Camellia

Криптоалгоритм Camellia[1] шифрует 128-битовые блоки открытых данных под управлением секретного ключа, длина которого может составлять 128, 192 или 256 битов. Далее рассматривается случай 128-битового ключа.

Алгоритм зашифрования построен в соответствии с 18-раундовой схемой Фейстеля, дополненной входным и выходным забеливанием, а также преобразованиями FL и FL^{-1} после 6-го и 12-го раундов. Процедура зашифрования иллюстрируется на рис.1. Раундовые подключи вычисляются на основе секретного ключа и имеют длину 64 бита. Подключи kw_t $(t = 1,2,3,4)$ используются для входного и выходного забеливания; k_u $(u = 1, 2, \dots, 18)$ – в раундовой функции, а kl_v $(v = 1, 2, 3, 4)$ – в функциях FL и FL^{-1}. Алгоритм симметричен, т.е. может быть использован и для расшифрования, но при расшифровании раундовые подключи используются в обратном порядке.

Алгоритм зашифрования

Вход: $M = L||R$ – 128-битовый блок открытых данных, представленный в виде конкатенации 64-битовых подблоков L и R.

$M := M \oplus (kw_1||kw_2)$;
for $i := 1$ ***to*** 6 ***do*** {
    $R := R \oplus F(L, k_i)$;
    $L \leftrightarrow R$ (L и R обмениваются значениями)
};
$(L, R) := (FL(L, kl_1), FL^{-1}(R, kl_2))$;
for $i := 7$ ***to*** 12 ***do*** {
    $R := R \oplus F(L, k_i)$; $L \leftrightarrow R$
};
$(L, R) := (FL(L, kl_3), FL^{-1}(R, kl_4))$;
for $i := 13$ ***to*** 18 ***do*** {
    $R := R \oplus F(L, k_i)$;
    $L \leftrightarrow R$
};
$C := (R \,||\, L) \oplus (kw_3 \,||\, kw_4)$.

Выход: C – 128-битовый блок шифртекста.

Вычисление раундовых подключей

На рис.2 представлена схема вычисления вспомогательного 128-битовго ключа Q на основе секретного ключа K. Значения используемых при этом 64-битовых раундовых констант $\sum_i$ приведены в табл.1. В качестве $\sum_i$ взяты шестнадцатеричные цифры дробной части числа $\sqrt{p_i}$, где p_i – i-ое простое число ($p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7$), начиная со второй цифры.

Таблица 1

Раундовые константы в Camellia при вычислении вспомогательного ключа Q

$\sum_1$	0x$a09e667f3bcc908b$
$\sum_2$	0x$b67ae8584caa73b2$
$\sum_3$	0x$c6ef372fe94f82be$
$\sum_4$	0x$54ff53a5f1d36f1c$

Значение раундовых подключей kw_t, kw_u и kw_v приведены в таблице 2, где $X.L$ и $X.R$ обозначают соответственно левую и правую половины блока X.

[1] Авторы шифра: *K.Aoki*, *M.Kanda*, *M.Matsui*, *S.Moriari*, *J.Nakajima* и *T.Tokita* (Япония, Японская телеграфная и телефонная корпорация и Электрическая корпорация Мицубиси)

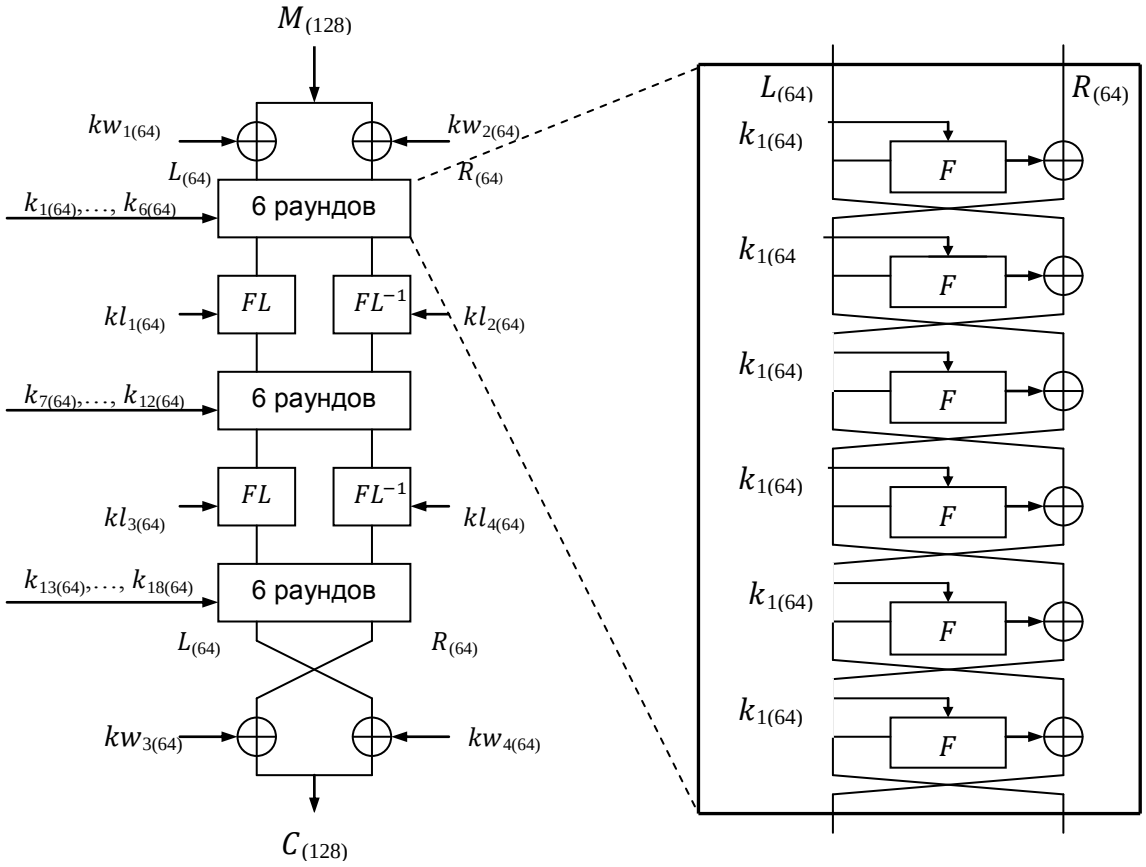

Рис.1. *Алгоритм зашифрования в Camellia* (*для* 128-*битового секретного ключа*)

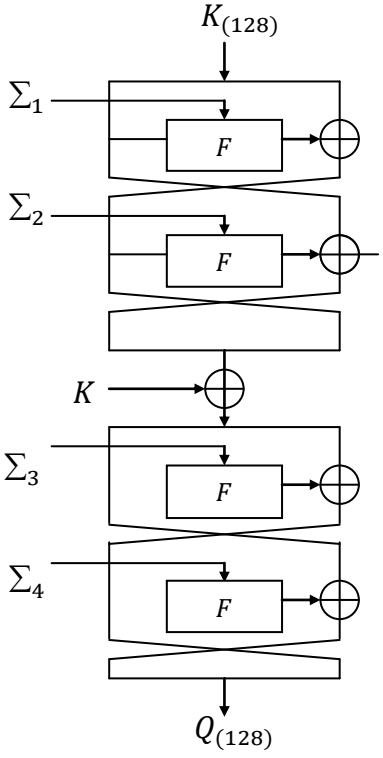

Рис.2. *Вычисление вспомогательного* 128-*битового ключа* Q *в Camellia* (*для 128-битового секретного ключа* K)

Таблица 2

Расписание раундовых подключей в $Camellia$ (*для* 128*-битового секретного ключа*)

Входное забеливание	Подключ	Значение
	kw_1	$K.L$
	kw_2	$K.R$
F (раунд 1)	k_1	$Q.L$
F (раунд 2)	k_2	$Q.R$
F (раунд 3)	k_3	$(rol_{15}K).L$
F (раунд 4)	k_4	$(rol_{15}K).R$
F (раунд 5)	k_5	$(rol_{15}Q).L$
F (раунд 6)	k_6	$(rol_{15}Q).R$
FL	kl_1	$(rol_{30}Q).L$
FL^{-1}	kl_2	$(rol_{30}Q).R$
F (раунд 7)	k_7	$(rol_{45}K).L$
F (раунд 8)	k_8	$(rol_{45}K).R$
F (раунд 9)	k_9	$(rol_{45}Q).L$
F (раунд 10)	k_{10}	$(rol_{60}K).R$
F (раунд 11)	k_{11}	$(rol_{60}Q).L$
F (раунд 12)	k_{12}	$(rol_{60}Q).R$
FL	kl_3	$(rol_{77}K).L$
FL^{-1}	kl_4	$(rol_{77}K).R$
F (раунд 13)	k_{13}	$(rol_{94}K).L$
F (раунд 14)	k_{14}	$(rol_{94}K).R$
F (раунд 15)	k_{15}	$(rol_{94}Q).L$
F (раунд 16)	k_{16}	$(rol_{94}Q).R$
F (раунд 17)	k_{17}	$(rol_{111}K).L$
F (раунд 18)	k_{18}	$(rol_{111}K).R$
Выходное забеливание	kw_3	$(rol_{111}Q).L$
	kw_4	$(rol_{111}Q).R$

Раундовая функция F. Схема вычисления значения функции F представлена на рис. 3. Пусть $a = (a_1, a_2,\ldots, a_8) \in \mathbb{F}_2^8$ – 8-битовый блок, a_1 – старший бит; $X = (x_1, x_2,\ldots, x_8) \in (\mathbb{F}_2^8)^8$ – 8-байтовый блок, причем x_1 – старший байт. Функция F: $(\mathbb{F}_2^8)^8 \times (\mathbb{F}_2^8)^8 \to (\mathbb{F}_2^8)^8$ является композицией функции S, P и $\oplus$, а именно:

$$F\ (X, k) = P(S(X \oplus k)).$$

Функция S: $(\mathbb{F}_2^8)^8 \to (\mathbb{F}_2^8)^8$ определяется как

$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) \mapsto (s_1(x_1), s_2(x_2), s_3(x_3), s_4(x_4), s_2(x_5), s_3(x_6), s_4(x_7), s_1(x_8))$,

где

$s_1\colon \mathbb{F}_2^8 \to \mathbb{F}_2^8,\ x \mapsto h(g(f(x \oplus 0\text{xc5}))) \oplus 0\text{x6}e,$

$s_2\colon \mathbb{F}_2^8 \to \mathbb{F}_2^8,\ x \mapsto rol_1 s_1(x),$

$s_3\colon \mathbb{F}_2^8 \to \mathbb{F}_2^8,\ x \mapsto ror_1 s_1(x),$

$s_4\colon \mathbb{F}_2^8 \to \mathbb{F}_2^8,\ x \mapsto s_1(rol_1 x).$

Функции s_1, s_2, s_3 и s_4 являются подстановками на множестве байтов. Участвующие в их определении функции f, g, h: $\mathbb{F}_2^8 \to \mathbb{F}_2^8$ заданы следующим образом:

$$f((a_1, a_2,\ldots, a_8)) = (b_1, b_2,\ldots, b_8),$$

где

$b_1 = a_6 \oplus a_2,\quad b_2 = a_7 \oplus a_1,\quad b_3 = a_8 \oplus a_5 \oplus a_3,\quad b_4 = a_8 \oplus a_3,$

$b_5 = a_7 \oplus a_4,\quad b_6 = a_5 \oplus a_2,\quad b_7 = a_8 \oplus a_1,\quad b_8 = a_6 \oplus a_4;$

$$g((a_1, a_2,\ldots, a_8)) = (b_1, b_2,\ldots, b_8),$$

где

$b_1 = a_5 \oplus a_6 \oplus a_2,\quad b_2 = a_6 \oplus a_2,\quad b_3 = a_7 \oplus a_4,\quad b_4 = a_8 \oplus a_2,$

$b_5 = a_7 \oplus a_3,\quad b_6 = a_8 \oplus a_1,\quad b_7 = a_5 \oplus a_1,\quad b_8 = a_6 \oplus a_3;$

$$h((a_1, a_2,\ldots, a_8)) = (b_1, b_2,\ldots, b_8),$$

где $b_1, b_2, \ldots, b_8 \in \mathbb{F}_2$– биты, удовлетворяющие соотношению

$$b_8 \oplus b_7\beta^{238} \oplus b_6\beta^{221} \oplus b_5\beta^{204} \oplus b_4\beta \oplus b_3\beta^{239} \oplus b_2\beta^{292} \oplus b_1\beta^{205}$$
$$= (a_8 \oplus a_7\beta^{238} \oplus a_6\beta^{221} \oplus a_5\beta^{204} \oplus a_4\beta \oplus a_3\beta^{239} \oplus a_2\beta^{292} \oplus a_1\beta^{205})^{-1},$$

$\beta = 0\text{x}02$ – байт, интерпретируемый как элемент конечного поля

$$\mathbb{F}_{256} \cong \mathbb{F}_2[x] \,/\, (x^8 + x^6 + x^5 + x^3 + 1)$$

(в данном случае операции возведения в степень и нахождения обратного элемента осуществляется в указанном поле, причем $0^{-1} = 0$; приведенное соотношение однозначно разрешимо относительно $(b_1, b_2,\ldots, b_8) \in \mathbb{F}_2^8$ для любого байта $(a_1, a_2,\ldots, a_8) \in \mathbb{F}_2^8$). Подстановки s_1, s_2, s_3 и s_4 следует задать таблицами.

Функция P определяется как

$$\text{P: } (\mathbb{F}_2^8)^8 \to (\mathbb{F}_2^8)^8,\ (x_1, x_2,\ldots, x_8) \mapsto (y_1, y_2,\ldots, y_8),$$

где

$$y_1 = x_1 \oplus x_3 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_8$$
$$y_2 = x_2 \oplus x_4 \oplus x_1 \oplus x_7 \oplus x_8 \oplus x_5$$
$$y_3 = x_3 \oplus x_1 \oplus x_2 \oplus x_8 \oplus x_5 \oplus x_6$$
$$y_4 = x_4 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7$$
$$y_5 = x_1 \oplus x_2 \oplus x_6 \oplus x_7 \oplus x_8$$
$$y_6 = x_2 \oplus x_3 \oplus x_7 \oplus x_8 \oplus x_5$$
$$y_7 = x_3 \oplus x_4 \oplus x8 \oplus x_5 \oplus x_6$$
$$y_8 = x_4 \oplus x_1 \oplus x_5 \oplus x_6 \oplus x_7.$$

Функция FL. Функция FL определяется как

$$FL\text{: } \mathbb{F}_2^{64} \times \mathbb{F}_2^{64} \to \mathbb{F}_2^{64},$$
$$(X.L \parallel X.R,\ kl.L \parallel kl.R) \mapsto Y.L \parallel Y.R,$$

где

$$X.R = (rol_1(X.L \,\&\, kl.L) \oplus X.R,$$
$$Y.R = (Y.R \vee kl.R) \oplus X.R.$$

Функция FL^{-1}является обратной к FL, т.е.

$$FL^{-1}(FL\ (\text{X}, k), k) \equiv \text{X}.$$

Схема вычисления этих функций представлены на рис. 3.

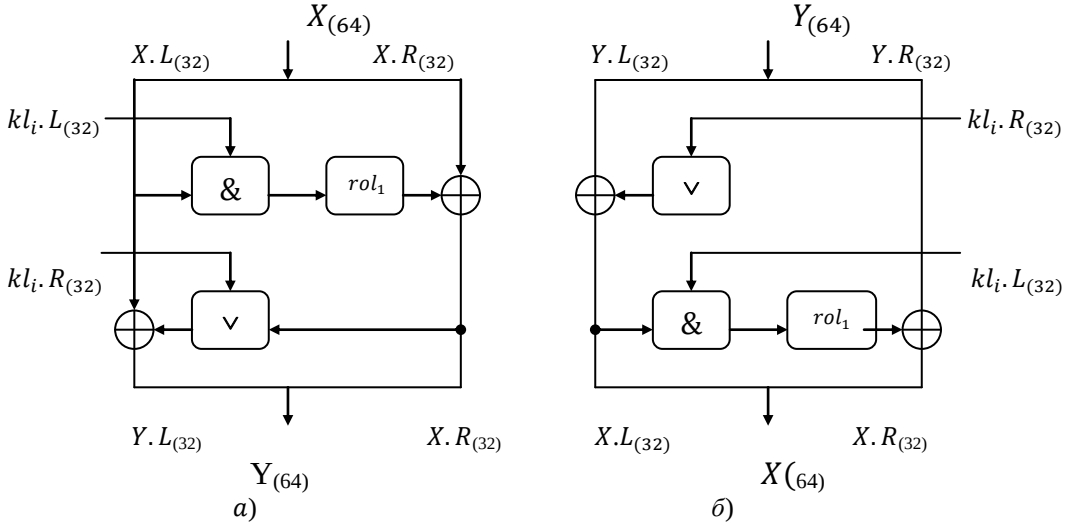

Рис.3. *Функции а)* FL *и б)* FL^{-1} *в Camellia*