrid Method," in *Proceedings Ubiquitous Information Technologies and Applications, Lecture Notes in Electrical Engineering*, pp. 285-291, 2014.

[10] P. M. Tuan, et al., "New Block Ciphers for Wireless Moblile Netwoks," in *Proceedings of the International Advances in Information and Communication Technology (ICTA 2016)*, pp. 393-402, 2017.

[11] A. A. Moldovyan, et al., "Controlled Elements for Designing Ciphers Suitable to Efficient VLSI Implementation," *Telecommunication Systems,* vol. 32, pp. 149-163, 2006.

[12] N. A. Moldovyan, "On Cipher Design Based on Switchable Controlled Operations," in *Proceedings of the International workshop on mathematical Methods, Models, and Architectures for Computer Network Security,* Berlin. Springer-Verlag, pp. 316-327, 2003.

[13] N. Moldovyan and A. Moldovyan, "Innovative Cryptography," *2 edition, Charles River Media,* 2006.

[14] Xilinx, "Xilinx Solutions," [Online], Available: http://www.xilinx.com/products/.

[15] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Journal of Cryptology,* vol. 4, no. 1, pp. 3-72, 1991.

[16] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," *Springer,* Verlag Berlin, Heidelberg, 1993.

[17] L. R. Knudsen, "Truncated and Higher Order Differentials," *International Workshop on Fast Software Encryption*, pp. 196-211, 1995.

[18] F. Chabaud and S. Vaudenay, "Links Between Differential and Linear Cryptanalysis," *Workshop on the Theory and Application of Cryptographic Technigues, Advances in Cryptology - EUROCRYPT '94,* pp. 356-365, 1994.

[19] Z. Pei and Z. Wenying, "Differential Cryptanalysis on Block Cipher Skinny with MILP Program," *Security and Communication Networks, Special Issue: Machine Learning for Wireless Multimedia Data Security*, 2018.

[20] M. ElSheikh and A. M. Youssef, "Related-key Differential Cryptanalysis of Full Round CRAFT," *International Conference on Security, Privacy, and Applied Cryptography Engineering*, pp. 50-66, 2019.

[21] M. H. Rais and S. M. Qasim, "Efficient Hardware Realization of Advanced Encryption Standard Algorithm using Virtex-5 FPGA," *International Journal of Computer Science and Network Security*, vol. 9, no. 9, pp. 59-63, 2009.

[22] L. Henzen and W. Fichtner, "FPGA parallel-pipelined AES-GCM core for 100G ethernet applications," in *Proceedings of ESSCIRC*, pp. 202-205, 2010.

[23] R. S. S. K. Reddy and P. Praneeth, "VLSI implementation of AES crypto processor for high throughput," *International Journal of Advances in Engineering, Science and Technology*, vol. 6, pp. 22-26, 2011.

[24] U. Hussain and H. Jamal, "An efficient high throughput FPGA implementation of AES for multi-gigabit protocols," in *10th International Conference on Frontiers of Information Technology*, pp. 215-218, 2012.

[25] Y. Wang and Y. Ha, "FPGA-based 40.9-gbits/s masked AES with area optimization for storage area network," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 60, no. 1, pp. 36-40, 2013.

[26] Q. Liu, et al., "High throughput and secure advanced encryption standard on field programmable gate array with fine pipelining and enhanced key expansion," *IET Computers Digital Techniques*, vol. 9, no. 3, pp. 175-184, 2015.

[27] H. Zodpe and A. Sapkal, "An efficient AES implementation using FPGA with enhanced security features," *Journal of King Saud University - Engineering Sciences*, vol. 32, no. 2, pp. 115-122, 2020.

BIOGRAPHIES OF AUTHORS

Minh Nguyen Hieu is a Vice dean with the Institute of Cryptographic Science and Technology, Hanoi, Vietnam. He received his Ph.D. from the Saint Petersburg Electrical Engineering University (2006). His research interests include cryptography, communication and network security. He has authored or co-authored more than 85 scientific articles, books chapters, reports and patents, in the areas of his research.

Duy Ho Ngoc is an expert of Cyber Command 86, Vietnam Ministry of Defence, Danang, Vietnam. His research interests include cryptography, communication and network security. He received his Ph.D. from the Saint Petersburg Electrical Engineering University (2009).

Canh Hoang Ngoc is a Lecturer with the Thuongmai University, Hanoi, Vietnam. He received his master-degree in information systems from Le Quy Don Technical University of Vietnam in 2012. His research interests include cryptography, database, machine learning. Currently, besides teaching, he works as a network administrator and database administrator at Thuongmai University.

Trung Dinh Phuong is a Researcher at the Vietnam Government Information Security Committee (VGISC), Hanoi, Vietnam. His research interests include network security and cryptography.

Manh Tran Cong got his master-degree in computer science from Le Quy Don Technical University of Vietnam in 2007. In 2017 Manh got his PhD degree from Department of Computer Science, National Defense Academy, Japan. His current research interests include network traffic classification/analysis and anomaly/malicious detection. Currently, Dr. Manh works as a researcher in Le Quy Don Technical University, Hanoi, Vietnam.