Misty

Криптоалгоритмы $Misty1$ и $Misty2$ [1] шифруют 64-битовые блоки открытых данных под управлением 128-битового секретного ключа.

В алгоритмах используются побитовые операции отрицания (not), сложения по модулю 2 ($\oplus$), дизъюнкции (V), коньюнкции (&), операция сдвига влево и вправо на n позиций (shl_n и shr_n), выполняемые над 2-байтовыми словами, и функции FI, FL и FO.

Функция $FI(X,Y)$ от 2-байтовых аргументов X и Y, возвращающая 2-байтовые значения, определяется следующим образом:

$FI(X,Y) \equiv \{$
$d9 := shr_7(X);$
$d7 := X \ \& \ 0x7f;$
$d9 := S_9[d9] \ \oplus d7;$
$d7 := ((S_7[d7] \oplus (d9 \ \& \ 0x7f) \oplus shr_9(Y);$
$d9 := S_9[d9 \oplus (Y \ \& \ 0x1ff)] \oplus d7;$
$FI := d7 \times 512 + d9$
$\}.$

Здесь $d7$, $d9$ – вспомогательные 2-байтовые переменные, в процессе вычислений $0 \le d7 \le 127$; $0 \le d9 \le 511$;

S_7 – подстановка на множестве $\{0, 1, \dots, 127\}$ 7-битовых чисел, а S_9 – подстановка на множестве $\{0, 1, \dots, 511\}$ 9-битовывх чисел. Подстановка S_7 задана табл. 1.

Таблица 1

Подстановка S_7 в Misty

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	1b	32	33	5a	3b	10	17	54	5b	1a	72	73	6b	2c	66	49
1	1f	24	13	6c	37	2e	3f	4a	5d	0f	40	56	25	51	1c	04
2	0b	46	20	0d	7b	35	44	42	2b	1e	41	14	4b	79	15	6f
3	0e	55	09	36	74	0c	67	53	28	0a	7e	38	02	07	60	29
4	19	12	65	2f	30	39	08	68	5f	78	2a	4c	64	45	75	3d
5	59	48	03	57	7c	4f	62	3c	1d	21	5e	27	6a	70	4d	3a
6	01	6d	6e	63	18	77	23	05	26	76	00	31	2d	7a	7f	61
7	50	22	11	06	47	16	52	4e	71	3e	69	43	34	5c	58	7d

Подстановка S_9 определена как $y_8 y_7 \dots y_0 = S_9[x_8 x_7 \dots x_0]$, где биты y_j, $0 \le j \le 8$ вычисляются по формулам (см. также табл. 2):

$y_0 := \ \neg (04 + 05 + 15 + 16 + 26 + 27 + 38 + 48);$
$y_1 := \ \neg (02 + 3 + 13 + 23 + 34 + 45 + 06 + 26 + 7 + 08 + 38 + 58);$
$y_2 := \ 01 + 13 + 4 + 04 + 24 + 34 + 45 + 06 + 56 + 17 + 37 + 8;$
$y_3 := \ 0 + 12 + 24 + 5 + 15 + 35 + 45 + 56 + 17 + 67 + 28 + 48;$
$y_4 := \ 1 + 03 + 23 + 05 + 35 + 6 + 26 + 46 + 56 + 67 + 28 + 78;$
$y_5 := \ 2 + 03 + 14 + 34 + 16 + 46 + 7 + 37\ 57 + 67 + 08 + 78;$
$y_6 := \ \neg (01 + 3 + 14 + 25 + 45 + 27 + 57 + 8 + 08 + 48 + 68 + 78);$
$y_7 := \ \neg (1 + 01 + 12 + 23 + 04 + 5 + 16 + 36 + 07 + 47 + 67 + 18);$
$y_8 := \ \neg (1 + 01 + 12 + 4 + 05 + 25 + 36 + 56 + 07 + 08 + 38 + 68).$

Здесь (для краткости) запись $y_0 := \neg (04 + 05 + 15 + 16 + 26 + 27 + 38 + 48)$ трактуется как $y_0 := not\ (x_0 x_4 \oplus x_0 x_5 \oplus \dots \oplus x_4 x_8)$ и т.д.

Отметим, что при фиксированном Y отображение $X \longrightarrow FI(X,Y)$ является взаимноодно-значным на множестве 2-байтовых слов. Обратная функция $FI^{-1}(Z,Y)$, возвращающая значение X, удовлетворяющее уравнению $FI(X,Y) = Z$, определяется как

[1] Авторы шифра: *Hidenori Ohta* и *Mitsuru Matsui* (Япония)

$FI^{-1}(Z, Y) \equiv \{$

$d7 := shr_9(Z);$

$d9 := Z \ \& \ 0\text{x}1ff;$

$d9 := S_9^{-1}[d9 \oplus d7] \oplus (Y \ \& \ 0\text{x}1ff);$

$d7 := S_7^{-1}[d7 \oplus shr_9(Y) \oplus (d9 \& 0\text{x}7f)];$

$d9 := S_9^{-1}[d9 \oplus d7];$

$FI^{-1} := d9 \times 128 + d7$

}.

Здесь S_7^{-1} и S_9^{-1} – подстановки, обратные к S_7 и S_9.

Таблица 2

Подстановка S_9

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	1c3	0cb	153	19f	1e3	0e9	0fb	035	181	0b9	117	1eb	133	009	02d	0d3
01	0c7	14a	037	07e	0eb	164	193	1d8	0a3	11e	055	02c	01d	1a2	163	118
02	14b	152	1d2	00f	02b	030	13a	0e5	111	138	18e	063	0e3	0c8	1f4	01b
03	001	09d	0f8	1a0	16d	1f3	01c	146	07d	0d1	082	1ea	183	12d	0f4	19e
04	1d3	0dd	1e2	128	1e0	0ec	059	091	011	12f	026	0dc	0b0	18c	10f	1f7
05	0e7	16c	0b6	0f9	0d8	151	101	14c	103	0b8	154	12b	1ae	017	071	00c
06	047	058	07f	1a4	134	129	084	15d	19d	1b2	1a3	048	07c	051	1ca	023
07	13d	1a7	165	03b	042	0da	192	0ce	0c1	06b	09f	1f1	12c	184	0fa	196
08	1e1	169	17d	031	180	10a	094	1da	186	13e	11c	060	175	1cf	067	119
09	065	068	099	150	008	007	17c	0b7	024	019	0de	127	0db	0e4	1a9	052
0a	109	090	19c	1c1	028	1b3	135	16a	176	0df	1e5	188	0c5	16e	1de	1b1
0b	0c3	1df	036	0ee	1ee	0f0	093	049	09a	1b6	069	081	125	00b	05e	0b4
0c	149	1c7	174	03e	13b	1b7	08e	1c6	0ae	010	095	1ef	04e	0f2	1fd	085
0d	0fd	0f6	0a0	16f	083	08a	156	09b	13c	107	167	098	1d0	1e9	003	1fe
0e	0bd	122	089	0d2	18f	012	033	06a	142	0ed	170	11b	0e2	14f	158	131
0f	147	05d	113	1cd	079	161	1a5	179	09e	1b4	0cc	022	132	01a	0e8	004
10	187	1ed	197	039	1bf	1d7	027	18b	0c6	09c	0d0	14e	06c	034	1f2	06e
11	0ca	025	0ba	191	0fe	013	106	02f	1ad	172	1db	0c0	10b	1d6	0f5	1ec
12	10d	076	114	1ab	075	10c	1e4	159	054	11f	04b	0c4	1be	0f7	029	0a4
13	00e	1f0	077	04d	17a	086	08b	0b3	171	0bf	10e	104	097	15b	160	168
14	0d7	0bb	066	1ce	0fc	092	1c5	06f	016	04a	0a1	139	0af	0f1	190	00a
15	1aa	143	17b	056	18d	166	0d4	1fb	14d	194	19a	087	1f8	123	0a7	1b8
16	141	03c	1f9	140	02a	155	11a	1a1	198	0d5	126	1af	061	12e	157	1dc
17	072	18a	0aa	096	115	0ef	045	07b	08d	145	053	05f	178	0b2	02e	020
18	1d5	03f	1c9	1e7	1ac	044	038	014	0b1	16b	0ab	0b5	05a	182	1c8	1d4
19	018	177	064	0cf	06d	100	199	130	15a	005	120	1bb	1bd	0e0	04f	0d6
1a	13f	1c4	12a	015	006	0ff	19b	0a6	043	088	050	15f	1e8	121	073	17e
1b	0bc	0c2	0c9	173	189	1f5	074	1cc	1e6	1a8	195	01f	041	00d	1ba	032
1c	03d	1d1	080	0a8	057	1b9	162	148	0d9	105	062	07a	021	1ff	112	108
1d	1c0	0a9	11d	1b0	1a6	0cd	0f3	05c	102	05b	1d9	144	1f6	0ad	0a5	03a
1e	1cb	136	17f	046	0e1	01e	1dd	0e6	137	1fa	185	08c	08f	040	1b5	0be
1f	078	000	0ac	110	15e	124	002	1bc	0a2	0ea	070	1fc	116	15c	04c	1c2

В алгоритмах используются 2-байтовые раундовые подключи $kl_0, kl_1, \dots, kl_{15}$, генерируемые на основе 16-байтового секретного ключа $K = (k_0, k_1, \dots, k_{15})$ по правилу:

for $i := 1$ ***to*** 7 ***do*** $ke_i := k_{2i} \times 256 + k_{2i+1}$;

for $i := 1$ ***to*** 7 ***do*** $ke_{i+8} := FI(ke_i, ke_{i+1 \bmod 8})$.

Схемы зашифрования $Misty1$ и $Misty2$ представлены на рис. 1, 2 (операция $\oplus$ в схемах завершает раунд; стандартное число раундов $N = 8$). Блок открытых данных P разбивается на два 32-битовых слова (левое и правое) и преобразуется в шифртекст C с использованием функций $FO^{(n)}$ и $FL^{(n)}$, зависящих от параметра n. Этот параметр управляет выбором раундовых подключей, используемых при вычислении входных значений функций.

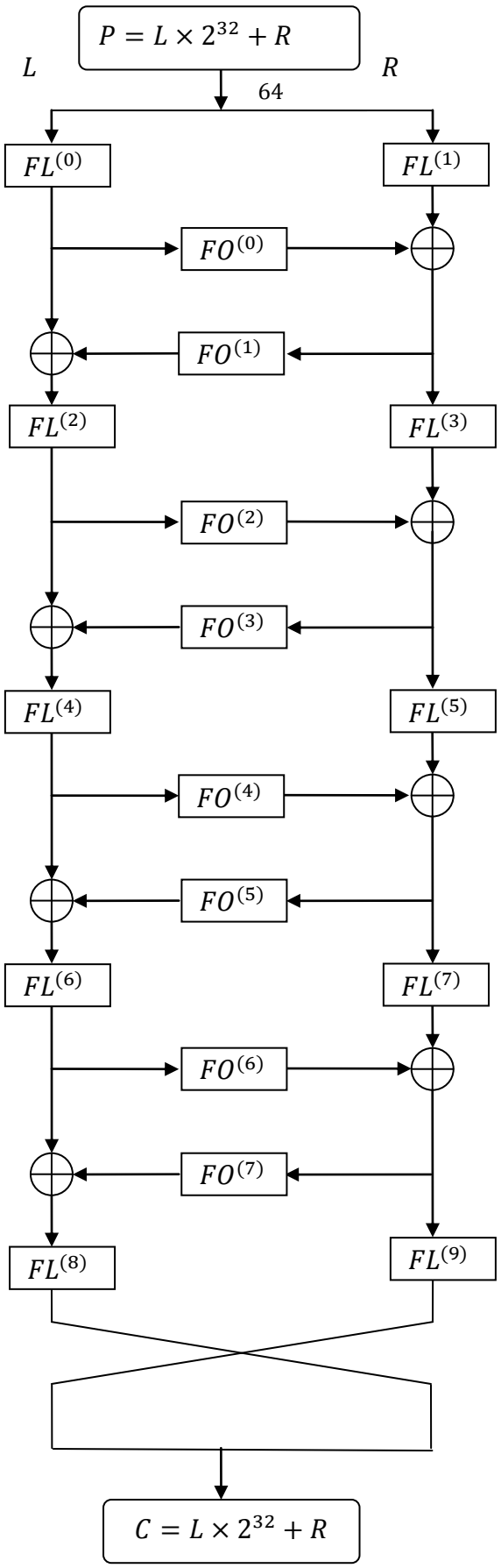


Рис. 1. *Структура алгоритма* $Misty1$

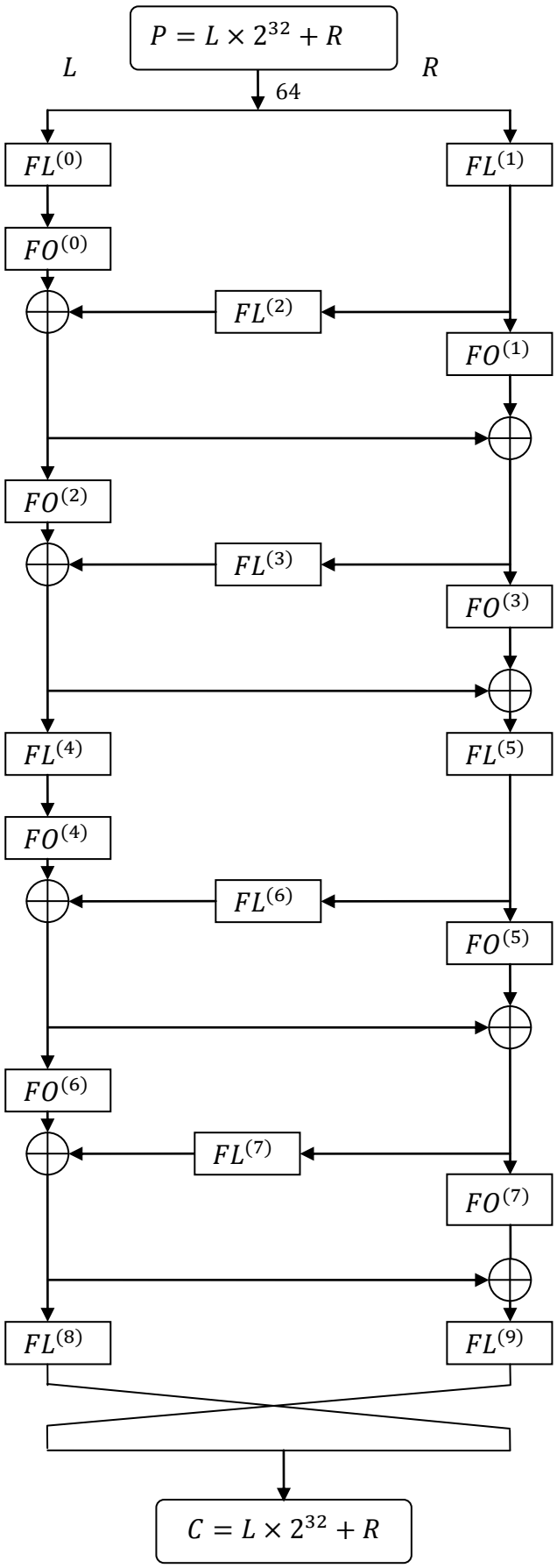


Рис. 2. *Структура алгоритма* $Misty2$

Схемы вычисления значений $FO^{(n)}$ и $FL^{(n)}$ представлены на рис. 3 и 4.

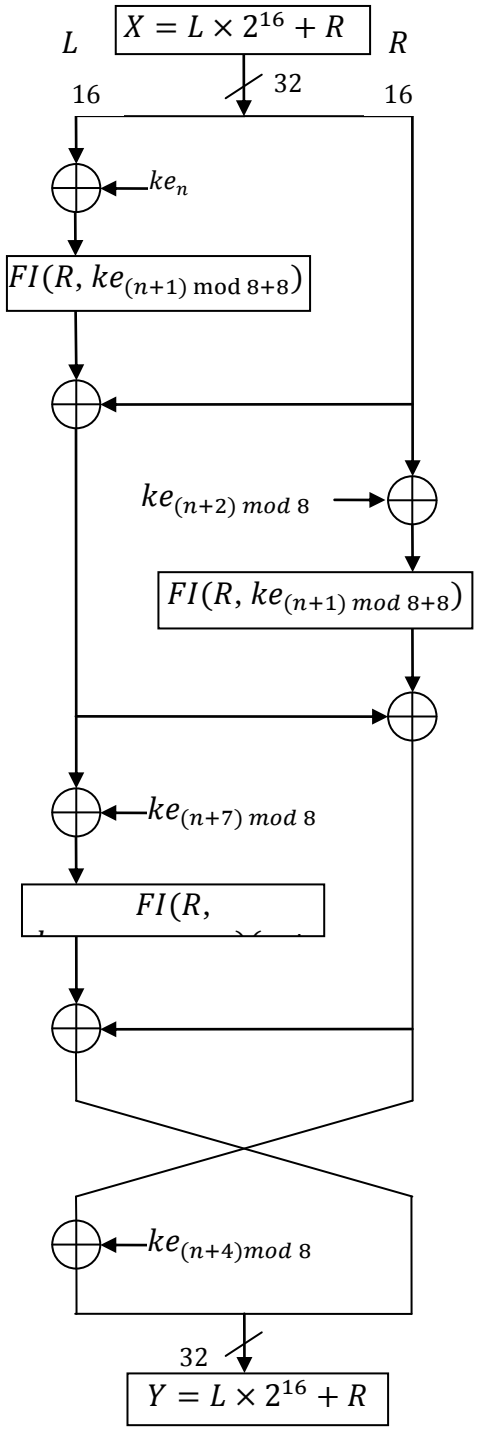
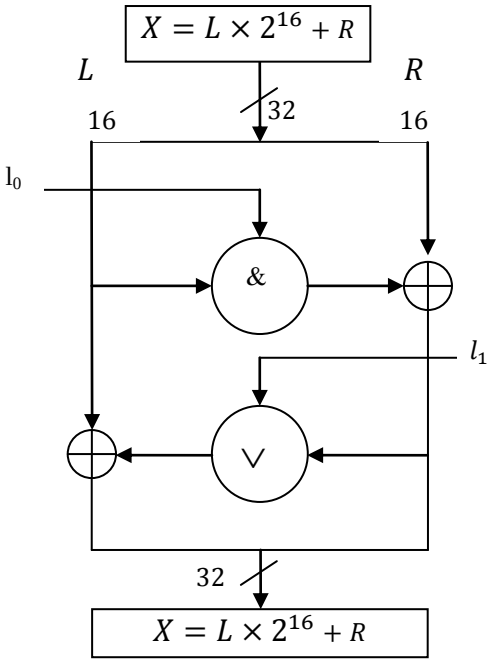


Рис. 3. *Функция* $FO^{(n)}$(X) *в Misty*.



Значения подключей:

if n четно

then {

$i := n \; div \; 2;$

$j := ((n + 12) \; \boldsymbol{div} \; 2) \; \boldsymbol{mod} \; 8 + 8$

}

else {

$i := (((n + 3) \; div \; 2) \; mod \; 8) + 8;$

$j := (n + 7) \; div \; 2$

};

$l_0 := ke_i;$

$l_1 := ke_j.$

Рис. 4. *Функция* $FI^{(n)}$(X) *в Misty*