HYBRID MODEL IN THE BLOCK CIPHER APPLICATIONS FOR HIGH-SPEED COMMUNICATIONS NETWORKS

Minh Nguyen Hieu[1], Bac Do Thi[2], Canh Hoang Ngoc[3], Manh Cong Tran[4], Phan Duong Phuc[5] and Khoa Nguyen Tuan[6]

[1]Institute of Cryptographic Science and Technology, Hanoi, Vietnam
[2]Thai Nguyen University of Information and Communication Technology, Thainguyen, Vietnam
[3]Thuongmai University, Hanoi, Vietnam
[4]Le Quy Don Technical University, Hanoi, Vietnam
[5]Academy of Cryptography Techniques, Hanoi, Vietnam
[6]Research Laboratories of Saigon High-Tech Park, Ho Chi Minh City, Vietnam

ABSTRACT

The article proposes two different designs for the new block cipher algorithm of 128-bit block size and key lengths of 128-bit or 192-bit or 256-bit. The basic cipher round is designed in a parallel model to help improve the encryption/decryption speed. The differences of this design compared to the previous one developed on Switchable Data Dependent Operations (SDDOs) lies in the hybrid of the controlled elements (CEs) in the structure. Each design has a specific strength that makes the selection more compatible with the objectives of each particular application. The designs all meet the high security standards and possess the ability to fight off the attacks currently known. The designs match the limited environment of the wireless network by integrating effectively when implemented on Field-programmable gate array (FPGA) with both iterative and pipeline architectures for high effective integration.

KEYWORDS

Controlled substitution–permutation network (CSPN), Switchable Data Dependent Operation (SDDO), Block cipher, Hybrid model, Field-programmable gate array (FPGA).

1. INTRODUCTION

A prior requirement for the cryptographic algorithm applied/employed to secure information in different wireless networks today is to save resources, low calculation costs, and low power consumption. This is a major requirement in wireless networks in general [1, 31]. Thus, the security designs are facing a critical requirementwhich is to secure by cipher for the increasingly complex wireless networks but must take into account more limits [2, 32]. The wireless devices working with battery power will be constrained by the environment in which they work and the resources with which they dealt. This makes the security designers unable to consider the security issues only from the property aspect. One of the most important current challenges is the gap between energy needs and the performance requirements for the handling of the security issues of [1, 2, 31, 32]. The processing gap which is the security system architecture of the current wireless network does not meet the required calculation of the security processing. The battery gap has emphasized that the cost for the current energy consumption to support the security problems of wireless networks working on batteries is very great. In addition to flexibility, it also requires the

DOI: 10.5121/ijcnc.2020.12404

mobile wireless networks to work on un-sync standards and security protocols. Tamper resistance has emphasized that the mobile wireless networks are on the face of the increasing number of attacks from the physical attacks to the software attacks. Assurance gaps regarding the reliability make the security systems demands continue to function reliably despite the attacks from the smart opponents intentionally looking forunexpected errors [2]. However, the level of security is not the only important issue, an efficient encryption algorithm is an algorithm that should occupy less storage capacity, optimal use of hardware resources and consume less power. The cost of encryption and decryption depends on several parameters: the size of plaintext and ciphertext respectively; the complexity of the algorithm, cipher mode selected; and the process of the key generator. In particular, the key length is an important factor, and the longer the key, the longer the cipher. Similarly, the cost of encryption is dependent and the cost needs to perform decryption.

To meet the design requirements, one of the known trends, meeting the construction of a high-speed cipher algorithm for wireless communication networks is the use of Data Dependent Permutations (DDPs) [3]. They are built based on permutation networks constructed from primitive operation $P_{2/1}$ proposed and used as a primary element to design of various block ciphers like CIKS-1[4], CIKS-128 [5], Spectr-H64 [6], Cobra-S128 [7], Cobra-H64 [7], Cobra-H128 [7]. The ciphers based on DDP, however, have a potential weakness for the attacks based on linear cryptanalysis and differential cryptanalysis, this has been demonstrated in studies [8-12].

To overcome the weakness of the cipher algorithms based on DDP, some cipher algorithms based on the Data Dependent Operations (DDOs), they are built from controlled elements (CEs) of $F_{2/1}$or $F_{2/2}$ recommended in some studies DDO-64 [13], DDO-128 [13], Eagle-64 [14], Eagle-128 [14], XO-64 [15], KT-64 [16]. These algorithms have proven to be suitable for the implementation of cheap hardware and high speed. However, these algorithms use only a simple key schedule; they can be related-key attacks (RKE) [21-25].

Thus, a new method against the related-key attacks is to develop algorithms based on the Switchable Data Dependent Operations (SDDO). SDDO is reviewed as the newest cipher operation, oriented to the design of a fast cipher algorithms suited to applications in the limited environment. SDDO is firstly suggested in Hawk-64 [17, 18]. Algorithms of MD-64 [19], BMD-128 [20] have also given and demonstrated their strengths in terms of security and integrated efficiency on the given hardware.

Integral efficacy advantages of SDDO combined with the CSPN design model in hybrid [26], a new block cipher algorithm named BM123-128 is proposed in this article. This is the block cipher algorithm of 128-bit block size with key lengths of 128-bit or 192-bit or 256-bit.

The algorithm is developed on various SDDOs with $F^{(V,e)}_{32/256}$and$F^{(V,e)}_{32/128}$ in which:

$F^{(V,e)}_{32/256}$hybrid CSPN structure built from two CEs are $F_{2/2}$ and $F'_{2/2}$.

$F^{(V,e)}_{32/128}$ built according to a uniform CSPN structure from CE $F_{2/1}$(using CE $Q_{2/1}$ [18]).

This is the special feature to create new designs. This solution helps each design have its own strength. Further advantages of the algorithm is it is designed according to the model of parallel processing for basic cipher round in order to enhance the encryption/decryption speed. At the same time, the algorithm that uses simple key schedule, but still ensures security against the random cryptanalysis. The process of encryption/decryption using the same structure with the use of switchable operation is set between the two modes of encryption and decryption. The results of integral efficacy evaluation of algorithms on hardware obtained high integration effect. This shows an algorithm that meets the design requirements.

The article is structured as follows: Following the introduction, section 2 will present a new block cipher algorithm: BM123-128 with two different designs; section 3 presents the security estimation, the results of implementation on FPGA and section 4concludes on matters closely related to the proposed algorithm.

2. RESEARCH METHOD

BM123-128 is an algorithm which is developed in the block cipher mode with a block size of 128-bit, with 8 transformation rounds and secret key able to be selected as 128-bit or 192-bit or 256-bit. BM123-128 is designed in a parallel model for basic cipher round. This model helps to make encryption and decryption faster than serial models or a combination of serial and parallel models. The algorithm has used various SDDOs ($\mathrm{F}_{\mathrm{n/m}}^{(\mathrm{V,e})}$)in each particular case. SDDO is built based on hybrid or uniform CSPNs, then adds operation to Switchable Controlled Operation (SCO). The use of SDDO has been suggested earlier in several studies and considered as an element helping supporting the design of block cipher by using a simple key schedule. This helps the algorithm eliminate weak key that has just created a higher performance when deploying the algorithm on FPGA by reducing the cost of resources.

The process of encryption/decryption of BM123-128 is described as follows:

Permutations in Figure 1(a_1) and Figure 2(a_2):

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)(55)(56,24)(57)(58,26)(59)(60,28)(61)(62,30)(63)(64,32).

I₁=(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)(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).

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)

BM123-128 algorithm
1.128-bit input data to be divided into 2 blocks A and B, each block sizes 64-bit
2.For j = 1 to 7 do $\{(A, B) \leftarrow \mathrm{Crypt}^{(e)}(A, B, Q_j, U_j);$ $(A, B) \leftarrow (B, A)\}$ 3. $\{(A, B) \leftarrow \mathrm{Crypt}^{(e)}(A, B, Q_8, U_8)\}$ 4.$\{(A, B) \leftarrow (A \oplus Q_9, B \oplus U_9)\}$.

The design model of BM123-128 algorithm is shown in Figure 1, Figure 2 and Figure 3. Crypt$^{(e)}$-transformed function is detail described through the basic cipher round based on Figure 1(a_1) and Figure 2(a_2). The algorithm is developed with 2 different designs as in Figure 1(a_1) and Figure 2(a_2).

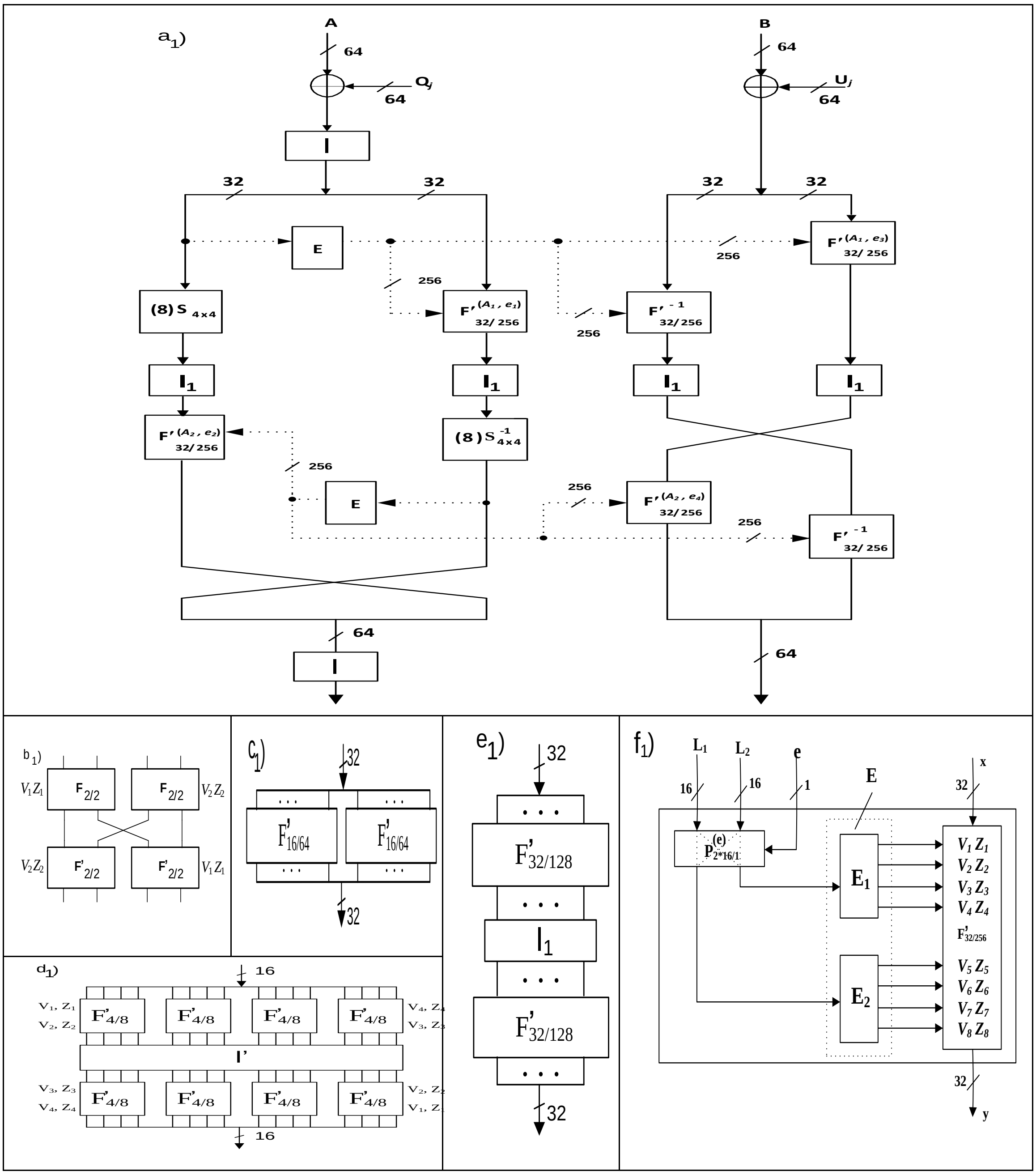

Figure 1. BM123-128 algorithm
(a_1) basic cipher round ($Crypt^{(e)}$) of case 1,
(b_1) $F'_{4/8}$, (c_1) $F'_{32/128}$, (d_1) $F'_{16/64}$, (e_1) $F'_{32/256}$, (f_1) $F'^{(L,e)}_{32/256}$.

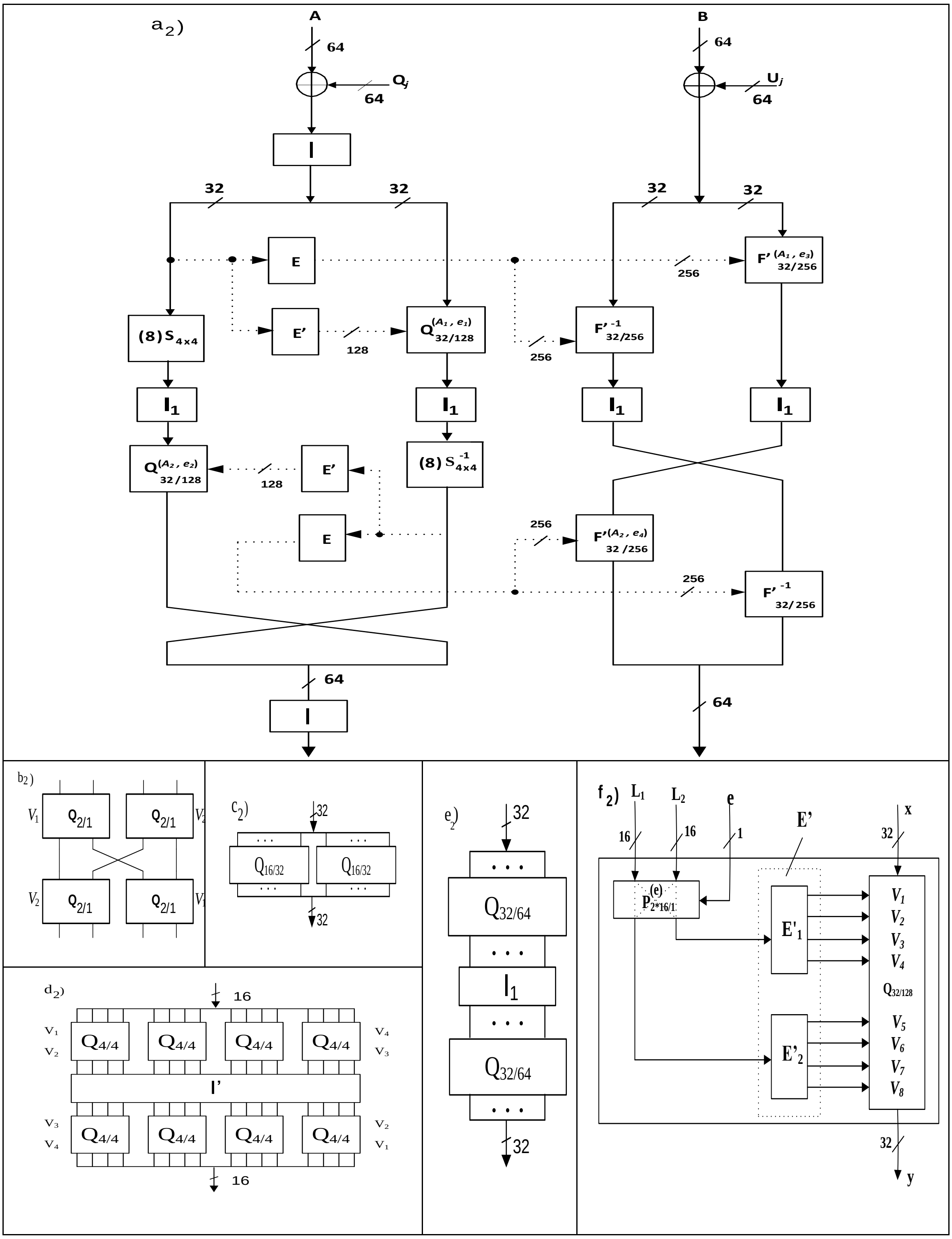

Figure 2.BM123-128 algorithm

(a2) basic cipher round (Crypt$^{(e)}$) of case 2,

(b2) $Q_{4/4}$,(c2) $Q_{32/64}$, (d2) $Q_{16/32}$, (e2) $Q_{32/128}$, (f2) $Q_{32/128}^{(L,e)}$.

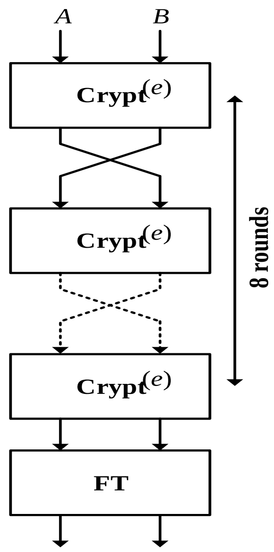

Figure 3.The general structure of BM123-128

The CSPN design process in cases of the algorithm is shortly described as follows:

+ **Case 1**: Use two CEs $F'_{2/2}$ and $F_{2/2}$ with a hybrid CSPN design model [26].The design process of operation is briefly described as follows: ($F'_{2/2}$ and $F_{2/2}$)→$F'_{4/8}$→$F'_{32/128}$→ $F'_{32/256}$, in which $F'_{4/8}$ described as Figure 1(b_1), $F'_{32/128}$ described as Figure 1(c_1), $F'_{16/64}$ described in Figure 1(d_1), $F'_{32/256}$ described in Figure 1(e_1). CSPNs are built using the hybrid method on the base element layers of $F_{2/2}$ (element of choice is (h, f, e, j)) and $F'_{2/2}$ (element of choice is (e, b, b, c)).

Specifically, the logic functions of $F_{2/2}$ are described as follows:

$y_1= vzx_2 \oplus vz \oplus vx_1 \oplus zx_1 \oplus z \oplus x_1 \oplus x_2$; $NL(y_1) = 4$ (1)

$y_2= vzx_1 \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus z \oplus x_2$; $NL(y_2) = 4$ (2)

$y_3= vzx_1 \oplus vzx_2 \oplus vz \oplus vx_2 \oplus x_1 \oplus zx_2$; $NL(y_3) = 4$ (3)

And the logic functions of $F'_{2/2}$ are described as follows:

$y_1= vzx_1 \oplus vzx_2 \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus z \oplus v \oplus x_2$;$NL(y_1) = 2$ (4)

$y_2= vzx_1 \oplus vzx_2 \oplus vz \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus x_1$; $NL(y_2) = 2$ (5)

$y_3 = vz \oplus v \oplus z \oplus x_1 \oplus x_2$;$NL(y_3) = 4$ (6)

Differential characteristics of CEs $F_{2/2}$ and $F'_{2/2}$ are described in Table 1.

Table 1.Probabilities$Pr(ijk) = Pr(\Delta_i^Y / \Delta_j^X, \Delta_k^V)$ of differential characteristics of CEs $F_{2/2}$, $F'_{2/2}$, $Q_{2/1}$.

Differential characteristics of $F_{2/2}$										
ijk	**001**	**002**	**011**	**101**	**110**	**120**	**002**	**102**	**201**	**202**
Pr	0,25	0,125	0,1875	0,375	0,75	0,5	0,125	0,5	0,375	0,375

Differential characteristics of $F'_{2/2}$											
ijk	**110**	**210**	**001**	**011**	**021**	**222**	**112**	**221**	**220**	**101**	**121**
Pr	1	0	0	0,5	0,5	1	1	1	1	0,5	0,5

Differential characteristics of $Q_{2/1}$													
ijk	**001**	**101**	**201**	**011**	**111**	**211**	**110**	**210**	**120**	**220**	**021**	**121**	**221**
Pr	0,25	0,5	0,25	0,25	0,5	0,25	0,5	0,5	1	0	0,25	0,5	0,25

Weakness in the choice of $F'_{2/2}$ is a balanced logic function with a nonlinearity lower than the balanced logic function of $F_{2/2}$, but has a higher differential characteristics (see Table 1). This yields a better avalanche effect of element than other cases, i.e. the ability to resist attacks by differential cryptanalysis of the algorithm, in this case, is also better.

+ Case 2: Use three CEs as $Q_{2/1}$, $F_{2/2}$ and $F'_{2/2}$ in which SDDO of the left branch of basic cipher round structure applies the basic operation $Q_{2/1}$ and the right branch of basic cipher round applies two CEs $F_{2/2}$ and $F'_{2/2}$ (see Figure 2(a_2)).

CSPN forming process of the left branch of the structure is described as follows: $Q_{2/1} \rightarrow Q_{4/4} \rightarrow Q_{32/64} \rightarrow Q_{32/128}$ and the right branch must be the same case 1. CSPNs used in the left branch built under a uniform model but CSPNs employed in the right branch built using the hybrid method on the element layer $F_{2/2}$ and $F'_{2/2}$. $Q_{4/4}$ is described as in Figure2(b_2), $Q_{32/64}$ in Figure2(c_2), $Q_{16/32}$ in Figure2(d_2), $Q_{32/128}$ in Figure 2(e_2),logical function shows elements $F_{2/2}$ and $F'_{2/2}$ as described in case 1, $Q_{2/1}$ CE in (7), (8), (9).

$y_1 = x_2v \oplus x_1 \oplus x_2$; $NL(y_1) = 2$ (7)

$y_2 = x_1v \oplus x_2$; $NL(y_2) = 2$ (8)

$y_3 = x_1v \oplus x_1 \oplus x_2v$; $NL(y_3) = 2$ (9)

$Q_{2/1}$ CE shows the greatest non-linearity for y_1, y_2. Differential characteristics are listed in Table 1.

SDDOs:SDDOs $F'^{(V,e)}_{32/256}$, $Q^{(V,e)}_{32/128}$used in the algorithm are described as in Figure 1(f_1)and Figure 2(f_2). The use of SDDO in the algorithm as mentioned will prevent possible weaknesses caused the only using a simple key schedule.

Expanding Box: Expansion box E including E_1 and E_2 of $F'^{(V,e)}_{32/256}$performs as follows: 16-bit of E_1 (or E_2) is 16-bit L_1 or L_2, where $L = (L_1, L_2)$ of $P_{2*16/1}$ and $L_1, L_2 \in \{0, 1\}^{16}$. Control 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) used in $F'^{(V,e)}_{32/256}$is described as follows:

$V_1 = L_1$, $V_2 = L_1^{<<<4}$, $V_3 = L_1^{<<<8}$, $V_4 = L_1^{<<<12}$;
$V_5 = L_2^{<<<14}$, $V_6 = L_2^{<<<10}$, $V_7 = L_2^{<<<6}$, $V_8 = L_2^{<<<2}$;
$Z_1 = L_1^{<<<2}$, $Z_2 = L_1^{<<<6}$, $Z_3 = L_1^{<<<10}$, $Z_4 = L_1^{<<<14}$;
$Z_5 = L_2$, $Z_6 = L_2^{<<<4}$, $Z_7 = L_2^{<<<8}$, $Z_8 = L_2^{<<<12}$

Expansion box E' including E'_1 and E'_2 of $Q^{(V,e)}_{32/128}$performs as follows: 16-bit of E'_1(or E'_2) to create control vector(V) = (V_1, V_2, V_3, V_4, V_5, V_6, V_7, V_8)of $F_{32/128}$ is formed as follows:

$V_1 = L_1$, $V_2 = L_1^{<<<4}$, $V_3 = L_1^{<<<8}$, $V_4 = L_1^{<<<12}$;
$V_5 = L_2^{<<<12}$, $V_6 = L_2^{<<<8}$, $V_7 = L_2^{<<<4}$, $V_8 = L_2$;

Also based on the results of the statistical analysis of the effects of keys and the analysis to eliminate weaknesses in related-key attacks, the key schedule of BM123-128 algorithm is designed as presented in Table 2.

Table 2. The key scheduling and lists the switch bits in BM123-128

Round	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**FT**
128-bit 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
192-bit 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
256-bit 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
Switchable bits (the same with different key lengths)									
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	-

In Table 2, there are sub-keys $K_i \in \{0,1\}^{64}$generated by secret keys of 256-bit: $K = (K_1, K_2, K_3, K_4,)$ or secret keys of 192-bit $K = (K_1, K_2, K_3)$ or secret keys of 128-bit $K = (K_1, K_2)$. In each transformation round, the design just uses 64-bit sub-keys for sub-block of data for both the left and the right. This helps the work done on the hardware reduce cost.

Bits e_i (i = 1...4) in the algorithm depends on bit e ($e \in \{0,1\}$) with a definition that e = 0 is encryption and e = 1 is decryption. Bits e_i are determined as follows: $e_1 = e \oplus e'_1$, $e_2 = e \oplus e'_2$, $e_3 = e \oplus e'_3$, $e_4 = e \oplus e'_4$ and e'_1, e'_2, e'_3, e'_4 as described in Table 2.

3. Security Estimation and FPGA Synthesis Results

The use of SDDO to design cipher algorithms using simple key schedule have been mentioned earlier in the studies [17-19, 27]. The use of SDDO also eliminates weak keys that may be generated due to not using complex key processes. This has been demonstrated in previous studies [8, 9].

Moreover, SDDO is built from a hybrid construction of CSPN in the design of algorithms. The hybrids will create greater space of choices that help the designers systemize the security by cipher with appropriate compromise between the security and integral efficacy of the algorithms on hardware.

3.1. Review of differential cryptanalysis

The resistance of a block cipher against differential cryptanalysis [18, 33, 34] depends on the maximum probability of differential characteristics, which are paths from the plaintext difference to the ciphertext difference.

Two designs proposed in the article are developed on SDDO, of which SDDO is designed from hybrid CSPNs. Based on the differential characteristics of basic elements and design structure of the expansion box, we can identify differential characteristic of the algorithm in the cases of using different SDDOs.

Formation schemes of the characteristic corresponding to the input difference (Δ^{L}_{1}, Δ^{R}_{0}) are presented in figure 4 and figure5.

+ Case 1:

$p_1 = 2^{-1}$.

$p_2 = 2^{-1}$.

$p_3 = \Pr(001) = \Pr_{F'_{32/256}}\left(\Delta_0^Y/\Delta_0^X, \Delta V_1\right) = 2^{-21}$.

$p_4 = \Pr(120) = \Pr_{F'_{32/256}}\left(\Delta_1^Y/\Delta_2^X, \Delta V_0\right) \approx 2^{-4}$.

$p_5 = \Pr(110) = \Pr_{F'_{32/256}}\left(\Delta_1^X/\Delta_1^Y, \Delta V_0\right) = 2^{-4}$.

So, we will calculate: $P(2) = p_1 \times p_2 \times p_3^3 \times p_4 \times p_5^2 = 2^{-1} \times 2^{-1} \times (2^{-21})^3 \times 2^{-4} \times (2^{-4})^2 \approx 2^{-77}$

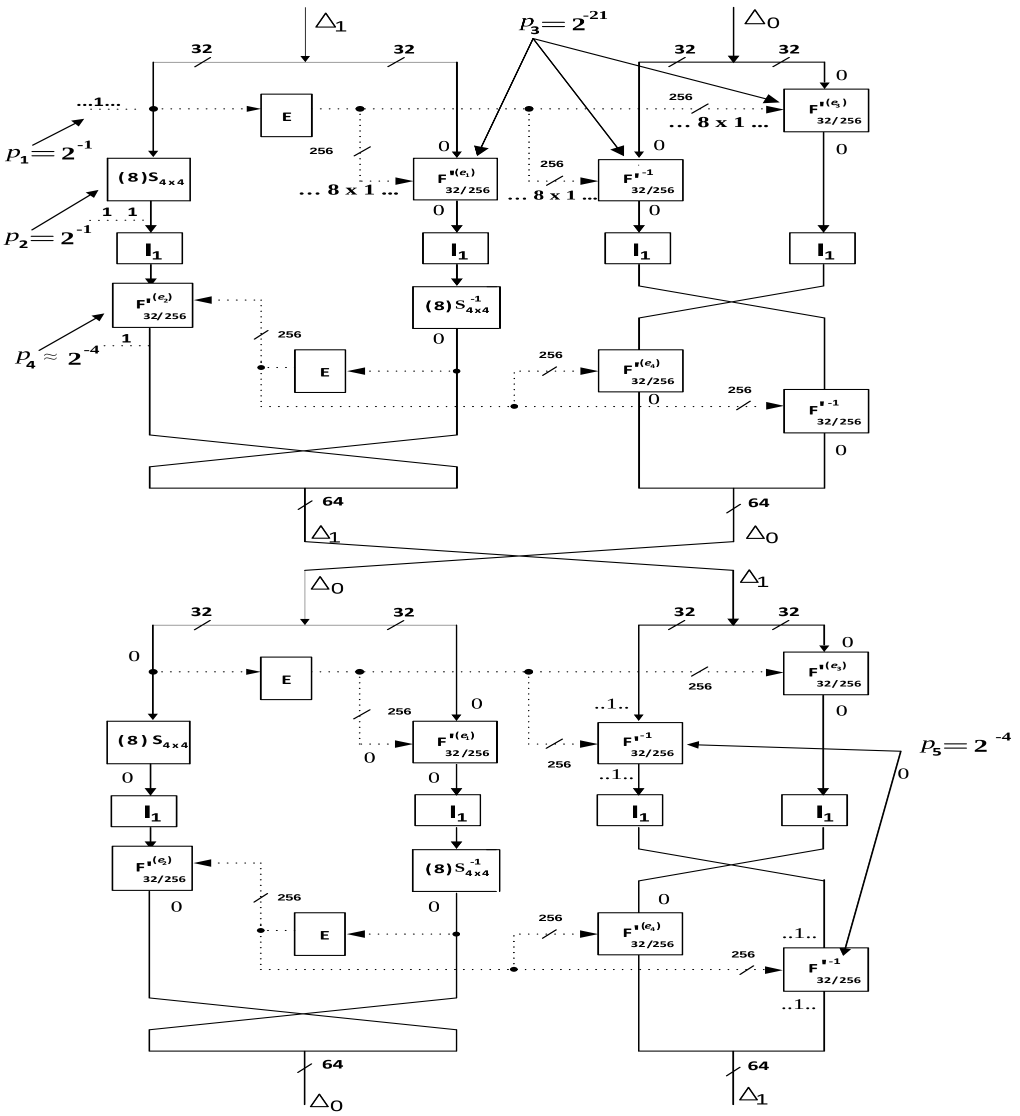

Figure 4.Formation of the two-round iterative differential characteristic with the difference (Δ^{L}_{1}, Δ^{R}_{0}) $\rightarrow$ (Δ^{L}_{0}, Δ^{R}_{1}) with probability $P(2) \approx 2^{-77}$.

+ Case 2:

$p_1 = 2^{-1}$.

$p_2 = 2^{-1}$.

$p_3 = \Pr(001) = \Pr_{F'_{32/256}}\left(\Delta_0^{Y}/\Delta_0^{X}, \Delta V_1\right) = 2^{-21}$.

$p_4 = \Pr(120) = \Pr_{Q_{32/128}}\left(\Delta_1^{Y}/\Delta_2^{X}, \Delta V_0\right) = 2^{-8}$.

$p_5 = \Pr(110) = \Pr_{F'_{32/256}}\left(\Delta_1^{X}/\Delta_1^{Y}, \Delta V_0\right) = 2^{-4}$.

$p_6 = \Pr(001) = \Pr_{Q_{32/128}}\left(\Delta_0^{X}/\Delta_0^{Y}, \Delta V_1\right) = 2^{-8}$.

So, we will calculate: $P(2) = p_1 \times p_2 \times p_3^2 \times p_4 \times p_5^2 \times p_6 = 2^{-1} \times 2^{-1} \times (2^{-21})^2 \times 2^{-8} \times (2^{-4})^2 \times 2^{-8} = 2^{-68}$.

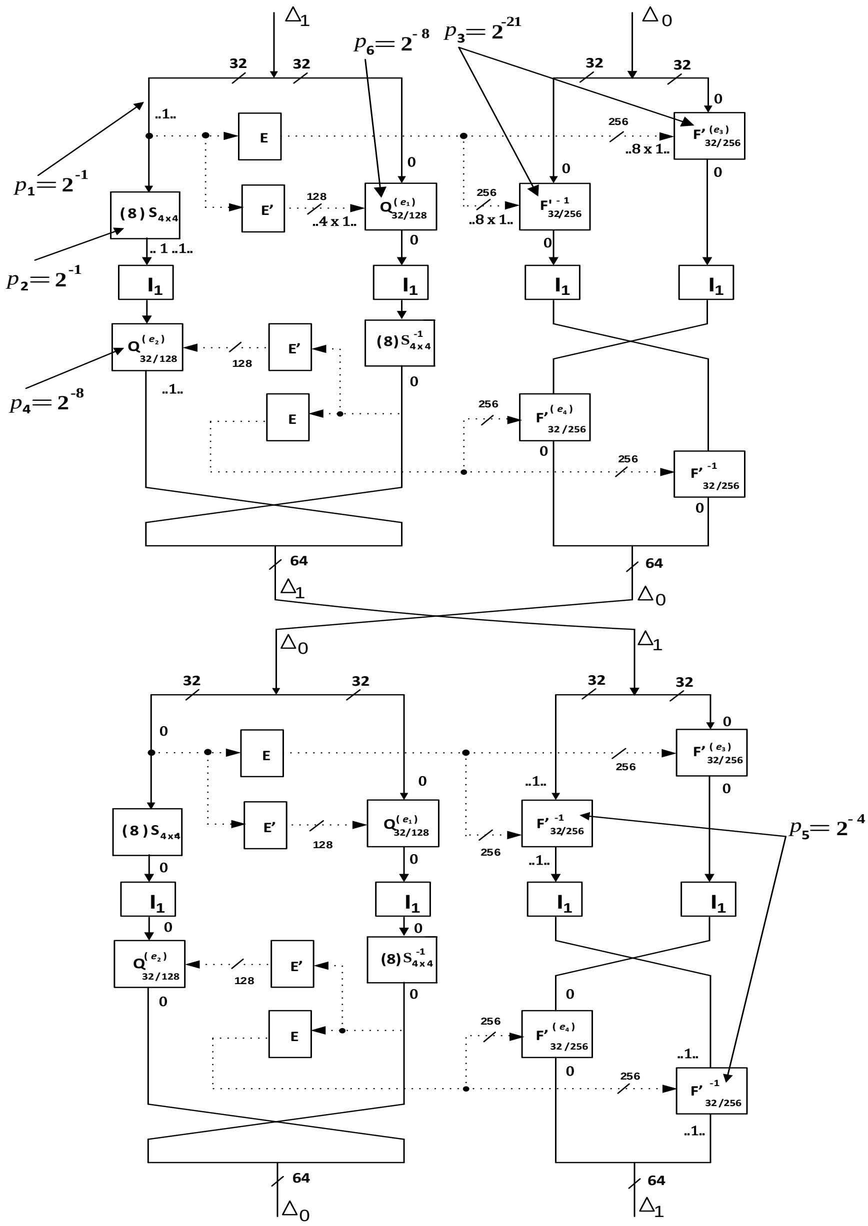

Figure 5.Formation of the two-round iterative differential characteristic with the difference $(\Delta^{L}_1, \Delta^{R}_0) \rightarrow (\Delta^{L}_0, \Delta^{R}_1)$ with probability $P(2) = 2^{-68}$.

Details of the results are presented in Table 3. The results show that the proposed designs have a differential characteristic better than the majority of the known block ciphers and have been the best ones in case 1, by the differential of $F_{2/2}$ elements chosen as the best ones and only after 4 rounds the design structure of the proposed algorithm can be able to resist differential cryptanalysis. However, to prevent the type of current un-predicted attacks, eight transformation rounds were used in the proposed designs.

Table 3. Security comparison of some cipher with BM123-128

Cipher	$\mathbf{R_{max}}$	**Differential characteristics**		$\mathbf{P(R_{max})}$
		Output Difference	**P(r)**	
COBRA-S128 [18]	10	$(0,\ \Delta_1^R)$	$P(2) < 2^{-50}$	$< 2^{-200}$
SS-128 [18]	10	$(0,\ \Delta_1^R)$	$P(2) \approx 2^{-34}$	$\approx 2^{-170}$
Eagle-128 [18]	10	$(0,\ \Delta_2^R)$	$P(2) \approx 2^{-35}$	$\approx 2^{-175}$
BM-128 [30]	8	$(\Delta^L{}_0, \Delta^R{}_1)$	$P(2) \approx 2^{-61,5}$	$\approx 2^{-246}$
BM123-128 (Case 1)	8	$(\Delta^L{}_0, \Delta^R{}_1)$	$P(2) \approx 2^{-77}$	$\approx 2^{-308}$
BM123-128 (Case 2)	8	$(\Delta^L{}_0, \Delta^R{}_1)$	$P(2) = 2^{-68}$	$= 2^{-272}$

3.2. Review of NESSIE test

For the purpose to check the statisticproperties of the block algorithm proposed in the article, we test it according to the method offered by the NESSIE Project (New European Schemes for Signatures, Integrity, and Encryption). In this method, we examine the statistic properties of the BM123-128 cipher corresponding to the following four dependence criteria [28]:

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).

According to NESSIE standard announced [28], we have tested with 10,000 random test samples with 2 models:

Model 1: X=100; K=100, reviewing the influence of the incoming text bits on the transformed text.

Model 2: X=100; K=100, reviewing the influence of the key bits on the transformed text.

Evaluating model 2 is a compelling factor for the security of the algorithm because the algorithm uses only simple key schedule without using complex key schedule but maintaining security standards.

Detailed statistical results are presented in Table 4 and Table 5 (Inthe case of a 128-bit key). The obtained results are shown after the third round, the algorithm has met the security standards required by NESSIE (for both cases of 192-bit and 256-bit keys, resulted corresponding to the third round).

Table 4.The values for criteria 1-4 (in case of 128-bit key ofcase 1)

	Model 1: #*X* = 100; #*K* = 100				Model 2: #*X* = 100; #*K* = 100			
	(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	29.383083	0.625000	0.459111	0.456983	29.383083	0.625000	0.459111	0.456983
2	62.124981	1.000000	0.970420	0.965538	62.156461	1.000000	0.970884	0.965964
3	63.994538	1.000000	0.999295	0.991948	63.999234	1.000000	0.999285	0.991982
4	64.004330	1.000000	0.999258	0.992037	64.007306	1.000000	0.999269	0.991969
5	63.996842	1.000000	0.999309	0.992101	64.003723	1.000000	0.999323	0.992037
6	64.000755	1.000000	0.999416	0.992077	64.009101	1.000000	0.999323	0.992072
7	64.001755	1.000000	0.999412	0.992066	63.999548	1.000000	0.999304	0.992083
8	64.003624	1.000000	0.999290	0.992009	64.001120	1.000000	0.999273	0.991962

Table 5. The values for criteria 1-4 (in case of 128-bit key ofcase 2)

	Model 1: #*X* = 100; #*K* = 100				Model 2: #*X* = 100; #*K* = 100			
	(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	33.937044	0.625000	0.530266	0.528869	33.937044	0.625000	0.530266	0.528869
2	63.683458	1.000000	0.994719	0.988183	63.691953	1.000000	0.994763	0.988179
3	63.999895	1.000000	0.999253	0.991982	64.007974	1.000000	0.999257	0.992031
4	64.003105	1.000000	0.999236	0.991932	64.005934	1.000000	0.999340	0.991972
5	63.998851	1.000000	0.999283	0.991996	63.998423	1.000000	0.999331	0.992101
6	64.010388	1.000000	0.999266	0.992075	63.994001	1.000000	0.999309	0.992084
7	63.992848	1.000000	0.999258	0.992090	63.999928	1.000000	0.999265	0.991988
8	64.000459	1.000000	0.999254	0.992047	64.000655	1.000000	0.999329	0.992024

3.3. Review of FPGA synthesis results and comparisons

Integral efficacy is the solution evaluating the relationship between the cost of resources in the algorithm for the encryption/decryption speed to be achieved. The integral efficacy evaluation is usually done under the two architectures described in detail in [18].

Hardware implementations of the proposed cipher are designed and coded in the VHDL language. The BM123-128 cipher is examined in hardware implementation by using iterative (IT)and pipeline (PP)architectures for XILINX FPGA Virtex Device.In the first one, only one round of BM123-128 cipher is implemented in order to decrement the required hardware resources.In a pipelined architecture where all R-rounds of the data encryption part and the key scheduling part are implemented, the required hardware resources are increased.

Due to the use of the FPGAorientedprimitives, the BM123-128 is significantly more efficient for the FPGA implementation against the majorityofthe known block ciphers. Under both architectures, the results showed that the proposed algorithm can integrate more efficiently than do other algorithms including the DDP-based ones (COBRA-H128, CIKS-1), DDO-based one (Eagle-128) and AES finalists(MARS, RC6, Rijndael, Serpent, and Twofish) [18]. In case 2, the integral efficacy is improved because the costof resources to design CE $F_{2/1}$ is less than that of CE $F_{2/2}$. Integral efficacy results implement the proposed algorithm on FPGA in comparison to other traditional algorithms, described in detail as in Table 6.

The comparisons are made in terms of Integral efficacy (IE). The Integral efficacy results are obtained by the following equations (two comparison models) [18]:

$$IE = \text{Throughput (Mbps)} / \text{Area (\#CLBs)}$$
$$IE = \text{Throughput (Mbps)} / ((\text{Area (\#CLBs)} \times \text{Frequency (MHz)})$$

Table 6. FPGA Synthesis Results of BM123-128 and Comparisons

Cipher	Block size	R_{max}	N	Area (#CLBs)	F (MHz)	Throughput (Mbps)	Integral efficacy	
							Mbps/ #CLBs	Mbps/ (#CLBs × GHz)
BM123-128 (case 1)(proposed)	128	8	8	5.585	94	12.032	2,15	22,92
BM123-128 (case 2)(proposed)	128	8	8	4.669	89	11.648	2,44	27,41
Eagle-128 [14]	128	10	10	4.120	95	12.160	2,95	31,07
AES [18]	128	10	10	17.314	28,5	3.650	0,21	7,40
Serpent [18]	128	32	8	7.964	13,9	444	0,06	4,01
BM123-128 (case1)(proposed)	128	8	1	1.114	86	1.392	1,25	14,36
BM123-128 (case 2)(proposed)	128	8	1	1.002	84	1.344	1,34	15,97
RC6 [18]	128	20	1	2.638	13,8	88,5	0,034	2,4
Twofish [18]	128	16	1	2.666	13	104	0,039	3,0
Eagle-128 [14]	128	10	1	781	92	1.177	1,51	16,38
AES-128 [29]	128	10	1	1.894	232,80	29.730	15,70	68,2

Notes: N-the number of cycles; N = 1 i.e. refers to the algorithm designed by FPGA according to iterative architecture (IT); N = R_{max} means algorithm designed on FPGA by Pipeline architecture) (PP).

4. CONCLUSIONS

The main research results in the article include:

- Analysis of the development trend of the cipher block at high speed and the challenge in the design of the cipher block algorithm in restricted environments.
- Proposed BM123-128 algorithm with two different specific designs. The designs use different hybrid CSPN models. The algorithm is a simple key schedule designed to help reduce the cost of the equipment when being implemented on the hardware.
- Demonstration of the security of the proposed algorithm design under the reviews of statistical standards by NESSIE and differential cryptanalysis.
- Proof of integral efficacy of the proposed algorithm designs with implementation efficiency on FPGA.Comparison of integral efficacy of some traditional cipher algorithms which have known for better results.
- Two designs of the proposed algorithm meet security against known attacks. The second design of the algorithm has an advantage in terms of integral efficacy, but it must accept the reduction in differential characteristics (though not significant).

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGMENTS

This research was supported by the project "Research, design and fabrication of IoT gateway devices integrated for the security solution in the IoT platform and applied for the air quality monitoring pilot in Ho Chi Minh City's Saigon High-Tech Park” (contract number 48/2018/HĐ-QKHCN).

REFERENCES

[1] Jie Wu,(2006),*Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless and Peer-to-Peer Networks*,Auerbach Publications Talor & Francis Group, New York.

[2] M. Razvi Doomun and KMS Soyjaudah, (2009) “Analytical Comparison of CryptographicTechniques for Resource-Constrained Wireless Security,” *International Journal of Network Security*, vol.9, no.1, pp.82–94.

[3] N.A.Moldovyan, A.A.Moldovyan, M.A.Eremeev andD.H.Summerville, (2004), “Wirelessnetworks security and cipher design based on data-dependent operations: Classification ofthe FPGA suitable controlled elements,”*Proceedings of the CCCT-2004*, Austin Texas,USA, pp.123–128.

[4] A. Moldovyan and N. Moldovyan, (2002), “A cipher based on data–dependent permutations,” *Journal of Cryptology*, vol. 15, pp.61–72.

[5] N.D.Goots, B.V.Izotov, A.A.Moldovyan and N.A.Moldovyan,(2003),*Modern cryptography: Protect Your Data with Fast Block Ciphers*, Wayne, A-LIST Publish.

[6] N.D.Goots, A.A.Moldovyan and N.A.Moldovyan, (2001),“Fast Encryption Algorithm Spectr-H64,”*MMM-ACNS 2001. LNCS*, vol.2052, pp.275–286.

[7] N.D.Goots, N.A.Moldovyan, P.A. Moldovyanu and D.H. Summerville, (2003),“Fast DDP-Based Ciphers: From Hardware to Software,”*46th IEEE Midwest International Symposium on Circuits and Systems.*

[8] Y.Ko, D. Hong, S.Hong, S. Lee and J. Lim, (2003),“Linear Cryptanalysis on SPECTR-H64 with Higher Order Differential Property,”*MMM-ACNS 2003. LNCS*, vol.2776, pp.298–307.

[9] Y.Ko, C. Lee, S. Hong and S. Lee, (2004),“Related Key Differential Cryptanalysis of Full-Round SPECTR-H64 and CIKS-1,”*ACISP 2004. LNCS*, vol.3108, pp.137–148.

[10] C.Lee, D. Hong, S. Lee, S. Lee, H. Yang and J. Lim, (2002),“A Chosen Plaintext Linear Attack on Block Cipher CIKS-1,”*ICICS 2002. LNCS*, vol.2513, pp.456–468.

[11] Y.Ko, C. Lee, S. Hong, J. Sung and S. Lee, (2004),“Related-Key Attacks on DDP based Ciphers: CIKS-128 and CIKS-128H,”*INDOCRYPT 2004. LNCS*, vol.3348, pp.191–205.

[12] C. Lee, J. Kim, S. Hong, J. Sung andS. Lee, (2005), “Related-Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b,”*Progress in Cryptology – Mycrypt 2005. Mycrypt 2005. Lecture Notes in Computer Science*, vol.3715, pp.244-262.

[13] A.Moldovyan, N. Moldovyan and N. Sklavos, (2004),“Minimum size primitives for efficient VLSI implementation of DDO-based ciphers,” *Electrotechnical Conference, MELECON 2004, Proceedings of the 12th IEEE Mediterranean*, vol.2, pp.807-810.

[14] N.A.Moldovyan,A.A. Moldovyan, M.A. EremeevandN. Sklavos, (2006), “New class of Cryptographic Primitives and Cipher Design for Network Security,”*International Journal of Network Security*,vol.2, pp.114–125.

[15] N.H. Minh, H.N. Duy and L.H. Dung, (2008), "Design and estimate of a new fast block cipher for wireless communication devices," in *Proceedings2008 International Conference on Advanced Technologies for Communications*, pp.409-412.

[16] N.H. Minh, N.T Luan and L.H Dung, (2010), "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.

[17] N.A.Moldovyan, (2008), “On Cipher Design Based on Switchable Controlled operations,”*International Journal of Network Security*,vol.7, pp.404–415.

[18] N.A.Moldovyan and A.A. Moldovyan, (2008),*Data-driven Ciphers for Fast Telecommunication Systems*, Auerbach Publications Taylor & Francis Group, New York.

[19] N.H.Minh, D.T. Bac and H.N. Duy, (2010),"New SDDO-Based Block Cipher for Wireless Sensor Network Security,"*International Journal of Computer Science and Network Security*,vol.10, pp.54–60.

[20] D.T. Bac, N.H. Minh and H.N. Duy, (2012),"An Effective and Secure Cipher Based on SDDO,"*International Journal of Computer Network and Information Security*, vol.11, pp.1–10.

[21] J.Kang, K.Jeong, C.LeeandS. Hong, (2014),"Distinguishing attack on SDDO-based block cipher BMD-128,"*In Ubiquitous Information Technologies and Applications,*vol.280, pp.595–602.

[22] T.S.D.Phuc, C.Lee and N.Xiong, (2017),"Cryptanalysis of the XO-64 Suitable forWireless Systems," *Wireless Personal Communications*, vol.93, pp.589–600.

[23] J.Kang, K. Jeong, S. Hong and C. Lee, (2013),"Related-key amplified boomerang attacks on KT-64 and MD-64 suitable for wireless sensor networks," *Sensor Letters*, vol.11(9), pp.1765–1770.

[24] J. Kang, K. Jeong, S. Yeo and C. Lee, (2012), "Related-key Attack on the MD-64 Block Cipher Suitable For Pervasive Computing Enviromnent", *Proceedings of International Conference on Advance Infonmtion Networking and Application Workshops*, no.26, pp.726-731.

[25] T.S.D. Phuc and C. Lee, (2018), "Cryptanalysis on SDDO-Based BM123-64 Designs Suitable for Various IoTApplicationTargets,"*Symmetry*, 10(8), pp.1-11.

[26] D.T. Bacand N.H. Minh, (2013), "High-speed block cipher algorithm based on hybrid method," *Proceedings of the 8th International Conference on Ubiquitous Information Technologies and Applications (CUTE 2013), Lecture Notes in Electrical Engineering*, vol.280, pp.285-291.

[27] P.M. Tuan, D.T. Bac, N.H. MinhandD.T. Nam, (2017), "New Block Ciphers for Wireless Moblile Netwoks. In: Advances in Information and Communication Technology,"*ICTA 2016. Advances in Intelligent Systems and Computing*, vol.538,pp.393-402.

[28] NESSIE. New European Schemes for Signatures, Integrity, and Encryption, https://www.cosic.esat.kuleuven.ac.be/nessie/

[29] HarshaliZodpe and Ashok Sapkal, (2018), "An efficient AES implementation using FPGA with enhanced security features," *Journal of King Saud University - Engineering Sciences*, pp.1-8.

[30] D.T. BacandN.H. Minh, (2013), "A High Speed Block Cipher Algorithm," *International Journal of Security and Its Applications*, vol.7, no.6, pp.43-54.

[31] Daniel G. Costa,Solenir Figuerêdo and Gledson Oliveira, (2017), "Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions,"*Cryptography 2017*, 1(1), 4.

[32] Ahmer Khan Jadoon, Licheng Wang, Tong Li and Muhammad Azam Zia, (2018), "Lightweight Cryptographic Techniques for Automotive Cybersecurity," *Wireless Communications and Mobile Computing*, Special Issue: Rethinking Authentication on Smart Mobile Devices, https://www.hindawi.com/journals/wcmc/2018/1640167/.

[33] Lorenzo Grassi, (2017), "Mixture Differential Cryptanalysis and Structural Truncated Differential Attacks on round-reduced AES," *Cryptology ePrint Archive: Report 2017/832*. https://eprint.iacr.org/2017/832.pdf.

[34] Lorenzo Grassi and Christian Rechberger, (2018),"New Rigorous Analysis of Truncated Differentials for 5-round AES," *Cryptology ePrint Archive: Report 2018/182*. https://eprint.iacr.org/2018/182.

AUTHORS

Minh Nguyen Hieu is a Vice Dean at the Institute of Cryptographic Science and Technology, Hanoi, Vietnam. He finished his Ph.D. at 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, book chapters, reports, and patents, in the areas of his research.

Bac DoThi is a Lecturer at the Faculty of Information Technology, Thai Nguyen University (Thainguyen,Vietnam). Her research interests include cryptography, communication, and network security. She received her Ph.D. from Le Quy Don Technical University (2014).

Canh Hoang Ngoc is a Lecturer at Thuongmai University, Hanoi, Vietnam. He received his master degree in information systems from the 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.

Manh Cong Tran 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.

Phan Duong Phuc is a Lecturer at the Academy of Cryptography Techniques, Hanoi, Vietnam. He received his master degree in Telecommunications Engineering from Posts and Telecommunications Institute of Technology, Vietnam in 2014. His research interests include electronics, telecommunications, and cryptography.

Khoa Nguyen Tuan is a Researcher at the Research Laboratories of Saigon High-Tech Park, Ho Chi Minh City, Vietnam (SHTP Labs). His research interests include electronics, telecommunications, and cryptography.