Н.Н. Ташатов, Д.Т. Санкибаев

Алгоритм быстрого шифрования FEAL-32x

(Евразийский Национальный университет им. Л.Н. Гумилева, г. Астана, Казахстан)

Актуальной задачей формирования системы безопасности информации государства, нормативно-правового обеспечения защиты информации является разработка национальных стандартов на механизмы криптографической защиты информации. Использование результатов и опыта международных конкурсов позволяет ускорить процесс разработки национальных стандартов.

Алгоритм FEAL-32X использует F-функцию f(A, Y), которая отображает входную пару 2x16 бит к 32-разрядному выходу.Внутри функции f, применяются две байтовых замены данных (S-преобразования) S0 и S1 (каждое используется дважды); каждое S-преобразование преобразует пару 8-разрядных входных данных в 8-разрядные выходные (см. таблицу 1). S0 и S1 используют функцию суммирования бита d $\in \{0,1\}$ с 8-разрядными параметрами x и y по модулю 256 и левый циклический сдвиг результата на 2 бита (ROT2):

$$\mathrm{Sd}\ (x, y) = \mathrm{ROT2}\ (x + y + d \bmod 256)$$

При формировании ключа используется функция f (A, B) подобная f-функции (см. таблицу 1; Ai, Bi, Yi, ti, и Ui – все 8-разрядные переменные), преобразующая два 32-разрядных входных слова в 32-разрядный выход [1].

Таблица 1

	U←f(A, Y)	U←f_K(A, B)
t1 =	(A0⊕A1)⊕Y0	A0⊕A1
t2 =	(A2⊕A3)⊕Y1	A2⊕A3
U1 =	S1(t1, t2)	S1(t1, t2⊕B0)
U2 =	S0(t2,U1)	S0(t2, U1⊕B1)
U0=	S0(A0,U1)	S0(A0, U1⊕B2)
U3=	S1(A3, U2)	S1(A3,U2⊕B3)

Поскольку операции 2-разрядного циклического сдвига и XOR - обе линейных, то единственными нелинейными операциями в FEAL-32X являются операции суммирования по модулю 256 [2].

Алгоритм FEAL-32x выглядит следующим образом:

ВХОД: 64-разрядный открытый текст M = m1 ... m64; 128-разрядный ключ K = k1 ... k128.

ВЫХОД: 64-разрядный шифртекст C = c1 ... c64

1. (Расширение ключа). Вычислить сорок 16-разрядных подключа K_i из K, с использованием алгоритма расширения ключа (приведён ниже).

2. Определить M_L = m1 ... m32, M_R = m33 ... m64.

3. (L0, R0) ← (m_l, m_r) ⊕ ((K32, K33), (K34, K35)). (Начальное преобразование входных данных).

4. r0 ← r0 ⊕ l0.

5. For i = 0 to 31 do: Li = Ri-1, Ri = Li-1 ⊕ f(Ri-1, Ki-1).

6. L32 ← L32 ⊕ R32.

7. (R32, L32) ← (R32, L32) ⊕ ((K36, K37), (K38, K39)). (Заключительное преобразование выходных данных).

8. C ← (R32, L32). (Обратите внимание, что выходные блоки меняются местами.)

Алгоритм расширения ключа для алгоритма FEAL-32x выглядит так:

ВХОД: 128-разрядный ключ K = k1 ... k128. Ключ разделяется на 64-разрядные половины K_L и K_R. K_R разбивается ещё на 2 32-разрядные половины ($K_{R\,1}$, $K_{R\,2}$)

ВЫХОД: 640-разрядный расширенный ключ (40x16-разрядных подключей Ki, $0 \le i \le 23$).

1. (Инициализировать) $U^{(-2)} \leftarrow 0$, $U^{(-1)} \leftarrow K_{L\,1}$, $U^{(0)} \leftarrow K_{L\,2}$.

2. U = (U0, U1, U2, U3) при 8-разрядных Ui. Вычислить K0, ..., K40, при изменении i от 1 до 20

(a) определяется Qi = KR1 $\oplus$ KR2 при i $\equiv$ 1 mod 3; Qi = KR1, при i $\equiv$ 2 mod 3; и Qi = KR2, при i $\equiv$ 0 mod 3

(b) $U \leftarrow f_k(U^{(i-2)}, U^{(i-1)} \oplus U^{(i-3)} \oplus Qi)$. (fk определен в таблице 1, где в качестве A и B используют 4-байтовые векторы (A0, A1, A2, A3), (B0, B1, B2, B3).)

(c) $K_{2i-2} = (U0, U1)$, $K_{2i-1} = (U2, U3)$, $U^{(i)} \leftarrow U$.

Расшифрование осуществляется в соответствии с тем же алгоритмом на тех же самых ключах и при входной криптограмме C = (R32, L32), но при этом ключи вводятся в обратном порядке: подключи ((K36, K37), (K38, K39)) используются для начального преобразования (шаг 3), ((K32, K33), (K34, K35)) - для заключительного (шаг 7), а при пошаговом расшифровании используются подключи K31...K0 (шаг 5) [1,3].

Заключение. Тенденции развития современных схем поточного шифрования показывают, что на сегодняшний день имеют преимущество классические схемы построения данных шифров на основе регистров сдвига с нелинейной функцией, т.н. фильтр-генераторы, построенные над расширенными полями

Актуальной задачей формирования системы безопасности информации государства, нормативно-правового обеспечения защиты информации является разработка национальных стандартов на механизмы криптографической защиты информации. Использование результатов и опыта международных конкурсов позволяет ускорить процесс разработки национальных стандартов.

ЛИТЕРАТУРА

1. А.В.Гусаров, В.И.Милашенко «Программная реализация криптографических алгоритмов», Орел:Орел,2002.-С.23-28.

2. Б.Шнаер „Прикладная криптография“, Триумф, 2(2002),С.132-136.

3. Henk C.A. van Tilborg «Encyclopedia of Cryptography and Security» Springer, (2005),С.134-136.

Ташатов Н. Н., Санкибаев Д.Т.
Алгоритм быстрого шифрования FEAL-32x

Нормативтік - құқықтық қамтамсыз ету, ұлттық механизмдерге стандарттарды дайындау, криптографиялық ақпараттық орғау, мемлекеттік ақпараттық қауіпсіздігінін жүйесін құрастырудың маңызды мақсаты болып табылады. Халықаралық конкурстардың нәтижелерін және тәжірибелерін қолдану ұлттық стандарттарды дайындауды жеделдетеді.

Tashatov N. N., Sankibaev D. T.
Algorithm for fast encryption FEAL-32x

Urgent task of forming the security of the State of information, regulatory information security is to develop national standards for cryptographic protection mechanisms. Using the results and experience of international competition to accelerate the process of developing national standards.

Поступила в редакцию 12.05.11

Рекомендована к печати 30.05.11