New SDDO-Based Block Cipher for Wireless Sensor Network Security

Nguyen Hieu Minh*, Do Thi Bac** and Ho Ngoc Duy*
* Faculty of Information Technology, Military Technical Academy 100 Hoang Quoc Viet, Ha Noi, Viet Nam
** Faculty of Information Technology, Thai Nguyen University, Quyet Thang, Thai Nguyen, Viet Nam

***Abstract* — Wireless sensor networks (WSNs) are exposed to a variety of attacks. The quality and complexity of attacks are rising day by day. Limitations in computational and battery power in sensor nodes are constraints on the diversity of security mechanisms. This paper concerns the problem of using of the switchable data-dependent operations (SDDOs) oriented to the design of fast cipher suitable to applications in constrained environments. The new SDDO-based block cipher using this approach presented and estimated. The security estimations show that cipher MD-64 is less likely to suffer intrusion of differential cryptanalysis than currently used popular WSN ciphers like DES, Camellia and so on. Moreover, FPGA synthesis result for hardware implementation (FPGA) proves that new cipher MD-64 is very efficient, especially for WSN.**

***Keywords* - Block cipher, Switchable data-dependent operations, Wireless sensor networks, Hardware implementation.**

I. INTRODUCTION

With the widespread use of wireless network services and applications, security becomes a major concern. From security aspects, data integrity and confidentiality are vital issues for information systems. Information transfer through wireless sensor networks (WSNs) needs to be protected from misuse. Modern security methods need to guarantee the safety of data transmission with respect to security needs, i.e., confidentiality, integrity, and availability (CIA). Providing information security in WSN is also necessary especially for those security-sensitive applications and is one of the major concerns of our proposal.

There are many countermeasure methods that have been extensively studied to provide WSN communication security [1, 2, 3]. However, WSN is still exposed to some kinds of attacks as can be seen in [1, 3, 4]. These defenses are ineffective against attacks from compromised servers due to the WSN level constantly increasing, and attacks are becoming more and more complicated, as presented in [1, 4]. Moreover WSN has some restrictions when it comes to its applications, like limited power supplies, low bandwidth, small memory sizes and limited energy, which make it more vulnerable [5]. And as information becomes more valuable and costly, intruders use more complicated methods in attacking WSN, this eventually makes the security issue highly sensitive. Due to the increase in new trends of attack, previous security methods cannot combat or resist modern attacks.

Successfully deployment of WSN is connected with the problem of embedding security mechanisms in constrained environments. Therefore designing ciphers suitable to cheap hardware implementation represents practical importance.

Many network applications of the encryption require development of the ciphers that are fast in the case of frequent change of keys. Such ciphers should use no time consuming key preprocessing, i.e. they should use very simple key scheduling. An attempt to simplify the key scheduling is the use of the Data-Dependent (DD) transformation of the subkeys, which is called internal key scheduling [6]. To implement data-driven processing of the subkeys different variants of the so called controlled operations (CO) are suitable [7]. Switchable DDOs (SDDOs) [8] have been used as a primitive suitable to designing efficient ciphers with simple key scheduling. Implementation results of the SDDO-based ciphers show they provide high performance while implemented in cheap hardware [9].

The paper is organized in the following way. Section II concerns the problem of outline briefly to efficiency of existing WSN algorithms. Section III presents minimum size controlled elements (CEs) $\mathbf{F}_{2/2}$ and controlled substitution-permutation networks (CSPNs) as variable operations. Section IV describes the structure of the new block cipher: eight-round MD-64 with 64-bit data input. Section V presents results on security estimations with NESSIE criteria and differential cryptanalysis. Section VI presents the FPGA synthesis result and comparisons of the proposed cipher with other block ciphers. Finally, conclusion.

II. EFFICIENCY OF EXISTING WSN ALGORITHMS

Crypto attack methods are very complicated. They combine mathematics, information science and even electronics with unusual thinking. WSN block ciphers

Manuscript received March 5, 2010
Manuscript revised March 20, 2010

design needs to consider stability against analytical crypto-attacks. The practice in past years has shown us differential cryptanalysis (DCA) [10] and linear cryptanalysis (LCA) [11] where the most powerful analytical crypto analysis methods were used. The main content of DCA is the propagation analysis of the influence of modifications in the plaintext on the modification in cipher text (propagation properties). Using DCA as a method of complex attack with complicated mathematical methods can be one way of verifying the stability of block ciphers.

Block cipher designers who are trying to use theoretical computing constructions that provided distinctness in the evaluation of block ciphers in modern cryptanalysis methods, should give consideration before putting all these into action [12].

We outline briefly the drawbacks of existing algorithmic methods which are being used in many current technologies:

- Widespread algorithms (end to end, single destination communication, IP overlays);
- Probabilistic broadcasts (discrete effort: does not handle disconnection);
- Scalable reliable multicast (multicast over a wired network, latency-based suppression);
- Public-key cryptography (too expensive);
- Fast symmetric-key ciphers (must be used sparingly).

On designing WSN algorithm it is necessary to consider all specific features of WSN. However, we present sets of requirements for WSN algorithm and use these requirements as the highlight in facilitating the design of our new cipher:

- The cipher should be fast, in the case of frequent key refreshing;
- Cipher suitable to cheap hardware implementation;
- Technical cryptanalysis stability.

III. Minimum Size CE $\mathbf{F}_{2/2}$ and Controlled Substitution-Permutation Networks as Variable Operations

The $\mathbf{F}_{2/2}$ type CEs controlled with two bits v and z (figure 1a) are proposed as main building block, while designing the DDO boxes. An element $\mathbf{F}_{2/2}$ can be described as a pair of BFs with four variables (figure 1b), or as a set of four 2×2 substitutions (figure 1c) called modifications $\mathbf{F}^{(00)}_{2/2}$, $\mathbf{F}^{(01)}_{2/2}$, $\mathbf{F}^{(10)}_{2/2}$, $\mathbf{F}^{(11)}_{2/2}$ [20].

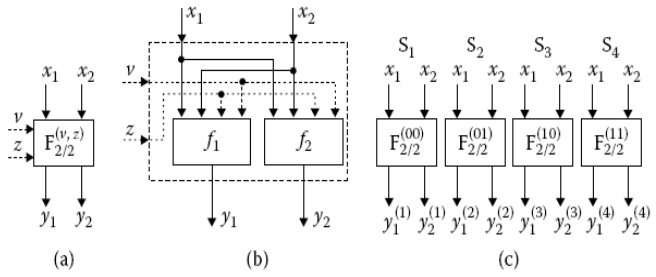


Figure 1. a) CE $\mathbf{F}_{2/2}$, b) represented as a pair of BFs in four variables, c) or as four 2×2 substitutions.

In order to select the $\mathbf{F}_{2/2}$ CEs suitable to design efficient cryptographic DDOs, the following criteria have to be applied:

1. Each one of the two outputs of CEs should be a non-linear BF having maximum possible non-linearity NL = 4 for balanced BFs in four variables.
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 = 4 for balanced BFs in four variables.

In order to try all possible variants of the $\mathbf{F}_{2/2}$ elements we have considered the $\mathbf{F}_{2/2}$ elements as sets of four 2×2 substitutions (S_1, S_2, S_3, S_4). For some CE $\mathbf{F}_{2/2}$ defined as a set (S_1, S_2, S_3, S_4) we can easy get BFs describing its outputs y_1 and y_2:

$$y_1 = vz({y^{(1)}}_1 \oplus {y^{(2)}}_1 \oplus {y^{(3)}}_1 \oplus {y^{(4)}}_1) \oplus v({y^{(1)}}_1 \oplus {y^{(3)}}_1) \oplus z({y^{(1)}}_1 \oplus {y^{(2)}}_1) \oplus {y^{(1)}}_1,$$

$$y_2 = vz({y^{(1)}}_2 \oplus {y^{(2)}}_2 \oplus {y^{(3)}}_2 \oplus {y^{(4)}}_2) \oplus v({y^{(1)}}_2 \oplus {y^{(3)}}_2) \oplus z({y^{(1)}}_2 \oplus {y^{(2)}}_2) \oplus {y^{(1)}}_2.$$

Figure 2 shows general topology of CSPN:

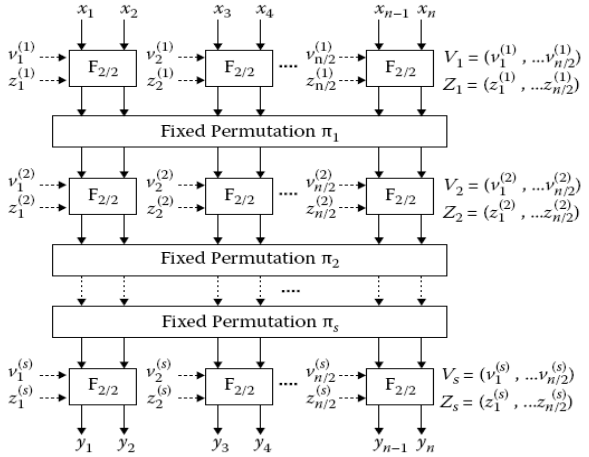


Figure 2. General structure of the $\mathbf{F}_{n/2m}$ boxes.

While performing DDOs some bits of data are used as v, z, x_1, x_2, therefore we have non-linear transformation performed on some encrypted data block.

Besides the NL value, differential characteristics (DCs) of the CE are important to characterize CEs as cryptographic primitives. Possible DCs are illustrated in figure 3, where $p\left(\Delta_i^Y / \Delta_j^X, \Delta_k^V\right)$ is probability to have the output difference is Δ_i^Y, if the input difference is Δ_j^X and the difference at the controlling input is Δ_k^V (indices indicate the number of non-zero bits in corresponding differences).

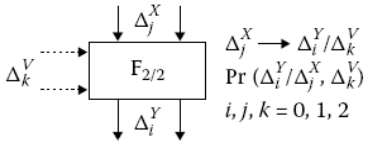


Figure 3. Differential characteristics of the $\mathbf{F}_{2/2}$ elements.

DDOs are very attractive to be used together with simple key scheduling. However the use of the simple key scheduling introduces the problem of weak keys. The property of the controllability of the operations used as cryptographic primitives provides possibility to design different types of the iterative block cryptoschemes with simple key scheduling, which can be implemented in cheap hardware. The property of the controllability allows avoiding the weak keys while using the simple key scheduling [20].

SDDOs have been used as a primitive suitable to designing efficient ciphers with simple key scheduling. The SDDOs are performed with switchable controlled operations (SCO) defined below:

Definition 1: Let $\mathbf{F}^{(e)}$, where $e \in \{0, 1\}$, be some e-dependent operation containing two modifications $\mathbf{F}^{(0)} = \mathbf{F}_1$ and $\mathbf{F}^{(1)} = \mathbf{F}_2$, where $\mathbf{F}_2 = \mathbf{F}_1^{-1}$. Then the operation $\mathbf{F}^{(e)}$ is called switchable.

Definition 2: Let two modifications of the switchable $\mathbf{F}^{(e)}$ be mutual inverses $\mathbf{F}^{(0)} = \mathbf{F}^{(V)}$ and $\mathbf{F}^{(1)} = (\mathbf{F}^{-1})^{(V)}$. Then $\mathbf{F}^{(e)}$ is called switchable controlled operation $\mathbf{F}^{(V,e)}$.

IV. Fast SCO-Based Cipher MD-64

Figure 4 presents new 64-bit cipher MD-64 particular feature of which is the combining SPN ($\mathbf{S}_i$ operation performed on the right data subblock) with CSPNs (two SCO boxes $F_{32/192}^{(B,e_1)}$ and $F_{32/192}^{(B',e_2)}$ in the left branch of the round cryptoscheme). MD-64 uses 128-bit key $K = (K_1, K_2, K_3, K_4)$ ($K \in \{0, 1\}^{32}$) and very simple key scheduling that is the same while enciphering and deciphering. However different scheduling of the bits e_1 and e_2 is used while encryption and decryption.

Ciphering procedure of MD-64 is described as follows:

$C = \mathrm{T}^{(e=0)}(M, K)$ and $M = \mathrm{T}^{(e=1)}(C, K)$, where M is the plaintext, C is the ciphertext (M, $C \in \{0,1\}^{64}$), T is the transformation function, and $e \in \{0,1\}$ is a parameter defining encryption ($e = 0$) or decryption ($e = 1$) mode.

First data block is divided into two 32-bit subblocks A and B and then using the procedure $\mathrm{Crypt}^{(e)}$ eight encryption rounds are performed. The last round is followed by final transformation (FT). The structure of the procedure $\mathrm{Crypt}^{(e)}$ is shown in figure 4b.

1. For $i = 1$ to 7 do: $\{(A, B) \leftarrow \mathrm{Crypt}^{(e)}(A, B, Q_j, U_j); (A, B) \leftarrow (B, A)\}$.
2. Perform transformation: $\{(A, B) \leftarrow \mathrm{Crypt}^{(e)}(A, B, Q_8, U_8)\}$
3. Perform final transformation: $\{(A, B) \leftarrow (A \oplus Q_9, B \oplus U_9); (A, B) \leftarrow (A, B)\}$.

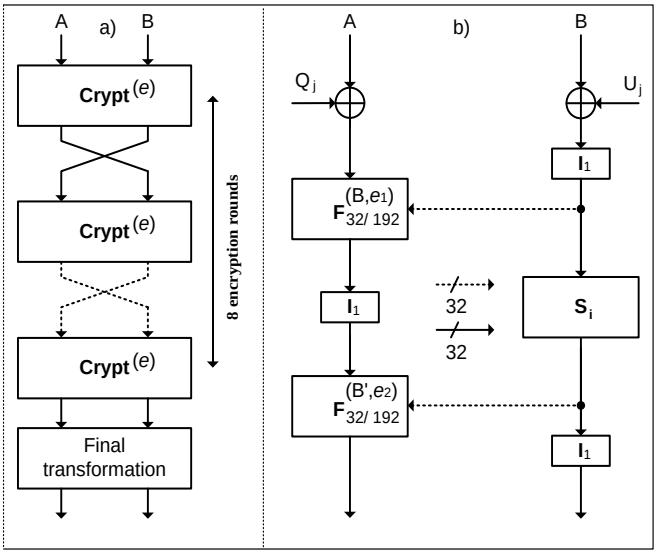


Figure 4. Cipher MD-64: a) iterative structure, b) procedure $\mathrm{Crypt}^{(e)}$.

Initially, we construct the boxes $\mathbf{F}_{32/192}$ (figure 6a) and $\mathbf{F}^{-1}{}_{32/192}$ (figure 6b) that are mutual inverses (the box $\mathbf{F}^{-1}{}_{32/192}$ is constructed inverse with box $\mathbf{F}_{32/192}$). The $\mathbf{F}_{32/192}$ and $\mathbf{F}^{-1}{}_{32/192}$ boxes are constructed using the CEs as standard building blocks. The permutational involution $\mathbf{I}_1$ in the left branch of the round transformation is the same as that corresponding to connection between cascade of four parallel boxes $\mathbf{F}_{8/24}$ and cascade of four boxes $\mathbf{F}^{-1}{}_{8/24}$ in the box $\mathbf{F}_{32/192}$ (see figure 5 and 6).

$\mathbf{I}_1$=(1)(2,9)(3,17)(4,25)(5)(6,13)(7,21)(8,29)(10)(11,18)(12,26)(14)(15,22)(16,30)(19)(20,27)(23)(24,31)(28)(32).

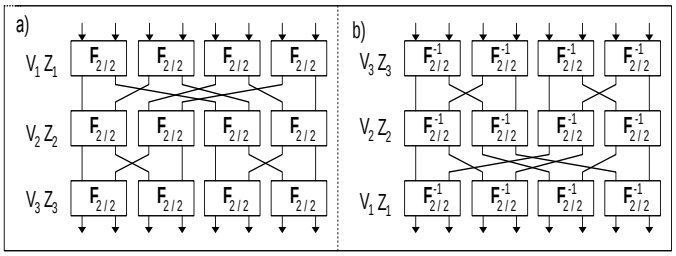


Figure 5. Topology of the DDO boxes: a) $\mathbf{F}_{8/24}$, b) $\mathbf{F}^{-1}{}_{8/24}$.

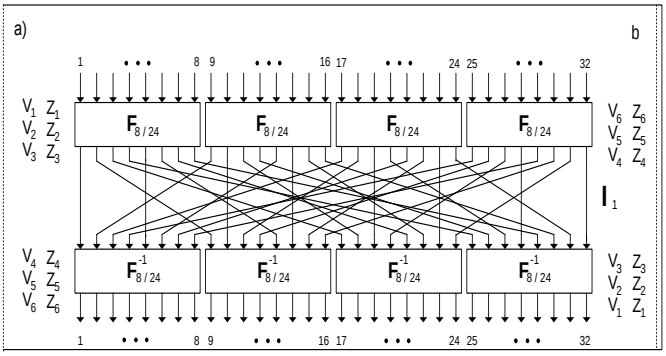


Figure 6. Topology of the DDO boxes: a) $\mathbf{F}_{32/192}$, b) $\mathbf{F}^{-1}{}_{32/192}$.

The design of the used SCO boxes is explained in figure 7. The $F_{32/192}^{(B,e_1)}$ and $F_{32/192}^{(B',e_2)}$ boxes can be constructed with the use of transposition box $P_{16\times2/1}^{(e)}$ and using the (*h*, *f*, *i*, *j*) element is standard building blocks. The e_1 and e_2 values depend on *e* and round number: $e_1 = e' \oplus e$ and $e_2 = e'' \oplus e$, where e' and e'' are specified in table 1.

For the (*h*, *f*, *e*, *j*) element we have [20]:

$y_1 = vzx_2 \oplus vz \oplus vx_1 \oplus zx_1 \oplus v \oplus z \oplus x_1 \oplus x_2$; $\mathrm{NL}(y_1) = 4$;

$y_2 = vzx_1 \oplus vx_1 \oplus vx_2 \oplus zx_2 \oplus zx_1 \oplus zx_2 \oplus x_1$; $\mathrm{NL}(y_2) = 4$;

$y_3 = y_1 \oplus y_2 = vzx_1 \oplus vzx_2 \oplus vz \oplus vx_2 \oplus zx_2 \oplus x_1$; $\mathrm{NL}(y_3) = 4$.

In figure 7, the box $P_{16\times2/1}^{(e)}$ represents 16 parallel $P_{2/1}^{(e)}$-boxes controlled with the same bit *e*. Input of $P_{16\times2/1}^{(e)}$ - box is divided into 16-bit left and 16-bit right inputs. The right (left) input (output) of 16 parallel boxes $P_{2/1}^{(e)}$ compose the right (left) 16-bit input (output) of the box $P_{16\times2/1}^{(e)}$. Thus, the box $P_{16\times2/1}^{(e)}$ performs *e*-dependent swapping of the respective pair of the 16-bit components of the controlling vectors L_1 and L_2.

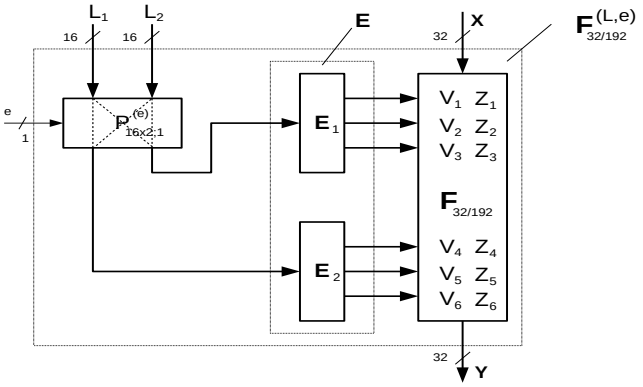


Figure 7. Structure of the SDDO $\mathbf{F}^{(L,e)}{}_{32/192}$.

The 192-bit controlling vectors *V* and *V*' corresponding to the $F_{32/192}^{(B,e_1)}$ and $F_{32/192}^{(B',e_2)}$ boxes are formed with the extension box **E** described as follows:

Let the 32 bits of the right branch $B = (L_1, L_2)$, $L_1, L_2 \in \{0, 1\}^{16}$. Controlling vector $V = (V_1, Z_1, V_2, Z_2, V_3, Z_3, V_4, Z_4, V_5, Z_5, V_6, Z_6)$, formed as follows:

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

$Z_1=L_1^{<<<6}$, $Z_2=L_1^{<<<12}$, $Z_3=L_1$; $Z_4=L_2$, $Z_5=L_2^{<<12}$, $Z_6=L_2^{<<<6}$;

We construct structure of the $\mathbf{S}_i$ box is involution substitution-permutation network (Figure 8). It is a SPN constructed using the P_1, P_2, and P_3 permutations (specified in table 2) 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,…, S_7 boxes of MD-64 in order to inspire a high level of public confidence that no trapdoor are inserted in MD-64. Similar justification of the S-boxes selection has been earlier used in the design of the Serpent cipher [13].

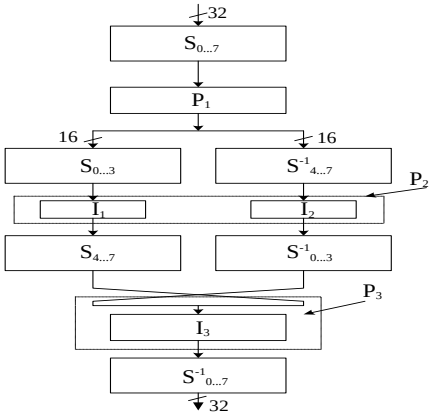


Figure 8. Structure of the $\mathbf{S}_i$ box.

TABLE I. KEY SCHEDULING AND SPECIFICATION OF THE SWITCHING BIT E' AND E''

j	1	2	3	4	5	6	7	8	FT
Q_j	K_1	K_2	K_3	K_4	K_4	K_1	K_2	K_3	K_1
U_j	K_3	K_3	K_2	K_1	K_4	K_4	K_3	K_2	K_3
e'	1	0	1	1	0	1	0	0	-
e''	0	0	1	0	1	1	0	1	-

TABLE II. 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)

V. SECURITY ESTIMATIONS

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 MD-64 cipher with respect to the following four dependence criteria [14, 15]:

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 MD-64 algorithm show in table 3 and 4.

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	21.910	0.7500	0.6835	0.6928
2	31.994	1.0000	0.9994	0.9960
3	32.000	1.0000	0.9997	0.9961
4	31.999	1.0000	0.9997	0.9961
5	32.000	1.0000	0.9996	0.9961
6	32.001	1.0000	0.9997	0.9960
7	31.999	1.0000	0.9997	0.9961
8	32.002	1.0000	0.9996	0.9960

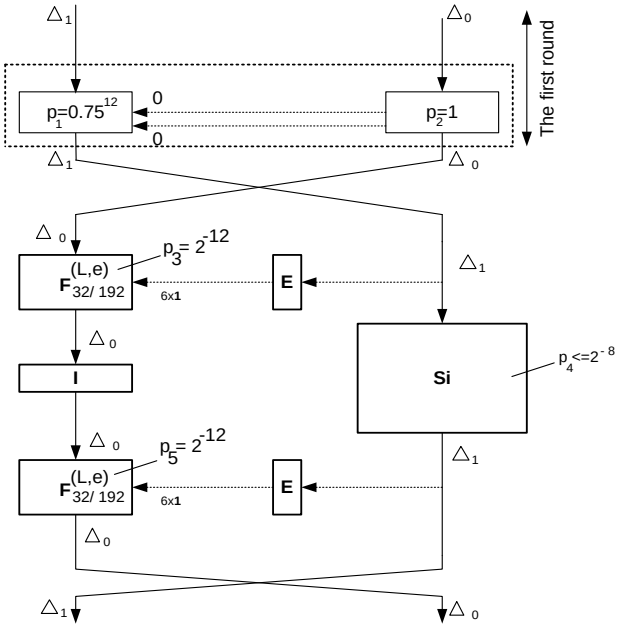
TABLE IV. THE VALUES FOR CRITERIA 1-4 ON THE INFLUENCE OF KEY BITS ON THE TRANSFORMED TEXT (FOR VARIOUS NUMBERS OF ROUNDS)

Number of rounds	$\#K = 100$ $\#X = 100$			
	(1) = d_1	(2) = d_c	(3) = d_a	(4) = d_{sa}
11.650	0.3628	0.3512	0.3487	21.910
27.501	0.8750	0.8600	0.8505	31.994
31.996	1.0000	0.9994	0.9960	32.000
32.000	1.0000	0.9996	0.9960	31.999
32.001	1.0000	0.9996	0.9961	32.000
32.000	1.0000	0.9997	0.9960	32.001
32.002	1.0000	0.9996	0.9960	31.999
31.999	1.0000	0.9996	0.9961	32.002

Our research results have shown that three rounds of MD-64 are sufficient to satisfy the test criteria (d_c =1, $d_a \approx 1$, $d_{sa} \approx 1$). Thus, MD-64 possesses good statistical properties like that of AES finalists.

Formation scheme of the two-round differential characteristic (DC) with the difference $(\Delta^A_1, \Delta^B_0) \rightarrow (\Delta^A_1, \Delta^B_0)$ is presented in figure 9. More precisely, one active bit Δ^A_1 passes through the first round with probability $P_1(\Delta^A_1 \rightarrow \Delta^A_1) = p_1 p_2 = (P(ijk))^{12} = (P(110))^{12} = 0.75^{12} \approx 2^{-5}$, while one active bit Δ^B_1 passes through the second round with probability $P_2(\Delta^B_1 \rightarrow \Delta^B_1) = p_3 p_4 p_5 = (P(001))^{12} P((\Delta^B_1 \xrightarrow{Si} \Delta^B_1) \leq 2^{-32}$.

Experimental studies also showed that one active bit passes through the two round $P(2) \approx 2^{-38}$. More precisely, one active bit Δ^A_1 passes through the first round with probability $P_1(\Delta^A_1 \rightarrow \Delta^A_1) \approx 2^{-5}$, while one active bit Δ^B_1 passes through the second round with probability $P_2(\Delta^B_1 \rightarrow \Delta^B_1) \approx 2^{-33}$.



Formation of the two-round iterative differential characteristic with the difference $(\Delta^A_1, \Delta^B_0) \rightarrow (\Delta^A_1, \Delta^B_0)$ with probability $P_2 \leq 2^{-37}$

Figure 9 shows that the probability of the existence of the differential trail after the second round is less than 2^{-37} and after the fourth round the probability of the differential trail is less than 2^{-74} 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.

In table 5, we present results of probability of breaking ciphers with differential cryptanalysis.

TABLE V. DIFFERENRTIAL CRYPTANALYSIS SECURITY ESTIMATION COMPARISION

Cipher	*R*max	*R*	*p*
Camelia	24	3	2^{-12}
DES	16	2	2^{-7}
Cobra-F64a [16]	16	3	2^{-21}
Spectr-H64 [17]	12	2	1.15×2^{-13}
MD-64 (proposed)	8	2	$< 2^{-37}$

*R*max: the maximum number of rounds; *R*: the number of rounds; *p*: the probability of attack success.

These results show that proposed cipher is less vulnerable to attacks when compared to DES or Camellia.

VI. FPGA SYNTHESIS RESULT AND COMPARISIONS

Hardware implementations of proposed cipher are designed and coded in VHDL language. The MD-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 FPGA implementation are illustrated in table 6. In the same table comparisons with the most widely used WSNs are given.

TABLE VI. FPGA SYNTHESIS RESULTS AND COMPARISONS

Block ciphers	Block size (bit)	F (Mhz)	Area (CLBs)	Rate (Mbps)
MD-64 (proposed)	64	95	500	760
AES [18]	128	22	2358	259
DES [19]	64	125	741	402

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

VII. CONCLUSION

In this paper, we propose a new fast cipher MD-64. This cipher is based on SDDO transformations. Security analysis has show that the cipher is secure against know attacks.

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 WSNs.

REFERENCES

[1] Hu F, Ziobro J, Tillett J, Sharma N. K, "Secure wireless sensor networks: problems and solutions," J. Syst., Cybern. Inf., 11(9):419-439, 2004.

[2] Saraogi M, "Security in Wireless Sensor Networks," Project Paper at Computer and Network Security, Sections 494/4 594/9. University of Tennesse, 2006.

[3] Mauw S, Vessem I, Bos B, "Forward secure communication in wireless sensor networks," LNCS, 3934:32-42, 2006.

[4] Kumar S, Valdez R, Gomez O, Bose S, "Survivability Evaluation of Wireless Sensor Network under DdoS Attack," ICN/ICONS/MCL, Mauritius, p.82, 2006.

[5] Bilstrup U, Sjoberg K, Svensson B, Wiberg P. A, "Capacity Limitations in Wireless Sensor Networks," Proc. 9th IEEE Int. Conf. on Emerging Technologies and Factory Automation, Lisbon, Portugal, p.529-536, 2003.

[6] A. A. Moldovyan and N. A. Moldovyan, "A cipher based on data dependent-permutations," Journal of Cryptology, vol.15, no.1 (2002), pp.61-72.

[7] N. A. Moldovyan and A. A. Moldovyan, Innovative cryptography. Charles River Media, 2006, 380 pp.

[8] N. A. Moldovyan, "On Cipher Design Based on Switchable Controlled operations," Springer-Verlag LNCS, vol.2776 (2003), pp.316-327.

[9] N. Sklavos and O. Koufopavlou, "Architectures and FPGA Implementations of the SCO (-1,-2,-3) Ciphers Family," Proceedings of the of 12th International Conference on Very Large Scale Integration, (IFIP VLSI SOC' 03), Darmstadt, Germany, December1-3, 2003.

[10] Biham E, Shamir A, 1993. Differential cryptanalysis of the full 16-round DES. LNCS, 740:487-496.

[11] Matsui M, "Linear cryptanalysis method for DES cipher," LNCS, 765:386-397, 1994.

[12] Schneier B, Applied Cryptography: Protocols, Algorithms, and Source Code (2nd Ed.). John Wiley & Sons, New York, 1996, p.758.

[13] R. Anderson, E. Biham, L. Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard," 1st Advanced Encryption Standard Candidate Conference Proceedings, Venture, California, Aug. 20-22, 1998.

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

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

[16] Lu J. Q, Lee C. H, Kim J. S, "Related-key attacks on the full-round Cobra-F64a and Cobra-F64b," LNCS, 4116:95-110, 2006.

[17] N. D. Goots, B. V. Izotov, A. A. Moldovyan, and A. N. Moldovyan, "Fast Ciphers for Cheap Hardware: Differential Analysis of SPECTR-H64," Springer-Verlag LNCS 2776 (2003) 449–452.

[18] 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.

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

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

Nguyen Hieu Minh 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 25 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). .

Do Thi Bac 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).

Ho Ngoc Duy is a Lecturer with the Military Technical Academy (Ha Noi, Viet Nam). His research interests include cryptography, communication and network security. He received his Diploma from the Saint Petersburg Electrical Engineering University (2009).