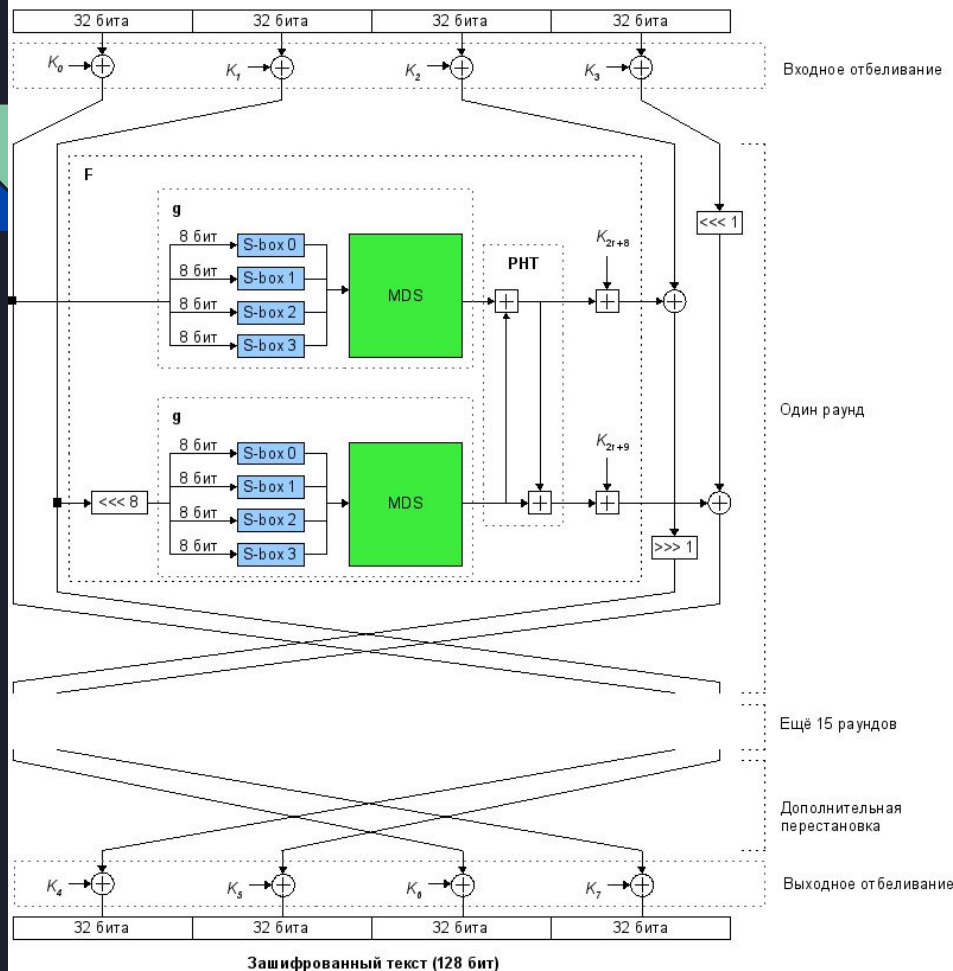




Twofish


Лундин Максим
Шарипов Самариддин

Открытый текст (128 бит)



\oplus - операция XOR

\oplus - сложение по модулю 32



$$\text{MDS} = \begin{pmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{pmatrix}$$

$$x^8 + x^6 + x^5 + x^3 + 1.$$

Функция Н

q_0 и q_1 — фиксированные перестановки 8 битов входного байта x .

Байт x разбивается на две 4-битные половинки a_0 и b_0 , над которыми проводятся следующие преобразования:

$$a_0 = x/16 \quad b_0 = x \bmod 16$$


$$a_1 = a_0 \oplus b_0 \quad b_1 = a_0 \oplus \text{ROR}_4(b_0, 1) \oplus 8a_0 \bmod 16$$

$$a_2 = t_0[a_1] \quad b_2 = t_1[b_1]$$

$$a_3 = a_2 \oplus b_2 \quad b_3 = a_2 \oplus \text{ROR}_4(b_2, 1) \oplus 8a_2 \bmod 16$$

$$a_4 = t_2[a_3] \quad b_4 = t_3[b_3]$$

$$y = 16b_4 + a_4$$



Для q_0 таблицы имеют вид:

$t_0 = [8\ 1\ 7\ D\ 6\ F\ 3\ 2\ 0\ B\ 5\ 9\ E\ C\ A\ 4]$

$t_1 = [E\ C\ B\ 8\ 1\ 2\ 3\ 5\ F\ 4\ A\ 6\ 7\ 0\ 9\ D]$

$t_2 = [B\ A\ 5\ E\ 6\ D\ 9\ 0\ C\ 8\ F\ 3\ 2\ 4\ 7\ 1]$

$t_3 = [D\ 7\ F\ 4\ 1\ 2\ 6\ E\ 9\ B\ 3\ 0\ 8\ 5\ C\ A]$

Для q_1 таблицы имеют вид:

$t_0 = [2\ 8\ B\ D\ F\ 7\ 6\ E\ 3\ 1\ 9\ 4\ 0\ A\ C\ 5]$

$t_1 = [1\ E\ 2\ B\ 4\ C\ 3\ 7\ 6\ D\ A\ 5\ F\ 9\ 0\ 8]$

$t_2 = [4\ C\ 7\ 5\ 1\ 6\ 9\ A\ 0\ E\ D\ 8\ 2\ B\ 3\ F]$

$t_3 = [B\ 9\ 5\ 1\ C\ 3\ D\ E\ 6\ 4\ 7\ F\ 2\ 0\ 8\ A]$



Генерация ключей

$$\rho = 2^{24} + 2^{16} + 2^8 + 2^0$$

$$A_i = h(2i\rho, M_e)$$

$$B_i = \text{ROL}(h((2i+1)\rho, M_0), 8)$$

$$K_{2i} = (A_i + B_i) \bmod 2^{32}$$

$$K_{2i+1} = \text{ROL}((A_i + 2B_i) \bmod 2^{32}, 9)$$

Генерация S-box

$$RS = \begin{pmatrix} 01 & A4 & 55 & 87 & 5A & 58 & DB & 9E \\ A4 & 56 & 82 & F3 & 1E & C6 & 68 & E5 \\ 02 & A1 & FC & C1 & 47 & AE & 3D & 19 \\ A4 & 55 & 87 & 5A & 58 & DB & 9E & 03 \end{pmatrix}$$

$$a' = a + b \pmod{2^n}$$

$$b' = a + 2b \pmod{2^n}$$



Спасибо за внимание!!