УДК 003.26
DOI: 10.25559/SITITO.18.202203.691-701

Оригинальная статья

Об одном режиме работы блочных шифров, используемом для защиты информации на носителях с блочно-ориентированной структурой

Г. В. Фирсов[1,2*], А. М. Коренева[3,2]
[1] ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
Адрес: 115409, Российская Федерация, г. Москва, Каширское шоссе, д. 31
[*] g.firsov@securitycode.ru
[2] ООО «Код Безопасности», г. Москва, Российская Федерация
Адрес: 129075, Российская Федерация, г. Москва, Мурманский проезд, д. 14, корп. 1
[3] ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», г. Москва, Российская Федерация
Адрес: 125167, Российская Федерация, г. Москва, пр. Ленинградский, д. 49/2

Аннотация
В 2021 году в Российской Федерации технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) принял методические рекомендации, определяющие режим работы блочных шифров (под названием DEC), используемый для защиты носителей информации с блочно-ориентированной структурой. Несмотря на ряд достоинств, режим DEC имеет эксплуатационные особенности, из-за чего востребован синтез альтернативных режимов для полнодискового шифрования, в частности, применимых для шифрования системных дисков. Известно, что в большинстве существующего ПО для шифрования системных дисков используется режим XTS, однако он имеет особенности, изучение которых является актуальной задачей. В настоящей работе предлагается методика оценки уровня информационной безопасности режимов работы блочных шифров с учётом специфики полнодискового шифрования и использованием техники доказуемой стойкости, рассматриваются некоторые атаки на режим XTS и предлагается его модификация – режим XEH (Xor-Encrypt-Hash), для которого получается нижняя граница оценки уровня информационной безопасности.

Ключевые слова: полнодисковое шифрование, режимы работы блочных шифров, блочные шифры, симметричная криптография, криптографическая защита информации, носители информации с блочно-ориентированной структурой, техника доказуемой стойкости

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Фирсов Г. В., Коренева А. М. Об одном режиме работы блочных шифров, используемом для защиты информации на носителях с блочно-ориентированной структурой // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 3. С. 691-701. doi: https://doi.org/10.25559/SITITO.18.202203.691-701

Original article

On One Block Cipher Mode of Operation Used to Protect Data on Block-Oriented Storage Devices

G. V. Firsov[a,b*], **A. M. Koreneva**[c,b]
[a] National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation
Address: 31 Kashirskoe shosse, Moscow 115409, Russian Federation
[*] g.firsov@securitycode.ru
[b] Securitycode, Moscow, Russian Federation
Address: 14 Murmanskij proezd, build. 1, Moscow 129075, Russian Federation
[c] Financial University under the Government of the Russian Federation, Moscow, Russian Federation
Address: 49/2 Leningradsky Prospekt, Moscow 125167, Russian Federation

Abstract
This research purpose is to develop a reduction-based method for analysis of cryptographic properties of block cipher modes of operation in context of full disk encryption (FDE) via provable security technique, to study weaknesses of widely spread among existing FDE solutions mode XTS through building an adversary, that breaks security of XTS, and then to create a variation of the mode, that fixes detected weaknesses. This new mode of operation is called XEH (Xor-Encrypt-Hash) and it uses "light-weight" polynomial permutation for mixing blocks of a sector after their "XTS-like" encryption. The proposed block cipher mode of operation does not require any space for additional data, and it allows us to use it for system disk encryption, unlike DEC mode proposed in the end of 2021 by TC 26. XEH was proved to be secure in a provable security model, which is described in this paper. This mode is compared with the existing ones, which can be used to encrypt block-oriented devices: it was shown, that XEH provides higher security bound, than other compared modes, and involves almost no degradation in performance with respect to XTS.

Keywords: full disk encryption, block cipher modes of operation, block ciphers, symmetric cryptography, data encryption, block-oriented storage devices, provable security

Conflict of interests: The authors declare no conflict of interest.

For citation: 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. doi: https://doi.org/10.25559/SITITO.18.202203.691-701

Введение

Для защиты данных от несанкционированного доступа используются средства защиты информации (СЗИ). При этом если для защиты информации используются криптографические методы (например, шифрование), то речь идет уже об использовании средств криптографической защиты информации (СКЗИ). Определяются несколько классов СКЗИ: КС1, КС2, КС3, КВ и КА[1]. К СКЗИ, в зависимости от класса, предъявляются разные требования. Соответствие разрабатываемого СКЗИ предъявляемым к нему требованиям проверяется и оценивается регулирующим органом.

Для классов СКЗИ, начиная с КС2 и выше, требуется обеспечить защиту от действий нарушителя (противника), который может осуществлять атаки, находясь внутри контролируемой зоны[2]. При наличии доступа противника в контролируемую зону, возникает также угроза кражи носителя информации. В связи с этим требуется обеспечить конфиденциальность хранимых данных при наличии у противника непосредственного доступа к носителю информации. Для решения данных задач в СКЗИ используется криптографическая подсистема с функцией полнодискового шифрования (ПДШ), то есть полного шифрования всех данных, расположенных на носителе информации.

В существующих на текущий момент технических решениях, используемых для ПДШ, чаще всего применяются симметричные блочные шифры[3]. С целью достижения возможности шифровать информацию произвольного размера, а не отдельные блоки, блочные шифры функционируют по определенной схеме, которая называется режимом работы блочных шифров [1, 2].

В контексте полнодискового шифрования на криптографическую подсистему накладываются определенные эксплуатационные ограничения, из-за чего использование изначально не предназначенных для шифрования носителей информации алгоритмов приводит к нарушению условий их криптографической стойкости. Таким образом, для обеспечения конфиденциальности и целостности данных на дисках требуется использование специально разработанных алгоритмов, в том числе и режимов работы блочных шифров [3].

В конце 2021 года в техническом комитете по стандартизации «Криптографическая защита информации» (ТК 26) завершилась разработка режима работы блочных шифров для защиты носителей информации с блочно-ориентированной структурой – Disk Encryption with Counter (DEC)[4]. Данный режим разрабатывался для достаточно сильной модели нарушителя[5], в связи с чем требует для своей работы относительно много дополнительных хранимых данных, что ухудшает его эксплуатационные характеристики. В связи с этим востребована разработка альтернативных режимов. Во многих существующих решениях для ПДШ используется режим XEX-based Tweaked-codebook mode with ciphertext Stealing (XTS)[6], который, однако, обладает некоторым слабостями, которые приводят к возможности построения атак на данный режим. Широта распространения режима XTS стала причиной выбора его в качестве базового при построении нового и учитывающего его особенности режима, что способствует более простому его внедрению в существующие решения.

Цель исследования

Целью настоящего исследования является разработка методики оценки уровня информационной безопасности режимов работы блочных шифров с учётом специфики полнодискового шифрования, определение целевых эксплуатационных и криптографических характеристик режима работы блочных шифров, используемого для полнодискового шифрования, а также синтез режима, обладающего заданными характеристиками.

Модель доказуемой стойкости, учитывающая особенности полнодискового шифрования

Полнодисковое шифрование отличается от шифрования сообщений, отправляемых, например, по некоторому каналу передачи данных. К подсистемам полнодискового шифрования (ПДШ) предъявляются повышенные требования эффективности, то есть скорости работы, так как обыкновенно подсистема ПДШ функционирует «между» файловой системой и драйвером носителя информации [4-9]. То есть интерфейс модуля

[1] Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности : приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 [Электронный ресурс]. URL: https://base.garant.ru/70727118 (дата обращения: 14.08.2022).

[2] Р 1323565.1.012-2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации: рекомендации по стандартизации: издание официальное: утверждены и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2017 г. № 2068-ст: введены впервые: дата введения 2018-05-01 / подготовлен Центром защиты информации и специальной связи ФСБ России. М. : Стандартинформ, 2018.

[3] VeraCrypt [Электронный ресурс]. URL: https://veracrypt.fr/en/Documentation.html (дата обращения: 14.08.2022); BitLocker overview [Электронный ресурс] // Microsoft, 2022. URL: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview (дата обращения: 14.08.2022).

[4] Р 1323565.1.042-2022 Информационная технология. Криптографическая защита информации. Режим работы блочных шифров, предназначенный для защиты носителей информации с блочно-ориентированной структурой: рекомендации по стандартизации: издание официальное: утверждены и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 01 декабря 2022 г. № 1285-ст: введены впервые: дата введения 2022-12-01 / подготовлен Центром защиты информации и специальной связи ФСБ России. М. : Стандартинформ, 2022.

[5] Богданов Д., Ноздрунов В. Шифрование носителей информации. Режим DEC [Электронный ресурс] // РусКрипто'2021. Ассоциация «РусКрипто», 2021. URL: https://www.ruscrypto.ru/resource/archive/rc2021/files/02_bogdanov_nozdrunov.pdf (дата обращения: 14.08.2022).

[6] Dworkin M. Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices. NIST Special Publication 800-38E. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2010. 9 p. [Электронный ресурс]. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904691 (дата обращения: 14.08.2022).

ПДШ обеспечивает так называемое «прозрачное» шифрование – для файловой системы модуль ПДШ как бы отсутствует. Операции доступа к диску являются наиболее затратными по времени операциями ввода-вывода[7]. Таким образом, подсистема ПДШ должна оказывать незначительное влияние на снижение производительности ОС.

Другой важной особенностью полнодискового шифрования является необходимость выделения некоторого пространства под дополнительные данные, необходимые для шифрования. Этими дополнительными данными могут являться имитовставки, синхропосылки, счетчики, используемые в режимах работы блочных шифров[8]. Это означает, что чем более «сильные» криптографические свойства требуется обеспечить, тем меньше становится объем пользовательских данных, который можно хранить на носителе информации.

При шифровании системных дисков проблема хранения дополнительных данных, необходимых для шифрования, может вовсе сводиться к отсутствию места под данную информацию, что требует использования шифрования, сохраняющего длину (т.н. length-preserving encryption).

Возможности нарушителя

При определении возможностей нарушителя будем исходить из принципа максимизации его возможностей при необходимости шифрования системного диска. Как было сказано выше, указанный сценарий использования подсистемы ПДШ не учитывает хранение дополнительных данных, таких как имитовставки и синхропосылки. Таким образом, обеспечение целостности методами имитозащиты не рассматривается в контексте данного исследования. Сосредоточимся на обеспечении конфиденциальности.

В качестве сценария атаки будем рассматривать кражу носителя информации. При этом полагаем, что перед изъятием носителя нарушитель может записать произвольные данные в произвольные расположения на носителе, пользуясь интерфейсом подсистемы ПДШ. Также в возможности нарушителя входит чтение произвольных данных из произвольного расположения напрямую с носителя, то есть в обход интерфейса подсистемы ПДШ. Такой тип атаки называется атакой на основе подобранного открытого текста (Chosen Plaintext Attack, сокращенно – CPA)[9] [10].

Известными нарушителю считаются:

– используемый шифр и его параметры (длина ключа, размер блока);
– используемый режим работы блочных шифров;
– при использовании настраиваемых шифров — все используемые настройки.

Неизвестной полагается только ключевая информация.

Целью нарушителя является раскрытие данных, хранимых на носителе информации. Рассмотрение более «сильных» нарушителей в рамках введенных эксплуатационных ограничений нецелесообразно. Пусть нарушитель способен записывать произвольные данные в произвольные расположения напрямую на носитель и считывать открытый текст через интерфейс подсистемы ПДШ. Данный тип атаки называется атакой на основе подобранного шифртекста (Chosen Ciphertext Attack, сокращенно – CCA)[10] [10]. Однако шифры, сохраняющие длину, не являются стойкими к атакам данного типа[11] [11-13].

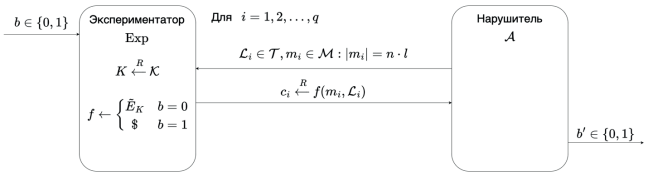
Формализация возможностей нарушителя

Для формализации возможностей нарушителя, описанных в предыдущем разделе, была выбрана модель доказуемой стойкости на основе неотличимости шифртекста от случайной битовой строки [14].

Прежде чем определить модель, которая будет использована в дальнейшем для анализа режимов работы блочных шифров, следует ввести некоторые обозначения. Через $\tilde{E}: \mathcal{K} \times \mathcal{M} \times \mathcal{T} \to \mathcal{C}$, где $\mathcal{M}$ – множество открытых текстов, $\mathcal{C}$ – множество шифртекстов, $\mathcal{K}$ – ключевое множество, $\mathcal{T}$ – множество настроек, обозначается семейство функций зашифрования настраиваемого шифра. При этом функцию зашифрования на конкретном ключе $K \in \mathcal{K}$ будем обозначать как $\tilde{E}_K$. Через $E: \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ обозначается семейство функций зашифрования блочного шифра, а функция зашифрования на конкретном ключе $K \in \mathcal{K}$ будет по аналогии записываться как E_K. Пара (E, E^{-1}) (или $(\tilde{E}, \tilde{E}^{-1})$) будет обозначаться через $\mathcal{E}$.

Для блочного шифра выполнено: $\mathcal{M} = \mathcal{C} = \{0,1\}^l$, где l – длина блока. Также обозначим длину сектора в блоках через n.

Определим теперь модель доказуемой стойкости на основе неотличимости шифртекста от случайной битовой строки – модель под названием RND-fdeCPA-sector. Рассмотрим вероятностный эксперимент, представленный на рисунке 1.



Р и с. 1. Вероятностный эксперимент модели RND-fdeCPA-sector

F i g. 1. Probabilistic experiment of the RND-fdeCPA-sector model

[7] Tanenbaum A., Austin T. Structured Computer Organization. 6th ed. Pearson, 2012. 808 p.

[8] Dworkin M. Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices. NIST Special Publication 800-38E. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2010. 9 p. [Электронный ресурс]. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904691 (дата обращения: 14.08.2022); ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 июня 2015 г. № 750-ст: введен впервые: дата введения 2016-01-01 / подготовлен Центром защиты информации и специальной связи ФСБ России, ОАО «ИнфоТеКС». М. : Стандартинформ, 2016.

[9] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. Wiley, 1996. 758 p.

[10] Там же.

[11] Bellare M., Rogaway P. Introduction to Modern Cryptography. San Diego: University of California, 2005 [Электронный ресурс]. URL: https://cseweb.ucsd.edu/~mihir/papers/br-book.pdf (дата обращения: 14.08.2022).

В эксперименте принимают два участника – экспериментатор Exp и нарушитель $\mathcal{A}$. Сам эксперимент состоит из трех стадий:

– *инициализация*, на которой случайно и равновероятно из множества {0,1} выбирается значение b – номер варианта эксперимента, неизвестный нарушителю, экспериментатор случайно и равновероятно выбирает ключ шифрования K, а также в зависимости от варианта эксперимента – функцию генерации ответа $f: \mathcal{M} \times \mathcal{T}$, которая при $b = 0$ полагается равной функции зашифрования на ключе K – $\tilde{E}_K$, а при $b = 1$ – функции \$, которая игнорирует свои аргументы и возвращает случайную битовую строку той же самой длины, которую возвращает $\tilde{E}_K$ на тех же аргументах;

– *ход эксперимента*. На этом этапе нарушитель отсылает $q \in \mathbb{N}$ запросов к экспериментатору, каждый из которых представляет собой пару $(m_i, \mathcal{L}_i) \in \mathcal{M} \times \mathcal{T}, i = \overline{1,q}$, где m_i – некоторый открытый текст длины nl, $\mathcal{L}_i$ – расположение на диске (например, номер сектора). Экспериментатор на каждый запрос отсылает ответ, состоящий из шифртекста $c_i \xleftarrow{R} f(m_i, \mathcal{L}_i)$, при этом данная запись подчеркивает возможный недетерминированный характер зашифрования;

– *завершение*. На данном этапе нарушитель на основе полученных от экспериментатора ответов возвращает значение $b' \in \{0,1\}$ – свою догадку о варианте эксперимента, выбранном на этапе инициализации.

На запросы нарушителя, генерируемые в ходе эксперимента, накладывается следующие ограничение:

$$\forall i, j \in \{1, \dots, q\} : i \neq j \Rightarrow (m_i, \mathcal{L}_i) \neq (m_j, \mathcal{L}_j), \qquad (1)$$

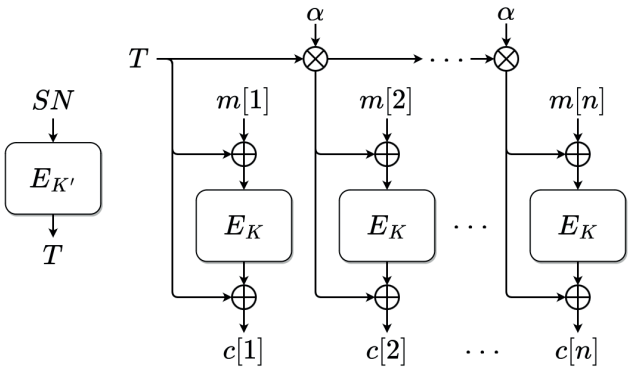
то есть в ходе одного и того же эксперимента запрещено для одного и того же расположения на диске запрашивать шифртекст для одного и того же открытого текста.

Мерой уровня информационной безопасности исследуемого настраиваемого шифра $\mathcal{E}$ принимается степень отличия стратегии нарушителя от случайного угадывания – преобладание нарушителя $\mathcal{A}$:

$$\mathbf{Adv}_{\mathcal{E}}^{\text{RND-fdeCPA-sector}}(\mathcal{A}) = \Pr[b' = 1 | b = 1] - \Pr[b' = 1 | b = 0]. \qquad (2)$$

Анализ криптографических характеристик режима XTS

Рассмотрим некоторые особенности режима работы блочных шифров XTS, которые позволяют построить атаки в рамках модели доказуемой стойкости RND-fdeCPA-sector. Функция зашифрования в режиме XTS изображена на рисунке 2. Через SN обозначается номер сектора, α – примитивный элемент поля $GF(2^l)$ [1] [12].



Р и с. 2. Функция зашифрования в режиме XTS

F i g. 2. Encryption function in XTS mode

Несложно отметить, что один и тот же блок на одной и той же позиции в секторе будет зашифрован в один и тот же блок шифртекста при условии использования одних и тех же ключей и номера сектора. Это видно из уравнения зашифрования i-го блока ($i = \overline{1,n}$):

$$c[i] = T_i \oplus E_K(m[i] \oplus T_i), \qquad (3)$$

где $T_i = T \otimes \alpha^{i-1}$.

Данная особенность приводит к построению атаки на режим XTS в модели доказуемой стойкости RND-fdeCPA-sector, что выражается в следующей теореме.

Теорема 1. Пусть $\mathcal{E}$ – блочный шифр с длиной блока l. Тогда существует нарушитель $\mathcal{A}$, который завершает работу за время, ограниченное сверху некоторой константой. При этом выполнено:

$$\mathbf{Adv}_{\text{XTS}^{\mathcal{E}}}^{\text{RND-fdeCPA-sector}}(\mathcal{A}) = 1 - 2^{-l}. \qquad (4)$$

В открытых комментариях к стандарту, определяющему режим XTS[2], приводится метод вычисления значения зашифрованного номера сектора на основе атаки по подобранному открытому тексту. Пусть найдены такие различные $k_1, k_2 \in \{1, \dots, n\}$, что в рамках одного сектора выполнено равенство:

$$m[k_1] \oplus c[k_1] = m[k_2] \oplus c[k_2], \qquad (5)$$

тогда с вероятностью $1 - 2^{-l}$ [11], [15] значение T может быть найдено из следующего уравнения:

$$T = (m[k_1] \oplus m[k_2]) \otimes (\alpha^{k_1 - 1} \oplus \alpha^{k_2 - 1})^{-1}. \qquad (6)$$

Данное свойство может быть использовано как для атаки на XTS в модели RND-fdeCPA-sector, так и для восстановления открытого текста [15, 16].

[12] IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices // IEEE Std 1619-2018 (Revision of IEEE Std 1619-2007). New York, NY: IEEE Computer Society, 2019. 41 p. doi: https://doi.org/10.1109/IEEESTD.2019.8637988

[13] Public Comments on the XTS-AES Mode. NIST, 2008. [Электронный ресурс]. URL: https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/comments/XTS/collected_XTS_comments.pdf (дата обращения: 14.08.2022).

Спецификация режима XEH

В докладе предлагается построить и оценить новый режим работы блочных шифров XEH, который является вариацией режима XTS. Целью его разработки является устранение особенностей режима XTS, приводящих к возможности построения атак на него.

Используемая схема универсального хэширования

Для того, чтобы показать нижнюю оценку уровня информационной безопасности режима XEH, используется свойство универсальности. Введем определение данного свойства, немного изменив его по сравнению с работой [17, 18].

Определение 1. Поблочно почти универсальная функция. Семейство функций $\mathcal{F}: \mathcal{K} \times \mathbb{F}^n \to \mathbb{F}^n$, где $\mathcal{K}$ – ключевое множество, $\mathbb{F}$ – некоторое поле, называется (ϵ_1, ϵ_2)-поблочно-почти-универсальным (block-wise almost universal, BAU), если:

$$\begin{aligned} \Pr_K\left[y[i] = y'[i']\right] \le \epsilon_1, i \ne i' \\ \Pr_K\left[y[i] = y'[i']\right] \le \epsilon_2, i = i' \end{aligned} \quad (7)$$

где $i, i' \in \{1, \dots, n\}$, $(y[1], \dots, y[n]) = \mathcal{F}(K, \mathbf{x})$, $(y'[1], \dots, y'[n]) = \mathcal{F}(K, \mathbf{x}'), \mathbf{x}, \mathbf{x}' \in \mathbb{F}^n, (\mathbf{x}, i) \ne (\mathbf{x}', i')$.

Определим две универсальные функции хэширования $f : \mathcal{K} \times \mathbb{F}^n \to \mathbb{F}^n$ и $g : \mathcal{K}^2 \times \mathbb{F}^n \to \mathbb{F}^n$, полагая при этом ключевое множество $\mathcal{K} = \mathbb{F}$. Также будем записывать: $f(\tau_2, x) = f_{\tau_2}(x)$ и $g(\tau_1, \tau_2, x) = g_{\tau_1,\tau_2}(x)$ для $\tau_1, \tau_2 \in \mathcal{K}$:

$$\begin{aligned} f_{\tau_2}(x) &= \left(x[1] + Y_{\tau_2}, \dots, x[n-1] + Y_{\tau_2}, Y_{\tau_2}\right) \\ Y_{\tau_2} &= \left(\sum_{j=1}^{n} x[j] \otimes \tau_2^{n-j}\right) \\ &\quad + \left(\sum_{j=1}^{n-1} x[j] \otimes j\right). \end{aligned} \quad (8)$$

На основе f определяется g следующим образом:

$$g_{\tau_1,\tau_2}(x) = f_{\tau_2}(x) + (\tau_1, \tau_1 \otimes \alpha, \dots, \tau_1 \otimes \alpha^{n-1}). \quad (9)$$

Лемма 1. Если $\tau_1 \xleftarrow{R} \mathcal{K}, \tau_2 \xleftarrow{R} \mathcal{K}$ и они независимы друг от друга, то g является $\left(\frac{1}{|\mathbb{F}|}, \frac{n-1}{|\mathbb{F}|}\right)$-BAU.

Определение режима XEH

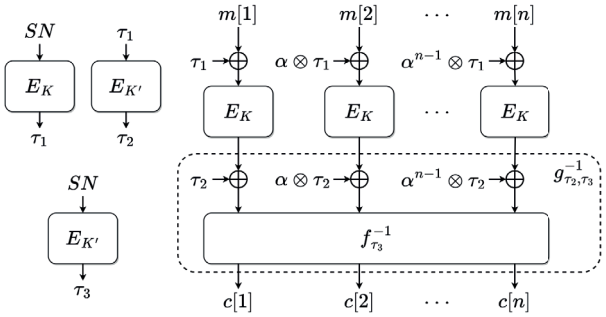
Режим XEH, как и XTS использует 2 ключа $K, K' \in \mathcal{K}$, где $\mathcal{K}$ – ключевое множество блочного шифра $\mathcal{E}$. Также режим использует 3 вспомогательных подключа $\tau_j, j \in \{1,2,3\}$, используемые в универсальной функции хэширования g, определенной в предыдущем подразделе (при этом $\mathbb{F} = GF(2^l)$). Данные подключи вырабатываются по следующему алгоритму:

$$\begin{aligned} \tau_1 &= E_K(SN) \\ \tau_2 &= E_{K'}(\tau_1) \\ \tau_3 &= E_{K'}(SN) \end{aligned} \quad (10)$$

где SN – номер сектора.

Функция зашифрования в режиме XEH изображена на рисунке 3. От режима XTS предлагаемая вариация отличается в двух местах:

– перед и после зашифрования блочным шифром к блоку прибавляются различные значения (маски): $\alpha^{j-1} \otimes \tau_1$ до зашифрования и $\alpha^{j-1} \otimes \tau_2$ – после ($j = \overline{1,n}$);
– блоки после зашифрования блочным шифром и применения маски поступают на вход частично примененной функции $f_{\tau_3}^{-1}$, выходные блоки которых являются итоговым шифртекстом.



Р и с. 3. Функция зашифрования в режиме XEH

F i g. 3. Encryption function in XEH mode

Оценка уровня информационной безопасности режима XEH

Для режима работы блочных шифров XEH получена нижняя оценка уровня информационной безопасности. Через $\mathbf{Adv}_{\mathcal{CS}}^{\text{MODEL-ATK}}(q)$ ($\mathbf{Adv}_{\mathcal{CS}}^{\text{MODEL-ATK}}(t, q)$) обозначается максимально возможное преобладание нарушителя, совершающего q запросов к экспериментатору (и завершает выполнение за время t) в вероятностном эксперименте в модели доказуемой стойкости MODEL-ATK против криптосистемы $\mathcal{CS}$.

Теорема 2. Пусть π – случайная подстановка на $GF(2^l)$. При фиксированных целых числах n, l и q верна нижняя оценка уровня информационной безопасности режима XEH:

$$\mathbf{Adv}_{\text{XEH}^\pi}^{\text{RND-fdeCPA-sector}}(q) \le \frac{(n+1)^2 q^2}{2^l}. \quad (11)$$

Теорема 3. Пусть $\mathcal{E}$ – симметричный блочный шифр с длиной блока l. При фиксированных целых числах n, l и q верна нижняя оценка уровня информационной безопасности режима XEH:

$$\begin{aligned} &\mathbf{Adv}_{\text{XEH}^\mathcal{E}}^{\text{RND-fdeCPA-sector}}(t, q) \\ &\quad \le \frac{(n+1)^2 q^2}{2^l} \\ &\quad + \mathbf{Adv}_{\mathcal{E}}^{\text{PRP}}(t', nq + q), \end{aligned} \quad (12)$$

где $t' = t + O(nq + q), q \to \infty$.

Сравнение с существующими режимами работы блочных шифров для ПДШ

Сравним предлагаемый режим XEH с существующими режимами, которые могут быть использованы для ПДШ. Критериями сравнения будут нижняя оценка уровня информационной безопасности, а также относительное время работы (по отношению к режиму XTS).

Для сравнения были выбраны следующие режимы:

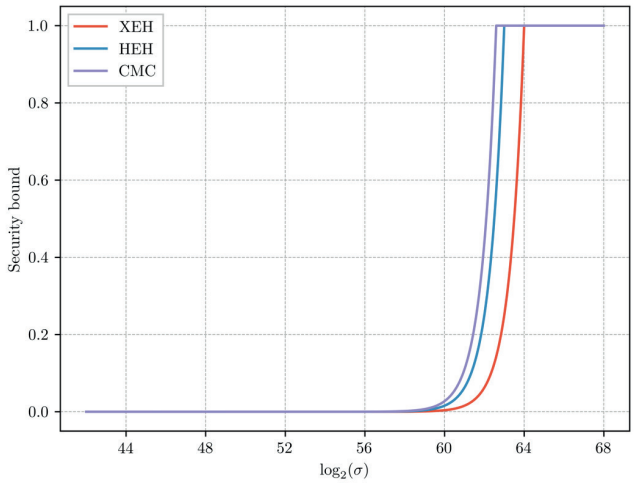
– XTS, как режим, который лег в основу предлагаемого, а также наиболее широко распространенный в существующих решениях для ПДШ. Кроме того, данный режим будет использоваться, как указано выше, в качестве «эталонного» значения времени работы;
– HEH (Hash-ECB-Hash), как режим, использующий похожую концепцию – применяющий полиномиальную

подстановку к шифруемым блокам, но при этом являющийся реализацией NR-схемы [19-21];

– CMC (CBC-Mask-CBC), как режим, использующий альтернативный подход к перемешиванию блоков – зашифрование в режиме CBC дважды с проходом по последовательности блоков в противоположных направлениях и сложением с маской между проходами [22, 23].

Отметим, что все эти режимы позволяют построить сохраняющий длину настраиваемый шифр с использованием симметричного блочного шифра [11], [18], [24, 25].

На рисунке 4 изображены нижние оценки уровня информационной безопасности для режимов XEH, HEH и CMC при использовании блочного шифра с размером блока l=128 бит в логарифмическом масштабе в зависимости от суммарной сложности запросов – величины σ, определяемой как количество блоков, зашифрованных нарушителем на одном ключе шифрования. В случае режима XEH $\sigma=(n+1)q$, так как на каждом запросе на ключе зашифровывается n+1 блок (n блоков маскированного открытого текста, а также номер сектора для выработки подключа τ_1). Для режима XTS оценка уровня информационной безопасности на графике не показана, так как на данный режим была построена атака (теорема 1).



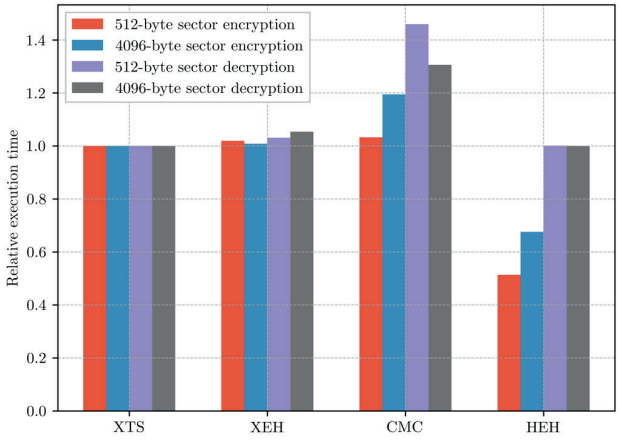
Р и с. 4. Оценки уровня информационной безопасности режимов XEH, HEH и CMC в зависимости от суммарной сложности запросов при использовании блочного шифра с размером блока l=128 бит

F i g. 4. Information security assessments of XEH, HEH and CMC modes depending on the cumulative complexity of queries when using a block cipher with a block size of l = 128 bits

По графику на рисунке 4 можно увидеть, что режим XEH обеспечивает более высокую нижнюю оценку уровня информационной безопасности (чем выше оценка, тем больше данных необходимо зашифровать нарушителю для достижения величины преобладания, которое не может считаться пренебрежимо малым).

На рисунке 5 изображена столбчатая диаграмма усредненного относительного времени, необходимого на зашифрование или расшифрование сектора размером 512 или 4096 байт при использовании режимов XTS, XEH, HEH и CMC. В качестве симметричного блочного шифра использовался шифр «Кузнечик»[14]. Так как время работы режима XTS принято за базовое значение, то соответствующие столбцы на диаграмме имеют высоту 1.

Отметим, что режим XEH работает в среднем работает дольше, чем XTS, однако разница в затраченном времени не превышает 6 процентов (при расшифровании сектора размером 4096 байт проигрыш относительно XTS является наибольшим и составляет 5.3 процента). Объясняется это применением полиномиальной подстановке к блокам сектора и выработкой дополнительных подключей.



Р и с. 5. Усредненное относительное время, затрачиваемое на зашифрование и расшифрование сектора размером 512 или 4096 байт с использованием симметричного блочного шифра «Кузнечик» и режимов XTS, XEH, CMC и HEH

F i g. 5. Average relative time spent on encryption and decryption of sector size 512 or 4096 bytes using symmetric block cipher "Grasshopper" and modes XTS, XEH, CMC and HEH

Наименее производительным оказался режим CMC, наибольший проигрыш по сравнению с режимом XTS составляет более 48 процентов (расшифрование сектора размером 512 байт). Связано это с тем, что в среднем полиномиальные подстановки для режимов XEH и HEH рассчитываются быстрее, чем происходит зашифрование того же объема данных в режиме CBC. В режиме XTS расчет полиномиальных подстановок и вовсе отсутствует.

Наиболее производительным решением оказался режим HEH, который выигрывает за счет меньшего количества умножений в поле $GL(2^l)$ по сравнению с режимами XEH и HEH.

[14] ГОСТ 34.12-2018 Информационная технология. Криптографическая защита информации. Блочные шифры: межгосударственный стандарт: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 4 декабря 2018 г. № 1061-ст: введен впервые: дата введения 2019-06-01 / подготовлен Центром защиты информации и специальной связи ФСБ России, ОАО «ИнфоТеКС». М. : Стандартинформ, 2018.

Заключение

В рамках данного исследования определены эксплуатационные ограничения, накладываемые спецификой полнодискового шифрования, а также максимально «широкие» возможности нарушителя, обеспечить защиту от которых теоретически возможно в рамках данных ограничений. Для формализации указанных возможностей нарушителя определена модель доказуемой стойкости на основе неотличимости шифртекста от случайной битовой строки, учитывающая важные особенности полнодискового шифрования, – модель RND-fdeCPA-sector.

В рамках модели RND-fdeCPA-sector построена атака на широко используемый в существующих решениях для ПДШ режим работы блочных шифров XTS, выявлены особенности режима, позволяющие построить атаку. С целью устранения данных особенностей на основе режима XTS разработан режим XEH, для которого получена нижняя оценка уровня информационной безопасности в рамках модели RND-fdeCPA-sector.

Произведено сравнение предложенного режима XEH с тремя существующими режимами, которые возможно использовать для ПДШ: XTS, HEH и CMC. Предложенный режим XEH незначительно уступает в производительности режиму XTS, широко распространенному среди существующих решений для ПДШ. Также он сильно уступает в производительности зашифрования режиму HEH, однако имеет более высокую нижнюю оценку уровня информационной безопасности по сравнению с остальными тремя. Полученные результаты могут быть востребованы разработчиками при синтезе систем ПДШ.

Приложение А

Доказательство теоремы 1

Доказательство состоит в прямом построении нарушителя и расчете его преобладания.

В ходе эксперимента нарушитель $\mathcal{A}$ отправляет два запроса к экспериментатору. В первом из них отправляется пара $(m_1, \mathcal{L})$, где $m_1 = m_1[1]||m_1[2]$, $\mathcal{L}$ – некоторое произвольное расположение на диске. Во втором запросе отправляется пара $(m_2, \mathcal{L})$, где $m_2 = m_2[1]||m_2[2]$ и $m_1[2] = m_2[2], m_1[1] \neq m_2[1]$.

Построенный набор запросов, очевидно, удовлетворяет условию (1). После получения ответов нарушитель возвращает $b' = [c_1[2] \neq c_2[2]]$. Рассчитаем преобладание нарушителя $\mathcal{A}$:

$$\mathbf{Adv}_{\mathrm{XTS}^{\varepsilon}}^{\mathrm{RND-fdeCPA-sector}}(\mathcal{A}) = \Pr[b' = 1|b = 1] - \Pr[b' = 1|b = 0] == 1 - 2^{-l}. \quad (13)$$

Теорема доказана.

Приложение Б

Доказательство теоремы 2

При доказательстве будет использована техника цепочки подстановок игр (экспериментов):

– в первой игре (*XEH*) экспериментатор зашифровывает пришедший ему открытый текст в режиме XEH, строя «на лету» подстановку π ∈ Perm(l), выбирая в качестве значения $\pi(x)$ для ранее не определенного x случайный еще неиспользованный элемент $GF(2^l)$;

– вторая игра (*RND1*) отличается от первой тем, что π более не обязана быть подстановкой и так же строится «на лету» путем выбора случайных элементов $GF(2^l)$ (необязательно неиспользованных). Таким образом, в области значений π (обозначается как $\mathcal{R}$) допустимы коллизии;

– в третьей игре (*RND2*) случайно выбираются отправляемые нарушителю блоки, а в качестве значений π берутся соответствующие блоки, полученные применением к сгенерированным блокам функции g_{τ_2,τ_3};

– последняя игра (*NON*) предназначена для ограничения сверху вероятности коллизии среди значений функции π. В данной игре нарушитель отправляет экспериментатору как открытый текст, так и соответствующий ему шифртекст. Предполагается, что он отсылает такие запросы, которые максимизируют вероятность коллизии в $\mathcal{R}$.

Основной (последний) этап доказательства состоит в анализе максимально возможной вероятности коллизии в выходах функции g_{τ_2,τ_3}.

Игра XEH. В данной игре нарушитель взаимодействует с экспериментатором, использующим режим XEH и некоторую подстановку $\pi \in Perm(l)$ в качестве блочного алгоритма.

Подстановка π будет строиться по следующему алгоритму:

– изначально берутся пустые множества $\mathcal{D}$ и $\mathcal{R}$;

– когда требуется получить значение $\pi(x)$ для $x \notin \mathcal{D}$, производятся следующие действия:

– $y \xleftarrow{R} GF(2^l)$ пока $y \in \mathcal{R}$;

– $\mathcal{R} \leftarrow \mathcal{R} \cup \{y\}$;

– $\mathcal{D} \leftarrow \mathcal{D} \cup \{x\}$;

– когда требуется получить значение $\pi(x)$ для $x \in \mathcal{D}$, возвращается соответствующее значение из множества $\mathcal{R}$.

Множества $\mathcal{D}$ и $\mathcal{R}$ упорядочены по моменту добавления в них значений, то есть:

$$\begin{gathered}\forall x, x' \in \mathcal{D}: x \prec x' \Leftrightarrow x \text{ добавлено } \mathcal{D} \text{ в раньше, чем } x' \\ \forall y, y' \in \mathcal{R}: y \prec y' \Leftrightarrow y \text{ добавлено } \mathcal{R} \text{ в раньше, чем } y'\end{gathered} \quad (14)$$

Данное свойство и позволяет сопоставить значению из $\mathcal{D}$ значение из $\mathcal{R}$.

Игра RND1. Отличие данной игры от предыдущей состоит в том, что при выборе значения $\pi(x)$ для нового значения x не производится проверка наличия его в $\mathcal{R}$. В связи с этим π необязательно является подстановкой, а $\mathcal{R}$ теперь представляет собой мультимножество.

Далее через $Coll_{i,\mathcal{R}}$ будем обозначать событие возникновения коллизии в мультимножестве $\mathcal{R}$ в игре *RNDi* для $i \in \{1,2\}$.

Игры *XEH* и *RND1* идентичны для нарушителя пока в $\mathcal{R}$ отсутствуют коллизии:

$$\Pr[b' = 1|\mathrm{XEH}] - \Pr[b' = 1|\mathrm{RND1}] \leq \Pr[Coll_{1,\mathcal{R}}] \quad (15)$$

Игра RND2. Данная игра отличается от предыдущей тем, что выбирается не значение $\pi(x)$ для нового входа x, а генерируются случайно и равновероятно блоки $c_j[1], \ldots, c_j[n]$, $j = \overline{1,q}$, которые будут переданы нарушителю в качестве шифртекста. В $\mathcal{R}$ добавляются следующие значения: $(cc_j[1], \ldots, cc_j[n]) = g_{\tau_2,\tau_3}(c_j[1], \ldots, c_j[n])$.

Для нарушителя игры *RND1* и *RND2* идентичны, так как в обеих играх он получает случайные битовые строки в качестве шифртекста. Таким образом:

$$\Pr[b' = 1|\mathrm{RND1}] = \Pr[b' = 1|\mathrm{RND2}] \text{ и } \Pr[Coll_{1,\mathcal{R}}] = \Pr[Coll_{2,\mathcal{R}}] \quad (16)$$

Второе равенство выполнено в силу того, что g_{τ_2,τ_3} – биекция, а значит значения $cc_j[1],\dots,cc_j[n]$, $j=\overline{1,q}$ являются так же случайными и равновероятными. Отметим, что в игре *RND2* нарушитель получает случайную битовую строку в качестве ответа на свой запрос, а значит:

$$\Pr[b'=1|\text{RND2}]=\Pr[b'=1|b=1] \quad (17)$$

Теперь оценим преобладание нарушителя:

$$\begin{aligned}&\mathbf{Adv}_{\text{XEH}^\pi}^{\text{RND-fdeCPA-sector}}(\mathcal{A})\\&=\Pr[b'=1|b=1]\\&-\Pr[b'=1|b=0]=\\&=\Pr[b'=1|\text{XEH}]\\&-\Pr[b'=1|\text{RND2}]=\\&=\Pr[b'=1|\text{XEH}]\\&-\Pr[b'=1|\text{RND1}]\\&\le\Pr\left[Coll_{1,\mathcal{R}}\right]=\\&=\Pr\left[Coll_{2,\mathcal{R}}\right]\end{aligned} \quad (18)$$

Игра NON. Данная игра позволяет получить оценку вероятности коллизии в $\mathcal{R}$, то есть оценить сверху $\Pr\left[Coll_{2,\mathcal{R}}\right]$. Нарушитель направляет в каждом своем запросе теперь не только настройку и открытый текст, но и шифртекст. Пусть нарушитель A отправляет такие запросы, которые максимизируют вероятность $\Pr\left[Coll_{2,\mathcal{R}}\right]$. Это позволяет абстрагироваться от конкретного нарушителя $\mathcal{A}$ и перейти к количеству используемых ресурсов – фактически количеству запросов к экспериментатору. В связи с этим производится переход к обозначению

Мультимножество $\mathcal{R}$ состоит из значений: $\tau_{1,j}$ и $\left(cc_j[1],\dots,cc_j[n]\right)=g_{\tau_2,\tau_3}\left(c_j[1],\dots,c_j[n]\right)$ для $j=\overline{1,q}$, где $\left(c_j[1],\dots,c_j[n]\right)$ – шифртекст, отправленный нарушителем.

Для удобства анализа представим значения $\left(cc_j[1],\dots,cc_j[n]\right)$, $j=\overline{1,q}$ в виде набора из p матриц, в каждой из которых собраны значения, рассчитанные для одного и того же расположения на диске (номера сектора). Матрицы имеют следующий вид:

$$\begin{bmatrix}cc_{k_1}[1] & \cdots & cc_{k_1}[n]\\ \vdots & \ddots & \vdots\\ cc_{k_{q_j}}[1] & \cdots & cc_{k_{q_j}}[n]\end{bmatrix} \quad (19)$$

где $j=\overline{1,p}$, q_j – количество запросов, в которых использовалось одно и то же расположение на диске. Отметим, что $\sum_{j=1}^{p}q_j$.

Оценим вероятность коллизии внутри сформированных матриц для блоков из одного и того же столбца. Всего можно сформировать $n\cdot C_{q_j}^2$, $j=\overline{1,p}$ пар таких блоков в рамках j-й матрицы. Действительно, всего в матрице (18) имеется n столбцов, в каждом из которых по q_j элементов, тогда в каждом таком столбце можно сформировать $C_{q_j}^2$ различных пар из элементов этого столбца. Вероятность коллизии в такой паре (по лемме 1) ограничена сверху значением $\frac{n-1}{2^l}<n/2^l$.

Тогда вероятность коллизии среди таких пар оценивается сверху следующим образом:

$$\begin{aligned}&\sum_{j=1}^{p}C_{q_j}^2 n\cdot\frac{n}{2^l}\le\sum_{j=1}^{p}\frac{q_j^2n^2}{2\cdot2^l}\\&\le\frac{n^2}{2\cdot2^l}\left(\sum_{j=1}^{p}q_j\right)^2\\&=\frac{1}{2}\cdot\frac{n^2q^2}{2^l}<\\&<\frac{1}{2}\cdot\frac{(n+1)^2q^2}{2^l}\end{aligned} \quad (20)$$

Теперь следует проанализировать все оставшиеся пары (также включающие значения $\tau_{1,j}$, $j=\overline{1,q}$). Количество таких пар, очевидно, не превосходит $C_{|\mathcal{R}|}^2\le|\mathcal{R}|^2/2$. Вероятность коллизии в такой паре не превосходит 2^{-l}.

Так как $|R|\le(n+1)q$, то вероятность коллизии среди таких пар не превосходит величины .

Таким образом, сложив данные оценки и подставив в (18), получаем требуемую оценку преобладания нарушителя, отправляющего на зашифрование q запросов:

$$\mathbf{Adv}_{\text{XEH}^\pi}^{\text{RND-fdeCPA-sector}}(q)\le\frac{(n+1)^2q^2}{2^l}. \quad (21)$$

Теорема доказана.

Приложение B

Доказательство теоремы 3

Доказательство сводится к построению нарушителя $\mathcal{B}$ в игре на стойкость PRP на основе имеющегося нарушителя $\mathcal{A}$ в игре на стойкость в модели RND-fdeCPA-sector.

Пусть нарушитель $\mathcal{A}$ работает за время t и отправляет экспериментатору q запросов. Нарушитель $\mathcal{B}$ работает следующим образом:

– на этапе инициализации генерирует новый ключ $K'\xleftarrow{R}\mathcal{K}$, где $\mathcal{K}$ – ключевое множество блочного шифра $\mathcal{E}$;

– в ходе эксперимента перехватывает запросы от $\mathcal{A}$ на зашифрование вида $\left(SN_j,\left(m_j[1],\dots,m_j[n]\right)\right)$, отправляет экспериментатору SN_j для зашифрования, после получения соответствующего шифртекста генерирует три вспомогательных подключа для режима XEH: τ_1, τ_2, τ_3, отправляет экспериментатору блоки $m_j[i]\oplus\tau_1\otimes\alpha^{i-1}$, $i=\overline{1,n}$ на зашифрование. К полученным блокам шифртекста применяется g_{τ_2,τ_3}^{-1}, а полученный результат возвращается нарушителю $\mathcal{A}$;

– на этапе завершения нарушитель $\mathcal{B}$ получает возвращаемое значение от $\mathcal{A}$ и возвращает его в качестве своего.

Оценим преобладание нарушителя $\mathcal{B}$, пользуясь результатом теоремы 2:

$$\begin{aligned}&\mathbf{Adv}_{\mathcal{E}}^{\text{PRP}}(\mathcal{B})=\Pr[\mathcal{B}^{\mathcal{E}}\to1]-\Pr[\mathcal{B}^{\pi}\to1]=\\&=\Pr\left[\mathcal{A}^{\text{XEH}^{\mathcal{E}}}\to1\right]-\Pr\left[\mathcal{A}^{\text{XEH}^{\pi}}\to1\right]=\\&=\left(\Pr\left[\mathcal{A}^{\text{XEH}^{\mathcal{E}}}\to1\right]-\Pr\left[\mathcal{A}^{\$}\to1\right]\right)\\&-\left(\Pr\left[\mathcal{A}^{\text{XEH}^{\pi}}\to1\right]-\Pr\left[\mathcal{A}^{\$}\to1\right]\right)=\\&=\mathbf{Adv}_{\text{XEH}^{\mathcal{E}}}^{\text{RND-fdeCPA-sector}}(\mathcal{A})\\&-\mathbf{Adv}_{\text{XEH}^{\pi}}^{\text{RND-fdeCPA-sector}}(\mathcal{A})\ge\\&\ge\mathbf{Adv}_{\text{XEH}^{\mathcal{E}}}^{\text{RND-fdeCPA-sector}}(\mathcal{A})\\&-\frac{(n+1)^2q^2}{2^l}.\end{aligned} \quad (22)$$

Очевидно, что нарушитель $\mathcal{B}$ совершает к своему экспериментатору $nq+q$ запросов, где q – количество запросов к экспериментатору нарушителя $\mathcal{A}$. Время работы нарушителя $\mathcal{B}$ составляет $t+O(nq+q)$, где t – время работы нарушителя $\mathcal{A}$.

Так как нарушитель $\mathcal{A}$ – произвольный, то рассмотренная схема построения нарушителя $\mathcal{B}$ является универсальной и позволяет абстрагироваться от конкретных нарушителей $\mathcal{A}$ и $\mathcal{B}$, сфокусировавшись сугубо на их ресурсах. Учитывая вышесказанное и перегруппировав слагаемые в неравенстве (22), несложно получить основное утверждение теоремы. Теорема доказана.

References

[1] Chakraborty D., Henríquez F.R. Block Cipher Modes of Operation from a Hardware Implementation Perspective. In: Koç Ç.K. (ed.) Cryptographic Engineering. Boston, MA: Springer; 2009. p. 321-363. doi: https://doi.org/10.1007/978-0-387-71817-0_12

[2] Sawka M., Niemiec M. A Sponge-Based Key Expansion Scheme for Modern Block Ciphers. *Energies*. 2022;15(19):6864. doi: https://doi.org/10.3390/en15196864

[3] Chakraborty D., López C.M., Sarkar P. Disk encryption: do we need to preserve length? *Journal of Cryptographic Engineering*. 2018;8(1):49-69. doi: https://doi.org/10.1007/s13389-016-0147-0

[4] Rogaway P. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In: Lee P.J. (ed.) Advances in Cryptology – ASIACRYPT 2004. ASIACRYPT 2004. Lecture Notes in Computer Science. Vol. 3329. Berlin, Heidelberg: Springer; 2004. p. 16-31. doi: https://doi.org/10.1007/978-3-540-30539-2_2

[5] Nawaz Y., Wang L., Ammour K. Processing Analysis of Confidential Modes of Operation. In: Wang G., Chen J., Yang L. (eds.) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2018. Lecture Notes in Computer Science. Vol. 11342. Cham: Springer; 2018. p. 98-110. doi: https://doi.org/10.1007/978-3-030-05345-1_8

[6] Khati L., Mouha N., Vergnaud D. Full Disk Encryption: Bridging Theory and Practice. In: Handschuh H. (ed.) Topics in Cryptology – CT-RSA 2017. CT-RSA 2017. Lecture Notes in Computer Science. Vol. 10159. Cham: Springer; 2017. p. 241-257. doi: https://doi.org/10.1007/978-3-319-52153-4_14

[7] Gjøsteen K. Security Notions for Disk Encryption. In: di Vimercati S.d.C., Syverson P., Gollmann D. (eds.) Computer Security – ESORICS 2005. ESORICS 2005. Lecture Notes in Computer Science. Vol. 3679. Berlin, Heidelberg: Springer; 2005. p. 455-474. doi: https://doi.org/10.1007/11555827_26

[8] Alekseev E.K., Akhmetzyanova L.R., Babueva A.A., Smyshlyaev S.V. Data Storage Security and Full Disk Encryption. *Applied Discrete Mathematics*. 2020;(49):78-97. (In Russ., abstract in Eng.) doi: https://doi.org/10.17223/20710410/49/6

[9] Bhargavan K., Leurent G. On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16). New York, NY, USA: Association for Computing Machinery; 2016. p. 456-467. doi: https://doi.org/10.1145/2976749.2978423

[10] Aizatulin M., Gordon A.D., Jürjens J. Extracting and verifying cryptographic models from C protocol code by symbolic execution. In: Proceedings of the 18th ACM conference on Computer and communications security (CCS'11). New York, NY, USA: Association for Computing Machinery; 2011. p. 331-340. doi: https://doi.org/10.1145/2046707.2046745

[11] Rudnytskyi V., Korchenko O., Lada N., Ziubina R., Wieclaw L., Hamera L. Cryptographic encoding in modern symmetric and asymmetric encryption. *Procedia Computer Science.* 2022;207:54-63. doi: https://doi.org/10.1016/j.procs.2022.09.037

[12] Wang Y., Kumar A., Ha Y. FPGA-based high throughput XTS-AES encryption/decryption for storage area network. In: 2014 International Conference on Field-Programmable Technology (FPT). Shanghai, China: IEEE Computer Society; 2014. p. 268-271. doi: https://doi.org/10.1109/FPT.2014.7082791

[13] Rackoff C., Simon D.R. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In: Feigenbaum J. (ed.) Advances in Cryptology – CRYPTO '91. CRYPTO 1991. Lecture Notes in Computer Science. Vol. 576. Berlin, Heidelberg: Springer; 1992. p. 433-444. doi: https://doi.org/10.1007/3-540-46766-1_35

[14] Dent A.W. Fundamental Problems in Provable Security and Cryptography. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences.* 2006;364(1849):3215-3230. doi: https://doi.org/10.1098/rsta.2006.1895

[15] Isobe T., Minematsu K. Plaintext Recovery Attacks Against XTS Beyond Collisions. In: Paterson K., Stebila D. (eds.) Selected Areas in Cryptography – SAC 2019. SAC 2019. Lecture Notes in Computer Science. Vol. 11959. Cham; Springer; 2020. p. 103-123. doi: https://doi.org/10.1007/978-3-030-38471-5_5

[16] Liskov M., Rivest R.L., Wagner D. Tweakable Block Ciphers. In: Yung M. (ed.) Advances in Cryptology – CRYPTO 2002. CRYPTO 2002. Lecture Notes in Computer Science. Vol. 2442. Berlin, Heidelberg: Springer; 2022. p. 31-46. doi: https://doi.org/10.1007/3-540-45708-9_3

[17] Halevi S. Invertible Universal Hashing and the TET Encryption Mode. In: Menezes A. (ed.) Advances in Cryptology – CRYPTO 2007. CRYPTO 2007. Lecture Notes in Computer Science. Vol. 4622. Berlin, Heidelberg: Springer; 2007. p. 412-429. doi: https://doi.org/10.1007/978-3-540-74143-5_23

[18] Gagné M., Lafourcade P., Lakhnech Y., Safavi-Naini R. Automated Security Proof for Symmetric Encryption Modes. In: Datta A. (ed.) Advances in Computer Science – ASIAN 2009. Information Security and Privacy. ASIAN 2009. Lecture Notes in Computer Science. Vol. 5913. Berlin, Heidelberg: Springer; 2009. p. 39-53. doi: https://doi.org/10.1007/978-3-642-10622-4_4

[19] Naor M., Reingold O. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *Journal of Cryptology*. 1999;12(1):29-66. doi: https://doi.org/10.1007/PL00003817

[20] Dementiev R., Sanders P., Schultes D., Sibeyn J. Engineering an External Memory Minimum Spanning Tree Algorithm. In: Levy J.J., Mayr E.W., Mitchell. J.C. (eds.) Exploring New Frontiers of Theoretical Informatics. IFIP International Federation for Information Processing. Vol. 155. Boston, MA: Springer; 2004. p. 195-208. doi: https://doi.org/10.1007/1-4020-8141-3_17

[21] Sarkar P. Efficient Tweakable Enciphering Schemes From (Block-Wise) Universal Hash Functions. *IEEE Transactions on Information Theory*. 2009;55(10):4749-4760. doi: https://doi.org/10.1109/TIT.2009.2027487

[22] Halevi S., Rogaway P. A Tweakable Enciphering Mode. In: Boneh D. (ed.) Advances in Cryptology – CRYPTO 2003. CRYPTO 2003. Lecture Notes in Computer Science. Vol. 2729. Berlin, Heidelberg: Springer; 2003. p. 482-499. doi: https://doi.org/10.1007/978-3-540-45146-4_28

[23] Bellare M., Rogaway P. On the Construction of Variable-Input-Length Ciphers. In: Knudsen L. (ed.) Fast Software Encryption. FSE 1999. Lecture Notes in Computer Science. Vol. 1636. Berlin, Heidelberg: Springer; 1999. p. 231-244. doi: https://doi.org/10.1007/3-540-48519-8_17

[24] Dolev D., Dwork C., Naor M. Non-malleable cryptography. *SIAM Journal on Computing*. 2000;30(2):391-437. doi: https://doi.org/10.1137/S0097539795291562

[25] Sagheer A.M. Counter Mode Development for Block Cipher Operations. *AL-Rafidain Journal of Computer Sciences and Mathematics*. 2009;6(1):133-144. doi: https://doi.org/10.33899/csmj.2009.163772

Поступила 14.08.2022; одобрена после рецензирования 27.09.2022; принята к публикации 09.10.2022.
Submitted 14.08.2022; approved after reviewing 27.09.2022; accepted for publication 09.10.2022.

Об авторах:

Фирсов Георгий Валентинович, магистрант Института интеллектуальных кибернетических систем, ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ» (115409, Российская Федерация, г. Москва, Каширское шоссе, д. 31); старший системный программист Отдела разработки решений для серверов и рабочих станций, ООО «Код Безопасности» (129075, Российская Федерация, г. Москва, Мурманский проезд, д. 14, корп. 1), **ORCID: https://orcid.org/0000-0001-5464-4045,** g.firsov@securitycode.ru

Коренева Алиса Михайловна, доцент Департамента информационной безопасности, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» (125167, Российская Федерация, г. Москва, пр. Ленинградский, д. 49/2); начальник отдела криптографического анализа, ООО «Код Безопасности» (129075, Российская Федерация, г. Москва, Мурманский проезд, д. 14, корп. 1), кандидат физико-математических наук, **ORCID: https://orcid.org/0000-0002-3186-0471,** A.Koreneva@securitycode.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the authors:

Georgii V. Firsov, Master degree student of the Institute of Cyber Intelligence Systems, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) (31 Kashirskoe shosse, Moscow 115409, Russian Federation); Senior Software Developer of the Department of Solutions Development for Servers and Workstations, Securitycode (14 Murmanskij proezd, build. 1, Moscow 129075, Russian Federation), **ORCID: https://orcid.org/0000-0001-5464-4045,** g.firsov@securitycode.ru

Alisa M. Koreneva, Associate Professor of the Department of Information Security, Financial University under the Government of the Russian Federation (49/2 Leningradsky Prospekt, Moscow 125167, Russian Federation); Head of Cryptographic Analysis Department, Securitycode (14 Murmanskij proezd, build. 1, Moscow 129075, Russian Federation), Cand.Sci. (Phys.-Math.), **ORCID: https://orcid.org/0000-0002-3186-0471,** A.Koreneva@securitycode.ru

All authors have read and approved the final manuscript.