

## О ФОРМАЛИЗАЦИИ И СИСТЕМАТИЗАЦИИ ОСНОВНЫХ ПОНЯТИЙ РАЗНОСТНОГО АНАЛИЗА ИТЕРАТИВНЫХ БЛОЧНЫХ ШИФРОВ

*Пестунов Андрей Игоревич*

ИВТ СО РАН, НГУЭУ

# Структура доклада

**Часть 1.** Обзор некоторых проблем и несоответствий в существующей терминологии разностного анализа.

**Часть 2.** Один из вариантов формализации и систематизации этих понятий.

# Основные понятия разностного анализа

- Характеристика, дифференциал;
- Усечённые характеристики и дифференциалы;
- Объединение характеристик и дифференциалов;
- Вероятность характеристик и дифференциалов;
- Вероятность объединения характеристик и дифференциалов.

# Вопрос 1. Относится ли вероятность к дифференциалам и характеристикам?

Пусть далее  $C$  есть  $r$ -раундовый итеративный блочный шифр с функцией раундового шифрования  $g: U \times K \rightarrow U$  и с аддитивными раундовыми ключами  $k_1, \dots, k_r$  в  $K$ , где  $k_i$  – ключ  $i$ -го раунда,  $i = 1, \dots, r$ . Для любого натурального  $t \leq r$  последовательность  $\chi_t = (a_0', a_1', p_1, a_2', p_2, \dots, a_t', p_t)$ , где все  $a_0', a_1', \dots, a_t'$  принадлежат  $U$ , называется  $t$ -раундовой дифференциальной вероятностной характеристикой шифра  $C$ , если для любого  $i \geq 1$  в ней  $p_i = p_g(a_i' | a_{i-1}')$ , т.е. если  $a_{i-1}$  и  $a_{i-1}^*$  выбраны в  $U$  так, что  $a_{i-1} - a_{i-1}^* = a_{i-1}'$ , и вычислены  $a_i = g(a_{i-1}, k_i)$  и  $a_i^* = g(a_{i-1}^*, k_i)$ , то  $a_i - a_i^* = a_i'$  с вероятностью  $p_i$ . Произведение  $p = p_1 \dots p_t$  называется вероятностью характеристики  $\chi_t$ .

**Definition 7.** An  $n$ -round characteristic is a tuple  $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_T)$  where  $\Omega_P$  and  $\Omega_T$  are  $m$ -bit numbers and  $\Omega_\Lambda$  is a list of  $n$  elements  $\Omega_\Lambda = (\Lambda_1, \Lambda_2, \dots, \Lambda_n)$ , each of which is a pair of the form  $\Lambda_i = (\lambda_i^i, \lambda_i^0)$  where  $\lambda_i^i$  and  $\lambda_i^0$  are  $(m/2)$ -bit numbers and  $m$  is the block size of the cryptosystem. A characteristic satisfies the following requirements:

$\lambda_1^1 =$  the right half of  $\Omega_P$ ,

$\lambda_1^2 =$  the left half of  $\Omega_P \oplus \lambda_0^1$ ,

$\lambda_i^n =$  the right half of  $\Omega_T$ ,

$\lambda_i^{n-1} =$  the left half of  $\Omega_T \oplus \lambda_0^n$ ,

## Вопрос 2. Относятся ли дифференциалы и характеристики к шифрам?

**Definition.** An *i*-round differential is a couple  $(\alpha, \beta)$ , where  $\alpha$  is the difference of a pair of distinct plaintexts  $X$  and  $X^*$  and where  $\beta$  is a possible difference for the resulting *i*-th round outputs  $Y(i)$  and  $Y^*(i)$ . The probability of an *i*-round differential  $(\alpha, \beta)$  is the conditional probability that  $\beta$  is the difference  $\Delta Y(i)$  of the ciphertext pair after *i* rounds given that the plaintext pair  $(X, X^*)$  has difference  $\Delta X = \alpha$  when the plaintext  $X$  and the subkeys  $Z^{(1)}, \dots, Z^{(i)}$  are independent and uniformly random. We denote this differential probability by  $P(\Delta Y(i) = \beta | \Delta X = \alpha)$ .

# Вопрос 3. Является ли объединение дифференциалов характеристикой?

use  $r_A$  to denote an A-round and  $r_B$  to denote a B-round. One useful truncated differential characteristic allows us to cover the first 16 rounds of Skipjack:

$$(a, b, 0, c) \xrightarrow{8r_A} (e, e, 0, 0) \xrightarrow{8r_B} (g, h, f, 0), \quad (1)$$

It is possible to add another four A-rounds to the latter differential while retaining the fact that the truncated differential holds with probability one. Thus, one gets the following twelve-round truncated differential with probability one

$$(0, a, 0, 0) \xrightarrow{8r_B} (0, b, c, d) \xrightarrow{4r_A} (h, h, f, g). \quad (2)$$

# Вопрос 4. Можно ли объединять дифференциал с характеристикой?

**Definition 9.** The *concatenation* of an  $n$ -round characteristic  $\Omega^1 = (\Omega_P^1, \Omega_\Lambda^1, \Omega_T^1)$  with an  $m$ -round characteristic  $\Omega^2 = (\Omega_P^2, \Omega_\Lambda^2, \Omega_T^2)$ , where  $\Omega_T^1$  equals the swapped value of the halves of  $\Omega_P^2$ , is the characteristic  $\Omega = (\Omega_P^1, \Omega_\Lambda, \Omega_T^2)$ , where  $\Omega_\Lambda$  is the concatenation of the lists  $\Omega_\Lambda^1$  and  $\Omega_\Lambda^2$ .

# Вопрос 5. Многие определения даются нестрого

Differential cryptanalysis, developed by Biham and Shamir [1], is a chosen-plaintext attack that exploits the correlation between the input and output differences of a pair of plaintext blocks encrypted under the same key. The first step in a differential attack is to find a *characteristic* of the cipher attacked. A characteristic is a sequence of differences between the round inputs in the encryption of two plaintext blocks with a given initial difference. For a characteristic to be useful in an attack, a plaintext pair with the given initial difference must have a non-trivial probability to follow the given sequence of differences during encryption. Having obtained such a characteristic, the attacker collects

## Вопрос 6. Как вычислять вероятность объединения усечённых характеристик и дифференциалов?

For a Markov cipher with independent and uniformly random round subkeys, the probability of an  $r$ -round characteristic is given by the Chapman-Kolmogorov equation for a Markov chain as

$$P(\Delta Y(1) = \beta_1, \Delta Y(2) = \beta_2, \dots, \Delta Y(r) = \beta_r | \Delta X = \beta_0) = \prod_{i=1}^r P(\Delta Y(i) = \beta_i | \Delta X = \beta_{i-1}).$$

# Вопрос 7. Является ли дифференциал характеристикой?

**Remark.** In [1], differential cryptanalysis of DES was described in terms of “i-round characteristics”. In our notation, an i-round characteristic as defined in [1] is an  $(i + 1)$ -tuple  $(\alpha, \beta_1, \dots, \beta_i)$  considered as a possible value of  $(\Delta X, \Delta Y(1), \dots, \Delta Y(i))$ . Thus, a one-round characteristic coincides with a one-round differential and an i-round characteristic determines a sequence of i differentials,  $(\Delta X, \Delta Y(j)) = (\alpha, \beta_j)$ . The probability of an i-round characteristic is defined in [1] as

$$P(\Delta Y(1) = \beta_1, \Delta Y(2) = \beta_2, \dots, \Delta Y(i) = \beta_i | \Delta X = \alpha)$$

# Усеченная характеристика

**Определение 1.** Пусть  $I = \{r_0, \dots, r_T\} \subseteq \{0, 1, \dots, R\}$ , где  $T \leq R$ , причём  $r_0 = 0$  и  $r_T = R$ . Пусть также  $\Delta = (\delta^{r_0}, \dots, \delta^{r_T})$  и  $M = (m^{r_0}, \dots, m^{r_T})$  — упорядоченные множества, где  $\delta^r \in \{0, 1\}^s$ ,  $m^r \in \{0, 1\}^s$ ,  $m^r \neq 0$  и  $r \in I$ . Тогда упорядоченная тройка  $(I, \Delta, M)$  называется  $R$ -раундовой усечённой характеристикой. Обозначим её

$$(\delta^{r_0}, m^{r_0}) \xrightarrow{r_1 - r_0 \text{ раундов}} (\delta^{r_1}, m^{r_1}) \xrightarrow{r_2 - r_1 \text{ раундов}} \dots \xrightarrow{r_T - r_{T-1} \text{ раундов}} (\delta^{r_T}, m^{r_T}).$$

**Пример 1.** Проиллюстрируем введённое определение на примере следующей усечённой характеристики:

$$(a, b, ?, c) \xrightarrow{8 \text{ round}} (e, e, ?, ?) \xrightarrow{8 \text{ round}} (g, h, f, ?).$$

Данная характеристика согласуется с определением при следующих параметрах:

$$T = 2, I = \{0, 8, 16\},$$

$$\Delta = ((a, b, 0, c), (e, e, 0, 0), (g, h, f, 0)),$$

$$M = ((1^{64}, 0^{32}, 1^{32}), (1^{64}, 0^{64}), (1^{96}, 0^{32})).$$

# Вероятность усеченной характеристики

**Определение 2.** Пусть  $E$  —  $R$ -раундовый блочный шифр с блоком размера  $s$ ,  $(I, \Delta, M)$  —  $R$ -раундовая усечённая характеристика и  $p \in [0, 1]$ . Будем говорить, что шифр  $E$  допускает (имеет) усечённую характеристику  $(I, \Delta, M)$  с вероятностью  $p$ , если при случайно и независимо выбранных ключах раундов и блоках открытого текста  $C^0$  и  $D^0$  выполняется равенство

$$\begin{aligned} P((C^{r_1} \oplus D^{r_1}) \& m^{r_1} = \delta^{r_1} \& m^{r_1}, \dots, (C^{r_T} \oplus D^{r_T}) \& m^{r_T} = \\ = \delta^{r_T} \& m^{r_T} | (C^{r_0} \oplus D^{r_0}) \& m^{r_0} = \delta^{r_0} \& m^{r_0}) = p. \end{aligned}$$

# Объединение характеристик

**Определение 3.** Характеристика  $(\widehat{I}, \widehat{\Delta}, \widehat{M})$  присоединима к  $\widetilde{R}$ -раундовой характеристике  $(\widetilde{I}, \widetilde{\Delta}, \widetilde{M})$ , если выполняются равенства  $\widetilde{m}^{\widetilde{R}} = \widehat{m}^0$  и  $\delta^{\widetilde{R}} \& m^{\widetilde{R}} = \widehat{\delta}^0 \& \widehat{m}^0$ .

**Определение 4.** Пусть  $H_1 = (\widetilde{I}, \widetilde{\Delta}, \widetilde{M})$  и  $H_2 = (\widehat{I}, \widehat{\Delta}, \widehat{M})$  — соответственно  $\widetilde{R}$ - и  $\widehat{R}$ -раундовые усечённые характеристики, причём  $H_2$  присоединима к  $H_1$ , тогда объединением  $H_1$  и  $H_2$  назовём характеристику  $H = (I, \Delta, M)$ , где  $I = \{0 = \widetilde{r}_0, \dots, \widetilde{r}_{\widetilde{T}} = \widetilde{R} + \widehat{r}_0, \widetilde{R} + \widehat{r}_1, \dots, \widetilde{R} + \widehat{r}_{\widehat{T}} = \widetilde{R} + \widehat{R}\}$ ,  $\Delta = (\widetilde{\delta}^{\widetilde{r}_0}, \dots, \widetilde{\delta}^{\widetilde{r}_{\widetilde{T}}}, \widehat{\delta}^{\widehat{r}_1}, \dots, \widehat{\delta}^{\widehat{r}_{\widehat{T}}})$  и  $M = (\widetilde{m}^{\widetilde{r}_0}, \dots, \widetilde{m}^{\widetilde{r}_{\widetilde{T}}}, \widehat{m}^{\widehat{r}_1}, \dots, \widehat{m}^{\widehat{r}_{\widehat{T}}})$ . По аналогии с операцией конкатенации будем использовать обозначение  $H = H_1|H_2$ .

**Определение 5.** Пусть дана последовательность усечённых характеристик  $H_1, \dots, H_L$ , для которых выполняется следующее свойство:  $H_{l+1}$  может быть присоединена к  $H_l$ ,  $l = 1, \dots, L - 1$ . Тогда объединением  $L$  характеристик  $H_1, H_2, \dots, H_L$  называется характеристика  $H = (\dots((H_1|H_2)|H_3)|\dots)|H_L$ . Легко видеть, что определённая таким образом операция объединения ассоциативна, поэтому можно использовать запись  $H = H_1|H_2|H_3|\dots|H_L$ .

# Вероятность объединения характеристик

**Утверждение 1.** Пусть марковский шифр  $E$  представим в виде композиции  $E = E^1 \circ \dots \circ E^L$ , где  $E_l$ ,  $l = 1, \dots, L$ , могут быть раундами или композицией раундов. Пусть также  $E_l$  допускает некоторую характеристику  $H_l$  с вероятностью  $p_l$ . Тогда шифр  $E$  допускает характеристику  $H = H_1 | \dots | H_L$  с вероятностью  $p_1 \cdot \dots \cdot p_L$ .

Из этого утверждения следует очевидная справедливость общепринятого обозначения для характеристик, состоящих из нескольких дифференциалов:

$$\begin{array}{ccccccccccc} \Delta_0 & \xrightarrow{p_1} & \Delta_1 & \xrightarrow{p_2} & \Delta_2 & \xrightarrow{p_3} & \dots & \xrightarrow{p_{L-1}} & \Delta_{L-1} & \xrightarrow{p_L} & \Delta_L; \\ & & \Delta_{\text{in}} & \xrightarrow[p]{\tilde{R} \text{ раундов}} & \Delta_{\text{mid}} & \xrightarrow[q]{\hat{R} \text{ раундов}} & & & \Delta_{\text{out}} & & \end{array}$$

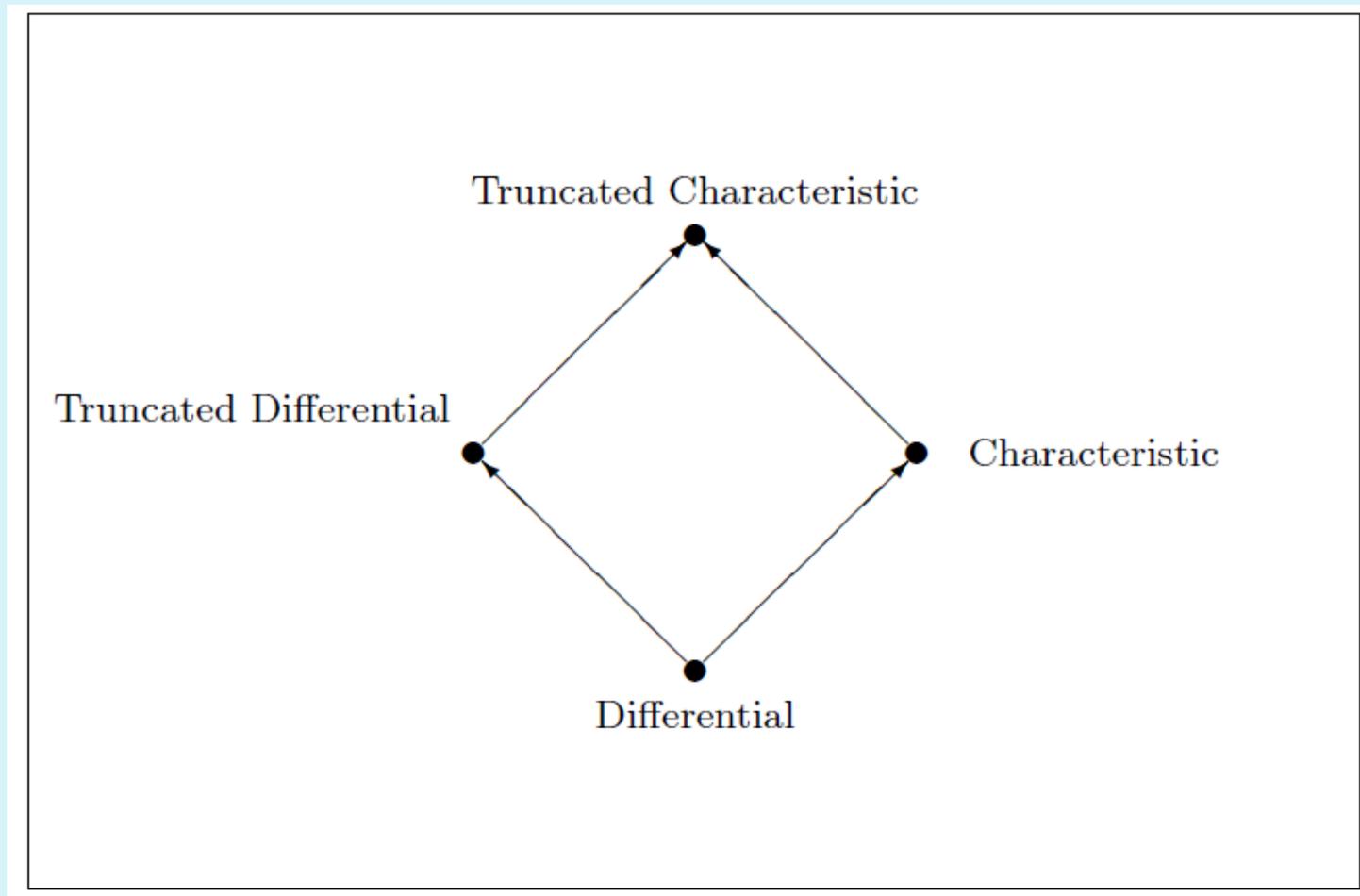
# Неусеченные характеристики и дифференциалы

**Определение 6.** Усечённую характеристику  $(I, \Delta, M)$  назовём *неусечённой характеристикой* или (сокращённо) *характеристикой*, если  $M = (1^s, \dots, 1^s)$ .

**Определение 7.** Усечённую характеристику  $(I, \Delta, M)$  назовём *усечённым дифференциалом*, если  $I = \{0, R\}$ .

**Определение 8.** Усечённую характеристику  $(I, \Delta, M)$  назовём *неусечённым дифференциалом* или (сокращённо) *дифференциалом*, если  $I = \{0, R\}$  и  $M = (1^s, 1^s)$

# Систематизация понятий



# Выводы

- Существующие понятия в разностном анализе слабо формализованы.
- Отсутствует их систематизация.
- Предложена формализация этих понятий на основе двоичных масок.
- Показано, что усеченная характеристика – это наиболее общее понятие, а неусеченные характеристики и дифференциалы являются усеченными характеристиками при определенных условиях.