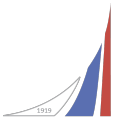
Характеристики режима работы блочных шифров, предлагаемого для защиты системных носителей информации с блочно-ориентированной структурой

Коренева А.М.[1,2], Фирсов Г.В.[1,3]

[1]ООО «Код Безопасности»
[2]Финансовый университет при Правительстве РФ
[3]НИЯУ МИФИ

23 марта 2023



Структура доклада

1. Актуальность исследования
2. Целевые характеристики предлагаемого режима XEH
3. Определение режима XEH
4. Уровень информационной безопасности режима XEH
5. Сравнение с существующими решениями

Научный фундамент

1. Bodganov D. Nozdrunov V. Some properties of one mode of operation of block ciphers // 10th Workshop on Current Trends in Cryptology (CTCrypt 2021). 2021.
2. Isobe T., Minematsu K. Plaintext Recovery Attacks Against XTS Beyond Collisions. 2020.
3. Firsov G.V., Koreneva A.M. On One Block Cipher Mode of Operation Used to Protect Data on Block-Oriented Storage Devices. Modern Information Technologies and IT-Education. 2022; 18(3):691-701.
4. Смышляев С. В. Математические методы обоснования оценок уровня информационной безопасности программных средств защиты информации, функционирующих в слабодоверенном окружении. Диссертация на соискание степени доктора физико-математических наук. 2022.
5. Ахметзянова Л. Р. Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации. Диссертация на соискание степени кандидата физико-математических наук. 2022.

Принятые сокращения

ИБ	—	Информационная безопасность
ПДШ (FDE)	—	Полнодисковое шифрование
CPA	—	Chosen plaintext attack (атака по подобранному открытому тексту)
DEC	—	Режим Disk Encryption with Counter
XEH	—	Режим Xor-Encrypt-Hash
XTS	—	Режим XEX-based Tweaked codebook with ciphertext Stealing

Актуальность исследования

- Необходимость обеспечения конфиденциальности хранимых данных при угрозе кражи носителя информации.
- Для ПДШ в существующих решениях используются специальные режимы работы блочных шифров.
- В 2022 году в России утвержден первый режим работы блочных шифров, предназначенный для защиты носителей информации (режим DEC) [1].

[1] *Р 1323565.1.042–2022 «Информационная технология. Криптографическая защита информации. Режим работы блочных шифров, предназначенный для защиты носителей информации с блочно-ориентированной структурой». — М. : Стандартинформ, 2022.*

Актуальность исследования

- Режим DEC имеет ограничения по применению при шифровании системных носителей.

В режиме DEC с каждым сектором и каждым разделом ассоциируются соответствующие счетчики, равные по длине половине блока.

Windows 10/11 x64 требует в среднем 32 Гб дискового пространства.

Шифр	Длина блока	Размер сектора	Требуемый объем дополнительных данных
Магма	64 бит	512 байт	256 Мб
	64 бит	4096 байт	32 Мб
Кузнечик	128 бит	512 байт	512 Мб
	128 бит	4096 байт	64 Мб

Стандартный объем системного раздела EFI составляет 100 Мб.

Эксплуатационные ограничения и возможности нарушителя

Эксплуатационные ограничения

- шифртекст должен иметь ту же длину, что и открытый текст;
- отсутствует место под дополнительные данные.

Использование «настройки» (tweak) для внесения «недетерминированности»

Возможности нарушителя

- произвольная запись через интерфейс ПДШ;
- произвольное чтение напрямую с диска.

Атаки на основе подобранных открытых текстов (CPA)

Целевые эксплуатационные характеристики предлагаемого режима

- Повышенные требования к производительности.

Минимальное количество обращений к примитиву блочного шифра

- При шифровании системного диска место под дополнительные данные отсутствует.

Отсутствие дополнительных данных, хранимых на носителе

- Режим XTS широко распространен в существующих решениях[a] для ПДШ.

Сохранение внешнего интерфейса режима XTS (ключи, настройка, входные данные...)

[a] VeraCrypt, Microsoft BitLocker, FileVault и др.

Целевые криптографические характеристики предлагаемого режима

- Обеспечение конфиденциальности на уровне сектора.

Неактуальность угрозы различения шифртекста и случайной строки (модель RND-fdeCPA-sector [2]).

- На режим XTS возможны атаки, основанные на коллизиях определенного вида [3].

Невозможность построения известных атак, к которым уязвим режим XTS.

[2] *Firsov G.V., Koreneva A.M. On One Block Cipher Mode of Operation Used to Protect Data on Block-Oriented Storage Devices. Modern Information Technologies and IT-Education. 2022.*
[3] *Isobe T., Minematsu K. Plaintext Recovery Attacks Against XTS Beyond Collisions. 2020.*

Принятые обозначения

l	—	длина блока в битах
n	—	количество блоков в секторе $(0 < n < 2^l)$
$\mathcal{M}$	—	множество открытых текстов
$\mathcal{C}$	—	множество шифртекстов
$\mathcal{K}$	—	ключевое множество
$\mathcal{E}$	—	симметричный блочный шифр
$E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$	—	функция зашифрования симметричного блочного шифра $\mathcal{E}$
V_l	—	множество битовых строк длины l
$\mathbb{F}$	—	поле $GF(2)[x]/p(x)$, где $p(x) = x^{128} + x^7 + x^2 + x + 1$ для $l = 128$, $p(x) = x^{64} + x^4 + x^3 + x + 1$ для $l = 64$
$\mathfrak{F}_l : \mathbb{Z}_{2^l} \to \mathbb{F}$	—	отображение, сопоставляющее элементу $r = \sum_{j=0}^{l-1} a_j 2^j$ кольца $\mathbb{Z}_{2^l}$ элемент $\tilde{r} = \sum_{j=0}^{l-1} a_j x^j$ поля $\mathbb{F}$
$\Delta_l : V_l \to \mathbb{F}$	—	отображение, сопоставляющее строке $a = (a_0, ..., a_{l-1})$ из V_l элемент $\tilde{a} = \sum_{j=0}^{l-1} a_j x^j$ поля $\mathbb{F}$
$\nabla_l : \mathbb{F} \to V_l$	—	отображение, обратное к Δ_l

Определение режима ХЕН

В предлагаемом режиме используется функция $g : \mathbb{F}^2 \times \mathbb{F}^n \to \mathbb{F}^n$.
Будем обозначать через $g_{\tau_2,\tau_3}(y_1, ..., y_n)$ значение функции $g((\tau_2, \tau_3), (y_1, ..., y_n))$ для $\tau_2, \tau_3 \in \mathbb{F}$:

$$g_{\tau_2,\tau_3}(y_1, ..., y_n) = \left(y_1 + Y_{\tau_3} + \tau_2 \cdot \alpha^0, ..., y_{n-1} + Y_{\tau_3} + \tau_2 \cdot \alpha^{n-2}, Y_{\tau_3} + \tau_2 \cdot \alpha^{n-1}\right)$$

$$Y_{\tau_3} = \left(\sum_{j=1}^{n} y_j \cdot \tau_3^{n-j}\right) + \left(\sum_{j=1}^{n-1} y_j \cdot \mathfrak{F}_l(j)\right),$$

где $\alpha = x$ — примитивный элемент поля $\mathbb{F}$.
Также будет применяется функция $\phi : \mathbb{F} \times \mathbb{F}^n \to \mathbb{F}^n$.
Аналогично через $\phi_{\tau_3}(y_1, ..., y_n)$ обозначим значение $\phi(\tau_3, (y_1, ..., y_n))$ для $\tau_3 \in \mathbb{F}$:

$$\phi_{\tau_3}(y_1, ..., y_n) = (Z_{\tau_3}, y_2 + Z_{\tau_3}, ..., y_n + Z_{\tau_3})$$

$$Z_{\tau_3} = \sum_{j=1}^{n} y_j \cdot \tau_3^{j-1}.$$

Определение режима ХЕН

Введем вспомогательное обозначение:

$$f_{\tau_3}(y_1, ..., y_n) = (y_1 + Y_{\tau_3}, \cdots, y_{n-1} + Y_{\tau_3}, Y_{\tau_3}),$$

то есть:

$$g_{\tau_2,\tau_3}(\mathbf{y}) = f_{\tau_3}(\mathbf{y}) + \mathbf{a}_{\tau_2}$$
$$\mathbf{a}_{\tau_2} = (\tau_2 \cdot \alpha^0, ..., \tau_2 \cdot \alpha^{n-1}).$$

Определение режима XEH

Из номера сектора SN при помощи двух ключей $K, K' \in \mathcal{K}$ вырабатываются три подключа:

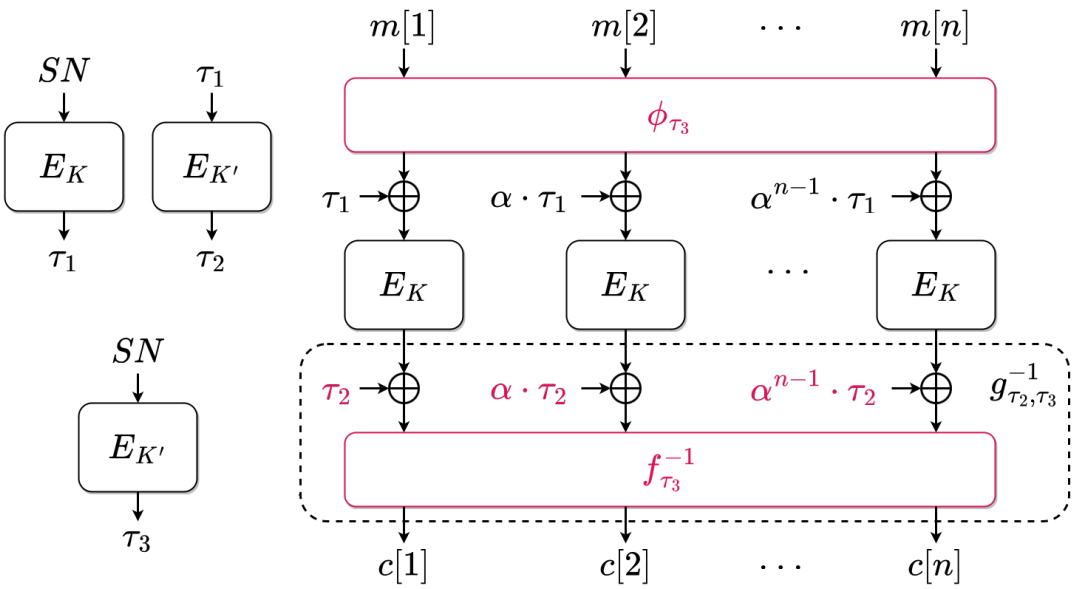
$$\tau_1 = \Delta_l(E_K(SN))$$
$$\tau_2 = \Delta_l(E_{K'}(\nabla_l(\tau_1)))$$
$$\tau_3 = \Delta_l(E_{K'}(SN))$$

Уравнение зашифрования в режиме XEH:

$$(w_1, ..., w_n) = \phi_{\tau_3}(\Delta_l(m_1), ..., \Delta_l(m_n))$$
$$y_j = \Delta_l(E_K(\nabla_l(w_j + \tau_1 \cdot \alpha^{j-1}))), j = \overline{1, n}$$
$$(z_1, ..., z_n) = g^{-1}_{\tau_2,\tau_3}(\mathbf{y}) = g^{-1}_{\tau_2,\tau_3}(y_1, ..., y_n)$$
$$\mathbf{c} = (\nabla_l(z_1), ..., \nabla_l(z_n))$$

где $\mathbf{c} = (c_1, ..., c_n)$ — шифртекст, $\mathbf{m} = (m_1, ..., m_n)$ — открытый текст, $m_j, c_j \in V_l$, $j = \overline{1, n}$.

Определение режима XEH



Уровень информационной безопасности режима XEH

Теорема 1.

Пусть π — случайная подстановка множества V_l. При фиксированных целых числах l, n и q верна следующая нижняя оценка уровня информационной безопасности режима XEH:

$$\mathbf{Adv}^{\text{RND-fdeCPA-sector}}_{\text{XEH}^{\pi}}(q) \leq \frac{2(n+1)^2 q^2}{2^l},$$

где l — длина блока в битах, n — количество блоков в секторе, q — количество запросов к экспериментатору.

RND-fdeCPA-sector — модель неразличимости шифртекста и случайной битовой строки [2].

[2] *Firsov G.V., Koreneva A.M. On One Block Cipher Mode of Operation Used to Protect Data on Block-Oriented Storage Devices. Modern Information Technologies and IT-Education. 2022.*

Уровень информационной безопасности режима XEH

Теорема 2.

Пусть $\mathcal{E}$ — симметричный блочный шифр. При фиксированных числах l, n и q верна оценка:

$$\mathbf{Adv}^{\text{RND-fdeCPA-sector}}_{\text{XEH}^{\mathcal{E}}}(t,q) \leq \frac{2(n+1)^2 q^2}{2^l} + \mathbf{Adv}^{\text{PRP}}_{\mathcal{E}}(t', nq+q),$$

где $t' = t + O(nq+q)$, $q \to \infty$, t — время работы нарушителя в эксперименте RND-fdeCPA-sector, t' — время работы нарушителя в эксперименте PRP.

PRP — модель неразличимости блочного шифра и случайной подстановки [4].

[4] *Boneh D., Shoup V. A Graduate Course in Applied Cryptography. 2023.*

Уровень информационной безопасности режима XEH

Режим работы (Mode)	$\mathbf{Adv}^{\text{RND-fdeCPA-sector}}_{\text{Mode}^{\mathcal{E}}}(\mathcal{A})$
XTS	$1 - 2^{-l}$
XEH	$\leq \frac{2(n+1)^2 q^2}{2^l} + \mathbf{Adv}^{\text{PRP}}_{\mathcal{E}}(t', nq + q)$

Для шифра «Кузнечик» (длина блока $l = 128$, длина ключа $k = 256$), сектора размером 4096 байт ($n = 2^8$) и количества запросов $q = 2^{16}$:

XTS	$\mathbf{Adv}^{\text{RND-fdeCPA-sector}}_{\text{XTS}^{\mathcal{E}}}(\mathcal{A}) = 1 - 2^{-128} \approx 1$
XEH	$\mathbf{Adv}^{\text{RND-fdeCPA-sector}}_{\text{XEH}^{\mathcal{E}}}(\mathcal{A}) \leq \frac{2 \cdot (2^8+1)^2 \cdot 2^{32}}{2^{128}} + \frac{2^{16} \cdot (2^8+1)}{2^{256}} \sim 2^{-79}$

Сравнение с существующими решениями

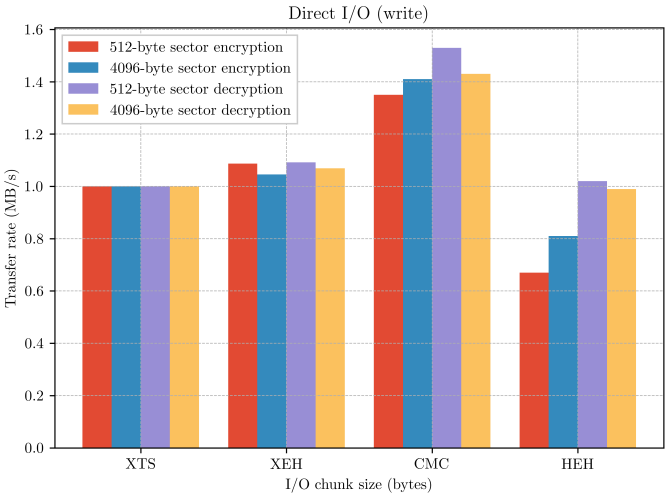
Существуют несколько *обобщенных* подходов к построению «широкоблочных» подстановок, в частности:

- Encrypt-Mix-Encrypt (примеры: **CMC**, EME, EME*);
- Hash-ECB-Hash (примеры: **HEH**, TET, PEP).

Сравним предлагаемый режим с выделенными красным.

Сравнение с существующими решениями

Производительность с использованием шифра «Кузнечик»

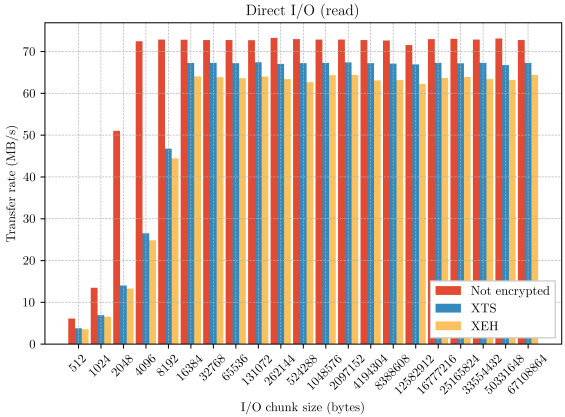


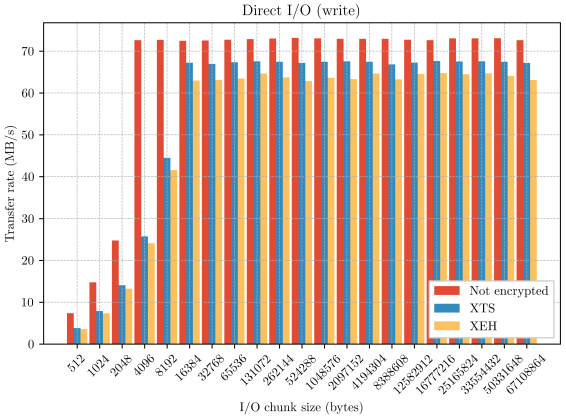
- Преимущество более 35% по сравнению с режимом CMC.
- Деградация производительности не более 10% по сравнению с режимом XTS.

Intel(R) Core(TM) i7-9750H (2.6 ГГц), DDR4 (8 Гб), macOS 13.1 (64-бит)

Сравнение с существующими решениями

Производительность с использованием шифра «Кузнечик»



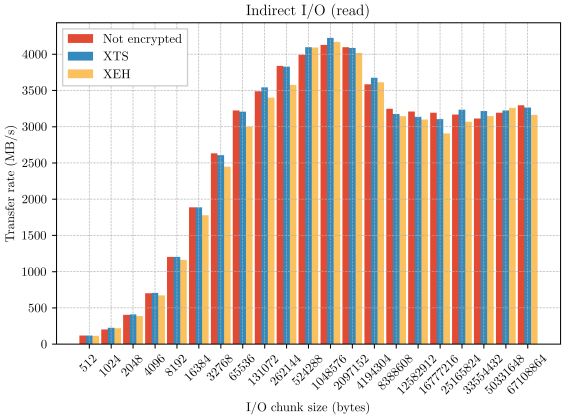


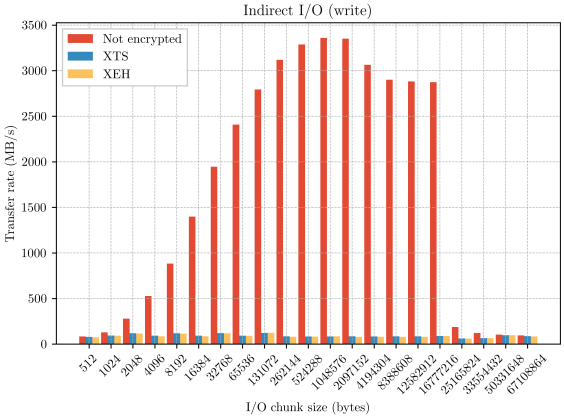
Прямой ввод/вывод

Intel(R) Core(TM) i7-3630QM (2.4 ГГц), DDR3 (6 Гб), Windows 10 (64-бит)

Сравнение с существующими решениями

Производительность с использованием шифра «Кузнечик»





Буферизованный ввод/вывод

Intel(R) Core(TM) i7-3630QM (2.4 ГГц), DDR3 (6 Гб), Windows 10 (64-бит)

Результаты

- Предложен режим работы блочных шифров для защиты информации на системных носителях — режим XEH.
- Для предложенного режима была получена нижняя оценка уровня информационной безопасности, превосходящая аналогичную оценку для режима XTS.
- Предложенный режим позволяет достичь преимущества более 35% в производительности в сравнении с подходом Encrypt-Mix-Encrypt и уступает не более 10% режиму XTS.

Направление дальнейших исследований

- Исследование возможности обеспечения нижних оценок уровня информационной безопасности за границей парадокса дней рождения (см. теорему 1).
- Исследование методами, отличными от методики редукционистской стойкости.
- Оптимизация производительности.

Спасибо за внимание!

Контактная информация

- Коренева Алиса Михайловна: A.Koreneva@securitycode.ru
- Фирсов Георгий Валентинович: G.Firsov@securitycode.ru