

# Алгоритм шифрования по СТБ 34.101.31-2011

## Входные и выходные данные

Входными данными алгоритмов зашифрования и расшифрования являются блок  $X \in \{0, 1\}^{128}$  и ключ  $\theta \in \{0, 1\}^{256}$ .

Выходными данными является блок  $Y \in \{0, 1\}^{128}$  — результат зашифрования либо расшифрования слова  $X$  на ключе  $\theta$ :  $Y = F_\theta(X)$  либо  $Y = F_\theta^{-1}(X)$ .

Входные данные подготавливаются следующим образом:

1 Слово  $X$  записывается в виде  $X = X_1 \parallel X_2 \parallel X_3 \parallel X_4$ , где  $X_i \in \{0, 1\}^{32}$ .

2 Ключ  $\theta$  записывается в виде  $\theta = \theta_1 \parallel \theta_2 \parallel \dots \parallel \theta_8$ ,  $\theta_i \in \{0, 1\}^{32}$ , и определяются тактовые ключи  $K_1 = \theta_1$ ,  $K_2 = \theta_2$ , ...,  $K_8 = \theta_8$ ,  $K_9 = \theta_1$ ,  $K_{10} = \theta_2$ , ...,  $K_{56} = \theta_8$ .

## Вспомогательные преобразования и переменные

Подстановка  $H$ . Подстановка  $H: \{0, 1\}^8 \rightarrow \{0, 1\}^8$  задается таблицей. В таблице используется шестнадцатеричное представление слов  $u \in \{0, 1\}^8$ . Если  $u = \text{IJ}_{16}$ , то значение  $H(u)$  находится на пересечении строки I и столбца J. Например,  $H(A2_{16}) = 9B_{16}$ .

Таблица — Подстановка  $H$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	B1	94	BA	C8	0A	08	F5	3B	36	6D	00	8E	58	4A	5D	E4
1	85	04	FA	9D	1B	B6	C7	AC	25	2E	72	C2	02	FD	CE	0D
2	5B	E3	D6	12	17	B9	61	81	FE	67	86	AD	71	6B	89	0B
3	5C	B0	C0	FF	33	C3	56	B8	35	C4	05	AE	D8	E0	7F	99
4	E1	2B	DC	1A	E2	82	57	EC	70	3F	CC	F0	95	EE	8D	F1
5	C1	AB	76	38	9F	E6	78	CA	F7	C6	F8	60	D5	BB	9C	4F
6	F3	3C	65	7B	63	7C	30	6A	DD	4E	A7	79	9E	B2	3D	31
7	3E	98	B5	6E	27	D3	BC	CF	59	1E	18	1F	4C	5A	B7	93
8	E9	DE	E7	2C	8F	0C	0F	A6	2D	DB	49	F4	6F	73	96	47
9	06	07	53	16	ED	24	7A	37	39	CB	A3	83	03	A9	8B	F6
A	92	BD	9B	1C	E5	D1	41	01	54	45	FB	C9	5E	4D	0E	F2
B	68	20	80	AA	22	7D	64	2F	26	87	F9	34	90	40	55	11
C	BE	32	97	13	43	FC	9A	48	A0	2A	88	5F	19	4B	09	A1
D	7E	CD	A4	D0	15	44	AF	8C	A5	84	50	BF	66	D2	E8	8A
E	A2	D7	46	52	42	A8	DF	B3	69	74	C5	51	EB	23	29	21
F	D4	EF	D9	B4	3A	62	28	75	91	14	10	EA	77	6C	DA	1D

Преобразования  $G_r$  ( $r = 5, 13, 21$ ). Преобразование  $G_r: \{0, 1\}^{32} \rightarrow \{0, 1\}^{32}$  ставит в соответствие слову  $u = u_1 \parallel u_2 \parallel u_3 \parallel u_4$ ,  $u_i \in \{0, 1\}^8$ , слово

$$G_r(u) = \text{RotHi}^r(H(u_1) \parallel H(u_2) \parallel H(u_3) \parallel H(u_4)).$$

Переменные. Используются переменные  $a, b, c, d, e$  со значениями из  $\{0, 1\}^{32}$ .

Для зашифрования блока  $X$  на ключе  $\theta$  выполняются следующие шаги:

1 Установить  $a \leftarrow X_1$ ,  $b \leftarrow X_2$ ,  $c \leftarrow X_3$ ,  $d \leftarrow X_4$ .

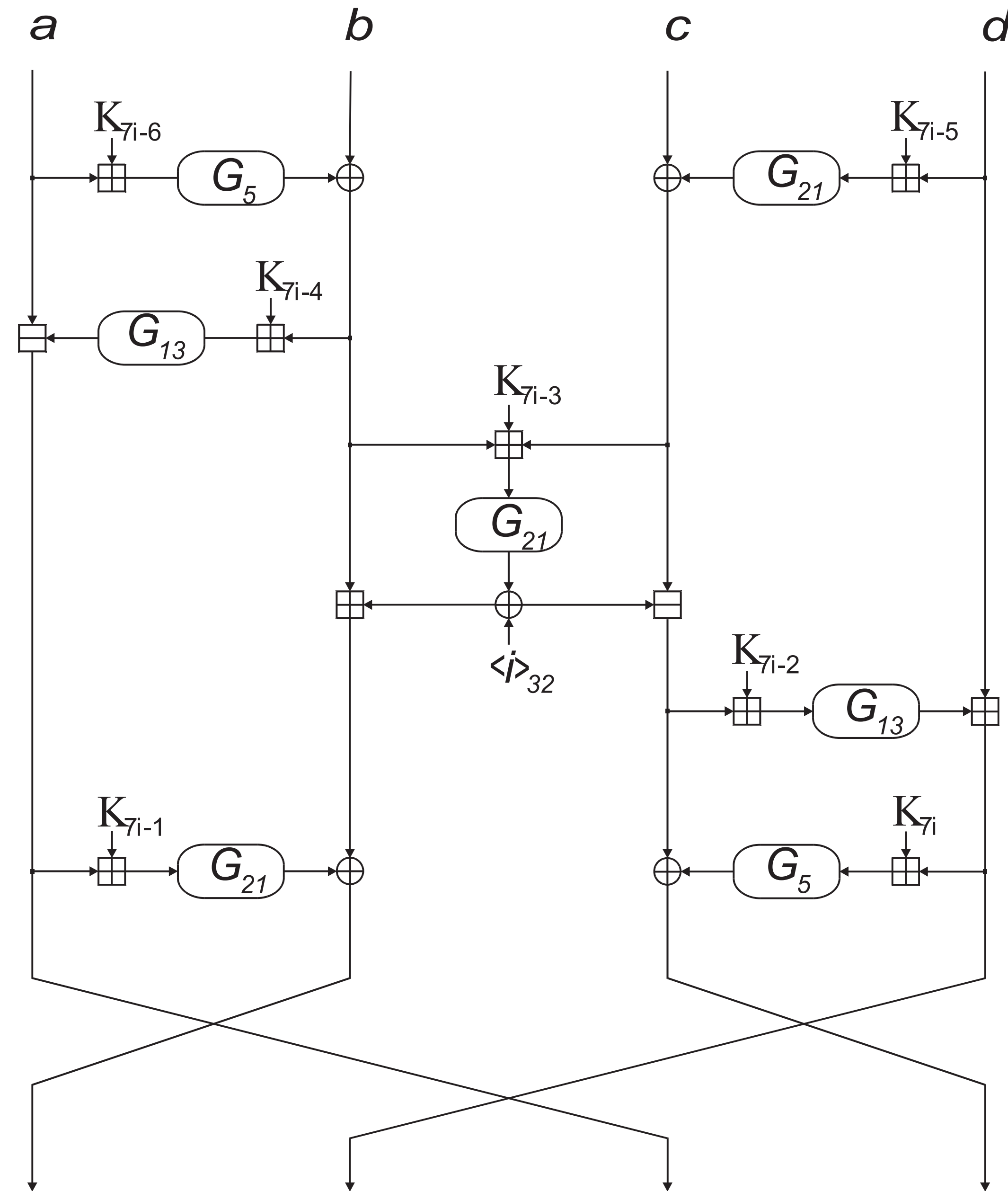
2 Для  $i = 1, 2, \dots, 8$  выполнить:

- 1)  $b \leftarrow b \oplus G_5(a \boxplus K_{7i-6})$ ;
- 2)  $c \leftarrow c \oplus G_{21}(d \boxplus K_{7i-5})$ ;
- 3)  $a \leftarrow a \boxplus G_{13}(b \boxplus K_{7i-4})$ ;
- 4)  $e \leftarrow G_{21}(b \boxplus c \boxplus K_{7i-3}) \oplus \langle i \rangle_{32}$ ;
- 5)  $b \leftarrow b \boxplus e$ ;
- 6)  $c \leftarrow c \boxplus e$ ;
- 7)  $d \leftarrow d \boxplus G_{13}(c \boxplus K_{7i-2})$ ;
- 8)  $b \leftarrow b \oplus G_{21}(a \boxplus K_{7i-1})$ ;
- 9)  $c \leftarrow c \oplus G_5(d \boxplus K_{7i})$ ;
- 10)  $a \leftrightarrow b$ ;
- 11)  $c \leftrightarrow d$ ;
- 12)  $b \leftrightarrow c$ .

3 Установить  $Y \leftarrow b \parallel d \parallel a \parallel c$ .

4 Возвратить  $Y$ .

## Вычисления на $i$ -м такте зашифрования



## Алгоритм зашифрования в режиме счётчика

Зашифрование сообщения  $X$  на ключе  $\theta$  при использовании синхропосылки  $S$  состоит в выполнении следующих шагов:

1 Установить  $s \leftarrow F_\theta(S)$ .

2 Для  $i = 1, 2, \dots, n$  выполнить:

1)  $s \leftarrow s \boxplus \langle 1 \rangle_{128}$ ,

2)  $Y_i \leftarrow X_i \oplus L_{|X_i|}(F_\theta(s))$ .

3 Установить  $Y \leftarrow Y_1 \parallel Y_2 \parallel \dots \parallel Y_n$ .

4 Возвратить  $Y$ .

## Алгоритм расшифрования в режиме счётчика

Расшифрование сообщения  $X$  на ключе  $\theta$  при использовании синхропосылки  $S$  состоит в выполнении тех же шагов, что и при зашифровании.