МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Ахметзянова Лилия Руслановна

Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации

Специальность 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2022

Работа выполнена на кафедре информационной безопасности факультета Вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова».

Научный руководитель — *Логачев Олег Алексеевич*,
доктор физико-математических наук, старший научный сотрудник, кафедра информационной безопасности факультета Вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», доцент

Официальные оппоненты — *Запечников Сергей Владимирович*,
доктор технических наук, доцент, отделение интеллектуальных кибернетических систем офиса образовательных программ ФГБОУ ВО «Национальный исследовательский ядерный университет «МИФИ», профессор

— *Захаров Владимир Анатольевич*,
доктор физико-математических наук, кафедра математической кибернетики факультета Вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», профессор

— *Шишкин Василий Алексеевич*,
кандидат физико-математических наук, АО «НПК «Криптонит», руководитель лаборатории криптографии

Защита диссертации состоится 1 июня 2022 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.05.01 ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» по адресу: 119234, Москва, ГСП-1, Ленинские горы, д. 1, ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», Механико-математический факультет, аудитория 14-08.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на сайте ИАС «ИСТИНА»: `https://istina.msu.ru/dissertations/450040043/`

Автореферат разослан 29 апреля 2022 г.

Ученый секретарь
диссертационного совета МГУ.05.01,
к.ф.-м.н. Кривчиков

Максим Александрович

М. Кривчиков

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Задача одновременного обеспечения конфиденциальности и целостности является актуальной в контексте многих механизмов защиты данных. Примерами могут быть протоколы защищенной передачи отдельных сообщений в службах электронной почты, протоколы обеспечения защищенного канала связи для клиент-серверных приложений и защищенного хранения данных на носителях.

Одним из основных блоков при построении таких протоколов являются симметричные схемы защиты данных, предполагающие наличие общего секрета у отправителя и получателя информации. Исторически для одновременного обеспечения конфиденциальности и целостности использовались комбинации базовых симметричных схем, обеспечивающих отдельно конфиденциальность и целостность. Такой подход требовал наличия у сторон двух независимых общих секретов, что приводило к необходимости использования дополнительных механизмов для порождения данных секретов из одного общего; это, в свою очередь, ухудшало эксплуатационные характеристики целевых протоколов. Более того, представленные Белларе М. и Нампремпре К.[1] исследования безопасности указанного подхода показали, что не любая комбинация стойких базовых схем является безопасной. Данное обстоятельство не позволяло разработчикам программных средств защиты данных встраивать базовые стойкие механизмы без дополнительных исследований безопасности способа их комбинирования, а отсутствие данных исследований приводило к использованию нестойких решений[2].

Данные аспекты привели к возникновению самостоятельных механизмов, позволяющих одновременно обеспечивать конфиденциальность и целостность с использованием *одного секрета*. Такие механизмы называют схемами одновременного обеспечения конфиденциальности и целостности, или AE-схемами (аббревиатура от «Authenticated Encryption», «аутентифицированное шифрование»). В случае если такие схемы дополнительно позволяют обеспечивать только целостность для части входных данных, их называют AEAD-схемами («Authenticated Encryption with Associated Data», «аутентифицированное шифрование с ассоциированными данными»).

Примерами AEAD-схем являются схемы AES-CCM[3] и AES-GCM[4], являющиеся стандартами организации NIST (National Institute of Standards and Technology) или отраслевыми стандартами организации IETF/IRTF, определяющей механизмы и протоколы для сети Интернет. Данные схемы используются в протоколе TLS 1.3[5].

---

[1]Bellare M., Namprempre C. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm // Journal of Cryptology, Vol. 21, Pp. 469–491, 2008.

[2]Bellare M., Kohno T., Namprempre C. Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm // In Proceedings of ACM Transactions on Information and System Security, Vol. 7(2), Pp. 206–241, 2004.

[3]Whiting D., Housley R., Ferguson. N. Counter with CBC-MAC (CCM) // RFC 3610, 2003.

[4]Dworkin M. Recommendation for BlockCipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC // NIST Special Publication 800-38D, 2007.

Использование данных механизмов в протоколе TLS 1.3, который является одним из основных перспективных механизмов безопасности при обеспечении защиты соединений в сети Интернет, требует глубоких исследований AEAD-схем на предмет обеспечения ими целевых свойств безопасности с применением математических методов. Однако для возможности их применения первоначально необходимо формализовать целевой объект исследования и требуемые свойства.

С формальной точки зрения любая AEAD-схема определяется множеством секретов $\boldsymbol{K}$, множеством векторов инициализации $\boldsymbol{N}$, множеством открытых текстов $\boldsymbol{P}$, для которых необходимо обеспечить конфиденциальность и целостность, множеством ассоциированных данных $\boldsymbol{A}$, для которых необходимо обеспечить только целостность, множеством преобразованных текстов $\boldsymbol{C}$, множеством имитовставок/кодов целостности $\boldsymbol{T}$ и набором из следующих алгоритмов:

— Enc – алгоритм прямого преобразования данных, принимающий на вход значения $K \in \boldsymbol{K}$, $N \in \boldsymbol{N}$, $A \in \boldsymbol{A}$ и $P \in \boldsymbol{P}$ и возвращающий значения $C \in \boldsymbol{C}$, $T \in \boldsymbol{T}$;

— Dec – алгоритм обратного преобразования данных, принимающий на вход значения $K \in \boldsymbol{K}$, $N \in \boldsymbol{N}$, $A \in \boldsymbol{A}$, $C \in \boldsymbol{C}$, $T \in \boldsymbol{T}$ и возвращающий значение $P \in \boldsymbol{P}$ или символ ошибки $\perp$.

Свойства безопасности AEAD-схем. Формализация целевых свойств заключается в формировании строгих определений безопасности путем построения математической модели нарушителя, а именно моделирования его возможностей по взаимодействию с механизмом, его целей и ресурсов. В рамках диссертации применяется алгоритмический подход[6], заключающийся в построении вероятностного интерактивного алгоритма, моделирующего работу схемы в присутствии нарушителя, и определении количественной характеристики успешности нарушителя по реализации угрозы — преобладания нарушителя.

Для анализа свойств безопасности AEAD-схем относительно угроз нарушения конфиденциальности и целостности в 2008 году Белларе М. и Нампремпре К. были введены базовые определения безопасности[7]. Так, базовой моделью нарушителя для исследования конфиденциальности AEAD-схем является модель IND-CPA (indistinguishable under chosen plaintext attack, неотличимость относительно атаки с выбором открытых текстов), для целостности — INT-CTXT (integrity of ciphertext, целостность шифртекстов). При синтезе любых AEAD-схем их исследование в этих моделях является первостепенной задачей. Например, в рамках конкурса CAESAR[8], проводимого NIST и посвященного AEAD-

[5]Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3 // RFC 8446, 2018.

[6]Bellare M., Rogaway P. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs // Lecture Notes in Computer Science, Vol. 4004, Pp. 409–426, 2004

[7]Bellare M., Namprempre C. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm // Journal of Cryptology, Vol. 21, Pp. 469–491, 2008.

[8]Competition for Authenticated Encryption: Security, Applicability, and Robustnes // NIST, `https://competitions.cr.yp.to/caesar.html`

схемам, наличие анализа относительно данных определений являлось необходимым условием для всех конкурсантов.

Отметим, что исследования AEAD-схем не ограничиваются только базовыми определениями. Их использование для всё большего числа различных прикладных задач приводит к необходимости наличия у таких схем дополнительных свойств безопасности. В качестве примеров таких расширенных свойств можно привести обеспечение стойкости при обработке сообщений, зависящих от секрета (KDM-стойкость[9]), или при условии рассмотрения атак, позволяющих нарушителю получать открытые сообщения для невалидных с точки зрения целостности преобразованных сообщений (RUP-стойкость[10]). В настоящей работе в дополнение к базовым свойствам рассматривается свойство «misuse resistance»[11] («устойчивость при неправильном использовании»), которое характеризует стойкость режима в моделях, в которых нарушитель может навязывать повторное использование вектора инициализации для обработки сообщений. Как правило, контроль за уникальностью вектора инициализации возлагается на сторону отправителя, однако такая возможность есть не во всех приложениях. Например, ее нет в системах защищенного хранения данных на носителях, где отсутствует возможность безопасно хранить внутреннее состояние в оперативной памяти на протяжении всего срока эксплуатации. Действительно, владельцы защищаемых данных могут использовать различные вычислительные средства для чтения и записи данных на носитель или просто отключать вычислительное средство. Более того, повтор может возникнуть из-за ошибок в реализации или эксплуатации. Например, в системах, от которых требуется большая пропускная способность, часто используют технику виртуализации для распараллеливания потоков обработки данных. Данная техника предполагает копирование виртуальных машин, что может привести к использованию на каждой машине одинаковых начальных состояний и, как следствие, одинаковых значений векторов инициализации.

AEAD-режимы. В основе многих AEAD-схем лежит такой математический объект, как блочный симметричный алгоритм (далее — БСА) $E = \{E_K \in \mathcal{S}_{2^n} \mid K \in \{0,1\}^k\}$ — семейство эффективно вычислимых подстановок на множестве битовых строк фиксированной длины n (блоков), индексируемых битовыми строками длины k (секретами). При этом, секрет K, являющийся входом для алгоритмов AEAD-схемы, используется только в качестве индекса K, определяющего подстановку в семействе E. Отметим, что в таких схемах в качестве базового примитива может использоваться любой БСА с подходящими длиной секрета и длиной блока, поэтому часть конструкции AEAD-схемы, не зависящую от БСА, называют AEAD-режимом работы

[9]Black J., Rogaway P., Shrimpton T. Encryption-Scheme Security in the Presence of Key-Dependent Messages // In Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography (SAC '02), Pp. 62–75, 2002.

[10]Andreeva E. et al. How to securely release unverified plaintext in authenticated encryption // Lecture Notes in Computer Science, Vol. 8873, Pp. 105–125, 2014.

[11]Rogaway P., Shrimpton T. A provable-security treatment of the key-wrap problem // Lecture Notes in Computer Science, Vol. 4004, Pp. 373–390, 2006

блочного симметричного алгоритма. Такие режимы являются основным объектом исследования настоящей диссертации. Ранее упомянутые конструкции CCM и GCM являются AEAD-режимами.

Исследование AEAD-схем указанного выше типа на предмет обеспечения ими целевых свойств безопасности в тех или иных моделях нарушителя обычно проводится в предположении, что базовый БСА обладает свойством PRP-CPA (PseudoRandom Permutation under Chosen Plaintext Attack): при случайно равновероятно выбранном секрете K соответствующая подстановка E_K должна быть вычислительно неотличима от подстановки π, выбранной случайно равновероятно из множества всех подстановок $\mathcal{S}_{2^n}$ (далее для краткости подстановку π будем называть случайной подстановкой)[12]. Указанное предположение позволяет рассматривать соответствующий конкретной схеме AEAD-режим как набор функций Enc и Dec, в которых вместо подстановки E_K используется случайная подстановка π, не известная нарушителю. В таком случае AEAD-режим является уже комбинаторным объектом, для которого возможно получение не только нижних, но и верхних оценок преобладаний нарушителей, формально определяемых целевой моделью. Далее по тексту оценки указанного типа будем называть верхними/нижними оценками уровня информационной безопасности (стойкости) AEAD-режимов в определенной модели нарушителя, их доказательство путем исследования комбинаторных свойств конструкций является основной задачей настоящей диссертации. Отметим, что нижние оценки уровня стойкости режимов в моделях не являются соответствующими оценками для используемых на практике AEAD-схем с конкретным БСА, полученные в диссертации оценки характеризуют целевые свойства безопасности AEAD-схем, не зависящие от свойств конкретного БСА.

Как правило, исследование комбинаторных свойств AEAD-режимов заключается в получении верхних и нижних оценок преобладаний нарушителей в целевых моделях как функции от размера блока и количества обработанной информации. При встраивании данных механизмов в высокоуровневые протоколы количество информации, которое может быть обработано с использованием одного секрета, ограничивается для достижения необходимого уровня безопасности на основе полученных оценок (см. например, RFC 8446, раздел Limits on Key Usage[13]), так как в противном случае становятся возможными атаки[14], основанные на большом количестве полученной нарушителем информации. Однако в контексте современных приложений возможность обработки как можно большего количества данных с помощью одного секрета является критичной для эффективного функционирования на практике. Таким образом, улучшение комбинаторных свойств самих AEAD-режимов с сохранением их эксплуатационных качеств является актуальной задачей.

[12]Bellare M., Rogaway P. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs // Lecture Notes in Computer Science, Vol. 4004, Pp. 409–426, 2006.

[13]Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3 // RFC8446, 2018.

[14]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), Pp. 456–467, 2016.

Цель диссертационной работы — построение новых математических методов получения обоснованных оценок уровня информационной безопасности в целевых моделях нарушителя для существующих AEAD-режимов путем исследования комбинаторных свойств соответствующих конструкций, разработка новых AEAD-режимов с целью улучшения комбинаторных свойств и достижения новых свойств безопасности.

Для достижения поставленной цели были решены следующие задачи:

1) разработать методы получения верхних и нижних оценок уровня информационной безопасности в базовых моделях нарушителя для AEAD-режимов, рассматриваемых в рамках процесса стандартизации AEAD-режимов в Российской Федерации;

2) разработать новый AEAD-режим с целью достижения обоснованных свойств безопасности, соответствующих расширенным моделям нарушителя, учитывающих возможность повтора вектора инициализации;

3) разработать методы обоснованного улучшения комбинаторных свойств для существующих AEAD-режимов с целью увеличения объема безопасно обрабатываемых данных.

На защиту выносятся: обоснование актуальности, научная новизна, теоретическая и практическая значимость работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в заключении диссертации.

1) Метод нарушения свойства целостности AEAD-режима «8 бит» при обработке $2^{n/2}$ сообщений, где n – длина блока базового блочного симметричного алгоритма. Метод получения обоснованной нижней оценки уровня стойкости AEAD-режима MGM в базовой модели нарушителя для конфиденциальности (без повтора вектора инициализации).

2) AEAD-режим MGM2, являющийся модификацией режима MGM с целью улучшения его комбинаторных свойств. Метод получения обоснованных нижних оценок (улучшенных по сравнению с режимом MGM) его уровня стойкости в расширенных моделях нарушителя для конфиденциальности и целостности (с повтором вектора инициализации).

3) Методы модификации режима выработки имитовставки OMAC и AEAD-режима GCM с применением внутреннего преобразования секрета. Методы получения обоснованных нижних оценок уровня стойкости модифицированных режимов в целевых для механизмов указанного типа моделях нарушителя. Обоснование повышения их уровня информационной безопасности по сравнению с оригинальными режимами.

Научная новизна. В диссертации получены следующие новые результаты.

1) Для AEAD-режимов «8 бит» (модификации режима CCM) и MGM, которые рассматривались при стандартизации AEAD-режимов в России, были доказаны оценки уровня информационной безопасности. Для режима «8 бит» был разработан метод нарушения свойства целостности в модели INT-CTXT при обработке $2^{n/2}$ сообщений, который демонстрирует, что введенная его авторами модификация ухудшила свойства безопасности оригинального режима. Для режима MGM была доказана содержательная верхняя оценка преобладаний нарушителей, определяемых базовой моделью конфиденциальности (IND-CPA). Доказанная оценка показывает, что режим MGM обеспечивает стандартный для AEAD-режимов уровень стойкости в части конфиденциальности (в модели IND-CPA).

2) На основе режима MGM был разработан режим MGM2. Для данного режима были доказаны содержательные верхние оценки преобладаний нарушителей, определяемых расширенными моделями для целостности (MRAE-int) и конфиденциальности (CPA-res), которые учитывают возможность повторного использования вектора инициализации. Полученные результаты демонстрируют, что в сравнении с оригинальным режимом предложенная модификация обладает лучшими оценками уровня стойкости даже в более сильных моделях нарушителя.

3) На основе режима выработки имитовставки OMAC был разработан режим OMAC-ACPKM-Master с внутренним преобразованием секрета. Для данного режима была доказана содержательная верхняя оценка преобладаний нарушителей, определяемых моделью PRF (псевдослучайная функция). На основе AEAD-режима GCM был разработан режим GCM-ACPKM с внутренним преобразованием секрета. Для данного режима была доказана содержательная верхняя оценка преобладаний нарушителей, определяемых базовой моделью для целостности (INT-CTXT). Доказанные оценки демонстрируют, что разработанные режимы обладают лучшими комбинаторными свойствами в сравнении с оригиналами, что позволяет безопасно обрабатывать значительно больший объем данных без существенного ухудшения производительности.

Методология и методы исследования. В рамках исследования применяется математический аппарат и подходы различных разделов математики, таких как комбинаторная теория вероятностей, теория сложности вычислений и теория алгоритмов.

Степень достоверности. Достоверность полученных результатов обеспечивается строгими математическими доказательствами утверждений.

Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

Соответствие диссертации паспорту научной специальности. Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 05.13.19 (физико-математические науки) по следующим областям исследования:

1. теория и методология обеспечения информационной безопасности и защиты информации;

4. системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации;

9. модели и методы оценки защищенности информации и информационной безопасности объекта;

13. принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Апробация работы. Результаты, полученные в диссертации, докладывались на международных и всероссийских конференциях и научных семинарах:

- семинаре «Математические методы криптографического анализа» кафедры информационной безопасности факультета Вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова, 2018 год;
- семинаре «Математическая криптография и теория сложности вычислений» кафедры информационной безопасности факультета Вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова, 2019 год;
- VII международной научной конференции «Современные тенденции в криптографии» (CTCrypt 2018), Суздаль, 2018 год;
- VI международной научной конференции «Security Standardisation Research» (SSR 2020), Лондон, 2020 год;
- X международной научной конференции «Современные тенденции в криптографии» (CTCrypt 2021), Москва, 2021 год;
- VI международной научно-практической конференции «Современные информационные технологии и ИТ-образование», Москва, 2021 год.

Публикации по теме исследования. Результаты работы изложены в 5 публикациях в изданиях, индексируемых в Web of Science, Scopus, RSCI и из списка ВАК Минобрнауки России; из них 3 — в изданиях, индексируемых в Web of Science, Scopus, RSCI.

Теоретическая значимость. Для AEAD-режимов «8 бит» и MGM были изучены комбинаторные свойства лежащих в их основе математических конструкций и получены строгие доказательства оценок уровня информационной безопасности в релевантных математических моделях нарушителя. Полученные результаты позволяют сделать выводы о допустимости использования указанных математических конструкций при синтезе AEAD-режимов с точки зрения обеспечения целевых свойств безопасности.

Режим MGM2 был разработан с учетом возможности дальнейшего усовершенствования механизма для достижения новых свойств безопасности, что со-

здает фундамент для будущих исследований по синтезу и анализу более безопасных и эффективных AEAD-схем.

При синтезе и анализе механизмов с внутренним преобразованием секрета (режим OMAC-ACPKM-Master и режим GCM-ACPKM) были выявлены особенности применения подхода преобразования секрета для обеспечения целостности и развиты математические методы обоснования оценок уровня стойкости, которые ранее применялись только для исследования свойства конфиденциальности.

Практическая значимость. Внедрение исследованных и разработанных в настоящей диссертации механизмов в средства защиты информации решает практическую задачу обеспечения конфиденциальности и целостности информации в таких прикладных системах, как службы электронной почты, системы электронного документооборота, системы асинхронной передачи сообщений (мессенджеры), хранение данных на носителях. Полученные обоснованные оценки уровня информационной безопасности в релевантных моделях для указанных схем позволяют осуществлять выбор безопасных значений параметров эксплуатации схем. Также разработанные методы могут использоваться при подготовке учебных пособий и разработке лекционных курсов.

Доказанные результаты о свойствах режима MGM использовались при его стандартизации в Российской Федерации (Рекомендации по стандартизации Р 1323565.1.026-2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование»). Также режим MGM был описан в международном документе RFC 9058 сообщества IETF/IRTF, определяющего механизмы защиты информации в Интернете.

Разработанный режим OMAC-ACPKM-Master был стандартизирован в Российской Федерации (Рекомендации по стандартизации Р 1323565.1.017–2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»).

Разработанные режимы GCM-ACPKM и OMAC-ACPKM-Master стали частью международного документа RFC 8645, разработанного исследовательской группой CFRG сообщества IETF/IRTF.

Структура и объем диссертации. Диссертационная работа состоит из введения, двух вспомогательных разделов, трех глав, заключения, списка литературы из 43 наименований и приложения. Работа изложена на 157 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во Введении обоснована актуальность темы диссертации, сформулированы цели и задачи исследований, отражены научная новизна, теоретическая и практическая значимость полученных результатов, представлены основные результаты, которые выносятся на защиту.

В разделе Обозначения, определения и общие сведения вводятся используемые в работе общие обозначения и определения, а также приводятся общие

концепции, связанные с формированием модели нарушителя для схем защиты информации, и описывается предложенный в работе Белларе М. и Рогавея Ф.[15] алгоритмический подход к формализации данной модели. В рамках данного подхода формально вводятся объекты «нарушитель $\mathcal{A}$» и «экспериментатор **Exp**» — пара вероятностных интерактивных алгоритмов, взаимодействующих друг с другом определенным образом и моделирующих функционирование схемы в условиях присутствия нарушителя. Вводится понятие «преобладание нарушителя Adv» как мера успешности нарушителя при реализации угрозы.

Раздел Свойства безопасности AEAD-схем посвящен описанию свойств безопасности AEAD-режимов и их формализации. В данном разделе приводятся базовые и расширенные определения безопасности для AEAD-схем. В качестве базовых определений рассматриваются модели IND-CPA и INT-CTXT. Стойкость в модели IND-CPA означает, что нарушитель не может отличить преобразованный текст C и имитовставку T для любого выбранного им набора (вектор инициализации N, сообщение P, ассоциированные данные A), где значение N используется только один раз, от случайных равновероятных строк той же длины. Стойкость в модели INT-CTXT означает, что нарушитель, имеющий возможность получать значения C и T для любых выбранных им наборов (N, A, P), где значение N также используется только один раз, не может сформировать новый корректный набор (N, A, C, T).

Далее приводятся известные расширенные определения безопасности, которые учитывают возможность использования одинаковых значений векторов инициализации при обработке различных сообщений. Первым рассматривается определение безопасности MRAE (Misuse Resistant Authenticated Encryption), введенное Рогавеем Ф. и Шримптоном Т.[16] и являющееся расширением базовых определений безопасности IND-CPA и INT-CTXT на случай, когда снимаются условия на одноразовое использование вектора инициализации. Свойство конфиденциальности в соответствии с моделью нарушителя MRAE достаточно трудно обеспечить. Так, например, любые режимы, в которых сокрытие данных происходит с помощью секретного маскирования (например, режимы GCM и CCM), не обладают им, а известные стойкие в такой модели механизмы теряют эксплуатационные свойства (например, требуют большого количества вызовов БСА или теряют свойство параллельной обработки данных). Поэтому также приводится более слабое определение безопасности CPA-res для конфиденциальности, предложенное в 2017 году Ашуром Т., Дункельманом О. и Луксом А.[17]. Оно также является расширением базового определения безопасности, но подразумевает более слабое в сравнении с MRAE свойство: конфиденциальность должна быть обеспечена только для корректно обработанных сообщений с использованием уникального значения вектора инициализации.

[15]Bellare M., Rogaway P. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs // Lecture Notes in Computer Science, Vol. 4004, Pp. 409–426, 2004

[16]Rogaway P., Shrimpton T. A provable-security treatment of the key-wrap problem // Lecture Notes in Computer Science, Vol. 4004, Pp. 373–390, 2006

[17]Ashur T., Dunkelman O., Luykx A. Boosting authenticated encryption robustness with minimal modifications // In Proceedings of Annual International Cryptology Conference, Pp. 3–33, 2017.

Далее описывается объект исследований — AEAD-схемы на основе БСА (как частный случай AEAD-схем). Приводится стандартный[18] подход к анализу свойств таких AEAD-схем, при котором не рассматриваются свойства отдельно взятого БСА. Используемый AEAD-режим рассматривается как набор алгоритмов, фиксирующих порядок использования базовой подстановки при обработке данных. При этом предполагается, что подстановка выбирается случайно равновероятно из множества всех подстановок на двоичных строках длины n и используется как подпрограмма-«черный ящик». Другими словами, исследуется комбинаторный объект — AEAD-схема, в основе которого лежит не БСА E с длиной блока n, а множество всех подстановок $\mathcal{S}_{2^n}$ на множестве $\{0,1\}^n$. В данном разделе демонстрируется, что анализ свойств безопасности такого объекта сводится к анализу сложным образом определенных комбинаторных свойств режима, а также обосновывается целесообразность рассмотрения таких комбинаторных свойств при анализе стойкости целевого объекта исследований, использующего конкретный БСА.

В Главе 1 представлены результаты исследований комбинаторных свойств, соответствующих базовым свойствам безопасности, для двух AEAD-режимов — «8 бит» и MGM. Данные исследования были проведены в рамках процесса стандартизации AEAD-схем в Российской Федерации в 2017 году.

Режим «8 бит» был предложен в результате деятельности рабочей группы Технического комитета 26 по стандартизации. Он является модификацией режима CCM[19]. Особенность режима CCM заключается в том, что он потенциально позволяет обеспечить достаточный уровень стойкости в модели INT-CTXT при обработке более $2^{n/2}$ сообщений (обладает повышенным уровнем безопасности, или в английской литературе, «beyond birthday»-безопасностью[20]). Режим MGM, впервые представленный Ноздруновым В.И. на конференции CTCrypt в 2017 году, является оригинальной конструкцией и помимо БСА дополнительно использует такой алгебраический объект, как мультилинейная функция в поле $GF(2^n)$[21] .

В разделе 1.1 исследуются базовые комбинаторные свойства AEAD-режима «8 бит» с помощью метода построения конкретного нарушителя. Предлагается метод реализации угрозы нарушения целостности в модели INT-CTXT с вероятностью близкой к 1 при обработке $2^{n/2}$ сообщений (раздел 4 [1]). Данный результат послужил свидетельством того, что предлагаемый режим не обеспечивает «beyond birthday»-безопасность. Другими словами, было показано, что введенная модификация, заключающаяся в отсутствии дополнительного преобразования значения имитовставки, ухудшила комбинаторные свойства режима CCM. По результатам исследований, проведенных в настоящей диссертации,

[18]Bellare M., Desai A., Jokipii E., Rogaway P. A concrete security treatment of symmetric encryption // In Proceedings of 38th Annual Symposium on Foundations of Computer Science, Pp. 394–403, 1997.

[19]Whiting D., Housley R., Ferguson. N. Counter with CBC-MAC (CCM) // RFC3610, 2003.

[20]Jonsson J. On the Security of CTR + CBC-MAC // Selected Areas in Cryptography, 2002.

[21]Nozdrunov V. Parallel and double block cipher mode of operation (PD-mode) for authenticated encryption // In Proceedings of 6th Workshop on Current Trends in Cryptology (CTCrypt 2017).

режим «8 бит» был исключен из рассмотрения в качестве стандарта.

В разделе 1.2 исследуются базовые комбинаторные свойства режима MGM, соответствующие модели IND-CPA (конфиденциальность). Доказывается содержательная верхняя оценка преобладаний всех возможных нарушителей, определенных рассматриваемой моделью, как функция от размера блока n, количества обрабатываемых сообщений q, максимальной длины открытых текстов и ассоциированных данных в блоках l (теорема V.1 [5]). На основе полученных результатов для свойства конфиденциальности Карпуниным Г.А.[22] была также получена оценка уровня информационной безопасности в модели INT-CTXT (целостность). Совокупность данных результатов позволила установить, что режим MGM обеспечивает стандартный для AEAD-режимов уровень стойкости в базовых моделях нарушителя.

В Главе 2 представлены результаты исследований возможности модификации режима MGM с целью улучшения его комбинаторных свойств, а также обеспечения расширенных свойств безопасности, соответствующих моделям с возможностью повтора вектора инициализации.

После принятия режима MGM в качестве стандартизированного решения его повсеместное использование в различных протоколах привело к необходимости исследования других свойств безопасности. Так, в силу его использования в российской версии протокола ESP[23], являющегося частью протокола IPsec и предполагающего возможность распараллеливания потоков обработки данных с помощью техники виртуализации, актуальной стала задача исследования устойчивости режима MGM к повтору вектора инициализации в соответствующих моделях.

С точки зрения конфиденциальности, определяемой моделью MRAE, режим MGM является тривиально нестойким. С точки зрения целостности режим MGM был проанализирован Курочкиным А. и Фоминым Д.[24]: была предложена атака, требующая объема обработанных данных не меньше $2^{n/2}$ блоков, где n – битовый размер блока используемого БСА. Данный результат позволяет выдвинуть гипотезу о том, что режим MGM обладает достаточным уровнем безопасности в модели MRAE-int (целостность). Однако получение нижних оценок стойкости для MGM, необходимое для подтверждения данной гипотезы, все еще остается открытой задачей. В то же время, негативной особенностью конструкции режима MGM является возможность возникновения «опасных» коллизий между любыми возможными значениями входов в БСА, что существенно использовалось при построении указанной выше атаки. Поэтому с целью одновременного нивелирования указанного недостатка режима MGM и получения оценок стойкости в расширенной модели MRAE-int (целостность) была разра-

[22]Akhmetzyanova L. R., Alekseev E. K., Karpunin G. A., Nozdrunov V. I. Security of Multilinear Galois Mode (MGM) // In Cryptology ePrint Archive, Report 2019/123.

[23]Рекомендации по стандартизации Р1323565.1.035-2021 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе защиты информации ESP» // Москва, Стандартинформ, 2021.

[24]Kurochkin A., Fomin D. MGM Beyond the Birthday Bound // In Proceedings of 8th Workshop on Current Trends in Cryptology (CTCrypt 2019)

ботана модификация режима MGM.

В разделе 2.1 представлен результат разработки модификации – режим MGM2. В нем сохраняется ядро изначальной конструкции – мультилинейная функция, но изменяется процедура выработки секретных маскирующих значений и коэффициентов мультилинейной функции таким образом, чтобы минимизировать вероятность «опасных» коллизий между входами в БСА.

Проводится анализ расширенных комбинаторных свойств режима MGM2, соответствующих моделям MRAE (целостность) и CPA-res (конфиденциальность). В результате были доказаны содержательные верхние оценки преобладаний всех возможных нарушителей, определенных соответствующими моделями (теоремы IV.1 и IV.2 [4]). Данные результаты демонстрируют, что разработанный режим обладает лучшими оценками уровня стойкости даже в более сильных моделях нарушителя.

В Главе 3 решена задача увеличения объема данных, которые могут быть безопасно обработаны на одном секрете, путем улучшения комбинаторных свойств AEAD-режимов.

В начале главы приводится обзор подхода к улучшению свойств, называемого internal re-keying (внутреннее преобразование секрета)[25]. Данный подход заключается в модификации некоторого конкретного режима работы БСА таким образом, чтобы секрет, с помощью которого происходит непосредственное преобразование данных, периодически изменялся по ходу обработки одного сообщения. Применение данной техники к режимам обеспечения конфиденциальности исследовалось Смышляевым С.В.[26]. В данных работах был разработан режим обеспечения конфиденциальности CTR-ACPKM с внутренним преобразованием секрета CTR-ACPKM (расширение стандартного режима CTR, описанного в ГОСТ Р 34.13-2015[27]) и доказано, что данный подход существенно улучшает уровень стойкости в части обеспечения конфиденциальности, что позволяет увеличивать объем обрабатываемых данных.

В настоящей диссертации исследована возможность применения аналогичной техники для улучшения уровня стойкости в части обеспечения не только конфиденциальности, но и целостности, что является не менее важным в контексте использования AEAD-режимов. Так, изучена возможность применения данного метода для режима «8 бит» и зарубежного стандартного режима GCM.

Режим «8 бит» является комбинацией режима обеспечения конфиденциальности CTR и режима выработки имитовставки OMAC, описанных в ГОСТ Р 34.13-2015. Как указано выше, для режима CTR вопрос улучшения комбинаторных характеристик уже был исследован. Поэтому в настоящей работе исследовалась отдельная задача улучшения комбинаторных характеристик режима OMAC с помощью подхода внутреннего преобразования секрета.

---

[25]Smyshlyaev S. Re-keying Mechanisms for Symmetric Keys // RFC8645, 2019.

[26]Ahmetzyanova L. R., Alekseev E. K., Sedov G. K., Smyshlyaeva E. S., Smyshlyaev S. V. Practical significance of security bounds for standardized internally re-keyed block cipher modes // Математические вопросы криптографии, 10(2), 31–46, 2019.

[27]ГОСТ Р 34.13–2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» // Москва, Стандартинформ, 2015.

В разделе 3.1 разработан режим OMAC-ACPKM-Master и доказываются оценки его стойкости в стандартной модели PRF (теорема 2 [2]). Данные оценки показывают, что введенная модификация позволяет существенно увеличить допустимый объем безопасно обрабатываемых данных.

В разделе 3.2 для классического режима GCM предлагается модификация – режим GCM-ACPKM с внутренним преобразованием секрета. Внутреннее преобразование секрета применяется к оригинальному режиму GCM образом, аналогичным режиму CTR-ACPKM. Поэтому оценка преобладаний нарушителей, соответствующих базовой модели IND-CPA (теорема 1 [3]), является следствием оценки для режима CTR-ACPKM, полученной Смышляевым С.В.[28]. В настоящей диссертации доказывается содержательная верхняя оценка преобладаний нарушителей, соответствующих базовой модели INT-CTXT (теорема 2 [3]). Показывается, что введенная модификация позволяет существенно увеличить допустимый объем безопасно обрабатываемых с помощью GCM данных, при несущественном снижении эффективности.

В Заключении перечислены основные результаты диссертации.

В Приложении содержится доказательство технической леммы, используемой для оценки вероятности успеха нарушителя свойства целостности AEAD-режима «8 бит».

Заключение. Основные результаты диссертационной работы состоят в следующем.

1) Для AEAD-режимов «8 бит» и MGM, которые рассматривались в рамках процесса стандартизации AEAD-режимов в Российской Федерации, доказаны новые оценки уровня информационной безопасности. Для режима «8 бит» разработан метод, с помощью которого удалось показать, что режим не обеспечивает свойство целостности при обработке $2^{n/2}$ сообщений. Для режима MGM доказана содержательная верхняя оценка преобладаний нарушителей, определяемых базовой моделью конфиденциальности (IND-CPA). Таким образом, доказано, что режим MGM обеспечивает стандартный для AEAD-режимов уровень стойкости в части обеспечения конфиденциальности.

2) С целью улучшения свойств режима MGM разработана его модификация – режим MGM2. Для режима MGM2 доказаны содержательные верхние оценки преобладаний нарушителей, определяемых расширенными моделями для целостности (MRAE-int) и конфиденциальности (CPA-res), которые учитывают возможность повторного использования вектора инициализации. Полученные результаты демонстрируют, что в сравнении с оригинальным режимом предложенная модификация обладает лучшими оценками уровня стойкости в тех же и в более сильных моделях нарушителя.

[28] Ahmetzyanova L. R., Alekseev E. K., Sedov G. K., Smyshlyaeva E. S., Smyshlyaev S. V. Practical significance of security bounds for standardized internally re-keyed block cipher modes // Математические вопросы криптографии, 10(2), 31–46, 2019

3) На основе стандартизированных механизмов разработаны два режима работы блочного симметричного алгоритма с внутренним преобразованием секрета с целью увеличения объема безопасно обрабатываемых данных.

   На основе стандартизированного в Российской Федерации режима выработки имитовставки OMAC разработан режим OMAC-ACPKM-Master. Для данного режима доказана содержательная верхняя оценка преобладаний нарушителей, определяемых моделью PRF.

   Для AEAD-режима GCM, являющегося стандартом организации NIST, разработана модификация с внутреннем преобразования секрета. Для данной модификации, названной GCM-ACPKM, доказана содержательная верхняя оценка преобладаний нарушителей, определяемых базовой моделью для целостности (INT-CTXT).

   Доказанные оценки демонстрируют, что разработанные режимы позволяют обрабатывать сообщения большей длины без потери стойкости.

Разработанные в диссертации подходы могут применяться при разработке и исследованиях средств защиты информации, а также быть интересны специалистам в областях математических методов анализа систем и средств защиты информации, теории алгоритмов.

Благодарности. Автор диссертации выражает благодарность своему научному руководителю доктору физико-математических наук, старшему научному сотруднику Логачеву Олегу Алексеевичу за постановку задачи, постоянное внимание к работе и поддержку, а также доктору физико-математических наук Смышляеву Станиславу Витальевичу, старшему научному сотруднику Варновскому Николаю Павловичу, кандидату физико-математических наук Алексееву Евгению Константиновичу, кандидату физико-математических наук Карпунину Григорию Анатольевичу, кандидату физико-математических наук Ошкину Игорю Борисовичу, доктору физико-математических наук Михаилу Алексеевичу Черепневу, Ноздрунову Владиславу Игоревичу за полезные обсуждения и рекомендации. Автор также признателен заведующему кафедры Информационной безопасности ВМК МГУ имени М.В. Ломоносова академику Соколову Игорю Анатольевичу и всем ее сотрудникам за поддержку и внимание к диссертационной работе.

СПИСОК ПУБЛИКАЦИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» и входящих в базы цитирования Scopus, Web of Science и RSCI:

[1] Ahmetzyanova L.R. Near birthday attack on “8 bits” AEAD mode / Ahmetzyanova L. R., Karpunin G. A., Sedov G. K. // Математиче-

ские вопросы криптографии. 2019. Т. 10. № 2. С. 47–60 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Соавторам принадлежит доказательство вспомогательной леммы, используемой для оценки вероятности успешности атаки (доказательство утверждения Леммы 1 по тексту статьи). Остальные результаты статьи получены Ахметзяновой Л.Р. /

[2] Ahmetzyanova L.R. Practical significance of security bounds for standardized internally re-keyed block cipher modes / Ahmetzyanova L.R., Alekseev E.K., Sedov G.K., Smyshlyaeva E.S., Smyshlyaev S.V. // Математические вопросы криптографии. 2019. Т. 10. № 2. С. 31–46 (RSCI WoS, ИФ РИНЦ 2020: 0,327).
/ Ахметзяновой Л.Р. принадлежит синтез режима OMAC-ACPKM-Master и его анализ (доказательство утверждения Теоремы 2 по тексту статьи). Остальные результаты статьи получены соавторами. /

[3] Akhmetzyanova L. On Internal Re-keying / Akhmetzyanova L., Alekseev E., Smyshlyaev S., Oshkin I. // Lecture Notes in Computer Science, 2020, vol. 12529, pp. 23–45 (Scopus, ИФ SJR 2020: 0.249).
/ Ахметзяновой Л.Р. принадлежит конструкция режима GCM-ACPKM, доказательство утверждения Теоремы 2 (по тексту статьи), выводы о защищенности режима GCM-ACPKM в части обеспечения целостности, сравнение с базовым режимом GCM. Остальные результаты статьи получены соавторами. /

Публикации в рецензируемых научных изданиях, входящих в перечень ВАК Минобрнауки России:

[4] Ахметзянова Л.Р. MGM2: режим аутентифицированного шифрования, устойчивый к повтору вектора инициализации / Ахметзянова Л.Р., Алексеев Е.К., Бабуева А.А., Божко А.А., Смышляев С.В.// International Journal of Open Information Technologies. ISSN: 2307-8162. 2022. Т. 10. № 1. С. 6–14.
/ Соавторам принадлежит постановка задачи и сравнение режима MGM2 с оригинальным режимом. Остальные результаты статьи получены Ахметзяновой Л.Р. /

[5] Ахметзянова Л.Р. О свойстве конфиденциальности AEAD-режима MGM // International Journal of Open Information Technologies. ISSN: 2307-8162. 2022. Т. 10. № 3. С. 1–9.