International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.43-54
http://dx.doi.org/10.14257/ijsia.2013.7.6.05

A High Speed Block Cipher Algorithm

Bac Do Thi[1] and Minh Nguyen Hieu[2]

[1]*University of Information and Communication Technology, Thai Nguyen, Viet Nam*
[2]*Le Qui Don Technical University, Ha Noi, Viet Nam*
dtbac@ictu.edu.vn; hieuminhmta@ymail.com

Abstract

The Block cipher BM–128 which is proved to be suitable to the applications in the wireless communication systems are proposed in this paper. It is developed based on SDDO which is constructed from CSPN. BM-128 also eliminates the weak keys without the complex round key proceduce and meet the requirements of NESSIE. Design shall meet all the security requirements to protect applications against the well-known threats. In addition, BM-128 evaluated to have higher performance than the other algorithms when they are used in cheap hardware.

Keywords: *high–performance, switchable data-dependent operations, controlled substitution permutation network, cheap hardware*

1. Introduction

Nowadays, wireless telecommunication networks play an important role in daily activities of individuals and organizations. The more developed the society is, the higher demand for wireless services so wireless telecommunication keeps growing in order to meet the increasing demand. In wireless networks, the need to access, store and exchange of information especially the sensitive information is increasing rapidly, this leads to the growth of illegal activities. The different forms of infringement could cause severe consequences for individuals and social organizations. In fact, there has been a contradiction between the need to develop wireless application and information security risks.

Cryptography has been employed to secure the information in wireless networks. However, in practice, there is a contradiction between modern encryption methods with technical features of wireless devices. In order to have high quality encryption, expensive specialized devices are needed. As a result, this will limit the popularity of devices. The increased energy (it takes more time to execute complicated algorithms) will lead to the reduced operation time of the device. Moreover, the time delay of coding and decoding will reduce the traffic of information channels and the device performance.

These contradictions can be solved by using new encryption methods. The new methods aim to reduce the complexity and increase the performance of algorithms. If the complexity is reduced, it will result in the cost, energy and active element reduction.

Therefore, it is essential to construct specialized encryption algorithms, which can be employed in individual applications in fast wireless telecommunication networks and achieve high performance in design. This problem has interested many scientists and in research [1-3] the block cipher on the basic of the controlled substitution permutation network (CSPN) has been proposed. Another important element that the modern

ISSN: 1738-9976 IJSIA

encryption algorithms need to achieve is to maintain the high speed even in case of frequent change of secret keys. This can be achieved by not using complex round key procedure [1-3]**.** This solution ensures the high encryption speed and keeps the cost low.

Therefore, in order to offer more options for applications, this paper presents block cipher aiming to be implemented in FPGA, the applications in wireless telecommunication networks which require high performance and speed.

The algorithm is called BM-128, of which BM-128 has the block size of 128 bits. BM-128 is developed on the basis of SDDO based on element $F_{2/2}$ which is very suitable for implementing on cheap hardware. It can be clearly seen in part 4 and part 5 that BM-128 is very suitable and flexible in fast wireless telecommunications networks and in the environment with high frequency of key-reestablishment.

This paper is organized as follows: part 2 we present the structure of data–controlled element used in developing algorithm; part 3 presents the new BM-128 block cipher design; part 4,5,6 presents the recommendations, forecasts and conclusions on issues closely related to the proposed algorithm.

2. The Structure of Controlled Element

The use of Controlled Element (CE) $F_{2/2}$ in place of CE $F_{2/1}$ in constructing Data Dependent Operation (DDO) is highly reasonable, effective and suitable for implementation on FPGAs hardware [3, 6]. For this reason, using the CE will exploit the maximum potential of devices particularly constructing DDOs from $F_{2/2}$, that means it will enlarge the data controlled bits input. This will create the prerequisite conditions for improving non-linear level and increasing avalanche effect of some transformations. These are two most important characteristics of cipher to ensure the security of algorithms.

2.1. Structure of CE $F_{2/2}$ and Selection Criteria for Cryptographic Targets

According to [4], each of minimum CE $F_{2/2}$ can be presented as follows:

- A pair of two 4-variables Boolean Function (BF).
- A pair of the 2x2 substitution, in which each substitution has two-bit input (x_1, x_2). Four substitutions equal a controlling vector with the values: v = (0, 0), (0, 1), (1, 0), (1, 1).

According to [4, 5], in order to construct CSPNs effectively, we need to build criteria in selecting the controlled element $F_{2/2}$. The criteria are:

- Each one of the two outputs of CEs should be a non-linear BF having maximum possible non-linearity (NL) NL = 4 for balanced BFs in four variables;
- Each modification of CEs should be objective transformation $(x_1, x_2) \rightarrow (y_1, y_2)$;
- Each modification of CEs should be involution;
- The linear combination of two outputs of CEs, i.e. $f = y_1 \oplus y_2$, should have maximum possible NL = 4 for balanced BFs in four variables.

The following is some illustration for selecting a pair of 4-CEs satisfying the above criteria in order to be able to apply in designing the cryptographic applications to construct the data controlled operators. Regarding to the representation in 4-variable BF, the elements $F_{2/2}$ will be presented in algebraic equation as follows:

$$y_1 = (v \oplus 1)(z \oplus 1)y_1^{(1)} \oplus z(v \oplus 1)y_1^{(2)} \oplus v(z \oplus 1)y_1^{(3)} \oplus vzy_1^{(4)}$$

$$y_2 = (v \oplus 1)(z \oplus 1)y_2^{(1)} \oplus z(v \oplus 1)y_2^{(2)} \oplus v(z \oplus 1)y_2^{(3)} \oplus vzy_2^{(4)}$$

The output of the controlled elements can also be presented as follows:

$$y_1 = vz\left(y_1^{(1)} \oplus y_1^{(2)} \oplus y_1^{(3)} \oplus y_1^{(4)}\right) \oplus v(y_1^{(1)} \oplus y_1^{(3)} \oplus z\left(y_1^{(1)} \oplus y_1^{(2)}\right) \oplus y_1^{(1)}$$
$$y_2 = vz\left(y_2^{(1)} \oplus y_2^{(2)} \oplus y_2^{(3)} \oplus y_2^{(4)}\right) \oplus v(y_2^{(1)} \oplus y_2^{(3)} \oplus z\left(y_2^{(1)} \oplus y_2^{(2)}\right) \oplus y_2^{(1)}$$

However, 4-variable logic functions have the different non-linear values. The number of non-linear values of 4-variable BF is much greater than those of 3-variable BF.

Also, its differential characteristic is much better than the differential characteristics of element $F_{2/1}$. Consequently, the selection of 4 CEs for $F_{2/2}$ has practical significance and influences the avalanche effect of cipher constructed from that element.

Element $F_{2/2}$ is selected to be used in the proposed algorithm is as follow, this element includes differential characteristics shown in [1].

$y_1 = vzx_1 \oplus vz \oplus vx_1 \oplus vx_2 \oplus v \oplus z \oplus x_1 \oplus 1;$ NL(y_1) = 4.
$y_2 = vzx_2 \oplus vz \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus x_2 \oplus v \oplus z \oplus 1;$ NL(y_2) = 4.
$y_3 = vzx_1 \oplus vzx_2 \oplus zx_1 \oplus x_1 \oplus x_2;$ NL(y_3) = 4.

2.2. Design CSPN and SDDO used in BM-128

The general structure of CSPN was described in detail by Nikolay A. Moldovyan in [4] and is applied to construct the SDDOs operators applied in many algorithms. According to design diagram in [4], we build up controlled elements which will be used in proposal algorithm.

The process of constructing the controlled element $F_{32/256}$ used in algorithm BM-128 is described as follows: $F_{2/2} \rightarrow F_{4/8} \rightarrow F_{32/128} \rightarrow F_{32/256}$. Element $F_{4/8}$ (see Figure 1) is constructed from $F_{2/2}$. Here, $F_{4/8}$ constructed into 4 parts from $F_{2/2}$, is divided into 2 layers, in which each layer consists of 2 elements $F_{2/2}$ in parallel. The middle of 2 layers is a fixed permutation described in Figure 1. In which $F_{32/128}$ (see Figure 2) constructed from 16 controlled elements $F_{4/8}$, is divided into 2 layers, each layer includes 8 elements $F_{4/8}$ in parallel and there is a twisted permutation between 2 layers described as follows:

I = (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)

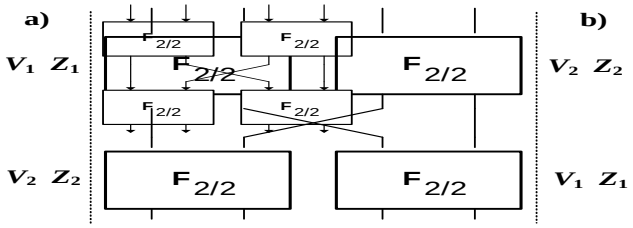

Figure 1. The structure of $F_{4/8}$ (a) and $F_{4/8}^{-1}(b)$

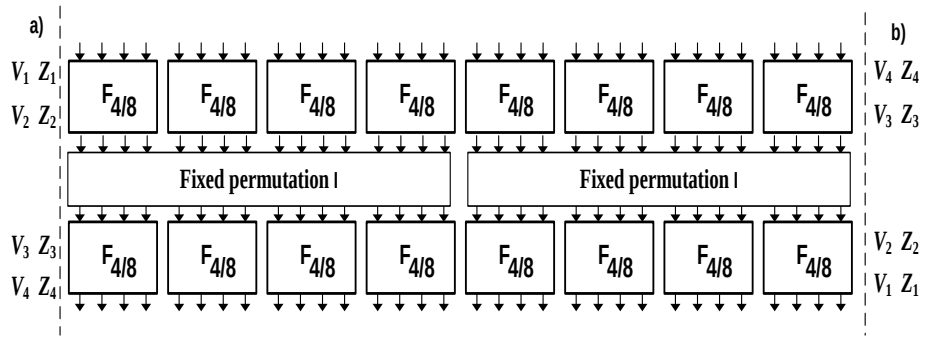

Figure. 2. The Structure of $F_{32/128}$ (a) and $F_{32/128}^{-1}(b)$

Finally, $F_{32/256}$ (see Figure 3) constructed from 2 elements $F_{32/128}$ is also divided into 2 layers and each layer only includes a $F_{32/128}$. The middle of 2 layers is a fixed permutation ***I'*** described as follows:

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

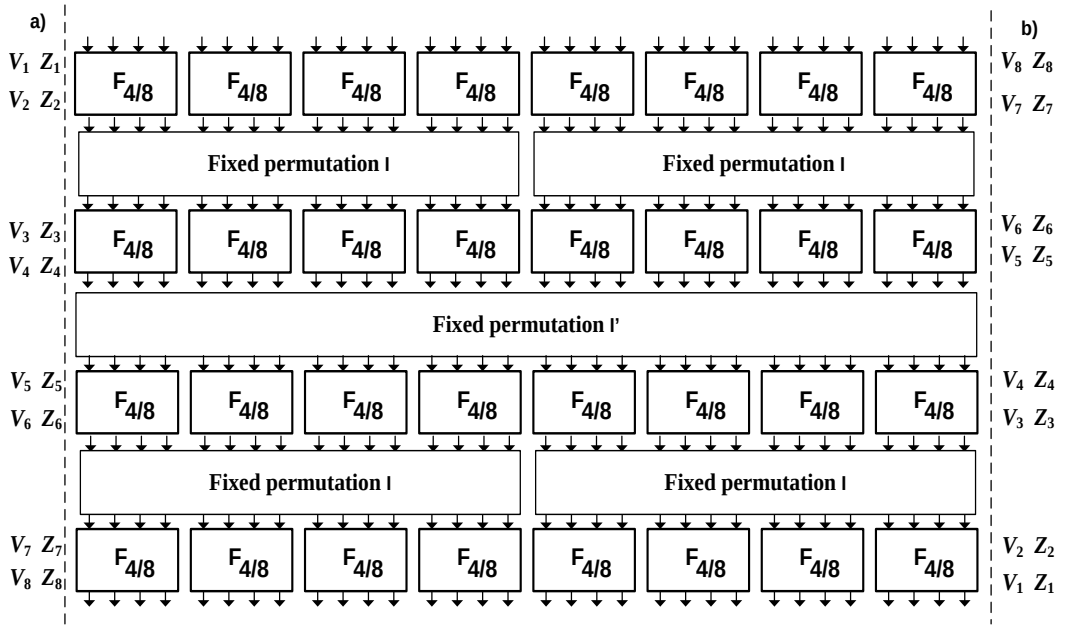

Figure 3. The Structure of $F_{32/256}$ (a) and $F_{32/256}^{-1}$ (b)

With this structure, it is more interesting to build from $F_{2/2}$ which will provide a huge support in generating the high performance cipher.

On the basic of $F_{32/256}$, 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_1, E_2. The detail structure of SDDO $F_{32/256}^{(L,e)}$ is shown in Figure 4.

In Figure 4, to control the distribution of the controlling vector in $F_{32/256}^{(L,e)}$, we use permutations $P_{2/1}$ which are connected parallel. The expansion of bits in E_1 and E_2 is performed as follows: 16 bits is an input of the extension box E_1 (or E_2) is $L = (L_1, L_2)$ with $L_1, L_2 \in \{0, 1\}^{16}$, while the controlling vector $(V, Z) = (V_1, Z_1, V_2, Z_2, V_3, Z_3, V_4, Z_4, V_5, Z_5, V_6, Z_6, V_7, Z_7, V_8, Z_8)$ uses the switchable controlled operator $F_{32/256}^{(L,e)}$ generated as follows:

$$V_1 = L_1, V_2 = L_1^{<<<4}, V_3 = L_1^{<<<8}, V_4 = L_1^{<<<12};$$
$$V_5 = L_2^{<<<12}, V_6 = L_2^{<<<8}, V_7 = L_2^{<<<4}, V_8 = L_2;$$
$$Z_1 = L_1^{<<<12}, Z_2 = L_1^{<<<8}, Z_3 = L_1^{<<<4}, Z_4 = L_1;$$
$$Z_5 = L_2, Z_6 = L_2^{<<<4}, Z_7 = L_2^{<<<8}, Z_8 = L_2^{<<<12}$$

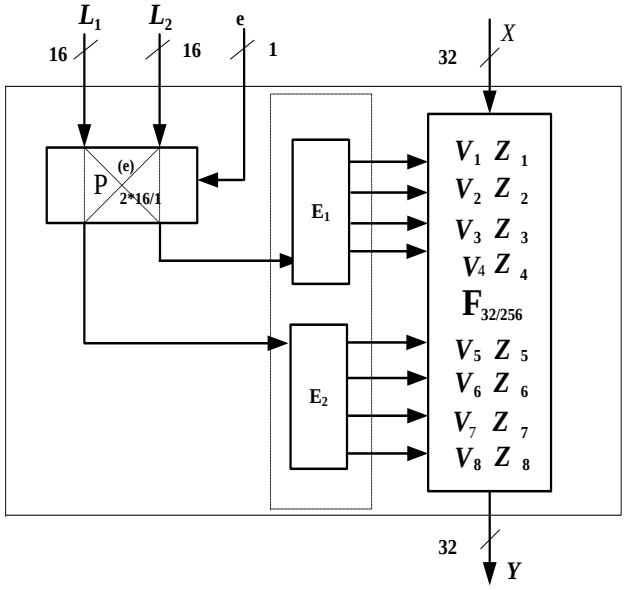

Figure 4. The Structure of SDDO $F_{32/256}^{(L,e)}$

Above is the whole structure of SDDO used in the algorithm BM-128. With this structure, SDDO gives solution to simple key schedule in proposed algorithm.

3. Design of Algorithm BM-128

BM-128 was developed by the same diagram (see Figure 5) and controlled elements, but use different controlled boxes. They consist of 8-round transformation without using the process of generating complex keys and constructed on the basic of CSPNs in association with the fixed permutations and boxes S_{4x4}, S^{-1}_{4x4}. These boxes constructed on the basic of permutational table used in algorithm Serpent. The use of minimum controlled element $F_{2/2}$ in CSPNs of algorithm helped to improve cryptographic criteria of expanded block operators which leads to the reduction of rounding number of encryption, but also preserves high durability of cryptographic algorithms (proved in part 5). Simultaneously, it reduces the complexity of devices when implemented in

FPGA with pipelining and increases encryption speed with iterative looping (proved in part 4). The outstanding features that BM-128 is aiming at are:

1) The process of the extension of keys is simple, so ensuring high encryption speed in condition of frequent change of session keys.
2) The mechanism of secret key selection is flexible, the secret key 128 bits or 192 bits or 256 bits can be used depending on requirement of a specific application.
3) Processing in basic encryption round is parallel, so it contributes to create high speed in encryption.
4) With results evaluated on combination efficiency and security estimation presented in part 4, 5, and 6 the algorithm aim at applications in fast wireless telecommunication network, which require little energy and surface area.

The steps of BM-128 are described as follows:

1. For $j = 1$ to 7 do: $\{(L, R) \leftarrow \mathbf{Crypt}^{(e)}(L, R, U_j, Q_j); (R, L) \leftarrow (L, R)\}$.
2. $(L, R) \leftarrow \mathbf{Crypt}^{(e)}(L, R, U_8, Q_8)$.
3. $\{(L, R) \leftarrow (L \oplus U_9, R \oplus Q_9); (L, R) \leftarrow (L, R)\}$

The scheme implementation of Cipher BM-128 is described in figure 6 and the transformations are used as follows: the SDDO $F^{(L,e)}_{32/256}$ (described in part 2); a pair of S_{4x4} and $S^{-1}{}_{4x4}$; permutations I and I_1 and expansion element E. The permutations and E are described as follows:

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

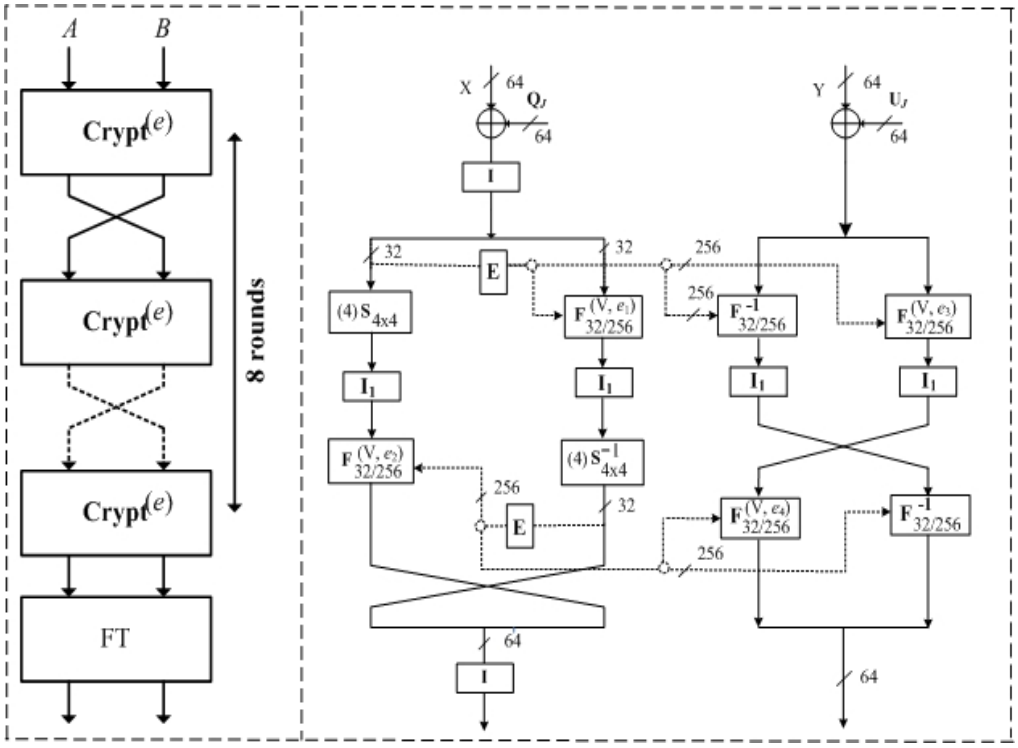

Figure 5. Structure and Round Transformation Crypt$^{(e)}$

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

The switchable bits e_i (i=1..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, e'_4 are described in Table I.

Subkeys $K_i \in \{0, 1\}^{64}$ are generated from 128 bits $K = (K_1, K_2)$ or 192 bits $K = (K_1, K_2, K_3)$ or 256 bits $K = (K_1, K_2, K_3, K_4)$ secret key K. The round keys U_j, Q_j are selected from subkeys K_i and listed in Table I.

Table I.
The Key Scheduling and Lists the Switch Bits

No. rounds j	1	2	3	4	5	6	7	8	FT
With 128 bits key									
Q_j =	K_1	K_2	K_2	K_2	K_1	K_2	K_1	K_2	K_1
U_j =	K_2	K_2	K_1	K_2	K_1	K_2	K_2	K_2	K_2
e'_1 =	1	0	1	1	0	1	0	0	-
e'_2 =	0	1	0	0	1	0	1	1	-
e'_3=	0	0	0	1	0	1	1	0	-
e'_4 =	1	0	0	1	1	0	1	0	-
With 192 bits key									
Q_j =	K_1	K_1	K_1	K_2	K_3	K_2	K_1	K_2	K_1
U_j =	K_3	K_2	K_1	K_2	K_3	K_2	K_1	K_1	K_3
e'_1 =	1	0	1	1	0	1	0	0	-
e'_2 =	0	1	0	0	1	0	1	1	-
e'_3=	0	0	0	1	0	1	1	0	-
e'_4 =	1	0	0	1	1	0	1	0	-
With 256 bits key									
Q_j =	K_1	K_4	K_4	K_4	K_3	K_2	K_1	K_2	K_1
U_j =	K_3	K_2	K_1	K_2	K_3	K_4	K_4	K_4	K_3
e'_1 =	1	0	1	1	0	1	0	0	-
e'_2 =	0	1	0	0	1	0	1	1	-
e'_3=	0	0	0	1	0	1	1	0	-
e'_4 =	1	0	0	1	1	0	1	0	-

4. Results on Security Estimation with Criteria NESSIE

As stated by NESSIE (New European Schemes for Signatures, Integrity and Encryption) [7], the security of encryption algorithm is considered based on 4 following criteria:

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)

Concurrently, based on that the security or transformations in encryption algorithms will be the best if the following conditions happen simultaneously: $d_c = 1$, $d_a \approx 1$, $d_{sa} \approx 1$ and $d_1 \approx ½ n$.

Based on that, we evaluated the statistical characteristics of encryption algorithm developed and it is found that it is very suitable with criteria that NESSIE proposed. Test are carried out with number of samples 1000 in 2 cases: K(Key) = 1, X(data) = 1000 and K(Key) = 1000, X(data) = 1. The results evaluated by tests of algorithm BM-128 are shown in Table II respectively. The results show that after 3 rounds of encryption they can satisfy the criteria of NESSIE with respect to the influence of the original data bits, as well as the influence of key bits. A study of statistical characteristics about the influence of key bits in this algorithm is the factor that helps to prove the security of algorithms. This algorithm used a simple method of key enlargment, but satisfied the statistical criteria of NESSIE.

Table II.
Influence of the Original Texts and Key Bit

	#X = 1000; #K = 1				#X = 1; #K = 1000			
	(1) = d_1	(2) = d_c	(3) = d_a	(4) = d_{sa}	(1) = d_1	(2) = d_c	(3)= d_a	(4)=d_{sa}
1	33.859641	0.625000	0.529057	0.523462	33.870594	0.625000	0.529228	0.523888
2	63.655055	1.000000	0.993154	0.971829	63.682258	1.000000	0.993510	0.972277
3	63.983844	1.000000	0.997977	0.97489	63.983891	1.000000	0.997824	0.974859
4	64.008383	1.000000	0.997994	0.974571	63.990039	1.000000	0.997715	0.974996
5	64.001203	1.000000	0.997977	0.974689	64.005922	1.000000	0.997549	0.974649
6	64.006344	1.000000	0.997652	0.974712	63.973766	1.000000	0.997606	0.975108
7	64.024828	1.000000	0.997676	0.974826	64.002188	1.000000	0.997568	0.974816
8	63.992063	1.000000	0.997786	0.974856	63.989250	1.000000	0.997709	0.974814

5. Differential Cryptanalysis

Differential cryptanalysis is seen as a popular solution used for cipher, so calculating differential trail to evaluate the ability against this cryptanalysis is the essential requirement in block cipher development.

In this algorithm, we use minimum controlled element $F_{2/2}$ and the transformation via element $F_{32/256}$ and a box S_{4x4}. Therefore, its differential value depends on the differential characteristics of the minimum controlled element $F_{2/2}$ and the distribution of the bit of the controlling vectors. It also depends on the structure of the expanded elements and the differential characteristic of the box S_{4x4}. It can be concluded that if the smaller number of active bits differential trail has, the larger the probability of the differential trail will be. Thus, we only analyze the differential trail with the number of active bits of 2.

Firstly, the existence of differential trail needs to be analysis. It can be seen that when differential trail go through half of left branch, which also go through the expanded element $E(32 \rightarrow 256)$, they will have the weight of 8 and is easy to find the probability $P_3 = F_{32/256}(\Delta_0 \rightarrow \Delta_0)$. Whereas, $P_1 = ½$ is the probability of differential

trail falling down on the half of left branch. By analyzing the interchangeable table S, we have $P_2 = S(\Delta_1 \rightarrow \Delta_2) = 1/2$. And the differential trail with the weight of 2 which goes through the transformation $F_{32/256}$ will have $P_4 = F_{32/256}(\Delta_2 \rightarrow \Delta_1)$ .. The differential trail in circle 1 will go through circle 2. It can be found that we only need to calculate the differential value $P_5 = F_{32/256}(\Delta_1 \rightarrow \Delta_1$. As a result, the largest probability exist the differential trail Δ_1 after through two-round is $2^{-61,5}$.

By testing program with 40.000 plaintexts, have the result P= $\{0.00000000000000000001065\} \wedge 4 \approx 2^{-252.103}$.

So, it can be concluded that after 4-round transformation BM-128, it has too enough the ability against differential cryptanalysis.

Clearly, it is shown that the ability against the differential cryptanalysis of developing algorithm much better than the common algorithms. Moreover, their differential value is farther ($\mathbf{2^{-61,5}}$) away than the objects with the adjacent values (2^{-56}). Only after three-rounds the differential cryptanalysis of BM-128 that it has a better safety.

In order to provide more information about the ability against differential cryptanalysis of BM-128, a comparison table about the differential characteristic of some ciphers is given in Table III.

Table III.
Security Comparision of Some Cipher With Bm-128

Cipher	*Rmax*	Differential characteristics		P(r)
		Min	P(2)	
COBRA-H128	10	$(0, \Delta_1^R)$	$P(2) \approx 1.25 \times 2^{-29}$	$\approx 2^{-144}$
COBRA-S128	12	$(0, \Delta_1^R)$	$P(2) = 2^{-32}$	$< 2^{-190}$
COBRA-S128	10	$(0, \Delta_1^R)$	$P(2) < 2^{-50}$	$< 2^{-200}$
COBRA-S128	8	$(0, \Delta_1^R)$	$P(2) < 2^{-56}$	$< 2^{-224}$
SG-128	10	$(0, \Delta_1^R)$	$P(2) \approx 2^{-32}$	$\approx 2^{-160}$
SS-128	10	$(0, \Delta_1^R)$	$P(2) \approx 2^{-34}$	$\approx 2^{-170}$
Eagle-128	10	$(0, \Delta_2^R)$	$P(2) \approx 2^{-35}$	$\approx 2^{-175}$
BM-128	8	$(0, \Delta_1^R)$	$P(2) \approx 2^{-61,5}$	$\approx 2^{-246}$

6. FPGA Synthesis Results and Comparisions

The study is carried out to do test which simulates the cipher BM–128 on FPGA and compare and evaluate its performance with the other algorithms (AES, COBRA-H64, Eagle_64, Rijndael, RC6, IDEA, *etc.*,). To ensure the objectivity, the study is also concurrently performed on chips Virtex-4FPGA, device 5vlx20tff323-2. The performance evaluation was reviewed basing on both models; first assessment model based on formula **IE = S/R** (S – speed of algorithm, R – resource); second assessment model based on **IE = S/(R x F)** (F – Frequency). The results in detail are described in Table IV. The results above show that the algorithm BM–128 has higher speed, but has smaller hardware requirement than the modern algorithms. Comparing the performance shows that they has higher performance than the algorithms. The evaluation implemented by pipeline (N = n) and iterative looping (N = 1) architecture aims to

evaluate the effectiveness of the algorithm in each case, so that it will be easier to select them in applications to meet a specific requirement.

7. Conclusion

All main results include in this paper as follows:

Table IV.
FPGA Synthesis Results of Bm-128 and Comparisons

Cipher	Block size	*Rmax*	*N*	R (#CLBs)	F (MHz)	S (Mbps)	Performance	
							S / R	S/(R × F)
BM-128	128	8	8	5585	95	12160	2.18	22.92
CIKS-1 [4]	128	8	8	6346	81	5184	0.82	10.09
EAGLE-128 [4]	128	10	10	4120	95	12160	2.95	31.07
COBRA-H128 [4]	128	12	12	22080	90	11500	0.06	4.10
AES [4]		10	10	17314	29	3650	0.21	7.40
Serpent [8]	128	32	8	7964	14	444	0.06	4.00
Serpent [10]	128	32	8	7964	14	444	0.06	4.01
BM-128	128	8	1	1114	89	1408	1.26	14.35
CIKS-128 [4]	128	8	1	1511	65	992	0.66	10.20
CIKS-1 [4]	128	8	1	907	81	648	0.71	8.82
IDEA [4]	128	8	1	2878	150	600	0.21	1.39
AES [9]	128	10	1	2358	22	259	0.11	4.99
COBRA-H128 [4]	128	12	1	2364	86	917	0.39	4.51
Rijndael [11]	128	10	1	2358	22	259	0.11	5.00
RC6 [12]	128	20	1	2638	14	88.5	0.03	2.40
Twofish [12]	128	16	1	2666	13	104	0.04	3.00

1) Design operator is controlled with $F_{32/256}$ in according to the structure of CSPN on the basis of the controlled element of the same class $F_{2/2}$ which are suitable for cryptography applications.
2) Simple key schedule will be applied to reduce the cost of the equipment installed on the hardware, but, SDDO based development SDDO shall eliminate attacks on weak keys. The analytical results show that applications are capable of against the known attacks.
3) Forecasting and estimating the costs of applications to FPGA, evaluating performance and comparing results with traditional efficient encryption algorithm.

The results of detailed, clear and scientific studies pointed out in Sections 3, 4, 5 and 6 shows that the proposed algorithm has a high potential of being applied in the communication systems requiring high speed and performance. It also contributes to creation of more appropriate options for each specific application which may require some specific security requirements with different levels.

References

[1] B. Do Thi and M. Nguyen Hieu. An Effective and Secure Cipher Based on SDDO. International Journal Computer Network and Information Security. 11(2012).
[2] N. H. Minh, H. N. Duy, Dung L H. Design and Estimate of a New Fast Block Cipher for Wireless Communications Devices. Proceedings of The International Conference on Advanced Technologies for Communications (ATC) , (2008), October 6-9, Ha noi, Viet Nam.
[3] Moldovyan N A, Sklavos N and Koufopavlou O. (2005). Pure DDP-base cipher: Architecture analysis, Hardware Implementation cost and Performance up to 6.5 Gbps. International Arab Journal of Information Technology, 2(2005).
[4] Moldovyan N A, Moldovyan A A. Data-driven Ciphers for Fast Telecommunication Systems. Auerbach Publications, New York, (2007).
[5] Sklavos N, Moldovyan N A and Koufopavlou O. High speed networking security. Design and implementation of two new DDP-based ciphers. Mobile Networksand Applications. 10 (2005).
[6] 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, 2 (2006).
[7] 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 2000.
[8] Moldovyan N A, Moldovyan A A, Eremeev M A and Summerville. Wireless networks security and cipher design based on data-dependent operations: Classification of the FPGA suitable controlled elements. Proceedings of International Conference on Computing, Communication and Control Technologies - CCCT (2004), August 14-17, Texas, USA.
[9] Sklavos N and Koufopavlou O. Architectures and VLSI implementations ofthe AES-proposal Rijndael. IEEE T COMPUT, 51(2002).
[10] Moldovyan A A, Moldovyan N A and Sklavos N. Controlled elementsfor designing ciphers suitable to efficient VLSI implementation. Telecommun Syst, 32(2006).
[11] Moldovyan N A. On cipher design based on switchable controlled operations. Proceedings of International workshop, Methods, Models, and Architectures for Network Security (2003), September 21-23, Petersburg, Russia.
[12] Yip W., Albirt A.J., Ghetwynd B., Paa C. FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists. 3rd Advanced Encryption Standard Conference Proceedings (2000), April 13-14, 2000, New York, NY, USA (http://www. nist.gov/aes).

Authors

Bac Do Thi, is a Lecturer with the Faculty of Information Technology of Thai Nguyen University (Thai Nguyen, Viet Nam). Her research interests include cryptography, communication and network security. She received her Diploma Information Technology from the Thai Nguyen University (2004). She has authored or co-authored more than 10 scientific articles, reports and patents, in the areas of her research.

Minh Nguyen Hieu is a Lecturer with the Military Technical Academy (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).