УДК 519.7

О ВЕРОЯТНОСТИ ПРОТЯЖКИ ОДНОБИТОВОЙ РАЗНОСТИ ЧЕРЕЗ СЛОЖЕНИЕ И ВЫЧИТАНИЕ ПО МОДУЛЮ

А. И. Пестунов

Институт вычислительных технологий СО РАН, г. Новосибирск, Россия

E-mail: pestunov@gmail.com

Доказано, что вероятность протяжки однобитовой разности через сложение и вычитание по модулю равна 1, если этот бит является старшим, и 1/2, если этот бит отличен от старшего. Проведённые эксперименты подтверждают эти результаты.

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

Введение

Разностный (дифференциальный) анализ [1] вместе со всевозможными своими разновидностями (см., например, [2 – 5]) является одним из наиболее распространённых методов исследования стойкости блочных шифров. К настоящему моменту в рамках этого подхода разработано довольно много атак, однако крайне редко построение характеристик и дифференциалов, лежащих в основе данных атак, а также вычисление их вероятностей обосновывается строго математически.

Отметим некоторые работы, посвящённые теоретической обоснованности разностного анализа. В [6] предложена модель так называемого марковского шифра, в рамках которой вычисляются вероятности характеристик и дифференциалов. В [7] сформулирована гипотеза стохастической эквивалентности, используемой, например, при оценке вероятности успеха разностных атак. В [8] разработана модель, в рамках которой можно создать шифр, доказуемо стойкий к разностному и линейному анализу. Работа [9] посвящена изложению разностного анализа в общем виде применительно к произвольным итеративным блочным шифрам с аддитивным раундовым ключом.

Другой важной проблемой является изучение возможности так называемой *протяжки* (propagation) разности через различные операции, используемые в блочном шифре, т. е. в оценивании вероятности того, что пара блоков (подблоков) с определённой разностью преобразуется в пару блоков с такой же или другой, но также определённой разностью. В частности, в работе по разностному анализу шифра RC5 [10] утверждается, что однобитовая разность остаётся неизменной после операции сложения с вероятностью 1/2 или с вероятностью 1, если этот единственный бит — старший. Данное утверждение никак не обосновывается, за исключением того, что проводятся некоторые эксперименты, подтверждающие достоверность разработанной атаки. В работах по разностному анализу шифров MARS [11] и CAST-256 [12] также используется этот факт со ссылкой на [10].

В настоящей работе данные факты доказываются математически строго и осуществляется экспериментальная проверка полученных теоретических результатов. Под протяжкой разности двоичных векторов $X \oplus Y$ через операцию $\circ$ понимается разность $D = (X \circ Z) \oplus (Y \circ Z)$ со случайным двоичным вектором Z. Вероятность того, что $D = X \oplus Y$, называется вероятностью этой протяжки.

1. Предварительные замечания

Проиллюстрируем обозначенную проблему на примере операций XOR и циклического сдвига, которые обозначим соответственно через $\oplus$ и $<<<$. Пусть даны два блока (подблока) X и Y с определённой разностью Δ, другими словами, $X \oplus Y = \Delta$.

Поскольку $\oplus$ — коммутативная операция, то

$$(X \oplus Z) \oplus (Y \oplus Z) = X \oplus Y.$$

Это означает, что операция XOR не изменяет разность, и вероятность протяжки разности через неё равна 1. Для наглядности изобразим этот факт следующим образом:

$$\Delta \xrightarrow[p=1]{\oplus Z} \Delta.$$

Подобным свойством обладает и операция циклического сдвига: она подчиняется закону дистрибутивности, поэтому

$$(X^{<<<Z}) \oplus (Y^{<<<Z}) = (X \oplus Y)^{<<<Z}.$$

Следовательно,

$$\Delta \xrightarrow[p=1]{<<<Z} \Delta^{<<<Z}.$$

Что касается арифметических операций, то в общем случае при произвольно взятой разности Δ не существует такой разности Δ^*, чтобы выполнялось

$$\Delta \xrightarrow[p=1]{\boxplus Z} \Delta^*,\ \Delta \xrightarrow[p=1]{\boxminus Z} \Delta^* \text{ или } \Delta \xrightarrow[p=1]{\circledast Z} \Delta^*.$$

Тем не менее в ряде случаев можно осуществить протяжку разности с достаточно большой вероятностью, в частности, в данной работе рассматривается случай однобитовой разности.

Обозначения, используемые в работе: s — длина двоичного вектора (в битах); $\{0,1\}^s$ — множество всех двоичных векторов длины s; $X \sim \mathcal{U}\{0,1\}^s$ — случайная величина X имеет равномерное распределение на $\{0,1\}^s$; $\boxplus$, $\boxminus$, $\circledast$ — соответственно сложение, вычитание и умножение по модулю 2^s; $X^{[i]}$ — i-й бит двоичного вектора X (0 — младший, $(s-1)$ — старший); $X^{[s_1,\ldots,s_2]}$ — двоичный вектор длины $(s_1 - s_2 + 1)$, $s_1 \geqslant s_2$, составленный из битов вектора X с номерами $s_1, \ldots, s_2$.

2. Теоретические результаты

Теорема 1. Пусть X, Y, $Z \in \{0,1\}^s$ и $X \oplus Y = 2^m$, где $0 \leqslant m \leqslant s-1$. Тогда

а) $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$, если $m = s-1$;

б) $\mathrm{P}\big((X \boxplus Z) \oplus (Y \boxplus Z) = 2^m\big) = 1/2$, если $m < s-1$ и $X, Y, Z \sim \mathcal{U}\{0,1\}^s$.

Доказательство. В пп. 1–2 производится представление используемых величин в удобном виде; п. 3 посвящён доказательству утверждения *а*; в пп. 4–7 доказывается утверждение *б*.

1. Условие $X \oplus Y = 2^m$ означает, что либо $Y^{[m]} = 0$ и $X = Y + 2^m$, либо $X^{[m]} = 0$ и $Y = X + 2^m$. Не ограничивая общности, положим, что $X^{[m]} = 0$ и $Y = X + 2^m$.

Представим X, Y и Z следующим образом:

$$X = x_1 \cdot 2^{m+1} + x_2,\ Y = x_1 \cdot 2^{m+1} + 2^m + x_2 \text{ и } Z = z_1 \cdot 2^{m+1} + \delta \cdot 2^m + z_2,$$

где $x_1 = X^{[s-1,\ldots,m+1]}$, $x_2 = X^{[m-1,\ldots,0]}$, $z_1 = Z^{[s-1,\ldots,m+1]}$, $z_2 = Z^{[m-1,\ldots,0]}$, $\delta = Z^{[m]}$.

Рассмотрим величины X и Y как s-битовые векторы и изобразим их схематично:

$$X = (\overbrace{?,\ldots,?}^{x_1}, 0, \overbrace{?,\ldots,?}^{x_2}); \quad Y = (\overbrace{?,\ldots,?}^{x_1}, 1, \overbrace{?,\ldots,?}^{x_2});$$

$$x_1 \cdot 2^{m+1} = (\overbrace{?,\ldots,?}^{x_1}, 0, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \; 2^m = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, 1, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \; x_2 = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, 0, \overbrace{?,\ldots,?}^{x_2}).$$

Аналогичная схематичная запись для Z примет следующий вид:

$$Z = (\overbrace{?,\ldots,?}^{z_1}, \delta, \overbrace{?,\ldots,?}^{z_2}); \quad z_1 \cdot 2^{m+1} = (\overbrace{?,\ldots,?}^{z_1}, 0, \overbrace{0,\ldots,0}^{m\,\text{бит}});$$

$$\delta \cdot 2^m = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, \delta, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \quad z_2 = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, 0, \overbrace{?,\ldots,?}^{z_2}).$$

2. Представим выражения $X \boxplus Z$ и $Y \boxplus Z$, используя введённые в п. 1 обозначения:

$$X \boxplus Z = (x_1 + z_1) \cdot 2^{m+1} + \delta \cdot 2^m + (z_2 + x_2) \pmod{2^s}; \tag{1}$$

$$Y \boxplus Z = (x_1 + z_1) \cdot 2^{m+1} + (\delta + 1) \cdot 2^m + (z_2 + x_2) \pmod{2^s}. \tag{2}$$

Из определений для x_2 и z_2 следует, что $x_2 \leqslant 2^m - 1$ и $z_2 \leqslant 2^m - 1$, поэтому $x_2 + z_2 < 2^{m+1}$, значит, эту сумму можно записать следующим образом:

$$x_2 + z_2 = \gamma \cdot 2^m + v, \text{ где } \gamma = (x_2 + z_2)^{[m]} \text{ и } v = (x_2 + z_2) - \gamma \cdot 2^m. \tag{3}$$

Смысл этого представления заключается в том, что величина $(x_2 + z_2)$ задаётся в виде суммы старшего m-го бита и всех остальных.

Аналогичным образом можно выразить сумму $(x_1 + z_1)$:

$$x_1 + z_1 = \hat{\gamma} \cdot 2^{s-1-m} + u, \text{ где } \hat{\gamma} = (x_1 + z_1)^{[s-1-m]} \text{ и } u = (x_1 + z_1) - \hat{\gamma} \cdot 2^{s-1-m}.$$

Отсюда вытекает, что первое слагаемое в формулах (1) и (2) можно записать так:

$$(x_1 + z_1) \cdot 2^{m+1} = \hat{\gamma} \cdot 2^{s-1-m} \cdot 2^{m+1} + u \cdot 2^{m+1} = \hat{\gamma} \cdot 2^s + u \cdot 2^{m+1}. \tag{4}$$

Подставим выражения (3) и (4) в формулы (1) и (2); с учётом того, что $\hat{\gamma} \cdot 2^s = 0 \pmod{2^s}$, получим

$$X \boxplus Z = u \cdot 2^{m+1} + (\gamma + \delta) \cdot 2^m + v \pmod{2^s}; \tag{5}$$

$$Y \boxplus Z = u \cdot 2^{m+1} + (\gamma + \delta + 1) \cdot 2^m + v \pmod{2^s}. \tag{6}$$

Слагаемые, присутствующие в этих суммах, изобразим схематично:

$$u \cdot 2^{m+1} = (\overbrace{?,\ldots,?}^{u}, 0, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \quad \gamma \cdot 2^m = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, \gamma, \overbrace{0,\ldots,0}^{m\,\text{бит}});$$

$$\delta \cdot 2^m = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, \delta, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \quad v = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, 0, \overbrace{?,\ldots,?}^{v}).$$

3. Докажем утверждение *а* теоремы. Заметим, что $x_1 = z_1 = 0$ при $m = s$, поэтому $u = 0$ и выражения (5) и (6) примут вид

$$X \boxplus Z = (\gamma + \delta) \cdot 2^{s-1} + v \pmod{2^s}; \tag{7}$$

$$Y \boxplus Z = (\gamma + \delta + 1) \cdot 2^{s-1} + v \pmod{2^s}. \tag{8}$$

Согласно введённым обозначениям, $v < 2^{s-1}$, поэтому $v^{[s-1]} = 0$. В то же время $(s-2)$ младших бит у выражений $(\gamma+\delta)\cdot 2^{s-1}$ и $(\gamma+\delta+1)\cdot 2^{s-1}$ равны нулю. Из формул (7) и (8) следует, что

$$\big((X \boxplus Z) \oplus (Y \boxplus Z)\big)^{[i]} = 0,\ i = 0, 1, \ldots, s-2.$$

Таким образом, осталось доказать, что $\big((X \boxplus Z) \oplus (Y \boxplus Z)\big)^{[s-1]} = 1$.

Рассмотрим два случая: $(\gamma + \delta) \bmod 2 = 0$ и $(\gamma + \delta) \bmod 2 = 1$.

В первом случае $(\gamma + \delta) \cdot 2^{s-1} = 0 \pmod{2^s}$, а $(\gamma + \delta + 1) \cdot 2^{s-1} = 1 \pmod{2^s}$. Значит,

$$(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m.$$

Во втором случае $(\gamma + \delta) \cdot 2^{s-1} = 1 \pmod{2^s}$, а $(\gamma + \delta + 1) \cdot 2^{s-1} = 0 \pmod{2^s}$. Следовательно, в этом случае также

$$(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m,$$

и утверждение *а* доказано.

4. Перейдём к доказательству утверждения *б*. Обозначим через $\mathcal{A}$ рассматриваемое событие $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$ и, используя формулу полной вероятности [13, с. 39], запишем

$$\mathrm{P}(\mathcal{A}) = \mathrm{P}(\mathcal{A}|\delta = 0)\mathrm{P}(\delta = 0) + \mathrm{P}(\mathcal{A}|\delta = 1)\mathrm{P}(\delta = 1).$$

По условию теоремы $Z \sim \mathcal{U}\{0,1\}^s$, поэтому $\mathrm{P}(\delta = 0) = \mathrm{P}(\delta = 1) = 1/2$. Следовательно,

$$\mathrm{P}(\mathcal{A}) = \big(\mathrm{P}(\mathcal{A}|\delta = 0) + \mathrm{P}(\mathcal{A}|\delta = 1)\big)/2. \tag{9}$$

5. Вычислим $\mathrm{P}(\mathcal{A}|\delta = 0)$. Рассмотрим случаи $\gamma = 0$ и $\gamma = 1$.

При $\delta = 0$ и $\gamma = 0$ выражения (5) и (6) примут вид

$$X \boxplus Z = (u \cdot 2^{m+1} + v) \bmod 2^s = u \cdot 2^{m+1} + v;$$
$$Y \boxplus Z = (u \cdot 2^{m+1} + 2^m + v) \bmod 2^s = u \cdot 2^{m+1} + 2^m + v.$$

Покажем схематично:

$$X \boxplus Z = (\overbrace{?, \ldots, ?}^{u}, 0, \overbrace{?, \ldots, ?}^{v}); \quad Y \boxplus Z = (\overbrace{?, \ldots, ?}^{u}, 1, \overbrace{?, \ldots, ?}^{v}).$$

Отсюда следует, что $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$.

Таким образом, если $\gamma = 0$, то $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$ с вероятностью 1.

Рассмотрим случай $\gamma = 1$. Выражения (5) и (6) примут вид

$$X \boxplus Z = u \cdot 2^{m+1} + 2^m + v \pmod{2^s};$$
$$Y \boxplus Z = u \cdot 2^{m+1} + 2^m + 2^m + v = (u+1) \cdot 2^{m+1} + v \pmod{2^s}.$$

Или схематично:

$$X \boxplus Z = (\overbrace{?, \ldots, ?}^{u}, 1, \overbrace{?, \ldots, ?}^{v}); \quad Y \boxplus Z = (\overbrace{?, \ldots, ?}^{(u+1) \bmod 2^{s-1-m}}, 0, \overbrace{?, \ldots, ?}^{v}).$$

Для наступления события $\mathcal{A}$ необходимо выполнение условия $u + 1 = u \pmod{2^{s-1-m}}$, однако такого u не существует, следовательно, при $\gamma = 1$ выполнено $\mathrm{P}(\mathcal{A}|\delta = 0) = 0$. Таким образом, $\mathrm{P}(\mathcal{A}|\delta = 0) = \mathrm{P}(\gamma = 0)$.

6. Аналогично рассуждениям из п. 5 вычислим $\mathrm{P}(\mathcal{A}|\delta = 1)$. Рассмотрим случай $\gamma = 1$, тогда выражения (5) и (6) примут вид

$$X \boxplus Z = (u+1)\cdot 2^{m+1} + v \pmod{2^s}; \quad Y \boxplus Z = (u+1)\cdot 2^{m+1} + 2^m + v \pmod{2^s},$$

или схематично:

$$X \boxplus Z = (\overbrace{?,\ldots,?}^{(u+1) \bmod 2^{s-1-m}}, 0, \overbrace{?,\ldots,?}^{v}); \quad Y \boxplus Z = (\overbrace{?,\ldots,?}^{(u+1) \bmod 2^{s-1-m}}, 1, \overbrace{?,\ldots,?}^{v}).$$

Таким образом, если $\gamma = 1$, то $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$ с вероятностью 1.

Если $\gamma = 0$, то выражения (5) и (6) примут вид

$$X \boxplus Z = u\cdot 2^{m+1} + 2^m + v \pmod{2^s}; \quad Y \boxplus Z = (u+1)\cdot 2^{m+1} + v \pmod{2^s},$$

или схематично:

$$X \boxplus Z = (\overbrace{?,\ldots,?}^{u}, 1, \overbrace{?,\ldots,?}^{v}); \quad Y \boxplus Z = (\overbrace{?,\ldots,?}^{(u+1) \bmod 2^{s-1-m}}, 0, \overbrace{?,\ldots,?}^{v}).$$

Для наступления события $\mathcal{A}$ необходимо выполнение условия $u + 1 = u \pmod{2^{s-1-m}}$, однако такого u не существует, следовательно, при $\gamma = 0$ получим $\mathrm{P}(\mathcal{A}|\delta = 1) = 0$.

Таким образом, $\mathrm{P}(\mathcal{A}|\delta = 1) = \mathrm{P}(\gamma = 1)$.

7. Подставляя вероятности, вычисленные в пп. 4–5, в формулу (9), получим

$$\mathrm{P}(\mathcal{A}) = \big(\mathrm{P}(\gamma = 0) + \mathrm{P}(\gamma = 1)\big)/2 = 1/2.$$

Следовательно, утверждение *б* теоремы доказано. ■

Следствие 1. Пусть $X, Y, Z \in \{0,1\}^s$ и $X \oplus Y = 2^m$, где $0 \leqslant m \leqslant s-1$. Тогда

а) $(X \boxminus Z) \oplus (Y \boxminus Z) = 2^m$, если $m = s-1$;

б) $\mathrm{P}\big((X \boxminus Z) \oplus (Y \boxminus Z) = 2^m\big) = 1/2$, если $m < s-1$ и $X, Y, Z \sim \mathcal{U}\{0,1\}^s$.

Доказательство. Если Z, Z' — случайные величины и $Z \sim \mathcal{U}\{0,1\}^s$, $Z' = -Z \pmod{2^s}$, то $Z' \sim \mathcal{U}\{0,1\}^s$, поскольку для каждого $x \in \{0,1\}^s$ существует единственный $y \in \{0,1\}^s$, такой, что $-x = y \pmod{2^s}$. Следовательно, для Z' выполнены условия теоремы 1, и следствие доказано. ■

3. Экспериментальное подтверждение теоретических результатов

Проверку утверждений *б* теоремы и следствия проведём двумя способами. Во-первых, предположим, что вероятность протяжки разности неизвестна, и вычислим для неё несмещённую состоятельную оценку. Во-вторых, при помощи критерия хи-квадрат [14] проверим гипотезу о том, что вероятность протяжки разности равна $1/2$. Эксперименты проведены при $s = 32$ и $m = 0, \ldots, 31$.

Для каждого m сгенерируем две выборки $\mathcal{X} = (X_1, \ldots, X_n)$ и $\mathcal{Z} = (Z_1, \ldots, Z_n)$, где $X_i, Z_i \sim \mathcal{U}\{0,1\}^{32}$ и $n = 10000$. Затем сформируем выборку $\mathcal{Y}^m = (Y_1^m, \ldots, Y_n^m)$, где $Y_i^m = X_i \oplus 2^m$.

Введём следующие величины ($i = 1, \ldots, n$):

$$\xi_i^m = \begin{cases} 1, & \text{если } (X_i \boxplus Z_i) \oplus (Y_i^m \boxplus Z_i) = 2^m, \\ 0, & \text{если } (X_i \boxplus Z_i) \oplus (Y_i^m \boxplus Z_i) \neq 2^m; \end{cases}$$

$$\eta_i^m = \begin{cases} 1, & \text{если } (X_i \boxminus Z_i) \oplus (Y_i^m \boxminus Z_i) = 2^m, \\ 0, & \text{если } (X_i \boxminus Z_i) \oplus (Y_i^m \boxminus Z_i) \neq 2^m. \end{cases}$$

Проверку утверждений теоремы и следствия проведём при помощи выборок $\Xi^m = (\xi_1^m, \ldots, \xi_n^m)$ и $\Theta^m = (\eta_1^m, \ldots, \eta_n^m)$ соответственно. При $m = 31$ проверим, что $\xi_i^m = \eta_i^m = 1$, $i = 1, \ldots, n$. При $m < 31$ проверим, что эти случайные величины имеют распределение Бернулли с параметром $1/2$, т. е.

$$\mathrm{P}(\xi_i^m = 0) = \mathrm{P}(\xi_i^m = 1) = \mathrm{P}(\eta_i^m = 0) = \mathrm{P}(\eta_i^m = 1) = 1/2.$$

Для этого вычислим величины $\nu_{\boxplus}^m = \sum\limits_{i=1}^{n} \xi_i^m$, $\nu_{\boxminus}^m = \sum\limits_{i=1}^{n} \eta_i^m$.

Кроме того, поскольку параметр распределения Бернулли является математическим ожиданием, а несмещённой состоятельной оценкой для него является выборочное среднее, то вычислим и его. Выборочные средние для выборок Ξ^m и Θ^m вычисляются по формулам $\nu_{\boxplus}^m/n$ и $\nu_{\boxminus}^m/n$ соответственно.

Очевидно, что если проверяемая гипотеза верна, то

$$\nu_{\boxplus}^m \approx \nu_{\boxminus}^m \approx n/2 = 5000.$$

Далее по каждому $\nu_{\boxplus}^m$ и $\nu_{\boxminus}^m$ вычисляем статистику хи-квадрат при $p = 1/2$ по следующей формуле [14]:

$$x_p^2(\nu) = \frac{(\nu - np)^2}{np} + \frac{((n - \nu) - n(1 - p))^2}{n(1 - p)}. \tag{10}$$

Результаты приведены в таблице, из которой видно, что выборочные средние $\nu_{\boxplus}^m/n$ и $\nu_{\boxminus}^m/n$ близки к $1/2$.

Для использования критерия хи-квадрат рассмотрим квантиль этого распределения уровня 0,05 с одной степенью свободы: $\chi_{1;0,05} = 3{,}84$. Как видно из таблицы, статистика $x_{0,5}^2$ превышает эту квантиль только в трёх случаях из 62 (эти значения выделены жирным шрифтом). Данные превышения могут быть отнесены к статистической погрешности, поскольку при используемой квантили ошибка первого рода составляет 5 %. Если взять $\chi_{1;0,01} = 6{,}64$, то превышений не будет.

Для генерации псевдослучайных чисел из выборок $\mathcal{X}$ и $\mathcal{Z}$ использован шифр MARS [15], состоящий из 10 раундов, поскольку в работе [16] показано, что уже такое сокращённое количество раундов обеспечивает удовлетворительные статистические свойства данного шифра. Программная реализация шифра MARS взята из библиотеки Б. Глэдмена [17], где на языке C++ реализованы шифры-кандидаты конкурса AES.

Для проверки утверждений a теоремы и следствия выбрано $n = 2^{32}$ и в качестве выборки $\mathcal{X}$ взяты не случайные числа, а все возможные значения. Выборка $\mathcal{Z}$ попрежнему формировалась из псевдослучайных чисел при помощи 10 раундов шифра MARS. Результаты экспериментов показали, что в 100 % случаев $\xi_i^m = \eta_i^m = 1$.

Экспериментальная проверка утверждений *б* теоремы и следствия

m (№ бита)	$\nu^m_{\boxplus}$	$\nu^m_{\boxplus}/n$	$x^2_{0,5}(\nu^m_{\boxplus})$	$\nu^m_{\boxminus}$	$\nu^m_{\boxminus}/n$	$x^2_{0,5}(\nu^m_{\boxminus})$
0	4990	0,499	0,04	4972	0,497	0,31
1	4957	0,496	0,74	4884	0,488	**5,38**
2	4958	0,496	0,71	4935	0,493	1,69
3	5077	0,508	2,37	4992	0,499	0,03
4	5100	0,510	**4,00**	4963	0,496	0,55
5	4951	0,495	0,96	4975	0,498	0,25
6	4991	0,499	0,03	5059	0,506	1,39
7	5023	0,502	0,21	4976	0,498	0,23
8	5024	0,502	0,23	4987	0,499	0,07
9	5010	0,501	0,04	4965	0,496	0,49
10	4923	0,492	2,37	4982	0,498	0,13
11	5062	0,506	1,54	5045	0,504	0,81
12	5095	0,510	3,61	5049	0,505	0,96
13	4920	0,492	2,56	4968	0,497	0,41
14	5076	0,508	2,31	5038	0,504	0,58
15	5046	0,505	0,85	5041	0,504	0,67
16	5058	0,506	1,35	4970	0,497	0,36
17	5049	0,505	0,96	5101	0,510	**4,08**
18	4960	0,496	0,64	5056	0,506	1,25
19	4945	0,495	1,21	5007	0,501	0,02
20	4975	0,498	0,25	5037	0,504	0,55
21	4989	0,499	0,05	4982	0,498	0,13
22	5017	0,502	0,12	5041	0,504	0,67
23	5033	0,503	0,44	4955	0,495	0,81
24	5073	0,507	2,13	4945	0,495	1,21
25	4914	0,491	2,96	5020	0,502	0,16
26	4961	0,496	0,61	4927	0,493	2,13
27	5083	0,508	2,76	5004	0,500	0,01
28	5009	0,501	0,03	4936	0,494	1,64
29	5041	0,504	0,67	5095	0,510	3,61
30	4970	0,497	0,36	5081	0,508	2,62

Заключение

В настоящей работе рассмотрена проблема теоретического вычисления вероятности протяжки разности через арифметические операции. Точнее, доказано, что вероятность протяжки однобитовой разности через сложение и вычитание по модулю равна $1/2$, если разность расположена не в старшем бите, и 1 — если в старшем.

Следующими шагами, продолжающими данную работу, могут стать исследования вероятности протяжки разности через умножение по модулю и вероятности протяжки разности в зависимости от её веса Хемминга.

ЛИТЕРАТУРА

1. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
2. *Wagner D.* The boomerang attack // LNCS. 1999. V. 1636. P. 156–170.
3. *Kelsey J., Kohno T, and Schneier B.* Amplified boomerang attacks against reduced-round MARS and Serpent // LNCS. 2001. V. 1978. P. 75–93.
4. *Biham E., Biryukov A, and Shamir A.* Cryptanalysis of Skipjack reduced to 31 round using impossible differentials // LNCS. 1999. V. 1592. P. 12–23.
5. *Пестунов А. И.* Блочные шифры и их криптоанализ // Вычислительные технологии. 2007. Т. 12, спец. вып. № 4. С. 42–49.

6. *Lai X. and Massey J.* Markov ciphers and differential cryptanalysis // LNCS. 1991. V. 547. P. 17–38.
7. *Nyberg K. and Knudsen L.* Provable security against a differential attack // J. Cryptology. 1995. No. 8. P. 27–37.
8. *Vaudenay S.* Decorrelation: a theory for block cipher security // J. Cryptology. 2003. No. 16. P. 249–286.
9. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1(1). С. 34–42.
10. *Biryukov A. and Kushilevitz E.* Improved cryptanalysis of RC5 // LNCS. 1998. V. 1403. P. 85–99.
11. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра MARS // Прикладная дискретная математика. 2009. № 4(6). С. 56–63.
12. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информационных технологий. 2009. № 4. С. 57–62.
13. *Боровков А. А.* Теория вероятностей. М.: Наука, 1976. 352 с.
14. *Боровков А. А.* Математическая статистика. М.: Наука, 1984. 472 с.
15. *Burwick C. et al.* MARS — a candidate cipher for AES // NIST AES Proposal, 1999.
16. *Пестунов А. И.* Статистический анализ современных блочных шифров // Вычислительные технологии. 2007. Т. 12. № 2. С. 122–129.
17. `www.gladman.me.uk` — Brian Gladman's Home Page. 2012.