конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто’2022»

Построение множества невозможных разностей алгоритмов шифрования Фейстеля с небиективной функцией усложнения для произвольного числа раундов

Захаров Дмитрий,
студент, НИЯУ МИФИ

Научный руководитель:
Пудовкина Марина Александровна, д.ф-м.н., профессор, НИЯУ МИФИ

Актуальность

- Метод невозможных разностей успешно применен при анализе многих блочных симметричных алгоритмов шифрования (AES, Present, Skipjack, Camellia)
- Основная задача при анализе методом невозможных разностей — поиск невозможных разностей для наибольшего числа раундов шифрования
- Многие используемые на практике алгоритмы шифрования являются алгоритмами шифрования Фейстеля (KASUMI, Blowfish)

Метод невозможных разностей

- Одна из разновидностей метода разностного анализа
- Предложен Ларсом Кнудсеном в 1998 году в процессе анализа алгоритма шифрования DEAL
- Обобщен Эли Бихамом, Алексом Бирюковым и Ади Шамиром в работе по анализу алгоритма шифрования Skipjack
- Атака с выбранным открытым текстом
- Невозможные разности используется для отсеивания ложных ключей

Невозможная разность

Определение 1. Для l −раундовой функции зашифрования $f^{(l)}: \{0,1\}^n \times K \to \{0,1\}^n$ $(\varepsilon, \delta) \in \{0,1\}^n \times \{0,1\}^n$ называется l −раундовой невозможной разностью (относительно операции $+$ покоординатного сложения n – мерных векторов по модулю 2), если для всех $(\alpha, k) \in \{0,1\}^n \times K$:

$$f_k^{(l)}(\alpha + \varepsilon) \neq f_k^{(l)}(\alpha) + \delta,$$

где $f_k^{(l)}(\beta) = f^{(l)}(\beta, k)$ для каждого $(\beta, k) \in \{0,1\}^n \times K$.

Метод рассогласования посередине (miss in the middle): $(\varepsilon, \delta) \in \{0,1\}^n \times \{0,1\}^n$ — $(m + d)$ −раундовая невозможная разность, если для всех $(\alpha, \gamma, k) \in \{0,1\}^n \times \{0,1\}^n \times K$:

$$f_k^{(m)}(\alpha + \varepsilon) + f_k^{(m)}(\alpha) \neq f_k^{(d)^{-1}}(\gamma + \delta) + f_k^{(d)^{-1}}(\gamma).$$

Семейство сбалансированных алгоритмов шифрования Фейстеля с небиективной функцией усложнения

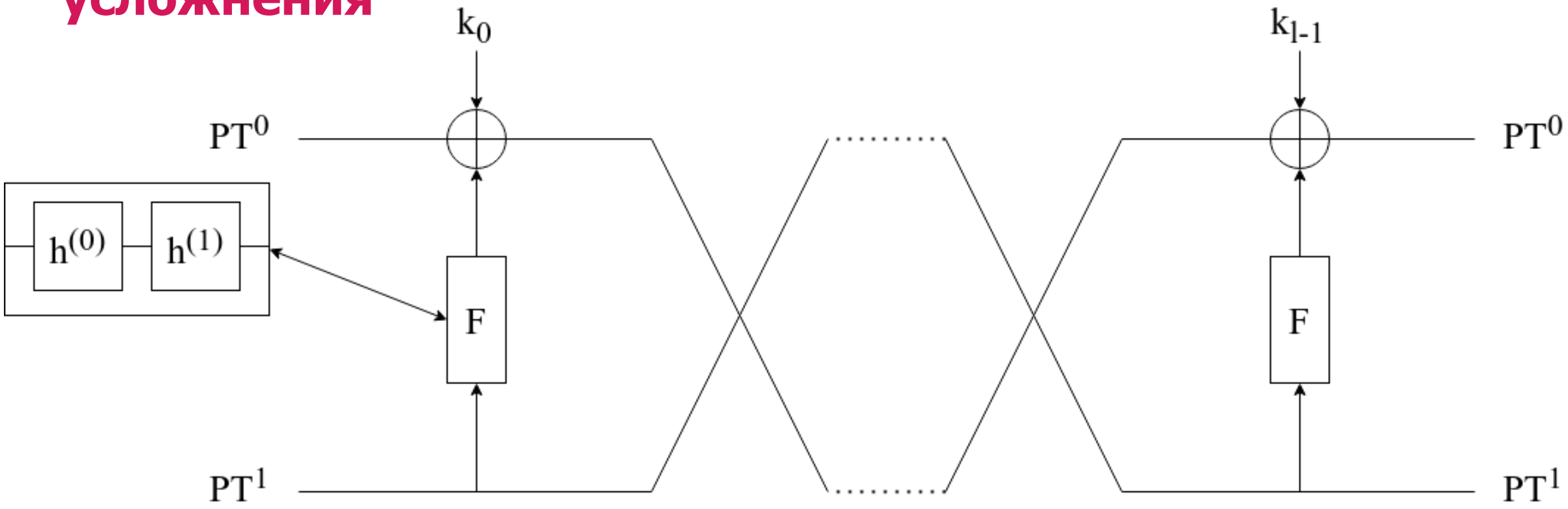
Пусть $m \in \mathbb{N}, m \geq 2$, $V_m - m$ – мерное векторное пространство над полем $GF(2)$ с «естественной» операцией $+$ сложения векторов.
$A -$ матрица $(m \times m)$ над $GF(2)$, $rank(A) = m - 1$. Зафиксируем отображения $f: V_m \to V_m$, $h^{(0)}: V_m \to V_m$, $h^{(1)}: V_m \to V_m$:

$$f: \alpha \longmapsto h^{(1)}(h^{(0)}(\alpha))$$
$$h^{(1)}: \alpha \longmapsto \alpha A$$

для каждого $\alpha \in V_m$.
Рассмотрим $\nu: V_m^2 \times V_m \to V_m^2$ с частичной функцией $\nu_k \in S(V_m^2)$, где

$$\nu_k: \big((\alpha_1, \alpha_0), k\big) \longmapsto (\alpha_0 + f(\alpha_1) + k, \alpha_1),$$
$$(\alpha_0, \alpha_1, k) \in V_m^3.$$

Семейство сбалансированных алгоритмов шифрования Фейстеля с небиективной функцией усложнения



$$k_i, PT^0, PT^1 \in \{0,1\}^m, i = \overline{0, l-1};$$

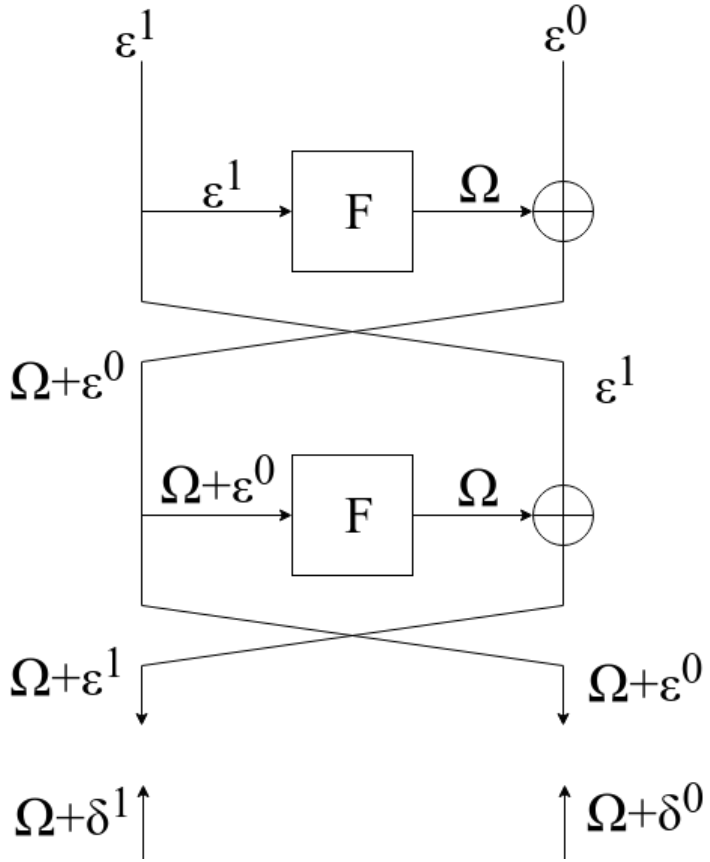
Теорема о невозможных разностях

Определение 2. $(\varepsilon, \delta) \in \{0,1\}^n \times \{0,1\}^n$ — невозможная нетривиальная разностью, если $\varepsilon \neq \bar{0}$ и $\delta \neq \bar{0}$.

Теорема 1. Пусть l-раундовый алгоритм шифрования принадлежит описанному выше семейству, тогда для каждого натурального $l > 3$ для данного алгоритма шифрования существует не менее $3 \times 2^{2n-2} - 2^{n+1}$ невозможных нетривиальных разностей.

- Полученный результат не зависит от биективной части функции усложнения, в том числе S-блока.
- Полученный результат не зависит от алгоритма развертывания ключа.
- Для матриц A: $rank(A) < m - 1$ можно построить еще больше невозможных разностей.

Основная идея доказательства

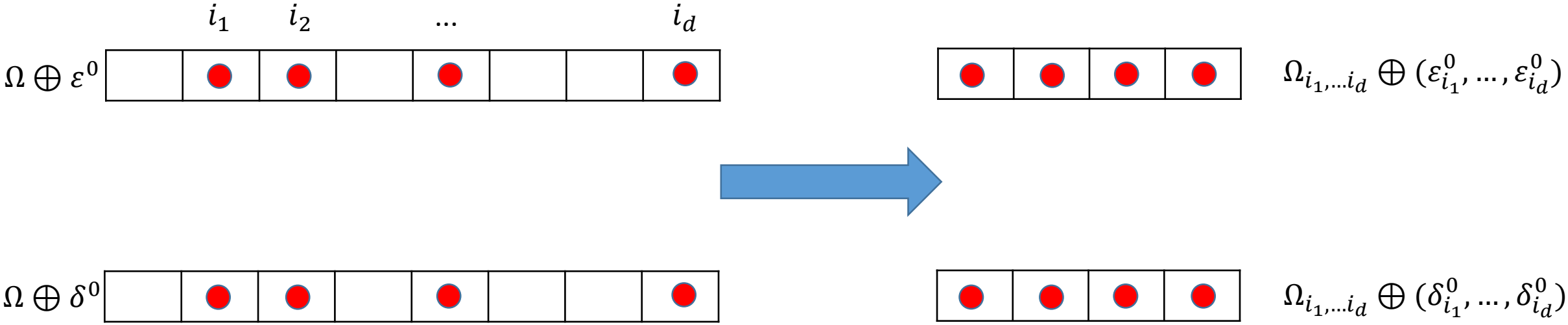


$$\varepsilon^0, \varepsilon^1, \delta^0, \delta^1 \in \{0,1\}^m;$$
$$\varepsilon = \varepsilon^1 || \varepsilon^0, \delta = \delta^1 || \delta^0;$$
$$\Omega = \{\omega : \omega = F(\epsilon), \forall \epsilon \in \{0,1\}^m\};$$

$$\forall \omega \in \Omega \exists (i_1, \dots, i_d): \sum_{j=1}^{d} \omega_{i_j} = 0, \text{т. к.} rank(A) = m - 1;$$
$$1 < d < m + 1$$

$$\left\| (\omega_{i_1}, \dots, \omega_{i_d}) \right\| \equiv 0 \ mod\ 2, \forall \omega \in \Omega.$$

Основная идея доказательства



$$\Omega_{i_1,\dots,i_d} = \{(\omega_{i_1}, \dots, \omega_{i_d}) : \forall \omega \in \Omega\};$$

$$\|(\omega_{i_1}, \dots, \omega_{i_d})\| \equiv 0 \ mod\ 2, \forall \omega \in \Omega, \text{следовательно}$$

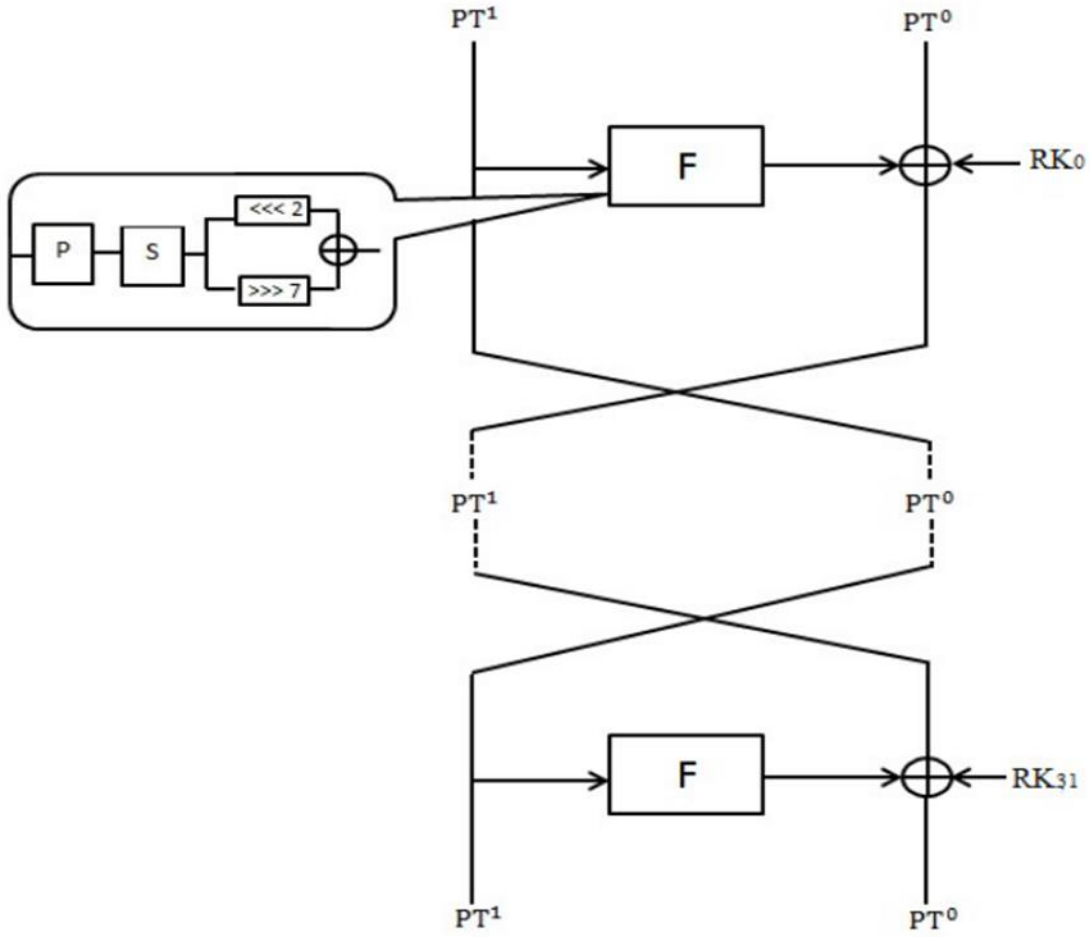
$$\|\mu\| \equiv \|(\varepsilon^0_{i_1}, \dots, \varepsilon^0_{i_d})\| mod\ 2, \forall \mu \in \Omega_{i_1,\dots i_d} \oplus (\varepsilon^0_{i_1}, \dots, \varepsilon^0_{i_d});$$

$$\|\nu\| \equiv \|(\delta^0_{i_1}, \dots, \delta^0_{i_d})\| mod\ 2, \forall \nu \in \Omega_{i_1,\dots i_d} \oplus (\delta^0_{i_1}, \dots, \delta^0_{i_d});$$

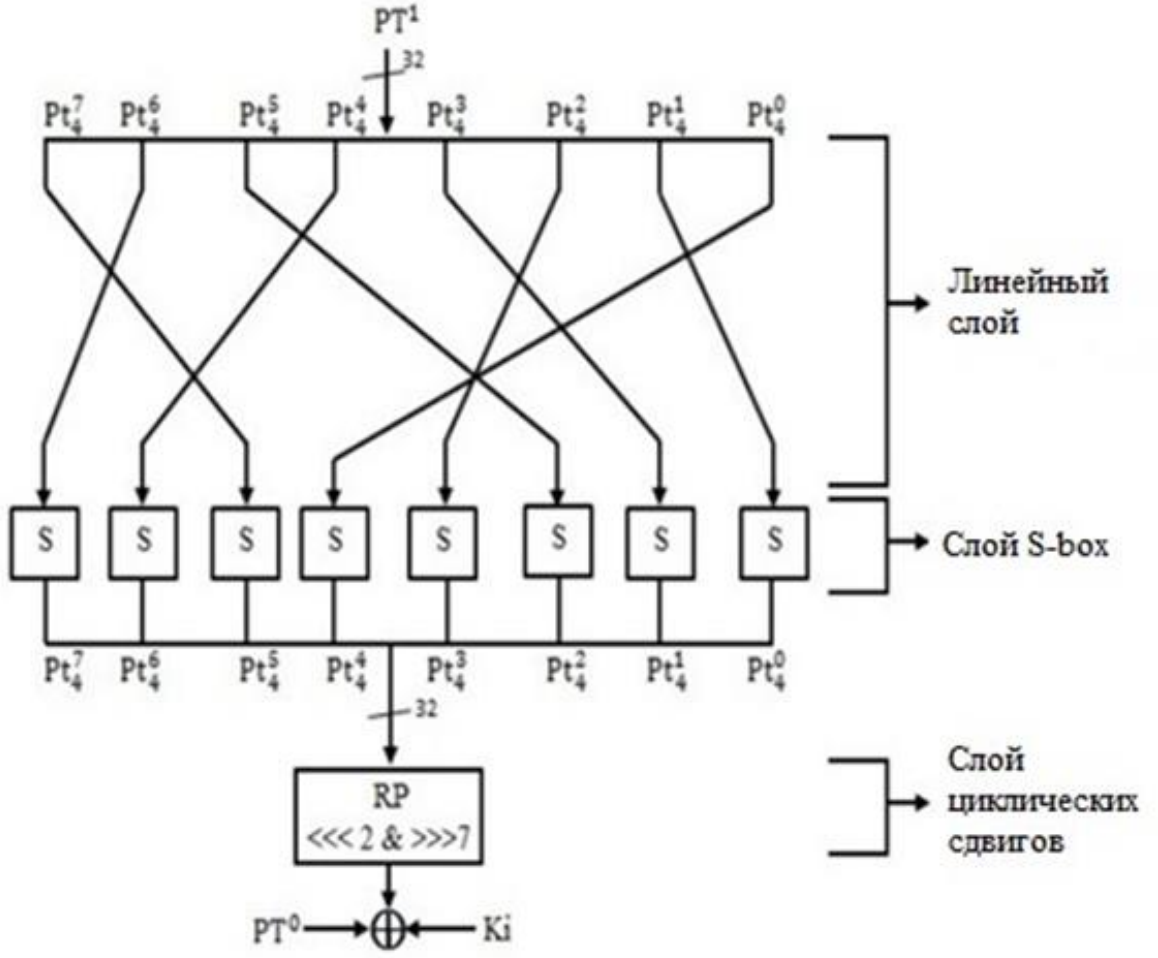
Если $\|(\varepsilon^0_{i_1}, \dots, \varepsilon^0_{i_d})\| \not\equiv \|(\delta^0_{i_1}, \dots, \delta^0_{i_d})\| mod\ 2$, то (ε, δ) — невозможная разность.

Алгоритм шифрования GRANULE

- GRANULE основан на сбалансированной сети Фейстеля с 32 раундами шифрования;
- Длина блока открытого текста — 64 бит;
- Длина секретного ключа — 80 или 128 бит;
- Предназначен для внедрения в сфере «Интернета вещей»



Функция усложнения GRANULE



$$S : \{0,1\}^4 \rightarrow \{0,1\}^4$$

S	--00	--01	--10	--11
00--	1110	0111	1000	0100
01--	0001	1001	0010	1111
10--	0101	1010	1011	0000
11--	0110	1100	1101	0011

Слой циклических сдвигов GRANULE

- Отображает множество 32-битных векторов в множество четных 32-битных векторов, т.е. преобразование необратимо.

$$RP: \{0,1\}^{32} \to \{0,1\}^{32},$$
$$Temp0 \leftarrow IN \lll 2,$$
$$Temp1 \leftarrow IN \ggg 7,$$
$$OUT \leftarrow Temp0 \oplus Temp1.$$

Сравнение полученных результатов

Метод анализа	Число раундов различителя	Число различителей	Число раундов атаки	Источник
Разностный	7	-	-	[1]
Линейный	6	-	-	[1]
Невозможные разности	5	9	11	[2]
Невозможные разности	7	144	-	[3]
Интегральный	10	-	12	[4]
Невозможные разности	32	$3 \times 2^{126} - 2^{65}$	32	Данная работа

Вопросы

???

Контактная информация

Электронная почта:

zakhar343@yandex.ru

Телефон:

+7 926 689-81-37

Facebook:

facebook.com/company

Сайт:

www.company.ru

Список использованных источников

1. **GRANULE: An Ultra lightweight cipher design for embedded security** [Электронный ресурс] — Режим доступа: https://eprint.iacr.org/2018/600— свободный

2. **Shuying, SHI.** Impossible Differential Cryptanalysis of GRANULE Algorithm [Текст] / SHI Shuying, HE Jun // Computer Engineering, 45(10) — 2019 — с. 134-138

3. **Wu, X.** Analysis of impossible differential distinguisher for GRANULE and MANTRA ciphers / X. Wu, Y. Li, Y. Wei, Y. Sun, // Journal on Communications, LNCS, 41 — 2020 — с. 94–101

4. **Li, Jun.** Integral analysis of GRANULE and ESF block ciphers based on MILP / Jun Li, Hongyan Wang, Xueying Qiu, Lingchen Li, Xiaonian Wu // 2021 12th International Conference on Information and Communication Systems (ICICS) — 2021 — с. 10–16

Алгоритм зашифрования разностей