Hierocrypt

$Hierocrypt-$ семейство блочных шифров[1]. Криптоалгоритм $Hierocrypt-$L1 шифрует 64-битовые блоки открытых данных под управлением 128-битового секретного ключа; $Hierocrypt-3$ шифрует 128-битовые блоки открытых данных под управлением секретного ключа, длина которого может составлять 128, 192 или 256 битов.

Обозначения. В записи $X_{(n)}$ нижний индекс, заключенный в скобки, обозначает длину блока X в битах. Заглавные буквы используются для обозначения блоков, длина которых не меньше16 битов, а строчные – для обозначения байтов и битов. Предполагается обратный ($big-endian\ convention$) порядок следования байтов (старший байт в блоке расположен слева, т.е. в младшей адресной позиции). Блок $X_{(mn)}$ рассматривается как конкатенация m n-битовых подблоков $X_{i(n)}$:

$X_{(mn)} = X_{1(n)}||X_{2(n)}|| \dots ||X_{m(n)}$,

причем

$X_{(mn)} = x_{1(1)}||x_{2(1)}|| \dots ||x_{mn(1)},\ X_{i(n)} = x_{ni-1(1)}||x_{ni-2(1)}|| \dots ||x_{ni-n(1)}$

В частности, для 64-битовых блоков имеем

$X_{(64)} = X_{1(32)}||\ X_{2(32)}$;

$X_{i(32)} = x_{4i-4+1(8)}||x_{4i-4+2(8)}||x_{4i-4+3(8)}||x_{4i-4+4(32)},\ i = 1,2$;

$x_{j(8)} = x_{8j-8+1(8)}||x_{8j-8+2(8)}|| \dots ||x_{8j-8+8(8)},\ j = 1,2,\dots,8.$

Аналогично, для 128-битовых блоков –

$X_{(128)} = X_{1(32)}||X_{2(32)}||X_{3(32)}||X_{4(32)}$;

$X_{i(32)} = x_{4i-4+1(8)}||x_{4i-4+2(8)}||x_{4i-4+3(8)}||x_{4i-4+4(32)},\ i = 1,2,3,4$;

$x_{j(8)} = x_{8j-8+1(8)}||x_{8j-8+2(8)}|| \dots ||x_{8j-8+8(8)},\ j = 1,2,\dots,16.$

Отметим, что $x_{in(1)}$ – младший бит в $X_{i(n)}$; он же – i-ый бит в $X_{(mn)}$. Другими словами $X_{(mn)}$ – блок с числовым значением

$$N(X_{(mn)}) = \sum_{j=1}^{mn} x_{j(1)}2^{mn-j} = \sum_{j=1}^{mn} N(X_{i(n)})2^{(j-1)n} = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} x_{in-n+j(1)}2^{n-j}\right)2^{(i-1)n}.$$

***Hierocrypt*–L1**. Структура алгоритма представлена на рис.1. В алгоритме используются 128-битовые раундовые подключи $K_{(128)}^{(1)}$, …, $K_{(128)}^{(7)}$, генерируемые на основе 128-битового секретного ключа K на этапе предвычислений.

Алгоритм зашифрования $Hierocrypt-L1$

Вход: P – 64-битовый блок открытых данных.

$C := P$;

for $t := 1$ ***to*** 5 ***do*** $C := \rho[K_{(128)}^{(t)}](C)$;

$C := XS[K_{(128)}^{(6)}](C)$;

$C := C \oplus (K_{1(32)}^{(7)}||K_{2(32)}^{(7)})$.

Выход: C – 64-битовый блок шифртекста.

Алгоритм расшифрования $Hierocrypt-L1$

Вход: C – 64-битовый блок шифртекста.

$P := C \oplus (K_{1(32)}^{(7)}||K_{2(32)}^{(7)})$;

$P := XS^{-1}[K_{(128)}^{(6)}](P)$;

for $t := 5$ ***downto*** 1 ***do*** $P := \rho^{-1}[K_{(128)}^{(t)}](P)$;

Выход: P – 64-битовый блок открытых данных.

---

[1] Авторы шифров: сотрудники японской корпорации Тошиба $H.Muratani,\ K.Ohkuma,\ F.Sano,$ $M.Motoyama$ и $S.Kawamura$.

Генерация раундовых подключей в $Hierocrypt-L1$

При вычислении раундовых подключей используются вспомогательные переменные

$Z_{(128)}^{(t)} = Z_{1(32)}^{(t)}||Z_{2(32)}^{(t)}||Z_{3(32)}^{(t)}||Z_{4(32)}^{(t)},\ t = -1, 0, 1, \dots, 7;$

$V_{(32)}^{(t)}, t = 1, \dots, 7;$

$W_{(64)}^{(t)} = W_{1(32)}^{(t)}||W_{2(32)}^{(t)},\ t = 5, 6, 7;$

$Y_{(32)},\ U_{(64)} = U_{1(32)}||U_{2(32)}$

и 32-битовые константы

$\mathrm{H}_0 = 0\mathrm{x}5a827999 = [2^{30}\sqrt{2}],$

$\mathrm{H}_1 = 0\mathrm{x}6ed9eba1 = [2^{30}\sqrt{3}],$

$\mathrm{H}_2 = 0\mathrm{x}8f1bbcdc = [2^{30}\sqrt{5}],$

$\mathrm{H}_3 = 0\mathrm{x}6ac2c1d6 = [2^{30}\sqrt{10}],$

$\mathrm{H}_4 = 0\mathrm{x}f7def58a = [2^{30}\sqrt{15}].$

Функции, используемые в $Hierocrypt-L1$

$x_{1(8)}||x_{2(8)}|| \dots ||x_{8(8)} = \mathrm{X}_{1(32)}\ ||\ \mathrm{X}_{2(32)} = \mathrm{X}_{(64)},$

$x_{1(8)}||x_{2(8)}||x_{3(8)}\ ||x_{4(8)} = \mathrm{X}_{(32)},$

$\mathrm{K}_{1(64)}||\mathrm{K}_{2(64)} = \mathrm{K}_{(128)}.$

Функции ρ (см. рис. 2) и ρ^{-1}:

$\rho\,(\mathrm{X}_{(64)}, \mathrm{K}_{(128)})_{(64)} = \mathrm{MDS}_{\mathrm{H}}\,(\mathrm{XS}\,(\mathrm{X}_{(64)}, \mathrm{K}_{(128)})),$

$\rho^{-1}(\mathrm{X}_{(64)}, \mathrm{K}_{(128)})_{(64)} = \mathrm{XS}^{-1}(\mathrm{MDS}_{\mathrm{H}}^{-1}(\mathrm{X}_{(64)}, \mathrm{K}_{(128)}).$

Функции XS и XS^{-1}:

$XS\,(\mathrm{X}_{(64)}, \mathrm{K}_{(128)})_{(64)} = S(\mathrm{MDS}_{\mathrm{L}}\,(\mathrm{X}_{(64)} \oplus \mathrm{K}_{1(64)})) \oplus \mathrm{K}_{2(64)}),$

$XS^{-1}(\mathrm{X}_{(64)}, \mathrm{K}_{(128)})_{(64)} = S^{-1}(\mathrm{MDS}_{\mathrm{L}}^{-1}\,(S^{-1}(\mathrm{X}_{(64)} \oplus \mathrm{K}_{2(64)})) \oplus \mathrm{K}_{1(64)}).$

Отметим, что

$\rho\big(\rho^{-1}\big(X_{(64)}, K'_{(128)}\big), K''_{(128)}\big) = \rho^{-1}\big(\rho\big(X_{(64)}, K''_{(128)}\big), K'_{(128)}\big) = X_{(64)},$

$XS\big(XS^{-1}\big(X_{(64)}, K'_{(128)}\big), K''_{(128)}\big) = XS^{-1}\big(XS\big(X_{(64)}, K''_{(128)}\big), K'_{(128)}\big) = X_{(64)},$

если $K'_{(128)} = K''_{(128)}$.

Функции S и S^{-1}:

$S(X_{(64)})_{(64)} = s\big(x_{1(8)}\big)\ ||\ s(x_{2(8)})|| \dots ||s(x_{8(8)}),$

$S^{-1}(X_{(64)})_{(64)} = s^{-1}\big(x_{1(8)}\big)\ ||\ s^{-1}\big(x_{2(8)}\big)||\ \dots\ ||\ s^{-1}(x_{8(8)}),$

где s – подстановка на множестве байтов, заданная табл.1, а s^{-1} – подстановка, обратная к s.

$Z_{(128)}^{(-1)} \coloneqq K;$

$Y_{(32)} \coloneqq M_5\left(Z_{3(32)}^{(-1)}\right) \oplus H_0;$

$Z_{(128)}^{(0)} \coloneqq Z_{2(32)}^{(-1)}\ ||\ Z_{1(32)}^{(-1)} \oplus F_\sigma\left(Z_{2(32)}^{(-1)} \oplus Y_{32}\right)||Y_{(32)}||M_B\left(Z_{4(32)}^{(-1)}\right);$

$\boldsymbol{for}\ \ t \coloneqq 1\ \boldsymbol{to}\ 4\ \boldsymbol{do}\ \{$

$U_{(64)} \coloneqq P^{(16)}\left(Z_{3(32)}^{(t-1)}||\ Z_{4(32)}^{(t-1)}\right);$

$Y_{32} \coloneqq M_5\big(U_{1(32)}\big) \oplus H_t;$

$V_{(32)}^{(t)} \coloneqq F_\sigma\left(Z_{2(32)}^{(t-1)} \oplus Y_{32}\right);$

$Z_{(128)}^{(t)} \coloneqq Z_{2(32)}^{(t-1)}\ ||\ Z_{1(32)}^{(t-1)} \oplus V_{(32)}^{(t)}||Y_{(32)}||M_B\big(U_{2(32)}\big)$

$\};$

$\boldsymbol{for}\ t \coloneqq 5\ \boldsymbol{to}\ 7\ \boldsymbol{do}\ \{$

$Z_{(128)}^{(t)} \coloneqq Z_{(128)}^{(8-t)};$

$V_{(32)}^{(t)} := F_\sigma\left(Z_{1(32)}^{(t-1)} \oplus Z_{3(32)}^{(t-1)}\right)$;

$W_{(64)}^{(t)} := M_B\left(Z_{3(32)}^{(t-1)} \oplus H_{9-t}\right) || M_5\left(Z_{4(32)}^{(t-1)}\right)$;

$Z_{3(32)}^{(t)} || Z_{4(32)}^{(t)} = P^{(16)^{-1}}\left(W_{1(32)}^{(t)} || W_{2(32)}^{(t)}\right)$

};

for $t := 1$ ***to*** 4 ***do***

$K_{(128)}^{(t)} := Z_{(128)}^{(t-1)} \oplus V_{(32)}^{(t)} || Z_{3(32)}^{(t)} \oplus V_{(32)}^{(t)} || Z_{4(32)}^{(t)} \oplus V_{(32)}^{(t)} || Z_{2(32)}^{(t-1)} \oplus Z_{4(32)}^{(t)}$.

Подстановка s в $Hierocrypt$ является композицией трех подстановок:

$$s(x_{(8)}) = Add\ (Power\ (Perm\ (x_{(8)}))),$$

$$y_{(8)} = Perm(x_{(8)})),\ y_{i(1)} = x_{\pi[i](1)}.$$

Преобразование $Perm$ осуществляет перестановку битов в байте $x_{(8)}$ согласно таблице 1 (бит 3 перемещается в позицию 1, бит 7 – в позицию 2 и т.д.; при этом бит 1 является старшим, т.е.

$$N(x_{(8)}) = \sum_{i=1}^{8} x_{i(1)}\, 2^{8-i});$$

Таблица 1

i	1	2	3	4	5	6	7	8
$\pi[i]$	3	7	5	8	6	2	4	1

$$Power: \mathbb{F}_{256} \longrightarrow \mathbb{F}_{256},\ \ Power\ (x_{(8)}) = (x_{(8)})^{247}.$$

В $Power$ байты интерпретируются как элементы конечного поля $\mathbb{F}_{256} \cong \mathbb{F}_2[z]\ /\ p(z))$, где $p(z) = z^8 + z^6 + z^5 + z + 1$; при этом байту $x_{(8)} = x_{1(1)}||x_{2(1)}|| \ldots ||x_{8(1)}$ сопоставляется многочлен $x_{1(1)}z^7 + x_{2(1)}z^6 + \cdots + x_{7(1)}z^1 + x_{8(1)}$, рассматриваемый как элемент поля $\mathbb{F}_{256}$;

$$Add\ (x_{(8)})) = x_{(8)} \oplus 0x07.$$

Обратная подстановка s^{-1} имеет вид:

$$s^{-1}(x) = Perm^{-1}\left(Power^{-1}\left(Add^{-1}(x)\right)\right) = Perm^{-1}\ ((x \oplus 0x07)^{223}),$$

где возведение в степень осуществляется в том же поле $\mathbb{F}_{256}$, а подстановка $Perm^{-1}$ задается таблицей 2:

Таблица 2

i	1	2	3	4	5	6	7	8
$\pi^{-1}[i]$	8	6	1	7	3	5	2	4

Функции MDS_L и MDS_L^{-1}, mds_L и mds_L^{-1}, MDS_H и MDS_H^{-1}, M_5 и M_B, F_σ, $P^{(n)}$ и $\left(P^{(n)}\right)^{-1}$определяются следующим образом:

$MDS_L\left(X_{(64)}\right)_{(64)} = mds_L\left(X_{1(32}\right)|| mds_L\left(X_{2(32}\right)$,

$MDS_L^{-1}\left(X_{(64)}\right)_{(64)} = mds_L^{-1}\left(X_{1(32}\right)|| mds_L^{-1}\left(X_{2(32}\right)$;

$mds_L\left(X_{(32}\right)_{(32)} = y_{1(8)} || y_{2(8)}|| y_{3(8)}||y_{4(8)}$,

$mds_L^{-1}\left(X_{(32}\right)_{(32)} = z_{1(8)} || z_{2(8)}|| z_{3(8)}||z_{4(8)}$,

где

$$\begin{pmatrix} y_{1(8)} \\ y_{2(8)} \\ y_{3(8)} \\ y_{4(8)} \end{pmatrix} = A \cdot \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \end{pmatrix}, \qquad \begin{pmatrix} z_{1(8)} \\ z_{2(8)} \\ z_{3(8)} \\ z_{4(8)} \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \end{pmatrix},$$

$$A = \begin{pmatrix} 0\text{x}c4 & 0\text{x}65 & 0\text{x}c8 & 0\text{x}8b \\ 0\text{x}8b & 0\text{x}c4 & 0\text{x}65 & 0\text{x}c8 \\ 0\text{x}c8 & 0\text{x}8b & 0\text{x}c4 & 0\text{x}65 \\ 0\text{x}65 & 0\text{x}c8 & 0\text{x}8b & 0\text{x}c4 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} 0\text{x}82 & 0\text{x}c4 & 0\text{x}34 & 0\text{x}f6 \\ 0\text{x}f6 & 0\text{x}82 & 0\text{x}c4 & 0\text{x}34 \\ 0\text{x}34 & 0\text{x}f6 & 0\text{x}82 & 0\text{x}c4 \\ 0\text{x}c4 & 0\text{x}34 & 0\text{x}f6 & 0\text{x}82 \end{pmatrix}.$$

Здесь байты $y_{1(8)}$, $z_{1(8)}$, $x_{i(8)}$ и элементы матриц A и A^{-1} интерпретируются как элементы указанного выше поля $\mathbb{F}_{256}$.

Функции MDS_H и MDS_H^{-1}:

$$MDS_H\left(X_{(64)}\right)_{(64)} = y_{1(8)} \,||\, y_{2(8)} || \, y_{3(8)} || y_{4(8)},$$

$$MDS_H^{-1}\left(X_{(64)}\right)_{(64)} = z_{1(8)} \,||\, z_{2(8)} || \, z_{3(8)} || z_{4(8)},$$

где

$$\begin{pmatrix} y_{1(8)} \\ y_{2(8)} \\ y_{3(8)} \\ y_{4(8)} \\ y_{5(8)} \\ y_{6(8)} \\ y_{7(8)} \\ y_{8(8)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \\ x_{5(8)} \\ x_{6(8)} \\ x_{7(8)} \\ x_{8(8)} \end{pmatrix},$$

(т.е. $y_{1(8)} = x_{1(8)} \oplus x_{3(8)} \oplus x_{5(8)} \oplus x_{6(8)} \oplus x_{7(8)}$ и т.д.),

$$\begin{pmatrix} z_{1(8)} \\ z_{2(8)} \\ z_{3(8)} \\ z_{4(8)} \\ z_{5(8)} \\ z_{6(8)} \\ z_{7(8)} \\ z_{8(8)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \\ x_{5(8)} \\ x_{6(8)} \\ x_{7(8)} \\ x_{8(8)} \end{pmatrix}.$$

Функции M_5 и M_B (см. рис. 3):

$$M_5\left(X_{(32)}\right)_{(32)} = y_{1(8)} \,||\, y_{2(8)} || \, y_{3(8)} || y_{4(8)},$$

где

$$\begin{pmatrix} y_{1(8)} \\ y_{2(8)} \\ y_{3(8)} \\ y_{4(8)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \end{pmatrix};$$

$$M_B\left(X_{(32)}\right)_{(32)} = y_{1(8)} \,||\, y_{2(8)} || \, y_{3(8)} || y_{4(8)},$$

где

$$\begin{pmatrix} y_{1(8)} \\ y_{2(8)} \\ y_{3(8)} \\ y_{4(8)} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \end{pmatrix};$$

Функция F_σ (см. рис.4):

$$F_\sigma\left(X_{(32)}\right)_{(32)} = P^{(8)}\left(s(x_{1(8)}) \,||\, s(x_{2(8)}) \,||\, s(x_{3(8)}) \,||\, s(x_{4(8)})\right).$$

Функции $P^{(n)}$ и $\left(P^{(n)}\right)^{-1}$, $n = 8$, 16 или 32 (см. рис.5):

$$P^{(n)}\left(X_{(4n)}\right)_{(4n)} = y_{1(n)} \,||\, y_{2(n)} || \, y_{3(n)} || y_{4(n)},$$

$$(P_{(n)})^{-1}\,(X_{(4n)})_{(4n)} = z_{1(n)} \,||\, z_{2(n)} || \, z_{3(n)} || z_{4(n)},$$

где

$$\begin{pmatrix} y_{1(8)} \\ y_{2(8)} \\ y_{3(8)} \\ y_{4(8)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \end{pmatrix}, \quad \begin{pmatrix} z_{1(8)} \\ z_{2(8)} \\ z_{3(8)} \\ z_{4(8)} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \end{pmatrix}.$$

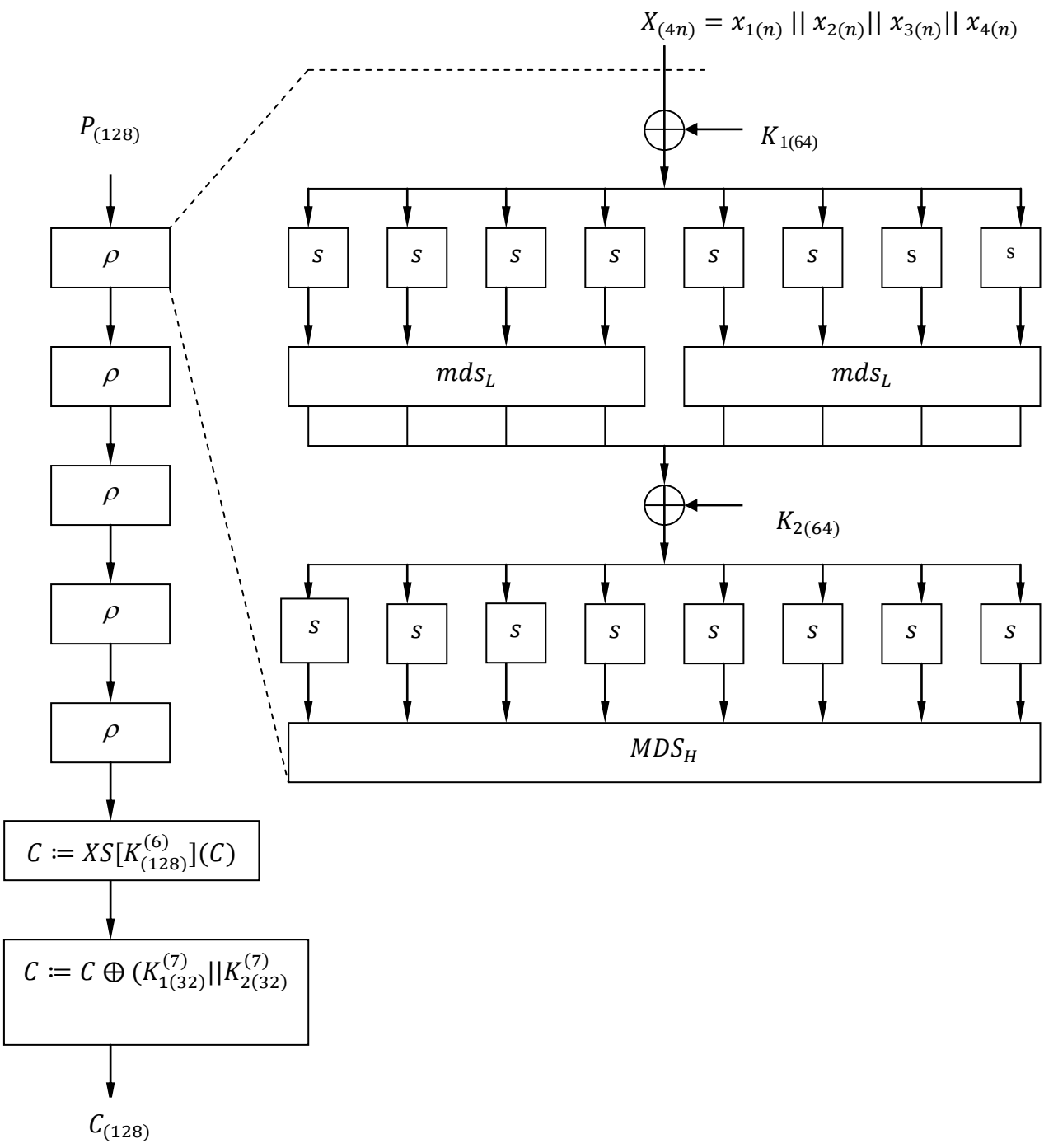


Рис. 1. *Структура алгоритма* $Hierocrypt - L1$

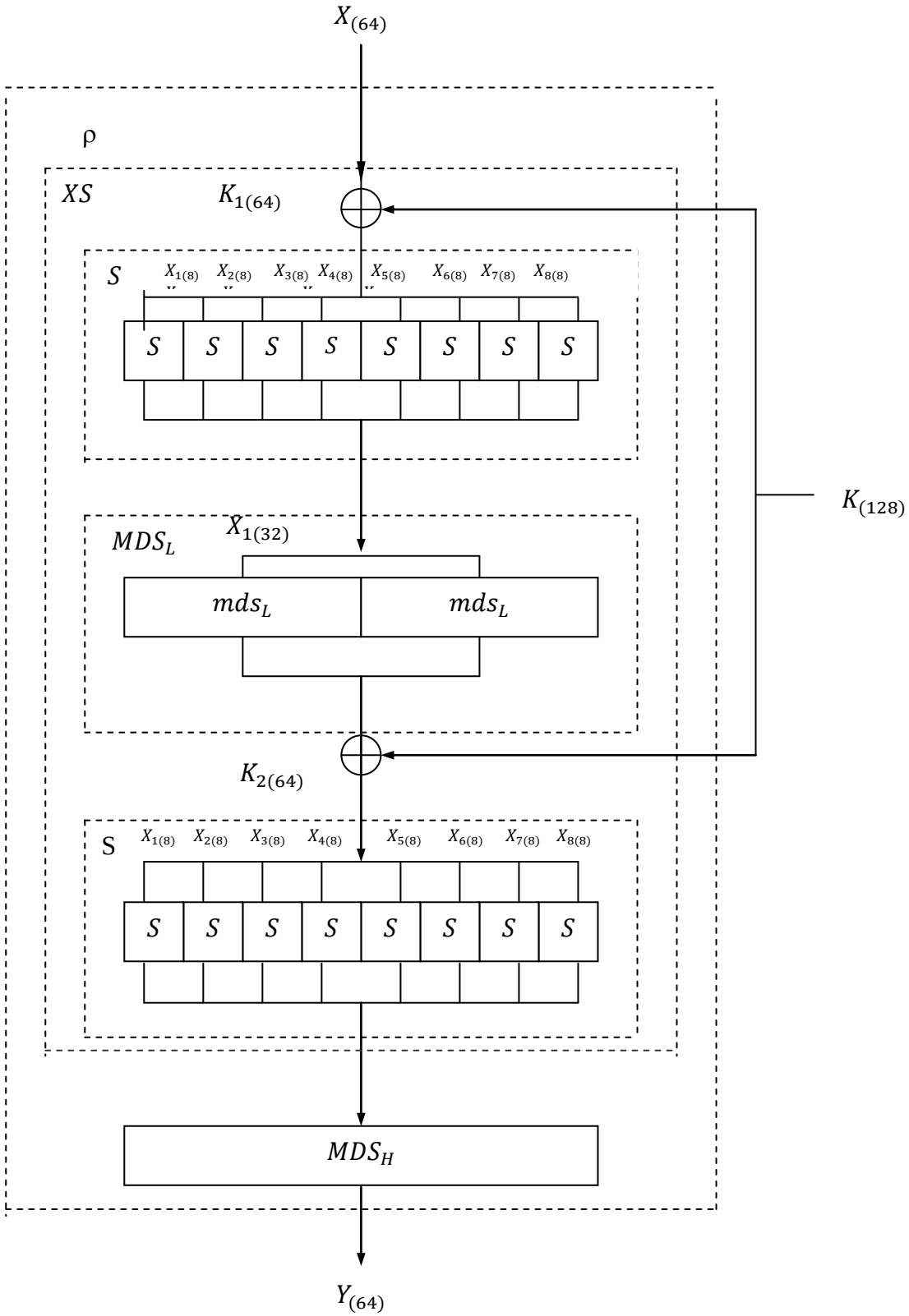


Рис. 2. *Функция* ρ

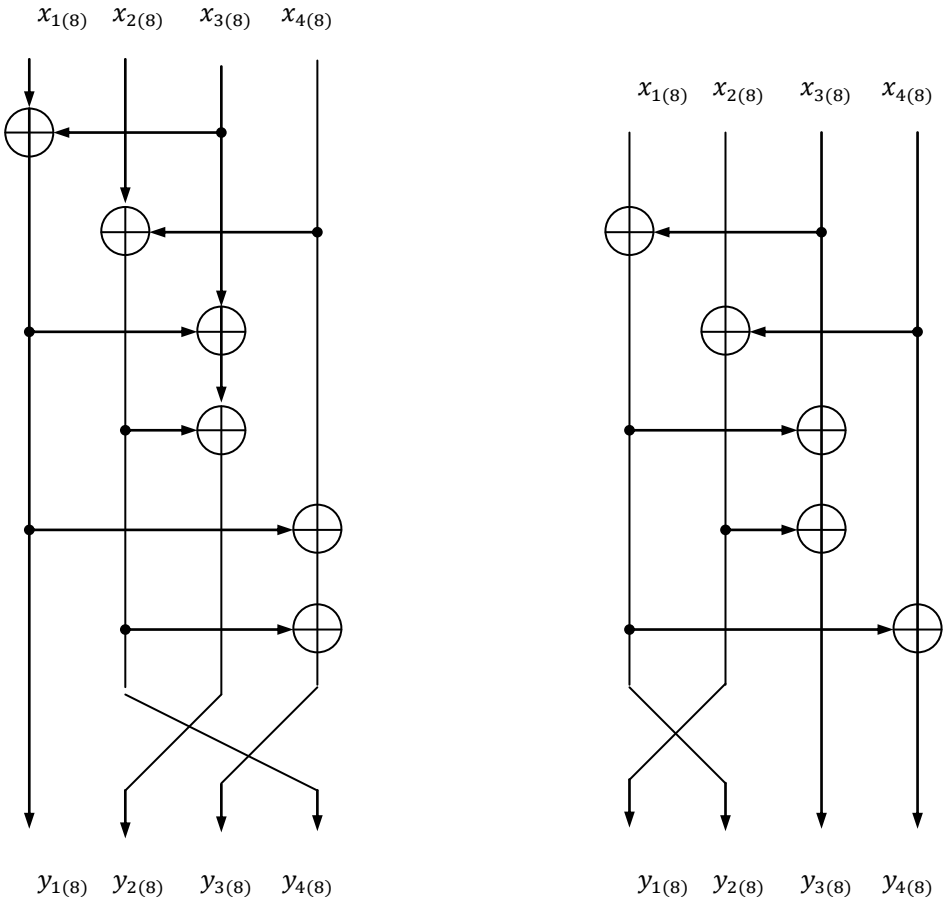


Рис. 3. *Функции* M_5 *и* M_B

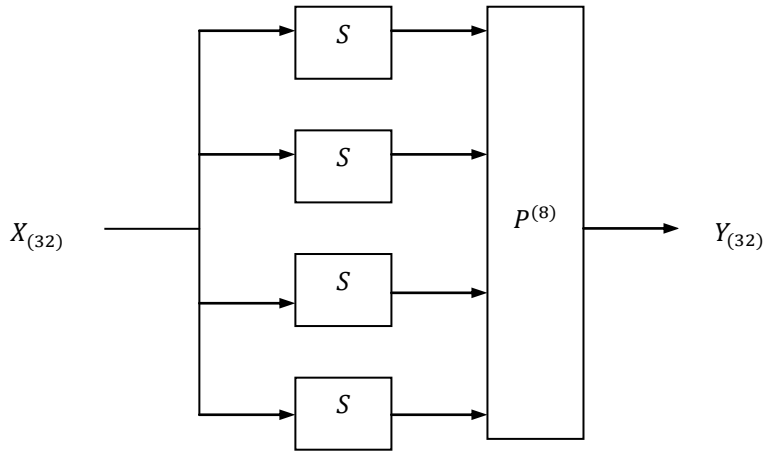
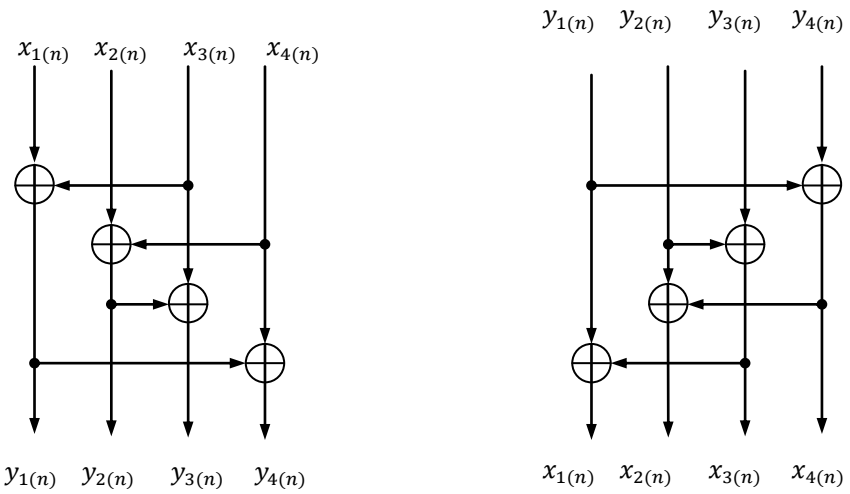


Рис. 4. *Функция* F_σ



$$y_1 := x_1 \oplus x_3 \qquad x_4 := y_1 \oplus y_4$$
$$y_2 := x_2 \oplus x_4 \qquad x_3 := y_2 \oplus y_3$$
$$y_3 := y_2 \oplus x_3 \qquad x_2 := y_2 \oplus x_4$$
$$y_4 := y_1 \oplus x_4 \qquad x_1 := y_1 \oplus x_3$$

Рис. 5. *Функции* $P^{(n)}$ *и* $(P^{(n)}))^{-1}$

$\boldsymbol{Hierocrypt-3}$. T-раундовый алгоритм $Hierocrypt-3$ состоит из $T-1$ раундов, в которых применяется преобразование ρ, преобразования XS и заключительного забеливания, выполняемых под управлением раундовых подключей $K_{(128)}^{(t)}$, $t = 1, 2, \dots, T+1$. Значение T равно 6, 7 или 8 соответственно для 128-, 192- и 256-битового секретного ключа K.

Алгоритм зашифрования $\boldsymbol{Hierocrypt-3}$

Вход: P – 128-битовый блок открытых данных.

$C := P$;

for $t := 1$ ***to*** $T-1$ ***do*** $C := \rho(C, K_{(256)}^{(t)})$;

$XS(C, K_{(256)}^{(T)})$;

$C := C \oplus (K_{1(64)}^{(T+1)} || K_{2(64)}^{(T+1)})$.

Выход: C – 128-битовый блок шифртекста.

Алгоритм расшифрования $\boldsymbol{Hierocrypt-3}$

Вход: C – 128-битовый блок шифртекста.

$P := C \oplus (K_{1(64)}^{(T+1)} || K_{2(64)}^{(T+1)})$;

$XS^{-1}(P, K_{(256)}^{(T)})$;

for $t := T-1$ ***downto*** 1 ***do*** $P := \rho^{-1}(P, K_{(256)}^{(T)})$.

Выход: P – 128-битовый блок открытых данных.

Генерация раундовых подключей в $\boldsymbol{Hierocrypt-3}$

При вычислении раундовых подключей $K_{(256)}^{(t)} = K_{1(64)}^{(t)} || K_{2(64)}^{(t)} || K_{3(64)}^{(t)} || K_{4(64)}^{(t)}$, $t = 1, 2, \dots, T+1$, используются вспомогательные переменные

$Z_{(256)}^{(t)} = Z_{1(64)}^{(t)} || Z_{2(64)}^{(t)} || Z_{3(64)}^{(t)} || Z_{4(64)}^{(t)}$, $K_{(64)}^{(t)}$, $t = -1, 0, 1, \dots, T+1$;

$W_{1(128)}^{(t)} = W_{1(64)} || W_{2(64)}$, $t = t_{turn} + 1, \dots, T+1$,

где $t_{turn} = (T+2)\ div\ 2$ (т.е. $t_{turn} = 4$ для 128- и 192-битового секретного ключа и $t_{turn} = 5$ для 256-битового секретного ключа); $Y_{(64)}$, $U_{(128)} = U_{1(64)} || U_{2(64)}$ и 64-битовые константы G_t, заданные таблицей 2 (значения 32-битовых констант H_0, H_1, H_2, H_3 те же, что и для алгоритма $Hierocrypt - L1$).

Таблица 2

Константы G_t в $Hierocrypt$-3

t	$L(K)$ – длина секретного ключа К		
	128	192	256
-1	$H_3 \| \| H_2$	$H_2 \| \| H_3$	–
0	$H_1 \| \| H_0$	$H_1 \| \| H_0$	$H_1 \| \| H_0$
1	$H_3 \| \| H_0$	$H_2 \| \| H_1$	$H_2 \| \| H_3$
2	$H_2 \| \| H_1$	$H_3 \| \| H_0$	$H_3 \| \| H_0$
3	$H_1 \| \| H_3$	$H_0 \| \| H_2$	$H_1 \| \| H_3$
4	$H_0 \| \| H_2$	$H_1 \| \| H_3$	$H_2 \| \| H_1$
5	$H_0 \| \| H_2$	$H_1 \| \| H_3$	$H_0 \| \| H_2$
6	$H_1 \| \| H_3$	$H_0 \| \| H_2$	$H_0 \| \| H_2$
7	$H_2 \| \| H_1$	$H_3 \| \| H_0$	$H_2 \| \| H_1$
8	–	$H_2 \| \| H_1$	$H_1 \| \| H_3$
9	–	–	$H_3 \| \| H_0$

$\boldsymbol{if}\ L(K) = 128\ \boldsymbol{then}\ Z_{(256)}^{(-1)} := K || K_{1(64)} || G_{-1}$

$\boldsymbol{else\ if}\ L(K) = 192\ \boldsymbol{then}\ Z_{(256)}^{(-1)} := K || G_{-1} \boldsymbol{else}\ Z_{(256)}^{(-1)} := K;$

$Y_{(64)} := M_{5E}\left(Z_{3(64)}^{(-1)} \right) \oplus G_0;$

$Z_{(256)}^{(0)} := Z_{2(64)}^{(-1)} || \left(Z_{1(64)}^{(-1)} \oplus F_\sigma \left(Z_{2(64)}^{(-1)} \oplus Y_{(64)} \right) \right) || Y_{(64)} || M_{5E}(Z_{4(64)}^{(-1)});$

$\boldsymbol{for}\ t := 1\ \boldsymbol{to}\ t_{turn}\ \boldsymbol{do}\ \{$

$U(128) := P^{(32)} \left(Z_{3(64)}^{(t-1)} || Z_{4(64)}^{(t-1)} \right);$

$Y_{(64)} := M_{5E}(U1(64) \oplus G_t;$

$V_{(64)} := F_\sigma \left(Z_{2(64)}^{(t-1)} \oplus Y_{(64)} \right);$

$Z_{(256)}^{(t)} := Z_{2(64)}^{(t-1)} || \left(Z_{1(64)}^{(t-1)} \oplus V_{(64)}^{(t)} \right) || Y_{(64)} || M_{5E}\left(U_{2(64)} \right)$

$\};$

$\boldsymbol{for}\ t := t_{turn} + 1\ \boldsymbol{to}\ T+1\ \boldsymbol{do}\ \{$

$Z_{(256)}^{(t)} := Z_{(256)}^{(2t_{turn}-t)};$

$V_{(64)}^{(t)} := F_\sigma \left(Z_{1(64)}^{(t-1)} \oplus Z_{3(64)}^{(t-1)} \right);$

$W_{(128)}^{(t)} := M_{B3}\left(Z_{3(64)}^{(t-1)} \oplus G_t \right) || M_{B3}\left(Z_{4(64)}^{(t-1)} \right)$

$\};$

$\boldsymbol{for}\ t := 1\ \boldsymbol{to}\ t_{turn}\ \boldsymbol{do}$

$K_{(256)}^{(t)} := Z_{1(64)}^{(t-1)} \oplus V_{(64)}^{(t)} || Z_{3(64)}^{(t-1)} \oplus V_{(64)}^{(t)} || Z_{4(64)}^{(t-1)} \oplus V_{(64)}^{(t)} || Z_{2(64)}^{(t-1)} \oplus V_{(64)}^{(t)};$

$\boldsymbol{for}\ t := t_{turn} + 1\ \boldsymbol{to}\ T+1\ \boldsymbol{do}$

$K_{(256)}^{(t)} := Z_{1(64)}^{(t)} \oplus Z_{3(64)}^{(t-1)} || W_{1(64)}^{(t)} \oplus V_{(64)}^{(t)} || W_{2(64)}^{(t)} \oplus V_{(64)}^{(t)} || Z_{1(64)}^{(t-1)} \oplus W_{2(64)}^{(t)}.$

Функции, используемые в $Hierocrypt$-3

Обозначения:

$x_{1(8)} || x_{2(8)} || \dots || x_{16(8)} = X_{1(32)} || X_{2(32)} || X_{3(32)} || X_{4(32)} = X_{(128)},$

$x_{1(8)} || x_{2(8)} || \dots || x_{8(8)} = X_{(64)},$

$K_{1(128)} || K_{2(128)} = K_{(256)}.$

Функция ρ:

$$\rho\,(X_{(128)}, K_{(256)})_{(128)} = MDS_H(XS(X_{(128)}, K_{(256)})).$$

Функция MDS_H:

$$MDS_H\big(X_{(128)}\big)_{(128)} = y_{1(8)} \,||\, y_{2(8)}|| \ldots ||y_{16(8)},$$

где

$$\begin{pmatrix} y_{1(8)} \\ y_{2(8)} \\ y_{3(8)} \\ y_{4(8)} \\ y_{5(8)} \\ y_{6(8)} \\ y_{7(8)} \\ y_{8(8)} \\ y_{9(8)} \\ y_{10(8)} \\ y_{11(8)} \\ y_{12(8)} \\ y_{13(8)} \\ y_{14(8)} \\ y_{15(8)} \\ y_{16(8)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \\ x_{5(8)} \\ x_{6(8)} \\ x_{7(8)} \\ x_{8(8)} \\ x_{9(8)} \\ x_{10(8)} \\ x_{11(8)} \\ x_{12(8)} \\ x_{13(8)} \\ x_{14(8)} \\ x_{15(8)} \\ x_{16(8)} \end{pmatrix},$$

т.е. $y_{1(8)} = x_{1(8)} \oplus x_{3(8)} \oplus x_{5(8)} \oplus x_{7(8)} \oplus x_{9(8)} \oplus x_{10(8)} \oplus x_{12(8)} \oplus x_{13(8)} \oplus x_{14(8)} \oplus x_{15(8)} \oplus x_{16(8)}$ и т.д.

Функция XS:

$$XS(X_{(128)}, K_{(256)})_{(128)} = S\,(MDS_L(S(X_{(128)} \oplus K_{1(128)})) \oplus K_{2(128)}).$$

Функция S:

$$S(X_{(128)})_{(128)} = s(x_{1(8)})||s(x_{2(8)})|| \ldots ||s(x_{16(8)}),$$

где s – подстановка на множестве байтов, заданная таблицей 1 (в описании $Hierocrypt - L1$).

Функция MDS_L:

$$MDS_L\,(X_{(128)})_{(128)} = mds_L(X_{1(32)}) \,||\, mds_L(X_{2(32)}) \,||mds_L(X_{3(32)}) \,||mds_L(X_{4(32)}),$$

где mds_L – функция, определенная в $Hierocrypt - L1$.

Функция $P^{(n)}$ – та же, что и в $Hierocrypt - L1$.

Функция M_{5E}:

$$M_{5E}(X_{(64)})_{(64)}) = y_{1(8)} \,||y_{2(8)} \,|| \ldots ||y_{8(8)}\,, \text{ где}$$

$$\begin{pmatrix} y_{1(8)} \\ y_{2(8)} \\ y_{3(8)} \\ y_{4(8)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \end{pmatrix} \qquad \begin{pmatrix} y_{5(8)} \\ y_{6(8)} \\ y_{7(8)} \\ y_{8(8)} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_{5(8)} \\ x_{6(8)} \\ x_{7(8)} \\ x_{8(8)} \end{pmatrix}$$

Функция M_{B3}:

$$M_{B3}(X_{(64)})_{(64)} = y_{1(8)} \,||y_{2(8)} \,|| \ldots ||y_{8(8)}\,,$$

где

$$\begin{pmatrix} y_{1(8)} \\ y_{2(8)} \\ y_{3(8)} \\ y_{4(8)} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_{1(8)} \\ x_{2(8)} \\ x_{3(8)} \\ x_{4(8)} \end{pmatrix}, \qquad \begin{pmatrix} y_{5(8)} \\ y_{6(8)} \\ y_{7(8)} \\ y_{8(8)} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_{5(8)} \\ x_{6(8)} \\ x_{7(8)} \\ x_{8(8)} \end{pmatrix}$$

Функция F_σ:

$$F_\sigma\,(\,X_{(64)})_{(64)} = P^{(16)}(s(x_{1(8)}) \,||\, s(x_{2(8)})|| \ldots || \,s(x_{8(8)})).$$