15. *Панкратова И. А.* Булевы функции в криптографии: учеб. пособие. Томск: Издательский Дом Томского государственного университета, 2014. 88 с.

УДК 519.24

АСИМПТОТИЧЕСКИЕ СВОЙСТВА МНОЖЕСТВА РЕШЕНИЙ ИСКАЖЁННЫХ СИСТЕМ УРАВНЕНИЙ

А. В. Волгин

Рассматриваются две однородные системы уравнений: система уравнений, в левой части которых стоят функции k-значной логики, и система уравнений, в левой части которых стоят функции, полученные из функций первой системы путём их независимого случайного искажения. Выведены условия на вероятностные законы искажений функций, обеспечивающие три варианта взаимного поведения множеств решений этих систем при согласованном увеличении числа уравнений и числа неизвестных.

Ключевые слова: *системы уравнений, функции k-значной логики, искажённые функции.*

Пусть $\Omega_k = \{0, 1, \ldots, k-1\}$, $F_k(n) = \{f : \Omega_k^n \to \Omega_k\}$ — множество всех n-местных функций k-значной логики от переменных $x_1, \ldots, x_n$, $n, k \in \mathbb{N}$. Рассмотрим систему из $T \in \mathbb{N}$ уравнений

$$f_t(x) = 0, \quad f_t \in F_k(n), \quad t = 1, \ldots, T. \tag{1}$$

Через S обозначим множество решений системы (1).

Каждой функции $f \in F_k(n)$ сопоставим множества $A_0(f)$ и $A_1(f)$ тех значений аргумента, на которых она принимает значение нуль и отлична от нуля соответственно. Обозначим $a_0(f) = |A_0(f)|$, $a_1(f) = |A_1(f)|$. Для каждой функции $f \in F_k(n)$ и целого числа $0 \leqslant d \leqslant a_0(f)$ рассмотрим множество функций

$$B(f, d) = \{g \in F_k(n) : |A_0(f) \cup A_1(g)| + |A_1(f) \cup A_0(g)| = d\},$$

таких, что при $g \in B(f, d)$ число значений аргументов, в которых одна из функций f и g принимает значение нуль, а другая отлична от нуля, равно d.

На множествах $B(f_1, d), \ldots, B(f_T, d)$ зададим равномерные вероятностные распределения, в соответствии с которыми выберем случайно и независимо функции $\tilde{f}_1, \ldots, \tilde{f}_T$. Рассмотрим систему случайных уравнений

$$\tilde{f}_t(x_1, \ldots, x_n) = 0, \quad \tilde{f}_t \in B(f_t, d), \quad t = 1, \ldots, T. \tag{2}$$

Множество её решений обозначим через $\tilde{S}$.

Рассматривается задача нахождения связи между множествами S и $\tilde{S}$ решений систем уравнений (1) и (2) при выполнении следующих асимптотических условий: при $T, n \to \infty$ сами функции $f_1, \ldots, f_T$ меняются так, что

1) число решений системы (1) имеет конечный предел, т. е. $|S| \to \Sigma \in \mathbb{N}$;

2) число значений аргументов, на которых функции f_t, $t = 1, \ldots, T$, принимают значение нуль, неограниченно возрастает, т. е. $a_0(f_t) \to \infty$, $t = 1, \ldots, T$.

В [1] данная задача рассматривается для случая булевых уравнений, при этом предполагается, что каждая функция системы (1) является уравновешенной, т. е. принимает каждое из значений нуль и единица ровно на 2^{n-1} значениях аргумента. В данной

работе рассматривается обобщение на случай произвольных функций k-значной логики с учётом асимптотических условий 1 и 2, при этом уравновешенности функций не требуется.

Обозначим $a_{\min} = \min\{a_0(f_1), \ldots, a_0(f_T)\}$, $a_{\max} = \max\{a_0(f_1), \ldots, a_0(f_T)\}$.

Теорема 1. Пусть $n, T \to \infty$, $|S| \to \Sigma \in \mathbb{N}$, $T/a_{\min} \to 0$. Тогда:

1) если параметр d меняется так, что $d\sum\limits_{t=1}^{T} \dfrac{N^n - a_0(f_t)}{a_0(f_t)N^n} \to \infty$, то

$$\mathbf{P}\{\tilde{S} \cap S = \varnothing\} \to 1;$$

2) если параметр d меняется так, что $d\sum\limits_{t=1}^{T} \dfrac{N^n - a_0(f_t)}{a_0(f_t)N^n} \to \varkappa \in (0, \infty)$ и $\dfrac{Td}{a_{\min}} < c$, $c = \mathrm{const} > 0$, то распределение случайной величины $|\tilde{S} \cap S|$ сходится к $\mathrm{Bi}(\Sigma, e^{-\varkappa})$ — биномиальному распределению с параметрами Σ и $e^{-\varkappa}$;

3) если параметр d меняется так, что $d\sum\limits_{t=1}^{T} \dfrac{N^n - a_0(f_t)}{a_0(f_t)N^n} \to 0$ и $a_{\max} < \dfrac{N^n}{2}$, то

$$\mathbf{P}\{S \subseteq \tilde{S}\} \to 1.$$

ЛИТЕРАТУРА

1. *Михайлов В. Г.* Оценка точности пуассоновской аппроксимации для числа пустых ячеек в равновероятной схеме размещения частиц комплектами и её применения // Труды Матем. ин-та им. В. А. Стеклова РАН. 2013. Т. 282. С. 165–180.

УДК 519.7

ВЛИЯНИЕ ВЕСА ХЭММИНГА РАЗНОСТИ НА ВЕРОЯТНОСТЬ ЕЁ СОХРАНЕНИЯ ПОСЛЕ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ[1]

А. И. Пестунов

Теоретически исследована зависимость между вероятностью сохранения разности двух величин после их сложения (вычитания) по модулю с третьей равномерно распределённой величиной и весом Хэмминга этой разности. Под разностью понимается общепринятая в криптоанализе операция XOR. Доказано, что если старший бит разности равен 0, то вероятность её сохранения равна 2^{-h}, где h — вес Хэмминга разности, и равна $2^{-(h-1)}$, если старший бит разности равен 1.

Ключевые слова: *дифференциальный криптоанализ, разностный анализ, блочный шифр, вес Хэмминга.*

Дифференциальный криптоанализ [1] вместе со своими модификациями является распространённым подходом к анализу стойкости итеративных блочных шифров, однако далеко не всегда авторы дифференциальных атак обосновывают их строго математически. Тем не менее некоторые шаги в этом направлении предпринимаются. Так, в работе [2] предложена модель марковского шифра, в рамках которой вычисляются вероятности характеристик; там же сформулирована гипотеза стохастической эквивалентности, негласно подразумеваемая в более ранних работах. В [3] показана возможность создания шифра, доказуемо стойкого к дифференциальному криптоанализу, а в [4] разработана модель, позволяющая создать такой шифр. Работа [5] посвящена изложению дифференциального криптоанализа в общем виде применительно

[1]Работа поддержана грантом РФФИ, проект № 14-01-31484 (мол_а).