I. J. Computer Network and Information Security, **2012, 11, 1-10**
Published Online October 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.11.01

An Effective and Secure Cipher Based on SDDO

Bac Do Thi
University of Information and Communication Technology, Thai Nguyen, Viet Nam
dtbac@ictu.edu.vn

Minh Nguyen Hieu
Le Qui Don Technical University, Ha Noi, Viet Nam
hieuminhmta@ymail.com

Duy Ho Ngoc
Department of Information Technology, Ha Noi, Viet Nam

Abstract — To improve the efficiency of security of the information secure mechanism, an algorithm BMD-128 is proposed. This algorithm is built on the SDDO. Using this operator decreases significanthy the cost of hardware implementation. Besides, it also ensures both the high applicability in the transaction needing the change of session keys with high frequency and the ability against slide attack. Concurrently, this algorithm also eliminates the weak keys without the complex round key proceduce. The algorithm is evaluated regards to the standard NESSIE and the ability against the differential cryptanalysis. Concurrently, it is also compared the performance with the other famous ciphers when implementing on hardware FPGA.

Index Terms — Switchable data-dependent operations, hardware implementation, block cipher, controlled substitution permutation network, FPGA

I. Introduction

Nowadays, the standard encryption AES [2] and other encryption algorithms are widely used in information security of Communication Networks. However, in the fast telecommunication systems requiring the optimization on hardware implementation or the specialized applications, it is very difficult to ensure when using those algorithms. To solve this requirement, [8-10, 13] have proposed the block cipher on the basis of the controlled substitution permutation network (CSPN). Besides, a very important element that the advanced encryption algorithms need to achieve is to ensure high speed in case of frequent change of secret keys. This was also studied and solved in [8-10, 12, 13] regards to synthetic methods of algorithms which don't used the complexity transformation generating subkeys but use very simple key schedules. This solution ensures both the fast encryption in the case of frequent change of keys and the cheap hardware implementation.

However, [10] also point out the weakness of non-use of that key change process. That is the existence of weak key layers, which mean that it will reduce security of the ciphering algorithm. The existence of this weak key layer is because of the lack of procedure to generate the complex key, which leads to the fad that the attacker could use attacking method based on related-key [1] as in the algorithm IDA, GOST 28147, TEA, [3, 5-7]. Some solutions to prevent related-key:

a) Precomputation of key scheduling, algorithms in reality often use this method. Howerer, the resources to perform this algorithm will increase while changing speed will derease.
b) Developing algorithm with round function is changed.
c) Generating round keys "on the fly" with this method, the resource to perform the algorithm will increase significautly while changing speed won't change.

With the second solution, against the weak key lagers is solved in [11-13] by proposing the building block cipher 64 bits based on SDDOs.

Moreover, block ciphers which are being used have block size of 64 bits, but it also needs to have larger size cipher in order to ensure high flexibility due to its requirement and different applications. Concurrently, the higher the block cipher is, the higher security is, before the attacks.

With the problems denoted, a new cipher BMD-128 is proposed. It is developed based on SDDO with the block size of 128 bit, not ues procedure to generate the complex key. Thus, it is evaluated to be more suitable in fast telecommunication network.

This article is organired as follows: part 1, general instruction; part 2, the structure of switchable data-dependent operations data used in developing algorithms; part 3, representing developing algorithms; part 4, the results of evaluation and comparision the statical characteristics of the algorithms developed based on NESSIE's criterias; part 5, differential analysis; part 6, evaluation and comparision performance when implementing developing algorithms on FPGA comparing with the famous algorithms and finally, conclusion.

II. THE STRUCTURE OF SDDO

The in [12], Moldovyan N.A described SDDO using Hawk 64 cipher based on minimum controlled element $F_{2/1}$. Next, on the basic of symmetry topology of CSPN, it is very easy for us to build SDDO, which is the combination of active layers L_i and the fixed permutation πj [10]. The general structure of SDDO is presented in figure 1. The structure of SDDO is also the structure of CSPN, but it has the switchable controlling bit e which is used to control the distribution of the controlling vectors of lagers in CSPN. If e = 0 then the controlling vectors is distributed as follows: V_1, V_2 … V_s and if e = 1 then the controlling vectors is presented as V_s, V_{s-i} , …,V_1. Therefore, the building SDDO on symmetry CSPNs is very simple. The structure of SDDOs which user BMD–128 and minimum controlled element $F_{2/2}$ is given below.

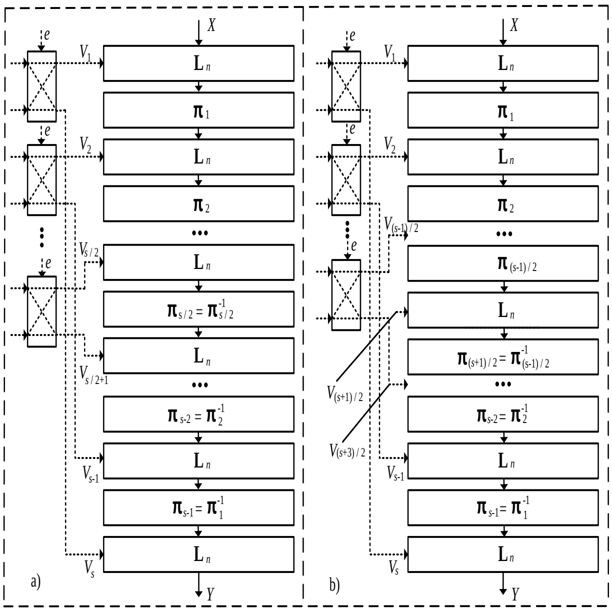

Fig 1.Structure of SCO $\mathbf{F}^{(V,e)}_{n/m}$. a. in case of even layer; b. in case of odd layer

The switchable data-dependent controlled operations which on in BMD-128 are built via CSPNs with symmetry topology. CSPNs are designed to enlarge directly and indirectly via the minimum controlled element $F_{2/2}$. $F_{2/2}$ is shown in figure 2. $F_{2/2}$ is represented as a pair of BFs in four variables or as four 2×2 substitutions. If it is described in logic function y_1, y_2 and y_3=y_1+y_2, they will have higher number of 3. Consequently, non-linear (NL) value NL=4. The algebraic normal form of logic function of y_1, y_2 and y_3 is shown below:

$$y_1 = vzx_1 \oplus vx \oplus zx_1 \oplus zx_2 \oplus v \oplus x_1 \oplus 1; NL(y_1) = 4;$$
$$y_2 = vzx_2 \oplus vz \oplus vx_1 \oplus zx_1 \oplus zx_2 \oplus v \oplus z \oplus x_2 \oplus 1; NL(y_2) = 4;$$
$$y_3 = vzx_1 \oplus vzx_2 \oplus vx_1 \oplus x_1 \oplus v \oplus x_1 \oplus x_2; NL(y_3) = 4;$$

NL(.) non-linearity of logic function for function affine based on the numbers of available variates. The differential characteristics of $F_{2/2}$ are described in table I.

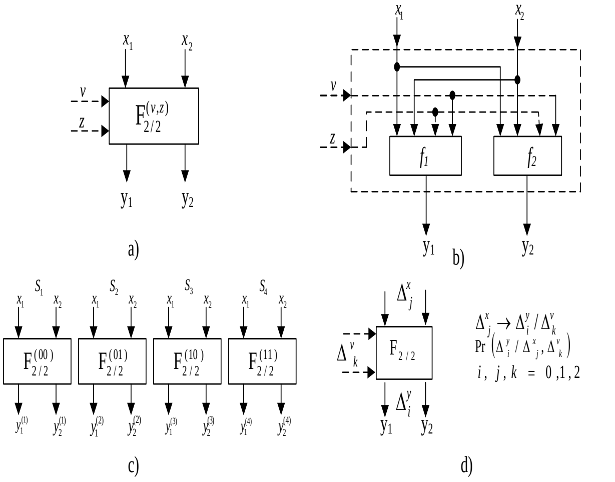

Fig 2.The representation of the $F_{2/2}$. a. General; b. represented as a pair of BFs in four variables; c. four 2×2 substitutions. d. Differential representation.

TABLE I. PROBABILITIES PR(IJK)=PR(Δ^Y_I / Δ^X_J, Δ^V_K) OF ANY DIFFERENTIAL CHARACTERISTICS OF $F_{2/2}$ ELEMENT.

i, j k	001	002	011	101	110	120	002	102	102	202
$F_{2/2}$	0,25	0,125	0,1875	0,375	0,75	0,5	0,125	0,5	0,375	0,375

From $F_{2/2}$, we synthesize and construct the structure of expanded operator with symmetry. In particular, $F_{8/32}$ is built from 16 elements $F_{2/2}$ which is divided into 4 layers in which each layer consists of 4 elements (see figure 3). Alternating between layers is the fixed permutations described in diagram. Then, 4 blocks $F_{8/32}$ are combined parallel, so $F_{32/128}$ is generated as a part in figure 5. In figure 5, the blocks $F_{32/128}$ and the blocks of substitution S_{4x4} in SPN with fixed permutation I_1 and I_2 are combined as seen in the figure. The fixed permutation network SPN (see Figure 5) is constructed on the basic of permutational table used the Cipher DES. Where I_1 and I_2 are described as follows:

I_1 = (1)(2,9)(3,17)(4,25)(5)(6,13)(7,21)(8,29)(9,2)(10)(11,18)(12,26)(13,6)(14)(15,22)(16,30)(17,3)(18,11)(19)(20,27)(21,7)(22,15)(23)(24,31)(25,4)(26,12)(27,20)(28)(29,8) (30,16) (31,24) (32)

I_2 = (1)(2,5)(3,9)(4,13)(5,2)(6)(7,10)(8,14)(9,3)(10,7)(11)(12,15)(13,4)(14,8)(15,12)(16)(17)(18,21)(19,25)(20,29)(21,18)(22)(23,26)(24,30)(25,19)(26,23)(27)(28,31) (29,20) (30,24) (31,28) (32).

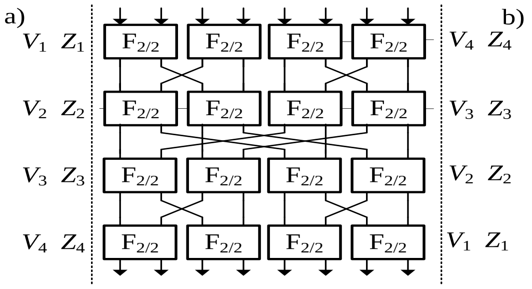

Fig 3.The structure of $F_{8/32}$ (a), $F^{-1}_{8/32}$ (b)

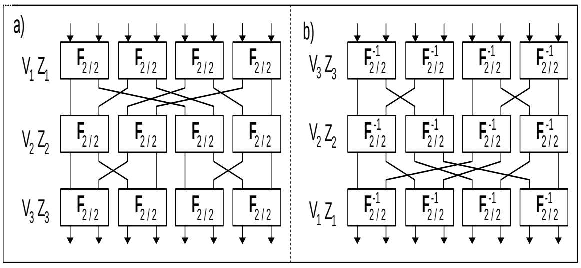

Fig 4.The structure of $F_{8/24}$ (a) and $F^{-1}_{8/24}$

With the block $F_{8/32}$ as figure 4, they are synthesized from 12 elements $F_{2/2}$ which are divided into 3 layers in which each layer includes 4 parallel elements. There are symmetric fixed permutations between layers shown in figure. Figure 6 describes detail the controlled block $F_{64/384}$; where $F_{64/384}$ is built indirectly via 16 blocks $F_{8/24}$ which is divided into 2 layers in which each layer includes 8 parallel blocks. Between 2 layers, it is the fixed permutation **I** described as follows:

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

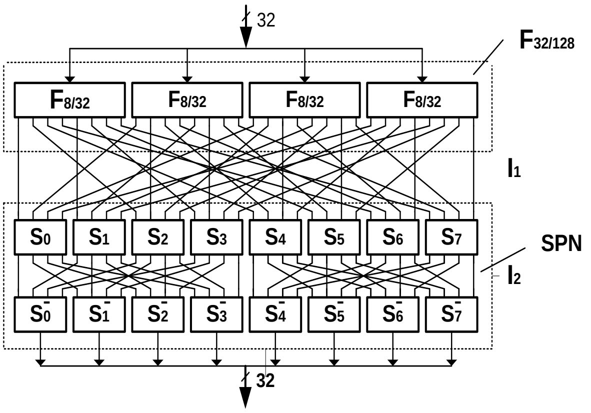
32
$F_{32/128}$
$F_{8/32}$
I_1
S_0 S_1 S_2 S_3 S_4 S_5 S_6 S_7
SPN
I_2
$\bar{S_0}$ $\bar{S_1}$ $\bar{S_2}$ $\bar{S_3}$ $\bar{S_4}$ $\bar{S_5}$ $\bar{S_6}$ $\bar{S_7}$
32

Fig 5.The structure of $F_{32/128}$, I_1 and SPN

On the basic of $F_{32/128}$ and $F_{64/384}$, we embed the switchable controlled operator (SCO) to generate SDDO. SCO is created via the combination of the controlled element of parallel combination $P_{2/1}$ and 2 expanded operators E and E'. The detail structure of SDDO $\mathbf{F}^{(L,e)}_{32/128}$ and $\mathbf{F}^{(L,e)}_{64/384}$ is shown in figure 7.

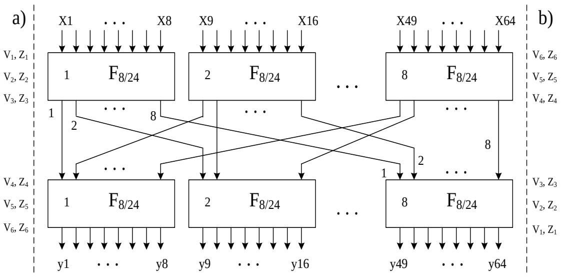

Fig 6.The structure of $F_{64/384}$ (a) and $F^{-1}_{64/384}$ (b)

In figure 7, to control the distribution of the controlling vector in $\mathbf{F}^{(L,e)}_{32/128}$ and $\mathbf{F}^{(L,e)}_{64/384}$, we use 16 permutations $P_{2/1}$ which are connected parallel. The expandion of bits in E and E' is performed as follows:

Box E: 32 bits which is seen as the right sub branch of figure 7 it is an input of the extension box E is $L=(L_1, L_2)$ with $L_1, L_2 \in \{0, 1\}^{16}$, while the controlling vector $V=(V_1,Z_1,V_2,Z_2,V_3,Z_3,V_4,Z_4,V_5,Z_5,V_6,Z_6)$ uses the switchable controlled operator $\mathrm{F}^{(L,e)}_{64/384}$ gerenerated as follows:

$$V_1=L_1\|L_2^{<<<2},\ V_2=L_1^{<<<4}\|L_2^{<<<6},\ V_3=L_1^{<<<8}\|L_2^{<<<10},$$
$$V_4=L_2^{<<<8}\|L_1^{<<<10},\ V_5=L_2^{<<<4}\|L_1^{<<<6},\ V_6=L_2\|L_1^{<<<2};$$
$$Z_1=L_1^{<<<6}\|L_2^{<<4},\ Z_2=L_1^{<<<12}\|L_2^{<<8},\ Z_3=L_1\|L_2^{<<<12},$$
$$Z_4=L_2\|L_1^{<<<12},\ Z_5=L_2^{<<12}\|L_1^{<<<8},\ Z_6=L_2^{<<<6}\|L_1^{<<<4};$$

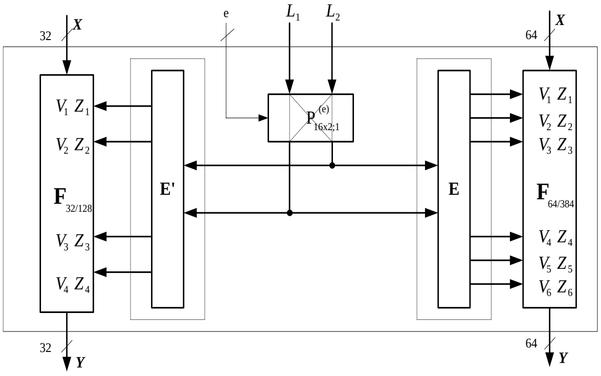

Fig 7.The structure of SDDO $\mathbf{F}^{(L,e)}_{32/128}$, $\mathbf{F}^{(L,e)}_{64/384}$

Box E′: Similary, 32 bits is seen as the left sub branch of figure 3 (it is an output of the extention block E') then the controlling vector $V=(V_1,Z_1,V_2,Z_2,V_3,Z_3,V_4,Z_4)$ uses the switchable controlled block $\mathrm{F}^{(L,e)}_{32/128}$ created as follows:

$$V_1=L_1,\ V_2=L_1^{<<<8},\ V_3=L_2^{<<<8},\ V_4=L_2;$$
$$Z_1=L_1^{<<<6},\ Z_2=L_1^{<<<12},\ Z_3=L_2^{<<<12},\ Z_4=L_2^{<<<6}.$$

Above is the whole structure of SDDOs used in the algorithm BMD-128. With this structure, it is more interesting to build from $F_{2/2}$ which will provide a huge support in generating the high performace Cipher.

III. The Cipher BMD-128

The Cipher BMD-128 is the block cipher with the block size of 128 bits. Its includes eight – round change as seen in figure 8, without the complex used secret key procedure and constructed on the basic of SDDO in combining with the fixed permutation network. The prominent characteristics that BMD-128 oriented to:

a) Using the nontinear transformation with the differential characteristics in correspondence with the minimum controlled element.
b) Orienting to implementation on hardware which has ability or cheap reconfiguration with high speed encryption.
c) The process in encrypted cirle is parellel so it help to create high speed encryption.
d) The process of the extention of keys is simple. Therefore, it ensures a high speed encryption in the case of frequent change of keys.
e) The encryption and decryption procedure are used the same diagram.
f) The security and efficiency are improved.

According to the diagram algorithm, each basic round unit of BMD-128 uses 2 elements SDDO which are $F^{(L,e)}_{32/128}$ and $F^{(L,e)}_{64/384}$ (as described detail in part 2). The elements used in this algorithm are basically synthesized from the minnimum controlled element $F_{2/2}$, so it helps to improve mainly the sandard cipher of algorithms. Using SDDOs contructed as above allows to decrease the encrytion loops of the algorithm, but it also ensures the high durability of the Cipher. Concurently , italso ensures to decrease the complex in device when implementing on FPGA with the pipelining architecture and improves speed encryption when implementing on FPGA with the Iterative Looping.

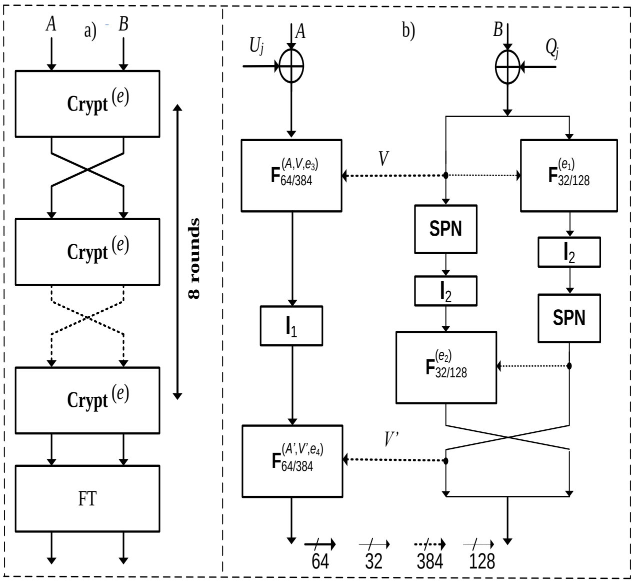

Fig 8.The diagram of the algorithm BMD-128.
General diagram (a); A basic round Cipher unit (b).

The subkeys $K_i \in \{0,1\}^{64}$ are constructed from the sceret key K including 256 bits $K = (K_1, K_2, K_3, K_4)$. The round key U_j, Q_j are selected from the subkeys K_i and listed in table II. Here, we don't used the complext transformation generating subkeys, aiming to minimise device and speed up when implementing on hardware, but it also ensures the security (see VI for more detail) of the cipher owing to special point of the switchable controlled operators which are used the algorithm to generate the data dependent controlling with $F^{(L,e)}_{32/128}$ and $F^{(L,e)}_{64/384}$. The switchable bits e_1, e_2, e_3 and e_4 depend on bit e ($e \in \{0,1\}$). Defining encryption (e=0) and decryption (e=1) mode and e_i is determined as follows:

$$e_1 = e \oplus e'_1,\ e_2 = e \oplus e'_2, e_3 = e \oplus e'_3, e_4 = e \oplus e'_4,$$

where e'_1, e'_2, e'_3 and e'_4 are described in table II.

The whole Cipher BMD-128 is briefted as follows:

1. For $j = 1$ to 7 do: $\{(L, R) \leftarrow$ **Crypt**$^{(e)}(L, R, U_j, Q_j)$; $(L, R) \leftarrow (L, R)\}$.
2. $(L, R) \leftarrow$ **Crypt**$^{(e)}(L, R, U_8, Q_{10})$.
3. $(L, R) \leftarrow (L \oplus U_9, R \oplus Q_9)$.

The final transformation (FT) is perpormed by implementing the operation XOR on left or right halfes data block with the round key corresponding to its selection. This algorithm enables the encryption and decryption processes to be used the same algorithm. Besides, it is shown that the encryption and decryption processes use the same key scheduling and transformation encryption and decryption mode only needing transformation of the controlling bit. This helps to reduce significantly the lost of hardware implementation.

TABLE II. THE KEY SCHEDULING AND LISTS THE SWITCH BITS IN BMD-128

j =	1	2	3	4	5	6	7	8	FT
Q =	K_1	K_3	K_1	K_2	K_3	K_4	K_3	K_4	K_1
U_j =	K_2	K_4	K_3	K_4	K_3	K_2	K_1	K_3	K_2
e'_1 =	1	0	1	1	0	1	0	0	-
e'_2 =	0	0	1	0	1	1	0	1	-
e'_3=	0	0	0	1	0	1	1	0	-
e'_4 =	0	1	1	0	1	0	0	0	-

IV. Security Estimations of the Algorithm BMD-128 According to Criteria NESSIE.

According to criteria of NESSIE [7], we have carried out to evaluate the statistical characteristics of the Cipher BMD-128, which also denotes that it is suitable with the criterias that NESSIE has given. We evaluated with the number of samples being 40.000 and carried out in 2 directions:

a) keeping keys and only changing data (#K=1;#X=40000);
b) keeping data and changing key (#K=40000;#X=1).

The evaluated testing results in to 2 directions above are represented in table IV (see part appendix). Based on the standard of NESSIE, the algorithm can meet a demand of this standard when $d_1 \approx 64$, d_c=1, $d_a \approx 1$, $d_{sa} \approx 1$.

From the testing results, the paper shows that the algorithm BMD-128 can satisfy the 4 criterias of NESSIE about the influence of the original data bits clear text, as the same as the influence of key bits. The research results of the statistical charateristics about the influence of key bits for this algorithm are very important because it used very simple key schedules, but it ensured the statistical properties in term of the standard of NESSIE.

V. Differential characteristics of BMD–128

To evaluate the reliability of cipher before the different attacks of the cryptanalysis is one of the important and necessary requirement. With block cipher, most effective cryptanalysis solution is the differential cryptanalysis method. It means that the probability *p* through the transformations of the ciphering diagram.

As you know, the differential characteristics of expanded controlling operations will depend on the building architecture, the distribution of controlling bit and the differential characteristics of the minimum controlled element used in that structure.

Firstly we should consider the mechanism creating avalanche effect or the differential characteristics of operations used in algorithm. For SPN, figure 6 shows that when changing any bit input of SPN blocks, it can transform the output less than 4 bits. For $F_{2/2}$ element, the differential characteristics is described in table I. Then the differential characteristics of expanded element from $F_{2/2}$ used in this algorithm will be studied.

Assume, input block X with one active bit, then the probability happening in case of output which has one active bit passing through $F^{(e3)}_{64/384}$ (or $F^{(e4)}_{64/384}$ and $F^{(e1)}_{32/128}$ (or $F^{(e2)}_{32/128}$)) with zero active bit of the controlling vector as follows:

$$\Pr(\Delta^{X}_{1} \xrightarrow{F_{64/384}} \Delta^{Y}_{1}) = (\Pr(ijk))^{6} = 0.75^{6} \approx 2^{-2.5},$$
$$\Pr(\Delta^{X}_{1} \xrightarrow{F_{32/128}} \Delta^{Y}_{1}) = (\Pr(ijk))^{4} = 0.75^{4} \approx 2^{-1.5}.$$

Where Pr(*ijk*)=Pr(110)=0.75 (see table I). Besides, because of data block X when passing through the extention block E (in Figure 8), which is repeated 12 times, when passing through the extention block *E*' which is repeated 4 times, active bit in data block X will generate the output of the extention block *E* being 12 active bit, and the output of the extion block *E*' being 4 active bits. Therefore, the input data block X has zero active bit, where the probability happening in case of the output without the active bits when passing through $F^{(e3)}_{64/384}$ (or $F^{(e4)}_{64/384}$) and $F^{(e1)}_{32/128}$ (or $F^{(e2)}_{32/128}$) when having an active bit in the controlling vector equals to:

$$\Pr(\Delta^{X}_{0} \xrightarrow{F_{64/384}} \Delta^{Y}_{0}) = (\Pr(ijk))^{12} = 2^{-24},$$
$$\Pr(\Delta^{X}_{0} \xrightarrow{F_{32/128}} \Delta^{Y}_{0}) = (\Pr(ijk))^{4} = 2^{-8},$$

where, Pr(*ijk*)=Pr(001)=1/4 (see table I). When having *k*, *k*<5, the active bits belonging to random type of the data block X for have $F^{(e3)}_{64/384}$ / (or $F^{(e4)}_{64/384}$) and $F^{(e1)}_{32/128}$ (or $F^{(e2)}_{32/128}$) the probabilities as follows:

$$\Pr(\Delta^{X}_{0} \xrightarrow{F_{64/384}} \Delta^{Y}_{0}) \approx (\Pr(ijk))^{12k} = 2^{-24k}.$$
$$\Pr(\Delta^{X}_{0} \xrightarrow{F_{32/128}} \Delta^{Y}_{0}) \approx (\Pr(ijk))^{4k} = 2^{-8k}.$$

The study shows that when having 2 active bits at input of the controlling vector $F_{2/2}$, the probability of Pr(*ijk*)=Pr(002)=1/8 (see table I). The output of the extention block *E* has 12 active bits and the output of the extention block *E*' is 4 active bits. The maximum value of the probability $\Pr(\Delta^{X}_{0}\rightarrow\Delta^{Y}_{0})$ is used to compare in the case of small probability when *tk* active bits of the controlling vector falling down the controlling *t/2k* of the Elements $F_{2/2}$, *t=2k* or *t=4k*. In case of this, we have the probability:

$$\Pr(\Delta^{X}_{0} \xrightarrow{F_{64/384}} \Delta^{Y}_{0}) = (\Pr(002))^{-6k} \approx 2^{-18k}.$$
$$\Pr(\Delta^{X}_{0} \xrightarrow{F_{32/128}} \Delta^{Y}_{0}) = (\Pr(002))^{-2k} \approx 2^{-6k}.$$

Thus, the controlling elements appeared above are the main part to create avalanche effect in this cryptographic algorithm. Concurrently, on the basic of the differential analysis above, the paper studies and calatates the two – round differential trace of BMD-128 in 2 cases (see figure 9, 10 part appendix) and collects the probability results of the existence of differential trace through two–round transformation being $p = 2^{-45.5}$ (figure 9) and p=$2^{-51.5}$ (figure 10 - see part appendix).

Combining with the analysic and the calculation above, the differential traces of the algorithm are carried out to evaluate via testing program on software. In this program, to reduce the numbers of calculation and exist the generality 2 cases are considered:

a) The samples given encryption only appear 2 active bits which go into the primarity at the left data halres *L* and appear at the output of the left halres *L*.
b) The samples given to encryption only appear 2 active bits which go into the primarily at the right data halres *R* and appear at the output of the right halres *L*.

With weight *w*=2, at the output of the algorithm after two-rounds of encryption has been calculated and the results were nearly equivalent $p \approx 2^{-54}$

Therefore, with both two methods given above, the following conclusions can show that after 4–round transformation, the cipher BMD–128 has excess capacity against differential cryptanalysic. However, the authors also has 4–round is order to increase the reliability of avoid the other cryptanalysis.

TABLE III. THE BEST DIFFERENTIAL CHARACTERISTICS OF BMD-128

Cipher	*Rmax*	Differential charactenstics		P(r)
		min	P(2)	
COBRA-H64	8	(0, Δ_1^R)	P(2) ≈ $1.13.2^{-19}$	≈ 2^{-75}
COBRA-H128	10	(0, Δ_1^R)	P(2) ≈ $1.25.2^{-29}$	≈ 2^{-144}
SG-128	10	(0, Δ_1^R)	P(2) ≈ 2^{-32}	≈ 2^{-160}
SS-128	10	(0, Δ_1^R)	P(2) ≈ 2^{-34}	≈ 2^{-170}
DDO-64	6	(0, Δ_1^R)	P(2) ≈ 2^{-29}	≈ 2^{-87}
Eagle-128	10	(0, Δ_2^R)	P(2) ≈ 2^{-35}	≈ 2^{-175}
BMD-128	8	(0, Δ_2^R)	P(2) ≈ $2^{\mathbf{-51.5}}$	≈ $2^{\mathbf{-206}}$

(*R*max: the maximum number of rounds)

In order to have more information for conclusion about the ability against differential cryptanalysis of the cipher BMD–128, the compared table about the differential cryptanalysis of some cipher (see table III). Through the compared table, the study show that the cipher BMD–128 has the ability against differential cryptanalysis best which is homogenised with BMD-128 which has a better security.

VI. FPGA SYNTHESIS RESULT AND COMPARISIONS

The study is carried out to do test which simulates the cipher BMD–128 on FPGA and compare and evaluate its performance with the other famous algorithms such as CIKS-128H, Rijndael, Serpent, RC6, Twofish, Cobra-H128, IDEA, AES. To ensure the objectivity, the study is also concurrently performed on chips FPGA Xilinx Virtex Device v200pq240. The results in detail are described in table V.

The results above shows that the algorithm BMD–128 has higher speed, but has smaller hardware requirement than the modern famous algorithms. Comparing the performance: speed/cost or speed/(cost * frequence) shows that BMD–128 has higher and higher performance than the famous algorithms.

TABLE IV. COMPARING THE IMPLEMENTATION RESULTS OF ALGORITHMS ON CHIPS FPGA XILINX VIRTEX DEVICE V200PQ240

Cipher	Block size	*Rmax*	*N*	Area (CLBs)	F (MHz)	Throughput (Mbps)	Performance	
							Mbps/#CLBs	Mbps/(#CLBs*GHz)
BMD-128	128	8	1	1006	89	1424	1.42	15.9
CIKS-128H [9]	128	8	1	1,511	65	992	0.66	10.2
Rijndael [10]	128	10	1	2,358	22	259	0.11	5.0
Serpent [11]	128	32	8	7,964	13.9	444	0.056	4.0
RC6 [11]	128	20	1	2,638	13.8	88.5	0.034	2.4
Twofish [11]	128	16	1	2,666	13	104	0.039	3.0
Cobra-H128 [3]	128	12	1	2364	86	917	0.39	4.51
IDEA [3]	128		1	2878	150	600	0.21	1.39
AES [3]	128	8	1	2358	22	259	0.11	4.99

VII. CONCLUSION

This paper proves the efficiency of using SDDOs which is constructed on the basic of CSPN_s in constructing the block cipher BMD–128, aim at implementing on the platform of FPGA technology. The evaluation of performance, statistical analysis and differential analysis show the high applicability of our algorithm in fast and highly efficient telecommumcation system.

REFERENCES

[1] Albirt A. J., Yip W., Ghetwynd B., Paar C. FPGA Implementation and Performance Evaluation of the AES Block Cipher CandidateAlgorithm Finalists // 3rd Advanced Encryption Standard Conference Proceedings. April 13-14, 2000. New York, NY, USA.

[2] Daemen J., Rijmen V. The design of Rijndael. AES – the Advanced Encryption Standard. – Berlin. Springer-Verlag. 2002. – 180 p.

[3] E. Biham, New types of cryptanalytic attacks using related keys, Journal of Cryptology, no.4, pp.229–246, 1994. An earlier version appeared in the proceedings of Eurocrypt'93, LNCS765.

[4] Ichikawa T., Kasuya T., Matsui M. Hardware Evaluation of the AES Finalists // Proc. 3rd Advanced Encryption Standard (AES) Candidate Conference, New York, April 13-14, 2000.

[5] J. Kelsey, B. Schneier, and D. Wagner, Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES, in Advances in Cryptology–CRYPTO'96 (N.Koblitz, ed.), vol.1109 of Lecture Notes in ComputerScience, pp. 237–251, Springer-Verlag, 1996.

[6] J. Kelsey, B. Schneier, and D. Wagner, Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA, in International Conference on Information and Communications Security, ICICS 97 (Y.Han, T.Okamoto, and S.Qing, eds.), vol.1334 of Lecture Notes in Computer Science, Springer-Verlag, 1997.

[7] L. R. Knudsen, Cryptanalysis of LOKI91, in Advances in Cryptology ASIACRYPT'92 (J.Seberry and Y.Zheng, eds.), vol.718 of Lecture Notes in Computer Science, pp. 22–35, Springer-Verlag, 1993.

[8] Minh N.H., Duy H.N., Dung L.H. Design and Estimate of a New Fast Block Cipher for Wireless Communications Devices // The 2008 International Conference on Advanced Technologies for Communications (ATC'08) and REV'08, Ha Noi, PP. 409-412 (2008).

[9] Moldovyan N.A., Moldovyan A.A., Eremeev M.A., Sklavos N. New class of Cryptographic Primitives and Cipher Design for Network Security // International Journal of Network Security. 2006. vol. 2, no. 2. P.114-125. (http://ijns.femto.com.tw).

[10] Moldovyan N.A., Moldovyan A.A. Data-driven Ciphers for Fast Telecommunication Systems. – Auerbach Publications. Talor & Francis Group. New York, London. 2008, 77p – 185 p.

[11] Moldovyan N.A.On cipher design based on switchable controlled operations // Proceedings of the International workshop, Methods, Models, and Architectures for Network Security / Lecture Notes in Computer Science. Berlin. Springer-Verlag. 2003. Vol. 2776.P. 316-327.

[12] Moldovyan N.A. On Cipher Design Based on Switchable Controlled Operations// International Journal of Network Security, Vol.7, No.3, PP.404–415, Nov. 2008.

[13] Nguyen Hieu Minh, Do Thi Bac, Ho Ngoc Duy. New SDDO-Based Block Cipher for Wireless Sensor Network Security // International Journal of Computer Science and Network Security, VOL.10 No.3, March 2010 PP. 54 – 60.

[14] Preneel B., Bosselaers A., Rijmen V., Van Rompay B., Granboulan L., Stern J., Murphy S., Dichtl M., Serf P., Biham., Dunkelman O., Furman V., Koeune F., Piret G., Qiusquater J-J., Knudsen L., Radum H. Comments by the NESSIE Project on the AES Finalists, 24 may 2000.

[15] Sklavos N., Moldovyan N.A., Koufopavlou O. A New DDP-Based Cipher CIKS-128h: Architecture, Design and VLSI Implementation Optimization of CBC Encryption and Hashing up to 1 Gbps // 46th IEEE Midwest Symposium on Circuite and Systems. Cairo, Egypt, December 27-30, 2003.

Do Thi Bac, born in 1970. Lecturer in University of Information and Communication Technology, Thai Nguyen, Viet Nam. Her research interests include cryptography, communication and network security.

Nguyen Hieu Minh is a Lecturer with the Le Qui Don Technical University (Ha Noi, Viet Nam). His research interests include cryptography, communication and network security. He has authored or co-authored more than 30 scientific articles, books chapters, reports and patents, in the areas of his research. He received his Ph.D. from the Saint Petersburg Electrical Engineering University (2006). Contact him at: hieuminhmta@ymail.com.

Ho Ngoc Duy is a Lecturer with the Le Qui Don Technical University (Ha Noi, Viet Nam). His research interests include cryptography, communication and network security. He has authored or co-authored more than 20 scientific articles, books chapters, reports and patents, in the areas of his research. He received his Ph.D. from the Saint Petersburg Electrical Engineering University (2012).

APPENDIX

TABLE V. INFLUENCE OF THE ORIGINAL TEXTS AND KEY BIT

Number of rounds	#X=40000; #K=1				#X=1; #K=40000			
	d_1	d_c	d_a	d_{sa}	d_1	d_c	d_a	d_{sa}
1	32.833	0.750	0.5130	0.5128	16.926	0.379	0.2644	0.2565
2	63.493	1.000	0.9920	0.9894	48.324	0.875	0.7550	0.7509
3	63.999	1.000	0.9998	0.9961	63.752	1.000	0.9958	0.9927
4	64.002	1.000	0.9997	0.9961	63.998	1.000	0.9998	0.9960
5	63.998	1.000	0.9998	0.9960	63.999	1.000	0.9997	0.9961
6	63.999	1.000	0.9998	0.9961	64.002	1.000	0.9998	0.9961
7	64.000	1.000	0.9998	0.9961	63.998	1.000	0.9997	0.9961
8	64.000	1.000	0.9998	0.9961	64.001	1.000	0.9998	0.9960

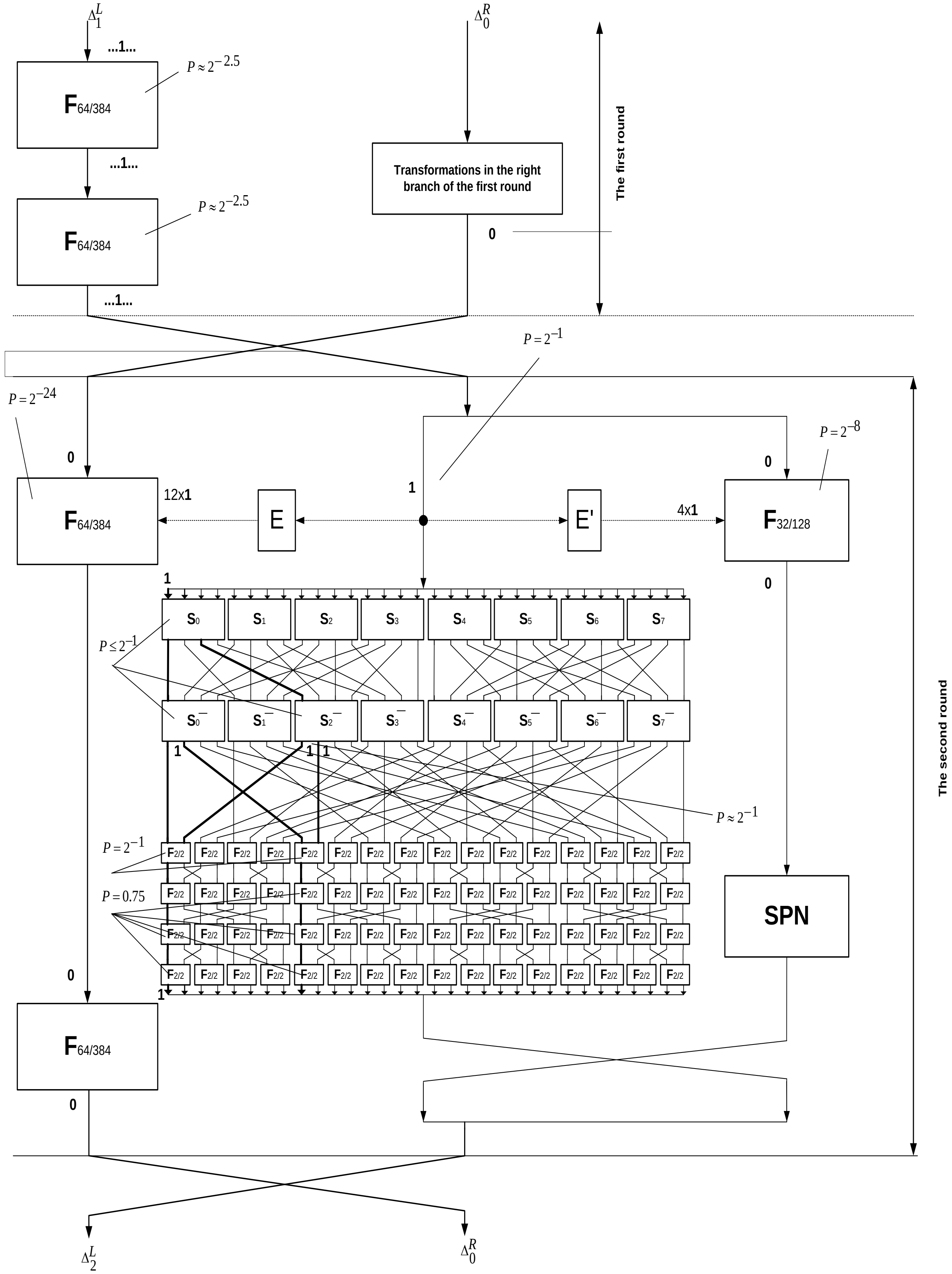

Fig 9.Formation of the two-round iterative differential characteristic with the difference ($\Delta^L{}_1$, $\Delta^R{}_0$)→($\Delta^L{}_2$, Δ_{R0})) with probability Pr(2)≈$2^{-45.5}$

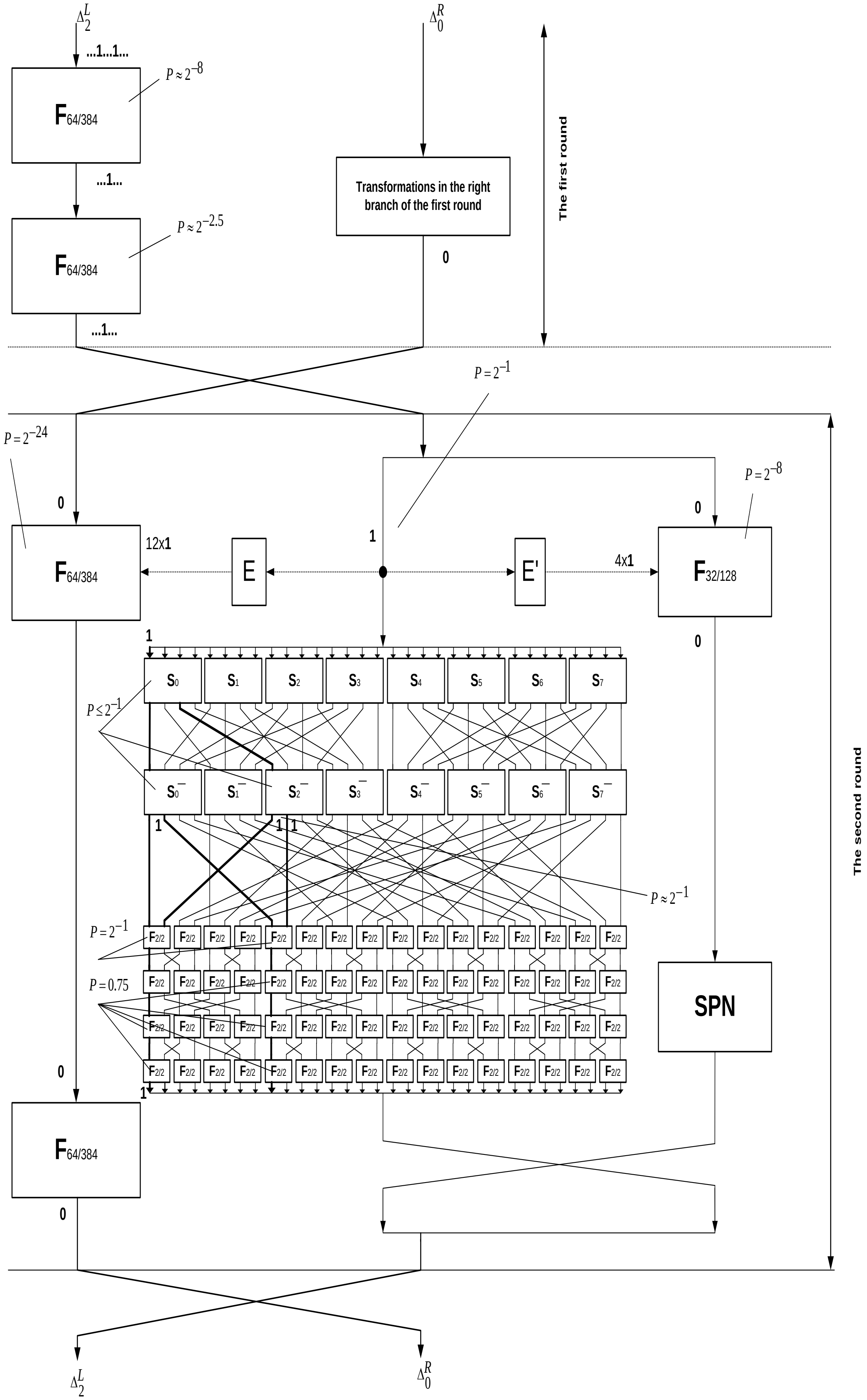

Fig 10.Formation of the two-round iterative differential characteristic with the difference (Δ^L_2, Δ^R_0)→ (Δ^L_2, Δ^R_0) with probability Pr(2)≈ $2^{-51.5}$