Design and Estimate of a New Fast Block Cipher for Wireless Communication Devices

Nguyen H. Minh
Le Qui Don Technical University
Ha Noi, Viet Nam
Email: minhnh@mail.ru

Ho N. Duy
Saint Petersburg State Electrotechnical University
St. Petersburg, Russia

Luu H. Dung
Le Qui Don Technical University
Ha Noi, Viet Nam

***Abstract* – This paper presents the problem of using the controlled substitution-permutation networks (CSPNs) based on controlled elements (CEs) for designing fast block ciphers suitable to cheap hardware implementation. By studying the properties of the CSPNs of different types CEs, we select a suitable CE and CSPN for propose algorithm and design of a new fast block cipher XO-64. Security estimations of XO-64 cipher with NEISSE criteria and differential cryptanalysis show that proposed cipher is high-level security. The synthesis results for hardware implementation (FPGA) prove that XO-64 is very efficient new cipher, especially for wireless devices.**

***Keywords* – Block cipher, data-dependent operations, hardware implementation.**

I. INTRODUCTION

Significant interest of modern applied cryptography lies in the field of research and use of cryptographic primitive for designing block ciphers. Cryptographic algorithms are meant to provide secure communications applications. However, if the system is not designed property, it may fail. Although there are many well know ciphers, with different specifications and characteristics, the security of them is under consideration.

In practice, wireless devices are resource-poor relative to wire devices and they rely on finite energy sources, limited channel bandwidth, and limited computational capabilities. These defects affect implementing security solutions. Optimizations of the existing security standards as well as novel designs are proved issues of major importance in order the high needs for security to be satisfied.

In this paper, we present a minimum size primitive using the controlled element (CE) with two-bit input as standard building block to design Data-Dependent operations (DDOs). It is efficient to design controlled substitution-permutation networks (CSPNs) [1, 2].

More specifically, first we show the general topology of the CSPNs. Besides that form of representation of the CE are considered. Then, study properties of the CSPN of different types of the CEs $\mathbf{F}_{2/1}$ to select a suitable CE $\mathbf{F}_{2/1}$ and CSPN.

Furthermore, a new crypto-scheme, XO-64 is proposed, based on efficient use of the CSPN and SPN. Its use very simple key scheduling that defines high performance, especially in the case of frequent key refreshing. The introduced crypto-scheme has been implemented in an FPGA device; results for FPGA implementation prove that new cipher XO-64 is effective, especially for wireless devices.

The paper is organized in the following way. In section 2, we consider minimum size CEs $\mathbf{F}_{2/1}$ and controlled substitution-permutation networks as variable operations. We present the design criteria and study properties of the CSPN of types of CE $\mathbf{F}_{2/1}$. Section 3 describes the structure of the new block cipher: eight-round XO-64 with 64-bit data input. Section 4 presents results on security estimation with NEISSE criteria and differential cryptanalysis. Section 5 presents the hardware implementation (FPGA) and comparisons of the proposed cipher with other block ciphers. Finally, conclusion is discussed.

II. MINIMUM SIZE CE $F_{2/1}$ AND CONTROLLED SUBSTITUTION-PERMUTATION NETWORKS AS VARIABLE OPERATIONS

The controlled operations are implemented as uniform CSPNs constructed using the minimum size CEs as standard building blocks (Figure 1a show general topology of CSPN). Let CSPN with n-bit input and n-bit output be controlled with m-bit vector v. Then we shall denote such CSPN as controlled operation $\mathbf{F}_{n/m}$. Selecting a set of the fixed permutations connecting active layers, we define some particular topology of controlled operation. Each active layer represents $n/2$ parallel CEs. A minimum size CE is denoted as the $\mathbf{F}_{2/1}$ box. It transforms two-bit input vector (x_1, x_2) into two-bit output (y_1, y_2) depending on a controlling bit v.

A CE can be represented as a pair of the 2×2 substitutions (elementary S-boxes) selected depending on bit v (Figure 1b) with substitution S_1 (if $v = 0$) and S_2 (if $v = 1$) on two-bit vectors. Such substitutions are denoted as $\mathbf{F}^{(0)}{}_{2/1}$ and $\mathbf{F}^{(1)}{}_{2/1}$ and CE implements the transformation $(y_1, y_2) = \mathbf{F}^{(v)}{}_{2/1}(x_1, x_2)$.

The $\mathbf{F}_{2/1}$ element can be also represented with a pair of BFs in three variables (Figure 1c): $y_1 = f_1(x_1, x_2, v)$; $y_2 = f_2(x_1, x_2, v)$. If the substitution $\mathbf{F}^{(0)}{}_{2/1}$ is described with two BFs $y'_1 = f'_1(x_1, x_2)$ and $y'_2 = f'_2(x_1, x_2)$, $\mathbf{F}^{(1)}{}_{2/1}$ is described with two BFs $y''_1 = f''_1(x_1, x_2)$ and $y''_2 = f''_2(x_1, x_2)$, then CE $\mathbf{F}^{(v)}{}_{2/1}$ is described with two BFs in three variables x_1, x_2, and v:

$$y_1 = (v \oplus 1) f'_1(x_1, x_2) \oplus v f''_1(x_1, x_2) = v(y'_1 \oplus y''_1) \oplus y'_1,$$
$$y_2 = (v \oplus 1) f'_2(x_1, x_2) \oplus v f''_2(x_1, x_2) = v(y'_2 \oplus y''_2) \oplus y'_2.$$

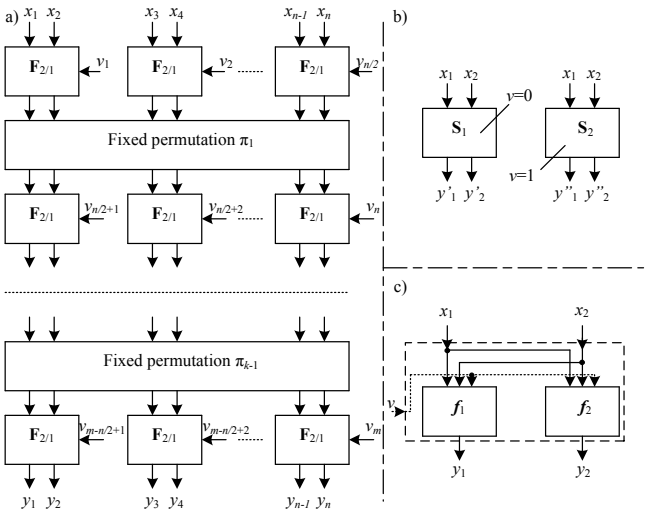

Figure 1. a) General structure of the $\mathbf{F}_{n/m}$ boxes, b) representation of the $\mathbf{F}_{2/1}$ as two 2×2 substitutions, c) or as a pair of BFs in three variables.

The selection of CEs $\mathbf{F}_{2/1}$ suitable to design efficient cryptographic DDO is based on the following criteria:

1. Each of two outputs of CEs should be a non-linear BF having maximum possible non-linearity NL (non-linearity in the sense of the distance of non-linear BF from set of affine BFs) for balanced BFs.
2. Each modification of CEs should be bijective transformation $(x_1, x_2) \rightarrow (y_1, y_2)$.
3. Each modification of CEs should be involution.
4. The linear combination of two outputs of CEs, i.e. $f = y_1 \oplus y_2$, should have maximum possible non-linearity NL for balanced BFs.

Trying all possible variants of the $\mathbf{F}_{2/1}$ elements we have established that there exist 24 different CEs $\mathbf{F}_{2/1}$ satisfying criteria 1-4. They implement only modifications shown in figure 2.

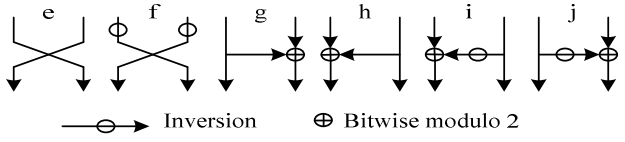

Figure 2. The 2×2 substitutions implemented by nonlinear controlled involutions.

Types of the CSPNs constructed using CEs $\mathbf{F}_{2/1}$ can be applied as DDOs suitable to designing fast hardware-oriented ciphers. For FPGA implementation, that has gained highly significant practical importance, all types of the CEs $\mathbf{F}_{2/1}$ are implemented using two 4-bit cells (Figure 1c), each implementing a Boolean Function (BF) with three variables. Advance of the DDO-based ciphers design, is to select and use non-linear CE with maximum non-linearity.

In [1] has show that with CEs $\mathbf{F}_{2/1}$ are divided into four subclasses $\{\mathbf{S}_{2/1}\}$, $\{\mathbf{R}_{2/1}\}$, $\{\mathbf{Z}_{2/1}\}$ and $\{\mathbf{L}_{2/1}\}$. The most interesting subclasses of CEs – namely $\{\mathbf{R}_{2/1}\}$ and $\{\mathbf{S}_{2/1}\}$ – for each specific type of CE also include its inverse element, it is meaning that $\mathbf{S}^{-1}_{2/1} = \mathbf{S}_{2/1}$ and $\mathbf{R}^{-1}_{2/1} = \mathbf{R}_{2/1}$. The subclasses $\mathbf{Z}_{2/1}$ and $\mathbf{L}_{2/1}$ be without such property, but $\mathbf{L}^{-1}_{2/1} = \mathbf{Z}_{2/1}$ and $\mathbf{Z}^{-1}_{2/1} = \mathbf{L}_{2/1}$.

When designing controlled operational blocks $\mathbf{F}_{n/m}$ for cryptographic applications, the order of controlled operations is interested specially. The controlled operations $\mathbf{F}_{n/m}$ based on $\mathbf{F}_{2/1}$, required of design such that reach to the expected order.

In this paper, block $\mathbf{F}_{32/80}$ will be chosen as this block satisfies all the requirements for avalanche effect in proposed algorithm (proven in section 4) and it has the simplest structure so it will be perfectly suitable for constructing high performance algorithm.

The results of the study of avalanche effect of different types CEs $\mathbf{F}_{2/1}$ used in controlled operational block $\mathbf{F}_{32/80}$ show that element types of **S** and **L** are with the best avalanche effect. However, the element **L** does not have the reversibility property as mentioned above, thus in designing **XO-64** algorithm the element $\mathbf{S}_{2/1}$ will be selected.

III. Design of the XO-64 Cipher

Our design criteria are the following:

1. The encryption algorithm should be an iterated 64-bit block cipher.
2. The cipher should be fast, in the case of frequent key refreshing. Therefore, the encryption algorithm should be able to perform encryption and decryption with simple and fast change of the used subkeys sequence.

Design of the operational boxes $\mathbf{F}_{n/m}$ ($\mathrm{S}_{n/m}$) includes the following two items: (1) selection of the fixed permutations between active layers and (2) selection of the types of active layers.

Initially, we construct the boxes $\mathbf{F}_{32/80}$ (Figure 3) and $\mathbf{F}^{-1}_{32/80}$ that are mutual inverses (the box $\mathbf{F}^{-1}_{32/80}$ is constructed inverse with box $\mathbf{F}_{32/80}$). The $\mathbf{F}_{32/80}$ and $\mathbf{F}^{-1}_{32/80}$ boxes are constructed using the CEs as standard building blocks in correspondence with topology described in figure 1a.

We assume that controlling vector V contains s components, where $s = 5$ is the number of the layers in the $\mathbf{F}_{32/80}$ box, i.e. $V = (v_1, v_2, v_3, v_4, v_5)$.

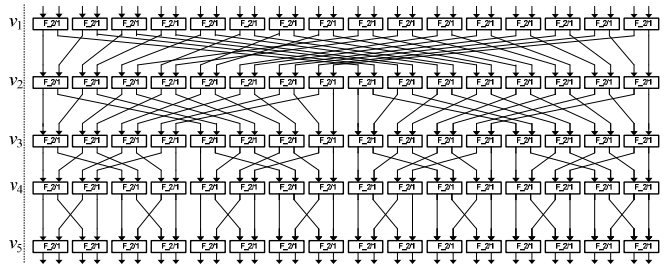

Figure 3. Structure of the $\mathbf{F}_{32/80}$ box.

Then, construct structure of the $\mathbf{S}_i$ box is involution substitution-permutation network (Figure 4). It is a SPN constructed using the P_1, P_2, and P_3 permutations (specified in table 1) and the following 4×4 S-box substitutions: direct ones S_0,..., S_7 and inverses S_0^{-1},..., S_7^{-1} boxes. Eight 4×4 S-boxes of the DES cipher (one from each of eight 6×4 S-boxes) have

been selected as the $S_0,\ldots, S_7$ boxes of XO-64 in order to inspire a high level of public confidence that no trapdoor are inserted in XO-64. Similar justification of the S-boxes selection has been earlier used in the design of the Serpent cipher [3].

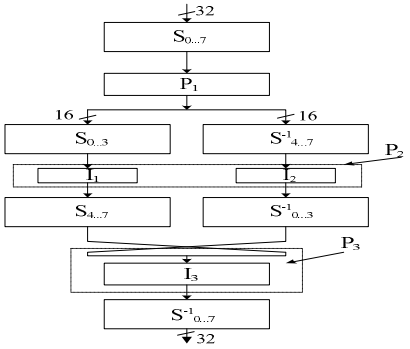

Figure 4. Structure of the $\mathbf{S}_i$ box.

TABLE I. THE FIXED PERMUTATIONS P_1, P_2 AND P_3 ARE THE FOLLOWING:

P_3	(1)(2,5)(3,17)(4,21)(6)(7,18)(8,22)(9)(10,13)(11,25)(12,29)(14)(15,26)(16,30)(19)(20,23)(24)(27)(28,31)(32)
P_2	(1)(2,5)(3,9)(4,13)(6)(7,10)(8,14)(11)(12,15)(16)(17)(18,21)(19,25)(20,29)(22)(23,26)(24,30)(27)(28,31)(32)
P_1	(1,3,19,17)(2,7,20,21)(4,23,18,5)(6,8,24,22)(11,27,25,9)(10,15,28,29)(12,31,26,13)(14,16,32,30)

Figure 5 presents new 64-bit cipher XO-64, particular feature of which is the combining SPNs ($\mathbf{S}_i$ operation performed on the left data subblock) with CSPNs (two boxes $\mathbf{F}_{32/80}$ and $\mathbf{F}^{-1}_{32/80}$ in the right branch of the round crypto-scheme).

In order to symmetries the full ciphering procedure we use very simple final transformation (FT) that is XORing two subkey with data subblocks. Due to FT in XO-64 the same algorithm performs both the encryption and the decryption, while different key scheduling is used.

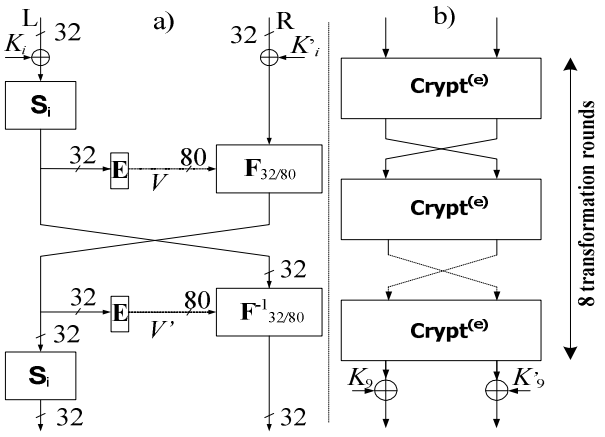

Figure 5. a) Round transformation Crypt in XO-64, b) and general structure of the XO-64.

The 80-bit controlling vectors V and V' corresponding to the $\mathbf{F}_{32/80}$ and $\mathbf{F}^{-1}_{32/80}$ boxes is formed with the extension box $\mathbf{E}$ described as follows:

$$\mathbf{E}(X) = V = (v_1, v_2, v_3, v_4, v_5);$$

$$v_1 = (x_0, \ldots, x_{15});\ v_2 = (x_{16}, \ldots, x_{31});\ v_3 = (x_5, \ldots, x_{20}),$$

$$v_4 = (x_{21}, \ldots, x_{31}, x_0, \ldots, x_4);\ v_5 = (x_{10}, \ldots, x_{25}).$$

The encryption algorithm is as follows:

1. For $i = 1$ to 7 do: $\{(L, R) \leftarrow \mathrm{Crypt}^{(e)}(L, R, K_i, K'_i);$
   $(L, R) \leftarrow (R, L)\}$.
2. Perform transformation: $\{(L, R) \leftarrow \mathrm{Crypt}^{(e)}(L, R, K_8, K'_8)\}$
3. Perform final transformation:
   $\{(L, R) \leftarrow (L \oplus K_9, R \oplus K'_9);$
   $(L, R) \leftarrow (L, R)\}$.

Subkeys $K_i \in \{0, 1\}^{32}$ of the 128-bit secret key $K = (K_1, K_2, K_3, K_4)$ are used directly in procedure $\mathrm{Crypt}^{(e)}$ ($e = 0$ – encryption and $e = 1$ – decryption) as round keys K_i and K'_i. The key scheduling is described in table 2. Thus, no preprocessing the secret key is used.

TABLE II. THE KEY SCHEDULING IN XO-64 ($J = 9$ CORRESPONDS TO FINAL TRANSFORMATION)

No. rounds j	1	2	3	4	5
Enc K_i/K'_i	K_1/K_2	K_3/K_4	K_3/K_1	K_4/K_1	K_2/K_3
Dec K_i/K'_i	K_1/K_3	K_3/K_4	K_2/K_1	K_4/K_3	K_3/K_2
No. rounds j	6	7	8	9	
Enc K_i/K'_i	K_3/K_4	K_1/K_2	K_4/K_3	K_1/K_3	
Dec K_i/K'_i	K_1/K_4	K_1/K_3	K_4/K_3	K_1/K_2	

IV. RESULTS ON SECURITY ESTIMATION WITH CRITERIA AND DIFFERENTIAL CRYPTANALYSIS

For the purpose to check the diffusion properties of the block algorithm proposed in the paper, we test it according to the method offered by the New European Project NESSIE (New European Schemes for Signatures, Integrity and Encryption). In this method, we examine the properties of the XO-64 cipher with respect to the following four dependence criteria [5, 6]:

1. the average number of output bits changed when changing one input bit – (1);
2. the degree of completeness – (2);
3. the degree of avalanche effect – (3);
4. the degree of strict avalanche criterion – (4).

The results of testing the XO-64 algorithm show in table 3 and 4.

Our research results have shown that two rounds of XO-64 are sufficient to satisfy the test criteria ($d_c = 1$, $d_a \approx 1$, $d_{sa} \approx 1$). Thus, XO-64 possesses good statistical properties like that of AES finalists. Our preliminary security estimation of XO-64 shows that it's two (four) rounds are sufficient to thwart linear (differential) attack.

Figure 6 shows that the probability of the existence of the differential trail after the first round is less than 2^{-17} and after the fourth round the probability of the differential trail is less than 2^{-68} thus 4 rounds is enough to prevent the difference cryptanalysis. In order for the security eight rounds is selected to prevent other types of attacks.

TABLE III. VALUES OF INFLUENCE CRITERIA 1-4 OF THE INCOMING TEXT BITS ON THE TRANSFORMED TEXT (FOR VARIOUS NUMBERS OF ROUNDS)

Number of rounds	#K = 100 #X = 100			
	(1) = d_1	(2) = d_c	(3) = d_a	(4) = d_{sa}
1	23.229096	0.997925	0.722330	0.709357
2	31.973480	1	0.999247	0.991923
3	32.000277	1	0.999363	0.992011
4	31.998552	1	0.999368	0.991986
5	31.996724	1	0.999277	0.992033
6	31.996731	1	0.999265	0.992071
7	31.997396	1	0.999355	0.992045
8	32.000224	1	0.999361	0.992002

TABLE IV. THE VALUES FOR CRITERIA 1-4 ON THE INFLUENCE OF KEY BITS ON THE TRANSFORMED TEXT (FOR VARIOUS NUMBERS OF ROUNDS)

Number of rounds	#K = 100 #X = 100			
	(1) = d_1	(2) = d_c	(3) = d_a	(4) = d_{sa}
1	21.531775	1	0.698621	0.692892
2	31.455716	1	0.990704	0.991161
3	31.969526	1	0.992145	0.992044
4	32.000830	1	0.999266	0.992038
5	32.001145	1	0.999306	0.991986
6	32.001600	1	0.999321	0.991977
7	32.002770	1	0.999280	0.992099
8	31.997309	1	0.999246	0.992016

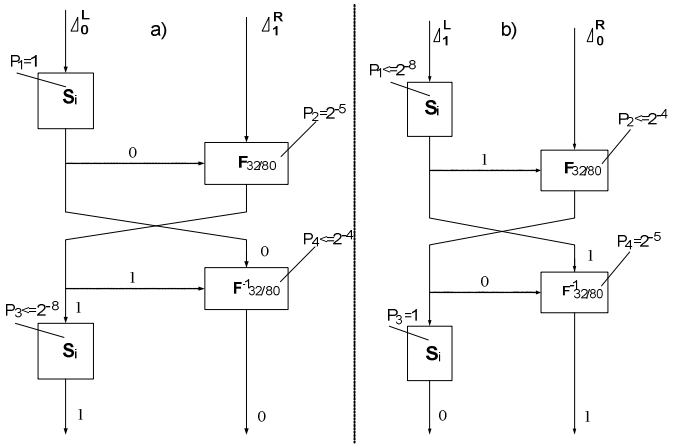

Figure 6. Formation of the one-round difference (Δ_0^L, Δ_1^R) and (Δ_1^L, Δ_0^R) with probability $P(1) < 2^{-16}$

V. HARDWARE IMPLEMETATION

Hardware implementations of proposed cipher are designed and coded in VHDL language. The XO-64 cipher is examined in hardware implementation by using architecture Full Rolling for XILINX FPGA Virtex Device. The used architecture Full Rolling is a typical architecture for secret key block cipher implementation. This architecture operates efficiently for both encryption and decryption process. The synthesis results of the VLSI implementation are illustrated in table 5. In the same table comparisons with the most widely used wireless networks are given (IEEE 802.11 security is based on RC4, AES ciphers; Bluetooth security is based on SAFER+ cipher; The Wireless Transport Layer Security (WTLS) ensure encryption in both Wireless Application Protocol (WAP) and Open Mobile Appliance (OMA). DES, IDEA and RC5 are the alternative ciphers that can be used for bulk encryption in WLTS).

TABLE V. FPGA SYNTHESIS RESULTS AND COMPARISONS

Block ciphers	Block size (bit)	F (Mhz)	Area (CLBs)	Rate (Mbps)
XO-64 (proposed)	64	86	570	690
AES[7]	128	22	2358	259
RC4[6]	-	70	255	5
SAFER+[9]	128	85	4000	320
IDEA[4]	64	150	2878	600
DES[10]	64	125	741	402

The above synthesis results for implementations FPGA prove that the proposed cipher XO-64 achieves higher throughput values and covers lower area resources.

VI. CONCLUSION

In this paper, we propose a new fast cipher XO-64. This cipher is based on DDO transformations. Security analysis has show that the cipher is secure against know attacks. Due to simple of transformation rounds and use very simple key scheduling that makes hardware implementation cheaper and faster in the case of frequent change of keys. The cipher achieve high-speed rate in FPGA devices. The implementation rate and area is compared with the most widely used wireless protocols. These comparisons prove the suitability of the proposed cipher for wireless devices.

REFERENCES

[1] Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004. 448 с.

[2] A. A Moldovyan, N. A Moldovyan, and N. Sklavos, " Controlled elements for designing ciphers suitable to efficient VLSI implementation," in Springer Science + Business Media, pp. 149-163, 2006.

[3] R. Anderson, E. Biham, and L. Knudsen, "Serpent: a proposal for the advanced encryption standard," in 1st Advanced Encryption Standard Candidate Conference Proceedings, Venture, California, Aug. 20-22, 1998.

[4] O. Y. H. Cheung, K. H. Tsoi, P. H. W. Leong, and M. P. Leong, "Tradeoffs in parallel and serial implementations of the international data encryption algorithm," in Proceedings of the 3rd International Workshop Cryptographic Hardware and Embedded Systems – CHES 2001, LNCS 2162, pp. 333-347, Springer-Verlag, 2001.

[5] B. Preneel et al., Performance of Optimized Implementations of the NESSIE Primitives, project IST-1999-12324, 2003. (see pp. 36; http://www.cryptonessie.org).

[6] B. Preneel et al., Comments by the NESSIE project on the AES finalists, May 24, 2000 (http://www.nist.gov/aes).

[7] N. Sklavos et al, "Encryption and data dependent permutations: implementation cost and performance evaluation," in Proceedings of the International Workshop, Methods, Models, and Architectures for Network Security, LCNS 2776, pp. 337-348, Springer-Verlag, 2003.

[8] A. A Moldovyan and N. A Moldovyan, "A cipher based on datadepenndent permutations," Journal of Cryptology 15(1) (2002) 61-72.

[9] M .Portz, "A generalized description of DES-based and benes-based permutation generators," Advances in cryptology, Lecture Notes in Computer Science, Vol. 718 (Springer, 1992), pp. 397-409.

[10] A. Schubert and A. Anheier, "Efficient VLSI implementation of modern symmetric block ciphers," in: Proceedings of ICECS'99, Cyprus (1999).