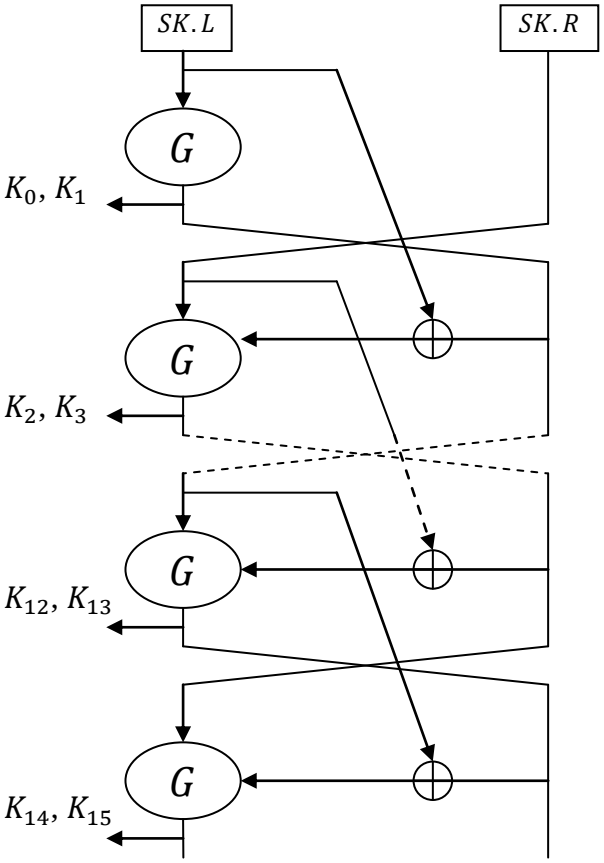
FEAL

***FEAL*-8.** Криптоалгоритм *FEAL*-8 (*Fast Data Encipherment Algorithm*) [1] шифрует 64-битовые блоки открытых данных под управлением открытого ключа такого же размера.



Вход: SK – 64-битовый секретный ключ. Ключ SK разбивается на две 32-битовые половины: $SK.L$ (левая) и $SK.R$ (правая), а $SK.L$, в свою очередь, разбивается на 16-битовые половины $SK.L.L$ (левая) и $SK.L.R$ (правая).

$A := SKL;$
$K_0 := SKLL;\ K_1 := SKLR;$
for $i :=\ 1$ ***to*** 6 ***do*** {
$SKL \leftrightarrow SKR;$
$B := SKL;$
$SKL := G(SKL, SKR \oplus A);$
$K_{2i} := SKLL;$
$K_{2i+1:} = SKLR;$
$A := B$
};
$SKL := G(SKR, SKL \oplus A);$
$K_{14} := SKLL;$
$K_{15} := SKLR\,.$

Выход: Раундовые подключи
$K_0, K_1, \ldots, K_{14}, K_{15}$.

Рис. 1. *Генерация раундовых подключей в FEAL-8*

$x_1 := x_0 \oplus x_1;$
$x_2 := x_2 \oplus x_3;$
$z_1 := S_1(x_1, x_2 \oplus y_0);$
$z_0 := S_0(x_0, z_1 \oplus y_2);$
$z_2 := S_0(x_2, z_1 \oplus y_1);$
$z_3 := S_1(x_3, z_2 \oplus y_3)\,.$

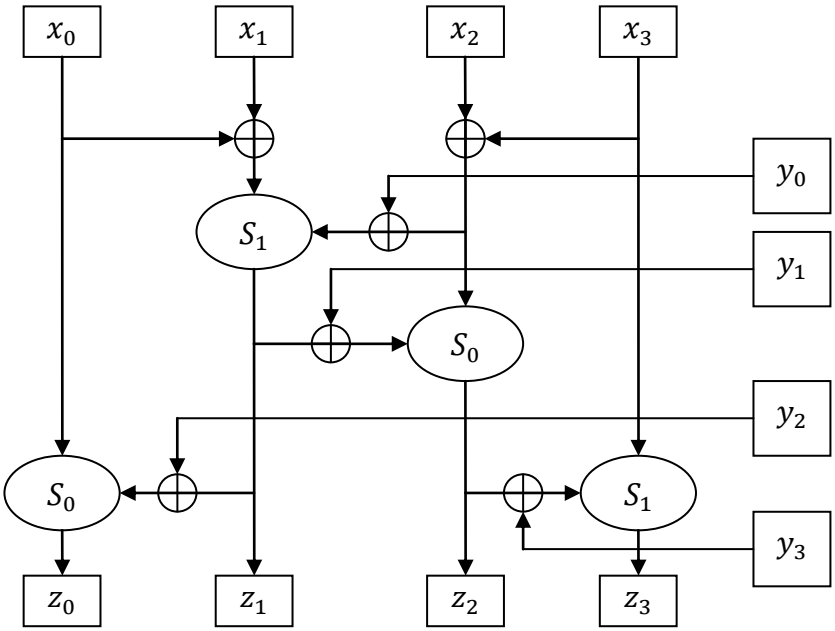
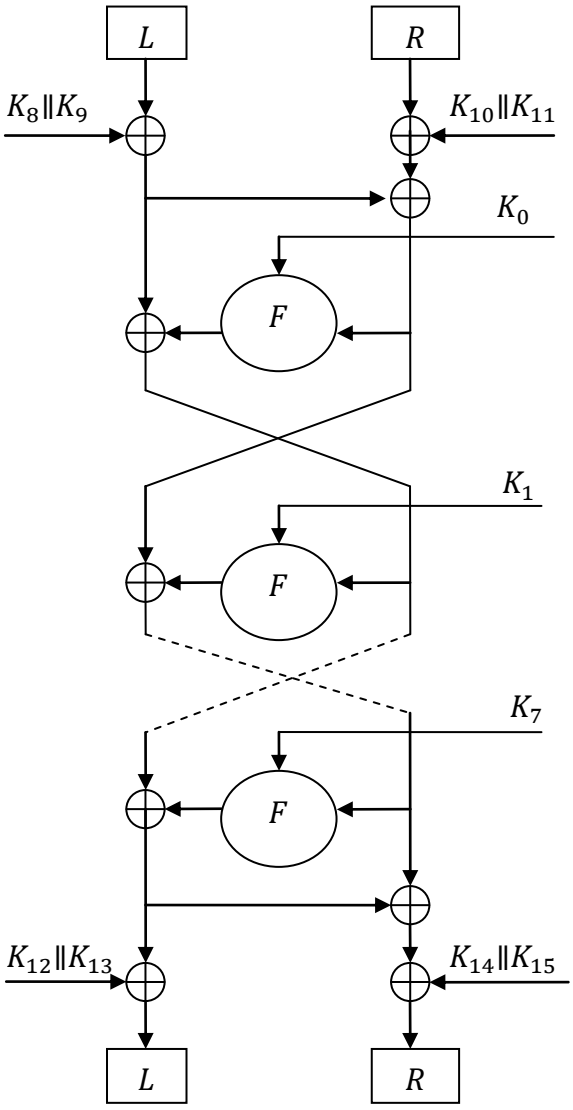


Рис. 2. *Функция g, используемая при генерации раундовых подключей в FEAL-8*

[1] Авторы шифра: *Akihiro Shimizu* и *Shoji Miyaguchi* (Япония)



Вход: $P = L \parallel R$ – 64-битовый блок открытых данных, представленный в виде конкатенаций 32-битовых подблоков L и R.

1. (Начальное забеливание.)
   $P := P \oplus (K_8 \parallel K_9 \parallel K_{10} \parallel K_{11})$;
   $P := R \oplus L$;
2. (8 раундов зашифрования.)
   for $i := 0$ ***to*** 6 ***do*** {
   $L \coloneqq L \oplus F(R, K_i)$;
   $L \leftrightarrow R$
   };
   $L := L \oplus F(R, K_7)$;
3. (Конечное забеливание.)
   $R := R \oplus L$;
   $C := P \oplus (K_{12} \parallel K_{13} \parallel K_{14} \parallel K_{15})$.

Выход: C– 64-битовый блок шифртекста.

Рис. 3. *Алгоритм зашифрования в* $FEAL$-8

На этапе предвычислений секретный ключ SK преобразуется в шестнадцать 16-битовых (2-байтовых) раундовых подключей: K_0, K_1,…, K_{14}, K_{15} (см. рис. 1).

Используемая при этом функция $G(\mathrm{X}, Y)$ от 4-байтовых аргументов $X = (x_0, x_1, \mathrm{x}_2, x_3)$ и $Y = (y_0, y_1, y_2, y_3)$, возвращающая 4-байтовое значение $Z = (z_0, z_1, z_2, z_3)$, представлена на рис.2

Функции $S_0(x, y)$ и $S_1(x, y)$ от однобайтовых аргументов x, y возвращают однобайтовые значения: $S_0(x, y) = (x + y)$, $S_1(x, y) = rol_2(x + y + 1)$, где $a + b$ – сложение байтов a и b по модулю 256, а $rol_2(a)$ – циклический сдвиг байта a на 2 бита влево.

По своей структуре $FEAL$-8 является классическим шифром Фейстеля (см. рис. 3). Раундовая функция $F(\mathrm{X}, K)$ от 4-байтового аргумента $X = (x_0, x_1, x_2, x_3)$ и двухбайтового аргумента $K = (k_0, k_1)$ представлена на рис. 4.

Для расшифрования используется тот же алгоритм, что и для зашифрования, но при другом порядке использования раундовых подключей, а именно:

$$K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_{12}, K_{13}, K_{14}, K_{15}, K_8, K_9, K_{10}, K_{11}.$$

$y_1 := S_1(x_0 \oplus x_1 \oplus k_0, x_2 \oplus x_3 \oplus k_1);$
$y_0 := S_0(x_0, y_0);$
$y_2 := S_0(y_1, x_2 \oplus x_3 \oplus k_1);$
$y_3 := S_1(x_3, y_2).$

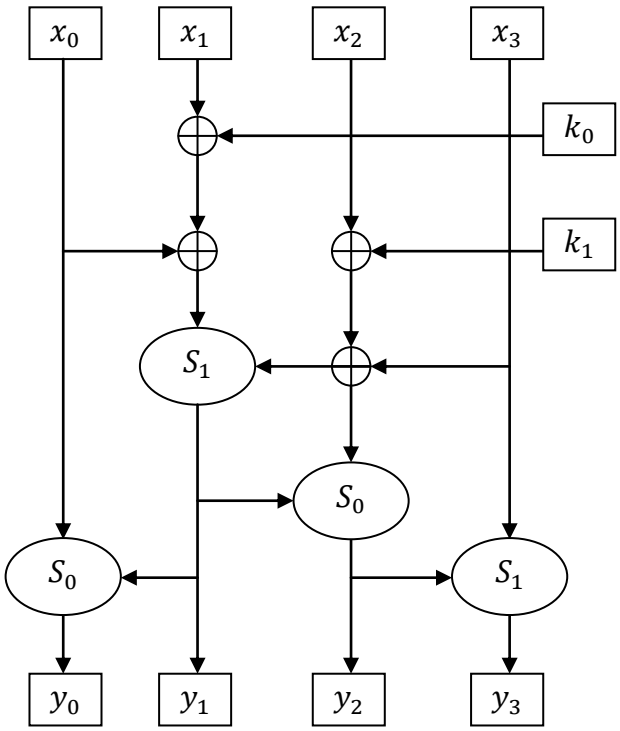


Рис. 4. *Раундовая функция F в $FEAL$-8*

***FEAL–NX*.** В FEAL-NX используется тот же алгоритм зашифрования (и расшифрования), что и в $FEAL$-8, но число N раундов шифрования может быть переменным (N – четное число ≥ 8; стандартное значение $N = 32$), а длина секретного ключа CK увеличена до 128 битов. (Если $N = 8$ и правая половина ключа Q нулевая, то $FEAL$-NX совпадает с $FEAL$-8.) Развертка ключа

$$SK = (SK_0, SK_1, SK_2, SK_3, SK_4, SK_5, SK_6, SK_7),$$

где SK_i – 16-битовые составляющие SK), в последовательность K_0, K_1,…, K_{n+7} 16-битных раундовых подключей, используемых в $FEAL$-NX, осуществляется по схеме, представленной на рис. 5.

Алгоритм генерации раундовых подключей в *FEAL-NX*

$L := (SK_0, SK_1);$
$R := (SK_2, SK_3);$
$C_1 := (SK_4, SK_5);$
$C_2 := (SK_6, SK_7);$
$C_0 := C_1 \oplus C_2;$
$A := L;$
$L := G(L, R \oplus C_0);$
$(K_0, K_1) := L;$
$L \leftrightarrow R;$
$n := (N + 4)\ div\ 2;$
for $i := 1$ ***to*** n ***do*** {
    $B := L;$
    $L := G(L, R \oplus A \oplus C_{i\ mod\ 3});$
    $A := B;$
    $(K_{2i}, K_{2i+1}) := L;$
    $L \leftrightarrow R$
};
$L := G(L, R \oplus A \oplus C_{(n+1)\ mod\ 3});$
$(K_{N+6}, K_{N+7}) := L.$

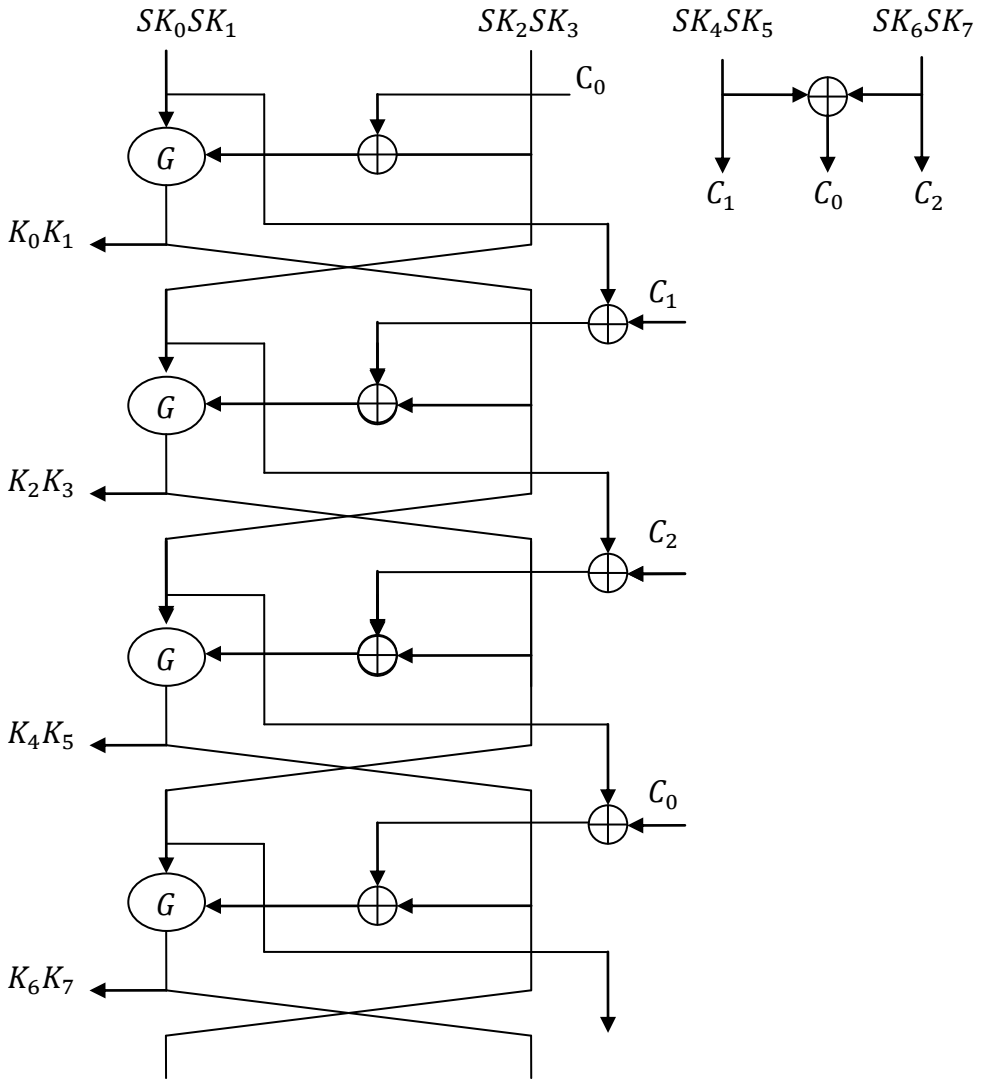


Рис. 5. *Генерация раундовых подключей в FEA*L-*NX*