11. *Shuying S. and Jun H.* Impossible differential cryptanalysis of GRANULE algorithm // Computer Engineering. 2019. V. 45(10). P. 134–138.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/15/13

КРИТЕРИЙ МИНИМАЛЬНОСТИ ПО ВКЛЮЧЕНИЮ СОВЕРШЕННЫХ ШИФРОВ

Н. В. Медведева, С. С. Титов

Исследуются совершенные по Шеннону (абсолютно стойкие к атаке по шифртексту) шифры. Сформулирован и доказан критерий минимальности множества ключей совершенного шифра.

Ключевые слова: *совершенные шифры, эндоморфные шифры, неэндоморфные шифры.*

В рамках вероятностной модели шифра Σ_B [1] рассмотрим произвольный совершенный по Шеннону шифр. Пусть X, Y — конечные множества соответственно шифрвеличин и шифробозначений, с которыми оперирует некоторый шифр замены, K — множество ключей, $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\lambda > 1$, $\mu \geqslant \lambda$, $\pi \geqslant \mu$. Это означает, что открытые и шифрованные тексты представляются словами (ℓ-граммами, $\ell \geqslant 1$) в алфавитах X и Y соответственно. Согласно [2, 3], под шифром Σ_B будем понимать совокупность множеств правил зашифрования и правил расшифрования с заданными распределениями вероятностей на множествах открытых текстов и ключей. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются совершенными.

Описание эндоморфных ($\lambda = \mu$) с минимально возможным числом ключей ($|K| = |Y|$) совершенных шифров даётся теоремой Шеннона, таблица зашифрования таких шифров — это латинский квадрат из равновероятных подстановок зашифрования [1]. При описании неэндоморфных ($\lambda < \mu$) совершенных шифров, как показано в [4], возникает естественная задача описания минимальных по включению (т. е. содержащих минимально возможное множество ключей зашифрования с ненулевыми вероятностями) совершенных шифров, не сводящихся к латинским прямоугольникам размера $\mu \times \lambda$, которые можно рассматривать как непосредственное обобщение теоремы Шеннона.

На первом этапе реализации данного подхода в работах [4, 5] получены достаточные условия того, что в таблице зашифрования как неэндоморфных, так и эндоморфных совершенных шифров с равновероятными ключами отсутствуют латинские соответственно прямоугольники и квадраты. В [5] на основе графового подхода к исследованию и описанию совершенных шифров, их аналогов и обобщений сформулировано достаточное условие минимальности шифра по включению.

Пусть дана таблица зашифрования совершенного шифра Σ_B с λ столбцами, π строками и μ шифробозначениями y_j, $j = 1, 2, \ldots, \mu$, где $\pi \geqslant \mu \geqslant \lambda > 1$. Обозначим через $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_\pi)^{\mathrm{T}}$ вектор-столбец вероятностей P_k ключей k ($k = 1, 2, \ldots, \pi$), через p_j — априорные вероятности шифробозначений y_j ($j = 1, 2, \ldots, \mu$) данного шифра. Для исходной таблицы зашифрования построим соответствующую ей $(0, 1)$-матрицу A с π строками и $\lambda\mu$ столбцами следующим образом:

1) каждому столбцу x_i таблицы зашифрования поставим в соответствие μ столбцов и занумеруем все получившиеся $\lambda\mu$ столбцы индексами (i, j), где $i = 1, 2, \ldots, \lambda$, $j = 1, 2, \ldots, \mu$;

2) на пересечении строки k ($k = 1, 2, \ldots, \pi$) и столбца (i, j) поставим единицу тогда и только тогда, когда $e_k(x_i) = y_j$, т. е. если шифрвеличина x_i на ключе k зашифровывается в шифробозначение y_j. В противном случае ставим нуль.

Соответствие таблицы зашифрования и матрицы A, можно считать, получено посредством замены каждого i-го столбца в таблице зашифрования на μ столбцов матрицы A, индексированных парами (i, j), где $i = 1, 2, \ldots, \lambda$, $j = 1, 2, \ldots, \mu$. Столбцы матрицы A можно упорядочить и занумеровать, например, естественным образом, присвоив индексу (i, j) номер $m = (i-1)\mu + j$, так что $\lambda\mu \geqslant m \geqslant 1$.

Используя $(0, 1)$-матрицу A, для которой $A_{k,(i,j)} = 1 \Leftrightarrow e_k(x_i) = y_j$, условие совершенности шифра можно записать в виде системы линейных уравнений

$$\sum_{k=1}^{\pi} \mathsf{P}_k \, A_{k,(i,j)} = p_j \quad (i = 1, 2, \ldots, \lambda, \ j = 1, 2, \ldots, \mu) \tag{1}$$

с дополнительным условием

$$\sum_{k=1}^{\pi} \mathsf{P}_k = 1. \tag{2}$$

К матрице A добавим столбец из π единиц. При предлагаемом способе упорядочивания столбцов этому столбцу естественно присвоить номер $m = 0$ и считать его добавленным к матрице A слева. В вектор правых частей добавим 1 (в соответствии с уравнением (2)). Получившуюся матрицу размером π строк на $1 + \lambda\mu$ столбцов обозначим через $\tilde{A}$, а вектор правых частей — через $\tilde{p} = (1, p_1, \ldots, p_\mu, \ldots, p_1, \ldots, p_\mu)^{\mathrm{T}}$, при этом $\operatorname{rank} \tilde{A} \leqslant \pi$.

Теорема 1. Множество ключей шифра минимально тогда и только тогда, когда ранг матрицы $\tilde{A}$ максимальный (равный π).

Доказательство. Рассматривая вероятности P_k ключей как неизвестные ненулевые искомые величины уравнений (1), а вероятности p_j — как их правые части, по теореме Кронекера — Капелли заключаем, что, поскольку система имеет решение, ранг матрицы $\tilde{A}$ равен рангу расширенной (посредством вектора $\tilde{p} = (1, p_1, \ldots, p_\mu, \ldots, p_1, \ldots, p_\mu)^{\mathrm{T}}$) матрицы. Максимально возможный ранг матрицы $\tilde{A}$ равен количеству её строк — π.

Предположим, что данный шифр не является минимальным по включению. Докажем, что тогда ранг матрицы $\tilde{A}$ меньше π. Действительно, пусть существует шифр с вероятностями ключей P'_k с теми же правыми частями p_j, в котором отсутствуют некоторые ключи из данного набора. Этот факт можно отразить в системе уравнений (1), (2), положив вероятности отсутствующих ключей равными нулю. Так, пусть без ограничения общности ключ $k = \pi$ отсутствует, тогда система уравнений (1), (2) имеет решение, в котором $\mathsf{P}'_\pi = 0$. Заметим, что неизвестные $\mathsf{P}''_k = \mathsf{P}_k - \mathsf{P}'_k$ ($k = 1, \ldots, \pi$) не все равны нулю (например, $\mathsf{P}''_\pi \neq 0$) и удовлетворяют однородной системе уравнений, откуда следует, что в матрице $\tilde{A}$ не может быть невырожденной квадратной подматрицы максимального размера π на π, т. е. её ранг строго меньше π.

Обратно, пусть ранг матрицы $\tilde{A}$ строго меньше π. Докажем, что данный шифр не является минимальным по включению. Действительно, в этом случае одна из строк матрицы $\tilde{A}$ (без ограничения общности пусть это π-я строка) есть линейная комбинация остальных. Пусть

$$A_{\pi,(i,j)} = \sum_{k=1}^{\pi-1} q_k A_{k,(i,j)}, \quad q_k \in \mathbb{R} \ (i = 1, 2, \ldots, \lambda, \ j = 1, 2, \ldots, \mu).$$

Для каждого $t \in [0,1]$ введём новые неизвестные $\mathsf{P}'_k = \mathsf{P}_k + q_k t\,\mathsf{P}_\pi$ $(k = 1, \ldots, \pi-1)$, $\mathsf{P}'_\pi = (1-t)\,\mathsf{P}_\pi$, где $q_1 + q_2 + \ldots + q_{\pi-1} = 1$ из-за столбца единиц в матрице $\tilde{A}$. В силу тождества

$$\begin{aligned}\sum_{k=1}^{\pi} \mathsf{P}_k\, A_{k,(i,j)} &= \sum_{k=1}^{\pi-1} \mathsf{P}_k\, A_{k,(i,j)} + \mathsf{P}_\pi\, A_{\pi,(i,j)} = \sum_{k=1}^{\pi-1} \mathsf{P}_k\, A_{k,(i,j)} + [t\,\mathsf{P}_\pi + (1-t)\,\mathsf{P}_\pi] A_{\pi,(i,j)} = \\ &= \left(\sum_{k=1}^{\pi-1} \mathsf{P}_k\, A_{k,(i,j)} + t\,\mathsf{P}_\pi \sum_{k=1}^{\pi-1} q_k A_{k,(i,j)}\right) + (1-t)\,\mathsf{P}_\pi\, A_{\pi,(i,j)} = \\ &= \sum_{k=1}^{\pi-1} (\mathsf{P}_k + t q_k\,\mathsf{P}_\pi) A_{k,(i,j)} + (1-t)\,\mathsf{P}_\pi\, A_{\pi,(i,j)} = \sum_{k=1}^{\pi} \mathsf{P}'_k\, A_{k,(i,j)}\end{aligned}$$

эти новые неизвестные P'_k удовлетворяют той же системе уравнений. Поскольку $\mathsf{P}'_k = \mathsf{P}_k > 0$ при $t = 0$ и линейная функция непрерывна, имеем $\mathsf{P}'_k > 0$ при всех достаточно малых $t > 0$. Ввиду того, что $\tilde{A}$ является $(0,1)$-матрицей и все координаты вектора $\tilde{p}$ положительны, среди чисел q_k должны быть и положительные; для таких ключей k имеем $\mathsf{P}'_k > 0$ для всех $t > 0$. Если для всех $k = 1, \ldots, \pi-1$ имеем $\mathsf{P}'_k > 0$ при всех $t \in [0,1]$, то при $t = 1$ получаем $\mathsf{P}'_\pi = 0$, $\mathsf{P}'_k > 0$ $(k = 1, \ldots, \pi-1)$, причём

$$\sum_{k=1}^{\pi-1} \mathsf{P}'_k = \sum_{k=1}^{\pi-1} \mathsf{P}_k = 1$$

для любого t ввиду равенства

$$\sum_{k=1}^{\pi-1} q_k = 1.$$

Следовательно, величины P'_k $(k = 1, \ldots, \pi-1)$ могут рассматриваться как вероятности ключей собственного подмножества ключей данного шифра, так как $\mathsf{P}'_\pi = 0$. Если же $\mathsf{P}'_k = 0$ при некотором $k = k_0$ и $t = t_0$, $0 < t_0 < 1$, то, выбрав t_0 наименьшим по всем таким k, получим тоже собственное подмножество ключей с ненулевыми вероятностями P'_k, что доказывает неминимальность данного шифра по включению. ■

Отметим, что для эндоморфного шифра равенство $q_1 + \ldots + q_{\pi-1} = 1$ выполняется уже при рассмотрении матрицы A без использования столбца из единиц.

Замечание 1. Из критерия минимальности по включению совершенных шифров следуют необходимые условия:

1) для минимальности по включению множества ключей шифра необходимо выполнение неравенства $\pi \leqslant \lambda\mu$;
2) для эндоморфного минимального по включению совершенного шифра выполняется неравенство $\pi \leqslant \lambda(\lambda - 1)$.

Полученные теоретические результаты могут быть положены в основу классификации минимальных совершенных шифров и исследований почти совершенных шифров [6, 7].

Таким образом, сформулирован и доказан критерий минимальности множества ключей совершенных шифров: множество ключей минимально, если и только если ранг бинарной матрицы, состоящей из π столбцов и $1 + \lambda\mu$ столбцов, максимален и равен количеству ключей, содержащихся в таблице зашифрования. Получены также необходимые условия минимальности по включению совершенных шифров.

ЛИТЕРАТУРА

1. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
4. *Медведева Н. В., Титов С. С.* Конструкции неэндоморфных совершенных шифров // Прикладная дискретная математика. Приложение. 2020. № 13. С. 51–54.
5. *Медведева Н. В., Титов С. С.* К задаче описания минимальных по включению совершенных шифров // Прикладная дискретная математика. Приложение. 2021. № 14. С. 91–95.
6. *Зубов А. Ю.* Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4(14). С. 28–33.
7. *Зубов А. Ю.* О понятии ε-совершенного шифра // Прикладная дискретная математика. 2016. № 3(33). С. 45–52.

УДК 519.7 DOI 10.17223/2226308X/15/14

ВЫЧИСЛЕНИЕ РАЗНОСТНЫХ ХАРАКТЕРИСТИК ДЛЯ СЛОЖЕНИЯ k ЧИСЕЛ ПО МОДУЛЮ 2^n [1]

А. С. Мокроусов

Рассматривается разностная характеристика $\mathrm{xdp}^+_{\mathrm{k}}(\alpha^1, \ldots, \alpha^k \to \alpha^0)$, где $\alpha^0, \alpha^1, \ldots, \alpha^k \in \mathbb{Z}_2^n$, которая определяет вероятность преобразования разностей $\alpha^1, \ldots, \alpha^k$ в разность α^0 (относительно побитового «исключающего или») функцией $f(x_1, \ldots, x_k) = x_1 + \ldots + x_k \mod 2^n$. Данная величина используется при разностном криптоанализе криптографических примитивов, содержащих «исключающее или» и сложение по модулю 2^n, например ARX-конструкций. Предложены аналитические выражения для матриц, используемых для вычисления $\mathrm{xdp}^+_{\mathrm{k}}$. Кроме того, рассмотрена разностная характеристика $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$, где $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$, определяющая вероятность преобразования разностей α, β в разность γ (относительно сложения по модулю 2^n) функцией $x \oplus y$, и получены все тройки разностей, вероятность которых больше $1/4$.

Ключевые слова: *ARX, исключающее или, сложение по модулю, разностный криптоанализ, разностные характеристики.*

Одним из подходов к построению криптографических примитивов является комбинирование сложения по модулю 2^n ($\boxplus$), побитовых операций (например, «исключающего или» — $\oplus$), битовых сдвигов ($\ll$), циклических сдвигов ($\lll$). Это позволяет получить очень быстрые в программной реализации алгоритмы. Особый интерес представляют ARX-конструкции, использующие только операции $\boxplus$, $\oplus$ и $\lll$. Примерами таких шифров являются FEAL [1], TEA [2], Salsa20 [3], Speck [4].

Хорошие шифры должны быть стойкими к различным видам криптоанализа, в частности к разностному криптоанализу [5]. Это один из основных статистических методов, основанный на исследовании того, в какие разности шифртекстов могут переходить разности открытых текстов. Важным шагом при реализации метода является вычисление разностных характеристик и их максимальных значений. Для базовых операций архитектуры ARX данные характеристики определяются следующим образом [6]:

[1] Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF-2022-0018).