Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7 DOI 10.17223/2226308X/11/17

КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ НА БУЛЕВЫХ ФУНКЦИЯХ[1]

Г. П. Агибалов, И. А. Панкратова

Даётся определение криптосистемы с открытым ключом на булевых функциях, общая схема построения атак на неё с известным открытым текстом и оценки вычислительной сложности таких атак.

Ключевые слова: *векторные булевы функции, обратимость, криптосистемы с открытым ключом, криптанализ.*

Введение

Целью данного сообщения является краткий обзор недавней работы авторов [1], в которой для шифрования и цифровой подписи предложена криптосистема с открытым ключом, построенная с использованием нетипичного для таких криптосистем математического аппарата — обратимых систем булевых функций, получаемых аналогично симметричному шифру в [2] из биективных векторных булевых функций при помощи операций перестановки и отрицания аргументов и координатных функций в них. Кроме определения криптосистемы, в [1] даются постановки и решения задач криптанализа как шифра, так и схемы цифровой подписи в криптосистеме атаками с известным открытым текстом, описывается общая схема построения таких атак, сводящаяся к решению системы логических уравнений методом линеаризационного множества [3, 4], излагаются конкретные атаки, построенные по этой схеме для всевозможных типов закрытого ключа, и приводятся асимптотические оценки вычислительной сложности этих атак. Все эти результаты, за исключением конкретных атак в частных случаях по причине их многочисленности, содержатся в данном обзоре.

1. Определение

Пусть $n \in \mathbb{N}$, $n \geqslant 2$, и $\mathbb{S}_n$ является множеством всех перестановок в строке $(1\,2\,\ldots\,n)$, т. е. $\mathbb{S}_n = \{(i_1 i_2 \ldots i_n) : i_j \in \{1,2,\ldots,n\}, j \neq r \Rightarrow i_j \neq i_r; j,r \in \{1,\ldots,n\}\}$. Перестановка $\pi = (i_1 i_2 \ldots i_n) \in \mathbb{S}_n$ называется *операцией перестановки*, если результат её применения к любому слову $w = w_1 w_2 \ldots w_n$ есть слово $\pi(w) = w_{i_1} w_{i_2} \ldots w_{i_n}$. Булев вектор $\sigma = b_1 b_2 \ldots b_n \in \mathbb{F}_2^n$ называется *операцией отрицания*, если результат его применения к набору $\alpha = a_1 a_2 \ldots a_n$ булевых величин (констант, переменных, функций) $a_1, \ldots, a_n$ является набором $\alpha^\sigma = a_1^{b_1} a_2^{b_2} \ldots a_n^{b_n}$, где для a и b в $\mathbb{F}_2$ имеет место $a^b = a$, если $b = 1$, и $a^b = \neg a$, если $b = 0$. Операции перестановки и отрицания называются тождественными, если $\pi = (1\,2\,\ldots\,n)$ и $\sigma = 11\ldots1$ соответственно.

Тройка $\mathcal{C} = (X, K, Y)$ называется *асимметричной криптосистемой на булевых функциях*, или сокращённо ACBF, если в ней X есть множество открытых текстов,

[1]Работа выполнена при поддержке РФФИ, проект № 17-01-00354.

или сообщений, $X \subseteq \mathbb{F}_2^n$; Y — множество шифртекстов, или (цифровых) подписей, $Y \subseteq \mathbb{F}_2^n$, и $K = K_1 \times K_2$ — множество ключей, где K_1 есть множество открытых ключей, $K_1 \subseteq K_n(g) = \{f(x) : f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1}))); \sigma_1, \sigma_2 \in \mathbb{F}_2^n; \pi_1, \pi_2 \in \mathbb{S}_n\}$; $x = (x_1, \ldots, x_n)$ — набор из различных булевых переменных; $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — биективная векторная булева функция $g(x) = g_1(x)g_2(x)\ldots g_n(x)$ (мы называем её *порождающей функцией* криптосистемы $\mathcal{C}$) со всеми её координатными функциями $g_1(x), \ldots, g_n(x)$, заданными некоторым конструктивным способом и вычислимыми с полиномиальной (от n) временной сложностью; π_1, π_2 и σ_1, σ_2 являются соответственно операциями перестановки и отрицания (мы называем их *ключевыми параметрами* криптосистемы $\mathcal{C}$); $K_2 = \{f^{-1} : f \in K_1\}$ — множество закрытых ключей.

В $\mathcal{C}$, как и в любом асимметричном шифре, открытый ключ f используется для зашифрования открытого текста x, а закрытый ключ f^{-1} — для расшифрования соответствующего шифртекста y, а именно: $y = f(x)$ и $x = f^{-1}(y)$ для $x \in X$, $y \in Y$, $f \in K_1$, $f^{-1} \in K_2$. Точно так же, в $\mathcal{C}$, как и в любой схеме цифровой подписи с подписанным сообщением, закрытый ключ f^{-1} используется для подписания сообщения x, а открытый ключ f — для проверки подписей, а именно: подпись под сообщением x есть $s = f^{-1}(x)$, и она действительна, если и только если $f(s) = x$.

Стойкость ACBF $\mathcal{C}$ основывается на трудности обращения больших биективных векторных булевых функций, то есть вычисления $x = f^{-1}(y)$ для $y = f(x)$. Для криптоаналитика, который, как предполагается, не знает значений ключевых параметров π_1, π_2, σ_1 и σ_2 в f, эта проблема действительно трудна с экспоненциальной временной сложностью алгоритма разрешения.

2. Задача криптанализа

Рассматриваемая задача криптанализа для ACBF $\mathcal{C}$ заключается в вычислении закрытого ключа в предположении, что известны некоторые открытые тексты или сообщения и соответствующие шифртексты или подписи. Если $\mathcal{C}$ является шифром, то задача состоит в следующем: даны $f(x) \in K_1$, $P_l \in X$ и $C_l = f(P_l)$, $l = 1, 2, \ldots, m$, требуется вычислить $f^{-1}(y)$. Иначе, т. е. если $\mathcal{C}$ есть схема цифровой подписи, задача иная: даны $f(x) \in K_1$, $M_l \in X$ и $S_l = f^{-1}(M_l)$, $l = 1, 2, \ldots, m$, требуется вычислить $f^{-1}(x)$. Задача в первом случае называется криптанализом шифра, во втором — криптанализом подписи, методы их решения называются атаками на шифр и на схему цифровой подписи соответственно. Направленные на раскрытие закрытого ключа, они являются атаками полного раскрытия. Предполагается, что при заданном открытом ключе $f(x)$ каждый имеет возможность вычислить его значение в любой точке x за полиномиальное время, но никакой криптоаналитик не знает его параметров $\pi_1, \pi_2, \sigma_1, \sigma_2$ (как в шифре ElGamal, например).

3. Общая схема атак

Такая схема описывается для произвольной криптосистемы $\mathcal{C}(J) = (X, K(J), Y)$, где $J \subseteq I = \{\pi_1, \pi_2, \sigma_1, \sigma_2\}$, $X = Y = \mathbb{F}_2^n$, $K(J) = K_1(J) \times K_2(J)$, $K_2(J) = \{f^{-1}(x) : f(x) \in K_1(J)\}$, $K_1(J) = K_n(g, J)$ и $K_n(g, J)$ есть множество всех функций $f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$, таких, что $\pi_1, \pi_2 \in \mathbb{S}_n$, $\sigma_1, \sigma_2 \in \mathbb{F}_2^n$ и каждый ключевой параметр в $I \setminus J$ тождественный. По определению, $K_n(g, J) \subseteq K_n(g)$, поэтому $\mathcal{C}(J)$ есть в действительности ACBF; $K_n(g, I) = K_n(g)$, поэтому $\mathcal{C}(I) = \mathcal{C}$; $K_n(g, \varnothing) = \{g(x)\}$, поэтому $\mathcal{C}(\varnothing)$ является тривиальной криптосистемой.

Вводятся следующие обозначения: A и D суть перестановочные матрицы перестановок π_1 и π_2 соответственно; b и d — булевы векторы-столбцы $\neg\sigma_1$ и $\neg\sigma_2$ соответствен-

но. Это позволяет применять символы переменных A, D, b, d вместо символов операций $\pi_1, \pi_2, \sigma_1, \sigma_2$ соответственно в множествах I, J, а также в формулах для $f(x), f^{-1}(x)$ и уравнениях для x, y и P_l, C_l, превращая эти формулы и уравнения в булевы (над $\mathbb{F}_2$). Например, $\{\pi_1, \sigma_2\} = \{A, d\}$ и $\pi_1(x^{\sigma_1}) = A(x \oplus b)$.

Атаки на шифр в ACBF $\mathcal{C}(J)$ строятся по следующей общей схеме:

1) Выразить функцию $f^{-1}(y)$ формулой из переменных и операций в множестве $J \cup \{y, g, \oplus, \cdot, ^{-1}\}$.
2) Записать систему уравнений E, выражающую зависимость переменных из множества J от значений P_l, C_l, $1 \leqslant l \leqslant n$, посредством операций $\oplus, \cdot, ^{-1}$ и функции g.
3) Решить систему E для неизвестных в J, применяя подходящий метод [3].
4) Заменить переменные из J в формуле для $f^{-1}(y)$ их значениями в решении системы E. Полученная формула и есть результат атаки.
5) Оценить вычислительную сложность атаки как временную сложность решения системы уравнений E.

Описание общей схемы атаки на цифровую подпись в ACBF $\mathcal{C}(J)$ получается из данной схемы для шифра подстановкой $f^{-1}(x)$, M_l и S_l вместо $f^{-1}(y)$, C_l и P_l соответственно.

Атаки на ACBF, построенные в [1] по данной схеме для $\mathcal{C}(J)$, $\varnothing \neq J \subseteq I$, в случаях нелинейной системы уравнений E решают последнюю методом линеаризационного множества (LS). Их построение ниже иллюстрируется атаками на шифр и подпись в криптосистеме $\mathcal{C}(I)$.

4. Атаки на ACBF $\mathcal{C}(I)$

4.1. Атака на шифр

Имеем $y = f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1}))) = D(g(A(x \oplus b)) \oplus d)$; $D^{-1}y \oplus d = g(A(x \oplus b))$, $A^{-1}(g^{-1}(D^{-1}y \oplus d)) \oplus b = x$, $f^{-1}(y) = x$ и $C_l = f(P_l)$, $l = 1, 2, \ldots, m$. Следовательно,

$$f^{-1}(y) = A^{-1}g^{-1}(D^{-1}y \oplus d) \oplus b,$$

где (D^{-1}, d, b, A) есть решение системы уравнений

$$D^{-1}C_l \oplus d = g(A(P_l \oplus b)), \quad l = 1, 2, \ldots, m,$$

которая решается методом LS, а именно поочерёдным присвоением различных значений переменным A, b и решением получаемой системы линейных уравнений с неизвестными в D^{-1} и d. Вычислительная сложность этой атаки равна асимптотически $\mathrm{O}(n!2^n)$.

4.2. Атака на подпись

Имеем $S_l = f^{-1}(M_l) = A^{-1}g^{-1}(D^{-1}M_l \oplus d) \oplus b$, $l = 1, 2, \ldots, m$, и

$$f^{-1}(x) = A^{-1}g^{-1}(D^{-1}x \oplus d) \oplus b,$$

где (D^{-1}, d, b, A) есть решение системы уравнений

$$D^{-1}M_l \oplus d = g(A(S_l \oplus b)), \quad l = 1, 2, \ldots, m,$$

которая решается методом LS: поочерёдно присваиваем различные значения переменным A, b и решаем получаемую систему линейных уравнений с неизвестными D^{-1} и d. Вычислительная сложность и этой атаки равна асимптотически $\mathrm{O}(n!2^n)$.

5. Вычислительная сложность атак на ACBF

В таблице приведён порядок $h(n)$ вычислительной сложности $\mathrm{O}(h(n))$ атаки, построенной по общей схеме на шифр и схему подписи в ACBF $\mathcal{C}(J)$ для каждого непустого подмножества ключевых параметров $J \subseteq I$. Здесь $p(n)$ — некоторый полином от n.

J	$\{\sigma_1\}$	$\{\pi_1\}$	$\{\pi_1,\sigma_1\}$	$\{\sigma_2\}$	$\{\sigma_1,\sigma_2\}$	$\{\pi_1,\sigma_2\}$	$\{\pi_1,\sigma_1,\sigma_2\}$	$\{\pi_2\}$
$h(n)$	$p(n)$	$p(n)$	$\mathrm{C}_n^{n/2}$	$p(n)$	2^n	$\mathrm{C}_n^{n/2}$	$2^n\mathrm{C}_n^{n/2}$	$p(n)$

J	$\{\pi_2,\sigma_1\}$	$\{\pi_1,\pi_2\}$	$\{\pi_1,\pi_2,\sigma_1\}$	$\{\pi_2,\sigma_2\}$	$\{\pi_2,\sigma_1,\sigma_2\}$	$\{\pi_1,\pi_2,\sigma_2\}$	$\{\pi_1,\pi_2,\sigma_1,\sigma_2\}$
$h(n)$	$\mathrm{C}_n^{n/2}$	$n!$	$n!$	$p(n)$	2^n	$n!$	$n!2^n$

ЛИТЕРАТУРА

1. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.
2. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
3. *Агибалов Г. П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского государственного университета. Приложение. 2006. № 17. С. 4–9.
4. *Агибалов Г. П.* Логические уравнения в криптоанализе генераторов ключевого потока // Вестник Томского государственного университета. Приложение. 2003. № 6. С. 31–41.

УДК 519.1 DOI 10.17223/2226308X/11/18

О СВОЙСТВАХ ДВУХ КЛАССОВ S-БОКСОВ РАЗМЕРА 16×16

В. М. Бобров, С. М. Комиссаров

Нелинейные отображения векторного пространства V_n (s-боксы размера $n \times n$) в симметричных алгоритмах блочного шифрования обычно реализуются в виде таблиц, содержащих множество всех образов. Для хранения одного такого массива требуется $n2^n$ бит памяти. Это вынуждает в алгоритмах блочного шифрования использовать s-боксы малых размеров (8×8 бит в алгоритме «Кузнечик», 4×4 в алгоритме «Магма», 6×4 в DES, 8×8 в AES). Предложена алгоритмическая реализация s-боксов 16×16 бит на основе функции модифицированного аддитивного генератора, а также на основе легковесного алгоритма блочного шифрования NASH. Лучшая максимальная разностная характеристика построенных s-боксов равна $18/2^{16}$. Минимальная степень нелинейности среди координатных функций равна 15. Минимальная степень нелинейности среди всех нетривиальных линейных комбинаций координатных функций равна 14–15. Лучшая линейная характеристика равна $764/2^{15}$.

Ключевые слова: *модифицированный аддитивный генератор, алгоритм NASH, s-бокс, максимальная разностная характеристика, максимальная линейная характеристика, степень нелинейности.*

Обозначим V_n — n-мерное векторное пространство над полем GF(2). Пусть $V_n^\times = V_n \backslash \{0\}$. Для некоторого вектора $a \in V_n$ определим линейную булеву функцию $l_a : V_n \to \mathrm{GF}(2)$:

$$l_a(x) = \bigoplus_{i=0}^{n-1} a_i \cdot x_i.$$

Корреляцию двух булевых функций f_1 и f_2 обозначим как

$$c(f_1, f_2) = 2^{1-n}|\{x : f_1(x) = f_2(x)\}| - 1.$$