Applied Mathematical Sciences, Vol. 7, 2013, no. 140, 6945 - 6960
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2013.310584

Security Evaluation of the SPECTR-128 Block Cipher

Manh Tuan Pham, Lam T. Vu

Posts and Telecommunications Institute of Technology
122 Hoang Quoc Viet Street, Ha Noi, Viet Nam
tuanpm.129@gmail.com

Moldovyan N.A., Morozova E.V.

St. Petersburg Institute for Informatics and Automation
of Russian Academy of Sciences
14 Liniya, 39, St. Petersburg 199178, Russia

Minh N.H., Cuong N.V., and Manh T.C.

Le Quy Don Technical University
100 Hoang Quoc Viet, Ha Noi, Viet Nam

Abstract

The evaluation of availability in resistant to differential and linear cryptanalytic attacks is essential in designing secure block ciphers. In this paper, we present evaluated results of security estimation for SPECTR-128 block cipher. The results show that SPECTR’-128 (modified version of SPECTR-128) is a highly-resistant to differential and linear cryptanalytic attacks.

Keywords: Controlled permutations (CP), data-dependent permutations (DDP), internal key scheduling (IKS), differential cryptanalysis (DC), linear cryptanalysis (LC).

1 Introduction

SPECTR-128 is a block cipher proposed by Moldovyan N.A in [1]. The specification of SPECTR-128 can be found in [1]. An overview of its architecture is given in Fig. 1.

This cipher is based on extensive use of CP-box operations. The left data subblock is used to specify the permutations on the right data subblock and round-subkey. The use of two mutually inverse DDP performed sequentially on the right subblock allows one to perform enciphering and deciphering with the same algorithm. A single-layer CP-box is used to quickly change the key schedule while changing encryption mode for decryption one. A peculiarity of SPECTR-128 is the use of the data-dependent transformation of round subkeys (so called internal key scheduling [2] - IKE). It is based on a combination of DDP and special fast operation G [3, 4] in order to greatly reduce the effectiveness of differential and linear cryptanalysis.

This paper provides the results of a cryptographic evaluation of SPECTR-128 (SPECTR'-128).

This paper is organized as follows. In Section 2, we briefly present 128-bit cipher SPECTR-128. Sections 3 and 4 present differential and linear cryptanalytic attacks of SPECTR-128, respectively. Finally, we conclude in Section 5.

2 Description of SPECTR-128

SPECTR-128 is a new 12-round block cipher with 128-bit input. The general encryption scheme is defined by the following formulas: $C = \mathbf{Encr}(M, K)$ and $M = \mathbf{Decr}(C, K)$, where M is the plaintext, C is the cipher text $(M, C \in \{0,1\}^{128})$, K is the secret key $(K \in \{0,1\}^{256})$, **Encr** is the encryption function, and **Decr** is the decryption function. In the block cipher SPECTR-128 encryption and decryption functions are described by formula $Y = \mathbf{F}(X, Q^{(e)})$, where $Q^{(e)} = \mathbf{H}(K, e)$ is the extended key (EK), the last being a function of the secret key $K = (K_1, ..., K_4)$ and of the transformation mode parameter e ($e = 0$ defines encryption, $e = 1$ defines decryption). We have $X = M$, for $e = 0$ and $X = C$ for $e = 1$. EK is represented as concatenation of 14 subkeys: $Q^{(e)} = (Q_{IT}^{(e)}, Q_1^{(e)}, ..., Q_{12}^{(e)}, Q_{FT}^{(e)})$ where $Q_{IT}^{(e)}, Q_{FT}^{(e)} \in \{0,1\}^{64}$ and $\forall j = 1, ..., 12$, $Q_j^{(e)} = (Q_j^{(1,e)}, ..., Q_j^{(4,e)})$, where $\forall h = 1, ..., 4$, $Q_j^{(h,e)} \in \{0,1\}^{64}$. Output value Y is the ciphertext C in the encryption mode or the plaintext M in the decryption mode.

The algorithm is designed as sequence of the following procedures [1]: 1) *initial transformation***IT**, 2) 12 rounds with procedure **Crypt**, and 3) *final transformation***FT**. Ciphering begins with the procedure **IT**: $Y' = \mathbf{IT}(X, Q_{IT}^{(e)})$. Then data block Y' is divided into two 64-bit blocks L_0 and R_0, i.e. $(L_0, R_0) = Y'$, where $L_0, R_0 \in \{0,1\}^{64}$. Then twelve sequential rounds are performed with procedures **Crypt** in accordance with the formulas: $L_j = \mathbf{Crypt}(R_{j-1}, L_{j-1}, Q_j^{(e)})$; $R_j = L_{j-1}$, where $j = 1, \ldots, 12$. Then the final transformation **FT** is executed: $Y = \mathbf{FT}(X, Q_{FT}^{(e)})$, where $X = (R_{12}, L_{12})$. The general encryption scheme is shown in Figure 1.

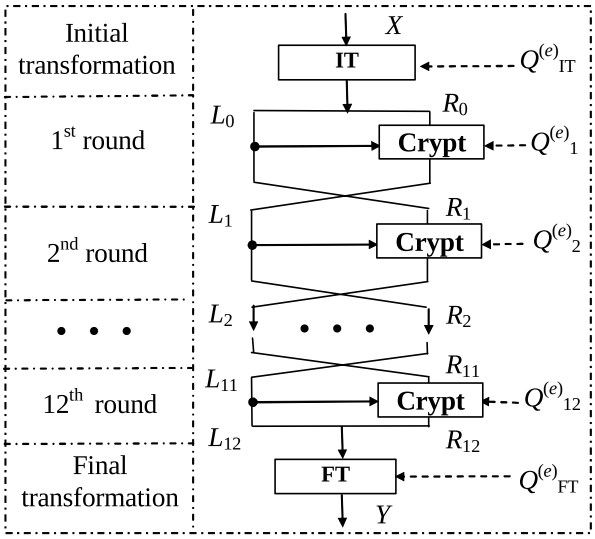

Figure1. General structure of SPECTR-128

The structure of the procedure Crypt is shown in Figure 2.

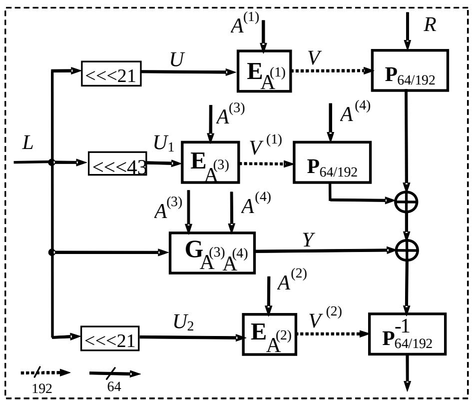

Figure2. Structure of the procedure Crypt

This procedure has the form: R = **Crypt** (R, L, $A^{(1)}$, $A^{(2)}$, $A^{(3)}$ and $A^{(4)}$) where R, L, $A^{(1)}$, $A^{(2)}$, $A^{(3)}$, $A^{(4)} \in \{0,1\}^{64}$. Thus, **Crypt** transforms the data subblock R under control of the data subblock L and 256-bit extendedsubkey. This procedure uses the following operations: to-left cyclic rotation “<<<” by fixed number of bits, XOR operation “⊕”, non-linear operation **G**, DDP operations $\mathbf{P}_{64/192}$ and $\mathbf{P}^{-1}_{64/192}$, and extension operation **E**.

For the block cipher SPECTR-128 see more details in [1].

3 Differential Cryptanalysis

3.1 Some properties of the controlled operations

Let Δ_q^W be the difference with arbitrary q active (non-zero) bits corresponding to the vector W. Let $\Delta_{q|i_1,\dots,i_q}$ be the difference with q active bits and $i_1,\dots,i_q$ be the numbers of digits corresponding to active bits. Note that Δ_1 corresponds to one of the differences $\Delta_{1|1}$, $\Delta_{1|2}$, …,$\Delta_{1|64}$. Let $P(\Delta_q \xrightarrow{\mathbf{F}} \Delta'_g)$ be the probability that input difference Δ_q transforms into output difference Δ'_g while passing some operation **F**. We shall also denote the event that at the output or input of the operation **F** we have the difference Δ_q as $\Delta_q^{\mathbf{F}}$ or $\Delta_q^{\mathbf{F}\downarrow}$ respectively.

Differential properties of the CP boxes with the given structure are defined by properties of the elementary switching element. Using the main properties of the last (see Figure 3) it is easy to find characteristics of the $\mathbf{P}_{64/192}$-box. Table 1 presents probabilities of different output differences corresponding to differences $\Delta_{q'}^L$ and Δ_q^R with few active bits ($q', q \in \{0,1,2\}$).

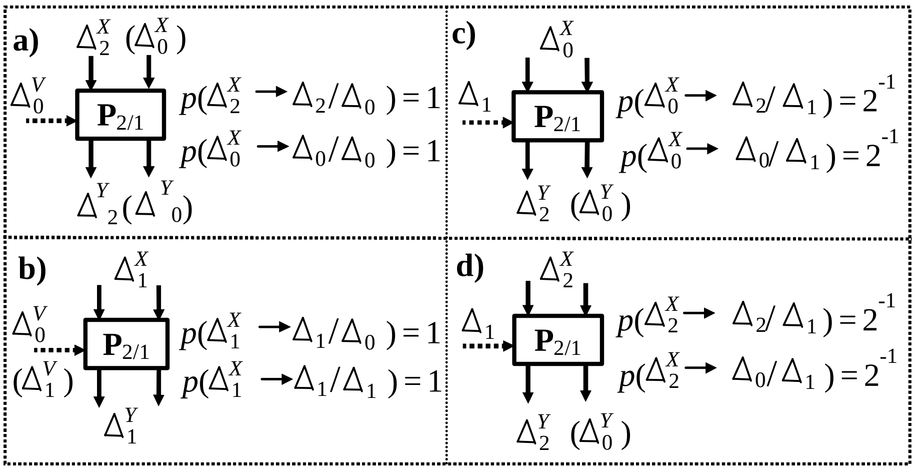

Figure3. Properties of the elementary box $\mathbf{P}_{2/1}$

Figure 3 illustrates the case when some difference with one active bit Δ_q^L passes the left branch of the crypto scheme. The difference Δ_q^L can cause generation or annihilation of *w* pairs of active bits in the CP box. Let consider the $\mathbf{P}_{64/192}$-box in right branch in the case $q = 1$. The difference Δ_1^L is transformed by the extension box into Δ_3^V at the controlling input of $\mathbf{P}_{64/192}$, i.e. one active bit in the left sub-block influences three switching elements $\mathbf{P}_{2/1}$ permuting six different bits of the right data subblock.Depending on value of the permuted bits and input difference Δ_q^R of the $\mathbf{P}_{64/192}$-box the output differences $\Delta_g'^R$ with different number of active bits can be formed by this CP box.

Table1. Values of probability $P\left((\Delta_q^R \xrightarrow{\mathbf{P}_{64/192}} \Delta_g'^R) / \Delta_{q'}^L\right)$

	$\Delta_0^R \to \Delta_0'^R$	$\Delta_0^R \to \Delta_2'^R$	$\Delta_0^R \to \Delta_4'^R$	$\Delta_0^R \to \Delta_6'^R$	$\Delta_1^R \to \Delta_1'^R$	$\Delta_1^R \to \Delta_3'^R$	$\Delta_1^R \to \Delta_5'^R$
Δ_0^L	1	0	0	0	1	0	0
Δ_1^L	2^{-3}	$1.5\cdot 2^{-2}$	$1.5\cdot 2^{-2}$	2^{-3}	$1.1\cdot 2^{-3}$	$1.55\cdot 2^{-2}$	$1.45\cdot 2^{-2}$
Δ_2^L	2^{-6}	$1.5\cdot 2^{-4}$	$1.88\cdot 2^{-3}$	$1.25\cdot 2^{-2}$	$1.19\cdot 2^{-6}$	$1.69\cdot 2^{-4}$	2^{-2}

	$\Delta_1^R \to \Delta_7'^R$	$\Delta_2^R \to \Delta_0'^R$	$\Delta_2^R \to \Delta_2'^R$	$\Delta_2^R \to \Delta_4'^R$	$\Delta_2^R \to \Delta_6'^R$	$\Delta_2^R \to \Delta_8'^R$
Δ_0^L	0	0	1	0	0	0
Δ_1^L	$0.91\cdot 2^{-3}$	$1.52\cdot 2^{-13}$	$1.11\cdot 2^{-3}$	$1.42\cdot 2^{-2}$	$1.27\cdot 2^{-2}$	$1.64\cdot 2^{-4}$
Δ_2^L	$1.25\cdot 2^{-2}$	$1.52\cdot 2^{-15}$	$1.1\cdot 2^{-6}$	$1.51\cdot 2^{-4}$	$1.72\cdot 2^{-3}$	$1.05\cdot 2^{-2}$

Avalanche effect corresponding to the operations **G** is defined by its structure that provides each input bit influences several (*u*) output bits (except the 64th input bit influences only the 64th output bit). Table 2 presents the formulas describing avalanche caused by inverting the bit l_i. Let Δl_i denote alteration of l_i. We shall consider the case when the data and key are uniformly distributed random values. One can see that l_i, where $7 \le i \le 55$, causes deterministic alteration of the output bit y_i and probabilistic alteration of the output bits y_{i+1}, y_{i+3}, $y_{i+6}, \ldots, y_{i+9}$ which change with probability $p = 0.5$ (for $1 \le i \le 6$ we have deterministic alteration of y_i and y_{i+3}, since $\Delta y_{i+3} = \Delta l_i l_{i-6}$). When passing through the operation **G** the difference $\Delta_{1|i}^L$ can be transformed with certain probability to the output differences $\Delta_{1|i}^Y$, Δ_2^Y, ..., Δ_7^Y (see Tables 3 and 4).

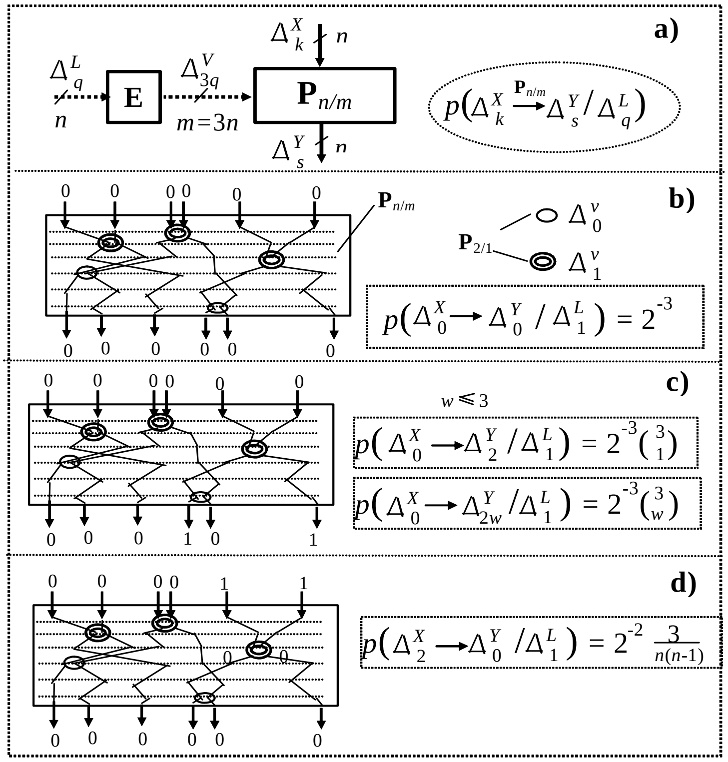

Figure 4. Some properties of the CP box: a - notation of the general case; b - zero difference passes the CP box; c - formation of two active bits; d - annihilation of two active bits.

Table 2. Changing output bits caused by single bit alteration (Δl_i=1) at input of the operation G

#	Expression	Probability
1	$\Delta y_i = \Delta l_i$	$p(\Delta y_i = 1) = 1$
2	$\Delta y_{i+1} = \Delta l_i (a_{i-1}^{(4)} \oplus a_{i-1}^{(3)} l_{i-8} \oplus a_i^{(4)} l_{i-5} l_{i-8})$	$p(\Delta y_{i+1} = 1) = 1/2$
3	$\Delta y_{i+2} = 0$	$p(\Delta y_{i+2} = 1) = 0$
4	$\Delta y_{i+3} = \Delta l_i l_{i-6}$	$p(\Delta y_{i+3} = 1) = 1/2$
5	$\Delta y_{i+4} = 0$	$p(\Delta y_{i+4} = 1) = 0$
6	$\Delta y_{i+5} = 0$	$p(\Delta y_{i+5} = 1) = 0$
7	$\Delta y_{i+6} = \Delta l_i (l_{i-2} \oplus l_{i-3} l_{i+5} a_{i+5}^{(4)})$	$p(\Delta y_{i+6} = 1) = 1/2$
8	$\Delta y_{i+7} = \Delta l_i a_{i+5}^{(3)}$	$p(\Delta y_{i+7} = 1) = 1/2$
9	$\Delta y_{i+8} = \Delta l_i l_{i+2}$	$p(\Delta y_{i+8} = 1) = 1/2$
10	$\Delta y_{i+9} = \Delta l_i (l_{i+6} \oplus l_{i+8} a_{i+7}^{(3)} \oplus l_{i+3} l_{i+8} a_{i+8}^{(4)}$	$p(\Delta y_{i+9} = 1) = 1/2$

Table3. Values of the probability $P(\Delta^L_{1|i} \xrightarrow{G} \Delta^Y_g)$

i	$\Delta^L_{1\|i} \to \Delta^Y_{1\|i}$	$...\Delta^Y_2$	$...\Delta^Y_3$	$...\Delta^Y_4$	$...\Delta^Y_5$	$...\Delta^Y_6$	$...\Delta^Y_7$
1-6	-	2^{-5}	$1.25\cdot2^{-3}$	$1.25\cdot2^{-2}$	$1.25\cdot2^{-2}$	$1.25\cdot2^{-3}$	2^{-5}
7-55	2^{-5}	$1.5\cdot2^{-4}$	$1.875\cdot2^{-3}$	$1.25\cdot2^{-2}$	$1.875\cdot2^{-3}$	$1.5\cdot2^{-4}$	2^{-6}
56	2^{-5}	$1.25\cdot2^{-3}$	$1.25\cdot2^{-2}$	$1.25\cdot2^{-2}$	$1.25\cdot2^{-3}$	2^{-5}	-
57	2^{-4}	2^{-2}	$1.5\cdot2^{-2}$	2^{-2}	2^{-4}	-	-
58	2^{-3}	$1.5\cdot2^{-2}$	$1.5\cdot2^{-2}$	2^{-3}	-	-	-
59-61	2^{-2}	2^{-1}	2^{-2}	-	-	-	-
62,63	2^{-1}	2^{-1}	-	-	-	-	-
64	1	-	-	-	-	-	-

Table 4. Values of the probability $P(\Delta^L_{1|i} \xrightarrow{G} \Delta^Y_{2|i,i'})$

i	u	$\Delta^L_{1\|i} \to \Delta^Y_{2\|i,i+1}$	$...\Delta^Y_{2\|i,i+3}$	$...\Delta^Y_{2\|i,i+6}$	$...\Delta^Y_{2\|i,i+7}$	$...\Delta^Y_{2\|i,i+8}$	$...\Delta^Y_{2\|i,i+9}$
1-6	7	-	2^{-5}	-	-	-	-
7-55	7	2^{-6}	2^{-6}	2^{-6}	2^{-6}	2^{-6}	2^{-6}
56	6	2^{-5}	2^{-5}	2^{-5}	2^{-5}	2^{-5}	-
57	5	2^{-4}	2^{-4}	2^{-4}	2^{-4}	-	-
58	4	2^{-3}	2^{-3}	2^{-3}	-	-	-
59-61	3	2^{-2}	2^{-2}	-	-	-	-
62-63	2	2^{-1}	-	-	-	-	-
64	1	-	-	-	-	-	-

3.2 Differential analysis

Our best variant of the differential cryptanalysis (DCA) [5, 6] of SPECTR-128 corresponds to two-round characteristic with difference (Δ^L_0, Δ^R_1). This difference passes two rounds in the following way (see Figure 5). It is easy to see that this difference passes the first round with probability 1 and after swapping subblocks it transforms to (Δ^L_1, Δ^R_0). In the second round the active bit passing through the left branch of crypto scheme can form at the output of the operation **G** the difference Δ^Y_g, where $g \in \{1,2,3,4,5,6,7\}$. Only differences with even number of active bits contribute to the probability of the two round iterative characteristic. The most contributing are the differences $\Delta^{Y}_{2|i,i+k}$. The most contributing mechanisms of the formation of the two-round characteristic belong to Cases 1, 2, and 3, where $i\in\{1,\ldots, 64\}$ and $k\in\{1,3,6,7,8,9\}$, described below.

Case 1:

- Difference $\Delta^{Y}_{2|i,i+k}$ is formed with probability $p_2^{(i,i+k)} = \Pr\left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right)$ at the output of the operation **G**.
- Difference $\Delta'_{2|i,i+k}$ is formed with probability $p_3^{(i,i+k)} = \Pr\left(\Delta^{\mathbf{P}'}_{2|i,i+k} / \Delta^{\mathbf{P}'\downarrow}_{0}\right)$ at the output of the CP box **P’**.
- Difference Δ''_0 is formed with probability $p_1 = 2^{-3} = \Pr\left(\Delta^{\mathbf{P}''}_{0} / \Delta^{\mathbf{P}''\downarrow}_{0}\right)$ at the output of the CP box **P”**.
- After XORing differences $\Delta^{Y}_{2|i,i+k}$, $\Delta'_{2|i,i+k}$, and Δ''_0 we have zero difference Δ_0 at the input of the $\mathbf{P}^*$-box. It passes this box with probability $p_4 = 2^{-3} = \Pr\left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{0}\right)$.

One can denote Case 1 as set of the following events:

$$\left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right)\bigcap\left(\Delta^{\mathbf{P}'}_{2|i,i+k} / \Delta^{\mathbf{P}'\downarrow}_{0}\right)\bigcap\left(\Delta^{\mathbf{P}''}_{0} / \Delta^{\mathbf{P}''\downarrow}_{0}\right)\bigcap\left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{0}\right).$$

Using such form of representation one can describe the following two cases:

Case 2: $\left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right)\bigcap\left(\Delta^{\mathbf{P}''}_{2|i,i+k} / \Delta^{\mathbf{P}''\downarrow}_{0}\right)\bigcap\left(\Delta^{\mathbf{P}'}_{0} / \Delta^{\mathbf{P}'\downarrow}_{0}\right)\bigcap\left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{0}\right).$

Case 3: $\left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right)\bigcap\left(\Delta^{\mathbf{P}'}_{0} / \Delta^{\mathbf{P}'\downarrow}_{0}\right)\bigcap\left(\Delta^{\mathbf{P}''}_{0} / \Delta^{\mathbf{P}''\downarrow}_{0}\right)\bigcap\left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{2|i,i+k}\right).$

Values $p_1^{(i,i+k)}$, $p_3^{(i,i+k)}$, and $p_4^{(i,i+k)}$ are calculated in the similar way using the structure of the box $\mathbf{P}_{64/192}$ and distribution of the controlling bits over elementary switching boxes $\mathbf{P}_{2/1}$ (this distribution is defined by Table A-2 and operation “>>>21”). For example, let us consider the mostly contributing difference $\Delta^{L}_{1|43}$ while calculating $p_3^{(i,i+k)}$. After being rotated by 21 bits this difference induces the difference $\Delta^{V}_{3} = \Delta^{V}_{3|109,133,182}$ at the 192-bit controlling input of the CP box $\mathbf{P}_{64/192}$ transforming the right data subblock R. The 43d bit of L controls one elementary box $\mathbf{P}_{2/1}$ in each of three lower active layers of the CP box $\mathbf{P}_{64/192}$, namely the 109th, 133d, and 182nd boxes $\mathbf{P}_{2/1}$ (such elementary boxes can be called active). For i = 43 we have six variants of $\Delta^{Y}_{2|i,j}$: $\Delta^{Y}_{2|43,44}$, $\Delta^{Y}_{2|43,46}$, $\Delta^{Y}_{2|43,49}$, $\Delta^{Y}_{2|43,50}$, $\Delta^{Y}_{2|43,51}$, and $\Delta^{Y}_{2|43,52}$. For the corresponding probabilities $p_3^{(i,j)}$ we have zero value, except $p_3^{(43,44)} = 2^{-3}$. The last value takes into account that the 109th and 133d boxes $\mathbf{P}_{2/1}$ do not generate non-zero output difference and the 182nd one generates two active bits.

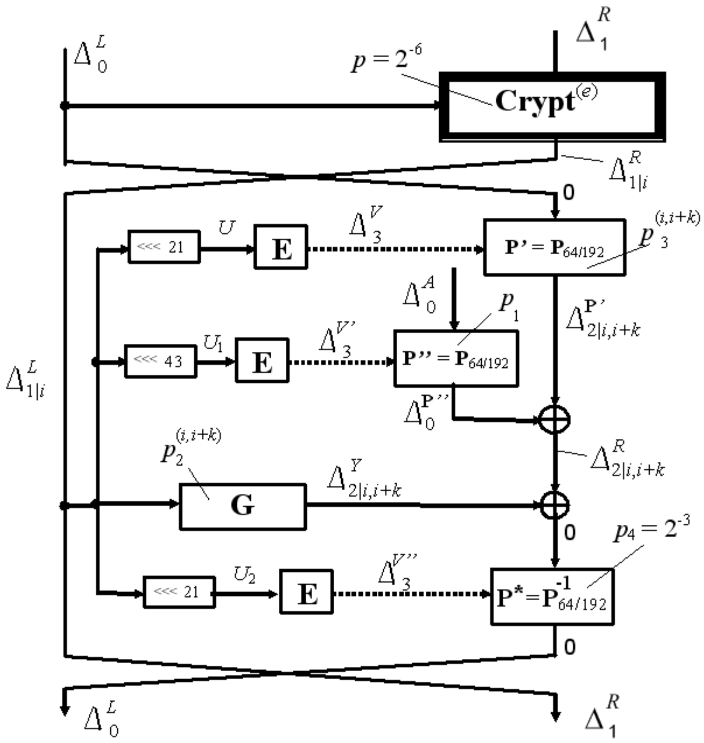

Figure 5. Formation of the two-round differential characteristic in Case 1

Taking into account the symmetric structure of the round transformation and symmetry of the boxes $\mathbf{P}_{64/192}$ and $\mathbf{P}^{-1}_{64/192}$ it is easy to see that $P''' = P'$, where P' and P''' are the contributions to the probability of the two-round differential characteristic corresponding to the first and third cases. Thus, it is sufficient to calculate P' and the contribution P'' of the second case. Due to different rotations before extension boxes corresponding to CP-box operations $\mathbf{P'}$ and $\mathbf{P''}$ we have $P'' \neq P'$.

Probability P' can be calculated using the following formula: $P' = p(i)\sum_{i,k} p_1 p_2^{(i,i+k)} p_3^{(i,i+k)} p_4 = 2^{-12} \sum_{i,k} p_2^{(i,i+k)} p_3^{(i,i+k)} \approx 1.5 \cdot 2^{-21}$, where $p(i) = 2^{-6}$ corresponds to probability that after the first round active bit moves to the ith digit. The value P' is defined mainly by the digit $i = 43$ (about 70 %) for which we have $p_3^{(43,44)} = 2^{-3}$. About 15% corresponds to digits $i = 33$ and $i = 34$ and about 15% correspond to digits i = 3,7,8,11,12,15,16,20,54. For all other digits we have zero contribution to P'.

Probability P'' can be calculated analogously to the case of P': $P'' = p(i)\sum_{i,k} p_1^{(i,i+k)} p_2^{(i,i+k)} p_3 p_4 \approx 1.5 \cdot 2^{-21}$. The digits contributing to P'' are only the following: $i = 54, 57$ ($p_1^{(54,55)} = p_1^{(57,60)} = 2^{-5}$), and i = 9,10,11,44

$(p_1^{(9,15)} = p_1^{(9,16)} = p_1^{(10,13)} = p_1^{(10,16)} = p_1^{(11,14)} = p_1^{(44,45)} = p_1^{(44,47)} = 2^{-7})$. Due to symmetry of the boxes $\mathbf{P}'$ and $\mathbf{P}^*$ there are possible contributing events (analogous to Cases 1 - 3) including generation of the additional pair of active bits in $\mathbf{P}'$ and annihilation of these bits in $\mathbf{P}^*$. The contribution of such events is $P_0 \approx 1.1 \cdot 2^{-21}$. *For probability of the two-round characteristic we have* $P(2) \approx P' + P'' + P''' + P_0 \approx 1.4.2^{-19}$.

3.3 Modified version SPECTR'-128

Differential analysis has shown that the structure of the extension box (i.e. the table describing distribution of the bits of the left data subblock over elementary switching elements of the CP boxes) is a critical part of SPECTR-128. It is easy to see that small change in the extension box leads to significant decrease or increase of the probability of two-round characteristic. Indeed, we can reduce the probability P(2) by factor $\approx 2^8$ using the extension box described by the Table 5.

Table 5. Distribution of bits of the vector *U*

V_1	33	34	35	36	37	38	39	40	41	42	43	44	62	63	34	60	35	36	37	43	44	54	55	56	57	58	59	60	61	62	63	64	V_1
V_2	50	41	52	53	42	61	56	57	61	38	48	55	45	46	47	49	64	49	50	51	38	39	40	41	42	48	53	45	46	47	52	33	V_2
V_3	58	59	45	58	62	49	64	63	33	51	52	53	54	55	39	54	57	46	44	60	43	47	48	50	34	35	36	37	59	56	40	51	V_3
V_4	26	27	28	29	1	19	10	17	18	31	20	21	14	23	24	25	32	11	8	9	22	15	16	30	2	3	4	5	6	7	12	13	V_4
V_5	18	19	20	21	14	23	24	25	26	27	28	29	30	31	32	17	2	3	4	5	6	7	8	9	10	1	12	13	22	15	16	11	V_5
V_6	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	28	23	24	25	26	27	22	29	30	31	32	V_6

Let call the modified version SPECTR'-128. For SPECTR'-128 cases 1, 2, and 3 give zero contribution to the probability of two-round characteristic. After modification of **E**-box the most contributing cases are the following ($\forall i,t,k\ i,t \in \{1,2,...,64\}$, $k \in \{1,3,6,7,8,9\}$, $t \neq i$, and $t \neq i+k$).

$$\text{Case 4a}: \left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right) \bigcap \left(\Delta^{\mathbf{P}'}_{2|i+k,t} / \Delta^{\mathbf{P}'\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}''}_{2|i,t} / \Delta^{\mathbf{P}''\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{0}\right).$$

$$\text{Case 4b}: \left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right) \bigcap \left(\Delta^{\mathbf{P}'}_{2|i,t} / \Delta^{\mathbf{P}'\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}''}_{2|i+k,t} / \Delta^{\mathbf{P}''\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{0}\right).$$

$$\text{Case 5a}: \left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right) \bigcap \left(\Delta^{\mathbf{P}'}_{0} / \Delta^{\mathbf{P}'\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}''}_{2|i+k,t} / \Delta^{\mathbf{P}''\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{2|i,t}\right).$$

$$\text{Case 5b}: \left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right) \bigcap \left(\Delta^{\mathbf{P}'}_{0} / \Delta^{\mathbf{P}'\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}''}_{2|i,t} / \Delta^{\mathbf{P}''\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{2|i+k,t}\right).$$

$$\text{Case 6a}: \left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right) \bigcap \left(\Delta^{\mathbf{P}''}_{0} / \Delta^{\mathbf{P}''\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}'}_{2|i+k,t} / \Delta^{\mathbf{P}'\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{2|i,t}\right).$$

$$\text{Case 6b}: \left(\Delta^{\mathbf{G}}_{2|i,i+k} / \Delta^{\mathbf{G}\downarrow}_{1|i}\right) \bigcap \left(\Delta^{\mathbf{P}''}_{0} / \Delta^{\mathbf{P}''\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}'}_{2|i,t} / \Delta^{\mathbf{P}'\downarrow}_{0}\right) \bigcap \left(\Delta^{\mathbf{P}^*}_{0} / \Delta^{\mathbf{P}^*_\downarrow}_{2|i+k,t}\right).$$

Calculating the total contribution of the cases 4a, 4b, 5a, 5b, 6a, and 6b we have obtained $P(2)=1.85 \cdot 2^{-28} \approx 2^{-27}$. Thus, after modification of the extension box the value $P(2)$ has been significantly reduced. Now the three-round characteristic becomes the most efficient one. One of possible mechanisms of the formation of this characteristic is shown in Fig. 5. This characteristic does not depend on small modifications of the distribution table. In the most contributing mechanisms of the formation of the three-round characteristic in second and third rounds the operation **G** produces output difference exactly with one active bit.

To calculate probability $p_2 = p\left(\Delta_{1|i}^{\mathbf{G}} / \Delta_{1|i}^{\mathbf{G}\downarrow}\right)$ one should take into account its dependence on *i*. Let $p_2^{(i)}$ be the probability that the output difference of **G** has exactly one active bit corresponding to the*i*th digit. Probability $p_2^{(i)}$ is equal to 2^{-6} for $i\in\{7,...,55\}$, 2^{-5} for $i = 56$, 2^{-4} for$i = 56$, 2^{-3} for $i = 58$, 2^{-2} for $i\in\{59,60,61\}$, 2^{-1} for $i\in\{62,63\}$, 1 for $i = 64$, and 0 for $i\in\{1,...,6\}$. For uniformly distributed random value *i* we have the average value $p_2 \approx 0.93\cdot 2^{-4}$ while considering the operation **G** as individual unit. Probability that in the second round the **P″**-box generates no pairs of active bits is $p^{(i)}=2^{-3}$ for all *i*. The same probability corresponds to the individual boxes **P’** and **P***, however, because of their mutual symmetry one has to consider these two boxes as a single unit. Probability that they generate no pair of active bits at the output of the operation **P*** is $p_{3,4}^{(i)} \approx 2^{-6}$ for $i\in\{1,2,...,21,54,...,64\}$ and $p_{3,4}^{(i)} \approx 1.32 \cdot 2^{-5}$ for $i\in\{22,23,...,53\}$. The last value takes into account the cases of including generation, and annihilation of the pairs of active bits in the boxes **P’** and **P***. If at the input of the first round we have the difference (Δ_0^L, Δ_1^R), then at the output of the second round we have the difference (Δ_1^L, Δ_1^R) with probability $p' = 2^{-6}\sum_i p_1^{(i)} p_2^{(i)} p_{3,4}^{(i)} \approx 1.14 \cdot 2^{-13}.\dfrac{n!}{r!(n-r)!}$

In the third round the active bit passing the box **P’** is XORed with the single output active bit of the operation **G** with probability $p''=2^{-6}$ and no new active bits are formed by operations **G**, **P’**, **P”**, and **P*** with probability $p' \approx 1.14\cdot 2^{-13}$. Thus, for probability of the three-round characteristic we get $P(3)=p'^2 p'' \approx 1.3\cdot 2^{-32}$.

Contribution of the two-round characteristic to the value $P(12)$ *is* $P_{(2)}(12) = P^6(2) \approx (2^{-27})^6 = 2^{-162}$. Contribution of the three-round characteristic is $P_{(3)}(12) = P^4(3) \approx 1.4\cdot 2^{-127} >> P_{(2)}(12)$. Probability to have at output of the random cipher the difference (Δ_0^L, Δ_1^R) is equal to $2^{-122} >> P_{(3)}(12)$. *Thus, the cipher SPECTR’128 with twelve encryption rounds is undistinguishable from a random cipher with the most efficient differential characteristic.*

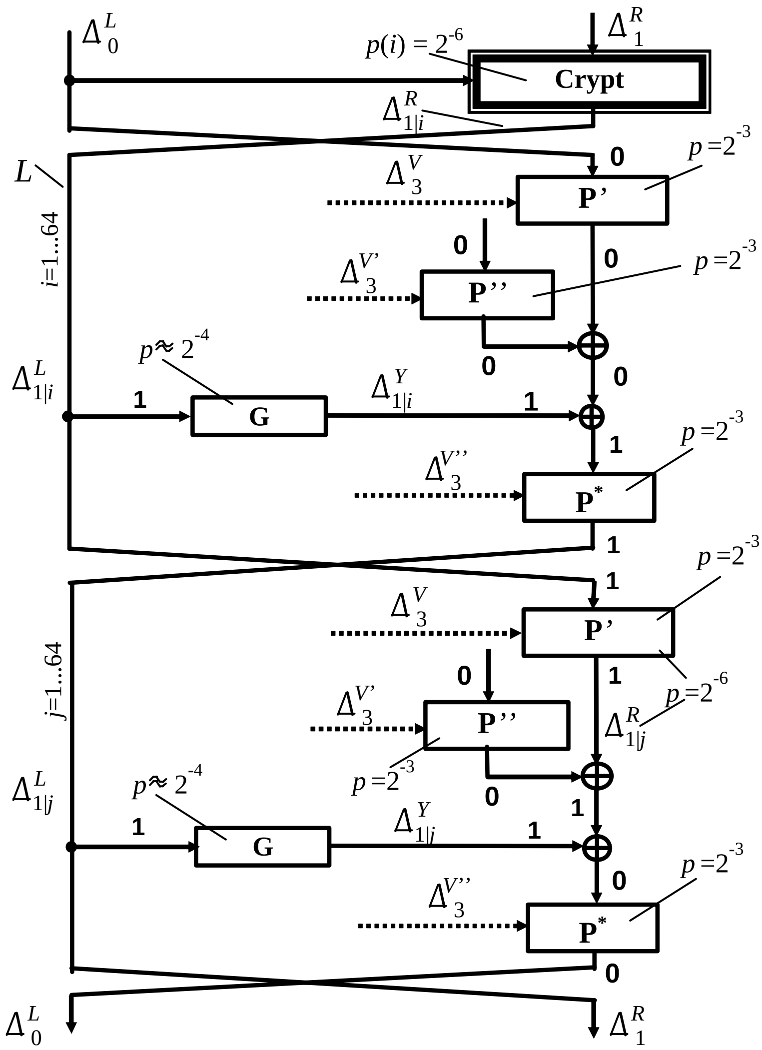

Figure 6. Formation of the three-round differential characteristic (mechanisms including generation of the active bits in the CP boxes are not shown)

4 Linear Cryptanalysis

Comparison of the known results on security estimation of the DDP-based ciphers shows that linear cryptanalysis (LCA) [7, 8] appears to be less efficient to attack DDP-based ciphers as compared with DCA. For example, to thwart the linear attack against SPECTR-H64 (DDP-64) seven [9] (three [10]) rounds are sufficient whereas to thwart the differential attack on that cipher at least ten [11] (eight [10]) rounds are required. Fixed permutations and the DDP operations are bijections that preserve the Hamming weight of the input vector, however to use this property in a linear attack one should apply masks having maximum weight. Such masks are note efficient due to non-linear operations used together with DDP. Detailed theory of the linear characteristics (LC) of the CP-boxes is presented in [9]. Let denote an input mask as M and the output mask as B. In that paper it has been shown that:

i) Bias of arbitrary LC for which $\varphi(M) \neq \varphi(B)$ is equal to zero;

ii) For the CP-boxes of the order $h \geq 1$ for $\varphi(M) = \varphi(B) \geq 1$ the bias b of the DDP operation satisfies condition $b \leq \frac{1}{2n}$ independently of the mask assigned to the controlling input of the CP-box (for the boxes $\mathbf{P}_{64/192}$ we have $b \leq 2^{-7}$) ; the value $b = \frac{1}{2n}$ corresponds to the to the masks with weight 1.

iii) Linear attacks using masks (1, 1,…, 1) are prevented efficiently with the **G-**like operations.

Performing linear analysis of the round transformation of SPECTR-128 we have found that the most efficient LC corresponds to the masks with two active bits in the left utmost positions in each of two data subblock s. Such mask works well in the case of key in whichsubkeysK_1 and K_2 as well as K_3 and K_4 contain equal bits in positions number 18, 25, 29, 50, 57. Probability to select such key is 2^{-10}. Let denote the mask corresponding to vector X as $M^{X}_{q|i_1,\dots,i_q}$, where q is the number of active bits and $i_1,\dots,i_q$ are the indices of the active bits. The LC with input $\left(M^{L_0}_{1|1}, M^{R_0}_{1|1}\right)$ and output $\left(M^{L_1}_{1|1}, M^{R_1}_{1|1}\right)$ masks of the first round has bias $b(1) \leq 2^{-7}$. The last value is calculated as follows (see fig.7). Note that for considered particular case of keys the $\mathbf{P}^*$-box moves the left most input bit to the left most digit at the output, if the **P'**-box moves the left most input bit to the left mostdigit at its output. Bias of the considered one-round LC is

$$b(1) = \left|\Pr\left(L_0 \bullet M^{L_0}_{1|1} \oplus R_0 \bullet M^{R_0}_{1|1} \oplus L_1 \bullet M^{L_1}_{1|1} \oplus R_1 \bullet M^{R_1}_{1|1} = 1\right) - \frac{1}{2}\right|.$$

If the **P'**-box moves the left umost input bit to the left umost digit at its output we have

$$\sigma = L_0 \bullet M^{L_0}_{1|1} \oplus R_0 \bullet M^{R_0}_{1|1} \oplus L_1 \bullet M^{L_1}_{1|1} \oplus R_1 \bullet M^{R_1}_{1|1} = l_{01} \oplus a^{(3)}_1 \oplus 1 \oplus z_1,$$

wherez_1 is the first bit of the vector Z at the output of the CP box **P'**. Probability of this event is $1/n = 2^{-6}$. Probability that $\sigma = l_{01} \oplus a^{(3)}_1 \oplus 1$ is t/n^2, where $t = \varphi(A^{(3)})$. If the **P'**-box moves any other input bit to the left umost digit at its output then we have $\sigma = l_{01} \oplus a^{(3)}_1 \oplus 1$ with probability $2^{-1}(1 - 1/n)$ independently of the value z_1. Thus, we have $\Pr\left(\sigma = l_{01} \oplus a^{(3)}_1 \oplus 1\right) = \frac{1}{2} - \frac{1}{2n} + \frac{t}{n^2}$ and

$$b(1) = \left|\Pr(\sigma = 1) - \frac{1}{2}\right| = \left|\Pr(\sigma = 0) - \frac{1}{2}\right| = \left|-\frac{1}{2n} + \frac{t}{n^2}\right| \leq \frac{1}{2n}.$$

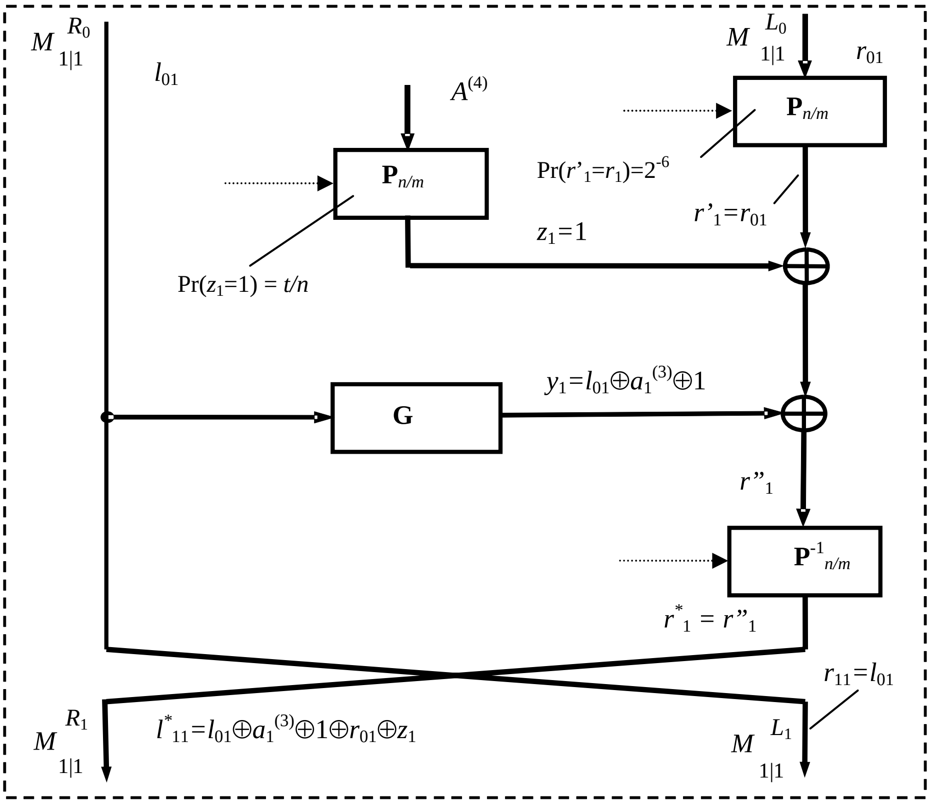

Figure7. Formation of the one-round linear

The bias gets maximum value for the cases $\varphi(A^{(3)}) = 1$ and $\varphi(A^{(3)}) = 0$. For the full round SPECTR-128 the LC with input $\left(M_{1|1}^{L_0}, M_{1|1}^{R_0}\right)$ and output $\left(M_{1|1}^{L_{12}}, M_{1|1}^{R_{12}}\right)$ masks have bias

$$b(12) = \frac{1}{2}\left(2b(1)\right)^{12} \leq \frac{1}{2n^{12}} = 2^{-73}.\infty$$

For eleven rounds we have $b(11) \leq 2^{-67}$. For the random cipher LCs have bias $b \approx 2^{-64} > b(11)$. Therefore we can conclude that for the worst case of the secret key selection eleven rounds of SPECTR-128 are sufficient to thwart linear attacks. In order to eliminate linear attacks based on the considered LC we propose to use in the modified version SPECTR'-128 the constant C = (101010…10) instead of thesubkey$A^{(3)}$ (earliersuch mechanism was used in DDP-64 [14]). Since in this case we have $t = \varphi(C) = n/2$, the bias of the considered characteristic equals to zero, therefore an attacker should add at least one active bit in used masks and this will reduce sharply the bias value due to both the variable permutations and the **G** operation.

5 Conclusion

Security of the 128-bit block cipher SPECTR-128 is based on the use of DDP performed with $\mathbf{P}_{64/192}$-boxes, specially designed extension boxes, and the nonlinear operation **G**.

Some remarks should be given about IKS. Actually it is a part of the round data transformation only. It introduces no delay, since it is executed in parallel with some data ciphering operations. Notion IKS corresponds to the part of encryption procedure related to the data-dependent transformation ofsubkey (orsubkeys) executed in parallel with the transformation of data. The internal key scheduling used in SPECTR-128 is not complex, but it changes from one data block to another, making the avalanche effect faster and crypto scheme significantly more secure against differential and linear cryptanalysis.

In one round of SPECTR-128 the left data subblock is kept constant, however this data subblock participates in round transformation influencing transformation of the right data subblock. Our DCA of SPECTR-128 has shown that the structure of the extension boxes is a critical part of the DDP-based ciphers. Presenting the modified version SPECTR'-128 we have shown the small modifications in the table describing the extension box significantly change the probability of the differential characteristics. Our preliminary LCA shows that SPECTR-128 secure against linear attacks, although much more work on LCA of this cipher is to be done. Because of the use very simple key scheduling there are possible weak keys having the structure $K = (K_1, K_2, K_3, K_4) = (X, X, Y, Y)$, their portion ($2^{-128}$) is negligible though. An interesting way to avoid weak keys is the use of the switchable (*e*-dependent) operations, one can use some complex key scheduling though (weak we call the keys for which encryption function is involution).

The aim of the description and discussion of the SPECTR ciphers is to illustrate the design of the DDP-based ciphers and to show that such ciphers represent a suitable model for calculation of the differential characteristics and security estimations. We estimate that introducing small changes if the structure of the operation **G** one can easy reduce the probability of the three-round differential characteristic and design secure ten-round or eight-round SPECTR-like cryptosystem. For example it is easy to compose a **G**-like function **G′** for which two output bits change deterministically when an input bit flips. Use of the operation **G′** in SPECTR reduces drastically the probability of the two-round and three-round differential characteristics as well as the bias of linear characteristics. Detailed design of the SPECTR-like cryptosystem with reduced number of rounds appears to be a subject of separate consideration.

References

[1] A.A. Moldovyan, N.A. Moldovyan, Innovative Cryptography, *Charles River Media,* 2007, 396p.

[2] A.A. Moldovyan, N.A. Moldovyan, “A cipher based on data-dependent permutations”, *Journal of Cryptology* vol. **15**, no. 1 (2002), pp. 61-72.

[3] Izotov, B.V., Moldovyan, A.A., Moldovyan, N.A.,“Fast Encryption Algorithm Spectr-H64”,*MMM-ACNS* ’01, LNCS 2052, pp. 275–286, Springer-Verlag 2001.

[4] Goots, N.D., Izotov, B.V., Moldovyan, A.A., Moldovyan, N.A.,“Fast Ciphers for Cheap Hardware: Differential Analysis of SPECTR-H64”,*MMM-ACNS* ’03, LNCS 2776, pp. 449–452, Springer-Verlag 2003.

[5] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", *Journal of Cryptology*, vol. **4**, no. 1, pp. 3-72, 1991.

[6] E. Biham and A. Shamir,“Differential Cryptanalysis of the Data Encryption Standard”,*Springer-Verlag*, New York, 1993.

[7] M. Matsui,“Linear cryptanalysis method for DES cipher”, In T. Helleseth, editor, *Advances in Cryptology | Eurocrypt* '93, volume **765** of Lecture Notes in Computer Science, pages 386{397, 1994. Springer-Verlag.

[8] E. Biham, "On Matsui’s Linear Cryptanalysis", *Advances in Cryptology - EUROCRYPT*’94 (Lecture Notes in Computer Science no. 950), Springer-Verlag,pp. 341-355, 1995.

[9] Y.Ko, D.Hong, S.Hong, S.Lee, J.Lim, “Linear Cryptanalysis on SPECTR-H64 with Higher Order Differential Property”, *International Workshop, Methods, Models, and Architectures for Network Security Proc. LNCS*, vol. **2776** (2003), pp. 298-307.

[10] N.A. Moldovyan, A.A. Moldovyan, N.D. Goots, “Variable Bit Permutations:Linear Characteristics and Pure VBP-based Cipher”, *Computer Science Journal of Moldova*. 2005. vol.**13**, No 1(37). P.84-109.

[11] A.V. Bodrov, A.A. Moldovyan, P.A. Moldovyanu, “DDP-based Ciphers:Differential Analysis of SPECTR-H64”, *Computer Science Journal of Moldova*. 2005. Vol. **13**, Number 3(39), pp.268-291.

[12] B.V.Izotov, A.A.Moldovyan, and N.A.Moldovyan, “Fast information protection methods based on controlled operations”, *Avtomatika i telemehanika, Moscow: Russian Academy of Sciences,* no 6, pp. 168-184 (in Russian).

[13] B.V.Izotov, A.A.Moldovyan, and N.A.Moldovyan, “Controlled operations as a cryptographic primitive”, *Proceedings of the International workshop, Methods, Models, and Architectures for Network Security*. Lect. Notes Comput. Sci. Berlin: Springer-Verlag, vol. **2052** (2001), pp. 230-241.

[14] N.A. Moldovyan, P.A. Moldovyanu, D.H. Summerville, “On Software Implementation of Fast DDP-Based Ciphers”, *International Journal of Network Security*. 2007. vol. **4**, no. 1. P.81-89.

Received: October 1, 2013