РусКрипто

КОМПАНИЯ АКТИВ

Алгоритмы аутентифицированного шифрования на основе отечественных криптографических примитивов в сценариях с вычислительными ограничениями

Борис Буинов,
Антон Васин,
Марина Скоробогатова

Компания «Актив»

Применение низкоресурсной криптографии

Низкоресурсные протоколы:

- Zigbee
- Bluetooth Low Energy
- Z-Wave
- TinySec
- EPC Tag Data Translation

Применение:

- Компоненты IoT
- RFID метки
- Банкоматы
- Кассовые терминалы
- СКУД

Рассматриваемые сценарии

- Защищённый обмен сообщениями после распределения общего секрета
- Небольшое количество ресурсов, выделяемых на шифрование
- Обеспечение конфиденциальности данных и целостности передаваемого сообщения $\Rightarrow$ AEAD
- Программная реализация
- Использование примитивов из отечественных стандартизированных алгоритмов
- **Ограниченные возможности противника**

Цель: получить ускорение в сравнении с существующими стандартизированными AEAD-схемами (MGM)

КОМПАНИЯ ПРАКТИВ

Модель противника: основные определения

Определение (Модель PRP)

Под ***преимуществом*** $\mathrm{Adv}_E^{\mathrm{PRP}}(A)$ ***противника*** A *в задаче различения случайной подстановки и подстановки* E*, задаваемой блочным шифром на случайном ключе* $K \xleftarrow{R} \{0,1\}^k$*, будем понимать*

$$\mathrm{Adv}_E^{\mathrm{PRP}}(A) = \left|\mathbb{P}(A^{E_K} = 1) - \mathbb{P}(A^{\pi} = 1,\ \pi \xleftarrow{R} S(\{0,1\}^n))\right|.$$

Определение

Под ***AEAD алгоритмом*** *будем понимать пару* $\mathcal{AE} = (\mathcal{E}, \mathcal{D})$*, где*
$\mathcal{E}\colon K \times N \times A \times P \to C \times T$ *– алгоритм зашифрования и вычисления имитовставки,*
$\mathcal{D}\colon K \times N \times A \times C \times T \to P \cup \{\perp\}$ *– алгоритм расшифрования и проверки имитовставки.*

Модель противника nAE

Определение

Для противника A определим его ***преимущество в модели*** nAE[1] *как*

$$\mathrm{Adv}^{\mathrm{AE}}_{\mathcal{AE}}(A) = \left|\mathbb{P}(A^{\mathcal{E}_K,\mathcal{D}_K} = 1) - \mathbb{P}(A^{\$,\perp} = 1)\right|.$$

Тогда максимум по всем противникам равен

$$\mathrm{Adv}^{\mathrm{AE}}_{\mathcal{AE}}(t, q_e, q_d, \sigma_e, \sigma_d) = \max_A \mathrm{Adv}^{\mathrm{AE}}_{\mathcal{AE}}(A).$$

- t – вычислительные возможности противника;
- q_e, q_d – количество запросов к оракулу зашифрования $\mathcal{E}_K$ и расшифрования $\mathcal{D}_K$;
- σ_e, σ_d – общее количество вызовов блочной шифрсистемы при запросах зашифрования и расшифрования соответственно.

[1] Fleischmann E., Forler C., Lucks S. McOE: A family of almost foolproof on-line authenticated encryption schemes //International Workshop on Fast Software Encryption. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. – С. 196-215.

Режим SAEB[2]

Модификации:

- Блочный шифр: Магма или Кузнечик (ГОСТ 34.12-2018)
- Длина блока: $n = 64$ бит или $n = 128$ бит соответственно

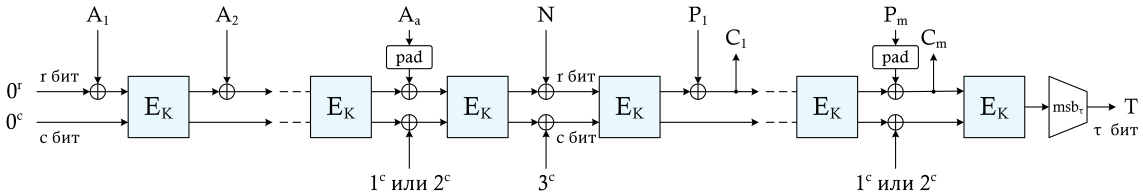


Рис. 1: Схема режима SAEB

[2]Naito Y. et al. SAEB: A lightweight blockcipher-based AEAD mode of operation //Cryptology ePrint Archive. – 2019.

Оценка для режима SAEB

Теорема (см. [2])

Пусть σ_A — количество вызовов с фиксированными ассоциированными данными, $\sigma = \sigma_e + \sigma_d$. Тогда для любого $\rho \geq 1$

$$\mathrm{Adv}^{\mathrm{AE}}_{SAEB}(t, q_e, q_d, \sigma_e, \sigma_d) \leq \mathrm{Adv}^{PRP}_{E}(t+O(\sigma), \sigma) + \frac{2\sigma^2}{2^n} + \frac{(\rho-1)(\sigma_A+\sigma_d)}{2^c} + 2^r \left(\frac{e\sigma_e}{\rho 2^r}\right)^{\rho} + \frac{q_d}{2^\tau}.$$

Здесь и далее считаем блочные шифры Магма и Кузнечик стойкими в модели PRP. Это означает, что слагаемое $\mathrm{Adv}^{\mathrm{PRP}}_{E}(t', q')$ пренебрежимо мало.

Пример применения оценки для SAEB

$q_e = q_d$	$\sigma_e = \sigma_d = \sigma_A$	r	c	$\mathrm{Adv}^{\mathrm{AE}}_{SAEB}$
2^{22}	2^{22} (32 МБ)	32	32	$< 10^{-2}$ $(\rho = 4)$
2^{11}	2^{11} (16 КБ)	45	19	$< 10^{-2}$ $(\rho = 2)$
2^{26}	2^{26} (512 МБ)	16	48	$< 10^{-2}$ $(\rho = 2809)$

Таблица 1: Магма в режиме SAEB

$q_e = q_d$	$\sigma_e = \sigma_d = \sigma_A$	r	c	$\mathrm{Adv}^{\mathrm{AE}}_{SAEB}$
2^{46}	2^{46} (1 ПБ)	64	64	$< 10^{-4}$ $(\rho = 5)$
2^{24}	2^{24} (256 МБ)	96	32	$< 10^{-2}$ $(\rho = 2)$
2^{46}	2^{46} (1 ПБ)	32	96	$< 10^{-9}$ $(\rho = 44592)$

Таблица 2: Кузнечик в режиме SAEB

КОМПАНИЯ ПРАКТИВ

Режим COFB[3]

Модификации:

- Блочный шифр: Магма или Кузнечик (ГОСТ 34.12-2018)
- Длина блока: $n = 64$ бит или $n = 128$ бит соответственно
- Функция G: $\{0,1\}^n \to \{0,1\}^n$ действует по правилу

$$G(Y) = G(Y_0 \mid\mid Y_1) = Y_1 \mid\mid (Y_0 \lll 1),$$

где $(Y_0, Y_1) \xleftarrow{\frac{n}{2}} Y$, $Y \lll r$ – циклический сдвиг влево на r бит.

- Умножение в поле $F = GF(2^{\frac{n}{2}}) = \mathbb{Z}_2[x]/f(x)$, где

$$f(x) = \begin{cases} x^{64} + x^4 + x^3 + x + 1, & \text{если } n = 128; \\ x^{32} + x^7 + x^3 + x^2 + 1, & \text{если } n = 64. \end{cases}$$

[3] Chakraborti A. et al. Blockcipher-based authenticated encryption: how small can we go? //Journal of Cryptology. – 2020. – Т. 33. – №. 3. – С. 703-741.

Схема режима COFB

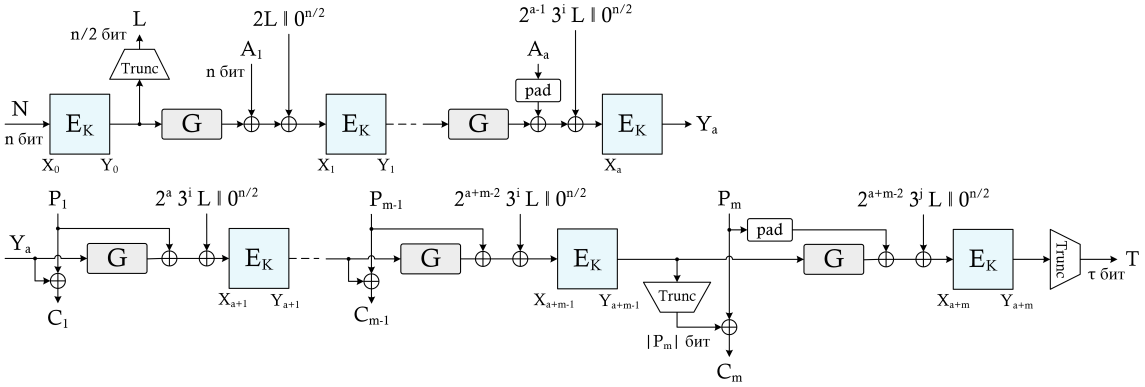


Рис. 2: Схема режима COFB

Оценка стойкости для режима COFB

Теорема (см. [4])

Пусть $q' = q_e + q_d + \sigma_e + \sigma_d$, $t' = t + O(q')$. *Тогда для* $q' \leq 2^{\frac{n}{2}-1}$ *справедливо*

$$\mathrm{Adv}^{\mathrm{AE}}_{COFB}(t, q_e, q_d, \sigma_e, \sigma_d) \leq \mathrm{Adv}^{\mathrm{PRP}}_{E}(t', q') + \frac{q'(q'-1)}{2^{n+1}} + \frac{\sigma_e + 1}{2^{\frac{n}{2}}} +$$

$$+ \frac{q_d(n+4)}{2^{\frac{n}{2}+1}} + \frac{3\sigma_e^2 + q_d + 2\sigma_d(q_e + \sigma_e + \sigma_d)}{2^n}.$$

Отметим, что в модифицированной схеме при $n = 64$ многочлен $f(x)$ является неприводимым, но не является примитивным. Однако, **для выбранного** $f(x)$ **гарантируется уникальность маски** $2^i 3^j$, что позволяет аналогичным образом доказать данную оценку.

[4] Banik S. et al. GIFT-COFB v1.2. - 2022.

Пример применения оценки для COFB

n	$q_e = q_d$	$\sigma_e = \sigma_d$	$\mathrm{Adv}^{\mathrm{AE}}_{COFB}$
64	2^{17}	2^{25} (256 МБ)	$< 10^{-2}$

Таблица 3: Магма в режиме COFB

n	$q_e = q_d$	$\sigma_e = \sigma_d$	$\mathrm{Adv}^{\mathrm{AE}}_{COFB}$
128	2^{39}	2^{47} (1 ПБ)	$< 10^{-5}$

Таблица 4: Кузнечик в режиме COFB

Режим Duplex[5]

Модификации:

- Подстановка $\Pi\colon \{0,1\}^{256} \to \{0,1\}^{256}$, $\Pi = \Pi_L \circ \Pi_S \circ \Pi_C$
- Π_C – сложение по модулю 2 с раундовой константой:

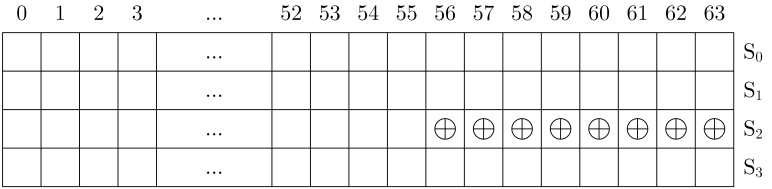


Рис. 3: Применение констант

Раунд	1	2	3	4	5	6	7	8	9	10	11	12
Константа	$f0$	$e1$	$d2$	$c3$	$b4$	$a5$	96	87	78	69	$5a$	$4b$

Таблица 5: Раундовые константы

Режим Duplex[5]

Модификации:

- Π_S – подстановка из блочного шифра Магма:

$$\pi_0 = (12, 4, 6, 2, 10, 5, 11, 9, 14, 8, 13, 7, 0, 3, 15, 1)$$

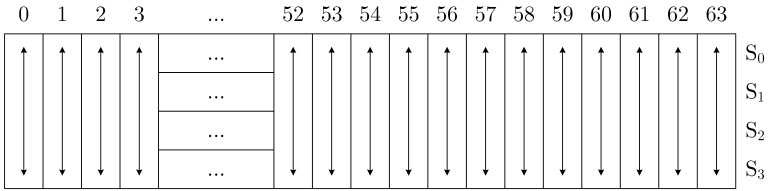


Рис. 4: Применение подстановки

Данная архитектура обеспечивает возможность реализации подстановки методом «битслайс».

Режим Duplex[5]

Модификации:

- Π_L – линейное преобразование:

$$S_0 = S_0 \oplus (S_0 \ggg 19) \oplus (S_0 \ggg 28), \qquad S_2 = S_2 \oplus (S_2 \ggg 1) \oplus (S_2 \ggg 6),$$
$$S_1 = S_1 \oplus (S_1 \ggg 39) \oplus (S_1 \ggg 61), \qquad S_3 = S_3 \oplus (S_3 \ggg 10) \oplus (S_3 \ggg 17).$$

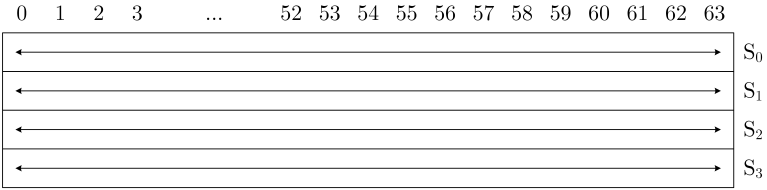


Рис. 5: Применение линейного слоя

[5]Bertoni G. et al. Duplexing the sponge: single-pass authenticated encryption and other applications //Selected Areas in Cryptography: 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers 18. – Springer Berlin Heidelberg, 2012. – С. 320-337.

Схема режима Duplex

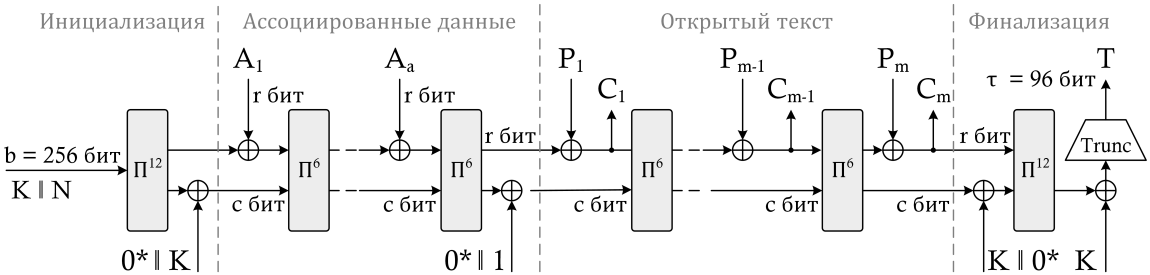


Рис. 6: Схема режима Duplex

Оценка для режима Duplex

Определение (см. [6])

$$\mathrm{col}(q,N)=\begin{cases}3, & 4\le q\le\sqrt{N};\\ \frac{4\log_2 q}{\log_2\log_2 q}, & \sqrt{N}<q\le N;\\ 5\log_2 N\lceil\frac{q}{N}\rceil, & N<q.\end{cases}$$

Теорема

Пусть $q_p(t)$ — число вызовов подстановки Π, $\sigma=\sigma_e+\sigma_d$. Тогда

$$\mathrm{Adv}^{\mathrm{AE}}_{duplex}(t,q_e,q_d,\sigma_e,\sigma_d)\le\frac{2q_d}{2^\tau}+\frac{\sigma_e^2+\sigma_d(q_p+\sigma_d)+q_eq_d+(2q_e+q_d)(\sigma+q_p)}{2^b}+$$
$$+\frac{\mathrm{col}(\sigma_e,2^r)(\sigma_d+q_p)+\mathrm{col}(\sigma_e,2^\tau)q_d}{2^c}+\frac{q_p+\sigma+\mathrm{col}(\sigma+q_p,2^\tau)q_d+\mathrm{col}(q_e,2^{b-k})q_d}{2^k}.$$

[6] Chakraborty B., Dhar C., Nandi M. Exact security analysis of ASCON //International Conference on the Theory and Application of Cryptology and Information Security. – Singapore : Springer Nature Singapore, 2023. – С. 346-369.

Пример применения оценки для Duplex

$q_e = q_d$	$\sigma_e = \sigma_d$	r	c	q_p	$\mathrm{Adv}^{\mathrm{AE}}_{duplex}$
2^{46}	2^{46} (1 ПБ)	128	128	10^{30}	$< 10^{-7}$
2^{46}	2^{46} (> 1 ПБ)	160	96	10^{23}	$< 10^{-5}$
2^{36}	2^{36} (> 1 ТБ)	171	85	10^{20}	$< 10^{-5}$

Таблица 6: Режим Duplex с примитивом из Магмы

Сравнение рассматриваемых режимов

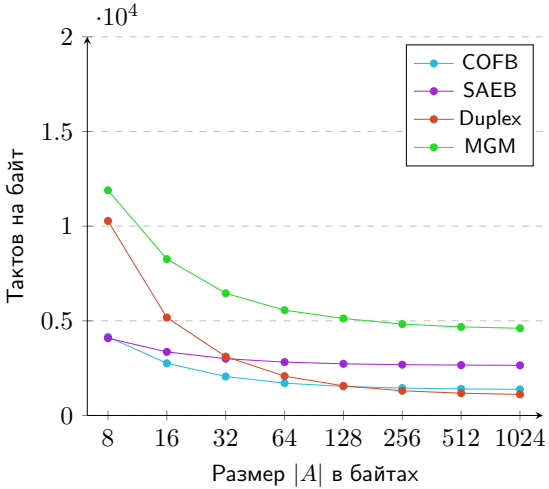
	COFB	**SAEB**	**Duplex**
Требуемая память	$k + \frac{3}{2}n = 352$ бит	$k + n = 320$ бит	$64 \cdot s = 256$ бит
Преимущества	Быстрая реализация; Стойкость не сильно ухудшается при повторе вектора инициализации (nonce misuse)	Эффективная обработка константных ассоциированных данных; Небольшое количество требуемой памяти	Быстрая реализация для данных произвольной длины; Более стойкий при фиксированных ресурсах противника
Недостатки	Менее стойкий при фиксированных ресурсах противника; Имеет операции, отличные от XOR	Менее стойкий при фиксированных ресурсах противника; Невысокая скорость	Оценку стойкости невозможно свести к стойкости блочного шифра; Медленный для данных небольшого размера

Используемые микроконтроллеры

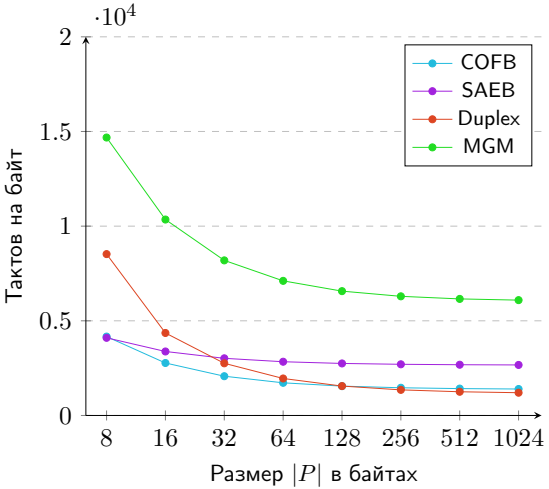
Характеристики	Atmega640	STM32F446RE	CH32V307VCT6
Архитектура	AVR (avr5)	Arm (Cortex-M4)	RISC-V (QingKe V4F с ISA RV32IMACF)
Регистры	8 бит	32 бита	32 бита
Тактовая частота	16 МГц	180 МГц	144 МГц
Производительность	0.54 CoreMark/MHz	3.35 CoreMark/MHz	3.19 CoreMark/MHz
Flash-память	64 КБ	512 КБ	256 КБ
EEPROM	4 КБ	Нет	Нет
SRAM	8 КБ	128 КБ	64 КБ

Таблица 7: Микроконтроллеры, для которых производились замеры скоростей

Сравнение скоростей для Atmega640 при r = c

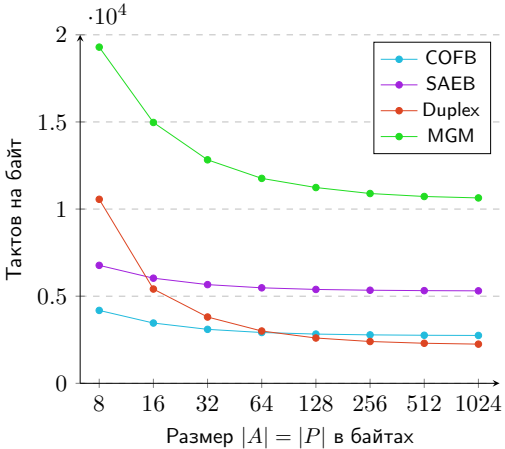


Только ассоциированные данные

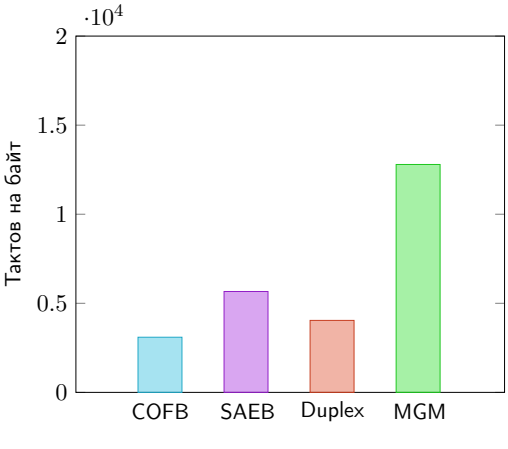


Только открытый текст

Сравнение скоростей для Atmega640 при r = c

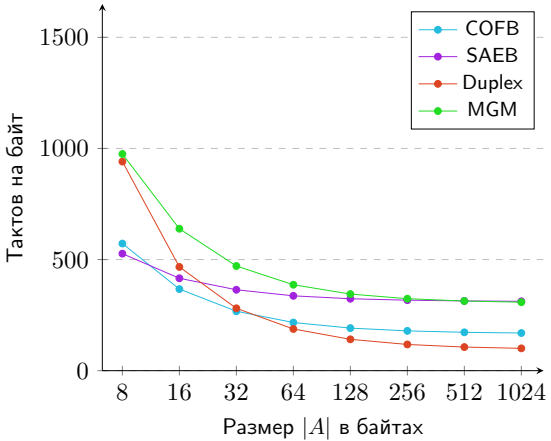


Ассоциированные данные и открытый текст

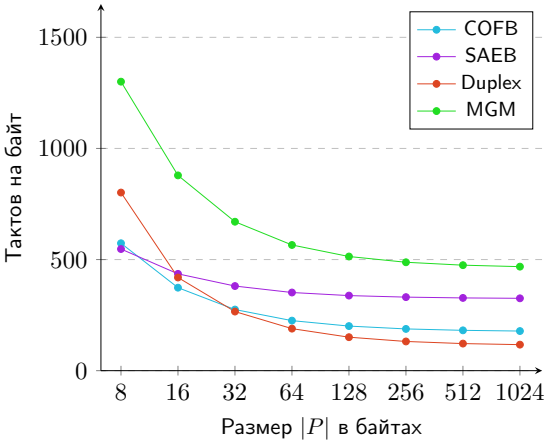


Усредненные значения для набора текстов

Сравнение скоростей для STM32F446RE при r = c

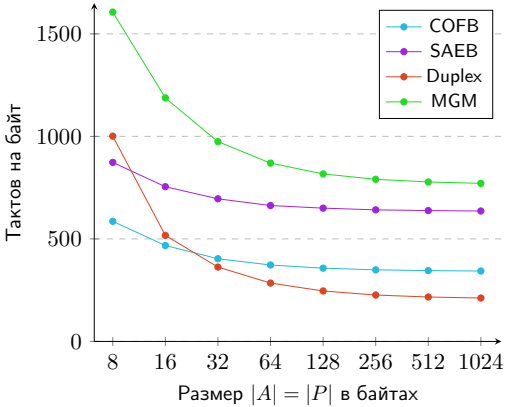


Только ассоциированные данные

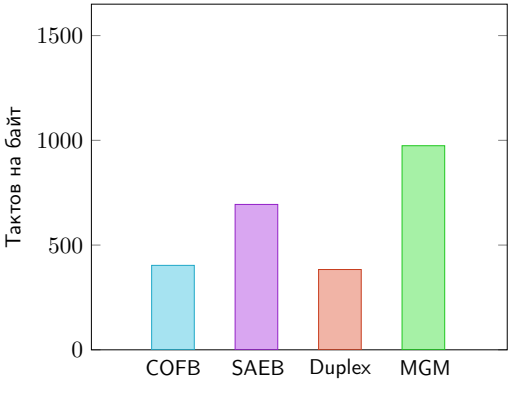


Только открытый текст

Сравнение скоростей для STM32F446RE при r = c

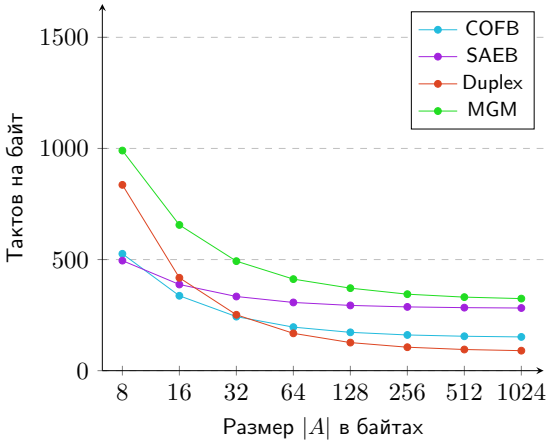


Ассоциированные данные и открытый текст

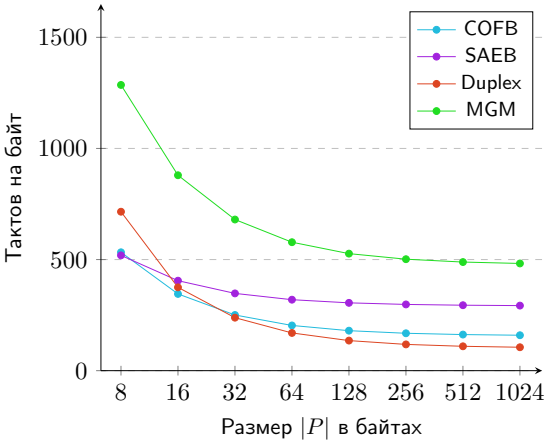


Усредненные значения для набора текстов

Сравнение скоростей для CH32V307VCT6 при r = c

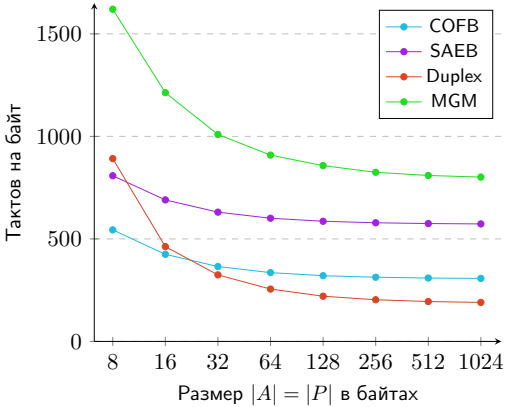


Только ассоциированные данные

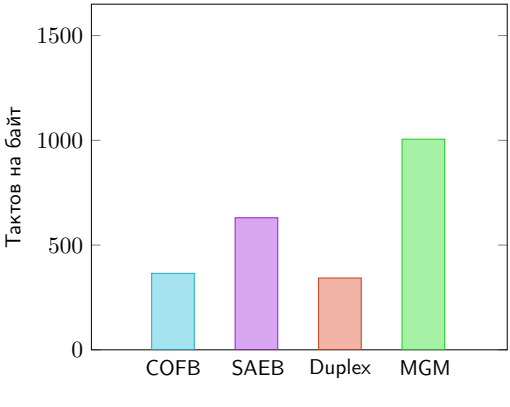


Только открытый текст

Сравнение скоростей для CH32V307VCT6 при r = c



Ассоциированные данные и открытый текст



Усредненные значения для набора текстов

Спасибо
за внимание!

Компания Актив

info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90

РусКрипто

Приложение: схема режима MGM

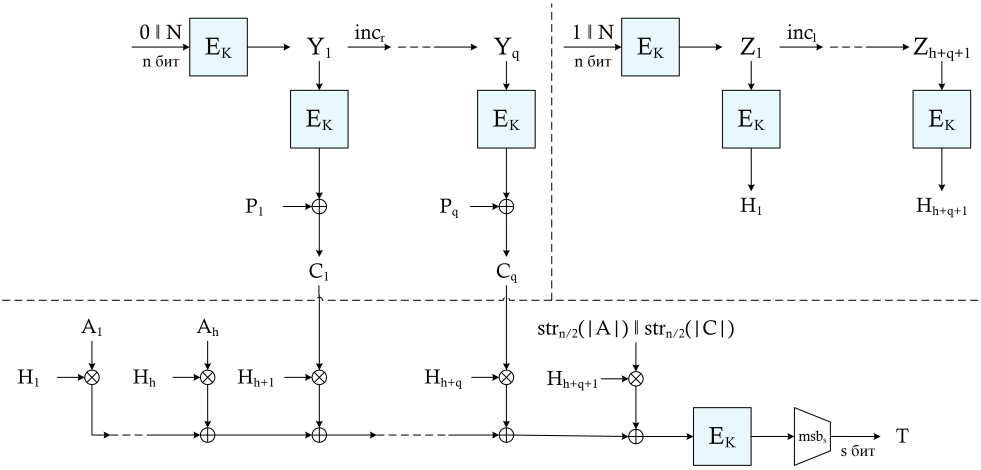


Рис. 7: Схема режима MGM