допустимого набора $[\mathtt{avls}](i,\ldots,j)$, соответствующего $[\mathtt{avl},\mathtt{avp}](i,\ldots,j)$ из сохранённого набора, то набор $[\mathtt{avl},\mathtt{avp}](i,\ldots,j)$ помечается как недопустимый и вычисления возвращаются ко второму этапу для уточнения минимума.

Метод 2. Во втором методе оценивается снизу число активных S-блоков на четырёх тактах. Использованы свойства преобразований $L3$, $S3$, P, заложенные при проектировании Bash-f [3]. Особую важность имеет следующий факт: если на выходе $L3$ получена вертикальная плоскость с малым числом активных линий, то на вход была подана плоскость с большим числом активных линий. Базовые свойства преобразований выступают в роли аксиом, из которых аналитически выводятся теоремы — новые свойства, имеющие отношение к оцениванию.

Затем просматриваются допустимые конфигурации, представляющие собой пары «число активных вертикальных линий на входах $L3$ на втором такте, проекция $[\mathtt{avp}](2)$». Для каждой конфигурации оценивается снизу проекция $[\mathtt{avl}](1)$ (как будто бы от второго такта мы возвращаемся к первому) и проекции $[\mathtt{avl}](3,4)$. В итоге получена оценка

$$s_A(4) = \min\left([\mathtt{avl}](1) + [\mathtt{avl}](2) + [\mathtt{avl}](3) + [\mathtt{avl}](4)\right) \geqslant 31,$$

откуда $s_A(24) \geqslant 6s_A(4) \geqslant 186$.

ЛИТЕРАТУРА

1. *Daemen J. and Van Assche G.* Differential propagation analysis of Keccak // FSE'2012. LNCS. 2012. V. 7549. P. 422–441.
2. *Mella S., Daemen J., and Van Assche G.* New techniques for trail bounds and application to differential trails in Keccak // IACR Trans. Symmetric Cryptology. 2017. No. 1. P. 329–357.
3. *Agievich S., Marchuk V., Maslau A., and Semenov V.* Bash-f: another LRX sponge function // Математические вопросы криптографии. 2017. Т. 8. № 2. С. 7–28.

УДК 519.7 DOI 10.17223/2226308X/12/28

КРИПТОАНАЛИЗ ШИФРСИСТЕМЫ ACBF[1]

И. В. Боровкова, И. А. Панкратова

Рассматривается асимметричная шифрсистема на булевых функциях с функциональным ключом. Предлагаются атаки с известным открытым текстом для двух подмножеств ключевых параметров.

Ключевые слова: *криптосистема ACBF, векторные булевы функции, асимметричная криптосистема, криптоанализ.*

Рассматривается шифрсистема ACBF (Asymmetric Cryptosystem on Boolean Functions) [1]. Она строится на основе двух операций — перестановки и отрицания, — применяемых к переменным и координатам обратимой векторной булевой функции. Открытый ключ $f(x)$ получается по формуле $f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$, где $g\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — биективная векторная булева функция; функции g и g^{-1} известны; $\sigma_1, \sigma_2 \in \mathbb{F}_2^n$ — операции отрицания; $\pi_1, \pi_2 \in \mathbb{S}_n$ — операции перестановки. Закрытый ключ — функция f^{-1}.

Ключевыми параметрами криптосистемы являются элементы любого непустого подмножества $J \subseteq \{\pi_1, \pi_2, \sigma_1, \sigma_2\}$; операции из $\{\pi_1, \pi_2, \sigma_1, \sigma_2\}\setminus J$ считаются тождественными. Таким образом, существует 15 различных подмножеств ключевых параметров.

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.

Целью работы является нахождение ключевых параметров по известным парам открытых текстов и соответствующих шифртекстов. Рассмотрены два базовых случая: $J = \{\pi_1\}$ и $J = \{\pi_1, \pi_2\}$. Для каждого из них разработана атака.

1. Случай $J = \{\pi_1\}$

Пусть $x, y \in \mathbb{F}_2^n$ — пара «открытый текст — соответствующий шифртекст». По определению криптосистемы ACBF получаем

$$y = f(x) = g(\pi_1(x)); \quad \pi_1(x) = g^{-1}(y).$$

Утверждение 1. Пусть P — матрица размера $m \times n$ со строками открытых текстов $P_1, \ldots, P_m$ в $\mathbb{F}_2^n$, с множеством Q векторов-столбцов в $\mathbb{F}_2^m$, разбитым на классы $Q_1, \ldots, Q_k$ одинаковых, $1 \leqslant k \leqslant n$, так, что $|Q_j| = r_j$, $j = 1, \ldots, k$, $r_1 + \ldots + r_k = n$. Пусть также $C_i = g(\pi_1(P_i))$ для некоторой перестановки $\pi_1 \in \mathbb{S}_n$, $i = 1, \ldots, m$. Тогда количество различных перестановок $\pi \in \mathbb{S}_n$, для которых $C_i = g(\pi(P_i))$, $i = 1, \ldots, m$, равно

$$I = \prod_{i=1}^{k} r_i!$$

Таким образом, перестановка π_1 определяется однозначно, если и только если все столбцы в матрице P различны. Экспериментально установлено, что для этого в среднем понадобится $2 \log_2 n$ открытых текстов при их случайном равновероятном выборе.

Следствие 1. Если производится атака с выбираемым открытым текстом, то можно подобрать такие P_i, что при рассмотрении $m = \lceil \log_2 n \rceil$ пар (P_i, C_i) искомая перестановка π_1 найдётся однозначно.

Пусть имеется m пар (P_i, C_i). Рассмотрим матрицу P' со строками $g^{-1}(C_i) = \pi_1(P_i)$, $i = 1, \ldots, m$; заметим, что P' содержит те же вектор-столбцы, что и матрица P, только в другом порядке — определяемом перестановкой π_1. Алгоритм 1 находит все возможные ключи шифрсистемы ACBF.

Алгоритм 1. Нахождение всех возможных ключей в случае $J = \{\pi_1\}$

Вход: (P_i, C_i), $i = 1, \ldots, m$.
Выход: все $\pi_1 \in \mathbb{S}_n$, такие, что $C_i = g(\pi_1(P_i))$, $i = 1, \ldots, m$.

1: Построим матрицы $P = \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_m \end{pmatrix}$, $P' = \begin{pmatrix} g^{-1}(C_1) \\ g^{-1}(C_2) \\ \vdots \\ g^{-1}(C_m) \end{pmatrix}$.

2: Для каждого столбца s матрицы P запоминаем номера столбцов $k_{i_1}, \ldots, k_{i_l}$, равных s. Для матрицы P' делаем то же самое.

3: Строим конструкцию следущего вида:

$$\begin{pmatrix} k_{i_1} & \ldots & k_{i_l} \\ k_{t_1} & \ldots & k_{t_l} \end{pmatrix} \qquad \begin{pmatrix} \ldots \\ \ldots \end{pmatrix} \qquad \begin{pmatrix} k_{j_1} & \ldots & k_{j_q} \\ k_{r_1} & \ldots & k_{r_q} \end{pmatrix}.$$

Здесь каждая скобка соответствует одному значению столбца s; в верхней строке находятся позиции, на которых столбец s встречается в P; в нижней — в P'.

4: Переставляя элементы нижней строки в каждой скобке всеми способами, получим всевозможные искомые перестановки π_1.

---

2. Случай $J = \{\pi_1, \pi_2\}$

По определению получаем

$$y = f(x) = \pi_2(g(\pi_1(x))).$$

Утверждение 2. Пусть имеется m пар открытых текстов и шифртекстов вида (P_i, C_i), $i = 1, \ldots, m$. Составим матрицы P и C из открытых текстов P_i и шифртекстов C_i соответственно:

$$P = \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_m \end{pmatrix}, \quad C = \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_m \end{pmatrix}.$$

Необходимым условием единственности решения системы уравнений

$$C_i = \pi_2(g(\pi_1(P_i))), \quad i = 1, \ldots, m, \tag{1}$$

является отсутствие одинаковых столбцов в каждой из матриц P и C.

Поиск всех решений системы (1) представлен в алгоритме 2.

Алгоритм 2. Нахождение всех возможных пар перестановок (π_1, π_2)

Вход: (P_i, C_i), $i = 1, \ldots, m$.
Выход: все пары (π_1, π_2), такие, что $C_i = \pi_2(g(\pi_1(P_i))), i = 1, \ldots, m$.

1: Строим матрицу P' из C_i.
2: Среди P_i, $i = 1, \ldots, m$, выбираем такой открытый текст P_j, который уравновешен или больше всего приближен к уравновешенности по сравнению с другими открытыми текстами. Пусть C_j — соответствующий шифртекст.
3: Ищем все x, такие, что $\mathrm{w}(x) = \mathrm{w}(P_j)$ и $\mathrm{w}(g(x)) = \mathrm{w}(C_j)$, где $\mathrm{w}(x)$ — вес вектора x.
4: **Для каждого** такого x по алгоритму 1 с исходными данными (P_j, x), $m = 1$ находим все перестановки π_1 со свойством $g^{-1}(x) = \pi_1(P_j)$.
5: **Для всех** найденных перестановок π_1:
6: строим матрицу

$$P = \begin{pmatrix} g(\pi_1(P_1)) \\ g(\pi_1(P_2)) \\ \vdots \\ g(\pi_1(P_m)) \end{pmatrix}.$$

7: **Если** каждый столбец матрицы P встречается в ней столько же раз, сколько и в P', **то**, выполняя шаги 2–4 алгоритма 1, находим все перестановки π_2 и пары (π_1, π_2) записываем в ответ.

Алгоритмы 1 и 2 реализованы программно, проведена серия экспериментов при значениях n от 3 до 29, количестве входных текстов, достаточных для однозначного определения ключа, и табличном задании функции g. Алгоритм 1 при всех n находит перестановку π_1 за доли секунды; алгоритм 2 работает гораздо дольше и время его работы зависит не только от n, но и от количества таких x, что $\mathrm{w}(x) = \mathrm{w}(P_j)$ и $\mathrm{w}(g(x)) = \mathrm{w}(C_j)$. Это количество растёт экспоненциально с ростом n и, например, для $n = 15$ в среднем равно 664.

ЛИТЕРАТУРА

1. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.

УДК 519.151, 519.725, 519.165 DOI 10.17223/2226308X/12/29

БЛОКИРОВКА ЛИНЕЙНЫХ МНОГООБРАЗИЙ И ТРОЙКИ ШТЕЙНЕРА

М. В. Ведунова, А. О. Игнатова, К. Л. Геут

Рассматриваются задачи блокировки троек Штейнера, применимые в схемах разделения секрета. Описан метод построения блокирующего множества минимальной и максимальной мощности. Для дополнительного множества найден метод оценки минимальной мощности дополнения как в линейных, так и в нелинейных системах троек Штейнера. Для соответствующих матроидов реализованы идеальные схемы разделения секрета на основе интерполяционных многочленов с нулевым следом. В нелинейной системе троек Штейнера с 13 элементами найдены максимальные и минимальные мощности дополнения блокирующего множества.

Ключевые слова: *системы троек Штейнера, схемы разделения секрета, блокирующие множества.*

Во втором раунде международной интернет-олимпиады по криптографии NSUCRYPTO-2015 [1] была предложена задача на специальный приз программного комитета «A secret sharing», в 2016 и 2017 гг. отмеченная как всё ещё не решённая [2, 3]. Решение этой задачи рассматривается с точки зрения блокировки двумерных аффинных многообразий над полем GF(2). Здесь под задачей блокировки семейства S подмножеств T множества E понимается задача построения такого минимального по включению подмножества M, что любое подмножество T из семейства S имеет непустое пересечение с M. Каждое такое подмножество M называется блокирующим множеством семейства S, а подмножество $L = E \setminus M$ — дополнением блокирующего множества. Задача блокировки троек Штейнера может трактоваться как вспомогательная при решении исходной задачи NSUCRYPTO, поскольку каждое такое многообразие является сдвигом однозначно определённого двумерного линейного многообразия, соответствующего линейной тройке Штейнера [4]. Проблеме вложимости произвольной системы троек Штейнера в совершенный двоичный код посвящена работа [5]. Проблеме реализации связи блок-схем с семейством троек Штейнера, где однородный матроид, когиперплоскости которого — это тройки Штейнера, соответствует идеальной схеме разделения секрета, посвящена работа [6]. Линейные системы троек Штейнера S_n — системы с $v = 2^n - 1$ элементами — ненулевыми битовыми строками длины n, $n \geqslant 3$, в которых бинарная операция квазигруппы Штейнера есть побитовое сложение по модулю два. Для матроидов линейных троек Штейнера ниже построены соответствующие им схемы разделения секрета [7, 8], а также рассмотрены методы построения блокирующих множеств минимальной и максимальной мощности.

Утверждение 1. Мощность l дополнения L блокирующего множества удовлетворяет неравенству $l(l+1)/2 \geqslant v$.

Используя данное неравенство, получим, что для нелинейной тройки Штейнера при $v = 13$ минимальная мощность дополнения $l = 5$, а для $v = 31$ не может быть меньше восьми.