2. *Перов А. А., Пестунов А. И.* Статистическое тестирование современных итеративных блочных шифров с помощью программной библиотеки «УНИБЛОКС-2015» // Инновации в жизнь. 2016. № 2. С. 89–97.

УДК 519.6 DOI 10.17223/2226308X/12/64

СПОСОБ РЕШЕНИЯ НЕДООПРЕДЕЛЁННЫХ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД GF(2) С ИСКАЖЁННЫМИ ПРАВЫМИ ЧАСТЯМИ И ОГРАНИЧЕНИЕМ НА МАЛЫЙ ВЕС РЕШЕНИЯ

Н. Ю. Руменко, А. В. Костюк

Рассматриваются недоопределённые случайные системы линейных булевых уравнений с искажёнными правыми частями, истинное решение которых имеет малый вес Хемминга. Экспериментально показывается, что для малых вероятностей искажения такие системы могут быть эффективно решены применением алгоритмов декодирования по информационным множествам.

Ключевые слова: *случайные системы линейных булевых уравнений, декодирование по информационным множествам.*

Рассмотрим систему из фиксированного числа $m < n$ линейных булевых уравнений (СЛУ)

$$Ax = b = Ax_0 \oplus \xi, \tag{1}$$

где A — случайная двоичная матрица размера $m \times n$; $\xi^{\mathrm{T}} = (\xi_0, \ldots, \xi_{m-1})$ — случайный двоичный вектор ошибок, координаты которого независимы и принимают значения с вероятностями $\mathsf{P}\{\xi_i = 1\} = 1 - \mathsf{P}\{\xi_i = 0\} = p$, $i \in \{0, \ldots, m-1\}$, $p \in [0, 1/2)$; x_0 — вектор истинного решения, $||x_0|| = w$, $||.||$ — вес Хемминга.

Для малых значений w известны алгоритмы решения таких систем, основанные на переборе возможных значений истинного решения [1, 2].

В алгоритме максимума правдоподобия [1] непосредственно вычисляются все возможные векторы y длины n веса w и в качестве решения выдаётся вектор с наименьшим значением $||Ay||$. Алгоритм имеет асимптотическую сложность $\mathrm{O}((1-2p)^{-2} n^w \log n)$ при использовании $\mathrm{O}(1)$ бит дополнительной (помимо хранения системы уравнений) памяти [2].

В работе [2] рассматривается вычислительно более эффективный алгоритм на основе метода «встречи посередине» с емкостной сложностью $\mathrm{O}(n^{w/2})$ и вычислительной сложностью $\mathrm{O}(n^{w/2} l((m-t)\log n^{w/2} + wm))$, где t — пороговое значение $||Ay||$; l — число итераций.

Вычислительная сложность алгоритмов данного класса более всего зависит от параметра w, что делает их малоприменимыми для слабоискажённых систем с достаточно большим весом истинного решения.

С другой стороны, матрицу A можно рассматривать как проверочную матрицу некоторого случайного линейного блокового кода $M(n, n-m)$, для которого вектор b является синдромом ошибки веса w, причём каждый бит синдрома дополнительно искажён с вероятностью p. Задача решения системы (1), таким образом, состоит в декодировании случайного кода по искажённому синдрому.

Составим расширенную систему

$$Ch = b, \tag{2}$$

где $C = \left[\, I \,\middle|\, A \,\right]$, I — единичная матрица размера $m \times m$; $h^{\mathrm{T}} = [\, \xi \,|\, x_0 \,]$ и $[\, \cdot \,|\, \cdot \,]$ обозначает конкатенацию.

В системе (2) правая часть уже «неискажённая», при этом вектор решения имеет некоторый случайный вес $w + t$, где t зависит только от m и p. По условию $p \ll 1/2$, поэтому с большой вероятностью вес решения по-прежнему останется малым. В рассмотренной постановке матрица C является проверочной матрицей для некоторого случайного кода $M'(n + m, n)$.

Известно [3], что почти все случайные коды лежат на границе Варшамова — Гилберта, т. е. код $M'(n + m, n)$ почти наверное исправляет все ошибки кратности до $\lfloor (d-1)/2 \rfloor$, где d удовлетворяет неравенству $2^m \leqslant \sum\limits_{i=0}^{d-2} \binom{n+m-1}{i}$. Таким образом, при достаточно малых значениях вероятности искажения p для решения системы (2) могут быть использованы алгоритмы декодирования по информационным множествам, большое количество которых было разработано в рамках криптоанализа систем Мак-Элиса и Нидеррайтера [4].

Для оценки эффективности предлагаемого способа использован алгоритм Мэя — Мюэра — Томае [4] (ALGORITHM 2), сравнение проводилось с алгоритмом из работы [2] (ALGORITHM 1), результаты среднего времени выполнения приведены в табл. 1 и 2. Проведённые эксперименты показывают, что для достаточно малых вероятностей искажения предложенный способ позволяет находить истинное решение более эффективно, чем перебор возможных решений.

Таблица 1

СЛУ с искажённой правой частью,
$n = 256$, $m = 128$, $w = 8$

Вероятность искажения p	Среднее время выполнения, с	
	ALGORITHM 1	ALGORITHM 2
0,001	144,284	0,062
0,005	164,131	0,120
0,010	191,219	0,355
0,020	305,235	1,625

Таблица 2

СЛУ с искажённой правой частью,
$n = 512$, $m = 200$, $w = 10$

Вероятность искажения p	Среднее время выполнения, с	
	ALGORITHM 1	ALGORITHM 2
0,001	> 7200	12,100
0,005	> 7200	49,021
0,010	> 7200	109,960
0,020	> 7200	576,460

ЛИТЕРАТУРА

1. *Балакин Г. В.* Введение в теорию случайных систем уравнений // Труды по дискретной математике. М.: ТВП, 1997. Т. 1. С. 1–18.
2. *Алексейчук А. Н., Грязнухин А. Ю.* Быстрый алгоритм восстановления истинного решения фиксированного веса системы линейных булевых уравнений с искажённой правой частью // Прикладная дискретная математика. 2013. Т. 20. № 2. С. 59–70.

3. *Варшамов Р. Р.* Оценка числа сигналов в кодах с коррекцией ошибок // Доклады АН СССР. 1957. С. 739–741.
4. *May A., Meurer A., and Thomae E.* Decoding random linear codes in $O(2^{0.054n})$ // Proc. Asiacrypt'2011. Seoul, South Korea, December 04–08, 2011. P. 107–124.

УДК 519.7 DOI 10.17223/2226308X/12/65

О ПОЧТИ СОВЕРШЕННЫХ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЯХ И РАЗДЕЛЯЮЩЕМ СВОЙСТВЕ МУЛЬТИМНОЖЕСТВ

М. А. Сорокин, М. А. Пудовкина

Рассматриваются некоторые классы APN-преобразований относительно возможности построения интегральных различителей с помощью разделяющего свойства. Проведён вычислительный эксперимент по определению величины $\lceil n/d \rceil$ для выбранных APN-преобразований $\mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$, где d — алгебраическая степень. Из полученных результатов следует, что не все APN-преобразования имеют наилучшее значение $\lceil n/d \rceil = 2$. Выделены APN-преобразования с параметрами, наиболее оптимальными для противодействия интегральному анализу с помощью разделяющего свойства.

Ключевые слова: *APN-преобразование, разделяющее свойство, интегральный различитель, интегральный метод.*

Разностный метод и его обобщения являются одними из основных методов анализа симметричных шифрсистем. Один из этапов разностного метода заключается в нахождении элементов матрицы вероятностей переходов разностей компонент функции зашифрования, включая S-боксы. В работе [1] для противодействия разностному методу при синтезе алгоритмов блочного шифрования в качестве S-бокса предложено использовать APN-преобразование (если оно существует).

Определение 1 [1]. Преобразование $s : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ называется APN-преобразованием, если для каждых ненулевых элементов $\alpha, \beta \in \mathrm{GF}(2^n)$ уравнение $s(x + \alpha) - s(x) = \beta$ имеет два или нуль решений.

Актуальной задачей является исследование APN-преобразований относительно других методов криптоанализа, в частности относительно интегрального метода. В [2] приводится способ построения интегрального различителя с использованием разделяющего свойства (англ. division property).

Пусть V_n — n-мерное векторное пространство над полем $\mathrm{GF}(2)$; $\|\alpha\|$ — вес Хэмминга вектора α; α_i — i-я координата вектора $\alpha = (\alpha_1, \ldots, \alpha_n) \in V_n$, $i \in \{1, \ldots, n\}$.

Для каждого элемента $\beta \in \mathrm{GF}(2)$ положим $\beta^1 = \beta$, $\beta^0 = 1$. Тогда корректно определено отображение $\pi : V_n \times V_n \to V_n$, заданное условием

$$\pi : (\alpha, \delta) \mapsto \prod_{i=1}^{n} \alpha_i^{\delta_i}, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in V_n, \ \delta = (\delta_1, \ldots, \delta_n) \in V_n.$$

Далее будем рассматривать отображение $\pi(x, \delta)$ только при фиксированном $\delta \in V_n$.

Определение 2 [2]. Пусть $n \in \mathbb{N}$, $k \in \{1, \ldots, n\}$, $S_k^{(n)} = \{\alpha \in V_n : k \leqslant \|\alpha\|\}$. Говорят, что мультимножество X с носителем V_n имеет разделяющее свойство $D_k^{(n)}$, если для каждого $\delta \in V_n \setminus S_k^{(n)}$ выполняется равенство $\bigoplus\limits_{\alpha \in X} \pi(\alpha, \delta) = 0$.