

УДК 519.7

О ВЛИЯНИИ ВЕСА ХЭММИНГА РАЗНОСТИ ДВУХ ВЕЛИЧИН НА ВЕРОЯТНОСТЬ ЕЁ СОХРАНЕНИЯ ПОСЛЕ СЛОЖЕНИЯ И ВЫЧИТАНИЯ

А. И. Пестунов

Аннотация. Исследуется зависимость между вероятностью сохранения разности двух величин после их сложения и вычитания по модулю и весом Хэмминга этой разности. Под разностью двух величин понимается стандартная для дифференциального криптоанализа операция XOR. Доказано, что если старший бит разности равен 0 (равен 1), то вероятность её сохранения равна 2^{-h} (равна $2^{-(h-1)}$), где h — вес Хэмминга разности. Проведено экспериментальное подтверждение полученных теоретических результатов.

Ключевые слова: дифференциальный криптоанализ, разностный анализ, блочный шифр, дифференциал, характеристика.

Введение

Разностный анализ (дифференциальный криптоанализ) [7] наряду со своими модификациями (см., например, [2, 6, 9, 13]) представляет собой широко распространённый метод анализа стойкости итеративных блочных шифров. Существует достаточно много атак, разработанных при помощи этого подхода, однако далеко не всегда авторы производят их строгое математическое обоснование.

Отметим некоторые работы, посвящённые математическому обоснованию разностного анализа. В [10] предложена модель так называемого марковского шифра, в рамках которой вычисляются вероятности характеристик и дифференциалов, а также сформулирована гипотеза стохастической эквивалентности, используемой, в частности, при оценке вероятности успеха разностных атак. В [11] доказана принципиальная возможность создания шифра, доказуемо стойкого к классической разностной атаке. В [12] разработана модель, позволяющая создать шифр, доказуемо стойкий к разностному и линейному анализу. Работа [1] посвящена

изложению разностного анализа в общем виде применительно к произвольным итеративным блочным шифрам с аддитивным раундовым ключом.

Другой важной, но не изученной глубоко проблемой является изучение того, как изменяется разность блоков или подблоков после различных операций, используемых в итеративных блочных шифрах. При этом оценивается вероятность того, что пара блоков (подблоков) с определённой разностью преобразуется некоторой операцией в пару блоков с той же или другой, но так же определённой разностью. Для некоторых операций, например, циклического сдвига или XOR, данная проблема решается тривиально (см. рассуждения ниже), но для таких часто используемых операций, как сложение, вычитание и умножение по модулю, изучение изменения разности не является тривиальной задачей.

В работе [8], посвящённой разностному анализу шифра RC5, утверждается, что однобитовая разность остаётся неизменной после операции сложения с вероятностью $1/2$ или с вероятностью 1 , если единственный бит старший. Это утверждение не доказано в [8], но проведены эксперименты, подтверждающие достоверность разработанной атаки. В работах по разностному анализу шифров MARS [4] и CAST-256 [3] данный факт используется со ссылкой на [8] и последующими экспериментами, подтверждающими достоверность разработанных атак. В [5] этот факт доказан и подтверждён экспериментально.

В [3] используется экспериментально найденная зависимость между весом Хэмминга разности и вероятностью её сохранения после сложения по модулю. В нашей работе существование этой зависимости обосновано. Доказано, что если старший бит разности равен 0 (равен 1), то вероятность её сохранения равна 2^{-h} (равна $2^{-(h-1)}$), где h — вес Хэмминга разности. Проведено экспериментальное подтверждение полученных результатов.

1. Предварительные замечания и обозначения

Введём следующие обозначения:

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 — сложение и вычитание по модулю 2^s соответственно;

\oplus — исключающее, или XOR;

\lll — операция циклического сдвига;

x_i, y_i, z_i, δ_i — i -е биты векторов X, Y, Z, Δ соответственно, где 0 — младший бит, $s - 1$ — старший;

$H(\Delta)$ — вес Хэмминга величины Δ .

Во введении замечено, что задача изучения преобразования разности после операций циклического сдвига и XOR решается тривиально. Поясним, как это делается. Пусть даны два блока (подблока) X и Y с определённой разностью Δ , другими словами, $X \oplus Y = \Delta$. Поскольку операция XOR коммутативна, имеем

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

Это означает, что операция XOR не изменяет разности, и вероятность её сохранения после операции XOR равна 1. Для наглядности данный факт изображают следующим стандартным образом:

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

Такая лёгкость возникает из-за того, что преобразование битов операцией XOR производится независимо.

Подобным свойством обладает и операция циклического сдвига:

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

Здесь разность не сохраняется, но преобразуется в другую с вероятностью 1, поэтому можно записать

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

Что же касается операций сложения и вычитания по модулю, то в общем случае при произвольно взятой разности Δ не существует разности Δ^* такой, что

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

Эта проблема возникает вследствие того, что на значения старших битов при сложении могут оказывать влияние младшие (происходит перенос разрядов) и преобразования битов не являются независимыми.

Тем не менее, в ряде случаев можно изучить, как преобразуется разность после этих операций, и оценить вероятность её сохранения. Этому вопросу и посвящена данная работа.

2. Теоретические результаты

Теорема 1. Пусть $X, Z \sim \mathcal{U}\{0, 1\}^s$ и $Y = X \oplus \Delta$, где $H(\Delta) = h$, $0 \leq h \leq s - 1$. Тогда

- (a) $P((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta) = 2^{-h}$, если $\delta_{s-1} = 0$;
- (b) $P((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta) = 2^{-(h-1)}$, если $\delta_{s-1} = 1$.

ДОКАЗАТЕЛЬСТВО.

(i) Для удобства введём обозначения $S^x = X \boxplus Z$, $S^y = Y \boxplus Z$. Представим величины S^x и S^y как двоичные векторы:

$$S^x = (s_0^x, \dots, s_{s-1}^x), \quad S^y = (s_0^y, \dots, s_{s-1}^y).$$

Ранее замечено, что при суммировании зависимость между разрядами возникает из-за наличия переноса. В данном случае речь идёт о битах, поэтому переносы равны 1 или 0.

Запишем известные формулы суммирования и вычисления переноса для нашего случая:

$$\begin{aligned} s_i^x &= x_i \oplus z_i \oplus p_i^x, & p_i^x &= x_i z_i \oplus x_i p_{i-1}^x \oplus z_i p_{i-1}^x, \\ s_i^y &= y_i \oplus z_i \oplus p_i^y, & p_i^y &= y_i z_i \oplus y_i p_{i-1}^y \oplus z_i p_{i-1}^y, \\ i &= \overline{0, s-1}, & p_{-1}^x &= p_{-1}^y = 0. \end{aligned} \tag{1}$$

(ii) Используя S^x и S^y , представим событие $(X \boxplus Z) \oplus (Y \boxplus Z) = \Delta$ в виде $s_i^x \oplus s_i^y = \delta_i$, $i = \overline{0, s-1}$.

В силу (1) имеем $s_i^x \oplus s_i^y = x_i \oplus y_i \oplus p_{i-1}^x \oplus p_{i-1}^y = \delta_i \oplus p_{i-1}^x \oplus p_{i-1}^y$. Тем самым

$$S^x \oplus S^y = \Delta \iff p_i^x \oplus p_i^y = 0, \quad i = \overline{0, s-2}.$$

(iii) Докажем, что при $\delta_i = 1$

$$p_i^x \oplus p_i^y = 0, \quad i = \overline{0, s-2} \iff z_i = p_{i-1}.$$

(\Rightarrow) Поскольку $p_i^x \oplus p_i^y = 0$, то $p_i^x = p_i^y = p_i$, значит,

$$0 = p_i^x \oplus p_i^y = x_i z_i \oplus x_i p_{i-1} \oplus z_i p_{i-1} \oplus y_i z_i \oplus y_i p_{i-1} \oplus z_i p_{i-1}.$$

Отсюда видно, что при $\delta_i = 0$, т.е. при $x_i = y_i$, равенство является тождеством. В то же время из того, что $\delta_i = 1$, следует, что $z_i = p_{i-1}$.

(\Leftarrow) Пусть при $\delta_i = 1$ выполняется $z_i = p_{i-1}$, $i = \overline{0, s-2}$. Доказательство того, что $p_i^x \oplus p_i^y = 0$ проведём индукцией по i .

БАЗА ИНДУКЦИИ. Пусть $i = 0$, тогда по формулам (1)

$$p_0^x \oplus p_0^y = x_0 z_0 \oplus x_0 p_{-1}^x \oplus z_0 p_{-1}^x \oplus y_0 z_0 \oplus y_0 p_{-1}^y \oplus z_0 p_{-1}^y = x_0 z_0 \oplus y_0 z_0.$$

При $\delta_0 = 0$ это равенство является тождеством. При $\delta_0 = 1$ требуется выполнение $z_0 = p_{-1}$, что истинно в силу условия $z_i = p_{i-1}$ при $\delta_i = 1$.

ПРЕДПОЛОЖЕНИЕ ИНДУКЦИИ. Предположим, что $p_i^x \oplus p_i^y = 0$ при $i < t$.

ШАГ ИНДУКЦИИ. Используя предположение индукции, докажем, что $p_t^x \oplus p_t^y = 0$. В силу (1) имеем

$$p_t^x \oplus p_t^y = x_t z_t \oplus x_t p_{t-1}^x \oplus z_t p_{t-1}^x \oplus y_t z_t \oplus y_t p_{t-1}^y \oplus z_t p_{t-1}^y.$$

Согласно предположению индукции $p_{t-1}^x = p_{t-1}^y = p_{t-1}$, поэтому

$$p_t^x \oplus p_t^y = x_t z_t \oplus x_t p_{t-1} \oplus y_t z_t \oplus y_t p_{t-1}.$$

Отсюда видно, что при $\delta_t = 0$ равенство является тождеством, а при $\delta_t = 1$ оно следует из условия $z_t = p_{t-1}$.

(iv) Утверждение, доказанное в п. (iii), означает, что $S^x \oplus S^y = \Delta$ при $\delta_i = 1$ тогда и только тогда, когда выполняется $z_i = p_{i-1}$, $i = \overline{0, s-2}$. Значит, вероятности этих двух событий равны. Вычислим вероятность второго события.

Пусть $\delta_i = 1$ при $i \in \{i_1, \dots, i_h\}$. Поскольку $i \leq s-2$, то $i = s-1$ не попадает в это условие, значит, необходимо рассмотреть $i \in \{i_1, \dots, i_{\hat{h}}\}$, где $\hat{h} = h$ при $\delta_{s-1} = 0$ и $\hat{h} = h-1$ при $\delta_{s-1} = 1$.

Воспользуемся тем, что z_i — координаты вектора $Z \sim \mathcal{U}\{0, 1\}^s$, и получим

$$\begin{aligned} P(S^x \oplus S^y = \Delta) &= P(z_{i_1} = p_{i_1-1}, \dots, z_{i_{\hat{h}}} = p_{i_{\hat{h}}-1}) \\ &= \prod_{j=1}^{\hat{h}} P(z_{i_j} = p_{i_j-1}) = 1/2^{\hat{h}}. \end{aligned}$$

Теорема 1 доказана.

Следствие 1. Пусть $X, Z \sim \mathcal{U}\{0, 1\}^s$ и $Y = X \oplus \Delta$, $H(\Delta) = h$, $0 \leq h \leq s-1$. Тогда

- (а) $P((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta) = 2^{-h}$, если $\delta_{s-1} = 0$;
- (б) $P((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta) = 2^{-(h-1)}$, если $\delta_{s-1} = 1$.

ДОКАЗАТЕЛЬСТВО очевидным образом следует из теоремы 1 и того факта, что если $Z \sim \mathcal{U}\{0, 1\}^s$ и $Z' = -Z \bmod 2^s$, то $Z' \sim \mathcal{U}\{0, 1\}^s$.

Сформулируем доказанные утверждения в частном случае при $h = 1$. Этот случай рассмотрен в [5].

Следствие 2. Пусть $X, Z \sim \mathcal{U}\{0, 1\}^s$ и $Y = X \oplus 2^m$. Тогда

- (a) $P((X \boxplus Z) \oplus (Y \boxplus Z) = 2^m) = 1/2$, если $m < s - 1$;
- (b) $P((X \boxminus Z) \oplus (Y \boxminus Z) = 2^m) = 1/2$, если $m < s - 1$;
- (c) $P((X \boxplus Z) \oplus (Y \boxplus Z) = 2^m) = 1$, если $m = s - 1$;
- (d) $P((X \boxminus Z) \oplus (Y \boxminus Z) = 2^m) = 1$, если $m = s - 1$.

3. Экспериментальное подтверждение теоретических результатов

В данном разделе описаны эксперименты, проведённые с целью подтверждения полученных теоретических результатов. Эксперименты проведены при $s = 16$ и $h = \overline{0, 16}$.

Говоря неформально, подтверждение заключается в том, что рассматриваются все возможные пары X и Z (всего их, очевидно, 2^{32}), по каждому X вычисляется $Y = X \oplus \Delta$ и определяется число таких пар, для которых выполняется условие $(X \boxplus Z) \oplus (Y \boxplus Z) = \Delta$ (подтверждение теоремы 1) или $(X \boxminus Z) \oplus (Y \boxminus Z) = \Delta$ (подтверждение следствия 1). Отношение полученного числа к числу всех пар должно соответствовать теоретическим результатам.

Перейдём к формальному описанию экспериментов. Занумеруем все возможные пары X и Z , обозначив их через $R_i = (X_i, Z_i)$, $i = \overline{1, 2^{32}}$. Возьмём некоторое значение Δ^h (индекс h подчёркивает, что Δ имеет такой вес Хэмминга), где $\delta_{s-1}^h = 0$, вычислим $Y_i = X_i \oplus \Delta^h$ и введём следующие величины:

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

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

Если старший бит равен 1, то величина снабжается тильдой: $\tilde{\Delta}$. Тильдой отметим и другие величины, зависящие от неё: \tilde{Y}_i , $\tilde{\xi}_i^h$ и $\tilde{\eta}_i^h$.

Введём следующие обозначения:

$$\nu_{\boxplus}^h = \sum_{i=1}^{2^s} \xi_i^h, \quad \tilde{\nu}_{\boxplus}^h = \sum_{i=1}^{2^s} \tilde{\xi}_i^h, \quad \nu_{\boxminus}^h = \sum_{i=1}^{2^s} \eta_i^h, \quad \tilde{\nu}_{\boxminus}^h = \sum_{i=1}^{2^s} \tilde{\eta}_i^h.$$

Пусть $\nu_{\text{теор.}}^h = 2^{32}/2^h$ и $\tilde{\nu}_{\text{теор.}}^h = 2^{32}/2^{h-1}$, тогда согласно теореме 1 и следствию 1 должны выполняться следующие равенства:

$$\nu_{\boxplus}^h = \nu_{\text{теор.}}^h, \quad \tilde{\nu}_{\boxplus}^h = \tilde{\nu}_{\text{теор.}}^h, \quad \nu_{\boxminus}^h = \nu_{\text{теор.}}^h, \quad \tilde{\nu}_{\boxminus}^h = \tilde{\nu}_{\text{теор.}}^h.$$

У $\nu_{\text{теор.}}^h$ и $\tilde{\nu}_{\text{теор.}}^h$ опущены нижние индексы \boxplus и \boxminus , поскольку теоретические значения для $\nu_{\boxplus}^h, \tilde{\nu}_{\boxplus}^h, \nu_{\boxminus}^h, \tilde{\nu}_{\boxminus}^h$ не зависят от операции.

Проведённые эксперименты подтверждают теоретические результаты.

Заключение

В работе обоснована зависимость между вероятностью сохранения разности двух величин после их сложения и вычитания по модулю и весом Хэмминга этой разности. Доказано, что если старший бит разности равен 0 (равен 1), то вероятность её сохранения равна 2^{-h} (равна $2^{-(h-1)}$), где h — вес Хэмминга разности. Проведено экспериментальное подтверждение полученных теоретических результатов. Результаты статьи предназначены для использования при построении характеристик и дифференциалов, а также при разработке разностных атак.

ЛИТЕРАТУРА

1. Агибалов Г. П. Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикл. дискрет. математика. — 2008. — № 1. — С. 34–42.
2. Пестунов А. И. Блочные шифры и их криптоанализ // Вычисл. технологии. — 2007. — Т. 12, спец. вып. № 4. — С. 42–49.
3. Пестунов А. И. Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информ. технологий. — 2009. — № 4. — С. 57–62.
4. Пестунов А. И. Дифференциальный криптоанализ блочного шифра MARS // Прикл. дискрет. математика. — 2009. — № 4. — С. 56–63.
5. Пестунов А. И. О вероятности протяжки однобитовой разности через сложение и вычитание по модулю // Прикл. дискрет. математика. — 2012. — № 4. — С. 53–60.
6. Biham E., Biryukov A., Shamir A. Cryptanalysis of Skipjack reduced to 31 round using impossible differentials // Proc. Eurocrypt-99. — Berlin: Springer-Verl., 1999. — P. 12–23. (Lect. Notes Comp. Sci.; Vol. 1592).
7. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystem // J. Cryptology. — 1991. — Vol. 4. — P. 3–72.
8. Biryukov A., Kushilevitz E. Improved cryptanalysis of RC5 // Proc. Eurocrypt-98. — Berlin: Springer-Verl., 1998. — P. 85–99. (Lect. Notes Comp. Sci.; Vol. 1403).

9. **Kelsey J., Kohno T., Schneier B.** Amplified boomerang attacks against reduced-round MARS and Serpent // Proc. FSE-00. — Berlin: Springer-Verl., 2001. — P. 75–93. (Lect. Notes Comp. Sci.; Vol. 1978).
10. **Lai X., Massey J.** Markov ciphers and differential cryptanalysis // Proc. Eurocrypt-91. — Berlin: Springer-Verl., 1991. — P. 17–38. (Lect. Notes Comp. Sci.; Vol. 547).
11. **Nyberg K., Knudsen L.** Provable security against a differential attack // J. Cryptology. — 1995. — N 8. — P. 27–37.
12. **Vaudenay S.** Decorrelation: a theory for block cipher security // J. Cryptology. — 2003. — N 16. — P. 249–286.
13. **Wagner D.** The boomerang attack // Proc. FSE-99. — Berlin: Springer-Verl., 1999. — P. 156–170. (Lect. Notes Comp. Sci.; Vol. 1636).

Пестунов Андрей Игоревич,
e-mail: pestunov@gmail.com

Статья поступила
24 сентября 2012 г.
Переработанный вариант —
25 января 2013 г.