# О марковских свойствах усреднённых разностных характеристик итеративных блочных шифров

Дрелихов В.О., Никифоров М.С.

22 марта 2017

РУСКРИПТО - 2017

$(G,+)$ конечная абелевая группа, 0 - нейтральный элемент, $K$ - конечное множество (множество ключей),

$h: K \times G \to G$, при этом для произвольного $k \in K$ отображение $x \to h(k,x)$, $x \in G$, биективно.

***Итеративный блочный шифр*** - последовательность $m$ раундовых преобразований:

$$x_{i+1} = h(k_i, x_i),\ i = 0,1,...,m-1,\ k_i \in K,$$

где $k_0,...,k_{m-1}$ - раундовые ключи.

$x_0 \in G$ - входной блок (открытый тест) итеративного шифра,

$x_m \in G$ - выходной блок.

Пусть $(x_0^{(1)}, x_0^{(2)}) \hat{I}\ G^2$ - случайный вектор, равномерно распределённый на $G^2$.

Рекуррентные уравнения

$$x_{i+1}^{(1)} = h(k_i, x_i^{(1)}),\ i = 0,1,...,m - 1,$$

$$x_{i+1}^{(2)} = h(k_i, x_i^{(2)}),\ i = 0,1,...,m - 1$$

задают последовательность векторов $(x_0^{(1)}, x_0^{(2)}),(x_1^{(1)}, x_1^{(2)}),...,(x_m^{(1)}, x_m^{(2)})$.

Последовательность разностей: $\mathrm{D}_i = x_i^{(2)} - x_i^{(1)},\ i = 0,1,2,....$

– статистически связанные между собой случайные величины.

*Различные подходы к исследованию статистических зависимостей* $\mathsf{D}_i = x_i^{(2)} - x_i^{(1)}$, $i = 0,1,2,\ldots$.

**1 подход**: исследование зависимостей, когда раундовые ключи $k_0,\ldots,k_{m-1}$ фиксированы.

Условная вероятность $\mathrm{P}(\mathsf{D}_i = \mathsf{a}_1 \,/\, \mathsf{D}_0 = \mathsf{a}_0)$ зависит от $k_0,\ldots,k_{i-1}$, $0 < i \le m$.

**2 подход:** (упрощенная вероятностная модель)

Раундовые ключи $k_0,\ldots,k_{m-1}$ независимые случайные величины, равномерно распределены на $K$ и не зависят от $(x_0^{(1)}, x_0^{(2)}) \in G^2$.

Усреднённая вероятность перехода разностей

$$\mathsf{p}^{(i)}_{\mathsf{a}_0,\mathsf{a}_1} = \mathrm{E}_{k_0,\ldots,k_{i-1}} \mathrm{P}(\mathsf{D}_i = \mathsf{a}_1 \,/\, \mathsf{D}_0 = \mathsf{a}_0).$$

*1. Lai X, Massey J. L., Murphy S. Markov ciphers and differential cryptanalysis // EuroCrypt'91. Lect. Notes Comp. Sci.- 1991,- V.547. -P. 17-38.*

*2. Lai X. On the design and security of block ciphers. - Zurich: PhD. Swiss Federal Institute of Technology, 1992.*

**«Марковские шифры»**

свойство «марковости» шифра - условие инвариантности разностной характеристики для раундовой функции $h(k,x)$:

$$\mathrm{P}(h(k,x+\mathrm{a})-h(k,x)=\mathrm{b}) \text{ не зависит от } x \text{ для всех } \mathrm{a},\mathrm{b}\,\hat{\mathrm{I}}\,G,$$

(случайность задаётся раундовым ключом $k$).

**Theorem 2.** *If an r-round iterated cipher is a Markov cipher and the r round keys are independent and uniformly random, then the sequence of differences* $\Delta X = \Delta Y(0), \Delta Y(1), ..., \Delta Y(r)$ *is a homogeneous Markov chain. Moreover, this Markov chain is stationary if* $\Delta X$ *is uniformly distributed over the non-neutral elements of the group.*

*Lai X, Massey J. L., Murphy S. Markov ciphers and differential cryptanalysis*

Для марковского итеративного шифра с независимыми и равномерно распределёнными раундовыми ключами случайные величины $\mathsf{D}_i = x_i^{(2)} - x_i^{(1)}$, $i = 0,1,2,...$ связаны в однородную цепь Маркова.

$$\mathsf{p}^{(i)} = (\mathsf{p}^{(1)})^i.$$

Как можно использовать теорему 2 о марковских шифрах?

Неравенство Маркова.

При доказательстве теоремы 2 используется следующее утверждение:

для марковского шифра система уравнений

$$\begin{cases} h(k,x) = \mathsf{g} \\ h(k,x+\mathsf{a}) = \mathsf{g}+\mathsf{b}_1 \end{cases}$$

для любых $\mathsf{g}, \mathsf{b}_1$ однозначно определяет разность $\mathsf{a}$ .

$$\begin{aligned}
&P(\Delta Y(2) = \beta_2 | \Delta Y(1) = \beta_1, \Delta X = \alpha) \\
&= \sum_\gamma P(Y(1) = \gamma, \Delta Y(2) = \beta_2 | \Delta Y(1) = \beta_1, \Delta X = \alpha) \\
&= \sum_\gamma P(Y(1) = \gamma | \Delta Y(1) = \beta_1, \Delta X = \alpha) P(\Delta Y(2) = \beta_2 | \Delta Y(1) = \beta_1, Y(1) = \gamma, \Delta X = \alpha) \\
&= \sum_\gamma P(Y(1) = \gamma | \Delta Y(1) = \beta_1, \Delta X = \alpha) P(\Delta Y(2) = \beta_2 | \Delta Y(1) = \beta_1, Y(1) = \gamma) \\
&= \sum_\gamma P(Y(1) = \gamma | \Delta Y(1) = \beta_1, \Delta X = \alpha) P(\Delta Y(2) = \beta_2 | \Delta Y(1) = \beta_1) \\
&= P(\Delta Y(2) = \beta_2 | \Delta Y(1) = \beta_1),
\end{aligned}$$

where the third equality comes from the fact that $Y(1)$ and $\Delta Y(1)$ together determine both $Y(1)$ and $Y(1)^*$ so that $\Delta Y(2)$ has no further dependence on $\Delta X$ when $Y(1)$ and $\Delta Y(1)$ are specified. Because the same round function is used in each round, this Markov chain is homogeneous. For any key $Z = z$, the round function $f(\cdot, z)$ is a bijective mapping from the set of plaintexts to the set of ciphertexts. This bijection in-

# Контрпример

$G = (Z_4, +)$, $K = \{0,1,2,3\}$,

$h(k,x)$ определяется таблицей (ключ $k$ - номер строки, $x$ - номер столбца)

$$\begin{pmatrix} 3 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \\ 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

Раундовая функция удовлетворяет условию марковского шифра:

для $x \in \{0,1,2,3\}$ вероятности $P(h(k, x+a) - h(k,x) = b)$ имеют вид

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{3}{4} & 0 & \frac{1}{4} \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{4} & 0 & \frac{3}{4} \end{pmatrix}$$

Решения системы уравнений

$$\begin{cases} h(k,x) = g_1 \\ h(k,x+a) = g_2 \end{cases}$$

могут содержать различные значения для разности $a$ .

Например, при $g_1 = 0$, $g_2 = 1$ возникают следующие решения

$$\begin{aligned} a &= 3 \quad \{x_1 = 0, x_2 = 3, k = 3\} \\ a &= 3 \quad \{x_1 = 1, x_2 = 0, k = 2\} \\ a &= 1 \quad \{x_1 = 1, x_2 = 2, k = 1\} \\ a &= 3 \quad \{x_1 = 2, x_2 = 1, k = 0\} \end{aligned}$$

## Достаточные условия

Утверждение 1.

Если выполнены условия:

1. $P(h(k,x+a)-h(k,x)=b)$ не зависит от $x$ для всех $a,b \in G$,

(условие марковости раундовой функции);

2. для произвольного $x \in G$ случайная величина $h(k,x)$ равномерно распределена на $G$,

то разности $D_i$ связаны в цепь Маркова.

**Схема Фейстеля** на группе $(G,+)$

Последовательность $m$ раундовых преобразований

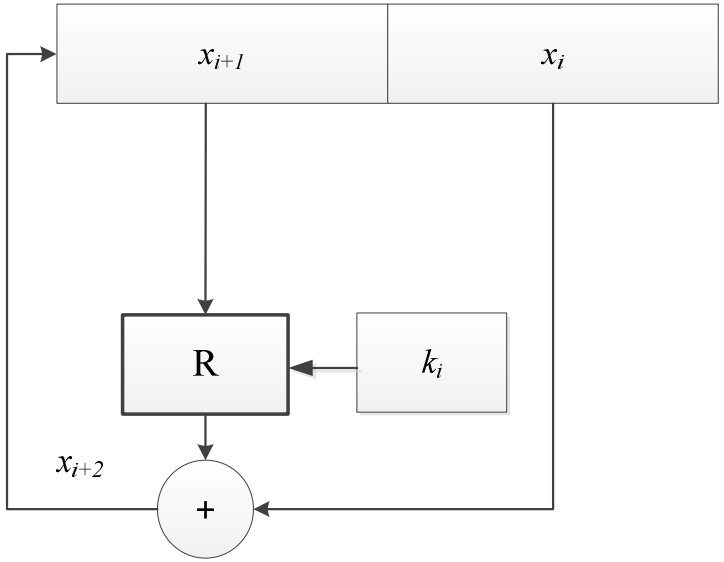
$$x_{i+2} = x_i + R(k_i, x_{i+1}),\ i = 0,1,...,m-1,$$

$R : K \times G \to G, x_i, x_{i+1}, x_{i+2} \in G,\ k_i \in K.$

Вход - вектор $(x_0, x_1) \in G^2$,

выход - вектор $(x_m, x_{m+1}) \in G^2$,

раундовые ключи - $k_0,...,k_{m-1}$.




Замечание: условие 2 утверждения 1 для схемы Фейстеля не выполнено, условие 1 выполнено.

Утверждение 2.

Если выполнены условия

1. $\mathrm{P}(R(k,x+\mathsf{a}) - R(k,x) = \mathsf{b})$ не зависит от $x$ для всех $\mathsf{a},\mathsf{b} \hat{\mathrm{I}} G$

(условие марковости для отображения $R$);

2. Для произвольного $x \hat{\mathrm{I}} G$ случайная величина $R(k,x)$ равномерно распределена на $G$

то разности $\mathsf{D}_i$ связаны в цепь Маркова.

Пары вида $(\mathsf{D}_i, \mathsf{D}_{i+1})$, $i = 0,1,\ldots$ также образуют цепь Маркова.

**Гипотеза о стохастической эквивалентности** для итеративных марковских шифров связывает вероятности $P(D_i = a_1 / D_0 = a_0)$ для фиксированных раундовых ключей $k_0,...,k_{i-1}$ и усреднённые значения $E_{k_0,...,k_{i-1}} P(D_i = a_1 / D_0 = a_0)$.

**Hypothesis of Stochastic Equivalence.** *For an (r-1)-round differential* $(\alpha, \beta)$,

$$P(\Delta Y(r-1) = \beta | \Delta X = \alpha) \approx P(\Delta Y(r-1) = \beta | \Delta X = \alpha, Z^{(1)} = \omega_1, ..., Z^{(r-1)} = \omega_{r-1})$$

*for almost all subkey values* $(\omega_1, ..., \omega_{r-1})$.

*Lai X, Massey J. L., Murphy S. Markov ciphers and differential cryptanalysis, 1991.*

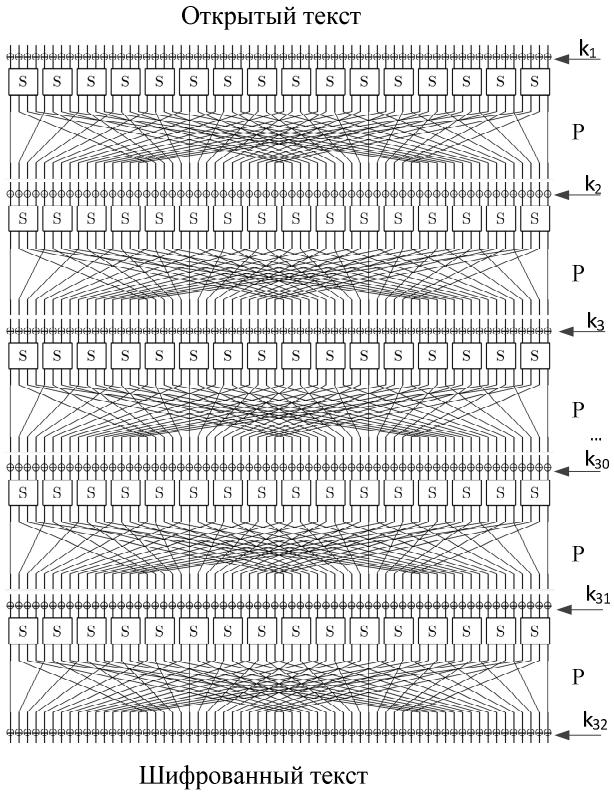
**Hypothesis of Stochastic Equivalence.** *For virtually all high probability* $(r-1)$*-round differentials* $(\alpha, \beta)$,

$$P(\Delta Y(r-1) = \beta | \Delta X = \alpha) \approx P(\Delta Y(r-1) = \beta | \Delta X = \alpha, Z^{(1)} = z_1, ..., Z^{(r-1)} = z_{r-1}) \qquad (4.2)$$

*holds for a substantial fraction of the subkey values* $(z_1, ..., z_{r-1})$.

Lai X. On the design and security of block ciphers. 1992.

Экспериментальная проверка гипотезы для редуцированного (6 раундов) алгоритма Present-80




Развёртка раундовых ключей $k_0,...,k_{31}$ из исходного ключа $K=(K_{79},...,K_0)$: 31 раз применяется композиция 3 преобразований:

1. $(K_{79},...,K_0)$ ® $(K_{18},K_{17}...,K_{19})$ (циклический сдвиг на 61 позицию влево);
2. $(K_{79},K_{78},K_{77},K_{76},K_{75},...,K_0)$ ® $(S[K_{79},K_{78},K_{77},K_{76}],K_{75},...,K_0)$;
3. $(K_{79},...,K_{19},K_{18},K_{17},K_{16},K_{15},...,K_0)$ ® ® $(K_{79},...,([K_{19},K_{18},K_{17},K_{16},K_{15}]$ Å $i),K_{14},...,K_0)$.

Раундовый ключ $k_i$ - 8 старших байтов ключа $K$: $k_i=(k_i^{63},...,k_i^{0})=(K_{79},...,K_{16})$.

Максимальные вероятности переходов разностей за 6 раундов:

$$p^{(6)}_{a_0,a_6} = E_{k_0,\ldots,k_6} P(D_6 = a_6 / D_0 = a_0).$$

| | $p^{(6)}_{a_0,a_6}$ | $a_0$ | $a_6$ |
|---|---|---|---|
| 1 | 1,191E-07 | 00000**4**0**4**00000000 | 0000000000001**0**0**1** |
| 2 | 1,191E-07 | 00000**4**0**4**0**4**0000 | 0000000000001**0**0**1** |
| 3 | 1,179E-07 | 00000**5**0000000**5**00 | 000**9**000000000009 |
| 4 | 1,179E-07 | 00000**5**0000000**5**00 | 000**D**00000000000**D** |
| 5 | 1,177E-07 | 00000**9**0000000**9**00 | 000**F**00000000000**F** |
| 6 | 1,067E-07 | 0**4**0**4**0**4**00000000 | 0000**1**00**1**00000000 |
| 7 | 1,06E-07 | 00000**3**0000000**3**00 | 000**7**000000000007 |
| 8 | 1,004E-07 | 0**4**0**4**0**4**00000000 | 00000000**1**00**1**0000 |
| 9 | 1,001E-07 | 00000**9**0000000**9**00 | 000**7**000000000007 |
| 10 | 9,425E-08 | 00000**4**0**4**0**4**000000 | 0000000000001**0**0**1** |

# Экспериментальная проверка.

## Расчёт вероятностей переходов разностей, $v = 10^{10}$ пар входов

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1,17E-07 | 1,14E-07 | 1,14E-07 | 1,23E-07 | 1,23E-07 | 1,16E-07 | 1,07E-07 | 9,46E-08 | 1,01E-07 | 9,87E-08 |
| 1,21E-07 | 1,29E-07 | 1,19E-07 | 1,26E-07 | **1,33E-07** | 1,02E-07 | 9,88E-08 | 1,04E-07 | 1,04E-07 | 9,33E-08 |
| 1,14E-07 | 1,24E-07 | 1,12E-07 | 1,28E-07 | 1,08E-07 | **1,20E-07** | 1,15E-07 | 9,71E-08 | 9,83E-08 | 9,37E-08 |
| 1,22E-07 | 1,22E-07 | 1,08E-07 | 1,18E-07 | **9,74E-08** | **1,20E-07** | 1,01E-07 | **8,47E-08** | 1,03E-07 | 1,00E-07 |
| 1,21E-07 | 1,17E-07 | 1,19E-07 | 1,22E-07 | 1,08E-07 | 9,89E-08 | 1,09E-07 | 9,18E-08 | 9,98E-08 | 9,38E-08 |
| 1,20E-07 | 1,18E-07 | 1,19E-07 | 1,13E-07 | **1,36E-07** | **9,18E-08** | **1,18E-07** | 9,52E-08 | 1,05E-07 | 9,04E-08 |
| 1,16E-07 | 1,28E-07 | 1,12E-07 | 1,14E-07 | **1,34E-07** | **1,17E-07** | 1,17E-07 | **8,94E-08** | 1,05E-07 | 9,72E-08 |
| 1,22E-07 | 1,25E-07 | 1,17E-07 | 1,13E-07 | **1,42E-07** | **1,17E-07** | 1,08E-07 | 9,84E-08 | 1,02E-07 | 9,06E-08 |
| 1,28E-07 | 1,18E-07 | 1,16E-07 | 1,18E-07 | **9,71E-08** | 1,13E-07 | 9,99E-08 | 9,94E-08 | 9,64E-08 | 1,01E-07 |
| 1,21E-07 | 1,22E-07 | 1,11E-07 | 1,14E-07 | 1,21E-07 | **1,39E-07** | 1,10E-07 | 9,36E-08 | 1,06E-07 | 9,22E-08 |

номер строки – номер ключа, жёлтым цветом выделены «выбросы за 3s ».

10 случайно выработанных ключей: 37AF54B83E4F6138880F, F5277A16BEFC90902935, 06ED8DD20CB47700EA40, B3537BC13619D34D647B, 28E6D7D95710B3638E5C, BE1D5EF408949C79D401, 4BF7F723F21E179455C0, 2E61DBE53DE3609A5F77, F6ED75E3434ED5D1D8F1, 0CB8501A89E3452DA404.