О некоторых вероятностных характеристиках алгоритма выработки ключа «CryptoPro Key Meshing»

Владимир Миронкин

Назначение

- Предназначен для преобразования 256-битового ключа k и 64-битового инициализирующего вектора IV после шифрования очередных 1024 байт (8192 битов, или 256 64-битовых блоков) информации.

- Зашифрование и расшифрование осуществляется на основе шифрующего преобразования алгоритма ГОСТ 28147-89 в режиме ECB.

Обозначения

- $k[0] = k$ - начальное значение ключа;
- $IV_0[0] = IV$ - начальное значение инициализирующего вектора;
- В процессе шифрования i-го блока открытой информации размера 1024 байт значение инициализирующего вектора $IV_0[i]$ некоторым образом преобразуется в значение $IV_n[i]$, $i = 0,1,2,...$

Замечание. *RFC4357 не определяет способ модификации вектора* $IV_n[i]$, $i = 0,1,2,...$ *в процессе шифрования на соответствующем ключе* $k[i]$, $i = 0,1,2,....$ *Будем считать, что* $IV_n[i]$ *вырабатывается на основе некоторого случайного отображения* $\varphi : V_{64} \to V_{64}$ *такого, что* $\varphi(IV_0[i]) = IV_n[i]$.

Т.о. $IV_0[i]$ *и* $IV_n[i]$, $i = 0,1,2,...$ *можно рассматривать как независимые случайные величины, равномерно распределенные на* V_{64}.

Алгоритм

1. $i = 0$;
2. Шифрование 1024 байт информации при $k[i]$ и $IV_0[i]$;
3. $k[i+1] = decryptECB(k[i], C)$;
4. $IV_0[i+1] = encryptECB(k[i+1], IV_n[i])$;
5. $i = i+1$, *переход на шаг 2 алгоритма*.

256-битовая константа C – параметр алгоритма

$$C = \{0x69, 0x00, 0x72, 0x22, \quad 0x64, 0xC9, 0x04, 0x23,$$
$$0x8D, 0x3A, 0xDB, 0x96, \quad 0x46, 0xE9, 0x2A, 0xC4,$$
$$0x18, 0xFE, 0xAC, 0x94, \quad 0x00, 0xED, 0x07, 0x12,$$
$$0xC0, 0x86, 0xDC, 0xC2, \quad 0xEF, 0x4C, 0xA9, 0x2B\},$$

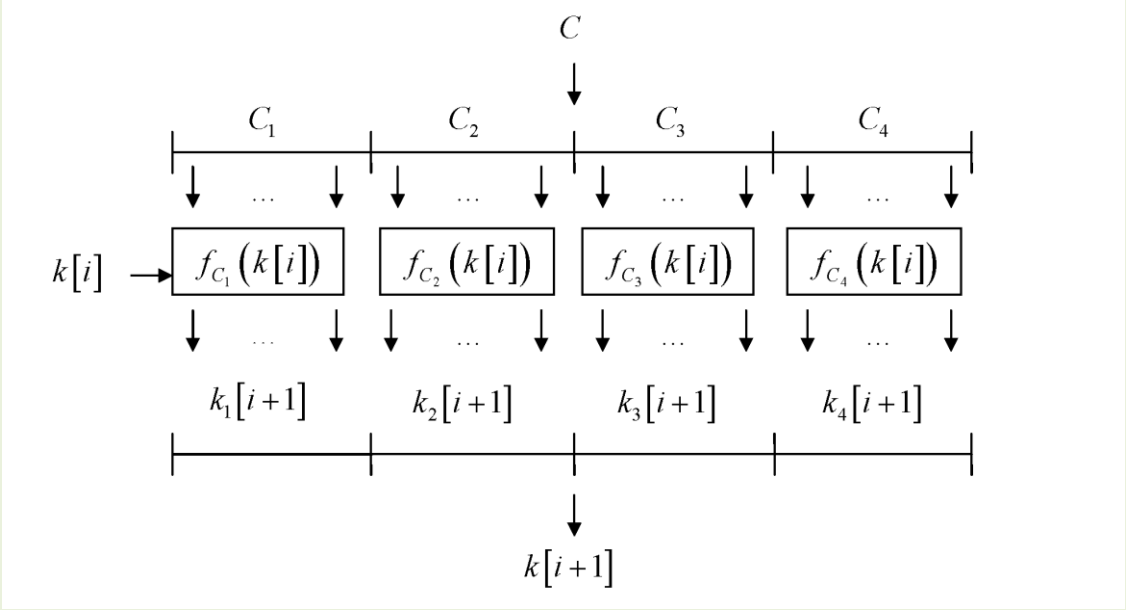
Функциональная схема

Константа $C = (C_1, C_2, C_3, C_4) \in V_{256}$, задает функцию преобразования ключей f_C:

$$f_C = (f_{C_1}, f_{C_2}, f_{C_3}, f_{C_4}) : V_{256} \to V_{256},$$

где $f_{C_i}(x) \equiv decryptECB(x, C_i) : V_{256} \to V_{64}$, $i = 1,2,3,4$.

$$\forall x \in V_{256} \quad f_C(x) = f_{C_1}(x) \| f_{C_2}(x) \| f_{C_3}(x) \| f_{C_4}(x).$$



Важное наблюдение

В заданной константе C подблоки $C_i \in V_{64}$, $\forall i = \overline{1,4}$, различны. В силу того, что каждое из отображений $f_{C_1}, f_{C_2}, f_{C_3}, f_{C_4}$ является функцией расшифрования, то для каждого значения ключа отображение f_C обладает свойством подстановочности следующего вида:

$$\forall x \in V_{256} \quad f_{C_k}(x) \neq f_{C_l}(x),\ k \neq l \in \overline{1,4}. \qquad (1)$$

Вероятностная модель

Пусть $\{f_i\} \mid f_i : V_{64} \to V_{64}, i = \overline{1,4}$, - совокупность отображений, имеющих равномерное распределение и обладающих указанным свойством:

$$\forall x \in V_{64} \;\; f_k(x) \neq f_l(x),\; k \neq l \in \overline{1,4}.$$

Совокупности этих отображений сопоставим отображение f:

$$f = (f_1, f_2, f_3, f_4).$$

Так как исходный ключ $k[0] \in V_{256}$ считается равномерно распределенным на V_{256}, то с учетом (1), начиная с первого выработанного ключа на основе отображения f, элементы ключевой последовательности $k[1], k[2], \ldots$ принадлежат уже множеству $B \subset V_{256}$, которое определяется следующим образом:

$$B = \left\{ (x_1, x_2, x_3, x_4) \mid x_i \neq x_j \in V_{64}, i \neq j \in \overline{1,4} \right\}.$$

Вероятностная модель

Важно: *После первого шага алгоритма выработки ключей «CryptoPro Key Meshing», не ограничивая общности, можно считать, что дальнейшее преобразование ключевого множества осуществляется на основе произвольного случайного отображения:*

$$f : B \to B,$$

где $|B| = 2^{64}\left(2^{64}-1\right)\left(2^{64}-2\right)\left(2^{64}-3\right) = 1{,}157 \cdot 10^{77}$.

В силу равномерности распределения отображений f_i, $i = \overline{1,4}$, на множестве всех отображений $V_{64} \to V_{64}$, отображение f также имеет равномерное распределение на множестве всех отображений $B \to B$.

Мощность множества ключей

$K_0, K_1, K_2, \ldots$ – последовательность ключевых множеств. Эта последовательность представляется в следующем виде:

$$K_0 = K,$$
$$K_1 = B,$$
$$K_2 = f(B),$$
$$K_3 = f^2(B),$$
$$\ldots$$

Обозначим $|B| = N$. Здесь и далее для любых $i_0, i_1 \in \mathbb{N}$, $i_0 > i_1$ положим $\prod_{j=i_0}^{i_1}(\ldots) \equiv 1$.

Предложение (Миронкин, 2014). *При условии, что $f : B \to B$ – случайное равновероятное отображение, для любого $r = 2,3,\ldots$ справедливо равенство:*

$$\mathbf{E}|K_r| = \sum_{t=1}^{N}\prod_{l=1}^{t-1}\left(1-\frac{l}{N}\right) + \sum_{t=1}^{N-r+1}\sum_{m=1}^{N-(k+t)}\prod_{l=1}^{r+t+m-2}\left(1-\frac{l}{N}\right).$$

Граф преобразования

κ_B – число циклических точек графа отображения $f : B \to B$:

$$\kappa_B = \left| \left\{ x \in B \mid x = f\left(x\right)^t, t \geq 1 \right\} \right|.$$

При условии, что f *– равновероятное случайное отображение* $B \to B$, *справедлива асимптотика при* $N \to \infty$*:*

$$E\kappa_B \sim \sqrt{\frac{\pi N}{2}}.$$

Для произвольного отображения $f : X \to X$ *назовем величину* $\mu_f^{(r)} = \frac{\left|X\right|}{\left|f^r\left(X\right)\right|}$ *коэффициентом сжатия при* r*-кратной итерации отображения* f.

Граф преобразования

Следствие. *Предельная оценка для среднего значения коэффициента сжатия* $\mu_f^{(r)}$ *для обобщенной модели выработки ключей алгоритма «CryptoPro Key Meshing» при* $r \to \infty$ *по порядку равна* $\frac{2^{256}}{\sqrt{|B|}}\sqrt{\frac{2}{\pi}}$. *Для эталонной модели предельная оценка коэффициента сжатия* $\mu_F^{(r)}$ *при* $r \to \infty$ *равна* $2^{128}\sqrt{\frac{2}{\pi}}$.

Граф преобразования

Предложение (Флажоле и Одлыжко, 1989). *При условии, что f является случайным равновероятным отображением $B \to B$, справедлива асимптотика при $N \to \infty$:*

$$\mathbf{E}\left|K_i\right| \sim \left(1-e^{\tau_{i-1}}\right)\left|B\right| \qquad (2)$$

где $\tau_0 = 0,\ \tau_{i+1} = e^{-1+\tau_i},\ i = 1,2,\ldots$

Отношение $\alpha_i,\ i = 1,2,\ldots$ средних мощностей множеств вырабатываемых ключей для эталонного случая и «CriptoPro Key Meshing»:

$$\alpha_i = \frac{\left|f^i\left(K\right)\right|}{\left|K_i\right|} = \frac{\left(1-e^{\tau_i}\right)\left|K\right|}{\left(1-e^{\tau_{i-1}}\right)\left|B\right|} = \frac{\left(1-e^{-1+\tau_{i-1}}\right)\left|K\right|}{\left(1-e^{\tau_{i-1}}\right)\left|B\right|} > 1.$$

Отличимость

Рассмотрим последовательность вырабатываемых ключей $k[1], k[2], k[3], \ldots$

Каждый элемент последовательности имеет вид:

$$k[i] = \left\{ \left(k_1[i], k_2[i], k_3[i], k_4[i] \right) \mid k_i[i] \neq k_j[i] \in V_{64}, i \neq j \in \overline{1,4} \right\}.$$

Определим необходимый объем вырабатываемого материала T, на котором можно отличить рассматриваемую ключевую последовательность от последовательности, формируемой на основе случайного равновероятного отображения $F : V_{256} \to V_{256}$.

Каждый элемент $x_i \in V_{256}$ случайной последовательности $\{x_i\}$, $i = 1, 2, \ldots$ представим в следующем виде:

$$x_i = \left(x_i^1, x_i^2, x_i^3, x_i^4 \right),\ x_i^j \in V_{64},\ j = \overline{1,4}.$$

Отличимость

ξ – случайная величина, равная номеру первого элемента рассматриваемой последовательности $\{x_i\}$, $i = 1, 2, \ldots$, в котором существуют совпавшие подблоки длины 64 бита рассмотренного вида.

Обозначим через W множество элементов случайной последовательности $\{x_i\}$, $i = 1, 2, \ldots$, в которых есть совпавшие блоки:

$$W = \left\{ (x_1, x_2, x_3, x_4) \mid \exists i \neq j \overline{\in 1,4} : x_i = x_j \right\},$$

его мощность:

$$|W| = C_4^2 2^{64} \left(2^{64} - 1\right)\left(2^{64} - 2\right) + C_4^2 2^{64} \left(2^{64} - 1\right) + C_4^3 2^{64} \left(2^{64} - 1\right) + 2^{64} \approx 3,76 \cdot 10^{58}.$$

Отличимость

Предложение. *При условии, что* $f : B \to B$ *– случайное равновероятное отображение, объема материала для выявления неравновероятности вырабатываемой последовательности ключей составляет* T *с вероятностью* $p = 3,24 \cdot 10^{-19} \cdot \prod_{i=0}^{T-2} \left(1 - \frac{|W| + i}{2^{256}} \right)$, *где* $T \in \overline{1, |V_{256} \setminus W| + 1}$.

Следствие. *В условиях предложения среднее значение требуемого материала, необходимого для выявления неравновероятности вырабатываемой последовательности ключей, составляет*

$$\mathbf{E}\xi = \frac{|W|}{2^{256}} \sum_{k=1}^{|V_{256} \setminus W| + 1} k \prod_{i=0}^{k-2} \left(1 - \frac{|W| + i}{2^{256}} \right).$$

Длина отрезка апериодичности последовательности ключей

G – граф отображения f в обобщенной схеме алгоритма «CryptoPro Key Meshing».

$\tau_B(x)$ - отрезок апериодичности отображения f для случайной вершины $x \in B$ – число ребер графа G, пройденных из вершины x до первого попадания в уже встречавшуюся вершину графа G:

$$\tau_B(x) = \min_{t \in \mathbb{N}} \left(t \mid f^t(x) \in \left\{ x, f(x), \ldots, f^{t-1}(x) \right\} \right).$$

Пусть $|B| = N$.

Длина отрезка апериодичности последовательности ключей

Предложение. (Колчин, 1984). *При условии, что f является случайным равновероятным отображением $B \to B$, справедливо*

$$\mathbf{P}\{\tau_B > x\sqrt{2N}\} \underset{N\to\infty}{\to} e^{-x^2} \text{ и } \mathbf{E}\,\tau_B \approx \sqrt{\frac{\pi N}{2}}.$$

Следствие. *Сокращение среднего объема материала, необходимого для отличения генерируемой последовательности от случайной равновероятной с использованием длины отрезка апериодичности для обобщенной схемы алгоритма «CryptoPro Key Meshing» относительно эталонной, составляет* $\frac{2^{128}}{\sqrt{|B|}}$.

Совпадение отрезков последовательностей ключей

Предложение. *При условии, что* f *– случайное равновероятное отображение* $B \to B$, *произвольные вершины* $x_0 \neq y_0 \in S$ *образуют коллизию при отображении* f^k *с вероятностью*

$$\mathbf{P}\left\{ f^k(x_0) = f^k(y_0); x_0 \neq y_0 \right\} = \frac{2(c_2 - c_1 + 1)}{N^2} \sum_{l=1}^{N-1} \sum_{t_1=1}^{\min(k, N-l)} \prod_{i=2}^{t_1+l-1} \left(1 - \frac{i}{N}\right) +$$

$$+ \frac{1}{N^2} \sum_{l=1}^{N-2} \sum_{t_1=1}^{\min(k, N-l)} \sum_{p_1=\max(0,c_3)}^{c_4} \sum_{\gamma=0}^{l-1} \sum_{p_2=\max(0,c_5)}^{c_6} \prod_{i=2}^{2t_1 - l(p_2 - p_1 - 1) - \gamma - 1} \left(1 - \frac{i}{N}\right),$$

где $c_1 = c_1(l, t_1, \alpha) = \left\lceil \frac{k - \alpha - t_1 + 1}{l} \right\rceil$, $c_2 = c_2(l, \alpha) = \left\lceil \frac{k - \alpha - 1}{l} \right\rceil$,

$c_3 = c_3(l, t_1) = \left\lceil \frac{k - t_1 - l + 1}{l} \right\rceil$, $c_4 = c_4(l, t_1) = \left\lceil \frac{k - t_1}{l} \right\rceil$,

$c_5 = c_5(l, t_1, p_1, \gamma) = \left\lceil \frac{2t_1 + l(p_1 + 1) - \gamma - N}{l} \right\rceil$, $c_6 = c_6(l, t_1, p_1, \gamma) = \left\lceil \frac{t_1 + lp_1 - \gamma - 1}{l} \right\rceil$.

Выводы

Рассмотренные вероятностные характеристики «CryptoPro Key Meshing» существенно отличаются от характеристик для эталонной модели.

Отличие:

– пропорционально отношению мощностей множеств формируемых ключей на каждом из шагов алгоритма выработки ключей (характеристика сжимаемости ключевого множества),

– пропорционально корню этого отношения (оценка на средний материал для выявления неравновероятности).

Существенный недостаток:

множество вырабатываемых ключей структурировано.