

Новое семейство алгоритмов блочного шифрования «Рамен-К»

Дмух А.А.*, Пасько Д.О.*, Пешков Д.К.**

*Лаборатория математических проблем теоретической криптографии
Академии криптографии Российской Федерации, Москва, Россия

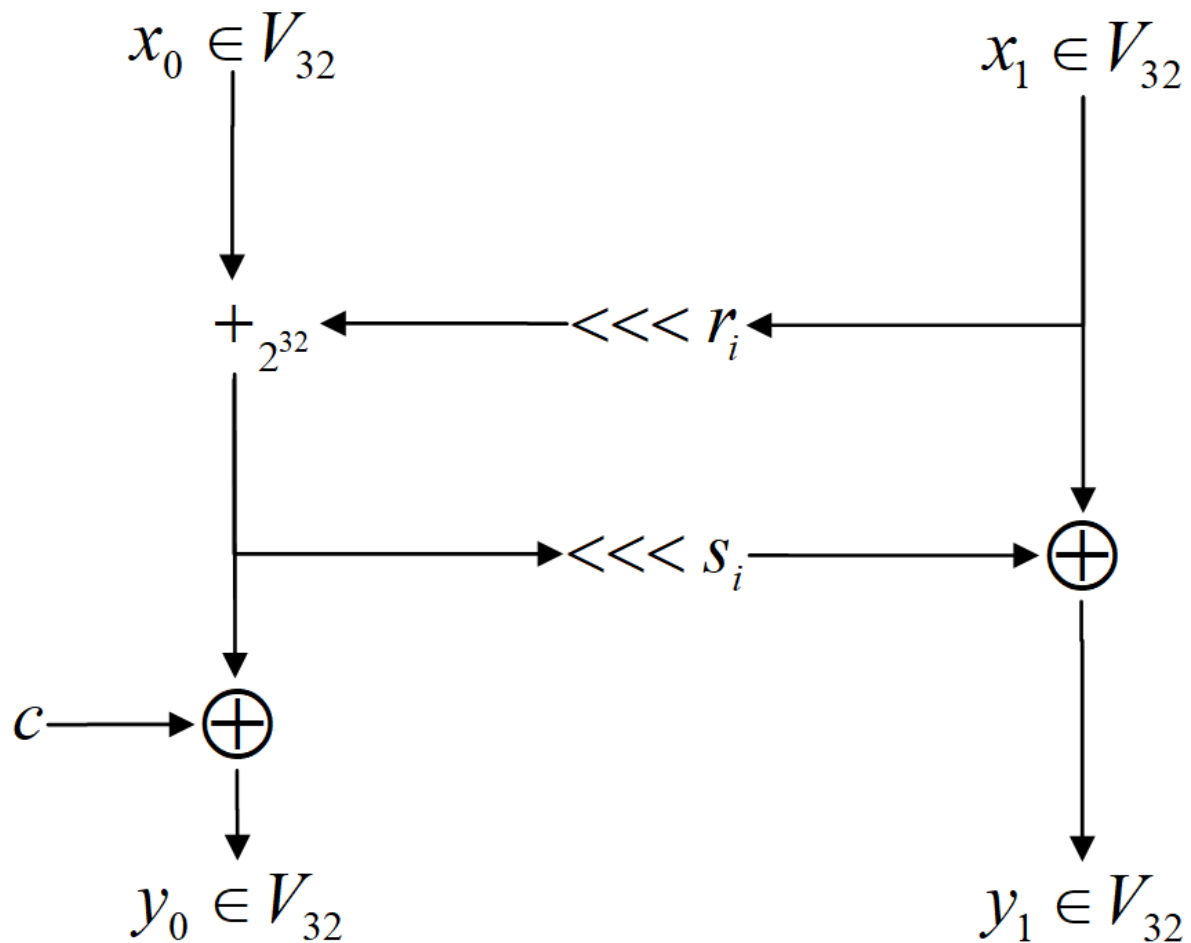
**Технический комитет по стандартизации ТК-26, Москва, Россия

Семейство алгоритмов «Рамен-К»

- ▶ Семейство «Рамен-К» состоит из трёх алгоритмов: «Рамен-128К», «Рамен-192К», «Рамен-256К».
- ▶ Алгоритм «Рамен- n К» имеет длину блока n битов и длину ключа $2n$ битов, $n \in \{128, 192, 256\}$.
- ▶ Предпочтительны для реализации на программно-аппаратных платформах, оперирующих 32- и 64-битовыми словами.
- ▶ Раундовое преобразование алгоритма «Рамен- n К» имеет структуру XSL с $n/64$ S-блоками. В качестве S-блока используется 64-битная ARX-подстановка «Альзет-К», основанная на подстановке «Альзет»*.

* Beierle C., Biryukov A., Cardoso dos Santos L. et al. Alzette: A 64-bit ARX-box (feat CRAX and TRAX) // Cryptology ePrint Archive. 2019. URL: <https://eprint.iacr.org/2019/1378>.

i -й шаг подстановки типа «Альзет»



- ▶ В подстановке «Альзет-К» 5 шагов (на 1 больше, чем в исходной подстановке «Альзет»).
- ▶ Значения $c, (r_1, \dots, r_5), (s_1, \dots, s_5)$ выбраны заново независимо от исходной подстановки.

Алгоритм «Рамен-128К»

- ▶ Длина блока – 128 битов, длина ключа – 256 битов, 13 раундов (12 полных + «отбеливание»).
- ▶ Два S-блока на раунде.
- ▶ Матрица линейного преобразования* представляется в виде

$$L_{128} = \begin{pmatrix} E & M \\ E & E \end{pmatrix} \cdot \begin{pmatrix} T_4 & 0 \\ 0 & T_{12} \end{pmatrix},$$

где $T_l, l \in \{4,12\}$ – матрицы циклического сдвига влево на l битов,

$$M = T_1 + \begin{pmatrix} 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

$\uparrow$
63

$\uparrow$
42

$\uparrow$
0

$\leftarrow 63$

$\leftarrow 42$

$\leftarrow 0$

* Здесь и далее линейные преобразования задаются умножением входного вектора-строки на матрицу.

Алгоритм «Рамен-192К»

- ▶ Длина блока – 192 бита, длина ключа – 384 бита, 15 раундов (14 полных + «отбеливание»).
- ▶ Три S-блока на раунде.
- ▶ Матрица линейного преобразования представляется в виде

$$L_{192} = \begin{pmatrix} S_1 & E & E \\ E & S_2 & E \\ E & E & S_3 \end{pmatrix} \cdot \begin{pmatrix} T_4 & 0 & 0 \\ 0 & E & 0 \\ 0 & 0 & T_{13} \end{pmatrix},$$

где T_l , $l \in \{4,13\}$ – матрицы циклического сдвига влево на l битов,

$$S_i = T_1 + \begin{pmatrix} 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix} \begin{matrix} \leftarrow 63 \\ \\ \\ \leftarrow k_i \\ \\ \leftarrow 0 \end{matrix}$$

$$(k_1, k_2, k_3) = (26, 14, 34).$$

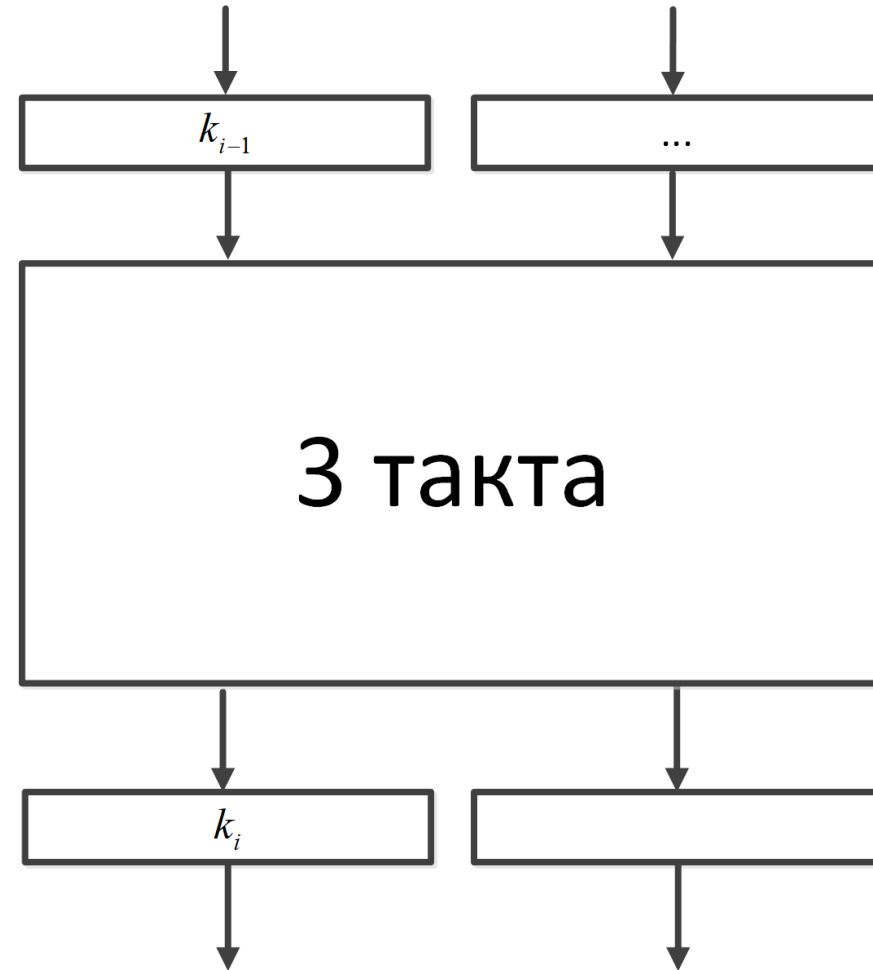
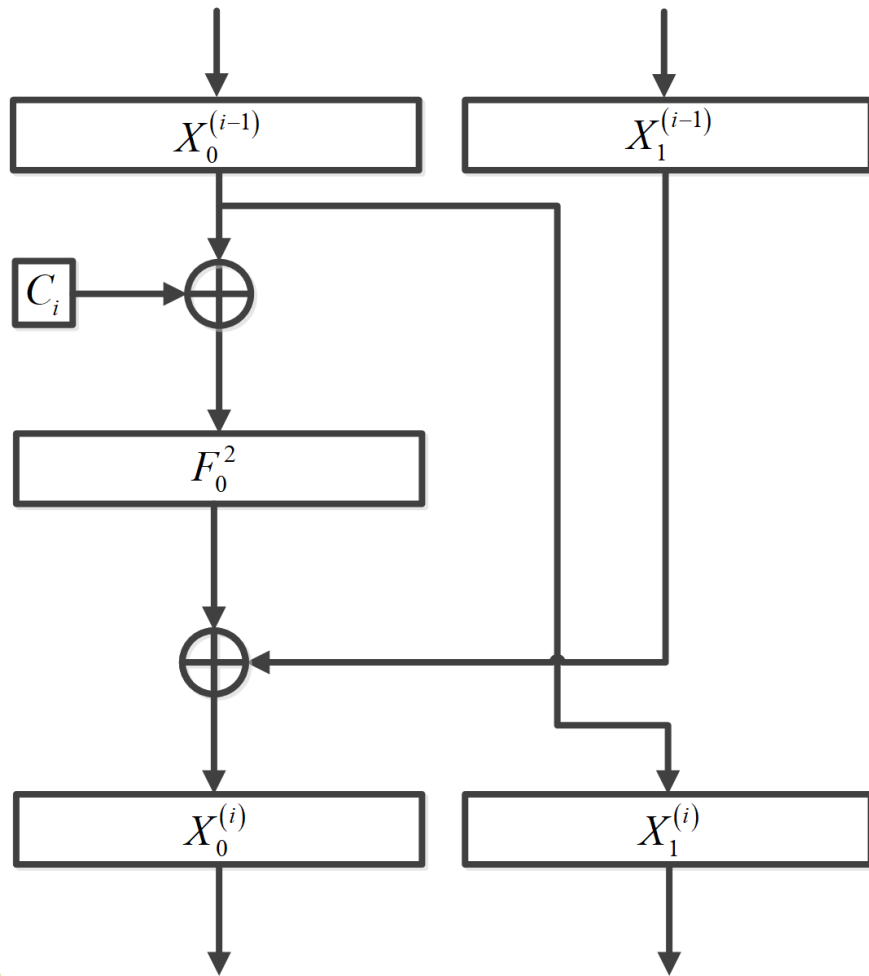
Алгоритм «Рамен-256К»

- ▶ Длина блока – 256 битов, длина ключа – 512 битов, 19 раундов (18 полных + «отбеливание»).
- ▶ Четыре S-блока на раунде.
- ▶ Матрица линейного преобразования представляется в виде

$$L_{256} = \begin{pmatrix} E & M & 0 & 0 \\ 0 & 0 & E & M \\ E & E & 0 & 0 \\ 0 & 0 & E & E \end{pmatrix} \cdot \begin{pmatrix} T_{14} & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & E \end{pmatrix},$$

где матрица M – такая же, как в «Рамен-128К», T_{14} – матрица циклического сдвига влево на 14 битов.

Алгоритмы развёртывания ключа



Алгоритмы развёртывания ключа

Константы C_i формируются следующим образом:

- ▶ для «Рамен-128К»

$$C_i = B_{128}^{i-1}(c_0^{(128)}, c_1^{(128)}), \text{ где}$$

$$B_{128}(x, y) = (y \oplus (x \ll 31), x);$$

- ▶ для «Рамен-192К»

$$C_i = B_{192}^{i-1}(c_0^{(192)}, c_1^{(192)}, c_2^{(192)}), \text{ где}$$

$$B_{192}(x, y, z) = (y \oplus (x \ll 53), z \oplus (x \ll 53), x);$$

- ▶ для «Рамен-256К»

$$C_i = B_{256}^{i-1}(c_0^{(256)}, c_1^{(256)}, c_2^{(256)}, c_3^{(256)}), \text{ где}$$

$$B_{256}(x, y, z, w) = (y \oplus (x \ll 7), z \oplus (x \ll 7), w \oplus (x \ll 7), x).$$

Начальные значения $c_0^{(n)}, \dots, c_{j(n)}^{(n)}, j(n) \in \{1, 2, 3\}, n \in \{128, 192, 256\}$ зафиксированы.

Режимы работы

- ▶ В соответствии с ГОСТ Р 34.13-2015: простая замена, гаммирование, гаммирование с обратной связью (по выходу, по шифртексту), простая замена с зацеплением, выработка имитовставки.
- ▶ Алгоритм «Рамен-128К» допускается к применению в режиме аутентифицированного шифрования с ассоциированными данными (AEAD) и режиме гаммирования с преобразованием ключа (CTR АСРКМ) в соответствии с Изменением №1 ГОСТ 34.13-2018.

Свойства подстановки «Альзет-К»

Характеристика подстановки π	Альзет-К	Альзет-5
$\tilde{p}^\pi$	2^{-10}	$2^{-10} *$
Всего систем с $\tilde{p}^\pi$	1	1 *
$\overline{p}^\pi$	$2^{-9.990}$	между $2^{-9.985}$ и $2^{-10.015} *$
$\tilde{\delta}^\pi$	2^{-6}	$2^{-5} *$
Всего систем с $\tilde{\delta}^\pi$	256	16 *
$\overline{\delta}^\pi$	от $2^{-5.701}$ до $2^{-6.636}$	от $2^{-5.47}$ до $2^{-5.62} *$
Δ^π	≥ 0.996	≥ 0.9995
$\deg \pi$	≥ 32	≥ 32
Существенная	да	да
$\deg \pi^{-1}$	≥ 32	≥ 32
Обратная – существенная	да	да
Чётность	чётная	чётная

Подстановка «Альзет-5» получена из исходной подстановки «Альзет» добавлением пятого шага, на котором циклические сдвиги совпадают со сдвигами первого шага.

* Результаты получены в работе Beierle C., Biryukov A., Cardoso dos Santos L. et al. Alzette: A 64-bit ARX-box (feat CRAX and TRAX) // Cryptology ePrint Archive. 2019. URL: <https://eprint.iacr.org/2019/1378>.

Свойства подстановки «Альзет-К», пояснения к таблице

- Величина $\tilde{p}^\pi$ – оценка разностной характеристики

$$p^\pi = \max_{\alpha, \beta \in V_{64} \setminus \{0\}} \mathbf{P}\{\pi(x) \oplus \pi(x \oplus \alpha) = \beta\}$$

по согласованным системам локальных разностных соотношений*, получена методом ветвей и границ с помощью программы, созданной разработчиками подстановки «Альзет» (программа была предварительной верифицирована), а также с помощью результатов работы**.

- Величина $\tilde{\delta}^\pi$ – оценка линейной характеристики

$$\delta^\pi = \max_{\alpha, \beta \in V_{64} \setminus \{0\}} |2 \cdot \mathbf{P}\{\pi(x) \cdot \beta^T = x \cdot \alpha^T\} - 1|$$

по согласованным системам локальных линейных вероятностных соотношений*, получена сведением к задаче смешанного целочисленного линейного программирования (MILP)***.

- $\overline{p}^\pi, \overline{\delta}^\pi$ – экспериментальные оценки соответствующих характеристик, полученные по глобальным соотношениям найденных систем.

* Малышев Ф.М. Методы линейных и разностных соотношений в криптографии // Дискретная математика, 34:1 (2022), 36–63.

** Дмух А.А., Пасько Д.О. О поиске разностных соотношений для подстановки Alzette с максимальным или близким к нему значением разностной характеристики. ПДМ, 2022, №58, сс. 40-56.

*** Fu K., Wang M., Guo Y. et al. MILP-based automatic search algorithms for differential and linear trails for SPECK // LNCS / Ed. by T. Peyrin. Vol. 9783. Springer, Heidelberg, 2016. P. 268–288.

Свойства подстановки «Альзет-К», пояснения к таблице

- ▶ $\Delta^\pi = \max_{\alpha, \beta \in V_{64} \setminus \{0\}} |2 \cdot \mathbf{P}\{(\pi(x) \oplus \pi(x \oplus \alpha)) \cdot \beta^T = 0\} - 1|$ – разностно-линейная характеристика.
- ▶ Значения Δ^π оценивались построением конкретных разностно-линейных соотношений при помощи методов, которые позволяли получать высокие модули преобладаний для других вариантов подстановки типа «Альзет»* (поэтому получена нижняя граница на Δ^π).
- ▶ Существенность – зависимость любой нетривиальной линейной комбинации координатных функций подстановки от всех переменных.
- ▶ $\deg \pi$ – алгебраическая степень подстановки π : максимальное значение степени нелинейности координатных функций подстановки π .
- ▶ Оценки $\deg \pi, \deg \pi^{-1}$ и существенность прямой и обратной подстановок определялись экспериментально поиском в координатных функциях мономов заданной степени или содержащих заданную переменную. Распространение на линейные комбинации координатных функций осуществляется построением матрицы коэффициентов при мономах и проверкой максимальности её ранга. В случае $\deg \pi, \deg \pi^{-1}$ это позволяет установить минимальную степень нелинейности нетривиальных линейных комбинаций координатных функций подстановок π, π^{-1} .
- ▶ Чётность доказана теоретически для любой подстановки типа «Альзет» с $t > 1$ шагами и любыми значениями параметров $c, (r_1, \dots, r_t), (s_1, \dots, s_t)$.

* Niu Z., Sun S., Liu Y., Li C. Rotational Differential-Linear Distinguishers of ARX Ciphers with Arbitrary Output Linear Masks. // LNCS / Ed. by Y. Dodis, T. Shrimpton. Vol. 13507. 2022. P. 3–32.

Свойства линейных преобразований

- ▶ Линейные преобразования алгоритмов «Рамен- n К» при $n \in \{128, 192\}$ – максимально рассеивающие*.
- ▶ Характеристические многочлены линейных преобразований всех алгоритмов «Рамен- n К» – неприводимые.

* Определение см. Малышев Ф.М., Трифонов Д.И. Рассеивающие свойства XSLP-шифров // Математические вопросы криптографии, 7:3 (2016), 47–60.

Свойства линейных преобразований

- ▶ $\theta_{\text{л}}^{(n)}(t), \theta_{\text{р}}^{(n)}(t)$ – показатели рассеивания линейной среды алгоритмов «Рамен- nK » относительно линейного и разностного методов соответственно в зависимости от числа раундов t^* .

- ▶ Для $t = 2a + b, a \geq 0, b \in \{0,1\}$:

$$\theta_{\text{л}}^{(128)}(t) = \theta_{\text{р}}^{(128)}(t) = \theta^{(128)}(t) = 3a + b,$$

$$\theta_{\text{л}}^{(192)}(t) = \theta_{\text{р}}^{(192)}(t) = \theta^{(192)}(t) = 4a + b.$$

- ▶ Для $t = 4a + b, a \geq 0, b \in \{1, \dots, 4\}$:

$$\theta_{\text{л}}^{(256)}(t) = \theta_{\text{р}}^{(256)}(t) = \theta^{(256)}(t) = \begin{cases} 9a + 1 & \text{при } b=1, \\ 9a + 3 & \text{при } b=2, \\ 9a + 5 & \text{при } b=3, \\ 9a + 9 & \text{при } b=4. \end{cases}$$

* Определение см. Малышев Ф.М. Методы линейных и разностных соотношений в криптографии // Дискретная математика, 34:1 (2022), 36–63.

Сравнение показателей рассеивания алгоритмов «Рамен-128К», «Рамен-256К» и алгоритмов TRAX-M, TRAX-L*

Число итераций t	1	2	3	4	5	6	7	8	9	10	11	12
TRAX-M, $\theta^{(M)}(t)$	1	2	4	5	6	8	9	10	12	13	14	16
«Рамен-128К», $\theta^{(256)}(t)$	1	3	4	6	7	9	10	12	13	15	16	18

Число итераций t	1	2	3	4	5	6	7	8	9	10	11	12
TRAX-L, $\theta_p^{(L)}(t)$	1	2	5	8	9	10	13	16	17	18	21	24
TRAX-L, $\theta_l^{(L)}(t)$	1	2	5	7	9	10	13	14	17	18	21	22
«Рамен-256К», $\theta^{(256)}(t)$	1	3	5	9	10	12	14	18	19	21	23	27

$\theta^{(M)}(t)$ - показатель рассеивания линейной среды алгоритма TRAX-M (показатели для линейного и для разностного методов совпадают)

$\theta_l^{(L)}(t), \theta_p^{(L)}(t)$ - показатели рассеивания линейной среды алгоритма TRAX-L относительно линейного и разностного методов соответственно

* Алгоритмы TRAX-M и TRAX-L предложены в Beierle C., Biryukov A., Cardoso dos Santos L. et al. Alzette: A 64-bit ARX-box (feat CRAX and TRAX) // Cryptology ePrint Archive. 2019. URL: <https://eprint.iacr.org/2019/1378>. Значения показателей рассеивания для алгоритмов TRAX-M, TRAX-L получены в работе Дмух А.А., Пасько Д.О. Значения показателей рассеивания линейной среды обобщённого семейства TRAX относительно разностного и линейного методов криптографического анализа. Тезисы доклада на конференции, посвящённой памяти А.М. Зубкова, 2026 г.

Результаты криптографического анализа

- ▶ Алгоритмы семейства «Рамен-К» были подвергнуты экспертным криптографическим исследованиям ФСБ России*. При условии использования в указанных выше стандартизированных режимах работы с соблюдением рекомендаций на объём материала, обрабатываемого на одном ключе (порядка $2^{n/2} \sqrt{\pi_0}$, где π_0 - максимальная допустимая вероятность эффективного применения методов криптографического анализа, n – размер блока в битах), не было найдено методов восстановления ключа более эффективных, чем полный перебор ключа. Средняя трудоёмкость полного перебора ключа алгоритма «Рамен- n К» составляет 2^{2n-1} зашифрований, $n \in \{128, 192, 256\}$.

* Матюхин Д.В. Если не ГОСТ, но очень хочется: «ПРАПОР-К» и «Рамен-К» – новые семейства (низкоресурсных) блочных шифров // Материалы конференции «Рускрипто'2026», 2026.

О выборе синтезных решений – структура алгоритмов

- ▶ Алгоритм «Рамен-128К» с «классическими» размерами блока и ключа.
- ▶ Алгоритм «Рамен-256К» – «расширение» алгоритма «Рамен-128К».
- ▶ Алгоритм «Рамен-192К» – «экспериментальный».

* Hadipour H., Derbez P., Eichlseder M. Revisiting Differential-Linear Attacks via a Boomerang Perspective With Application to AES, Ascon, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBlock, Simeck, and SERPENT // Cryptology ePrint Archive 2024/255 <https://eprint.iacr.org/2024/255>, 2024.

** Sabaly T., Minier M. Differential-Linear Attacks from new Distinguishers: The Case of SERPENT and PRESENT. // <https://link.springer.com/article/10.1007/s10623-025-01790-x>, 2025.

О выборе синтезных решений – подстановка

- ▶ Изначальная ориентация на 32- и 64-битные платформы позволила улучшить линейные характеристики подстановки «Альзет-К» по сравнению с подстановкой «Альзет-5» за счёт выбора значений параметров, не входящих в множество «удобных» для 8- и 16-битных платформ.
- ▶ Высокое значение разностно-линейной характеристики, как правило, не приводит к построению эффективных методов криптографического анализа: разностно-линейные соотношения с преобладанием 1 найдены для алгоритмов AES (2 раунда из 10, 12 или 14), Ascon (4 раунда подстановки, используемой с 6, 8 и 12 раундами), WARP (11 раундов из 40), Simeck-32, Simeck-48, Simeck-64 (соответственно 7, 8, 10 раундов из 32, 36, 44), SERPENT (значение $2^{-0.68}$ близко к 1, 3 раунда из 32), PRESENT (3 раунда из 31) и других*. Эффективные методы построены для усечённых алгоритмов SERPENT (12 из 32) и PRESENT (16 или 18 из 31)**.

* Hadipour H., Derbez P., Eichlseder M. Revisiting Differential-Linear Attacks via a Boomerang Perspective With Application to AES, Ascon, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBlock, Simeck, and SERPENT // Cryptology ePrint Archive 2024/255 <https://eprint.iacr.org/2024/255>, 2024.

** Sabaly T., Minier M. Differential-Linear Attacks from new Distinguishers: The Case of SERPENT and PRESENT. // <https://link.springer.com/article/10.1007/s10623-025-01790-x>, 2025.

О выборе синтезных решений – линейные преобразования

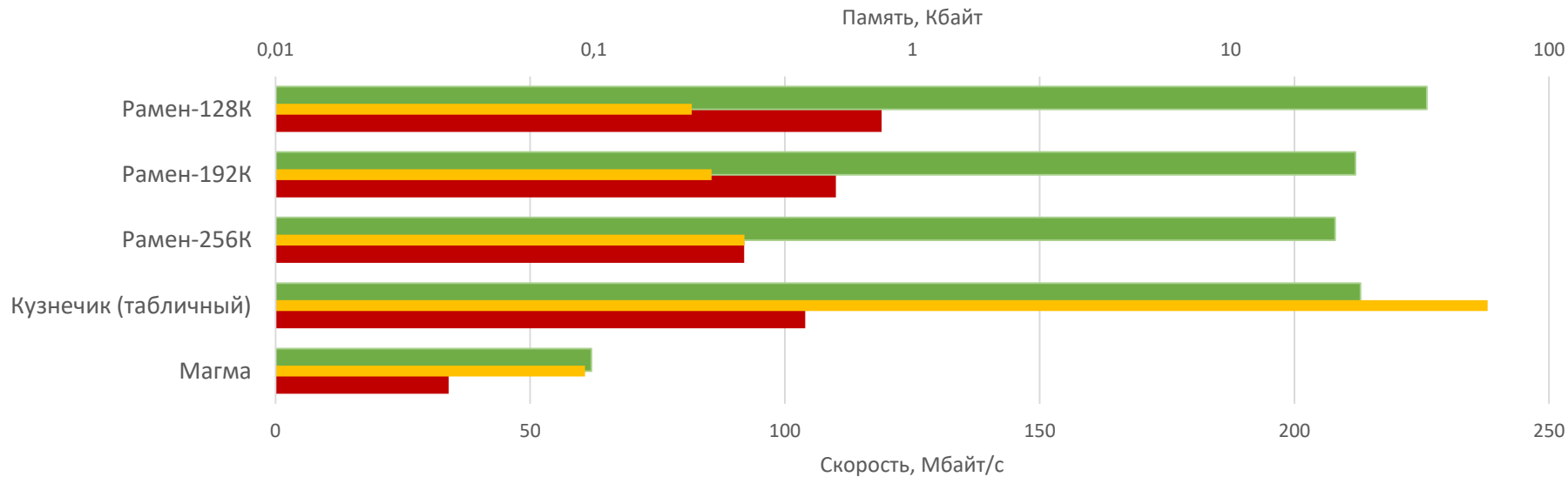
- ▶ Сочетают высокие криптографические качества с производительностью и удобством реализации на платформах, оперирующих 64- и, в несколько меньшей степени, 32-битными словами.
- ▶ Недостаток – относительно высокая трудоёмкость обращения.

О выборе синтезных решений – алгоритмы развёртывания ключа

- ▶ Довольно высокая трудоёмкость алгоритмов развёртывания ключа обусловлена желанием затруднить восстановление рабочего ключа или других раундовых ключей в случае нахождения одного или нескольких раундовых ключей
- ▶ Двойное применение раундовой функции в функции усложнения связано с относительной разреженностью матриц линейных преобразований.
- ▶ Алгоритм выработки констант АРК основан на обобщённой сети Фейстеля, начальные значения выбраны случайно. К константам предъявлялось требование максимальности ранга набора двоичных представлений констант для каждого из трёх алгоритмов как системы векторов над полем $GF(2)$.

Эксплуатационные характеристики*

Скорость базового алгоритма зашифрования и требуемый объём памяти



■ Скорость на AMD Ryzen 7 7800X3D, Мбайт/с ■ Скорость Raspberry Pi 5 Cortex A76, Мбайт/с ■ Расчётная память, Кбайт

- ▶ ПК с процессором AMD Ryzen 7 7800X3D @ 4.2 GHz, ОС Linux Mint 22.2, 1 ядро, 1 поток.
- ▶ Одноплатный компьютер RaspberryPi 5 8Gb, Cortex A76 @ 2.4 GHz, ОС RaspberryPi Bookworm, 1 ядро, 1 поток.
- ▶ Компилятор clang 18.1.3 с оптимизацией -O3, язык C.
- ▶ «Кузнечик» реализован с помощью таблиц, алгоритмы «Магма» и «Рамен-К» реализованы без специальной алгоритмической оптимизации (референсная реализация). Расчёт памяти: для «Рамен-К» - раундовые ключи, для «Кузнечика» — раундовые ключи и таблицы, для «Магмы» - ключ и подстановки.

* Матюхин Д.В. Если не ГОСТ, но очень хочется: «ПРАПОР-К» и «Рамен-К» — новые семейства (низкоресурсных) блочных шифров // Материалы конференции «Рускрипто'2026», 2026.