

$$4) L_H = 00110011101011110010100011101010$$

$$5) y_L = x_R = \underbrace{0 \dots 0}_{2^8} 0100$$

Backup:

$$6) y_R = x_L \oplus L_H(S(\dots)) = 00110011101011110010100011101010$$

Payung 2

$$y_R + k_2 = 00110011101011110010100011101010$$

$$S(y_R + k_2)$$

$$u_1 = 0101_2 = 5 = S_1(5) = 8 \rightarrow 1000$$

$$u_2 = 1111_2 = 15 = S_2(15) = 9 \rightarrow 1001$$

$$u_3 = 1000_2 = 8 = S_3(8) = 14 \rightarrow 1110$$

$$u_4 = 0010_2 = 2 = S_4(2) = 10 \rightarrow 1010$$

$$u_5 = 1111_2 = 15 = S_5(15) = 2 \rightarrow 0010$$

$$u_6 = 1010_2 = 10 = S_6(10) = 8 \rightarrow 1000$$

$$u_7 = 0011_2 = 3 = S_7(3) = 1 \rightarrow 0001$$

$$u_8 = 0011_2 = 3 = S_8(3) = 0 \rightarrow 0000$$

$$S_{p+1} = 00000001100000101010111010101000$$

$$L_H(S(y_R + k_2)) = 0001010101011101001100000000001100$$

Backup:

$$z_L = y_R = 00110011101011110010100011101010$$

$$z_L = y_L \oplus L_H(S(\dots)) = 0001010101011101001100000000001000$$

Восна-форм. Дифне ТК-31.  
Восна-форм 2. - конур 6 мургу

Вире-пан:

1) S-форм

$$\begin{aligned} S_1 &= (4, 10, 2, 2, 13, 8, 0, 14, 6, 11, 1, 12, 7, 15, 5, 3) \\ S_2 &= (14, 11, 4, 12, 6, 13, 15, 10, 2, 3, 8, 1, 0, 7, 5, 9) \\ S_3 &= (5, 8, 1, 13, 10, 3, 4, 2, 14, 15, 12, 7, 6, 0, 9, 11) \\ S_4 &= (7, 13, 10, 1, 0, 8, 9, 15, 14, 4, 6, 12, 11, 2, 5, 3) \\ S_5 &= (6, 12, 7, 1, 5, 15, 13, 8, 4, 10, 9, 14, 0, 3, 11, 2) \\ S_6 &= (4, 11, 10, 0, 7, 2, 1, 13, 3, 6, 8, 5, 9, 12, 15, 14) \\ S_7 &= (13, 11, 4, 1, 3, 15, 5, 9, 0, 10, 14, 7, 6, 8, 2, 12) \\ S_8 &= (1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14, 6, 11, 8, 12) \end{aligned}$$

2) Кире-глох-пагур-к:  $k_1 = (0, 0, 1, 0, 1, 0)$   $k_2 = (0, 0, 1, 0, 1, 1)$

3) Бире-вире-форм-тук-тук:  $x = (0, 0, 0, 0, 1, 0)$

но 32-бит:

$$x = (x_L, x_R) \quad 1) \quad x_L = 00...00, \quad x_R = 00...00100$$

Пагур-1.

1)  $x_R + k_1 = 4 + 10 = 14 \rightarrow 0...01110$

2)  $S(x_R + k_1)$   
бир-г:  $0...01110$

$$\begin{aligned} u_1 &= 1110_2 (8) \rightarrow S_1 = S_1(14) = 5 \rightarrow 0101 \\ u_2 &= 0000_2 (0) \rightarrow S_2 = S_2(0) = 14 \rightarrow 1110 \\ u_3 &= 0000_2 (0) \rightarrow S_3 = S_3(0) = 5 \rightarrow 0101 \\ u_4 &= 0000_2 (0) \rightarrow S_4 = S_4(0) = 7 \rightarrow 0111 \\ u_5 &= 0000_2 (0) \rightarrow S_5 = S_5(0) = 6 \rightarrow 0110 \\ u_6 &= 0000_2 (0) \rightarrow S_6 = S_6(0) = 4 \rightarrow 0100 \\ u_7 &= 0000_2 (0) \rightarrow S_7 = S_7(0) = 13 \rightarrow 1101 \\ u_8 &= 0000_2 (0) \rightarrow S_8 = S_8(0) = 1 \rightarrow 0001 \end{aligned}$$