Московский государственный университет имени М.В. Ломоносова
Факультет Вычислительной математики и кибернетики

На правах рукописи

Ахметзянова Лилия Руслановна

Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации

05.13.19 – Методы и системы защиты информации,
информационная безопасность

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
доктор физико-математических наук,
старший научный сотрудник
Логачев Олег Алексеевич

Москва – 2022

Оглавление

Введение

Общая характеристика работы. Диссертация посвящена задаче разработки симметричных схем одновременного обеспечения конфиденциальности и целостности информации и задаче получения для них обоснованных оценок уровня информационной безопасности. Данные схемы применяются в программных и аппаратных средствах защиты информации, используемых для обеспечения конфиденциальности и целостности данных при их передаче и хранении.

Разработка схем рассматриваемого типа и получение для них обоснованных оценок уровня информационной безопасности являются важными задачами как с практической, так и с теоретической точки зрения для обеспечения защиты информации. Так, при использовании таких схем в прикладных информационных системах наличие обоснованных оценок позволяет выбирать безопасные значения параметров эксплуатации, например, максимальное количество данных, которое разрешено обработать с помощью используемой схемы. При этом задача разработки схем сводится к поиску математических конструкций, которые позволяют обеспечивать наиболее высокий уровень информационной безопасности, а методы обоснования оценок уровня предполагают исследование комбинаторных и/или алгебраических свойств используемых конструкций и получение строгих доказательств в математических моделях, формально описывающих целевые свойства информационной безопасности и возможности нарушителей данных свойств.

В диссертации разработаны математические методы обоснования оценок уровня информационной безопасности для ряда схем, предложен-

ных в рамках процесса стандартизации схем обеспечения конфиденциальности и целостности информации в Российской Федерации; разработаны новые схемы указанного типа, для которых доказывается, что они обладают лучшими свойствам безопасности в сравнении с существующими аналогами. По результатам проведенных в настоящей диссертации исследований несколько механизмов стали частью документов отечественной и международной систем стандартизации.

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.

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

Актуальность темы. Задача одновременного обеспечения конфиденциальности и целостности является актуальной в контексте многих меха-

низмов 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 в работе [1] исследования безопасности указанного подхода показали, что не любая комбинация безопасных базовых схем является безопасной. Данное обстоятельство не позволяло разработчикам программных средств защиты данных встраивать базовые механизмы без дополнительных исследований безопасности способа их комбинирования, а отсутствие данных исследований приводило к использованию нестойких решений (см., например, [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], AES-GCM [4], ChaCha20-Poly1305 [5], 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 [6].

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 $\perp$.

Как правило, AEAD-схемы требуют, чтобы в рамках фиксированного секрета одно значение вектора инициализации использовалось для обработки только одного сообщения. Такие схемы называют «nonce-based» (Number used only ONCE) схемами (подробнее см. [7, 8]).

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, подробно описанный в [9] и 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 работе [1] были введены базовые определения безопасности. 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 [10], проводимого NIST и посвященного AEAD-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 [11]), или при условии рассмотрения атак, позволяющих нарушителю получать открытые сообщения для невалидных с точки зрения целостности преобразованных сообщений (RUP-стойкость [12]). В настоящей работе в дополнение к базовым свойствам рассматривается свойство «misuse resistance» [13] («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 сред-

ства 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 блочного симметричного алгоритма. Такие режимы являются основным объектом исследования настоящей диссертации. Ранее упомянутые конструкции CCM, 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 обла-

дает свойством PRP-CPA [9] (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). 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 становится 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 модели 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 некоторой модели нарушителя как функции от размера блока и количества обработанной информации. При встраивании данных механизмов в высокоуровневые протоколы количество информации, ко-

торое может быть обработано с использованием одного секрета, ограничивается для достижения необходимого уровня безопасности на основе полученных оценок (см. например, RFC 8446 [6], раздел Limits on Key Usage), так как в противном случае становятся возможными атаки (см. например, [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.

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 моде-

лям 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 модификация ухудшила свойства безопасности оригинального режима. Для режима MGM была доказана 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 обеспечения конфиденциальности (в модели IND-CPA).

2) На основе режима MGM был разработан режим MGM2. Для данного режима были доказаны 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 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 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.

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.

Публикации в рецензируемых научных изданиях, индексируемых в базах данных Web of Science (WoS), Scopus, RSCI:

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

[40] 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. /

[41] 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:

[42] 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. /

[43] 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.

Апробация работы. Результаты, полученные в диссертации, докладывались на международных и всероссийских конференциях и научно-исследовательских 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.

Теоретическая значимость. В ходе исследования получены результаты, существенно развивающие математические методы, применяемые при синтезе и анализе механизмов обеспечения конфиденциальности и целостности информации.

Для AEAD-режимов «8 бит» и MGM были изучены комбинаторные свойства лежащих в 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.

Синтез AEAD-режима MGM2 проводился, в том числе, с целью нивелирования отрицательных особенностей режима MGM, выявленных непосредственно при исследовании его комбинаторных свойств. Также режим MGM2 был разработан с учетом возможности дальнейшего усовершенствования механизма для достижения новых свойств безопасности, что создает 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 в соответствующих моделях, которые ранее применялись только для исследования свойства конфиденциальности в модели IND-CPA.

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 целевых для указанных схем моделях 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 работы

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

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 [9] алгоритмический подход к формализации данной модели. В рамках данного подхода формально вводятся объекты «нарушитель $\mathcal{A}$» и «экспериментатор $\mathbf{Exp}$» — 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, введенные в работе [1]. 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 и Шримптоном в работе [13] и являющееся расширением базовых определений безопасности IND-CPA и INT-CTXT на случай, когда снимаются условия на одноразовое использование вектора инициализации. Конфиденциальность, определенная моделью нарушителя MRAE, является достаточно трудно обеспечиваемым свойством. Так, например, любые режимы, в которых сокрытие данных происходит с помощью секретного маскирования (на-

пример, режимы GCM и CCM), не обладают им, а известные стойкие в такой модели механизмы теряют эксплуатационные свойства (например, требуют большого количества вызовов БСА [15] или теряют свойство параллельной обработки данных [16]). Поэтому также приводится более слабое определение безопасности CPA-res для конфиденциальности, предложенное в работе [17]. Оно также является расширением базового определения безопасности, но подразумевает более слабое в сравнении с MRAE свойство безопасности: конфиденциальность должна быть обеспечена только для корректно обработанных сообщений с использованием уникального значения вектора инициализации.

Далее описывается объект исследований — AEAD-схемы на основе БСА (как частный случай AEAD-схем). Приводится стандартный (см., например, [7]) 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 целевых моделях нарушителя (см. формулу (1)).

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 [18]. Он является модификацией режима CCM, описанного в [3]. 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, см. [19]). Режим MGM, впервые представленный Ноздруновым В.И. на конференции CTCrypt в 2017 году [20], является оригинальной конструкцией и помимо БСА дополнительно использует такой алгебраический объект, как мультилинейная функция в поле $GF(2^n)$.

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. 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, 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 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 1.2.1). На основе полученных результатов для свойства конфиденциальности в работе [21] Карпуниным Г.А. была также получена оценка уровня информационной безопасности в модели INT-CTXT (см. Теорема 1.2.4). Совокупность данных результатов позволила установить, что режим MGM обеспечивает стандартный для AEAD-режимов уровень стойкости в базовых моделях нарушителя. Полученные в настоящей диссертации результаты о свойствах режима MGM использовались при стандартизации данного режима в Российской Федерации [22].

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 в работе [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 разработана модификация режима MGM.

При разработке также выдвигалось следующее дополнительное требование по дальнейшему усовершенствованию режима: модифицированный режим должен удовлетворять требованиям для непосредственного применения SIV-конструкции, идея которой была предложена в работе [13], с целью достижения стойкости в полной модели MRAE (целостность и конфиденциальность).

В разделе 2.1 представлен результат разработки модификации – режим MGM2. В нем сохраняется ядро изначальной конструкции – муль-

тилинейная 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 верхние оценки преобладаний всех возможных нарушителей, определенных соответствующими моделями (Теорема 2.1.1 и Теорема 2.1.3). 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). Данный подход был описан в документе [28] и 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. в работах [40, 41]. В данных работах был разработан режим обеспечения конфиденциальности с внутренним преобразованием секрета CTR-ACPKM (расширение стандартного режима CTR, описанного в ГОСТ Р 34.13-2015) и доказано, что данный подход существенно улучшает уровень стойкости в части обеспечения конфиденциальности (в модели IND-

CPA), что позволяет увеличивать объем обрабатываемых данных.

В настоящей диссертации исследована возможность применения аналогичной техники для улучшения уровня стойкости в части обеспечения не только конфиденциальности (например, в модели IND-CPA), но и целостности (например, в модели INT-CTXT), 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.

В разделе 3.1 разработан режим OMAC-ACPKM-Master и доказываются оценки его стойкости в модели PRF [9] (pseudorandom function, псевдослучайная функция). 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 3.2.1), является следствием оценки для режима CTR-ACPKM, полученной Смышляевым С.В. в работе [40]. В настоящей диссертации

доказывается верхняя оценка преобладаний нарушителей, соответствующих базовой модели INT-CTXT (Теорема 3.2.2). Проводится сравнительный анализ полученных оценок с оценками из работ [26, 27] для оригинального режима. 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».

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.

Обозначения, определения и общие сведения

Через $\{0,1\}^u$ будем обозначать множество всех u-битовых строк, и через $\{0,1\}^*$ — множество всех битовых строк конечной длины. Битовую строку, состоящую из u нулей, будем обозначать через 0^u. Конкатенацию двух строк U и V будем обозначать через $U\|V$. Длину битовой строки U будем обозначать через $|U|$. Через $|U|_u = \lceil |U|/u \rceil$ обозначим длину битовой строки U в u-битовых блоках. Для произвольного множества $A \subseteq \{0,1\}^*$ через A_n обозначим множество всех строк $U \in A$, таких что $|U|$ кратно n и $|U| > 0$. Через $\{0,1\}^{\leqslant n}$ обозначим множество всех битовых строк, длина которых меньше или равна n.

Для битовой строки U и целого числа $0 < l \leqslant |U|$ через $\mathrm{msb}_l(U)$ ($\mathrm{lsb}_l(U)$) будем обозначать строку, состоящую из l крайних левых (правых) бит строки U. Для целых чисел $l > 0$ и $2^l > i \geqslant 0$ через $\mathrm{str}_l(i)$ будем обозначать l-битовое представление числа i, в котором наименее значащий бит находится справа. Для целого числа $l \geqslant 0$ и битовой строки $U \in \{0,1\}^l$ через $\mathrm{int}(U)$ будем обозначать целое число $i < 2^l$, такое что $\mathrm{str}_l(i) = U$. Для произвольного целого числа $u \geqslant 0$ определим функцию дополнения $\mathrm{pad}_u(U)$ строки $U \in \{0,1\}^*$ следующим образом: $\mathrm{pad}_u(U) = U$, если $u \mid |U|$ (u делит $|U|$); $\mathrm{pad}_u(U) = U\|10^{u|U|_u - |U| - 1}$ в противном случае.

Для множеств A и B через $Func(A,B)$ обозначим множество всех отображений множества A в множество B. Через $\mathcal{S}_{2^n}$ обозначим множество всех биективных отображений множества $\{0,1\}^n$ в себя, а через $\mathcal{F}_{2^n}$ — множество всех отображений множества $\{0,1\}^n$ в себя. Факт того, что значение s выбрано из некоторого множества S в соответствии с некото-

рым распределением $\mathfrak{D}$, будем обозначать через $s \xleftarrow{\mathfrak{D}} S$. Через $\mathcal{U}$ будем обозначать равномерное распределение.

Алгоритмический подход к формализации свойств безопасности. Одним из центральных понятий, используемых в рамках алгоритмического подхода, является «эксперимент» («experiment», «game» в англоязычной литературе). Под экспериментом подразумевается совокупность двух взаимодействующих друг с другом вероятностных алгоритмов — экспериментатора **Exp** («challenger» в англоязычной литературе) и нарушителя $\mathcal{A}$. Алгоритмы **Exp** и $\mathcal{A}$ можно формально описывать с помощью различных моделей вычислений, но обычно данные алгоритмы представляются в виде двух взаимодействующих друг с другом интерактивных машин Тьюринга, определение которых дано ниже.

Определение 0.1 ([29], [30])**.** Алгоритм $\mathcal{A}$ (вообще говоря, вероятностный) называется интерактивным, если он имеет (кроме других обычных лент, например, входной, выходной, рабочей) две выделенные ленты, называемые коммуникационными и обладающие следующими свойствами. Одна из этих лент (обозначим ее через $R_{\mathcal{A}}$) доступна только на чтение и служит для приема сообщений, а другая (обозначим ее через $S_{\mathcal{A}}$) доступна только на запись и служит для посылки сообщений. В любой момент вычисления алгоритм либо активен, либо находится в специальном состоянии, называемом состоянием ожидания. В период активности алгоритм производит обычные вычисления, включающие чтение с коммуникационной ленты $R_{\mathcal{A}}$ и запись на коммуникационную ленту $S_{\mathcal{A}}$. Информация, прочитанная с коммуникационной ленты $R_{\mathcal{A}}$ (записанная на коммуникационную ленту $S_{\mathcal{A}}$) в течение данного периода активно-

сти, называется сообщением, полученным (соответственно, посланным) алгоритмом в течение этого периода активности. Если же алгоритм находится в состоянии ожидания, то никакие вычисления не производятся; вывод алгоритма из этого состояния производится с помощью вспомогательной переменной другим интерактивным алгоритмом, совместно с котором производится вычисление.

Формализация модели нарушителя, в первую очередь, состоит в строгом описании алгоритма **Exp** (возможно, нескольких), моделирующего функционирование исследуемой системы $\boldsymbol{S}$ (например, работу «честных» участников протокола) в условиях присутствия нарушителя. Моделирование присутствия нарушителя осуществляется путем предоставления экспериментатором алгоритму $\mathcal{A}$ определенного интерфейса для взаимодействия с исследуемой системой, что позволяет нарушителю, например, влиять на ее внутреннее состояние или получать какую-либо информацию (например, результаты преобразования данных, подаваемых в качестве запросов). Данный интерфейс формализует первую компоненту модели — **тип атаки**. При этом нарушитель $\mathcal{A}$ явно не описывается (т.е. при задании эксперимента он является «черным ящиком»). Единственными предположениями о внутреннем устройстве алгоритма $\mathcal{A}$ является то, что он делает только корректные запросы к интерфейсам экспериментатора и возвращает ему только корректные ответы, для которых определен порядок его функционирования.

Процесс взаимодействия нарушителя и экспериментатора состоит из трех этапов: инициализации, запросов, финализации. На первом этапе производится инициализация параметров системы, например, экспе-

риментатор может выбирать ключ подписи и возвращать нарушителю соответствующий открытый ключ проверки подписи. На втором этапе нарушитель может делать запросы к определенным подпрограммам экспериментатора – оракулам (например, запросы на подписание сообщений) и получать от них соответствующие ответы. В ходе финализации экспериментатор обрабатывает данные, полученные от нарушителя, и возвращает значение $res \in \{0, 1\}$. Отметим, что при фиксации нарушителя $\mathcal{A}$ совокупность его и взаимодействующего с ним экспериментатора **Exp** — эксперимент — можно представить в виде одного вероятностного алгоритма, результатом работы которого является результат работы экспериментатора, т.е. значение res. Эксперимент, представленный в виде такого вероятностного алгоритма, обозначают через $\mathbf{Exp}(\mathcal{A})$. Заметим, что результат эксперимента является случайной величиной $\widetilde{res}$. Далее через $\mathbf{Exp}(\mathcal{A}) \to res$ будем обозначать событие, состоящее в том, что результатом эксперимента $\mathbf{Exp}(\mathcal{A})$ оказалось значение res или, другими словами, случайная величина $\widetilde{res}$ приняла значение res.

С помощью случайной величины $\widetilde{res}$ формализуется вторая компонента модели — **угроза**. Отметим, что качественная характеристика угрозы (например, факт подделки подписи) формализуется непосредственно при описании экспериментатора. Обычно это делается с помощью процедуры финализации, определяющей результат работы и наделяющей его смыслом. При этом количественная характеристика угрозы (например, вероятность подделки подписи) формализуется путем задания «меры успешности» нарушителя $\mathcal{A}$. Такая характеристика обычно называется *преобладанием* («advantage») нарушителя и обозначается через $\mathsf{Adv}(\mathcal{A})$.

Формализация **ресурсов** нарушителя, а именно – доступных ему объема информации и вычислительных ресурсов, осуществляется следующим образом. Объем информации определяется с помощью количественных ограничений его взаимодействий с экспериментатором. Например, при анализе симметричных схем обеспечения конфиденциальности ими могут быть максимальные количество осуществляемых нарушителем запросов на преобразование открытых текстов и длина (например, в битах) составляющих эти запросы текстов.

В зависимости от выбранной модели вычислений, вычислительные ресурсы нарушителя могут определяться по-разному. Например, в случае использования машины Тьюринга вычислительные ресурсы определяются количеством тактов работы нарушителя и размером его программы, зависящего от способа кодирования и измеряющегося, например, в элементарных командах или битах. Отметим, что ресурсы экспериментатора не включаются в затрачиваемые нарушителем ресурсы.

Таким образом, формальное определение модели нарушителя заключается в описании экспериментатора/ов, задании преобладания нарушителя и ограничений доступных ему объемов информации и вычислительных ресурсов. Отметим, что последние ограничения обычно не фиксируют и относят к параметрам модели, поэтому в результате формализации получается не одна модель, а целое параметризованное семейство моделей. При этом под термином «модель нарушителя» часто понимают именно данное семейство.

Для различения моделей, соответствующих экспериментаторов и преобладаний им присваиваются уникальные содержательные названия.

Некоторое название модели M может указываться в качестве верхнего индекса при обозначении экспериментатора — $\mathbf{Exp}^{\mathrm{M}}$ ($\mathbf{Exp}^{\mathrm{M\text{-}1}}/\mathbf{Exp}^{\mathrm{M\text{-}0}}$ в случае определения двух экспериментаторов) или использоваться в качестве непосредственного обозначения экспериментатора — вместо $\mathbf{Exp}^{\mathrm{M}}$ пишут просто M ($\mathrm{M}^1/\mathrm{M}^0$ соответственно). Если экспериментатор задавался для целого класса систем, то для фиксации алгоритма экспериментатора в качестве нижнего индекса при используемом обозначении экспериментатора указывают название конкретной системы $\boldsymbol{S}$ — $\mathbf{Exp}^{\mathrm{M}}_{\boldsymbol{S}}$ или $\mathrm{M}_{\boldsymbol{S}}$ (аналогично для двух экспериментаторов). Также для краткости под «нарушитель в модели M для системы $\boldsymbol{S}$» будем подразумевать нарушителя, согласованного с интерфейсом экспериментатора $\mathbf{Exp}^{\mathrm{M}}_{\boldsymbol{S}}$ (экспериментаторов $\mathbf{Exp}^{\mathrm{M\text{-}1}}_{\boldsymbol{S}}/\mathbf{Exp}^{\mathrm{M\text{-}0}}_{\boldsymbol{S}}$). При этом преобладание нарушителя $\mathcal{A}$ в модели M для системы $\boldsymbol{S}$ обозначается через $\mathsf{Adv}^{\mathrm{M}}_{\boldsymbol{S}}(\mathcal{A})$.

О релевантности моделей нарушителя. Любая математическая модель является упрощением реальности, поэтому некоторые свойства модели могут отличаться от свойств реального объекта. Как следствие, вывод о «стойкости» любого механизма в рамках выбранной модели нарушителя не гарантирует ее абсолютную «стойкость» на практике, так как она зависит от многих дополнительных факторов. Модель нарушителя может не учитывать какие-то его реальные качественные возможности и цели. Так, например, все используемые в диссертации модели явным образом исключают наличие у нарушителя таких возможностей, как получение дополнительной информации о секрете через побочные каналы по времени или внесение в реализацию «закладок» – функциональных объектов, которые при определенных условиях (входных данных)

инициируют выполнение функций, позволяющих осуществлять несанкционированные воздействия на информацию.

Отметим, что выбор модели нарушителя особенно важен при синтезе универсальных механизмов (например, в ходе разработки тех или иных стандартов). Это объясняется тем, что в таких условиях известны лишь наиболее общие характеристики высокоуровневых систем, которые будут использовать разрабатываемый механизм. От того, в какой модели нарушителя механизм является стойким, зависят требования к условиям его эксплуатации, а следовательно, и возможности по встраиванию его в высокоуровневые системы. AEAD-схемы, являющиеся основным объектом исследования диссертации, также являются универсальным механизмом. Поэтому в диссертации рассматриваются базовые модели нарушителя, которые покрывают внешних активных нарушителей, имеющих доступ только к каналу передачи данных между отправителем и получателем и не имеющих доступ к программно-аппаратному обеспечению, реализующему данные схемы. При встраивании AEAD-схем в системы, для которых рассматриваются нарушители с бóльшими возможностями, необходимо проведение дополнительных исследований.

Всюду по тексту диссертации под «стойкостью» механизма в модели нарушителя понимается наличие у механизма определенных математических свойств, которые строго задаются при формализации рассматриваемой модели. Отметим, что понятие «стойкость» может быть определено только в рамках некоторой формальной модели нарушителя, однако после слова «стойкость» словосочетание «в модели» иногда будет опускаться, если из контекста очевидно, какая именно модель нарушителя имеется в виду.

Свойства безопасности AEAD-схем

Определение 0.2. *AEAD-схемой* для множества секретов $\boldsymbol{K}$, множества векторов инициализации $\boldsymbol{N}$, множества открытых текстов $\boldsymbol{P}$, множества ассоциированных данных $\boldsymbol{A}$, множества преобразованных текстов $\boldsymbol{C}$ и множества имитовставок $\boldsymbol{T}$ является следующий набор функций:

- $\mathsf{Enc} : \boldsymbol{K} \times \boldsymbol{N} \times \boldsymbol{A} \times \boldsymbol{P} \to \boldsymbol{C} \times \boldsymbol{T}$.
- $\mathsf{Dec} : \boldsymbol{K} \times \boldsymbol{N} \times \boldsymbol{A} \times \boldsymbol{C} \times \boldsymbol{T} \to \boldsymbol{P} \cup \{\perp\}$.

В диссертации рассматриваются AEAD-схемы только для множеств $\boldsymbol{K}, \boldsymbol{N}, \boldsymbol{P}, \boldsymbol{A}, \boldsymbol{C}, \boldsymbol{T} \subseteq \{0,1\}^*$.

AEAD-схему Π будем называть *корректной*, если для любых $K \in \boldsymbol{K}$, $N \in \boldsymbol{N}$, $P \in \boldsymbol{P}$, $A \in \boldsymbol{A}$ и для $(C, T) = \Pi.\mathsf{Enc}(K, N, A, P)$ выполняется равенство $\Pi.\mathsf{Dec}(K, N, A, C, T) = P$. Далее для AEAD-схемы с длиной имитовставки s будем полагать, что $\boldsymbol{T} = \{0,1\}^s$.

Заметим, что в отличие от классических схем, обеспечивающих только конфиденциальность, результатом работы алгоритма обратного преобразования для AEAD-схемы может быть ошибка $\perp$, с помощью которой выявляется факт нарушения целостности принятого сообщения.

Отсутствие возможности обеспечения конфиденциальности режимами без вектора инициализации является известным общим результатом [7]. Однако требования, предъявляемые к вектору инициализации, могут различаться в зависимости от конкретного режима. Как правило, выделяют следующие требования:

- непредсказуемость;

- уникальность.

Будем называть вектор инициализации, единственным требованием к которому является уникальность, нонсом (nonce, Number used only ONCE, [8]).

Во всех нижеприведенных моделях корректным запросом к оракулу *Encrypt* (*Encrypt-b*) является набор (N, A, P), где $N \in \boldsymbol{N}$, $A \in \boldsymbol{A}$, $P \in \boldsymbol{P}$, корректным запросом к оракулу *Decrypt* является набор (N, A, C, T), где $N \in \boldsymbol{N}$, $A \in \boldsymbol{A}$, $C \in \boldsymbol{C}$, $T \in \boldsymbol{T}$. Для моделей, в которых исследуется свойство конфиденциальности, корректным ответом нарушителя является значение $b' \in \{0, 1\}$, а для моделей, в которых исследуется свойство целостности, нарушитель всегда должен возвращать значение 1.

Базовые свойства безопасности. Приведем базовые модели нарушителя, используемые для анализа стойкости AEAD-схем к угрозам нарушения конфиденциальности (модели IND-CPA и IND-CCA) и целостности (модель INT-CTXT) [1].

Для простоты изложения будем определять модели для AEAD-схем с нонсом.

Определение 0.3. [1] Преобладание нарушителя $\mathcal{A}$ в модели IND-CPA для AEAD-схемы Π с длиной имитовставки s определяется следующим образом:

$$\mathsf{Adv}_{\Pi}^{\text{IND-CPA}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_{\Pi}^{\text{IND-CPA-1}}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}_{\Pi}^{\text{IND-CPA-0}}(\mathcal{A}) \to 1\right],$$

где $\mathbf{Exp}_{\Pi}^{\text{IND-CPA-}b}(\mathcal{A}),\ b \in \{0, 1\}$, описываются следующим образом:

$\mathbf{Exp}_{\Pi}^{\text{IND-CPA-}b}(\mathcal{A})$	Oracle $\mathit{Encrypt}\text{-}b(N, A, P)$
$K \xleftarrow{\mathcal{U}} \boldsymbol{K}$	**if** $N \in \mathcal{L}$:
$\mathcal{L} \leftarrow \emptyset$	**return** $\perp$
$b' \leftarrow \mathcal{A}^{\mathit{Encrypt}\text{-}b}(\,)$	$(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$
return b'	**if** $b = 0$:
	$C \parallel T \xleftarrow{\mathcal{U}} \{0,1\}^{\lvert C\rvert+\lvert T\rvert}$
	$\mathcal{L} \leftarrow \mathcal{L} \cup \{N\}$
	return (C, T)

Ограничением в модели IND-CPA является запрет на подачу одинаковых запросов к оракулу *Encrypt*. Это объясняется тем, что в таком случае нарушитель тривиально различает случаи, когда оракул *Encrypt* реализует случай $b = 0$. В множестве $\mathcal{L}$ накапливаются все нонсы, поданные к оракулу *Encrypt*. В случае, если нарушитель дублирует нонс, ему возвращается ошибка.

Модель IND-CCA определяется похожим образом. Отличие состоит в том, что у нарушителя дополнительно появляется доступ к оракулу *Decrypt*, который всегда реализует «честное» обратное преобразование данных. При этом накладывается ограничение, что ответы оракула *Encrypt* нельзя подавать на вход оракулу *Decrypt*.

Определение 0.4. [1] Преобладание нарушителя $\mathcal{A}$ в модели IND-CCA для AEAD-схемы Π с длиной имитовставки s определяется следующим образом:

$$\mathsf{Adv}_{\Pi}^{\text{IND-CCA}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_{\Pi}^{\text{IND-CCA-1}}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}_{\Pi}^{\text{IND-CCA-0}}(\mathcal{A}) \to 1\right],$$

где $\mathbf{Exp}_{\Pi}^{\text{IND-CCA-}b}(\mathcal{A}), b \in \{0,1\}$ описываются следующим образом:

$\underline{\mathbf{Exp}_{\Pi}^{\text{IND-CCA-}b}(\mathcal{A})}$

$K \xleftarrow{\mathcal{U}} \boldsymbol{K}$

$sent, \mathcal{L} \leftarrow \emptyset$

$b' \leftarrow \mathcal{A}^{Encrypt\text{-}b, Decrypt}(\,)$

return b'

$\underline{\text{Oracle } Encrypt\text{-}b(N, A, P)}$

if $N \in \mathcal{L}$:

  return $\perp$

$(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$

if $b = 0$:

  $C \parallel T \xleftarrow{\mathcal{U}} \{0,1\}^{|C|+|T|}$

$sent \leftarrow sent \cup \{(N, A, C, T)\}$

$\mathcal{L} \leftarrow \mathcal{L} \cup \{N\}$

return (C, T)

$\underline{\text{Oracle } Decrypt(N, A, C, T)}$

if $(N, A, C, T) \in sent$:

  return $\perp$

$P \leftarrow \Pi.\mathsf{Dec}(K, N, A, C, T)$

return P

Модель INT-CTXT характеризует стойкость AEAD-схемы к угрозе построения подделки. В данной модели нарушителю предоставляется доступ к оракулам *Encrypt* и *Decrypt*. С помощью оракула *Decrypt* моделируется возможность нарушителя на практике подбирать и тестировать подделки. В данной модели нарушитель реализует угрозу, если он подает оракулу *Decrypt* валидный набор (N, A, C, T), который не был получен тривиальным образом с помощью оракула *Encrypt*.

Определение 0.5. [1] Преобладание нарушителя $\mathcal{A}$ в модели INT-CTXT для AEAD-схемы Π определяется следующим образом:

$$\mathsf{Adv}_{\Pi}^{\text{INT-CTXT}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_{\Pi}^{\text{INT-CTXT}}(\mathcal{A}) \to 1\right],$$

где $\mathbf{Exp}_{\Pi}^{\text{INT-CTXT}}(\mathcal{A})$ описываются следующим образом:

$\mathbf{Exp}_{\Pi}^{\text{INT-CTXT}}(\mathcal{A})$	Oracle $Encrypt(N, A, P)$	Oracle $Decrypt(N, A, C, T)$
$K \xleftarrow{\mathcal{U}} \boldsymbol{K}$	**if** $N \in \mathcal{L}$:	$P \leftarrow \Pi.\mathsf{Dec}(K, N, A, C, T)$
$sent, \mathcal{L} \leftarrow \emptyset$	**return** $\perp$	**if** $((N, A, C, T) \notin sent) \wedge (P \neq \perp)$:
$win \leftarrow 0$	$(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$	$win \leftarrow 1$
$1 \leftarrow \mathcal{A}^{Encrypt, Decrypt}(\,)$	$sent \leftarrow sent \cup \{(N, A, C, T)\}$	**return** P
return win	$\mathcal{L} \leftarrow \mathcal{L} \cup \{N\}$	
	return (C, T)	

Наиболее актуальными для практики являются модели INT-CTXT и IND-CCA. Однако в работах [1, 31] показывается, что из стойкости в моделях IND-CPA и INT-CTXT следует стойкость в модели IND-CCA. Поэтому при анализе свойств безопасности AEAD-схем стандартно рассматривают только модели IND-CPA и INT-CTXT.

Расширенные свойства безопасности. Приведем модели нарушителя, в рамках которых в настоящей диссертации будет исследоваться устойчивость AEAD-схем при повторном использовании вектора инициализации для обработки сообщений.

Приведем модель нарушителя MRAE-int («Misuse-Resistant Authenticated Encryption - integrity»), которая является частью модели MRAE, определенной в [13]. Стойкость в данной модели означает обеспечение целевой схемой свойства целостности при повторном использовании вектора инициализации.

Определение 0.6. [13] Преобладание нарушителя $\mathcal{A}$ в модели MRAE-int для AEAD-схемы Π определяется следующим образом:

$$\mathsf{Adv}_{\Pi}^{\text{MRAE-int}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_{\Pi}^{\text{MRAE-int}}(\mathcal{A}) \to 1\right],$$

где эксперимент $\mathbf{Exp}_{\Pi}^{\text{MRAE-int}}$ описан ниже:

$\mathbf{Exp}_{\Pi}^{\text{MRAE-int}}(\mathcal{A})$	Oracle $Encrypt(N, A, P)$	Oracle $Decrypt(N, A, C, T)$
$K \xleftarrow{\mathcal{U}} \boldsymbol{K}$	$(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$	$P \leftarrow \Pi.\mathsf{Dec}(K, N, A, C, T)$
$sent \leftarrow \emptyset$	$sent \leftarrow sent \cup \{(N, A, C, T)\}$	**if** $(P \neq \perp) \wedge ((N, A, C, T) \notin sent)$:
$win \leftarrow 0$	**return** (C, T)	$win \leftarrow 1$
$1 \leftarrow \mathcal{A}^{Encrypt, Decrypt}(\,)$		**return** P
return win		

Приведем модель нарушителя CPA-res («Chosen Plaintext Attack - resilience»), определенную в работе [17]. Данная модель является расширением базового определения безопасности для свойства конфиденциальности IND-CPA на случай, когда у нарушителя появляется возможность делать запросы с одинаковым значением нонса. При этом стойкость в данной модели означает, что конфиденциальность обеспечивается только для корректно обработанных сообщений с использованием уникального значения вектора инициализации.

Определение 0.7. [17] Преобладание нарушителя $\mathcal{A}$ в модели CPA-res для AEAD-схемы Π определяется следующим образом:

$$\mathsf{Adv}_{\Pi}^{\text{CPA-res}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_{\Pi}^{\text{CPA-res-1}}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}_{\Pi}^{\text{CPA-res-0}}(\mathcal{A}) \to 1\right],$$

где эксперименты $\mathbf{Exp}^{\text{CPA-res-}b}$, $b \in \{0, 1\}$, описаны ниже:

$\mathbf{Exp}_{\Pi}^{\text{CPA-res-}b}(\mathcal{A})$	Oracle $Encrypt_1(N, A, P)$	Oracle $Encrypt_2(N, A, P)$
$K \xleftarrow{\mathcal{U}} \boldsymbol{K}$	**if** $N \in \mathcal{L}_1 \cup \mathcal{L}_2$:	**if** $N \in \mathcal{L}_1$:
$\mathcal{L}_1, \mathcal{L}_2 \leftarrow \emptyset$	**return** $\perp$	**return** $\perp$
$b' \leftarrow \mathcal{A}^{Encrypt_1, Encrypt_2}(\,)$	$(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$	$(C, T) \leftarrow \Pi.\mathsf{Enc}(K, N, A, P)$
return b'	**if** $b = 0$:	**if** $N \notin \mathcal{L}_2$:
	$C \parallel T \xleftarrow{\mathcal{U}} \{0,1\}^{\lvert C\rvert + \lvert T\rvert}$	$\mathcal{L}_2 \leftarrow \mathcal{L}_2 \cup \{N\}$
	$\mathcal{L}_1 \leftarrow \mathcal{L}_1 \cup \{N\}$	**return** (C, T)
	return (C, T)	

В работе [17] также вводится модель нарушителя CCA-res («Chosen Ciphertext Attack - resilience»). Данная модель отличается от модели CPA-res тем, что она предоставляет дополнительный доступ к оракулу *Decrypt*, что является более релевантным с точки зрения практики. С помощью техники доказательства, описанной в [1, 31], легко показать что из стойкости в моделях MRAE-int и CPA-res следует стойкость в модели CCA-res. Поэтому далее будет рассматриваться только модель CPA-res.

Комбинаторные свойства AEAD-режимов работы блочных преобразований. В основе превалирующего количества AEAD-схем лежит такой математический объект, как блочный симметричный алгоритм (далее — БСА). Отметим, что в таких схемах в качестве базового примитива может использоваться любой БСА с подходящими параметрами, поэтому часть конструкции AEAD-схемы, не зависящую от БСА, называют AEAD-режимом работы блочного симметричного алгоритма.

Приведем стандартное формальное определение БСА и известные определения безопасности для данного объекта.

Определение 0.8. Под блочным симметричным алгоритмом (БСА) E с длиной блока n и длиной секрета k будем понимать произвольное семейство подстановок на множестве $\{0,1\}^n$, параметризованное параметром $K \in \{0,1\}^k$, т.е. $E = \left\{E_K \in \mathcal{S}_{2^n} \mid K \in \{0,1\}^k\right\}$. Параметр K в этом семействе E называется секретом БСА.

Приведем стандартные модели PRP-CPA («PseudoRandom Permutation») и PRF («PseudoRandom Function») [9], которые используются для оценки уровня стойкости БСА.

Определение 0.9. [9] Преобладание нарушителя $\mathcal{A}$ в модели PRP-CPA для БСА E с длиной блока n и длиной секрета k определяется следующим образом:

$$\mathsf{Adv}_E^{\text{PRP-CPA}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_E^{\text{PRP-CPA}-1}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}_E^{\text{PRP-CPA}-0}(\mathcal{A}) \to 1\right],$$

где эксперименты $\mathbf{Exp}_E^{\text{PRP-CPA}}(\mathcal{A}),\ b \in \{0,1\}$ определяются следующим образом:

$\underline{\mathbf{Exp}_E^{\text{PRP-CPA}-b}(\mathcal{A})}$	$\underline{\text{Oracle } \mathit{Encrypt}^b(M),\ M \in \{0,1\}^n}$
if $b = 1$:	**if** $b = 1$:
$K \xleftarrow{\mathcal{U}} \{0,1\}^k$	**return** $E_K(M)$
else :	**else** :
$\pi \xleftarrow{\mathcal{U}} \mathcal{S}_{2^n}$	**return** $\pi(M)$
$b' \leftarrow \mathcal{A}^{\mathit{Encrypt}^b}(\,)$	
return b'	

Определение 0.10. [9] Преобладание нарушителя $\mathcal{A}$ в модели PRF для БСА E с длиной блока n и длиной секрета k определяется следующим

образом:

$$\mathsf{Adv}_E^{\mathrm{PRF}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_E^{\mathrm{PRF}-1}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}_E^{\mathrm{PRF}-0}(\mathcal{A}) \to 1\right],$$

где эксперименты $\mathbf{Exp}_E^{\mathrm{PRF}}(\mathcal{A}),\ b \in \{0,1\}$ определяются следующим образом:

$\mathbf{Exp}_E^{\mathrm{PRF}-b}(\mathcal{A})$	Oracle $Encrypt^b(M),\ M \in \{0,1\}^n$
if $b = 1$:	**if** $b = 1$:
$K \xleftarrow{\mathcal{U}} \{0,1\}^k$	**return** $E_K(M)$
else :	**else** :
$F \xleftarrow{\mathcal{U}} \mathcal{F}_{2^n}$	**return** $F(M)$
$b' \leftarrow \mathcal{A}^{Encrypt^b}(\ )$	
return b'	

В работе [32] доказано следующее соотношение для преобладаний нарушителя в моделях PRF и PRP-CPA для БСА E.

Лемма 0.1 ([32] PRP/PRF switching lemma)**.** *Для любого БСА E с длиной блока n и любого нарушителя $\mathcal{A}$, определенного в моделях PRF и PRP-CPA, делающего не более q запросов к оракулу, справедливо*

$$\mathsf{Adv}_E^{\mathrm{PRF}}(\mathcal{A}) \leqslant \mathsf{Adv}_E^{\mathrm{PRP\text{-}CPA}}(\mathcal{A}) + \frac{q(q-1)}{2^{n+1}}.$$

При исследовании стойкости в тех или иных моделях нарушителя AEAD-схем $\Pi[E]$, являющихся комбинацией конкретного БСА E и конкретного AEAD-режима работы БСА Π, обычно применяется метод построения сведéний, идея которого заключается в следующем:

Для любого нарушителя $\mathcal{A}$, атакующего AEAD-схему в некоторой модели M*, строится нарушитель $\mathcal{B}$, атакующий БСА в модели*

PRP-CPA, *и находится соотношение между преобладаниями данных нарушителей.*

Вне зависимости от используемого AEAD-режима нарушитель $\mathcal{B}$ всегда строится одинаковым образом (см., например, [7, 13, 26]). Так как AEAD-режим Π всегда можно рассмотреть как набор алгоритмов, фиксирующий порядок использования определяемой секретом K базовой подстановки E_K при обработке данных, нарушитель $\mathcal{B}$ может моделировать экспериментаторов для AEAD-схем, где вместо вычисления значения базовой подстановки E_K он делает запрос к своему оракулу $Encrypt^b$. Таким образом,

1. если оракул $Encrypt^b$ реализует подстановку E_K для случайно равновероятно выбранного секрета K (то есть при $b = 1$), нарушитель $\mathcal{B}$ в точности моделирует эксперименты, определяемые моделью M для целевой схемы $\Pi[E]$;

2. если оракул $Encrypt^b$ реализует подстановку π, выбранную случайно равновероятно из множества $\mathcal{S}_{2^n}$ (то есть при $b = 0$), нарушитель $\mathcal{B}$ моделирует эксперименты, определяемые моделью M для комбинаторной конструкции $\Pi[\mathcal{S}_{2^n}]$.

При финализации нарушитель $\mathcal{B}$ возвращает тот же бит, что и соответствующий эксперимент, который он моделирует.

При этом преобладания нарушителей связаны следующим образом (соотношение выписано для моделей M, определяемых одним экспериментом; для моделей, определяемых двумя экспериментами, может быть

выписано аналогичное соотношение):

$$\begin{aligned}\mathsf{Adv}_E^{\text{PRP-CPA}}(\mathcal{B}) &= \Pr\left[\mathbf{Exp}_E^{\text{PRP-CPA}-1}(\mathcal{B}) \to 1\right] - \\ &= \Pr\left[\mathbf{Exp}_E^{\text{PRP-CPA}-0}(\mathcal{B}) \to 1\right] = \\ &= \Pr\left[\mathbf{Exp}_{\Pi[E]}^{\text{M}}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}_{\Pi[\mathcal{S}_{2^n}]}^{\text{M}}(\mathcal{A}) \to 1\right] = \\ &= \mathsf{Adv}_{\Pi[E]}^{\text{M}}(\mathcal{A}) - \mathsf{Adv}_{\Pi[\mathcal{S}_{2^n}]}^{\text{M}}(\mathcal{A}).\end{aligned}$$

Таким образом,

$$\mathsf{Adv}_{\Pi[E]}^{\text{M}}(\mathcal{A}) = \mathsf{Adv}_E^{\text{PRP-CPA}}(\mathcal{B}) + \mathsf{Adv}_{\Pi[\mathcal{S}_{2^n}]}^{\text{M}}(\mathcal{A}), \tag{1}$$

где количество запросов нарушителя $\mathcal{B}$ к оракулу $Encrypt^b$ всегда можно выразить через определяемые моделью M параметры нарушителя $\mathcal{A}$ для конкретного режима.

Согласно данной формуле, исследование стойкости конкретной схемы $\Pi[E]$, используемой на практике, в целевой модели нарушителя сводится к двум независимым этапам:

1. исследование свойств конкретного блочного БСА в базовой модели PRP-CPA (подобные исследования проводятся классическими методами и являются фундаментом для стойкости более высокоуровневых механизмов; опровержение предположения о стойкости некоторого БСА в базовой модели PRP-CPA неминуемо влечет его замену как базового примитива);

2. получение строгих оценок стойкости для режима в целевой модели нарушителя (со случайной подстановкой).

Путем получения нижних оценок для второго слагаемого в равенстве (1) доказывается, что конечная схема может быть «взломана» только по причине использования нестойкого БСА.

Таким образом, исследование стойкости AEAD-схемы (вне зависимости от свойств базового БСА) в целевой модели нарушителя сводится к

- построению нарушителя $\mathcal{A}$ с заданными ограничениями и оценке снизу величины $\mathsf{Adv}^{\mathrm{M}}_{\Pi[\mathcal{S}_{2^n}]}(\mathcal{A})$;
- оценке сверху величины $\mathsf{Adv}^{\mathrm{M}}_{\Pi[\mathcal{S}_{2^n}]}(\mathcal{A})$ для любого нарушителя $\mathcal{A}$ в модели M с заданными ограничениями.

Заметим, что конструкция $\Pi[\mathcal{S}_{2^n}]$ является уже абстрактным (эффективно не реализуемым на практике) теоретико-информационным объектом. В отличие от исходного режима с БСА, для такого объекта есть возможность получить оценку сверху на величину $\mathsf{Adv}^{\mathrm{M}}_{\Pi[\mathcal{S}_{2^n}]}(\mathcal{A})$ для любого нарушителя $\mathcal{A}$, определяемого моделью M и обладающего ограниченными информационными ресурсами (при этом, вычислительные ресурсы могут быть неограниченными). Так, данная оценка получается как функция от длины блока БСА и доступного нарушителю объема данных. Получение такой оценки далее будем называть *исследованием комбинаторных свойств режима*. Получение именно таких оценок посвящены главы 1, 2, 3 настоящей диссертации.

Глава 1

Комбинаторные свойства AEAD-режимов

В настоящей главе исследуются базовые комбинаторные свойства AEAD-режимов «8 бит» и MGM. Данные исследования проводились в рамках процесса стандартизации схем одновременного обеспечения конфиденциальности и целостности информации в России при Техническом комитете 26 по стандартизации [18].

1.1. Режим «8 бит»

Режим «8 бит» был предложен в результате деятельности рабочей группы по сопутствующим алгоритмам при Техническом комитете 26. Прототипом данного режима является режима CCM, описанный в [3]. Режим CCM является комбинацией стандартных режимов обеспечения конфиденциальности CTR и режима выработки имитовставки CBC в режиме MAC-then-Encrypt (подробнее см. [1]): сначала вычисляется имитовставка для специальным образом закодированных открытого текста и ассоциированных данных, после чего открытый текст и имитовставка преобразовываются в защищеннное сообщение. При этом режим использует исходный секрет только для определения подстановки БСА.

Режим «8 бит» является комбинацией стандартных режимов обеспечения конфиденциальности CTR и режима выработки имитовставки OMAC в режиме MAC-and-Encrypt (также подробнее см. [1]). Основным отличием от оригинального режима CCM является отсутствие дополнительного преобразования имитовставки после ее вычисления, то есть за-

щищенное сообщение состоит непосредственно из значения имитовставки и преобразованного открытого текста. Данная особенность привела к возможности построения атаки – нарушителя свойства целостности, определяемого моделью INT-CTXT. В следующих трех подразделах описываются целевой режим «8 бит» и метод построения нарушителя.

1.1.1. Описание AEAD-режима «8 бит»

Режим «8 бит» описан для фиксированной длины блока БСА, равной $n = 128$ бит. Параметром режима является длина имитовставки $s \leqslant n$, s фиксируется в начале информационного обмена и считается известной как получателю, так и отправителю сообщения.

Режим «8 бит» определен для следующих множеств: $\boldsymbol{K} = \{0,1\}^k$, $\boldsymbol{N} = \{0,1\}^{56}$, $\boldsymbol{A} = \boldsymbol{P} = \boldsymbol{C} = \{0,1\}^{\leqslant 2^{n/2}-1}$, $\boldsymbol{T} = \{0,1\}^s$. Дополнительно на длину открытого текста накладывается следующее ограничение: $|P| > 0$.

Алгоритм OMAC. Выработка имитовставки в режиме «8 бит» происходит с помощью алгоритма OMAC, описанного в ГОСТ Р 34.13-2015 [33]. Приведем описание данного алгоритма. Для обработки сообщения M сначала вырабатываются производные секреты имитовставки. Процедура выработки производных секретов заключается в выполнении следую-

щих присваиваний:

$$R = E_K(0^{128}),$$

$$K_1 = \begin{cases} R \ll 1, & \text{если } \mathrm{msb}_1(R) = 0; \\ (R \ll 1) \oplus B_{128}, & \text{иначе;} \end{cases} \tag{1.1}$$

$$K_2 = \begin{cases} K_1 \ll 1, & \text{если } \mathrm{msb}_1(R) = 0; \\ (K_1 \ll 1) \oplus B_{128}, & \text{иначе,} \end{cases}$$

где $B_{128} = 0^{120}||10000111$.

Затем исходное сообщение $M \in \{0,1\}^*$ разбивается на $t = |M|_n$ блоков $M_1, \ldots, M_{t-1} \in \{0,1\}^n$ и $M_t \in \{0,1\}^r$, $r \leqslant n$, таких что $M = M_1 \| \ldots \| M_{t-1} \| M_t$. Описание алгоритма OMAC представлено на Рис. 1.1.

$\underline{OMAC^{(s)}(M = M_1 \| \ldots \| M_t, K)}$

$C_0 = 0^n$

$C_i = E_K(C_{i-1} \oplus M_i), i = 1, \ldots, t-1$

if $|M_t| = n$:

  $K^* = K_1, M^* = M_t$

else

  $K^* = K_2, M^* = M_t \| 1 \| 0^{n-|M_t|-1}$

$T = \mathrm{msb}_s(E_K(C_{t-1} \oplus M^* \oplus K^*))$

return T

Рис. 1.1. Режим OMAC

В дальнейшем через $MAC_K^{(s)}(M)$ в режиме «8 бит» будем обозначать процедуру выработки имитовставки для сообщения M длины s на

секрете K в соответствии с алгоритмом OMAC.

Алгоритмы режима «8 бит». Обозначим через t длину сообщения в блоках, то есть $t = |P|_{128}$. Положим $d = \left\lceil \frac{|P|+|A|+72}{128} \right\rceil$. Алгоритмы «8 бит» определены на Рис. 1.2.

$8\text{bits}^{(s)}.\mathsf{Enc}(K, N, P, A)$

$S_i \leftarrow 0^8 \| N \| \text{str}_{64}(i), i = 1, \ldots, t$
$\Gamma \leftarrow E_K(S_1) \| E_K(S_2) \| \ldots \| E_K(S_t)$
$C \leftarrow P \oplus \text{msb}_{|P|}(\Gamma)$
if $|A| = 0$:
  $F \leftarrow 1^7 \| 0$
else
  $F \leftarrow 1^7 \| 1$
$c \leftarrow 128d - |C| - |A| - 72$
$len \leftarrow \text{str}_{64}(|A|) \| \text{str}_{64}(|C|)$
$B \leftarrow F \| \text{str}_8(s) \| N \| A \| C \| 0^c \| len$
$T \leftarrow \text{MAC}_K^{(s)}(B)$
return (C, T)

$8\text{bits}^{(s)}.\mathsf{Dec}(K, N, C \| T, A, s)$

if $|A| = 0$:
  $F = 1^7 \| 0$
else
  $F = 1^7 \| 1$
$c \leftarrow 128d - |C| - |A| - 72$
$len \leftarrow \text{str}_{64}(|A|) \| \text{str}_{64}(|C|)$
$B \leftarrow F \| \text{str}_8(s) \| N \| A \| C \| 0^c \| len$
$T' = \text{MAC}_K^{(s)}(B)$
if $T \neq T'$:
  return $\perp$
$S_i = 0^8 \| N \| \text{str}_{64}(i), i = 1, \ldots, t$
$\Gamma = E_K(S_1) \| E_K(S_2) \| \ldots \| E_K(S_t)$
$P = C \oplus \text{msb}_{|C|}(\Gamma)$
return P

Рис. 1.2. Определение алгоритмов Enc и Dec AEAD-режима «8 бит»

В результате исследований комбинаторных свойства режима «8 бит» был разработан метод нарушения целостности в модели INT-CTXT. Его описание представлено в Подразделе 1.1.2.

1.1.2. Метод нарушения целостности

Общая идея метода заключается в использовании нарушителем преобразованных текстов для нарушения свойства целостности. При исследовании стойкости схем выработки имитовставки нарушитель получает в качестве информации только имитовставки от поданных на вход значений. При исследовании AEAD-схем нарушитель получает дополнительную информацию за счет выдаваемого преобразованного текста. В предлагаемом методе используется возможность получать значения преобразованного счетчика (гамму) и сравнивать их со значениями имитовставки. При совпадении данных значений появляется возможность сформировать подделку – новый корректный набор (N, A, C, T).

Опишем подробно действия нарушителя.

Будем рассматривать схему, в которой длина имитовставки s принимает значение 128 бит. Будем также считать, что значение нонса генерируется с помощью счетчика, то есть для каждого нового сообщения нонс $N' = \mathrm{str}_{56}(\mathrm{int}_{56}(N) + 1)$, где N — это нонс предыдущего сообщения. Нонс первого сообщения будем считать равным 0^{56}.

Первый шаг. Введем параметр l, такой что $6 \leqslant l < 55$. Затем сделаем 2^l запросов $P_1, P_2, \ldots, P_{2^l}$, $|P_i| = 2^{64} - 128$, с пустыми ассоциированными данными к оракулу *Encrypt*. В ответ оракул *Encrypt* возвращает соответствующие преобразованные тексты $C_1, C_2, \ldots, C_{2^l}$. Заметим, что для открытого текста P_i соответствующий вектор инициализации принимает значение $N_i = \mathrm{str}_{64}(i-1)$. Через $\mathcal{N}' = \{N_i |\ i = 1, \ldots, 2^l\}$ обозначим множество всех значений вектора инициализации, используемых для преобразования открытых текстов $P_1, P_2, \ldots, P_{2^l}$. Заметим, что длина откры-

тых текстов является максимально возможной для кратных длине блока. Количество 128-битных блоков в любом таком сообщении равно $2^{57}-1$.

Через $P_i[j]$ обозначим j-й 128-битный блок в сообщении P_i, а через $S_i[j]$ строку $0^8\|N\|\mathrm{str}_{64}(j)$, которая используется при преобразовании блока $P_i[j]$: $C_i[j] = P_i[j] \oplus E_K(S_i[j])$.

Обозначим через $\mathcal{S} = \{S_i[j]|\ i = 1, \ldots, 2^l,\ j = 1, \ldots, 2^{57}-1\}$ множество всех таких строк $S_i[j]$.

Для данных блоков открытого текста $P_i[j]$ и блоков преобразованного текста $C_i[j]$ в результате данного шаг получаем блоки гаммы $\Gamma_i[j] = E_K(S_i[j])$ для всех строк $S_i[j]$ из множества $\mathcal{S}$.

Второй шаг. На втором шаге вычислим $2^{56}-2^l$ значений преобразованных текстов и имитовставок для всех оставшихся значений вектора инициализации $\mathcal{N}'' = V_{56} \setminus \mathcal{N}'$. Более точно, сделаем $2^{56}-2^l$ запросов (N, P, A) к оракулу *Encrypt*, где $N \in \mathcal{N}''$, $P = 0^1 \in V_1$, $A = 0^1 \in V_1$. В ответ на запрос (N, P, A) оракул *Encrypt* возвращает значение $C\|T$, где C – преобразованный текст и T – имитовставка. Значение T вычисляется с помощью алгоритма $\mathrm{MAC}_K^{(128)}$, которому подается строка B, имеющая следующий формат

$$B = \underbrace{F\|\mathrm{str}_8(128)\|N\|A\|C\|0^{54}}_{B_0} \| \underbrace{\mathrm{str}_{64}(1)\|\mathrm{str}_{64}(1)}_{B_1}.$$

Так как B состоит только из двух блоков, имитовставка T равна значению $E_K(E_K(B_0) \oplus K_1 \oplus B_1)$.

Заметим, что для каждого нового значения N строка B_0 также новая, а строка B_1 является константой и равна значению $\mathrm{str}_{64}(1)\|\mathrm{str}_{64}(1)$. Через $\mathcal{B} = \{(F\|\mathrm{str}_8(128)\|N\|A\|C\|0^{54})|\ N \in \mathcal{N}''\}$ обозначим множество

всех таких B_0.

Таким образом, в конце данного шага получены имитовставки $E_K(E_K(B_0) \oplus K_1 \oplus B_1)$ для всех $2^{56} - 2^l$ блоков $B_0 \in \mathcal{B}$.

Третий шаг. На третьем шаге оценим вероятность p коллизии между значениями имитовставки, полученными на втором шаге, и значениями $\Gamma_i[j]$, полученными на первом шаге.

Оценим следующую вероятность

$$p = \Pr_K \left[\{E_K(S)_{S\in\mathcal{S}}\} \cap \{E_K(E_K(B_0) \oplus K_1 \oplus B_1)\}_{B_0\in\mathcal{B}} \neq \varnothing\right]$$

при следующих условиях: $\mathcal{S} \cap \mathcal{B} = \varnothing$, $0^{128} \notin \mathcal{S}$, $0^{128} \notin \mathcal{B}$, $|\mathcal{S}| = 2^l(2^{57} - 1)$, $|\mathcal{B}| = 2^{56} - 2^l$, $K_1 = K_1(E_K(0^{128}))$ – функция, зависящая только от значения $E_K(0^{128})$.

Оценим данную вероятность при условии, что E_K является случайной подстановкой на множестве $\{0,1\}^{128}$.

Применяя техническую Лемму 1.1, доказанную Г.К Седовым и представленную в Приложении 1, мы получаем

$$p \geqslant 1 - e^{-\frac{(2^{56}-2^l)(2^l(2^{57}-1)-1)}{2^{128}}} = 1 - e^{-2^{l-15}\left(1-\frac{1}{2^{56-l}}\right)\left(1-\frac{1}{2^{57}}-\frac{1}{2^{57+l}}\right)}.$$

Данная оценка растет монотонно при $6 \leqslant l < 55$, и при $l = 15$ мы получаем $p > 0.63 \approx 1 - e^{-1}$.

Таким образом, если получить 2^{15} преобразованных сообщений на первом шаге, тогда хотя бы одно значение имитовставки совпадет с одним из преобразованных значений счетчика с вероятностью $p > 0.63$.

Формирование подделки. Предположим, что коллизия произошла, и $\mathrm{MAC}_K^{(128)}(B) = \Gamma_i[j] = E_K(0^8 \| N_i \| \mathrm{str}_{64}(j))$, где

$$B = \underbrace{F \| \mathrm{str}_8(128) \| N \| A \| C \| 0^{54}}_{B_0} \| \underbrace{\mathrm{str}_{64}(1) \| \mathrm{str}_{64}(1)}_{B_1}.$$

Рассмотрим пары (C', A'), где $C' = 0^1 \in V_1$ и $A' = 0 \| C \| 0^u$, $u = 0, \ldots, 53$. Заметим, что для таких пар строка B', от которой будет вычисляться имитовставка, будет выглядеть следующим образом:

$$B' = \underbrace{F \| \mathrm{str}_8(128) \| N \| A' \| C' \| 0^{55-(u+2)}}_{B'_0} \| \underbrace{\mathrm{str}_{64}(u+2) \| \mathrm{str}_{64}(1)}_{B'_1}.$$

Заметим, что $B'_0 = B_0$, а следовательно, значение имитовставки от строки B' равно $E_K(E_K(B'_0) \oplus K_1 \oplus B'_1) = E_K(E_K(B_0) \oplus K_1 \oplus B'_1)$.

Рассмотрим множество строк

$$\hat{\mathcal{B}} = \{\hat{B} \in \{0,1\}^{128} |\ \hat{B} = \mathrm{str}_{64}(r) \| \mathrm{str}_{64}(1), r = 2, \ldots, 55\}.$$

Данное множество строк включает все возможные значения B'_1 для рассматриваемых пар (C', A'). Заметим, что для любого $\hat{B} \in \hat{\mathcal{B}}$ выполняется следующее равенство

$$\begin{aligned} E_K(B_0) \oplus K_1 \oplus \hat{B} &= E_K(B_0) \oplus K_1 \oplus B_1 \oplus (B_1 \oplus \hat{B}) = \\ &= 0^8 \| N_i \| \mathrm{str}_{64}(j) \oplus ((\mathrm{str}_{64}(1) \| \mathrm{str}_{64}(1)) \oplus (\mathrm{str}_{64}(r) \| \mathrm{str}_{64}(1))) = \\ &= 0^8 \| N_i \| \mathrm{str}_{64}(j) \oplus ((\mathrm{str}_{64}(1) \oplus \mathrm{str}_{64}(r)) \| \mathrm{str}_{64}(0)) = 0^8 \| N_t \| \mathrm{str}_{64}(j), \end{aligned}$$

где N_t может отличаться от N_i только в 6 наименее значащих битах. Следовательно $0^8 \| N_t \| \mathrm{str}_{64}(j) \in \mathcal{S}$, и значение $E_K(0^8 \| N_t \| \mathrm{str}_{64}(j))$, полученное на первом шаге, нам известно.

Таким образом, подделка для пары (C', A'), соответствующая значению $\hat{B}$, может быть сформирована следующим образом:

$$E_K(E_K(B_0) \oplus K_1 \oplus \hat{B}) = E_K(0^8 \| N_t \| \mathrm{str}_{64}(i)),$$

где $\hat{B} = \mathrm{str}_{64}(r) \| \mathrm{str}_{64}(1)$. Таким образом, можно получить 54 подделки с вероятностью $p > 0.63$.

Сложность метода. На первом шаге нарушитель должен сформировать 2^{15} запросов длины $2^{57}-1$ блоков и, следовательно, хранить не более 2^{72} блоков в сортированном списке. Таким образом, сложность первого шага составляет $72 \cdot 2^{72} \leqslant 2^{79}$.

На втором шаге нарушителю необходимо обработать $(2^{56}-2^{15})$ оставшихся сообщений и найти коллизию со значениями в отсортированном списке. Сложность второго шага может быть оценена сверху величиной $72 \cdot 2^{56} \leqslant 2^{63}$.

Вероятность успешности метода больше 0.63.

Таким образом, итоговая сложность метода (по времени и количеству запросов) оценивается сверху величиной 2^{79} и 2^{56} запросов. В результате данного метода с вероятностью $p > 0.63$ нарушитель может сформировать корректные значения имитовставки для 54 новых сообщений.

1.1.3. Сравнение с режимом CCM

Таким образом, для режима «8 бит» доказана приведенная далее теорема.

Теорема 1.1.1 (Ахметзянова Л.Р.)**.** *Существует нарушитель* $\mathcal{A}$ *в модели* INT-CTXT*, делающий* 2^{56} *запросов к оракулу Encrypt, такой что*

$$\mathsf{Adv}_{8\text{bits}}^{\text{INT-CTXT}}(\mathcal{A}) > 0.63.$$

Для оригинального режима CCM не известны методы нарушения целостности при наличии материала такого количества. Так, в работе [19] была выдвинута гипотеза, что для успешного формирования подделки нарушителю необходимо получить результат обработки порядка 2^{128} сообщений. Отметим, что отсутствие возможности применения предложенного метода к режиму CCM объясняется наличием в режиме CCM дополнительного маскирования значения имитовставки, которое отсутствует в режиме «8 бит». В связи с получением данного результата более перспективным для стандартизации AEAD-режимом стал второй претендент – оригинальный режим MGM, результаты исследования которого приведены в следующем разделе.

1.2. Режим MGM

Режим MGM впервые был предложен на конференции CTCrypt в 2017 (см. [20]). Процедура преобразования открытых текстов в режиме MGM аналогична указанной процедуре в режиме CTR2 [8]. Основным элементом процедуры формирования имитовставки в режиме MGM является мультилинейная функция, секретные коэффициенты которой вырабатываются способом, аналогичным процедуре выработки секретных масок для преобразования открытых текстов.

В докладе, представленном на конференции, были приведены принципы построения режима MGM с точки зрения обеспечения конфиденциальности и целостности информации. Исследование комбинаторных свойств, соответствующих формальной модели нарушителя IND-CPA (конфиденциальность), впервые было проведено в рамках настоящей диссертации. Исследование комбинаторных свойств, соответствующих модели нарушителя INT-CTXT (целостность), было проведено Карпуниным Г.А. в работе [21] на основе полученных для конфиденциальности результатов.

В настоящем разделе приводится описание режима MGM и доказывается верхняя оценка преобладаний нарушителей, определяемых моделью IND-CPA.

1.2.1. Дополнительные обозначение

Обозначим через $\{0,1\}^{n\times m}$ множество всех упорядоченных наборов из m элементов, где каждый элемент является n-битовой строкой, значение m будем называть длиной набора. Для набора $X \in \{0,1\}^{n\times m}$ через

$\{X\}$ будем обозначать множество всех его элементов. Для упрощения формул для $x \in \{0,1\}^n$, $X, Y \in \{0,1\}^{n \times m}$ будем использовать обозначения $x \in X$, $x \notin X$, и $X \cap Y$ вместо $x \in \{X\}$, $x \notin \{X\}$, и $\{X\} \cap \{Y\}$.

Через $inc_r(U)$ $(inc_l(U))$ будем обозначать функцию, которая принимает на входу строку $L\|R$, где $L, R \in \{0,1\}^{n/2}$, и возвращает строку $L\|\mathrm{str}_{n/2}(\mathrm{int}(R) + 1 \bmod 2^{n/2})$ $\big(\mathrm{str}_{n/2}(\mathrm{int}(L) + 1 \bmod 2^{n/2})\|R\big)$.

1.2.2. Описание AEAD-режима MGM

Параметрами режима MGM являются БСА E с длиной секрета k и длиной блока n, а также длина имитовставки в битах s, $1 \leqslant s \leqslant n$. Данные параметры фиксируются в рамках конкретного протокола.

Схема MGM$[E, s]$ определена для следующих множеств: $\boldsymbol{K} = \{0,1\}^k$, $\boldsymbol{N} = \{0,1\}^{n-1}$, $\boldsymbol{A} = \boldsymbol{P} = \boldsymbol{C} = \{0,1\}^{\leqslant 2^{n/2}-1}$, $\boldsymbol{T} = \{0,1\}^s$. Дополнительно на длину открытого текста и ассоциированных данных накладывается следующее ограничение: $0 < |A| + |P| \leqslant n \cdot 2^{n/2}$. Алгоритмы режима определены на Рис. 1.3.

MGM.$\mathsf{Enc}(K, N, A, P)$

$h \leftarrow |A|_n, t \leftarrow |P|_n$

$\ell \leftarrow h + t + 1$

. . . . . .

$Y_1 \leftarrow E_K(0\|N),\ \Gamma_1 \leftarrow E_K(Y_1)$

for $i = 2 \ldots t$ **do**:

$Y_i \leftarrow inc_r(Y_{i-1}),\ \Gamma_i \leftarrow E_K(Y_i)$

$C \leftarrow P \oplus \mathrm{msb}_{|P|}(\Gamma_1 \,\|\, \ldots \,\|\, \Gamma_t)$

. . . . . .

$a \leftarrow n|A|_n - |A|$

$c \leftarrow n|C|_n - |C|$

$len \leftarrow \mathrm{str}_{n/2}(|A|) \,\|\, \mathrm{str}_{n/2}(|C|)$

$M_1\| \ldots \|M_\ell \leftarrow A\|0^a\|C\|0^c\|len$

. . . . . .

$Z_1 \leftarrow E_K(1\|N),\ H_1 \leftarrow E_K(Z_1)$

for $i = 2 \ldots \ell$ **do**:

$Z_i \leftarrow inc_l(Z_{i-1}),\ H_i \leftarrow E_K(Z_i)$

$\tau \leftarrow \bigoplus_{i=1}^{l} M_i \otimes H_i$

$T \leftarrow \mathrm{msb}_s(E_K(\tau))$

return (C, T)

MGM.$\mathsf{Dec}(K, N, A, C, T)$

$h \leftarrow |A|_n, t \leftarrow |C|_n$

$\ell \leftarrow h + t + 1$

. . . . . .

$a \leftarrow n|A|_n - |A|$

$c \leftarrow n|C|_n - |C|$

$len \leftarrow \mathrm{str}_{n/2}(|A|) \,\|\, \mathrm{str}_{n/2}(|C|)$

$M_1\| \ldots \|M_l \leftarrow A\|0^a\|C\|0^c\|len$

. . . . . .

$Z_1 \leftarrow E_K(1\|N),\ H_1 \leftarrow E_K(Z_1)$

for $i = 2 \ldots \ell$ **do**:

$Z_i \leftarrow inc_l(Z_{i-1}),\ H_i \leftarrow E_K(Z_i)$

$\tau \leftarrow \bigoplus_{i=1}^{l} M_i \otimes H_i$

$T' \leftarrow \mathrm{msb}_s(E_K(\tau))$

if $T' \neq T$: **return** $\perp$

. . . . . .

$Y_1 \leftarrow E_K(0\|N),\ \Gamma_1 \leftarrow E_K(Y_1)$

for $i = 2 \ldots t$ **do**:

$Y_i \leftarrow inc_r(Y_{i-1}),\ \Gamma_i \leftarrow E_K(Y_i)$

$P \leftarrow C \oplus \mathrm{msb}_{|C|}(\Gamma_1 \,\|\, \ldots \,\|\, \Gamma_t)$

return P

Рис. 1.3. Определение алгоритмов Enc и Dec AEAD-режима MGM

Далее через $\mathrm{MGM}[\mathcal{S}_{2^n}, s]$ ($\mathrm{MGM}[\mathcal{F}_{2^n}, s]$) обозначим схему, в которой при обработке данных с помощью функций MGM.Enc и MGM.Dec используется подстановка $\pi \xleftarrow{\mathcal{U}} \mathcal{S}_{2^n}$ (функция $\rho \xleftarrow{\mathcal{U}} \mathcal{F}_{2^n}$) вместо преобразования E_K, $K \xleftarrow{\mathcal{U}} \{0,1\}^k$ (на Рис. 1.4 E_K заменяется на π или ρ).

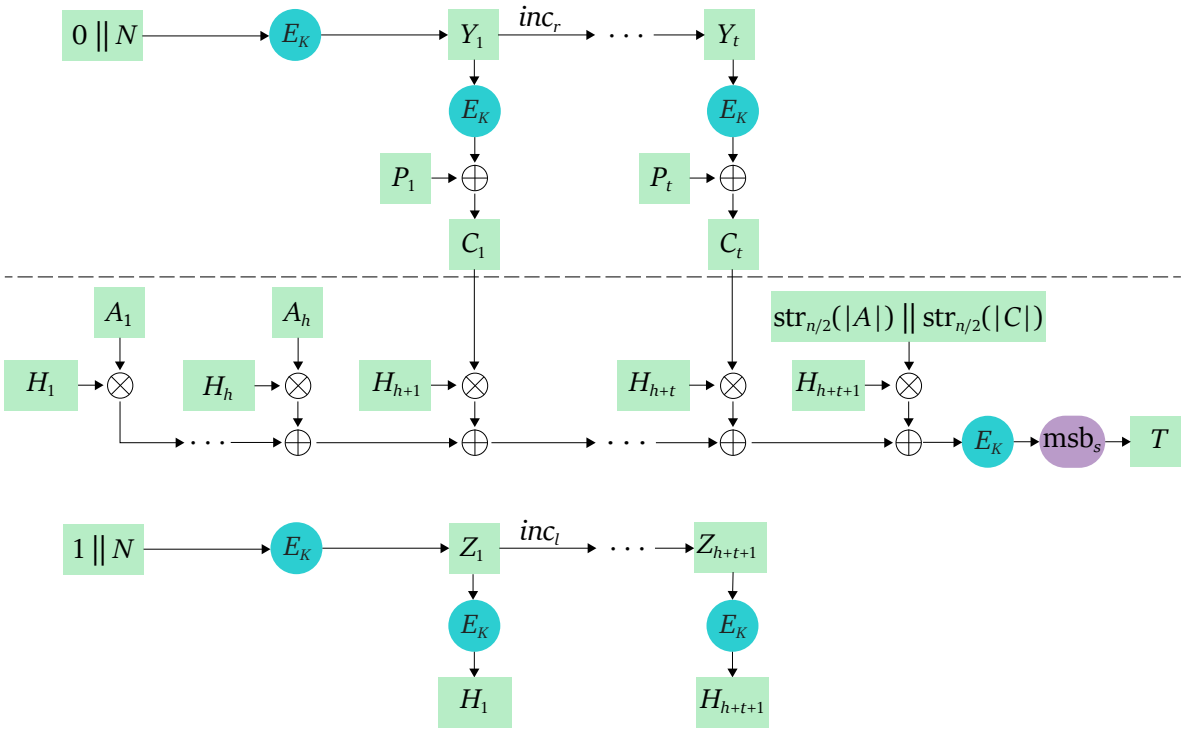

Рис. 1.4. Схематичное описание алгоритма Enc AEAD-режима MGM

В результате исследований комбинаторных свойств режима MGM доказана верхняя оценка преобладаний всех нарушителей, определяемых моделью IND-CPA (конфиденциальность без повтора вектора инициализации). Данная оценка и метод ее обоснования представлены в Подразделе 1.2.3.

1.2.3. Конфиденциальность

В настоящем подразделе приводится доказательство оценки сверху величины $\mathbf{Adv}^{\text{IND-CPA}}_{\text{MGM}[\mathcal{S}_{2^n},s]}(\mathcal{A})$ для любого нарушителя $\mathcal{A}$ в модели IND-CPA, которая представлена в виде функции от длины блока и заданных ограничений на информационные ресурсы нарушителя.

Теорема 1.2.1 (Ахметзянова Л.Р.)**.** *Для любого нарушителя $\mathcal{A}$ в модели IND-CPA, который делает не более q запросов, где максимальная суммарная длина открытого текста и ассоциированных данных не превосходит l блоков, выполнено следующее неравенство:*

$$\mathbf{Adv}^{\text{IND-CPA}}_{\text{MGM}[\mathcal{S}_{2^n},s]}(\mathcal{A}) \leqslant \frac{(2ql+5q)^2}{2^n}.$$

Для доказательства данной теоремы сначала вводится вспомогательная модель mIND-CPA для семейства функций $\mathcal{F} \subseteq \mathcal{F}_{2^n}$. Далее доказывается, что из стойкости в данной модели для семейства $\mathcal{S}_{2^n}$ следует стойкость схемы $\text{MGM}[\mathcal{S}_{2^n}, s]$ в модели IND-CPA (см. Утверждение 1.2.2).

После этого доказывается оценка для семейства $\mathcal{S}_{2^n}$ в модели mIND-CPA (см. Теорему 1.2.3).

Вспомогательная модель mIND-CPA. Введем вспомогательную модель нарушителя mIND-CPA с параметрами l и s для семейства функций $\mathcal{F} \subseteq \mathcal{F}_{2^n}$. При инициализации эксперимента выбирается функция $f \xleftarrow{\mathcal{U}} \mathcal{F}$. Далее нарушителю предоставляется доступ к оракулу *Encrypt-b*, $b \in \{0,1\}$, к которому он делает два последовательных запроса, описанных далее.

1. Первый запрос состоит из вектора инициализации $N \in \{0,1\}^{n-1}$.

   В случае оракула *Encrypt*-1 ответом на запрос является набор $\Gamma \in \{0,1\}^{n \times l}$, состоящий из l блоков $\Gamma_k \in \{0,1\}^n$, $k = 1, \ldots, l$. Также оракул сохраняет значения N и l, которые далее будут использоваться для обработки следующего запроса.

   Обработка первого запроса:

$$\begin{cases} Y_1 = f(0 \| N), \\ Y_k = inc_r(Y_{k-1}), & 2 \leqslant k \leqslant l, \\ \Gamma_k = f(Y_k), & 1 \leqslant k \leqslant l. \end{cases}$$

   В случае оракула *Encrypt*-0 ответом является набор $\Gamma \in \{0,1\}^{n \times l}$, состоящий из l блоков $\Gamma_k \xleftarrow{\mathcal{U}} \{0,1\}^n$, каждый из которых выбирается случайно равновероятно из множества $\{0,1\}^n$.

2. Второй запрос содержит набор $X \in \{0,1\}^{n \times l}$, состоящий из l блоков $X_k \in \{0,1\}^n$, $k = 1, \ldots, l$.

   В случае оракула *Encrypt*-1 данный набор используется в качестве входа в мультилинейную функцию алгоритма вычисления имитовставки, который также принимает на вход вектор инициализации N, переданный на предыдущем запросе. Для предотвращения тривиальных атак введем следующее ограничение на набор X: $X_l \neq 0^n$. В качестве ответа нарушителю возвращается значение $T \in \{0,1\}^s$.

Обработка второго запроса:

$$\begin{cases} Z_1 = f(1\|N), \\ Z_k = inc_l(Z_{k-1}), & 2 \leqslant k \leqslant l, \\ H_k = f(Z_k), & 1 \leqslant k \leqslant l, \\ \tau = \sum\limits_{k=1}^{l} H_k \cdot X_k, \\ T = \mathrm{msb}_s(f\,(\tau)). \end{cases}$$

В случае оракула *Encrypt*-0 нарушитель получает значение $T \xleftarrow{\mathcal{U}} \{0,1\}^s$, которое выбирается случайно равновероятно из $\{0,1\}^s$.

Определение 1.2.1. Преобладание нарушителя $\mathcal{A}$ в модели mIND-CPA с параметрами l и s для семейства функций $\mathcal{F}$ определяется следующим образом:

$$\mathsf{Adv}_{\mathcal{F}}^{\text{mIND-CPA}_{l,s}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_{\mathcal{F}}^{\text{mIND-CPA}_{l,s}\text{-1}}(\mathcal{A}) \to 1\right] - \\ - \Pr\left[\mathbf{Exp}_{\mathcal{F}}^{\text{mIND-CPA}_{l,s}\text{-0}}(\mathcal{A}) \to 1\right],$$

где $\mathbf{Exp}_{\mathcal{F}}^{\text{mIND-CPA}_{l,s}\text{-}b}(\mathcal{A}), b \in \{0,1\}$, определены выше.

Легко показать, что верно следующее утверждение.

Предложение 1.2.2. Для любого нарушителя $\mathcal{A}$ в модели IND-CPA для схемы $\mathrm{MGM}_{\mathcal{F},s}$, делающего не более q запросов, где максимальная суммарная длина открытого текста и ассоциированных данных не превосходит l блоков, существует нарушитель $\mathcal{A}'$ в модели mIND-CPA с параметрами $l+1$ и s для семейства $\mathcal{F}$, такой что

$$\mathbf{Adv}_{\mathrm{MGM}_{\mathcal{F},s}}^{\text{IND-CPA}}(\mathcal{A}) = \mathbf{Adv}_{\mathcal{F}}^{\text{mIND-CPA}_{l+1,s}}(\mathcal{A}'),$$

где $\mathcal{A}'$ делает не более q пар связанных запросов.

Доказательство. Построим нарушителя $\mathcal{A}'$ в модели mIND-CPA для семейства $\mathcal{F}$, использующего нарушителя $\mathcal{A}$. Алгоритм $\mathcal{A}'$ запускает алгоритм $\mathcal{A}$, перехватывает его запросы и сам их обрабатывает. Алгоритм симулирует оракул *Encrypt-b* для $\mathcal{A}$, делая специальные запросы к своему оракулу *Encrypt-b*. Перехватывая запросы (N, A, P) от $\mathcal{A}$ нарушитель $\mathcal{A}'$ делает пару следующих связанных запросов к своему оракулу.

Первый запрос состоит из вектора инициализации N. Получая в ответ набор $\Gamma = (\Gamma_1, \ldots, \Gamma_l)$, нарушитель $\mathcal{A}'$ формирует значение $C = P \oplus \mathrm{msb}_{|P|}(\Gamma_1 \| \ldots \| \Gamma_{|P_n|})$ (заметим, что $l \geqslant |P|_n$). После этого $\mathcal{A}'$ делает второй запрос — набор X, состоящий из блоков строки $A\|0^{n-a}\|C\|0^{n-c}\|(\mathrm{str}_{n/2}(|A|)\|\mathrm{str}_{n/2}(|C|))\|0^{n(l-|A|_n-|P|_n)}$. Заметим, что длина набора X в точности равна $l+1$ блоков, а дополнение нулями не влияет на процесс вычисления T. Получая в ответ на второй запрос значение T, алгоритм $\mathcal{A}'$ возвращает значение (C, T) алгоритму $\mathcal{A}$. В качестве результата своей работы алгоритм $\mathcal{A}'$ возвращает то же самое, что и алгоритм $\mathcal{A}$.

Заметим, что нарушитель $\mathcal{A}'$, взаимодействующий с оракулом *Encrypt-b* в модели mIND-CPA, в точности симулирует для нарушителя $\mathcal{A}$ работу оракула *Encrypt-b* в модели IND-CPA. Поэтому

$$\mathbf{Adv}_{\mathcal{F}}^{\mathrm{mIND\text{-}CPA}_{l+1,s}}(\mathcal{A}') = \mathbf{Adv}_{\mathrm{MGM}_{\mathcal{F}}}^{\mathrm{IND\text{-}CPA}}(\mathcal{A}).$$

□

Оценка в модели mIND-CPA для семейства $\mathcal{S}_{2^n}$. Рассмотрим детерминированный алгоритм-нарушитель $\mathcal{A}$ с неограниченными вычисли-

тельными ресурсами, который делает в точности q пар связанных запросов. Тогда алгоритм определяется описанными далее $2q$ функциями.

- Первые q функций $N_i^{\mathcal{A}},\ i = 1, \ldots, q$, определяют выбор параметра N из первой части запросов к оракулу *Encrypt-b*.

  Функция $N_1^{\mathcal{A}}$ является константной, т.е. $N_1^{\mathcal{A}} = N_1$. Следующие функции $N_i^{\mathcal{A}},\ i = 2, \ldots, q$, определяются следующим образом:

$$N_i = N_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}) :$$
$$\underbrace{\{0,1\}^{n\times l} \times \{0,1\}^s \times \ldots \times \{0,1\}^{n\times l} \times \{0,1\}^s}_{2(i-1)} \to \{0,1\}^{n-1}.$$

  Данные функции для $\forall\ \Gamma^1, T_1, \ldots, \Gamma^q, T_q$ должны удовлетворять следующему условию:

$$\forall\ 1 \leqslant i, j \leqslant q,\ i \neq j,$$
$$N_i^{\mathcal{A}}(\Gamma^1, \ldots, T_{i-1}) \neq N_j^{\mathcal{A}}(\Gamma^1, \ldots, T_{j-1}).$$

- Следующие q функций $X_i^{\mathcal{A}},\ i = 1, \ldots, q$, определяют значение набора X из второй части запросов к оракулу *Encrypt-b*:

$$X^i = X_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}, \Gamma^i) :$$
$$\underbrace{\{0,1\}^{n\times l} \times \{0,1\}^s \times \ldots \times \{0,1\}^{n\times l} \times \{0,1\}^s}_{2(i-1)} \times \{0,1\}^{n\times l} \to \{0,1\}^{n\times l}.$$

  Данные функции для $\forall\ \Gamma^1, T_1, \ldots, \Gamma^{q-1}, T_{q-1}, \Gamma^q$ должны удовлетворять следующему условию:

$$\forall\ 1 \leqslant i \leqslant q,\ X_l^i \neq 0^n\ .$$

Далее через $\mathbf{D}^i$, $i = 1, \ldots, q$, будем обозначать набор, состоящий из всех значений, поступивших на вход функции f после обработки первых i запросов в модели mIND-CPA. В данный набор входят значения $0\|N_j$, $1\|N_j$, τ_j и значения элементов наборов $Y^j = (Y_1^j, \ldots, Y_l^j)$, $Z^j = (Z_1^j, \ldots, Z_l^j)$, $j = 1, \ldots, i$.

Докажем вспомогательную комбинаторную лемму 1.2.1, в рамках которой оценивается вероятность коллизии в наборе $\mathbf{D}^q$. Основная идея доказательства заключается в подсчете количества различных размещений с пересечением в пространстве $\{0,1\}^n$, представленном в виде тора $\{0,1\}^{n/2} \times \{0,1\}^{n/2}$, объектов разного типа: «точки», «горизонтальные отрезки» и «вертикальные отрезки» длины l (см. Рис. 1.5 далее по тексту).

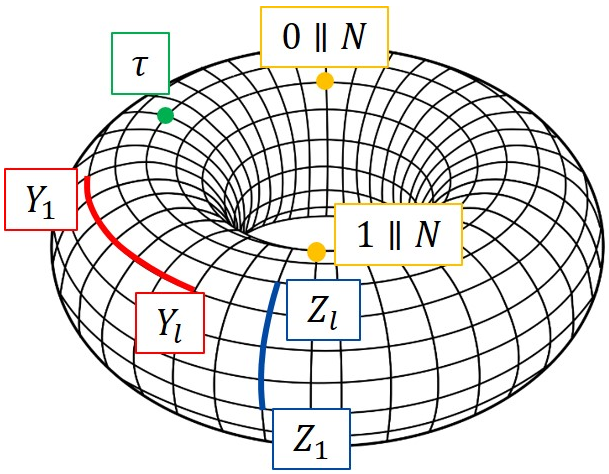

Рис. 1.5. Размещение объектов на торе $\{0,1\}^{n/2} \times \{0,1\}^{n/2}$: «точками» являются значения $\tau, 0\|N, 1\|N$, «горизонтальными отрезками» являются наборы $Y = \{Y_1, \ldots, Y_l\}$, т.к. $Y_i = inc_{\mathbf{r}}(Y_{i-1})$, «вертикальными отрезками» являются наборы $Z = \{Z_1, \ldots, Z_l\}$, т.к. $Z_i = inc_{\mathbf{l}}(Z_{i-1})$

.

Введем дополнительные обозначения, которые далее используются при доказательстве леммы.

Дополнительные обозначения. Далее будем обозначать случайную величину с использованием символа тильда (например, $\widetilde{\lambda}$), а конкретные ее значения – без символа тильда (λ). Пусть $\widetilde{\Lambda} = (\widetilde{\lambda}_1, \ldots, \widetilde{\lambda}_m)$ – набор из m случайных величин $\widetilde{\lambda}_i \colon \mathcal{F}_{2^n} \to \{0,1\}^n$, $i = 1, \ldots, m$, при этом на множестве $\mathcal{F}_{2^n}$ задано равновероятное распределение. Для $\omega \in \mathcal{F}_{2^n}$, через $\widetilde{\Lambda}(\omega)$ обозначим набор $(\widetilde{\lambda}_1(\omega), \ldots, \widetilde{\lambda}_1(\omega))$.

Пусть Λ — некоторое значение набора $\widetilde{\Lambda}$. Через $\widetilde{\Lambda} \setminus \{\widetilde{\lambda}_i\}$ будем обозначать набор $\widetilde{\Lambda}$, из которого убрали величину $\widetilde{\lambda}_i$. Тогда через $\Lambda \setminus \{\widetilde{\lambda}_i\}$ обозначим конкретное значение набора $\widetilde{\Lambda} \setminus \{\widetilde{\lambda}_i\}$.

Через $\Lambda\, coll$ обозначим предикат, который выполняется тогда и только тогда, когда произошла коллизия среди элементов набора Λ. Обозначим через $\Lambda\ \overline{coll}$ отрицание предиката $\Lambda\ coll$. Для набора $\widetilde{\Lambda}$ через $\widetilde{\Lambda}\, coll$ обозначим событие $\{\omega \in \mathcal{F}_{2^n} \mid \widetilde{\Lambda}(\omega)\ coll = 1\}$, т.е. набор Λ содержит одинаковые элементы. Через $\widetilde{\Lambda}\ \overline{coll}$ будем обозначать отрицание события $\widetilde{\Lambda}\ coll$.

Лемма 1.2.1. *Для любого нарушителя $\mathcal{A}$ в модели mIND-CPA с параметрами l и s для семейства $\mathcal{F}_{2^n}$, который делает q пар связанных запросов, выполнено следующее неравенство:*

$$\Pr\left[\widetilde{\mathbf{D}}^q\ coll\right] \leqslant \frac{(2ql + 3q)^2}{2^n}.$$

Доказательство. По формуле полной вероятности имеем:

$$\begin{aligned}\Pr\left[\widetilde{\mathbf{D}}^q\ coll\right] &= \Pr\left[\widetilde{\mathbf{D}}^q\ coll \cap \widetilde{\mathbf{D}}^{q-1}\ \overline{coll}\right] + \\ &\quad + \Pr\left[\widetilde{\mathbf{D}}^q\ coll \cap \widetilde{\mathbf{D}}^{q-1}\ coll\right] = \\ &\quad = \Pr\left[\widetilde{\mathbf{D}}^q\ coll \cap \widetilde{\mathbf{D}}^{q-1}\ \overline{coll}\right] + \Pr\left[\widetilde{\mathbf{D}}^{q-1}\ coll\right].\end{aligned}$$

Заметим, что аналогичная формула верна и для $\Pr\left[\widetilde{\mathbf{D}}^{q-1}\ coll\right]$. Поэтому

$$\Pr\left[\widetilde{\mathbf{D}}^{q}\ coll\right] = \sum_{i=1}^{q} \Pr\left[\widetilde{\mathbf{D}}^{i}\ coll \cap \widetilde{\mathbf{D}}^{i-1}\ \overline{coll}\right].$$

Здесь для удобства записи формулы через $\widetilde{\mathbf{D}}^{0}\ \overline{coll}$ обозначен истинный предикат.

Рассмотрим вероятность $\Pr\left[\widetilde{\mathbf{D}}^{i}\ coll \cap \widetilde{\mathbf{D}}^{i-1}\ \overline{coll}\right]$, $i = 1, \ldots, q$. Применим формулу полной вероятности по всем возможным значениям $\Gamma^j, T_j,\ j = 1, \ldots, i-1$:

$$\Pr\left[\widetilde{\mathbf{D}}^{i}\ coll \cap \widetilde{\mathbf{D}}^{i-1}\ \overline{coll}\right] = \\ = \sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1} \\ T_1,\ldots,T^{i-1}}} \Pr\left[\widetilde{\mathbf{D}}^{i}\ coll \cap \widetilde{\mathbf{D}}^{i-1}\ \overline{coll} \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j \\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{i-1}\right]. \quad (1.2)$$

Рассмотрим слагаемое под знаком суммы для любых $\Gamma^j, T_j,\ j = 1, \ldots, i-1$,. Заметим, что после фиксации этих значений

1. в наборе $\widetilde{\mathbf{D}}^{i}$ случайные величины $\widetilde{N}_j$ принимают конкретные значения $N_j = N_j^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{j-1}, T_{j-1})$, $j = 1, \ldots, i$, аналогично в наборе $\widetilde{\mathbf{D}}^{i-1}$ случайные величины $\widetilde{N}_1, \ldots, \widetilde{N}_{i-1}$ также принимают соответствующие конкретные значения.

2. случайные величины $\widetilde{X}^j$ принимают конкретные значения $X^j = X_j^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{j-1}, T_{j-1}, \Gamma^j)$, $j = 1, \ldots, i-1$.

Также заметим, что после дополнительной фиксации значений $Y^j, Z^j, H^j,\ j = 1, \ldots, i-1$, все случайные величины в наборе $\widetilde{\mathbf{D}}^{i-1}$ принимают конкретные значения, в том числе случайные величины $\widetilde{\tau}_j$ принимают конкретные значения $\tau_j = \sum_{k=1}^{l} H_k^j \cdot X_k^j$, $j = 1, \ldots, i-1$. Отметим,

что однозначная фиксация наборов Y^j, Z^j происходит после фиксации значений Y_1^j, Z_1^j, так как последующие значения в этих наборах однозначно определяются по первым блокам.

Таким образом, при фиксированных $\Gamma^j, T_j, Y^j, Z^j, H^j,\ j = 1, \ldots, i-1$, значение предиката $\mathbf{D}^{i-1}\ \overline{coll}$, становится определенным. Поэтому для каждого слагаемого из формулы (1.2) верно следующее равенство:

$$\Pr\left[\widetilde{\mathbf{D}}^i\ coll \cap \widetilde{\mathbf{D}}^{i-1}\ \overline{coll} \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{i-1}\right] =$$

$$= \sum_{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ \mathbf{D}^{i-1}\ \overline{coll}}} \Pr\left[\widetilde{\mathbf{D}}^i\ coll \cap \left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{i-1} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{i-1}\right].$$

Далее для краткости событие

$$\left\{\begin{smallmatrix}\widetilde{\Gamma}^j=\Gamma^j\\ \widetilde{T}_j=T_j\end{smallmatrix}\right\}_{j=1}^{i-1} \cap \left\{\begin{smallmatrix}\widetilde{Y}^j=Y^j\\ \widetilde{Z}^j=Z^j\\ \widetilde{H}^j=H^j\end{smallmatrix}\right\}_{j=1}^{i-1}$$

будем обозначать через **fix**. Вероятность данного события при условии выполнения предиката $\mathbf{D}^{i-1}\ \overline{coll}$ равна

$$\frac{1}{2^{n(i-1)(2l+2)+s(i-1)}}. \tag{1.3}$$

Последняя сумма может быть разбита на две подсуммы по событию, когда хотя бы одно из значений $0\|N_i$ или $1\|N_i$ попало в множество $\mathbf{D}^{i-1}$:

$$sum_1 = \sum_{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ \mathbf{D}^{i-1}\ \overline{coll}\\ 0\|N_i \vee 1\|N_i \in \mathbf{D}^{i-1}}} \Pr\left[\mathbf{fix}\right];$$

$$sum_2 = \sum_{\substack{Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ \mathbf{D}^{i-1}\ \overline{coll}\\ 0\|N_i,1\|N_i\notin\mathbf{D}^{i-1}}} \Pr\left[\widetilde{\mathbf{D}}^i\ coll \cap \mathbf{fix}\right].$$

Оценка первой суммы. Рассмотрим слагаемое sum_1. Применяя формулу (1.3), получим следующее неравенство:

$$sum_1 \leqslant \underbrace{\#\left\{\begin{array}{c} Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}:\\ 0\|N_i\vee 1\|N_i\in\mathbf{D}^{i-1}\end{array}\right\}}_{A} \cdot \frac{1}{2^{n(i-1)(2l+2)+s(i-1)}}. \qquad (1.4)$$

Оценим мощность множества A для фиксированных $\Gamma^j, T_j,\ j = 1,\ldots,i-1$ (как следствие, для фиксированных N_j, X^j, $j = 1,\ldots,i-1$, и N_i). Множество A принадлежит объединению следующих подмножеств:

$$A \subseteq \bigcup_{b\in\{0,1\}} \bigcup_{j=1}^{i-1} \Bigg(\left\{\begin{array}{c} Y^j:\\ b\|N_i\in Y^j\end{array}\right\} \times \left\{\begin{array}{c} Y^1,\ldots,Y^{j-1},Y^{j+1},\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}\end{array}\right\} \cup$$
$$\cup \left\{\begin{array}{c} Z^j:\\ b\|N_i\in Z^j\end{array}\right\} \times \left\{\begin{array}{c} Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{j-1},Z^{j+1},\ldots,Z^{i-1}\\ H^1,\ldots,H^{i-1}\end{array}\right\} \cup$$
$$\cup \left\{\begin{array}{c} H^j:\\ b\|N_i=\tau_j\end{array}\right\} \times \left\{\begin{array}{c} Y^1,\ldots,Y^{i-1}\\ Z^1,\ldots,Z^{i-1}\\ H^1,\ldots,H^{j-1},H^{j+1},\ldots,H^{i-1}\end{array}\right\} \Bigg).$$

Здесь в первой строке выписано множество, при котором одна из двух «точек» $b\|N_i$ попала на один из $i-1$ «горизонтальных отрезков» Y^j длины l, во второй строке – на один из $i-1$ «вертикальных отрезков» Z^j длины l, в третьей строке – в одну из $i-1$ «точек» τ_j.

Таким образом, мощность множества A можно оценить следующим

образом:

$$\#A \leqslant \sum_{b\in\{0,1\}} \sum_{j=1}^{i-1} \Big(\underbrace{\#\left\{Y^j : b \| N_i \in Y^j\right\}}_{=l} \cdot 2^{n(i-1)(l+2)-n} + \\ + \underbrace{\#\left\{Z^j : b \| N_i \in Z^j\right\}}_{=l} \cdot 2^{n(i-1)(l+2)-n} + \\ + \underbrace{\#\left\{H^j : b \| N_i = \tau_j\right\}}_{=2^{nl-n}} \cdot 2^{n(i-1)(l+2)-nl} \Big) = \\ = \underbrace{(i-1)(4l+2)}_{\omega_1} \cdot 2^{n(i-1)(l+2)-n}.$$

Подставив полученную оценку для мощности в формулу (1.4) и проведя простые арифметические действия, получим оценку для первого слагаемого:

$$sum_1 \ \leqslant \ \omega_1 \cdot 2^{n(i-1)(l+2)-n} \cdot \frac{1}{2^{n(i-1)(2l+2)+s(i-1)}} \ = \ \frac{\omega_1}{2^{n(i-1)l+s(i-1)+n}}. \quad (1.5)$$

Оценка второй суммы. Рассмотрим второе слагаемое sum_2. Оно отражает вероятность коллизии за счет выбора «отрезков» Y^i, Z^i и за счет выбора «точек» τ_i. Для каждого слагаемого под знаком суммы верно

$$\Pr\left[\widetilde{\mathbf{D}}^i \ coll \cap \mathbf{fix}\right] = \underbrace{\sum_{\substack{Y^i,Z^i:\\ \mathbf{D}^i\setminus\{\widetilde{\tau}_i\}\ coll}} \Pr\left[\mathbf{fix} \cap \left\{\begin{smallmatrix}\widetilde{Y}^i=Y^i\\ \widetilde{Z}^i=Z^i\end{smallmatrix}\right\}\right]}_{sum_2^1} + \\ + \underbrace{\sum_{\substack{Y^i,Z^i:\\ \mathbf{D}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \Pr\left[\widetilde{\mathbf{D}}^i \ coll \cap \mathbf{fix} \cap \left\{\begin{smallmatrix}\widetilde{Y}^i=Y^i\\ \widetilde{Z}^i=Z^i\end{smallmatrix}\right\}\right]}_{sum_2^2}.$$

Рассмотрим слагаемое sum_2^1. В силу (1.3) и того, что вероятность события $\left\{\begin{smallmatrix}\widetilde{Y}^i=Y^i\\ \widetilde{Z}^i=Z^i\end{smallmatrix}\right\}$ при условии выполнения предиката $\mathbf{D}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}$ равна

$\frac{1}{2^{2n}}$, верно следующее неравенство:

$$sum_2^1 \leqslant \#\underbrace{\left\{{}^{Y^i,Z^i:}_{\mathbf{D}^i\setminus\{\widetilde{\tau}_i\}\ coll}\right\}}_{B}\cdot\frac{1}{2^{n(i-1)(2l+2)+s(i-1)+2n}}. \tag{1.6}$$

Оценим мощность множества B для фиксированных значений $\Gamma^j, T_j, Y^j, Z^j, H^j,\ j = 1,\ldots,i-1$ (как следствие, для фиксированных N_i и всех значений из $\mathbf{D}^{i-1}$). Множество B принадлежит объединению следующих множеств:

$$\begin{aligned}
B \subseteq \bigcup_{j=1}^{i-1}\left(\left\{{}^{Z^i:}_{Z^i\cap Z^j\neq\emptyset}\right\}\cup\left\{{}^{Z^i:}_{\tau_j\in Z^i}\right\}\right)\times\left\{Y^i\right\}\ \cup \\
\cup\ \bigcup_{j=1}^{i-1}\left(\left\{{}^{Y^i:}_{Y^i\cap Y^j\neq\emptyset}\right\}\cup\left\{{}^{Y^i:}_{\tau_j\in Y^i}\right\}\right)\times\left\{Z^i\right\}\ \cup \\
\cup\ \bigcup_{j=1}^{i-1}\bigcup_{k_j=1}^{l}\left(\left\{{}^{Z^i:}_{Y^j_{k_j}\in Z^i}\right\}\times\left\{Y^i\right\}\cup\left\{{}^{Y^i:}_{Z^j_{k_j}\in Y^i}\right\}\times\left\{Z^i\right\}\right)\ \cup \\
\cup\ \bigcup_{j=1}^{i}\bigcup_{b\in\{0,1\}}\left(\left\{{}^{Z^i:}_{b\| N_j\in Z^i}\right\}\times\left\{Y^i\right\}\cup\left\{{}^{Y^i:}_{b\| N_i\in Y^i}\right\}\times\left\{Z^i\right\}\right)\ \cup \\
\cup\ \left\{{}^{Y^i,Z^i:}_{Y^i\cap Z^i\neq\emptyset}\right\}.
\end{aligned}$$

Здесь в первой (второй) строке выписано множество, в котором «вертикальный отрезок» Z^i («горизонтальный отрезок» Y^i) длины l пересекается с одим из $i-1$ «вертикальных отрезков» Z^j («горизонтальных отрезков» Y^j) длины l или с одной из $i-1$ «точек» τ_j. В третьей строке выписано множество, в котором «вертикальный отрезок» Z^i («горизонтальный отрезок» Y^i) длины l пересекается с одним из $i-1$ «горизонтальных отрезков» Y^j («вертикальных отрезков» Z^j) длины l. В четвертой строке выписано множество, в котором «отрезок» Z^i (Y^i) длины l пере-

секается с одной из $2i$ точек $b\|N_j$. В пятой строке выписано множество, в котором «отрезки» Z^i и Y^i пересекаются между собой.

Таким образом, $\forall\ \Gamma^j, T_j, Y^j, Z^j, H^j,\ j = 1, \ldots, i-1$, мощность множества B может быть оценена следующим образом:

$$\begin{aligned}
\#B \leqslant \sum_{j=1}^{i-1} \Big(\underbrace{\#\left\{Z^i : Z^i \cap Z^j \neq \emptyset\right\}}_{=(l+l-1)} + \underbrace{\#\left\{Z^i : \tau_j \in Z^i\right\}}_{=l} \Big) \cdot 2^n + \\
+ \sum_{j=1}^{i-1} \Big(\underbrace{\#\left\{Y^i : Y^i \cap Y^j \neq \emptyset\right\}}_{=(l+l-1)} + \underbrace{\#\left\{Y^i : \tau_j \in Y^i\right\}}_{=l} \Big) \cdot 2^n + \\
+ \sum_{j=1}^{i-1} \sum_{k_j=1}^{l} \Big(\underbrace{\#\left\{Z^i : Y^j_{k_j} \in Z^i\right\}}_{=l} \cdot 2^n + \underbrace{\#\left\{Y^i : Z^j_{k_j} \in Y^i\right\}}_{=l} \cdot 2^n \Big) + \\
+ \sum_{j=1}^{i} \sum_{b \in \{0,1\}} \Big(\underbrace{\#\left\{Z^i : b\|N_j \in Z^i\right\}}_{=l} \cdot 2^n + \underbrace{\#\left\{Y^i : b\|N_j \in Y^i\right\}}_{=l} \cdot 2^n \Big) + \\
+ \sum_{Z_i} \underbrace{\#\left\{Y^i : Y^i \cap Z^i \neq \emptyset\right\}}_{l^2} = \\
= \underbrace{\left((i-1)(6l + 2l^2 - 2) + 4il + l^2\right)}_{\omega_2^1} \cdot 2^n.
\end{aligned}$$

Подставляя полученную оценку для мощности в формулу (1.6), имеем

$$sum_2^1 \ \leqslant\ \omega_2^1 \cdot 2^n \cdot \frac{1}{2^{n(i-1)(2l+2)+s(i-1)+2n}} \ \leqslant\ \frac{\omega_2^1}{2^{n(i-1)(2l+2)+s(i-1)+n}}. \quad (1.7)$$

Рассмотрим слагаемое sum_2^2. Оно отражает вероятность попадания «точки» τ_i на «отрезки» Y^i, Z^i, в «точки» $0\|N_1$ и $1\|N_1$ или в множество $\mathbf{D}^{i-1}$ (при условии, что среди последних не было пересечений).

Заметим, что после фиксации значений Γ^i, H^i случайные величины $\widetilde{\tau}_i$ принимают конкретные значения $\tau_i = \sum_{k=1}^{l} H_k^i \cdot X_k^i$, где

$X^i = X_i^{\mathcal{A}}(\Gamma^1, T_1, \ldots, \Gamma^{i-1}, T_{i-1}, \Gamma^i)$. Поэтому,

$$sum_2^2 = \sum_{\substack{Y^i,Z^i:\\ \mathbf{D}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \sum_{\substack{\Gamma^i,H^i:\\ \mathbf{D}^i\ coll}} \Pr\left[\mathbf{fix} \cap \begin{Bmatrix} \widetilde{Y}^i{=}Y^i \\ \widetilde{Z}^i{=}Z^i \\ \widetilde{\Gamma}^i{=}\Gamma^i \\ \widetilde{H}^i{=}H^i \end{Bmatrix}\right] =$$

$$= \sum_{\substack{Y^i,Z^i:\\ \mathbf{D}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \underbrace{\#\left\{\begin{smallmatrix}\Gamma^i,H^i:\\ \mathbf{D}^i\ coll\end{smallmatrix}\right\}}_{C} \cdot \frac{1}{2^{n(i-1)(2l+2)+s(i-1)+n(2l+2)}}. \quad (1.8)$$

Оценим мощность множества C при фиксированных значениях $\Gamma^j, T_j, Y^j, Z^j, H^j,\ j = 1, \ldots, i-1$ (как следствие, для фиксированных значений N_i и всех значений из $\mathbf{D}^{i-1}$), Y^i, Z^i. Множество C принадлежит объединению следующих множеств:

$$C \subseteq \bigcup_{\Gamma^i} \left(\left\{ \begin{smallmatrix} H^i: \\ \tau_i \in \mathbf{D}^{i-1} \end{smallmatrix} \right\} \cup \left\{ \begin{smallmatrix} H^i: \\ \tau_i \in Z^i \end{smallmatrix} \right\} \cup \left\{ \begin{smallmatrix} H^i: \\ \tau_i \in Y^i \end{smallmatrix} \right\} \cup \bigcup_{b\in\{0,1\}} \left\{ \begin{smallmatrix} H^i: \\ \tau_i = b \| N_i \end{smallmatrix} \right\} \right).$$

Здесь в первой фигурной скобке выписано множество, при котором «точка» τ_i попала в множество $\mathbf{D}^{i-1}$ мощности $(i-1)(2l+3)$. Во второй (третьей) скобке выписано множество, при котором «точка» τ_i попала на «отрезок» Z^i (Y^i) длины l. В четвертой скобке выписано множество, при котором «точка» τ_i попала в одну из двух «точек» $b\|N_i$.

Таким образом, мощность множества C может быть оценена следующим образом:

$$\#C \leqslant 2^{nl}\Big(\underbrace{\#\left\{ \begin{smallmatrix} H^i: \\ \tau_i \in \mathbf{D}^{i-1} \end{smallmatrix} \right\}}_{=(i-1)(2l+3)\cdot 2^{nl-n}} + \underbrace{\#\left\{ \begin{smallmatrix} H^i: \\ \tau_i \in Z^i \end{smallmatrix} \right\}}_{=l\cdot 2^{nl-n}} +$$

$$+ \underbrace{\#\left\{ \begin{smallmatrix} H^i: \\ \tau_i \in Y^i \end{smallmatrix} \right\}}_{=l\cdot 2^{nl-n}} + \sum_{b\in\{0,1\}} \underbrace{\#\left\{ \begin{smallmatrix} H^i: \\ \tau_i = b\|N_i \end{smallmatrix} \right\}}_{2^{nl-n}} \Big) =$$

$$= (i-1)(2l+3)\cdot 2^{2nl-n} + (2l+2)\cdot 2^{2nl-n} = \underbrace{\big((i-1)(2l+3)+(2l+2)\big)}_{\omega_2^2} \cdot 2^{2nl-n}.$$

Подставим полученную оценку для мощности в формулу (1.8):

$$sum_2^2 \leqslant \sum_{\substack{Y^i,Z^i: \\ \mathbf{D}^i\setminus\{\widetilde{\tau}_i\}\ \overline{coll}}} \frac{\omega_2^2 \cdot 2^{2nl-n}}{2^{n(i-1)(2l+2)+s(i-1)+n(2l+2)}} \leqslant$$

$$\leqslant \#\left\{Y^i,Z^i\right\} \cdot \frac{\omega_2^2}{2^{n(i-1)(2l+2)+s(i-1)+3n}} =$$

$$= 2^{2n} \cdot \frac{\omega_2^2}{2^{n(i-1)(2l+2)+s(i-1)+3n}} =$$

$$= \frac{\omega_2^2}{2^{n(i-1)(2l+2)+s(i-1)+n}}. \quad (1.9)$$

Просуммируем полученные оценки (1.7) и (1.9) и получим оценку для sum_2:

$$sum_2 = \sum_{\substack{Y^1,\ldots,Y^{i-1} \\ Z^1,\ldots,Z^{i-1} \\ H^1,\ldots,H^{i-1}: \\ \mathbf{D}^{i-1}\ \overline{coll} \\ 0\|N_i,1\|N_i\notin\mathbf{D}^{i-1}}} \left(sum_2^1 + sum_2^2\right) \leqslant \#\left\{\begin{matrix} Y^1,\ldots,Y^{i-1} \\ Z^1,\ldots,Z^{i-1} \\ H^1,\ldots,H^{i-1} \end{matrix}\right\} \left(sum_2^1 + sum_2^2\right) =$$

$$= 2^{n(i-1)(l+2)} \cdot \frac{\omega_2^1 + \omega_2^2}{2^{n(i-1)(2l+2)+s(i-1)+n}}. = \frac{\omega_2^1 + \omega_2^2}{2^{n(i-1)l+s(i-1)+n}}.$$

Теперь просуммируем оценки для sum_1 (1.5) и sum_2:

$$\Pr\left[\widetilde{\mathbf{D}}^i\ coll \cap \widetilde{\mathbf{D}}^{i-1}\ \overline{coll}\right] = \sum_{\substack{\Gamma^1,\ldots,\Gamma^{i-1} \\ T_1,\ldots,T_{i-1}}} (sum_1 + sum_2) \leqslant$$

$$\leqslant \#\left\{\begin{matrix} \Gamma^1,\ldots,\Gamma^{i-1} \\ T_1,\ldots,T_{i-1} \end{matrix}\right\} (sum_1 + sum_2) =$$

$$= 2^{n(i-1)l} \cdot 2^{s(i-1)} \cdot \frac{\omega_1 + \omega_2^1 + \omega_2^2}{2^{n(i-1)l+s(i-1)+n}} = \frac{\omega_1 + \omega_2^1 + \omega_2^2}{2^n}.$$

Итого,

$$\Pr\left[\widetilde{\mathbf{D}}^q \; coll\right] = \sum_{i=1}^{q} \Pr\left[\widetilde{\mathbf{D}}^i \; coll \cap \widetilde{\mathbf{D}}^{i-1} \; \overline{coll}\right] \leqslant$$

$$\leqslant \sum_{i=1}^{q} \frac{(i-1)(4l+2)}{2^n} +$$

$$+ \sum_{i=1}^{q} \frac{(i-1)(6l+2l^2-2)+4il+l^2}{2^n} +$$

$$+ \sum_{i=1}^{q} \frac{(i-1)(2l+3)+(2l+2)}{2^n} \leqslant$$

$$\leqslant \frac{4(ql)^2+12q^2l+9q^2}{2^{n+1}} = \frac{(2ql+3q)^2}{2^{n+1}}.$$

□

Теорема 1.2.3. *Для любого нарушителя $\mathcal{A}$ в модели mIND-CPA с параметрами l и s для семейства $\mathcal{S}_{2^n}$, который делает в точности q пар связанных запросов, верно следующее неравенство:*

$$\mathbf{Adv}^{\text{mIND-CPA}_l}_{\mathcal{S}_{2^n}}(\mathcal{A}) \leqslant \frac{(2ql+3q)^2}{2^n}.$$

Доказательство. Заметим, что до наступления события $\widetilde{\mathbf{D}}^q \; coll$ оракул *Encrypt*-1 порождает такое же распределение на ответах, что и оракул *Encrypt*-0.

Тогда, согласно Лемме 2, [9], верно следующее соотношение:

$$\mathbf{Adv}^{\text{mIND-CPA}_{l,s}}_{\mathcal{F}_{2^n}}(\mathcal{A}) \leqslant \Pr\left[\widetilde{\mathbf{D}}^q \; coll\right].$$

Используя Лемму «PRP-PRF Switching», см. [32], и Лемму 1.2.1, мы

получаем следующую оценку:

$$\mathbf{Adv}^{\text{mIND-CPA}_{l,s}}_{\mathcal{S}_{2^n}}(\mathcal{A}) \leqslant \mathbf{Adv}^{\text{mIND-CPA}_{l,s}}_{\mathcal{F}_{2^n}}(\mathcal{A}) + \frac{(2ql+3q)^2}{2^{n+1}} \leqslant$$
$$\leqslant \Pr\left[\widetilde{\mathbf{D}}^q \; coll\right] + \frac{(2ql+3q)^2}{2^{n+1}} \leqslant \frac{(2ql+3q)^2}{2^{n+1}} +$$
$$+ \frac{(2ql+3q)^2}{2^{n+1}} \leqslant \frac{(2ql+3q)^2}{2^n}.$$

Второе неравенство верно в силу того, что в рамках эксперимента в модели mIND-CPA_l нарушитель делает не более $2ql + 3q$ запросов к функции f. □

1.2.4. Целостность

Используя Лемму 1.2.1, можно аналогичным образом получить оценку для режима MGM в модели INT-CTXT с одной попыткой подделки. Действительно, если при обработке всех запросов к оракулу *Encrypt* и последнего запроса-подделки не возникло коллизий среди входов в случайную функцию, то вероятность осуществления подделки в точности равна вероятности случайного угадывания значения имитовставки.

Теорема 1.2.4 ([21], Карпунин Г.А.)**.** *Для любого нарушителя $\mathcal{A}$ в модели* INT-CTXT*, который делает не более q запросов к оракулу Encrypt с суммарной длиной открытых текстов и ассоциированных данных не более σ блоков и не более одного запроса к оракулу Decrypt длины не более l блоков, выполнено следующее неравенство:*

$$\mathbf{Adv}^{\text{INT-CTXT}}_{\text{MGM}[\mathcal{S}_{2^n},s]}(\mathcal{A}) \leqslant \frac{3(\sigma+4q+l+3)^2}{2^n} + \frac{2}{2^s}.$$

Отметим, что особенностью конструкции режима MGM является возможность возникновения коллизий между любыми возможными вхо-

дами используемой подстановки (вероятность данного события оценивалась в Лемме 1.2.1). В работе [24] была представлена атака на свойство целостности, существенно использующая возможность коллизий между входами. В следующей главе разработана модификация режима MGM, в котором отсутствует указанный недостаток.

Выводы

Для режима «8 бит», модификации режима CCM, был построен метод нарушения целостности при наличии материала порядка $2^{n/2}$ блоков. Данный метод существенно использует отличительную особенность конструкции «8 бит», заключающуюся в отсутствии дополнительного маскирования значения имитовставки, и поэтому не применим к оригинальному режиму CCM. На основе полученных в настоящей диссертации результатов режим «8 бит» был исключен из рассмотрения в процессе стандартизации AEAD-схем в Российской Федерации.

Для режима MGM доказана оценка уровня стойкости в базовой модели нарушителя IND-CPA, в которой для обработки каждого сообщения используется уникальное значение вектора инициализации. Данная оценка демонстрирует, что режим MGM обеспечивает конфиденциальность при обработке данных, суммарный объем которых не превышает $2^{n/2}$ блоков. Данный уровень стойкости является стандартным для AEAD-режимов. Полученные в настоящей диссертации результаты о стойкости режима MGM использовались при стандартизации данного режима в Российской Федерации.

Глава 2

Устойчивость к повтору вектора инициализации

С целью одновременного получения оценок уровня стойкости в моделях нарушителя с повтором вектора инициализации и нивелирования недостатка режима MGM, указанного в Главе 1, далее в диссертации разработана модификация режима MGM — режим MGM2. Основное различие между двумя режимами заключается в способе создания секретных маскирующих блоков и секретных коэффициентов мультилинейной функции. Отметим, что основное ядро конструкции, а именно, мультилинейная функция, не изменилось.

Основным результатом настоящей главы является конструкция режима MGM2 и доказанные оценки уровня стойкости в моделях MRAE-int и CPA-res.

2.1. Режим MGM2

В настоящем разделе вводится формальное описание разработанного режима MGM2 (см. Подраздел 2.1.1), для которого далее проводится анализ расширенных комбинаторных свойств, соответствующих моделям MRAE-int и CPA-res (см. подразделы 2.1.2 и 2.1.3).

2.1.1. Описание AEAD-режима MGM2

Параметрами режима MGM2 являются БСА E с длиной блока n и длиной секрета k, длина нонса r, $\frac{n}{2} \leqslant r \leqslant \frac{3n}{4}$, и длина имитовставки s, $1 \leqslant s \leqslant n$. Введем функцию $\mathsf{Set1}_r \colon \{0,1\}^n \to \{0,1\}^n$, $\mathsf{Set1}_r(x) = x \text{ or } (\overbrace{0\ldots0}^{r}1\overbrace{0\ldots0}^{n-r-1})$, $0 \leqslant r < n$.

Схема MGM2$[E, r, s]$ определена для следующих множеств: $\boldsymbol{K} = \{0,1\}^k$, $\boldsymbol{N} = \{0,1\}^r$, $\boldsymbol{A} = \boldsymbol{P} = \boldsymbol{C} = \{0,1\}^{\leqslant 2^{n/2}-1}$, $\boldsymbol{T} = \{0,1\}^s$. Дополнительно на длину открытого текста и ассоциированных данных накладывается следующее ограничение: $0 < |A| + |P| \leqslant n(2^{n-r-2} - 1)$. Алгоритмы режима определены на Рис. 2.1 (см. ниже). На указанном рисунке определены алгоритмы Enc и Dec в формате псевдокода.

MGM2.$\mathsf{Enc}(K, N, A, P)$

$h \leftarrow |A|_n, t \leftarrow |P|_n$

$\ell \leftarrow h + t + 1$

. . . . . .

for $i = 1 \ldots t$ **do**:

  $\Gamma_i \leftarrow \mathsf{E}_K(N \| 00 \| \mathrm{str}_{n-r-2}(i-1))$

$C \leftarrow P \oplus \mathrm{msb}_{|P|}(\Gamma_1 \parallel \ldots \parallel \Gamma_t)$

. . . . . .

$a \leftarrow n|A|_n - |A|$

$c \leftarrow n|C|_n - |C|$

$len \leftarrow \mathrm{str}_{n/2}(|A|) \parallel \mathrm{str}_{n/2}(|C|)$

$M_1 \| \ldots \| M_l \leftarrow A \| 0^a \| C \| 0^c \| len$

. . . . . .

for $i = 1 \ldots \ell$ **do**:

  $H_i \leftarrow \mathsf{E}_K(N \| 01 \| \mathrm{str}_{n-r-2}(i-1))$

$\tau \leftarrow \mathsf{Set1}_r \left(\bigoplus_{i=1}^{l} M_i \otimes H_i \right)$

$T \leftarrow \mathrm{msb}_s(\mathsf{E}_K(\tau))$

return (C, T)

MGM2.$\mathsf{Dec}(K, N, A, C, T)$

$h \leftarrow |A|_n, t \leftarrow |C|_n$

$\ell \leftarrow h + t + 1$

. . . . . .

$a \leftarrow n|A|_n - |A|$

$c \leftarrow n|C|_n - |C|$

$len \leftarrow \mathrm{str}_{n/2}(|A|) \parallel \mathrm{str}_{n/2}(|C|)$

$M_1 \| \ldots \| M_l \leftarrow A \| 0^a \| C \| 0^c \| len$

. . . . . .

for $i = 1 \ldots \ell$ **do**:

  $H_i \leftarrow \mathsf{E}_K(N \| 01 \| \mathrm{str}_{n-r-2}(i-1))$

$\tau \leftarrow \mathsf{Set1}_r \left(\bigoplus_{i=1}^{l} M_i \otimes H_i \right)$

$T' \leftarrow \mathrm{msb}_s(\mathsf{E}_K(\tau))$

if $T' \neq T$: **return** $\perp$

. . . . . .

for $i = 1 \ldots t$ **do**:

  $\Gamma_i \leftarrow \mathsf{E}_K(N \| 00 \| \mathrm{str}_{n-r-2}(i-1))$

$P \leftarrow C \oplus \mathrm{msb}_{|C|}(\Gamma_1 \parallel \ldots \parallel \Gamma_t)$

return P

Рис. 2.1. Определение алгоритмов Enc и Dec AEAD-режима MGM2

Отличия от MGM. Отличия режима MGM2 от режима MGM состоят в способах вычисления маскированных значений для процедуры

преобразования открытых текстов (Γ_i), коэффициентов мультилинейной функции (H_i), и формирования имитовставки T. В режиме MGM2 множества входных значений БСА, используемые для различных целей (а именно, для формирования значений Γ_i, H_i, T), не пересекаются за счет фиксации определенных битов (для наглядности см. Рис. 2.2). Такая модификация позволяет существенно улучшить оценки уровня стойкости в целевых моделях нарушителя, так как, в отличие от режима MGM, коллизия между входами БСА возможна только среди значений мультилинейной функции τ.

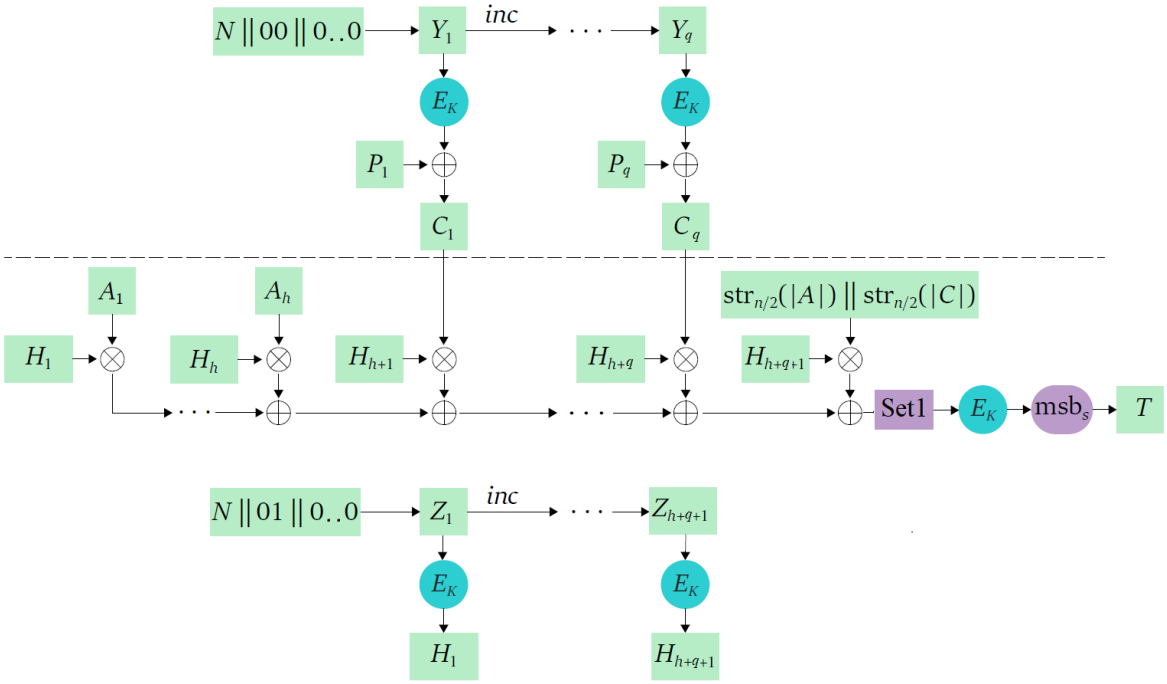

Рис. 2.2. Режим MGM2

Далее через MGM2$[\mathcal{S}_{2^n}, r, s]$ (MGM2$[\mathcal{F}_{2^n}, r, s]$) обозначим схему, в которой при обработке данных с помощью функций MGM2.Enc и MGM2.Dec используется подстановка $\pi \xleftarrow{\mathcal{U}} \mathcal{S}_{2^n}$ (функция $\rho \xleftarrow{\mathcal{U}} \mathcal{F}_{2^n}$) вместо преобразования E_K, $K \xleftarrow{\mathcal{U}} \{0,1\}^k$ (на Рис. 2.2 E_K заменяется на π или ρ).

В результате исследований комбинаторных свойств режима MGM2 доказаны верхние оценки преобладаний всех нарушителей, определяемых моделью MRAE-int и CPA-res (целостность и конфиденциальность при повторе вектора инициализации). Данные оценки и методы их обоснования представлены в в подразделах 2.1.2 и 2.1.3 соответственно.

2.1.2. Целостность

В настоящем подразделе приводится доказательство оценки сверху величины $\mathsf{Adv}^{\text{MRAE-int}}_{\text{MGM2}[\mathcal{S}_{2^n},r,s]}(\mathcal{A})$ для любого нарушителя $\mathcal{A}$ в модели MRAE-int, которая представлена в виде функции от длины блока и заданных ограничений на информационные ресурсы нарушителя.

Теорема 2.1.1 (Ахметзянова Л.Р.)**.** *Для любого нарушителя $\mathcal{A}$ в модели* MRAE-int*, делающего не более q_E запросов к оракулу Encrypt и не более q_D запросов к оракулу Decrypt, при условии, что суммарное количество блоков ассоциированных данных в запросах равно σ_A, а суммарное количество блоков открытых текстов и преобразованных текстов равно σ_P, справедливо*

$$\mathsf{Adv}^{\text{MRAE-int}}_{\text{MGM2}[\mathcal{S}_{2^n},r,s]}(\mathcal{A}) \leqslant \left(\frac{q(q-1)}{2^n} + \frac{q_D}{2^s}\right)\left(1 - \frac{\sigma-1}{2^n}\right)^{-\sigma/2}, \qquad (2.1)$$

где $q = q_E + q_D$ и $\sigma = 2\sigma_P + \sigma_A + 2q$.

В частном случае, когда значение σ не превышает $2^{n/2}$ и $n \geqslant 128$, оценка (2.1) принимает следующий вид:

$$\mathsf{Adv}^{\text{MRAE-int}}_{\text{MGM2}[\mathcal{S}_{2^n},r,s]}(\mathcal{A}) \leqslant 1.7\left(\frac{q(q-1)}{2^n} + \frac{q_D}{2^s}\right). \qquad (2.2)$$

Заметим, что для оригинального режима MGM, если суммарная длина всех обработанных данных достигает $2^{n/2}$ блоков, то оценка из Теоремы 1.2.4 вырождается. Оценка для режима MGM2 выродится, только если будет обработано $2^{n/2}$ отдельных сообщений. Данный результат также позволяет использовать MGM2 как функцию выработки имитовставки путем фиксации N. Далее представлено доказательство Теоремы 2.1.1.

Доказательство. Доказательство проводится в два этапа. На первом этапе вводится вспомогательный режим выработки имитовставки MGM2-MAC$[r, s]$ и доказывается оценка его уровня стойкости в модели UF-CMA.

На втором этапе показывается, что из стойкости MGM2-MAC$[r, s]$ в модели UF-CMA следует стойкость режима MGM2$[\mathcal{F}_{2^n}, r, s]$ в модели MRAE-int.

Оценка уровня стойкости режима MGM2$[\mathcal{S}_{2^n}, r, s]$ в модели MRAE-int непосредственно вытекает из оценки уровня стойкости режима MGM2$[\mathcal{F}_{2^n}, r, s]$ в модели MRAE-int с применением оценки Бернштейна [34], Теорема 2.3. Согласно данной теореме для любого алгоритма $\mathcal{D}^f$ с оракулом
$f\colon \{0,1\}^n \to \{0,1\}^n$, который делает не более q запросов, верно следующее неравенство:

$$\Pr[\mathcal{D}^{\pi} \to 1] \leqslant \Pr[\mathcal{D}^{\rho} \to 1] \cdot \left(1 - \frac{q-1}{2^n}\right)^{-q/2},$$

где $\pi \xleftarrow{\mathcal{U}} \mathcal{S}_{2^n}$ и $\rho \xleftarrow{\mathcal{U}} \mathcal{F}_{2^n}$.

Положив в качестве алгоритма $\mathcal{D}$ алгоритм $\mathbf{Exp}^{\text{MRAE-int}}_{\text{MGM2}[\cdot,r,s]}(\mathcal{A})$, в котором вместо вызовов БСА осуществляется запрос к оракулу, получим

требуемую оценку. □

Оценка уровня стойкости MGM2-MAC в модели UF-CMA. Введем вспомогательную схему выработки имитовставки с нонсом MGM2-MAC$[r, s]$, основанную на схеме MGM2$[\mathcal{F}_{2^n}, r, s]$. Такая схема определяется как набор алгоритмов $\mathsf{MAC} = \{\mathsf{MAC.Gen}, \mathsf{MAC.Tag}, \mathsf{MAC.Verify}\}$, для схемы MGM2-MAC$[r, s]$ данные алгоритмы определены на Рис. 2.3.

Данная схема определена для множества сообщений $\{M = M_1\| \ldots \|M_\ell \colon M_i \in \{0,1\}^n,\ M_\ell \neq 0^n,\ 1 \leqslant \ell \leqslant 2^{n-r-2}\}$ (длина сообщения кратна n, последний блок ненулевой), и для множества нонсов $\{0,1\}^r$.

MGM2-MAC.$\mathsf{Gen}()$

$\rho, \rho' \xleftarrow{\mathcal{U}} \mathcal{F}_{2^n}$

$K \leftarrow (\rho, \rho')$

return K

MGM2-MAC.$\mathsf{Tag}(K, N, M)$

$\tau \leftarrow \mathsf{PreTag}(\rho', N, M)$

$T \leftarrow \mathrm{msb}_s(\rho(\tau))$

return T

$\mathsf{PreTag}(\rho', N, M)$

$l \leftarrow |M|_n$

for $i = 1 \ldots \ell$ **do**:

$H_i \leftarrow \rho'(N\|01\|\mathrm{str}_{n-r-2}(i-1))$

$\tau \leftarrow \mathsf{Set1}_r\left(\bigoplus_{i=1}^{l}(M_i \otimes H_i)\right)$

return τ

MGM2-MAC.$\mathsf{Verify}(K, N, M, T)$

$\tau \leftarrow \mathsf{PreTag}(\rho', N, M)$

$T' \leftarrow \mathrm{msb}_s(\rho(\tau))$

if $T' \neq T$: **return** false

return true

Рис. 2.3. Схема MGM2-MAC

Сначала введем вспомогательную модель PRF для схемы выработки имитовставки с нонсом и получим в ней оценку для схемы MGM2-MAC.

Определение 2.1.1 (PRF)**.** Для схемы MAC преобладание нарушителя $\mathcal{A}$ в модели PRF определяется следующим образом:

$$\mathsf{Adv}^{\mathrm{PRF}}_{\mathsf{MAC}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-1}_{\mathsf{MAC}}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-0}_{\mathsf{MAC}}(\mathcal{A}) \to 1\right],$$

где эксперименты $\mathbf{Exp}^{\mathrm{PRF}-b}_{\mathsf{MAC}}(\mathcal{A}),\ b \in \{0,1\}$, описаны ниже.

$\mathbf{Exp}^{\mathrm{PRF}-b}_{\mathsf{MAC}}(\mathcal{A})$	Oracle $Tag^1(N, M)$	Oracle $Tag^0(N, M)$
if $b = 1$:	**if** $(N, M) \in sent$:	**if** $(N, M) \in sent$:
$K \leftarrow \mathsf{MAC.Gen}(\,)$	**return** $\perp$	**return** $\perp$
$sent \leftarrow \emptyset$	$T \leftarrow \mathsf{MAC.Tag}(K, N, M)$	$T \xleftarrow{\mathcal{U}} \{0,1\}^s$
$b' \leftarrow \mathcal{A}^{Tag^b}(\,)$	$sent \leftarrow sent \cup \{(N, M)\}$	$sent \leftarrow sent \cup \{(N, M)\}$
return b'	**return** T	**return** T

Лемма 2.1.1. *Для любого нарушителя $\mathcal{A}$ в модели* PRF*, делающего не более q запросов к оракулу Tag:*

$$\mathsf{Adv}^{\mathrm{PRF}}_{\text{MGM2-MAC}[r,s]}(\mathcal{A}) \leqslant \frac{q(q-1)}{2^n}.$$

Доказательство. Определим эксперименты $\mathbf{Exp}^0$ и $\mathbf{Exp}^1$ (см. Рис. 2.4), которые отличаются от эксперимента $\mathbf{Exp}^{\mathrm{PRF}-1}_{\text{MGM2-MAC}[r,s]}$ следующим образом. На этапе инициализации дополнительно вводится множество tau, которое инициализируется пустым множеством, а также флаг bad, который изначально полагается равным значению false. Во время выполнения эксперимента проверяется, лежит ли очередное значение τ в множестве tau, и если лежит, то флаг bad выставляется равным true, после этого значение τ добавляется в множество. Также в эксперименте $\mathbf{Exp}^0$ значение

имитовставки T выбирается из множества $\{0,1\}^s$ случайно равновероятно, в случае если $\tau \in tau$ (см. выделенную строку в рамке).

$\mathbf{Exp}^b(\mathcal{A}),\ b \in \{0,1\}$	Oracle $Tag^b(N, M)$
$(\rho, \rho') \leftarrow$ MGM2-MAC.Gen( )	**if** $(N, M) \in sent$:
$bad \leftarrow$ false	**return** $\perp$
$tau, sent \leftarrow \emptyset$	$\tau \leftarrow \mathsf{PreTag}(\rho', N, M)$
$b' \leftarrow \mathcal{A}^{Tag^b}( )$	$T \leftarrow \mathrm{msb}_s(\rho(\tau))$
return b'	**if** $\tau \in tau$:
	$bad \leftarrow$ true
	if $b = 0$: $T \xleftarrow{\mathcal{U}} \{0,1\}^s$
	$tau \leftarrow tau \cup \{\tau\}$
	$sent \leftarrow sent \cup \{(N, M)\}$
	return T

Рис. 2.4. Эксперименты $\mathbf{Exp}^0$ и $\mathbf{Exp}^1$

Легко заметить, что эксперимент $\mathbf{Exp}^1$ в точности совпадает с экспериментом $\mathbf{Exp}^{\mathrm{PRF}-1}_{\text{MGM2-MAC}[r,s]}$. Более того, для любого нарушителя $\mathcal{A}$ в модели PRF значение $\Pr\left[\mathbf{Exp}^0(\mathcal{A}) \to 1\right]$ в точности равно значению $\Pr\left[\mathbf{Exp}^{\mathrm{PRF}-0}_{\text{MGM2-MAC}[r,s]}(\mathcal{A}) \to 1\right]$. Действительно, в эксперименте $\mathbf{Exp}^0$ все значения T генерируются в соответствии с равновероятным распределением, как и в эксперименте $\mathbf{Exp}^{\mathrm{PRF}-0}_{\text{MGM2-MAC}[r,s]}$, по следующим причинам. Для запросов, в которых соответствующее значение τ является новым (т.е. не лежит в текущем множестве tau), к данному новому входу применяется случайная функция ρ и поэтому возвращает равновероятные значения T. Для других запросов значение T непосредственно выбирает-

ся случайно равновероятно (см. выделенную строку на Рис. 2.4). Поэтому

$$\mathsf{Adv}^{\mathrm{PRF}}_{\text{MGM2-MAC}[r,s]}(\mathcal{A}) = \Pr\left[\mathbf{Exp}^1(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}^0(\mathcal{A}) \to 1\right].$$

Заметим, что до выставления флага *bad* равным true (обозначим это событие как $\{bad = \mathsf{true}\}$) эксперименты $\mathbf{Exp}^0$ и $\mathbf{Exp}^1$ функционируют идентичным образом. Поэтому (согласно Лемме 2, [9]) верно следующее неравенство:

$$\Pr\left[\mathbf{Exp}^1(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}^0(\mathcal{A}) \to 1\right] \leqslant \Pr[bad = \mathsf{true}].$$

Оценим величину $\Pr[bad = \mathsf{true}]$. Без ограничения общности, будем считать, что нарушитель является детерминированным и делает q попарно различных запросов $(N_i, M^i),\ i = 1, \ldots, q$. Будем использовать обозначение $\mathsf{coll}^i,\ i = 2, \ldots, q$, для обозначения события, что флаг *bad* принял значение true во время обработки первых i запросов. Тогда,

$$\Pr[bad = \mathsf{true}] = \sum_{i=2}^{q} \Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right].$$

Оценим вероятность $\Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right]$ для любого $i = 2, \ldots, q$.

Заметим, что каждый i-й запрос является парой (N_i, M^i), где $M^i = M^i_1 \| \ldots \| M^i_{l_i},\ M^i_j \in \{0,1\}^n$, и определяется значениями $T_1, \ldots, T_{i-1}$, полученными в предыдущих запросах. Без ограничения общности, будем считать, что $l_1 = \ldots = l_i$. Действительно, если это не так, то мы всегда можем дополнить сообщение нулевыми блоками до длины $l := \max(l_1, \ldots, l_i)$. Данное дополнение не повлияет на значение имитовставки, а дополненные сообщения останутся попарно различными, так как $M^j_{l_j} \neq 0^n$. Поэтому значения $T_1, \ldots, T_{i-1}$ однозначно определяют l и пары $(N_1, M^1), \ldots, (N_i, M^i)$.

Для фиксированного N_j обозначим через $\widetilde{H_k^j}$, $j = 1, \ldots, i$; $k = 1, \ldots, l$, случайную величину $\widetilde{\rho}'(N_j \| 01 \| \mathrm{str}_{n-r-2}(k-1))$.

Заметим, что $\Pr\left[\widetilde{H_k^j} = B\right] = \dfrac{1}{2^n}$ для любого $B \in \{0,1\}^n$. Также заметим, что случайные величины $\widetilde{H_k^j}$ и $\widetilde{H_k^t}$ для любых $j \neq t$ и любого k независимы, при этом $\Pr\left[\widetilde{H_k^j} = \widetilde{H_k^t}\right] = 1$, тогда и только тогда, когда $N_k = N_j$.

Для краткости обозначим через $\widetilde{H^j}$ набор случайных величин $(\widetilde{H_1^j}, \ldots, \widetilde{H_\ell^j})$. Также для набора $H = (H_1, \ldots, H_\ell)$ с сообщения $M = M_1 \| \ldots \| M_\ell$ через $\tau(H, M)$ обозначим функцию $\mathsf{Set1}_r\left(\bigoplus\limits_{k=1}^{l} H_k \otimes M_k\right)$. Таким образом, мы имеем

$$\Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right] = \sum_{T_1,\ldots,T_{i-1}} \Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}} \cap \{\widetilde{T_j} = T_j\}_{j=1}^{i-1}\right],$$

где через $\widetilde{T_j}$ обозначены случайные величины $\mathrm{msb}_s(\widetilde{\rho}(\tau(\widetilde{H^j}, M^j)))$, и суммирование ведется по всем наборам $(T_1, \ldots, T_{i-1}) \in (\{0,1\}^s)^{i-1}$.

Для фиксированных $(N_1, M^1), \ldots, (N_i, M^i)$ введем следующие условия на множество $H^1, \ldots, H^i$, $H^j := (H_1^j, \ldots, H_\ell^j)$, $j = 1, \ldots, i$:

Условие E_1: $\forall\ j, t,\ 1 \leqslant j < t \leqslant i-1$: $\tau(H^j, M^j) \neq \tau(H^t, M^t)$.

Условие E_2: $\exists\ j,\ 1 \leqslant j \leqslant i-1$: $\tau(H^i, M^i) = \tau(H^j, M^j)$.

Для любых фиксированных $T_1, \ldots, T_{i-1}$, и следовательно, фиксированных $(N_1, M^1), \ldots, (N_i, M^i)$, событие $\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}$ возникает тогда и только тогда, когда случайные величины $\widetilde{H^1}, \ldots, \widetilde{H^i}$ приняли такие значения $H^1, \ldots, H^i$, для которых выполнены условия E_1 и E_2. Для краткости, мы будет обозначать события, что выполнены данные условия, таким же образом, а именно, через E_1 и E_2 соответственно.

Заметим, что фиксации значений H^j, $j = 1, \ldots, i$, приводит к фиксации значений $\tau_j := \tau(H^j, M^j)$. Поэтому

$$\Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right] = \sum_{T_1,\ldots,T_{i-1}} \Pr\left[\mathsf{E}_1 \cap \mathsf{E}_2 \cap \{\widetilde{T}_j = T_j\}_{j=1}^{i-1}\right] =$$

$$= \sum_{T_1,\ldots,T_{i-1}} \sum_{\substack{H^1,\ldots,H^i\colon \\ \mathsf{E}_1\cap\mathsf{E}_2}} \Pr\left[\{\widetilde{H^j} = H^j\}_{j=1}^{i} \cap \{\mathrm{msb}_s(\widetilde{\rho}(\tau_j)) = T_j\}_{j=1}^{i-1}\right] =$$

$$= \sum_{T_1,\ldots,T_{i-1}} \sum_{\substack{H^1,\ldots,H^i\colon \\ \mathsf{E}_1\cap\mathsf{E}_2}} \Pr\left[\{\widetilde{H^j} = H^j\}_{j=1}^{i}\right] \cdot \Pr\left[\{\mathrm{msb}_s(\widetilde{\rho}(\tau_j)) = T_j\}_{j=1}^{i-1}\right].$$

Здесь суммирование ведется по всем $H^1, \ldots, H^i$, $H^j \in (\{0,1\}^n)^l$, для которых выполнены условия E_1 и E_2. Последний переход верен в силу того, что величины $\widetilde{\rho}$ и $\widetilde{H^j}$, $j = 1, \ldots, i$, независимы.

Рассмотрим значение $\Pr\left[\{\mathrm{msb}_s(\widetilde{\rho}(\tau_j)) = T_j\}_{j=1}^{i-1}\right]$. Для любых $T_1, \ldots, T_{i-1}$ и $H^1, \ldots, H^{i-1}$, для которых выполнено условие E_1, данная вероятность в точности равна вероятности выбора функции ρ, для которой $i-1$ фиксированным входам соответствуют выходы с фиксированными первыми s битами, а именно, $\dfrac{1}{2^{s(i-1)}}$. Таким образом:

$$\Pr\left[\mathsf{coll}^i \cap \overline{\mathsf{coll}^{i-1}}\right] = \sum_{T_1,\ldots,T_{i-1}} \sum_{\substack{H^1,\ldots,H^i\colon \\ \mathsf{E}_1\cap\mathsf{E}_2}} \Pr\left[\{\widetilde{H^j} = H^j\}_{j=1}^{i}\right] \cdot \frac{1}{2^{s(i-1)}} =$$

$$= \frac{1}{2^{s(i-1)}} \sum_{T_1,\ldots,T_{i-1}} \Pr[\mathsf{E}_1 \cap \mathsf{E}_2] \leqslant \frac{1}{2^{s(i-1)}} \sum_{T_1,\ldots,T_{i-1}} \Pr[\mathsf{E}_2].$$

Теперь рассмотрим $\Pr[\mathsf{E}_2]$ при фиксированных $T_1, \ldots, T_{i-1}$, и, сле-

довательно, при фиксированных $(N_1, M^1), \ldots, (N_i, M^i)$.

$$\Pr[\mathsf{E}_2] = \Pr\Big[\exists\ j,\ 1 \leqslant j \leqslant i-1\colon\ \tau(\widetilde{H^i}, M^i) = \tau(\widetilde{H^j}, M^j)\Big] =$$
$$= \Pr\left[\bigcup_{j=1}^{i-1}\Big\{\tau(\widetilde{H^i}, M^i) = \tau(\widetilde{H^j}, M^j)\Big\}\right] \leqslant \sum_{j=1}^{i-1}\Pr\Big[\tau(\widetilde{H^i}, M^i) = \tau(\widetilde{H^j}, M^j)\Big].$$

Оценим значение $p := \Pr\Big[\tau(\widetilde{H^i}, M^i) = \tau(\widetilde{H^j}, M^j)\Big]$ для любых $j = 1, \ldots, i-1$. Рассмотрим два случая:

1. $N_i \neq N_j$ (в данном случае $\widetilde{H_k^i}$ и $\widetilde{H_k^j}$ являются независимыми).
2. $N_i = N_j$ (в данном случае $\widetilde{H_k^i}$ и $\widetilde{H_k^j}$ являются зависимыми).

Первый случай: $p = \dfrac{\#\{H^i, H^j\colon \tau(H^i, M^i) = \tau(H^j, M^j)\}}{2^{2nl}}$.

$$\#\{H^i, H^j\colon \tau(H^i, M^i) = \tau(H^j, M^j)\} =$$
$$= \#\Big\{H^i, H^j\colon \bigoplus_{k=1}^{l} H_k^i \otimes M_k^i = \bigoplus_{k=1}^{l} H_k^j \otimes M_k^j\Big\} +$$
$$+ \#\Big\{H^i, H^j\colon \bigoplus_{k=1}^{l} H_k^i \otimes M_k^i = \bigoplus_{k=1}^{l} H_k^j \otimes M_k^j \oplus \mathsf{Set1}_r(0^n)\Big\}.$$

Так как $M_{\ell_i}^i \neq 0^n$ для любого i, мощность множества равна $2 \cdot 2^{n(2l-1)}$, и $p = \dfrac{2}{2^n}$.

Второй случай: $p = \dfrac{\#\{H^i\colon \tau(H^i, M^i) = \tau(H^i, M^j)\}}{2^{nl}}$.

$$\#\{H^i\colon \tau(H^i, M^i) = \tau(H^i, M^j)\} =$$
$$= \#\Big\{H^i\colon \bigoplus_{k=1}^{l} H_k^i \otimes (M_k^i \oplus M_k^j) = 0^n\Big\} +$$
$$+ \#\Big\{H^i\colon \bigoplus_{k=1}^{l} H_k^i \otimes (M_k^i \oplus M_k^j) = \mathsf{Set1}_r(0^n)\Big\}.$$

Так как для одинаковых нонсов M^i и M^j должны быть различными, существует k, такой что $M_k^i \oplus M_k^j \neq 0^n$. Таким образом, мощность множества равна $2 \cdot 2^{n(l-1)}$, и $p = \dfrac{2}{2^n}$.

Суммируя, получаем искомую оценку:

$$\Pr[bad = \mathsf{true}] = \sum_{i=2}^{q} \frac{1}{2^{s(i-1)}} \sum_{T_1,\ldots,T_{i-1}} \sum_{j=1}^{i-1} \frac{2}{2^n} = \sum_{i=2}^{q} \frac{i-1}{2^{n-1}} = \frac{q(q-1)}{2^n}.$$

□

Теперь вспомогательную модель UF-CMA для схем выработки имитовставки с нонсом и получим оценку в данной модели для MGM2-MAC.

Определение 2.1.2. Для схемы MAC преобладание нарушителя $\mathcal{A}$ в модели UF-CMA определяется следующим образом:

$$\mathsf{Adv}_{\mathsf{MAC}}^{\text{UF-CMA}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_{\mathsf{MAC}}^{\text{UF-CMA}}(\mathcal{A}) \to 1\right],$$

где эксперимент $\mathbf{Exp}_{\mathsf{MAC}}^{\text{UF-CMA}}(\mathcal{A})$ описан ниже:

$\mathbf{Exp}_{\mathsf{MAC}}^{\text{UF-CMA}}(\mathcal{A})$	Oracle $Tag(N, M)$	Oracle $Verify(N, M, T)$
$K \leftarrow \mathsf{MAC.Gen}(\,)$	**if** $(N, M) \in sent$:	$res \leftarrow \mathsf{MAC.Vf}(K, N, M, T)$
$sent \leftarrow \emptyset$	**return** $\perp$	**if** $res \wedge ((N, M) \notin sent)$:
$win \leftarrow \mathsf{false}$	$T \leftarrow \mathsf{MAC.Tag}(K, N, M)$	$win \leftarrow \mathsf{true}$
$\mathcal{A}^{Tag, Verify}(\,)$	$sent \leftarrow sent \cup \{(N, M)\}$	**return** res
return win	**return** T	

Используя Предложение 7.3 [9] и Лемму 2.1.1, легко доказать следующее утверждение.

Следствие 2.1.2. Для любого нарушителя $\mathcal{A}$ в модели UF-CMA, делающего не боле q_T запросов к оракулу Tag и не более q_V запросов к оракулу $Verify$:

$$\mathsf{Adv}^{\text{UF-CMA}}_{\text{MGM2-MAC}[r,s]}(\mathcal{A}) \leqslant \frac{q(q-1)}{2^n} + \frac{q_V}{2^s},$$

где $q = q_T + q_V$.

Оценка уровня стойкости MGM2[$\mathcal{F}_{2^n}$] в модели MRAE-int**.** Для завершения доказательства Теоремы 2.1.1 докажем следующую лемму.

Лемма 2.1.2. *Для любого нарушителя $\mathcal{A}$ в модели* MRAE-int*, делающего не более q_E запросов к оракулу $Encrypt$ и не более q_D запросов к оракулу $Decrypt$, существует нарушитель $\mathcal{B}$ в модели* UF-CMA*, делающий не более q_E запросов к оракулу Tag и не более q_D запросов к оракулу $Verify$, такой что*

$$\mathsf{Adv}^{\text{MRAE-int}}_{\text{MGM2}[\mathcal{F}_{2^n},r,s]}(\mathcal{A}) \leqslant \mathsf{Adv}^{\text{UF-CMA}}_{\text{MGM2-MAC}[r,s]}(\mathcal{B})$$

Доказательство. Построим нарушителя $\mathcal{B}$, который использует нарушителя $\mathcal{A}$ в качестве черного ящика. Нарушитель $\mathcal{B}$ (см. Рис. 2.5) перехватывает запросы нарушителя $\mathcal{A}$ и самостоятельно их обрабатывает с использованием своих оракулов. Для прямого и обратного преобразования данных $\mathcal{B}$ реализует процедуру «lazy sampling» (подробнее, см. [9]) для функции ρ'', то есть вместо случайного выбора функции ρ'' в начале эксперимента, нарушитель определяет значения функции на входах непосредственно в процессе обработки запросов и ведет таблицу уже определенных переходов. Более формально, нарушитель выбирает значение b случайно равновероятно из множества $\{0,1\}^n$, если вход a ранее не

встречался, и использует уже ранее определенное значение, записанное в таблице, иначе. Для вычисления/проверки имитовставки нарушитель $\mathcal{B}$ реализует процедуру дополнения и отправляет соответствующие запросы своему оракулу.

$\mathcal{B}_{\mathcal{A}}^{Tag,Verify}$

$\rho'' \xleftarrow{\mathcal{U}} \mathcal{F}_{2^n}$ // lazy sampling

return $\mathcal{A}^{SEncrypt,SDecrypt}(\,)$

$SEncrypt(N, A, P)$

$h \leftarrow |A|_n, t \leftarrow |P|_n$

. . . . . .

for $i = 1 \ldots t$ **do**:

$\Gamma_i \leftarrow \rho''(N \| 00 \| \mathrm{str}_{n-r-2}(i-1))$

$C \leftarrow P \oplus \mathrm{msb}_{|P|}(\Gamma_1 \| \ldots \| \Gamma_t)$

. . . . . .

$a \leftarrow n|A|_n - |A|$

$c \leftarrow n|C|_n - |C|$

$len \leftarrow \mathrm{str}_{n/2}(|A|) \| \mathrm{str}_{n/2}(|C|)$

$M \leftarrow A \| 0^a \| C \| 0^c \| len$

. . . . . .

$T \leftarrow Tag(N, M)$

return (C, T)

Oracle $SDecrypt(N, A, C, T)$

$h \leftarrow |A|_n, t \leftarrow |C|_n$

. . . . . .

$a \leftarrow n|A|_n - |A|$

$c \leftarrow n|C|_n - |C|$

$len \leftarrow \mathrm{str}_{n/2}(|A|) \| \mathrm{str}_{n/2}(|C|)$

$M \leftarrow A \| 0^a \| C \| 0^c \| len$

. . . . . .

if $Verify(N, M, T) = \mathsf{false}$:

return $\perp$

. . . . . .

for $i = 1 \ldots t$ **do**:

$\Gamma_i \leftarrow \rho''(N \| 00 \| \mathrm{str}_{n-r-2}(i-1))$

$P \leftarrow C \oplus \mathrm{msb}_{|C|}(\Gamma_1 \| \ldots \| \Gamma_t)$

return P

Рис. 2.5. Нарушитель $\mathcal{B}$

Заметим, что нарушитель $\mathcal{B}$ симулирует для нарушителя $\mathcal{A}$ в точности эксперимент $\mathbf{Exp}^{\text{MRAE-int}}_{\text{MGM2}[\mathcal{F}_{2^n},r,s]}$. Действительно, так как для схемы $\text{MGM2}[\mathcal{F}_{2^n}, r, s]$ входы в случайную функцию в случае 1) вычисления имитовставки, 2) вычисления значения H_i и 3) вычисления значений Γ_i являются различными (в силу фиксации битов у входов), использование одной случайной функции абсолютно неотличимо от использования трех различных случайных функций ρ, ρ', ρ'' для этих трех случаев. Также заметим, что сообщения M, формируемые нарушителем $\mathcal{B}$, удовлетворяют условиям на множество сообщений для схемы $\text{MGM2-MAC}[r, s]$.

Если нарушитель $\mathcal{A}$ успешно формирует подделку, то нарушитель $\mathcal{B}$ также успешно формирует подделку в своем эксперименте $\mathbf{Exp}^{\text{UF-CMA}}_{\text{MGM2-MAC}[r,s]}(\mathcal{B})$. Действительно, непосредственной проверкой можно убедиться, что если $\mathcal{A}$ делает нетривиальный валидный запрос (N, A, C, T) к оракулу $Decrypt$, то нарушитель $\mathcal{B}$ делает соответствующий запрос $(N, M = A\|0^a\|C\|0^c\|len, T)$ к оракулу $Verify$, который также будет валидным и нетривиальным. □

2.1.3. Конфиденциальность

В настоящем подразделе приводится доказательство оценки сверху величины $\mathsf{Adv}^{\text{CPA-res}}_{\text{MGM2}[\mathcal{S}_{2^n},r,s]}(\mathcal{A})$ для любого нарушителя $\mathcal{A}$ в модели CPA-res, которая представлена в виде функции от длины блока и заданных ограничений на информационные ресурсы нарушителя.

Теорема 2.1.3 (Ахметзянова Л.Р.). *Для любого нарушителя $\mathcal{A}$ в модели* CPA-res*, делающего не более q_1 запросов к оракулу $Encrypt_1$ и не более q_2 запросов к оракулу $Encrypt_2$, где суммарная длина ассоциро-*

ванных данных не превосходит σ_A блоков, а суммарная длина открытых текстов не превосходит σ_P блоков, верно

$$\mathsf{Adv}^{\text{CPA-res}}_{\text{MGM2}[\mathcal{S}_{2^n},r,s]}(\mathcal{A}) \leqslant \frac{\sigma^2}{2^n} + \frac{q(q-1)}{2^{n-1}}, \tag{2.3}$$

где $q = q_1 + q_2$ и $\sigma = 2\sigma_P + \sigma_A + 2q$.

Доказательство. Сначала дважды применим Лемму [32] для замены семейства $\mathcal{S}_{2^n}$ на семейство $\mathcal{F}_{2^n}$ (это даст дополнительный член $\frac{\sigma^2}{2^n}$ в оценке) и далее получим оценку в модели CPA-res для схемы $\text{MGM2}[\mathcal{F}_{2^n}, r, s]$.

Оценку для схемы $\text{MGM2}[\mathcal{F}_{2^n}, r, s]$ можно получить аналогичным Теореме 2.1.1 образом. Действительно, преобразованные тексты C, полученные от оракула $Encrypt_1$, абсолютно неотличимы от случайных равновероятных строк, так как входы в случайную функцию ρ, используемые для вычисления значений Γ_i, всегда уникальны. Неотличимость имитовставок T, полученных от оракула $Encrypt_1$, от случайных равновероятных строк можно оценить путем построения двух нарушителей в модели PRF для схемы MGM2-MAC, которые используют нарушителя $\mathcal{A}$ в качестве черного ящика. Таким образом, $\mathsf{Adv}^{\text{CPA-res}}_{\text{MGM2}[\mathcal{F}_{2^n},r,s]}(\mathcal{A}) \leqslant \frac{q(q-1)}{2^{n-1}}$. □

2.1.4. Модификации MGM2

Режим MGM2 допускает прозрачное применение SIV-конструкции, идея которой была предложена в работе [13], с целью достижения стойкости в полной модели MRAE (целостность и конфиденциальность). Идея применения SIV-конструкции состоит в следующем:

1. Применить к сообщению (N, A, P) функцию выработки имитов-

ставки, которая должна быть стойкой в модели PRF с возможностью повтора нонса. Отметим, что для процедуры выработки имитовставки режима MGM2 показана стойкость именно в такой модели.

2. Применить к открытому тексту P стойкую в модели IND-CPA схему обеспечения конфиденциальности, положив в качестве вектора инициализации значение имитовставки, выработанное на предыдущем шаге. В случае режима MGM2 в качестве такой схемы целесообразно использовать режим CTR со случайно выбираемыми значениями нонсов (стойкость такой схемы в модели IND-CPA показана в работе [7]).

При этом обязательным условием является то, что функция выработки имитовставки и режим обеспечения конфиденциальности должны использовать независимые секреты. Для режима MGM2 выполнение данного условия можно обеспечить за счет фиксации битов входов в блочный симметричный алгоритм для различных целей.

Выводы

Разработана модификация режима MGM – режим MGM2, который обладает следующими лучшими свойствами в сравнении с оригиналом:

– В новом режиме нивелирована отрицательная особенность оригинальной конструкции: путем фиксации значений битов минимизирована вероятность возникновения коллизий, что позволило получить лучшие оценки уровня стойкости в целевых моделях.

– Для нового режима были доказаны оценки в расширенных моделях нарушителя MRAE (целостность) и CPA-res, учитывающих возможность повтора вектора инициализации. Оценка для целостности также позволяет использовать процедуру вычисления имитовставки в режиме MGM2 в качестве псевдослучайной функции.

– Конструкция режима MGM2 и полученные результаты по обоснованию его стойкости в рассмотренных моделях являются фундаментом для разработки режима, стойкого в полной модели MRAE (конфиденциальность и целостность), с помощью SIV-конструкции.

Отметим, что в отличие от оригинального режима MGM, конструкция нового режима определялась непосредственно в процессе получения как можно лучших оценок уровня стойкости в целевых формальных моделях. Такой подход к синтезу (в процессе анализа) позволяет получать лучшие и легко обосновываемые оценки уровня стойкости в целевых моделях и, как следствие, видится перспективным при синтезе и анализе других математических механизмов защиты данных. Данный подход также используется в следующей главе при разработке конструкций с внутренним преобразованием секрета.

Глава 3

Методы улучшения свойств AEAD-режимов

Вероятность успеха многих методов нарушения свойств безопасности в значительной степени зависит от количества данных, обрабатываемых на одном секрете [36, 14]. Этот факт приводит к необходимости ограничивать в используемых на практике системах данное количество. Максимальное количество данных, которые могут быть безопасно обработаны на одном секрете, называется *сроком жизни секрета*. Для схем на основе БСА одним из эффективных способов увеличения срока жизни секрета является механизм внутреннего преобразования секрета, описанный в документе [28].

Внутреннее преобразование секрета — это подход к увеличению срока жизни секрета, при котором каждое сообщение начинает обрабатываться с использованием начального секрета, который периодически изменяется с помощью специального преобразования после обработки определенного количества блоков сообщения (секции). Это количество является параметром режима, и далее будет называться размером секции. Размер секции фиксируется в рамках одного протокола, в котором данный режим используется.

Применение данной техники к режимам обеспечения конфиденциальности исследовалось Смышляевым С.В. в работах [40, 41]. В данных работах был разработан режим CTR-ACPKM с внутренним преобразованием секрета и доказано, что данный подход существенно улучшает уровень обеспечиваемой конфиденциальности, что позволяет увеличивать

срок жизни секрета.

В настоящей главе представлены результаты исследований возможности применения аналогичной техники для улучшения уровня обеспечения не только конфиденциальности, но и целостности, что является важным в контексте использования режимов одновременного обеспечения целостности и конфиденциальности информации.

3.1. Режим OMAC-ACPKM-Master

Описанный в Разделе 1.1 режим «8 бит» является комбинацией режима обеспечения конфиденциальности CTR и режима обеспечения целостности OMAC. Как уже упоминалось ранее, для режима CTR вопрос улучшения комбинаторных характеристик уже был исследован. Поэтому целесообразной является задача исследовать возможность улучшения комбинаторных характеристик режима OMAC с помощью подхода внутреннего преобразования секрета.

Далее в диссертации разработан режим OMAC-ACPKM-Master, в котором периодическое преобразование секрета происходит с помощью алгоритма ACPKM-Master. В отличие от алгоритма ACPKM, применяемого в режиме CTR, в данном алгоритме исходный секрет используется в качестве мастер-секрета для выработки секционных секретов и не используется для обработки данных. Выбор такого механизма обоснован тем, что в алгоритме OMAC значения входов в БСА являются непредсказуемыми, и поэтому при использовании алгоритма ACPKM возможно совпадение блоков секретов секций и значений имитовставки, что может привести к полной компрометации секретов.

3.1.1. Описание режима OMAC-ACPKM-Master

Определим режим OMAC-ACPKM-Master с параметрами N и T^*, который далее будем обозначать через OMAC-ACPKM-Master$_{N,T^*}$. Параметр N определяет размер секции в блоках, а параметр T^* является параметром внутренней процедуры выработки секционных секретов, который называется частотой смены мастер-секрета.

Схема данного режима представлена на Рис. 3.1. В процессе обработки сообщения M с длиной блока $m = |M|_n$ на исходном секрете K сообщение M разбивается на $l = \lceil m/N \rceil$ секций M^i (так что $M = M^1 \| M^2 \| \ldots \| M^l$), где $M^i \in \{0,1\}^{nN}$ для $i \in \{1, 2, ..., l-1\}$, $M^l \in \{0,1\}^r$, $r \leqslant nN$. Секция с индексом j обрабатывается на секретном материале $K^j \| K_1^j$, $j \in \{1, ..., l\}$, $K^j \in \{0,1\}^k$, $K_1^j \in \{0,1\}^n$, который вычисляется с помощью специальной процедуры ACPKM-Master$_{T^*}$:

$$K^1 \| K_1^1 \| \ldots \| K^l \| K_1^l = \text{ACPKM-Master}_{T^*}(K, d, l) = \\ = \text{CTR-ACPKM}_{T^*}.\mathsf{Enc}(K, 1^{n/2}, 0^{dln}),$$

где $d = \lceil k/n \rceil + 1$, а через CTR-ACPKM$_{T^*}$.$\mathsf{Enc}$ обозначена процедура обработки открытых текстов в режиме CTR-ACPKM, определенного в [40], с размером секции равным T^*. Заметим, что параметры d и l должны удовлетворять неравенству $d \cdot l \leqslant 2^{n/2-1}$.

Все секции за исключением последней обрабатываются процедурой CBCMAC, а последняя секция — процедурой TMAC (подробнее, см. [37]). Алгоритм вычисления имитовставки в виде псевдокода приведен на Рис. 3.2.

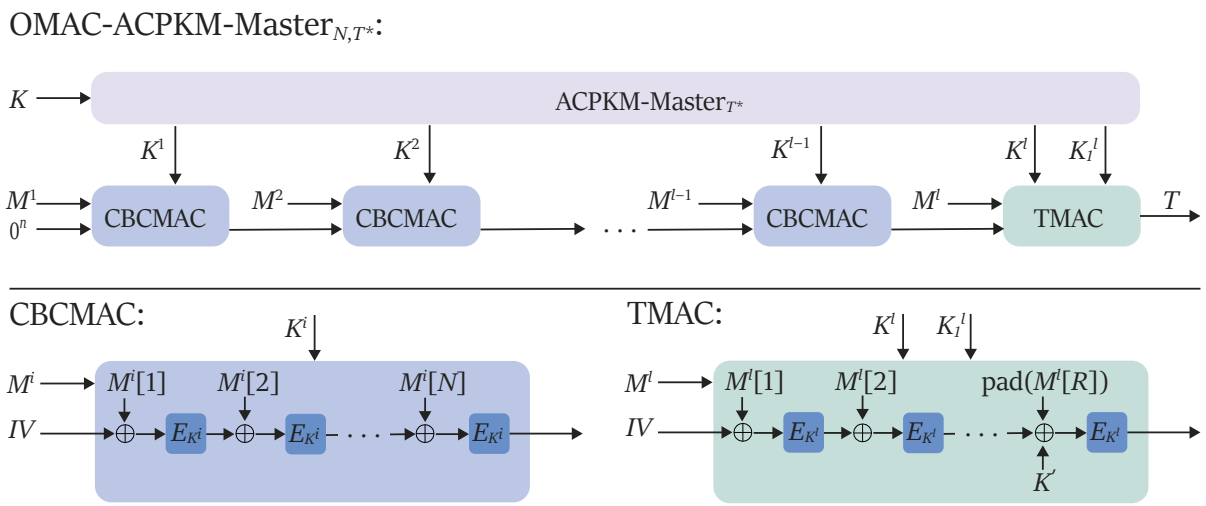

Рис. 3.1. Режим OMAC-ACPKM-Master$_{N,T^*}$ аутентифицирует сообщение $M \in \{0,1\}^*$ на секрете $K \in \{0,1\}^k$, вырабатывая имитовставку $T \in \{0,1\}^n$. Процедура ACPKM-Master$_{T^*}$ порождает секретный материал для каждой секции на основе исходного секрета K. Процедура CBCMAC обрабатывает все секции сообщения M за исключением последней $M^1, \ldots, M^{l-1}$. Процедура TMAC обрабатывает последнюю секцию M^l, размер которой не превосходит nN бит (на рисунке $R = |M^l|_n$). Секрет K' для процедуры TMAC равен K_1^l, если последний блок $M^l[R]$ полный, и равен $K_1^l \cdot \alpha$ в противном случае (операция «$\cdot$» является операцией умножения в конечном поле из 2^n элементов, элемент α является примитивным элементом в этом поле).

OMAC-ACPKM-Master$_{N,T^*}(K, M)$

$b = |M|_n$

$C_0 \leftarrow 0^n$

$l \leftarrow \lceil b/N \rceil$

$K^1 \| K_1^1 \| ... \| K^l \| K_1^l \leftarrow$ ACPKM-Master$_{T^*}(K, k/n + 1, l)$

for $i \leftarrow 1 to b - 1$:

  $j \leftarrow \lceil i/N \rceil$

  $C[i] \leftarrow E_{K^j}(M[i] \oplus C[i-1])$

$SK \leftarrow$ Gen_Subkey$(K_1^l, |M[b]|)$

if $|M[b]| = n$:

  $M'[b] \leftarrow M[b]$

else :

  $M'[b] \leftarrow M[b] \| 1 \| 0^{n-1-|M[b]|}$

$T \leftarrow E_{K^l}(M'[b] \oplus C[b-1] \oplus SK)$

return T

Gen_Subkey(K, r)

if $r = n$:

  return K

if $r < n$:

return $K \cdot \alpha$

Рис. 3.2. Режим выработки имитовставки OMAC-ACPKM-Master

Анализ стойкости механизма OMAC-ACPKM-Master проводится в формальной модели нарушителя PRF [37], в которой также проводился анализ режима OMAC. Получение верхних оценок уровня стойкости в данной модели позволяет установить, что исследуемый режим при случайном равновероятном выборе секрета является псевдослучайной функцией.

3.1.2. Оценка уровня стойкости в модели PRF

В данном подразделе представлена и доказана оценка сверху преобладаний всех нарушителей в модели PRF для режима OMAC-ACPKM-Master с внутренним преобразованием секрета.

Теорема 3.1.1 (Ахметзянова Л.Р.)**.** *Для любого нарушителя $\mathcal{A}$ в модели PRF, с вычислительными ресурсами не более t, максимальная длина запросов которого не более m блоков, а суммарная длина всех запросов не более σ блоков, существует нарушитель $\mathcal{B}$, такой что*

$$\mathsf{Adv}^{\mathrm{PRF}}_{\mathit{OMAC\text{-}ACPKM\text{-}Master}_{N,T^*}}(\mathcal{A}) \leqslant \left(l + \left\lceil \frac{dl}{T^*} \right\rceil\right) \cdot \mathsf{Adv}^{\text{PRP-CPA}}_{E}(\mathcal{B}) + \\ + f(d,l,T^*) + \frac{4\left(\sigma_1^2 + \ldots + \sigma_l^2\right)}{2^n},$$

где

$$f(d,l,T^*) = \begin{cases} \left\lceil \dfrac{dl}{T^*} \right\rceil \dfrac{(T^* + d - 1)^2}{2^n}, & \text{если } \lceil dl/T^* \rceil > 1, \\ \dfrac{(dl)^2}{2^n}, & \text{если } \lceil dl/T^* \rceil = 1, \end{cases}$$

$d = \lceil k/n \rceil + 1$, $l = \lceil m/N \rceil$, $dl \leqslant 2^{n/2-1}$, *через* σ_j *обозначена суммарная длина в блоках данных, обработанных с помощью секционного секрета* K^j, *при этом* $\sigma_j \leqslant 2^{n-1}$, $\sigma_1 + \ldots + \sigma_l = \sigma$. *Нарушитель* $\mathcal{B}$ *делает не более* $\max(\sigma_1, dl)$ *запросов, если* $dl \leqslant T^*$, *и не более* $\max(\sigma_1, T^* + d - 1)$ *запросов, иначе. Более того, вычислительные ресурсы* $\mathcal{B}$ *не превосходят величины* $t + cn(\sigma + d^2 l)$, *где* c *— это константа, зависящая только от модели вычислений.*

Доказательство представлено ниже. Анализ стойкости рассматриваемого режима проводится в три этапа.

На первом этапе (Раздел 3.1.3) доказывается, что стойкость режима OMAC-ACPKM-Master в модели PRF определяется стойкостью процедуры ACPKM-Master в модели PRG и некоторого абстрактного режима OMAC-RK в модели PRF. Данный режим в точности соотвествует исходному режиму OMAC-ACPKM-Master, за исключением того, что секционные секреты в данном режиме вырабатываются случайно равновероятно и независимо.

На втором этапе (Раздел 3.1.4) анализируются свойства процедуры ACPKM-Master выработки секционных секретов в модели PRG с точки зрения неотличимости выработанных секретов от секретов, выбранных случайно равновероятно и независимо. На третьем этапе (Раздел 3.1.5) проводится анализ абстрактного режима OMAC-RK (OMAC with Random Keys) в модели PRF.

3.1.3. Анализ стойкости OMAC-ACPKM-Master

Введем вспомогательные определения псевдослучайного генератора определенного типа (с внутренним состоянием) и модели нарушителя PRG для данного механизма.

Определение 3.1.1. *Псевдослучайным генератором* для множества состояний $\boldsymbol{K}$ будем называть пару алгоритмов $\mathcal{G} = (\mathcal{G}.\mathsf{K}, \mathcal{G}.\mathcal{N})$. Вероятностный алгоритм $\mathcal{G}.\mathsf{K}$ генерирует начальное состояние генератора $K^* \in \boldsymbol{K}$, а детерминированный алгоритм $\mathcal{G}.\mathcal{N}$, получая на вход состояние $K^* \in \boldsymbol{K}$ и натуральное число $h \in \mathbb{N}$, возвращает строку длины h блоков.

Определение 3.1.2. Преобладание нарушителя $\mathcal{A}$ в модели PRG для псевдослучайного генератора $\mathcal{G} = (\mathsf{K}, \mathcal{N})$ определяется следующим обра-

зом:

$$\mathsf{Adv}^{\mathrm{PRG}}_{\mathcal{G}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}^{\mathrm{PRG}-1}_{\mathcal{G}}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}^{\mathrm{PRG}-0}_{\mathcal{G}}(\mathcal{A}) \to 1\right],$$

где эксперименты $\mathbf{Exp}^{\mathrm{PRG}-1}_{\mathcal{G}}(\mathcal{A})$ и $\mathbf{Exp}^{\mathrm{PRG}-0}_{\mathcal{G}}(\mathcal{A})$ задаются следующим образом:

$\mathbf{Exp}^{\mathrm{PRG}-1}_{\mathcal{G}}(\mathcal{A})$	$\mathbf{Exp}^{\mathrm{PRG}-0}_{\mathcal{G}}(\mathcal{A})$
$h \leftarrow \mathcal{A},\ h \in \mathbb{N}$	$h \leftarrow \mathcal{A},\ h \in \mathbb{N}$
$K^* \leftarrow \mathcal{G}.\mathsf{K}()$	$s \xleftarrow{\mathcal{U}} \{0,1\}^{nh}$
$s \leftarrow \mathcal{G}.\mathcal{N}(K^*, h)$	$b' \leftarrow \mathcal{A}(s)$
$b' \leftarrow \mathcal{A}(s)$	**return** b'
return b'	

Алгоритм выработки секретов ACPKM-Master$_{T^*}$, где T^* определяет частоту смены мастер-секрета, можно интерпретировать в качестве псевдослучайного генератора, где алгоритмы ACPKM-Master$_{T^*}.\mathsf{K}$ и ACPKM-Master$_{T^*}.\mathcal{N}$ определяются следующим образом:

– ACPKM-Master$_{T^*}.\mathsf{K}() \to K^* :\ K^* \xleftarrow{\mathcal{U}} \{0,1\}^k$;

– ACPKM-Master$_{T^*}.\mathcal{N}(K^*, h) \to s :\ s = \text{CTR-ACPKM}_{T^*}(K^*, 1^{n/2}, 0^{nh})$.

Определение 3.1.3. Через OMAC-RK$_N$ (OMAC with Random Keys), где N — размер секции в блоках, будем обозначать следующий режим выработки имитовставки. Сообщения M, $|M| \leqslant m$, обрабатываются способом, описанным в разделе 3.1.1, причем секреты $K^1, \ldots, K^l \xleftarrow{\mathcal{U}} \{0,1\}^k$, $K^1_1, \ldots, K^l_1 \xleftarrow{\mathcal{U}} \{0,1\}^n$, где $l = \lceil m/N \rceil$, выбираются случайно равновероятно и независимо друг от друга.

Легко показать, что верно следующее утверждение.

Лемма 3.1.1. *Пусть $\mathcal{A}$ — нарушитель в модели* PRF *для режима выработки имитовставки OMAC-ACPKM-Master$_{N,T^*}$, суммарная длина запросов которого не более σ блоков, а максимальная длина не более m блоков. Тогда существует нарушитель $\mathcal{B}$ в модели* PRG *для преобразования ACPKM-Master$_{T^*}$, делающий запрос длины не более $\lceil m/N \rceil \cdot d$, где $d = \lceil k/n \rceil + 1$, и нарушитель $\mathcal{C}$ в модели* PRF *для режима выработки имитовставки OMAC-RK$_N$, суммарная длина запросов которого не более σ блоков, а максимальная длина не более m блоков, такие что*

$$\mathsf{Adv}^{\mathrm{PRF}}_{\mathit{OMAC\text{-}ACPKM\text{-}Master}_{N,T^*}}(\mathcal{A}) \leqslant \mathsf{Adv}^{\mathrm{PRG}}_{\mathit{ACPKM\text{-}Master}_{T^*}}(\mathcal{B}) + \mathsf{Adv}^{\mathrm{PRF}}_{\mathit{OMAC\text{-}RK}_N}(\mathcal{C}).$$

Приведенная лемма демонстрирует, что для получения оценки уровня стойкости целевого режима достаточно провести анализ стойкости отдельно для процедуры ACPKM-Master и отдельно для вспомогательной конструкции OMAC-RK в подходящих моделях нарушителя. Результаты анализа этих объектов представлены в следующих подразделах.

3.1.4. Анализ стойкости процедуры ACPKM-Master

В формулировке следующего утверждения используется модель нарушителя IND-CPNA (см. [40]).

Предложение 3.1.1. *Пусть $\mathcal{A}$ — нарушитель в модели* PRG *для генератора ACPKM-Master$_{T^*}$, запрашивающий не более h блоков. Тогда существует нарушитель $\mathcal{B}$ в модели* IND-CPA *для режима CTR-ACPKM$_{T^*}$, делающий не более одного запроса длины не более h блоков. Для всех чи-*

сел $T^* \in \mathbb{N} : n \mid T^*$, *выполнено соотношение*

$$\mathsf{Adv}^{\text{IND-CPNA}}_{CTR\text{-}ACPKM_{T^*}}(\mathcal{B}) \geqslant \mathsf{Adv}^{\text{PRG}}_{ACPKM\text{-}Master_{T^*}}(\mathcal{A}).$$

Доказательство данного утверждения непосредственно вытекает из определений моделей PRG и IND-CPNA.

Следствие 3.1.2. Пусть $\mathcal{A}$ — нарушитель в модели PRG для генератора ACPKM-Master$_{T^*}$ на основе БСА E, запрашивающий не более h блоков, $h \leqslant 2^{n/2-1}$. Тогда существует нарушитель $\mathcal{B}$ в модели PRP-CPA для БСА E, такой что

$$\mathsf{Adv}^{\text{PRG}}_{\text{ACPKM-Master}_{T^*}}(\mathcal{A}) \leqslant \left\lceil \frac{h}{T^*} \right\rceil \cdot \mathsf{Adv}^{\text{PRP-CPA}}_{E}(\mathcal{B}) + f(\lceil k/n \rceil, h, T^*),$$

где

$$f(s, h, T^*) = \begin{cases} \left\lceil \dfrac{h}{T^*} \right\rceil \dfrac{(T^* + s)^2}{2^n}, & \text{если } \lceil h/T^* \rceil > 1, \\ \dfrac{h^2}{2^n}, & \text{если } \lceil h/T^* \rceil = 1. \end{cases}$$

Нарушитель $\mathcal{B}$ делает не более $T^* + \lceil k/n \rceil$ запросов, если $h > T^*$, и не более h запросов, иначе.

Доказательство данного следствия следует из Теоремы 3.1 из [40] и Леммы 3.1.1.

3.1.5. Анализ стойкости режима OMAC-RK в модели PRF

Для получения оценок уровня стойкости для конструкции OMAC-RK в модели PRF вводится ряд вспомогательных математических объектов и промежуточных моделей нарушителя.

Определение 3.1.4. Через CBCMAC_P для $P \in \mathcal{S}_{2^n}$ будем обозначать функцию, которая принимает на вход сообщение $M = M[1]||\ldots||M[r],\ r \in \mathbb{N},\ M[1],\ldots,M[r] \in \{0,1\}^n$, и возвращает значение

$$\mathrm{CBCMAC}_P(M) = P(P(\ldots(P(M[1]) \oplus M[2])\ldots) \oplus M[r]).$$

Определение 3.1.5. Через CBC-E_P для $P \in \mathcal{S}_{2^n}$ будем обозначать функцию, которая принимает на вход сообщение $M \in \{0,1\}_n^*$ и возвращает значение

$$\text{CBC-E}_P(M) = P^{-1}(\mathrm{CBCMAC}_P(M)).$$

Определение 3.1.6. Через MAC_{P,K_1} для $P \in \mathcal{S}_{2^n}$ и блока $K_1 \in \{0,1\}^n$ будем обозначать функцию, которая принимает на вход сообщение $M \in \{0,1\}_n^*$ и возвращает значение

$$\mathrm{MAC}_{P,K_1}(M) = P(\text{CBC-E}_P(M) \oplus K_1).$$

Определение 3.1.7. Через MAC_{P_1,P_2} для $P_1, P_2 \in \mathcal{S}_{2^n}$ будем обозначать функцию, которая принимает на вход сообщение $M \in \{0,1\}_n^*$ и возвращает значение

$$\mathrm{MAC}_{P_1,P_2}(M) = P_2(\text{CBC-E}_{P_1}(M)).$$

Определение 3.1.8. Через $\mathcal{F}_E$ для БСА E с параметрами k и n будем обозначать следующее семейство:

$$\mathcal{F}_E = \left\{(\mathrm{CBCMAC}_{E_K}, \mathrm{MAC}_{E_K,K_1}, \mathrm{MAC}_{E_K,K_1\cdot\alpha}) \mid K \in \{0,1\}^k,\ K_1 \in \{0,1\}^n\right\},$$

где α — примитивный элемент поля $GF(2^n)$, $\cdot$ — операция умножения в поле.

Определение 3.1.9. Через $\mathcal{F}_{\mathcal{S}_{2^n}}$ будем обозначать следующее семейство:

$$\mathcal{F}_{\mathcal{S}_{2^n}} = \{(\mathrm{CBCMAC}_P, \mathrm{MAC}_{P,K_1}, \mathrm{MAC}_{P,K_1\cdot\alpha}) \mid P \in \mathcal{S}_{2^n}, K_1 \in \{0,1\}^n\},$$

где α — примитивный элемент поля $GF(2^n)$, $\cdot$ — операция умножения в поле.

Определение 3.1.10. Через $\mathcal{F}_{3\mathcal{S}_{2^n}}$ будем обозначать следующее семейство:

$$\mathcal{F}_{3\mathcal{S}_{2^n}} = \{(\mathrm{CBCMAC}_{P_1}, \mathrm{MAC}_{P_1,P_2}, \mathrm{MAC}_{P_1,P_3}) \mid P_1, P_2, P_3 \in \mathcal{S}_{2^n}\}.$$

Рассмотрим вспомогательную модель нарушителя $3\mathrm{PRF}_N$.

Определение 3.1.11. Преобладание нарушителя $\mathcal{A}$ в модели $3\mathrm{PRF}_N$ для конечного семейства

$$\mathcal{F} = \left\{(F_1, F_2, F_3),\ \begin{matrix} F_1 \in Func\left(\{0,1\}^{nN}, \{0,1\}^n\right), \\ F_2, F_3 \in Func\left(\{0,1\}_n^{\leqslant nN}, \{0,1\}^n\right) \end{matrix}\right\},$$

на котором определено некоторое распределение $\mathfrak{D}$, определяется следующим образом:

$$\mathsf{Adv}_{\mathcal{F}}^{3\mathrm{PRF}_N}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_{\mathcal{F}}^{3\mathrm{PRF}_N-1}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}_{\mathcal{F}}^{3\mathrm{PRF}_N-0}(\mathcal{A}) \to 1\right],$$

где эксперименты $\mathbf{Exp}_{\mathcal{F}}^{3\mathrm{PRF}_N-1}(\mathcal{A})$ и $\mathbf{Exp}_{\mathcal{F}}^{3\mathrm{PRF}_N-0}(\mathcal{A})$ задаются следующим образом:

$\underline{\mathbf{Exp}_{\mathcal{F}}^{3\mathrm{PRF}_N-b}(\mathcal{A})}$ $\underline{\mathsf{Oracle}\ \mathsf{F}_i^b(M)}$

if $b = 0$: **return** $F_i(M)$

$F_1 \xleftarrow{\mathcal{U}} Func\left(\{0,1\}^{nN}, \{0,1\}^n\right)$

$F_2, F_3 \xleftarrow{\mathcal{U}} Func\left(\{0,1\}_n^{\leqslant nN}, \{0,1\}^n\right)$

else :

$(F_1, F_2, F_3) \xleftarrow{\mathfrak{D}} \mathcal{F}$

$b' \leftarrow \mathcal{A}^{\mathsf{F}_1^b,\ \mathsf{F}_2^b,\ \mathsf{F}_3^b}$

return b'

Предложение 3.1.2. *Пусть $\mathcal{A}$ — нарушитель в модели* $3\mathrm{PRF}_N$ *для семейства $\mathcal{F}_E$, суммарная длина запросов которого не более σ блоков. Тогда существует нарушитель $\mathcal{B}$ в модели* PRP-CPA *для БСА E, делающий не более σ запросов к оракулу, и нарушитель $\mathcal{C}$ в модели* $3\mathrm{PRF}_N$ *для семейства $\mathcal{F}_{\mathcal{S}_{2^n}}$, суммарная длина запросов которого не более σ блоков, такие что*

$$\mathsf{Adv}_E^{\text{PRP-CPA}}(\mathcal{B}) \geqslant \mathsf{Adv}_{\mathcal{F}_E}^{3\mathrm{PRF}_N}(\mathcal{A}) - \mathsf{Adv}_{\mathcal{F}_{\mathcal{S}_{2^n}}}^{3\mathrm{PRF}_N}(\mathcal{C}).$$

Определение 3.1.12. Преобладание нарушителя $\mathcal{A}$ в модели 3PRP-CPA для семейства $\mathcal{F} \subseteq \mathcal{S}_{2^n}$ определяется следующим образом:

$$\mathsf{Adv}_{\mathcal{F}}^{3\text{PRP-CPA}}(\mathcal{A}) = \Pr\left[\mathbf{Exp}_{\mathcal{F}}^{3\text{PRP-CPA}-1}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}_{\mathcal{F}}^{3\text{PRP-CPA}-0}(\mathcal{A}) \to 1\right],$$

где эксперименты $\mathbf{Exp}_{\mathcal{F}}^{3\text{PRP-CPA}-1}(\mathcal{A})$ и $\mathbf{Exp}_{\mathcal{F}}^{3\text{PRP-CPA}-0}(\mathcal{A})$ задаются следующим образом:

$\underline{\mathbf{Exp}^{\text{3PRP-CPA}-b}_{\mathcal{S}_{2^n}}(\mathcal{A})}$ $\quad$ $\underline{\mathsf{Oracle}\ \mathsf{P}^b_i(M)}$

if $b = 0$: $\quad$ **return** $P_i(M)$

$P_1, P_2, P_3 \xleftarrow{\mathcal{U}} \mathcal{S}_{2^n}$

else :

$P \xleftarrow{\mathcal{U}} \mathcal{F},\ K_1 \xleftarrow{\mathcal{U}} \{0,1\}^n$

$P_1 \leftarrow P$

$P_2 \leftarrow P \circ [\oplus\ K_1]$

$P_3 \leftarrow P \circ [\oplus\ K_1 \cdot \alpha]$

$b' \leftarrow \mathcal{A}^{\mathsf{P}^b_1,\ \mathsf{P}^b_2,\ \mathsf{P}^b_3}$

return b'

Лемма 3.1.2 ([37]). *Пусть $\mathcal{A}$ — нарушитель в модели* 3PRP-CPA*, делающий не более q запросов к оракулу. Тогда*

$$\mathsf{Adv}^{\text{3PRP-CPA}}_{\mathcal{S}_{2^n}}(\mathcal{A}) \leqslant \frac{q^2}{2^n}.$$

Предложение 3.1.3. *Пусть $\mathcal{A}$ — нарушитель в модели* 3PRF_N *для семейства $\mathcal{F}_{\mathcal{S}_{2^n}}$, суммарная длина запросов которого не более σ блоков. Тогда существует нарушитель $\mathcal{B}$ в модели* 3PRP-CPA*, делающий не более σ запросов к оракулу, и нарушитель $\mathcal{C}$ в задаче* 3PRF_N *для семейства $\mathcal{F}_{3\mathcal{S}_{2^n}}$, суммарная длина запросов которого не более σ блоков, такие что*

$$\mathsf{Adv}^{\text{3PRP-CPA}}_{\mathcal{S}_{2^n}}(\mathcal{B}) \geqslant \mathsf{Adv}^{3\text{PRF}_N}_{\mathcal{F}_{\mathcal{S}_{2^n}}}(\mathcal{A}) - \mathsf{Adv}^{3\text{PRF}_N}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{C}).$$

Лемма 3.1.3. *Пусть натуральные $n, N, q_1, q_2, m_1, \ldots, m_{q_2}$ таковы, что $m_j \leqslant N$ и $q_1 N + m_1 + \ldots + m_{q_2} \leqslant 2^{n-1}$. Пусть также $T_1, \ldots, T_{q_1} \in \{0,1\}^n$ различны, а две группы строк $M^{(1)}_1, \ldots, M^{(1)}_{q_1}$ и $M^{(2)}_1, \ldots, M^{(2)}_{q_2}$ таковы, что:*

- $M_1^{(1)}, \ldots, M_{q_1}^{(1)} \in \{0,1\}^{n \cdot N}$ *различны;*
- $M_1^{(2)}, \ldots, M_{q_2}^{(2)}$ *различны и* $M_j^{(2)} \in \{0,1\}^{n \cdot m_j}$, $j = 1, \ldots, q_2$.

Будем говорить, что при случайном равновероятном выборе P *из множества* $\mathcal{S}_{2^n}$ *осуществилось событие* $Event$*, если одновременно выполнены следующие условия:*

- $CBCMAC_P(M_j^{(1)}) = T_j$, $j = 1, \ldots, q_1$*;*
- $CBC\text{-}E_P(M_1^{(2)}), \ldots, CBC\text{-}E_P(M_{q_2}^{(2)})$ *различны.*

Тогда

$$\Pr[Event] \geqslant \frac{1}{2^{q_1 n}} \left(1 - \frac{2(q_1 N + m_1 + \ldots + m_{q_2})^2}{2^n}\right).$$

Доказательство. Первый шаг доказательства состоит в построении вероятностного алгоритма, который гарантированно строит перестановку из $\mathcal{S}_{2^n}$, для которой выполнены условия события $Event$. Далее мощность множества перестановок, которые могут быть порождены данным алгоритмом, оценивается снизу. Преобразовав отношение полученной оценки к мощности множества $\mathcal{S}_{2^n}$, получим искомую оценку вероятности $\Pr[Event]$.

Опишем вероятностный алгоритм построения перестановки $P \in \mathcal{S}_{2^n}$, для которой выполнены условия события $Event$. Данный алгоритм строит перестановку P, определяя образы $P(x)$ строк $x \in \{0,1\}^n$. При этом изначально считаем, что ни для одной строки x ее образ $P(x)$ не определен. Через $Domain(P)$ будем обозначать множество строк x, чей образ $P(x)$ уже определен, а через $Free(P)$ будем обозначать множество строк из $\{0,1\}^n$, еще не поставленных в соответствие какой-либо

строке x в качестве образа. Так, в начале работы алгоритма $Domain(P) = \emptyset$, а $Free(P) = \{0,1\}^n$. Через $\mathcal{T}$ обозначим множество $\{T_1, \ldots, T_{q_1}\}$. Для множеств $A, B \subseteq \{0,1\}^n$ через $A \oplus B$ будем обозначать множество $\{a \oplus b \mid a \in A, b \in B\}$ (справедливо неравенство $|A \oplus B| \leqslant |A| \cdot |B|$).

Перейдем к описанию алгоритма. Напомним, что при вычислении значений функций CBCMAC_P или $\mathrm{CBC\text{-}E}_P$ блоки входной строки используются последовательно. Через $X_i^{(k)}[j]$ в описании алгоритма обозначается строка, которая поступает на вход перестановке P непосредственно после прибавления j-ого блока сообщения $M_i^{(k)}$ к текущему внутреннему состоянию. В этих обозначениях условия события $Event$ записываются следующим образом: $P(X_i^{(1)}[N]) = T_i$, $i = 1, \ldots, q_1$, и $X_1^{(2)}[m_1], \ldots, X_{q_2}^{(2)}[m_{q_2}]$ различны. Все $X_i^{(k)}[j]$ кроме первых ($X_i^{(k)}[1]$) зависят от перестановки P. В основной части алгоритма образы $P(X_i^{(k)}[j])$ определяются последовательно для всех j кроме последних (N-го для $k = 1$ и m_i для $k = 2$) так, чтобы были выполнены следующие условия:

1. строки $X_i^{(k)}[j]$ для различных i, k, j совпадают только в том случае, если они не могут отличаться хотя бы для какой-то перестановки P (так происходит, если все предшествующие блоки сообщений совпадают);

2. образы $P(X_i^{(k)}[j])$ выбираются не равными ни одной из строк $T_1, \ldots, T_{q_1}$, т.к. эти строки используются для определения образов $P(X_1^{(1)}[N]), \ldots, P(X_{q_1}^{(1)}[N])$, являющихся значениями функции CBCMAC_P от строк первой группы.

Легко видеть, что для определенной с учетом этих требований перестановки, условия события $Event$ будут выполнены.

Описание алгоритма:

1. $X_1^{(1)}[1] \leftarrow M_1^{(1)}[1], \ldots, X_{q_1}^{(1)}[1] \leftarrow M_{q_1}^{(1)}[1]$
2. $X_1^{(2)}[1] \leftarrow M_1^{(2)}[1], \ldots, X_{q_2}^{(2)}[1] \leftarrow M_{q_2}^{(2)}[1]$
3. $Defined \leftarrow \{X_1^{(1)}[1], \ldots, X_{q_1}^{(1)}[1], X_1^{(2)}[1], \ldots, X_{q_2}^{(2)}[1]\}$
4. for $j \leftarrow 1$ to $N-1$ do
5. for $k \leftarrow 1$ to 2 do
6. for $i \leftarrow 1$ to q_k do
7. if $((k=1)$ or $(k=2$ and $j \leqslant m_i - 1))$ and $(X_i^{(k)}[j] \notin Domain(P))$ then
8. $Equal \leftarrow \{(k', i') \mid X_i^{(k)}[j] = X_{i'}^{(k')}[j],\ k' = 1, 2,\ i' = 1, \ldots, q_{k'}\}$;
9. $Bad \leftarrow Defined \oplus \{M_{i'}^{(k')}[j+1] \mid (k', i') \in Equal\}$;
10. $P(X_i^{(k)}[j]) \stackrel{\mathcal{U}}{\leftarrow} Free(P) \setminus (Bad \cup \mathcal{T})$;
11. for all $(k', i') \in Equal$ do
12. $X_{i'}^{(k')}[j+1] \leftarrow P(X_i^{(k)}[j]) \oplus M_{i'}^{(k')}[j+1]$;
13. $Add \leftarrow \{X_{i'}^{(k')}[j+1] \mid (k', i') \in Equal\}$;
14. $Defined \leftarrow Defined \cup Add$;
15. for $i \leftarrow 1$ to q_1 do $P(X_{(i)}^1[N]) \leftarrow T_i$;
16. Доопределить образы в перестановке P произвольным образом строками множества $Free(P)$.

Отметим, что на шагах с 8 по 14 осуществляется определение образа для совпадающих строк $X_i^{(k)}[j]$ (они совпадают только в случае равенства префиксов строк $M_i^{(k)}$). При этом образ $P(X_i^{(k)}[j])$ на шаге 10 задается так, чтобы $P(X_i^{(k)}[j])$ при сложении с любым из следующих блоков $M_{i'}^{(k')}[j+1]$ не попал в строки $Defined$. Для этого используется множество Bad. Невозможность выбора ранее использованной строки для определения нового образа обеспечивается множеством $Free(P)$. Таким образом, обеспечивается выполнение второго условия $Event$. Первое выполняется за счет за счет шага 15.

Для удобства дальнейшего изложения введем дополнительные обозначения и отметим некоторые свойства описанного алгоритма. Через l_0 обозначим мощность множества $Defined$ после выполнения шага 3, а через l_t, $t = 1, 2, \ldots$, обозначим мощности множеств Add на шаге 13 после определения t-ого образа в перестановке P. Заметим, что множество Add никогда не пересекается с множеством $Defined$, поэтому после определения t-го образа в перестановке P справедливо $|Defined| = l_0 + l_1 + \ldots + l_t$. Также заметим, что мощность множества $\{M_{i'}^{(k')}[j+1] \mid (k', i') \in Equal\}$, участвующего в определении множества Bad, совпадает с мощностью множества Add, которое будет определено на этой же итерации цикла на шаге 13 (Add определяется прибавлением к элементам множества $\{M_{i'}^{(k')}[j+1] \mid (k', i') \in Equal\}$ одной и той же строки).

Перейдем к оценке мощности множества возможных результатов работы алгоритма. Искомая мощность равна произведению мощностей множеств, из которых выбирается образ $P(X_i^{(k)}[j])$ на шаге 10, и мощности множества $Free(P)$ на шаге 16. При определении t-го образа мощность

множества $Free(P) \setminus (Bad \cup \mathcal{T})$ не превосходит следующего значения:

$$2^n - (t-1) - q_1 - ((l_0 + \ldots + l_{t-1}) \cdot l_t).$$

Действительно,

$$|Bad| = |Defined \oplus \{M_{i'}^{(k')}[j+1] \mid (k', i') \in Equal\}| \leqslant (l_0 + \ldots + l_{t-1}) \cdot l_t,$$

а $|Free(P)| = 2^n - (t-1)$, $|\mathcal{T}| = q_1$.

Через s обозначим количество образов в перестановке P, определенных перед началом исполнения шага 15.

Заметим, что $s \leqslant q_1(N-1) + (m_1 - 1) + \ldots + (m_{q_2} - 1)$. Таким образом, для вероятности события $Event$ справедливо соотношение:

$$\Pr[Event] \geqslant \frac{(2^n - s - q_1)! \cdot \prod_{t=1}^{s}(2^n - (t-1) - (q_1 + (l_0 + \ldots + l_{t-1})l_t))}{(2^n)!} =$$

$$= \frac{1}{(2^n - s) \cdot \ldots \cdot (2^n - s - q_1 + 1)} \cdot \prod_{t=1}^{s} \frac{2^n - (t-1) - (q_1 + (l_0 + \ldots + l_{t-1})l_t)}{2^n - (t-1)} \geqslant$$

$$\geqslant \frac{1}{2^{nq_1}} \cdot \prod_{t=1}^{s} \left(1 - \frac{q_1 + (l_0 + \ldots + l_{t-1})l_t}{2^n - (t-1)}\right) \geqslant$$

$$\geqslant \frac{1}{2^{nq_1}} \cdot \left(1 - \sum_{t=1}^{s} \frac{q_1 + (l_0 + \ldots + l_{t-1})l_t}{2^n - (t-1)}\right).$$

Отметим, что мощность множества $Defined$ не может превзойти суммарного количества блоков в строках первой и второй группы, поэтому $l_0 + \ldots + l_s \leqslant q_1 N + m_1 + \ldots + m_{q_2}$. Также из условий леммы следует, что $s \leqslant q_1(N-1) + (m_1 - 1) + \ldots + (m_{q_2} - 1) \leqslant 2^{n-1}$. Учитывая это,

получаем следующую оценку, которая завершает доказательство леммы:

$$\sum_{t=1}^{s} \frac{q_1 + (l_0 + \ldots + l_{t-1})l_t}{2^n - (t-1)} \leqslant \frac{1}{2^{n-1}} \sum_{t=1}^{s} (q_1 + (l_0 + \ldots + l_{t-1})l_t) =$$

$$= \frac{1}{2^{n-1}} \sum_{t=1}^{s} q_1 + \frac{1}{2^{n-1}} \sum_{t=1}^{s} (l_0 + \ldots + l_{t-1})l_t =$$

$$= \frac{2q_1 \cdot s}{2^n} + \frac{(l_0 + \ldots + l_s)^2 - l_0^2 - \ldots - l_s^2}{2^n} \leqslant$$

$$\leqslant \frac{2q_1(q_1(N-1) + (m_1 - 1) + \ldots + (m_{q_2} - 1))}{2^n} +$$

$$+ \frac{(q_1 N + m_1 + \ldots + m_{q_2})^2}{2^n} \leqslant$$

$$\leqslant \frac{2(q_1 N + m_1 + \ldots + m_{q_2})^2}{2^n}.$$

□

Лемма 3.1.4. *Пусть натуральные* $n, N, q_1, q_2, q_3, m_1, \ldots, m_{q_2}, m_1, \ldots, m_{q_3}$ *таковы, что* $\sigma = q_1 N + m_1 + \ldots + m_{q_2} + m_1 + \ldots + m_{q_3} \leqslant 2^{n-1}$. *Зафиксируем* $q = q_1 + q_2 + q_3$ *битовых строк* $M_1^{(i)}, \ldots, M_{q_i}^{(i)}$, $1 \leqslant i \leqslant 3$, *таких что*

- $M_1^{(1)}, \ldots, M_{q_1}^{(1)} \in \{0,1\}^{n \cdot N}$ *различны;*
- $M_1^{(2)}, \ldots, M_{q_2}^{(2)}$ *различны и* $M_j^{(2)} \in \{0,1\}^{n \cdot m_j}$, $j = 1, \ldots, q_2$;
- $M_1^{(3)}, \ldots, M_{q_3}^{(3)}$ *различны и* $M_j^{(3)} \in \{0,1\}^{n \cdot m_j}$, $j = 1, \ldots, q_3$

и q *различных битовых строк* $T_1^{(i)}, \ldots, T_{q_i}^{(i)} \in \{0,1\}^n$, $1 \leqslant i \leqslant 3$, *таких что* $\{T_1^{(i)}, \ldots, T_{q_i}^{(i)}\}$ *— различные. Тогда количество перестановок* $P_1, P_2, P_3 \in \mathcal{S}_{2^n}$, *для которых выполняются следующие условия (*)*

- $CBCMAC_{P_1}(M_j^{(1)}) = T_j^{(1)}$, $j = 1, \ldots, q_1$;

- $MAC_{P_1,P_2}(M_j^{(2)}) = T_j^{(2)},\ j = 1, \ldots, q_2$;
- $MAC_{P_1,P_3}(M_j^{(3)}) = T_j^{(3)},\ j = 1, \ldots, q_3$;

не меньше $((2^n)!)^3 \left(1 - \frac{2\sigma^2}{2^n}\right) \frac{1}{2^{nq}}$.

Доказательство. Из Леммы 3.1.3 количество перестановок P_1, для которых одновременно выполняются условия

- $\text{CBCMAC}_{P_1}(M_j^{(1)}) = T_j^{(1)}$, $j = 1, \ldots, q_1$;
- $\text{CBC-E}_{P_1}(M_j^{(2)}) \neq \text{CBC-E}_{P_1}(M_k^{(2)})$, $j \neq k$, $j, k = 1, \ldots, q_2$.
- $\text{CBC-E}_{P_1}(M_j^{(3)}) \neq \text{CBC-E}_{P_1}(M_k^{(3)})$, $j \neq k$, $j, k = 1, \ldots, q_3$.

не менее $(2^n)! \cdot \frac{1}{2^{q_1 n}} \left(1 - \frac{2\sigma^2}{2^n}\right)$.

Заметим, что после фиксации перестановки P_1, удовлетворяющей данным условиям, аргументы для каждой из перестановок P_2 и P_3, определяемые при вычислении сообщений $M_j^{(2)}$ и $M_j^{(3)}$, являются различными. Поэтому для перестановок P_2 и P_3 достаточно зафиксировать q_2 и q_3 переходов, значения которых принадлежат множествам $\{T_1^{(2)}, \ldots, T_{q_2}^{(2)}\}$ и $\{T_1^{(3)}, \ldots, T_{q_3}^{(3)}\}$ соответственно.

Таким образом количество наборов из трех перестановок $P_1, P_2, P_3 \in \mathcal{S}_{2^n}$, для которых выполняются условия

- $\text{CBCMAC}_{P_1}(M_j^{(1)}) = T_j^{(1)},\ j = 1, \ldots, q_1$;
- $\text{MAC}_{P_1,P_2}(M_j^{(2)}) = T_j^{(2)},\ j = 1, \ldots, q_2$;
- $\text{MAC}_{P_1,P_3}(M_j^{(3)}) = T_j^{(3)},\ j = 1, \ldots, q_3$;

не менее

$$(2^n)! \cdot \frac{1}{2^{q_1 n}} \left(1 - \frac{2\sigma^2}{2^n}\right) \cdot (2^n - q_2)! \cdot (2^n - q_3)! \geqslant$$
$$\geqslant (2^n)! \cdot \frac{1}{2^{q_1 n}} \left(1 - \frac{2\sigma^2}{2^n}\right) \cdot \frac{(2^n)!}{2^{q_2 n}} \cdot \frac{(2^n)!}{2^{q_3 n}} = ((2^n)!)^3 \left(1 - \frac{2\sigma^2}{2^n}\right) \frac{1}{2^{qn}}.$$

□

Лемма 3.1.5. *Для любого нарушителя $\mathcal{A}$ в модели $3\mathrm{PRF}_N$ для трех перестановок, суммарная длина запросов которого не более σ блоков, причем $\sigma \leqslant 2^{n-1}$,*

$$\mathsf{Adv}^{3\mathrm{PRF}_N}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \leqslant \frac{2.5\sigma^2}{2^n}.$$

Доказательство. Не исключая общности будем рассматривать только детерминированных противников, так как для семейства $\mathcal{F}_{3\mathcal{S}_{2^n}}$ преобладание противника не зависит от количества его вычислительных ресурсов.

Пусть противник $\mathcal{A}$ сделал $q = q_1 + q_2 + q_3$ запросов:

- q_1 запросов $M_j^{(1)} \in \{0,1\}^{nN}, j = 1, \ldots, q_1$, к оракулу F_1^b и получил в ответ значения $T_j^{(1)} \in \{0,1\}^n, j = 1, \ldots, q_1$;
- q_2 запросов $M_j^{(2)} \in \{0,1\}_n^{\leqslant nN}, j = 1, \ldots, q_2$, к оракулу F_2^b и получил в ответ значения $T_j^{(2)} \in \{0,1\}^n, j = 1, \ldots, q_2$;
- q_3 запросов $M_j^{(3)} \in \{0,1\}_n^{\leqslant nN}, j = 1, \ldots, q_3$, к оракулу F_3^b и получил в ответ значения $T_j^{(3)} \in \{0,1\}^n, j = 1, \ldots, q_3$.

Так как противник является детерминированным, количество запросов q_1, q_2, q_3, значения запросов $M_j^{(1)}, M_j^{(2)}, M_j^{(3)}$ к оракулам и результат работы противника однозначно определены возвращаемыми оракулами значениями $T_j^{(1)}, T_j^{(2)}, T_j^{(3)}$.

Через $\mathcal{T}_{one}$ будем обозначать множество таких наборов из $q = q_1+q_2+q_3$ элементов из $\{0,1\}^n$

$$T = \{T_1^{(1)}, \ldots, T_{q_1}^{(1)}, T_1^{(2)}, \ldots, T_{q_2}^{(2)}, T_1^{(3)}, \ldots, T_{q_3}^{(3)}\},$$

для которых противник вернет 1 в качестве результата. Через $\mathcal{T}_{good}$ будем обозначать множество таких наборов T, для которых выполняется условие отсутствия коллизий среди его элементов. Заметим, что мощность множества, для которых не выполняется данное условие не более $\binom{q}{2}\frac{2^{qn}}{2^n}$. Тогда верна следующая оценка:

$$|\{T : T \in \mathcal{T}_{good} \cap \mathcal{T}_{one}\}| \geqslant |\mathcal{T}_{one}| - \binom{q}{2}\frac{2^{qn}}{2^n}.$$

Очевидно, что

$$\Pr\left[\mathbf{Exp}^{3\mathrm{PRF}_N-0}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \to 1\right] = \sum_{T\in\mathcal{T}_{one}} \frac{1}{2^{qn}} = \frac{|\mathcal{T}_{one}|}{2^{qn}}.$$

Теперь получим оценку снизу на $\Pr\left[\mathbf{Exp}^{3\mathrm{PRF}_N-1}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \to 1\right]$.

$$\Pr\left[\mathbf{Exp}^{3\mathrm{PRF}_N-1}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \to 1\right] = \frac{|\{(P_1,P_2,P_3) : 1 \leftarrow \mathcal{A}\}|}{((2^n)!)^3} \geqslant$$
$$\geqslant \sum_{T\in\mathcal{T}_{good}\cap\mathcal{T}_{one}} \frac{|\{(P_1,P_2,P_3)\ satisfying\ *3.1.4\}|}{((2^n)!)^3} \geqslant$$
$$\geqslant \left(|\mathcal{T}_{one}| - \binom{q}{2}\frac{2^{qn}}{2^n}\right)\cdot\left(1-\frac{2\sigma^2}{2^n}\right)\frac{1}{2^{nq}} \geqslant$$
$$\geqslant \frac{|\mathcal{T}_{one}|}{2^{qn}} - \binom{q}{2}\frac{1}{2^n} - \frac{2\sigma^2}{2^n} \geqslant \frac{|\mathcal{T}_{one}|}{2^{qn}} - \frac{2.5\sigma^2}{2^n}.$$

Таким образом,

$$\Pr\left[\mathbf{Exp}^{3\mathrm{PRF}_N-0}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}^{3\mathrm{PRF}_N-1}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \to 1\right] \leqslant \frac{2.5\sigma^2}{2^n}.$$

Проведя аналогичные рассуждения для значений $\Pr\left[\mathbf{Exp}^{3\mathrm{PRF}_N-0}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \to 0\right]$ и $\Pr\left[\mathbf{Exp}^{3\mathrm{PRF}_N-1}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \to 0\right]$, получим искомую оценку

$$\Pr\left[\mathbf{Exp}^{3\mathrm{PRF}_N-1}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}^{3\mathrm{PRF}_N-0}_{\mathcal{F}_{3\mathcal{S}_{2^n}}}(\mathcal{A}) \to 1\right] \leqslant \frac{2.5\sigma^2}{2^n}.$$

□

Лемма 3.1.6. *Пусть $\mathcal{A}$ — нарушитель в модели* $3\mathrm{PRF}_N$ *для семейства $\mathcal{F}_E$, суммарная длина запросов которого не более σ блоков, причем $\sigma \leqslant 2^{n-1}$. Тогда существует нарушитель $\mathcal{B}$ в модели* PRP-CPA *для БСА E, делающий не более σ запросов к оракулу, такой что*

$$\mathsf{Adv}^{\text{PRP-CPA}}_E(\mathcal{B}) \geqslant \mathsf{Adv}^{3\mathrm{PRF}_N}_{\mathcal{F}_E}(\mathcal{A}) - \frac{3.5\sigma^2}{2^n}.$$

Доказательство. Доказательство следует из предложений 3.1.2, 3.1.3 и лемм 3.1.2, 3.1.5. □

Определим семейство случайных функций OMAC-RSF $\subseteq Func(\{0,1\}^*_n, \{0,1\}^n)$, каждому элементу F которого соответствуют три функции G_1, G_2, G_3, где

1. $G_1 \in Func(\{0,1\}^{nN}, \{0,1\}^n)$;
2. $G_2 \in Func(\{0,1\}^*_n, \{0,1\}^n)$;
3. $G_3 \in Func(\{0,1\}^{\leqslant nN}_n, \{0,1\}^n)$.

Для сообщения $M \in \{0,1\}^*_n$, $M = M^1||\ldots||M^l$, $l \in \mathbb{N}$, где $M^1, \ldots, M^{l-1} \in \{0,1\}^{nN}$, $M^l \in \{0,1\}^{nR}$, $R \leqslant N$, функция F определяется описанным далее образом.

1. Если $|M| \leqslant nN$, то $F(M) = G_3(M)$;

2. Если $|M| > nN$, то

$$F(M) = G_2\left((G_1(M^1) \oplus M^2[1]) \| M^2[2] \| \ldots \| M^2[N] \| M^3 \| \ldots \| M^l\right);$$

Покажем, что семейство OMAC-RSF статистически неотличимо от семейства всех функций $Func(\{0,1\}_n^*, \{0,1\}^n)$.

Лемма 3.1.7. *Для любого нарушителя $\mathcal{A}$ в модели* PRF*, делающего не более q запросов,*

$$\mathsf{Adv}^{\mathrm{PRF}}_{OMAC\text{-}RSF}(\mathcal{A}) \leqslant \frac{q^2}{2^{n+1}};$$

Доказательство. Пусть нарушитель сделал q различных запросов $M_1, \ldots, M_q$. Рассмотрим следующие три случая:

1. $|M_i| \leqslant nN$ для всех $i \in \{1, \ldots, q\}$;

2. $M_i^1 = M_j^1$ для всех $i, j \in \{1, \ldots, q\}$, таких что $|M_i| > nN, |M_j| > nN$;

3. $\exists\ i, j \in \{1, \ldots, q\}$, такие что $|M_i| > nN$, $|M_j| > nN$, для которых $M_i^1 \neq M_j^1$.

Пусть в ответ на запрос M_i оракул вернул значение $T_i \in \{0,1\}^n$, $1 \leqslant i \leqslant q$. Через $T \in \{0,1\}^{n \times q}$ будем обозначать вектор $(T_1, \ldots, T_q)$.

По определению, для любых запросов $M_1, \ldots, M_q$

$$-\mathsf{Adv}^{\mathrm{PRF}}_{\mathrm{OMAC\text{-}RSF}}(\mathcal{A}) \leqslant \sum_{T \in \{0,1\}^{n \times q} : \Pr[T] < \frac{1}{2^{qn}}} \left(\frac{1}{2^{qn}} - \Pr[T]\right).$$

Очевидно, что для первого и второго случая $\mathsf{Adv}^{\mathrm{PRF}}_{\mathrm{OMAC\text{-}RSF}}(\mathcal{A}) = 0$.

Рассмотрим третий случай.

Через $Coll$ будем обозначать следущее событие: $\exists\ i, j \in \{1, \ldots, q\}$, такие что $|M_i| > nN$, $|M_j| > nN$, для которых

$$G_3(M_i^1) \oplus M_i^2[1] = G_3(M_j^1) \oplus M_j^2[1].$$

Рассмотрим подробнее величину $\Pr[T]$.

$$\Pr[T] = \Pr[T \mid Coll] \cdot \Pr[Coll] + \Pr\left[T \mid \overline{Coll}\right] \cdot \Pr\left[\overline{Coll}\right] \geqslant$$
$$\geqslant \Pr\left[T \mid \overline{Coll}\right] \cdot \Pr\left[\overline{Coll}\right] = \frac{1}{2^{qn}} \cdot \Pr\left[\overline{Coll}\right].$$

Вероятность события $Coll$ не превосходит $\binom{q}{2}\frac{1}{2^n}$. Поэтому

$$\Pr[T] \geqslant \frac{1}{2^{qn}}\left(1 - \binom{q}{2}\frac{1}{2^n}\right) \geqslant \frac{1}{2^{qn}}\left(1 - \frac{q^2}{2^{n+1}}\right).$$

Таким образом, для любого $\mathcal{A}$ в модели PRF

$$-\mathsf{Adv}^{\mathrm{PRF}}_{\text{OMAC-RSF}}(\mathcal{A}) \leqslant \sum_{T \in \{0,1\}^{n\times q}:\Pr[T] < \frac{1}{2^{qn}}} \left(\frac{1}{2^{qn}} - \Pr[T]\right) \leqslant$$
$$\leqslant 2^{nq} \cdot \frac{q^2}{2^{n+1}} \cdot \frac{1}{2^{qn}} \leqslant \frac{q^2}{2^{n+1}}.$$

Применяя аналогичные рассуждения, можно показать, что

$$\mathsf{Adv}^{\mathrm{PRF}}_{\text{OMAC-RSF}}(\mathcal{A}) =$$
$$= \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-1}_{\text{OMAC-RSF}}(\mathcal{A}) \to 1\right] - \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-0}_{\text{OMAC-RSF}}(\mathcal{A}) \to 1\right] =$$
$$= (1 - \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-0}_{\text{OMAC-RSF}}(\mathcal{A}) \to 1\right]) - (1 - \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-1}_{\text{OMAC-RSF}}(\mathcal{A}) \to 1\right]) =$$
$$= \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-0}_{\text{OMAC-RSF}}(\mathcal{A}) \to 0\right] - \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-1}_{\text{OMAC-RSF}}(\mathcal{A}) \to 0\right] =$$
$$= -\mathsf{Adv}^{\mathrm{PRF}}_{\text{OMAC-RSF}}(\mathcal{A}) \leqslant \frac{q^2}{2^{n+1}}.$$

□

Теорема 3.1.3. *Пусть $\mathcal{A}$ — нарушитель в модели* PRF *для режима выработки кода аутентификации OMAC-RK_N, суммарная длина запросов которого не более σ блоков, а максимальная длина не более m блоков. Тогда существует набор нарушителей $\mathcal{B}_j$, $j = 1, \ldots, \lceil m/N \rceil$, в задаче* $3\mathrm{PRF}_N$ *для семейства $\mathcal{F}_E$, суммарная длина запросов которых не более σ_j, причем $\sigma_j \leqslant 2^{n-1}$, $\sigma_1 + \ldots + \sigma_{\lceil m/N \rceil} = \sigma$, такие что*

$$\sum_{j=1}^{\lceil m/N \rceil} \mathsf{Adv}^{3\mathrm{PRF}_N}_{\mathcal{F}_E}(\mathcal{B}_j) \geqslant \mathsf{Adv}^{\mathrm{PRF}}_{OMAC\text{-}RK_N}(\mathcal{A}) - \frac{\left(\sigma_1^2 + \ldots + \sigma^2_{\lceil m/N \rceil}\right)}{2^{n+1}}.$$

Доказательство. Определим набор гибридных экспериментов $Hybrid_j(\mathcal{A})$ для $j \in \{0, 1, \ldots, \lceil m/N \rceil\}$. В эксперименте $Hybrid_j(\mathcal{A})$ оракул F, доступный $\mathcal{A}$, подменяется оракулом F_j, который работает описанным далее образом.

- Оракул F выбирает j секретов $K^1, K^2, \ldots, K^j \xleftarrow{\mathcal{U}} \{0,1\}^k$ и j блоков $K_1^1, K_1^2, \ldots, K_1^j \xleftarrow{\mathcal{U}} \{0,1\}^n$. Также оракул выбирает некоторые случайные функции $F_1, F_2 \xleftarrow{\mathcal{U}} Func(\{0,1\}_n^*, \{0,1\}^n)$.

- В ответ на запрос M, где $|M| \leqslant mn$, он возвращает значение $T \in \{0,1\}^n$, которое формируется следующим образом. Первые j секций обрабатываются с помощью первых выбранных j секретов и j блоков соотвественно. Если длина сообщения больше jnN, т.е. $M = M^1 || \ldots || M^j || M'$, $|M'| \leqslant (\lceil m/N \rceil - j)nN$, то оракул вычисляет значение $F_1(M'')$, если $n \mid |M'|$, либо $F_2(M'')$, если $n \nmid |M'|$, где сообщение M'' формируется следующим образом. Первый блок $M''[1]$ сообщения M'' получается прибавлением к первому блоку

сообщения $M' = \mathrm{pad}_n(M')$ результата обработки первых j секций:

$$M''[1] = M'[1] \oplus \mathrm{CBCMAC}_{E_{K^1},\dots E_{K^j}}(M^1||\dots||M^j).$$

Следующие блоки $M''[i]$ сообщения M'', $i \geqslant 2$, в точности равны блокам $M'[i]$ сообщения M'.

Результатом любого из описанных экспериментов считается то, что вернул в качестве результата нарушитель $\mathcal{A}$.

Заметим, эксперимент $Hybrid_{\lceil m/N \rceil}(\mathcal{A})$ в точности соответствует эксперименту $\mathbf{Exp}^{\mathrm{PRF}-1}_{\text{OMAC-RK}_N}(\mathcal{A})$, а эксперимент $Hybrid_0(\mathcal{A})$ — эксперименту $\mathbf{Exp}^{\mathrm{PRF}-0}_{\text{OMAC-RK}_N}(\mathcal{A})$, то есть справедливы следующие равенства:

$$\Pr\left[Hybrid_{\lceil m/N \rceil}(\mathcal{A}) \to 1\right] = \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-1}_{\text{OMAC-RK}_N}(\mathcal{A}) \to 1\right].$$

$$\Pr\left[Hybrid_0(\mathcal{A}) \to 1\right] = \Pr\left[\mathbf{Exp}^{\mathrm{PRF}-0}_{\text{OMAC-RK}_N}(\mathcal{A}) \to 1\right],$$

Последнее равенство следует из того факта, что семейство случайных функций, реализуемых с помощью пары случайных функций $F_1, F_2 \xleftarrow{\mathcal{U}} Func(\{0,1\}^*_n, \{0,1\}^n)$, где F_1 применяется к сообщения кратной блоку длины, F_2 применяется к сообщениям некратной блоку длины, дополненным до кратной длины функцией pad_n, статистически неотличимо от семейства случайных функции $F \xleftarrow{\mathcal{U}} Func(\{0,1\}^*, \{0,1\}^n)$, которые применяются к любым сообщениям.

Построим нарушителей $\mathcal{B}_j$ в модели $3\mathrm{PRF}_N$ для БСА E, использующих $\mathcal{A}$ в качестве черного ящика.

Нарушитель $\mathcal{B}_j$ в начале работы выбирает следующие случайные значения:

1. $j-1$ секретов $K^1, K^2, \ldots, K^{j-1} \xleftarrow{\mathcal{U}} \{0,1\}^k$;
2. $j-1$ блоков $K_1^1, K_1^2, \ldots, K_1^{j-1} \xleftarrow{\mathcal{U}} \{0,1\}^n$;
3. случайные функции $F_1, F_2 \xleftarrow{\mathcal{U}} Func(\{0,1\}_n^*, \{0,1\}^n)$ (реализует таблично в ходе атаки).

Нарушитель $\mathcal{B}_j$ моделирует оракул F^b для нарушителя $\mathcal{A}$. На запрос M, сделанный нарушителем $\mathcal{A}$, нарушитель $\mathcal{B}$ вычисляет значение кода аутентификации T следующим образом. Нарушитель $\mathcal{B}$ обрабатывает все секции сообщения, кроме j-ой, в соответствии с гибридным экспериментом $Hybrid_j(\mathcal{A})$. Для обработки j-ой секции он делает запрос к оракулам $\mathsf{F}_1^b,\ \mathsf{F}_2^b,\ \mathsf{F}_3^b$:

- если j-ая секция промежуточная, то он делает запрос $(M')^j$ к оракулу F_1^b;
- если j-ая секция последняя и ее длина кратна n, то он делает запрос $(M')^j$ к оракулу F_2^b;
- если j-ая секция последняя и ее длина не кратна n, то он делает запрос $(M')^j$ к оракулу F_3^b;

где сообщение $(M')^j$ формируется следующим образом. Первый блок $(M')^j[1]$ сообщения $(M')^j$ получается прибавлением к первому блоку секции $M^j = \mathrm{pad}_n(M^j))$ результата обработки первых $j-1$ секций, то есть

$$(M')^j[1] = M^j[1] \oplus \mathrm{CBCMAC}_{K^1,\ldots K^{j-1}}(M_1||\ldots||M_{j-1}).$$

Следующие блоки $(M')^j[i]$ сообщения $(M')^j$, $i \geqslant 2$, в точности равны блокам $M^j[i]$ сообщения M^j.

В качестве ответа нарушитель $\mathcal{B}$ возвращает то, что вернул нарушитель $\mathcal{A}$.

Справедливы соотношения

$$\Pr\left[\mathbf{Exp}_{\mathcal{F}_E}^{3\mathrm{PRF}_N-1}(\mathcal{B}_j)\to 1\right] = \Pr\left[Hybrid_j(\mathcal{A})\to 1\right],$$

$$\Pr\left[\mathbf{Exp}_{\mathcal{F}_E}^{3\mathrm{PRF}_N-0}(\mathcal{B}_j)\to 1\right] = \Pr\left[Hybrid'_{j-1}(\mathcal{A})\to 1\right],$$

где через $Hybrid'_j(\mathcal{A})$ обозначается модификация эксперимента $Hybrid_j(\mathcal{A})$: $j+1$-ая секция сообщения обрабатывается с помощью независимых случайных функций G_1, G_2, G_3 описанным далее образом.

- С помощью функции $G_1 \xleftarrow{\mathcal{U}} Func(\{0,1\}^{nN}, \{0,1\}^n)$ обрабатывается промежуточная j-ая секция.
- С помощью функции $G_2 \xleftarrow{\mathcal{U}} Func(\{0,1\}_n^{\leqslant nN}, \{0,1\}^n)$ обрабатывается последняя j-ая секция, длина которой кратна n.
- С помощью функции $G_3 \xleftarrow{\mathcal{U}} Func(\{0,1\}_n^{\leqslant nN}, \{0,1\}^n)$ обрабатывается последняя j-ая секция, длина которой не кратна n, дополненная функцией pad_n.

Тогда для преобладаний нарушителей $\mathcal{B}_j$ справедлива оценка

$$\sum_{j=1}^{\lceil m/N \rceil} \mathsf{Adv}^{3\mathrm{PRF}_N}_{\mathcal{F}_E}(\mathcal{B}_j) = \sum_{j=1}^{\lceil m/N \rceil} \Pr\left[Hybrid_j(\mathcal{A}) \to 1\right] -$$

$$- \sum_{j=1}^{\lceil m/N \rceil} \Pr\left[Hybrid'_{j-1}(\mathcal{A}) \to 1\right] =$$

$$= \Pr\left[Hybrid_{\lceil m/N \rceil}(\mathcal{A}) \to 1\right] - \Pr\left[Hybrid_0(\mathcal{A}) \to 1\right] +$$

$$+ \sum_{j=0}^{\lceil m/N \rceil - 1} \left(\Pr\left[Hybrid_j(\mathcal{A}) \to 1\right] - \Pr\left[Hybrid'_j(\mathcal{A}) \to 1\right]\right) =$$

$$= \mathsf{Adv}^{\mathrm{PRF}}_{\text{OMAC-RK}_N}(\mathcal{A}) + \sum_{j=0}^{\lceil m/N \rceil - 1} \left(\Pr\left[Hybrid_j(\mathcal{A}) \to 1\right] - \Pr\left[Hybrid'_j(\mathcal{A}) \to 1\right]\right).$$

По Лемме 3.1.7 для $\forall\, j = 0, \ldots, \lceil m/N \rceil - 1$ справедливо соотношение

$$\Pr\left[Hybrid_j(\mathcal{A}) \to 1\right] - \Pr\left[Hybrid'_j(\mathcal{A}) \to 1\right] = -\mathsf{Adv}^{\mathrm{PRF}}_{\text{OMAC-RSF}}(A'_j) -$$

$$- \mathsf{Adv}^{\mathrm{PRF}}_{\text{OMAC-RSF}}(A''_j) \geqslant -\frac{(q'_{j+1})^2}{2^{n+1}} - \frac{(q''_{j+1})^2}{2^{n+1}} \geqslant -\frac{\sigma^2_{j+1}}{2^{n+1}};$$

Где A'_j и A''_j — нарушители для OMAC-RSF в модели PRF, которые в точности реализуют эксперимент $Hybrid_j(\mathcal{A})$ для нарушителя $\mathcal{A}$, за исключением того, что вместо вычислений функций F_1 и F_2 соответственно делается q'_{j+1} (части сообщений кратной длины после обработки j секции) и q''_{j+1} (части сообщений некратной длины после обработки j секции) запросов к оракулам нарушителей.

Таким образом,

$$\sum_{j=1}^{\lceil m/N \rceil} \mathsf{Adv}^{3\mathrm{PRF}_N}_{\mathcal{F}_E}(\mathcal{B}_j) \geqslant \mathsf{Adv}^{\mathrm{PRF}}_{\text{OMAC-RK}_N}(\mathcal{A}) - \frac{\left(\sigma^2_1 + \ldots + \sigma^2_{\lceil m/N \rceil}\right)}{2^{n+1}}.$$

□

Лемма 3.1.8. *Пусть $\mathcal{A}$ — нарушитель в модели* PRF *для режима выработки кода аутентификации OMAC-RK$_N$, суммарная длина запросов которого не более σ блоков, а максимальная длина запросов не более m блоков. Тогда существует нарушитель $\mathcal{B}$ в модели* PRP-CPA *для БСА E, делающий не более σ_1, запросов, где σ_j — суммарная длина данных в блоках, обрабатываемая секретом j-секции, причем $\sigma_j \leqslant 2^{n-1}$, $\sigma_1 + \ldots + \sigma_{\lceil m/N \rceil} = \sigma$. Тогда*

$$\mathsf{Adv}^{\mathrm{PRF}}_{OMAC\text{-}RK_N}(\mathcal{A}) \leqslant \frac{4\left(\sigma_1^2 + \ldots + \sigma_{\lceil m/N \rceil}^2\right)}{2^n} + \left\lceil \frac{m}{N} \right\rceil \cdot \mathsf{Adv}^{\mathrm{PRP\text{-}CPA}}_{E}(\mathcal{B})$$

Доказательство. Доказательство непосредственно вытекает из леммы 3.1.6 и теоремы 3.1.3. □

3.1.6. Сравнительный анализ оценок

В настоящем разделе проводится сравнительный анализ оценок уровня стойкости для предлагаемого режима OMAC-ACPKM-Master с внутренним преобразованием секрета и для оригинального режима OMAC (см. [37]). Оценки представлены в Таблице 3.1.

Mode	$\mathsf{Adv}^{\mathrm{PRF}}_{\mathrm{Mode}}(\mathcal{A})$
OMAC	$\approx \frac{4\sigma^2 + 1}{2^{n+1}}$
OMAC-ACPKM-Master$_{N,\infty}$	$\approx \frac{4\left(\sigma_1^2 + \ldots + \sigma_l^2\right)}{2^{n+1}} + \frac{(dl)^2}{2^n}$

Таблица 3.1. Оценки уровня стойкости для режима OMAC и режима OMAC-ACPKM-Master$_{N,\infty}$ в модели PRF (в предположении стойкости блочного симметричного алгоритма).

Рассмотрим случай $l = 1$ (преобразование секрета не применялось). Заметим, что оценка для режима OMAC-ACPKM-Master$_{N,\infty}$ становится хуже, чем для оригинального режима OMAC в силу наличия слагаемого $d^2/2^n$, которое отвечает за дополнительное преобразование секрета перед обработкой сообщения. Однако значение $d = k/n$, как правило, является достаточно маленьким (для стандартных блочных БСА равно 2-4). Поэтому данное ухудшение справедливо считать пренебрежимым.

В случае $l > 1$ оценка для режима OMAC-ACPKM-Master меньше оценки для оригинального режима для все практических сценариев в силу неравенства $\sigma^2 > \sigma_1^2 + \ldots + \sigma_l^2$, где $\sigma = \sigma_1 + \ldots + \sigma_l$. Заметим, что оценка для режима с внутренними преобразованием секрета достигает своего минимума в случае $\sigma_1 = \ldots = \sigma_l = m$, т.е. когда все сообщения одинаковой длины. В таком случае оценки для режимов примут следующий вид:

$$\mathsf{Adv}^{\mathrm{PRF}}_{\mathrm{OMAC}}(\mathcal{A}) \approx \frac{4q^2m^2}{2^n},$$

$$\mathsf{Adv}^{\mathrm{PRF}}_{\mathrm{OMAC\text{-}ACPKM\text{-}Master}_{N,\infty}}(\mathcal{A}) \approx \frac{4q^2mN}{2^n}.$$

Данные оценки показывают, что внутреннее преобразование секрета позволяет безопасно (без потери стойкости) увеличить длину m обрабатываемых сообщений в m/N раз. .

3.2. Режим GCM-ACPKM

В настоящем разделе исследуется возможность улучшения комбинаторных свойств режима GCM, описанного в [4], с помощью внутреннего преобразования секрета. Режим GCM является стандартом организации

NIST и является одним из наиболее часто используемых режимов в высокоуровневых протоколах. Так, данный режим является рекомендованным механизмов для использования в протоколе TLS 1.3, так как он обеспечивает приемлемый уровень стойкости в базовых моделях и является наиболее эффективным по производительности среди известных AEAD-режимов.

Режим GCM представляет собой комбинацию режима CTR [8], который используется для обеспечения конфиденциальности данных, и конструкции Вегмана-Картера [38], которая используется для обеспечения целостности данных. Особенностью конструкции Вегмана-Картера является то, что для обработки q сообщений произвольной длины исходный секрет используется только для выработки $q + 1$ блоков, т.е. частота использования секрета не зависит от длины сообщений. Более того, существующие оценки уровня стойкости [38] в модели UF-CMA демонстрируют, что данная конструкция, в отличие, например, от режима OMAC, уже позволяет безопасно обрабатывать сообщения, длина которых существенно превосходит $2^{n/2}$ блоков.

С учетом данного наблюдения, а также с целью сохранения эффективности механизма, был разработан модифицированный режим GCM-ACPKM с внутренним преобразованием секрета, в котором изменяется только процедура преобразования открытых текстов (аналогично режиму CTR-ACPKM). Для данного режима были проведены исследования целевых свойств безопасности путем получения оценок уровня стойкости в базовых моделях нарушителя. Данные результаты изложены в следующих подразделах.

3.2.1. Описание AEAD-режимов GCM и GCM-ACPKM

Сначала приведем описание режима GCM [4]. Рассматривается режим GCM с длиной нонса 96 бит.

GCM. Обозначим через GCM[E] режим GCM, использующий в качестве параметра БСА E с длиной блока $n = 128$.

Сначала определим вспомогательные функции. Для битовых строк A, B произвольной (возможно, нулевой) длины и строки $H \in \{0,1\}^n$ введем функцию

$$\mathrm{GHASH}_H(A,B) = \sum_{i=1}^{m} X_i \cdot H^{m+1-i},$$

где «$\sum$» и «$\cdot$» – операции сложения и умножения в поле $GF(2^n)$, и строка $X = X_1\| \ldots \|X_m$, $X_i \in \{0,1\}^n$ формируется следующим образом. Пусть $a = n \cdot |A|_n - |A|$, $b = n \cdot |B|_n - |B|$, $m = |A|_n + |B|_n + 1$, тогда $X = A\|0^a\|B\|0^b\|\mathrm{str}_{n/2}(|A|)\|\mathrm{str}_{n/2}(|B|)$.

Для $0 \leqslant a < n$ через $\mathrm{incr}_a : \{0,1\}^n \to \{0,1\}^n$ будем обозначать функцию, которая принимает на вход строку $I \in \{0,1\}^n$, и возвращает сроку

$$\mathrm{msb}_{n-a}(I)\|\mathrm{str}_a(\mathrm{int}(\mathrm{lsb}_a(I)) + 1 \bmod 2^a).$$

Схема GCM$[E]$ определена для следующих множеств: $\boldsymbol{K} = \{0,1\}^k$, $\boldsymbol{N} = \{0,1\}^{96}$, $\boldsymbol{A} = \boldsymbol{P} = \boldsymbol{C} = \{0,1\}^{\leqslant 2^{n/2}-1}$, при этом $|P| \leqslant n(2^{32}-2)$, $\boldsymbol{T} = \{0,1\}^n$. Алгоритмы определены на Рис. 3.3.

GCM.$\mathsf{Enc}(K, N, A, P)$

$q \leftarrow |P|_n$
$H \leftarrow E_K(0^n)$
$I_0 \leftarrow N \| 0^{31}1$

. . . . . .

for $i = 1 \ldots q$ **do**:
  $I_i \leftarrow \mathrm{incr}_{32}(I_{i-1})$
  $\Gamma_i \leftarrow E_K(I_i)$
$C \leftarrow P \oplus \mathrm{msb}_{|P|}(\Gamma_1 \| \ldots \| \Gamma_q)$

. . . . . .

$T \leftarrow E_K(I_0) \oplus \mathrm{GHASH}_H(A, C)$
return (C, T)

GCM.$\mathsf{Dec}(K, N, A, C, T)$

$q \leftarrow |C|_n$
$H \leftarrow E_K(0^n)$
$I_0 \leftarrow N \| 0^{31}1$

. . . . . .

$T' \leftarrow E_K(I_0) \oplus \mathrm{GHASH}_H(A, C)$
if $T \neq T'$:
  return $\perp$

. . . . . .

for $i = 1 \ldots q$ **do**:
  $I_i \leftarrow \mathrm{incr}_{32}(I_{i-1})$
  $\Gamma_i \leftarrow E_K(I_i)$
$P \leftarrow C \oplus \mathrm{msb}_{|C|}(\Gamma_1 \| \ldots \| \Gamma_q)$
return P

Рис. 3.3. Определение алгоритмов Enc и Dec AEAD-режима GCM

Далее введем режим GCM-ACPKM с внутренним преобразованием секрета.

GCM-ACPKM. Для удобства изложения введем вспомогательную функцию $\varphi_i : \{0,1\}^n \to \{0,1\}$, $\varphi_i(X) = X_{(i)}$, $0 \leqslant i < n$. Данная функция возвращает i-й бит строки (считая слева направо с нуля).

В отличие от GCM, для режима GCM-ACPKM длина нонса может варьироваться, но должна быть фиксированной для секрета. Она является параметром режима и обозначается через c, $0 < c \leqslant n$. Для фиксированного значения c введем функцию преобразования секрета ACPKM:

$$K^1 = K, \quad K^{i+1} = \mathrm{ACPKM}(K^i) = \mathrm{msb}_k(E_{K^i}(D_1) \| \ldots \| E_{K^i}(D_s)),$$

где $s = \lceil k/n \rceil$, $D_1, \ldots, D_s \in \{0,1\}^n$ – попарно различные произвольные константы, такие что $\varphi_c(D_1) = \ldots = \varphi_c(D_s) = 1$.

Через GCM-ACPKM$[E, c, l]$ будем обозначать схему с $|N| = c$, в которой используется преобразование секрета согласно процедуре ACPKM после обработки каждых l блоков открытого текста P. При этом после обновления секрета внутреннее состояние счетчика не сбрасывается. Такой подход выбран для противодействия атакам с предвычислениями (см. [36]). Секрет для вычисления значения $E_K(I_0)$ и $H = E_K(0^n)$ не обновляется и полагается равным изначальному секрету. Алгоритмы определены на Рис. 3.4 (см. ниже).

GCM-ACPKM.Enc(K, N, A, P)

$q \leftarrow |P|_n$

$H \leftarrow E_K(0^n)$

$K_1 \leftarrow K$

$I_0 \leftarrow N \| 0^{n-c-1}1$

. . . . . .

for $i = 1 \ldots q$ **do**:

  $I_i \leftarrow \mathrm{incr}_{n-c}(I_{i-1})$

  $j \leftarrow \lceil q/l \rceil$

  $K^j \leftarrow ACPKM(K^{j-1})$

  $\Gamma_i \leftarrow E_{K^j}(I_i)$

$C \leftarrow P \oplus \mathrm{msb}_{|P|}(\Gamma_1 \| \ldots \| \Gamma_q)$

. . . . . .

$T \leftarrow E_K(I_0) \oplus \mathrm{GHASH}_H(A, C)$

return (C, T)

GCM-ACPKM.Dec(K, N, A, C, T)

$q \leftarrow |C|_n$

$H \leftarrow E_K(0^n)$

$K_1 \leftarrow K$

$I_0 \leftarrow N \| 0^{n-c-1}1$

. . . . . .

$T' \leftarrow E_K(I_0) \oplus \mathrm{GHASH}_H(A, C)$

if $T \neq T'$:

  return $\perp$

. . . . . .

for $i = 1 \ldots q$ **do**:

  $I_i \leftarrow \mathrm{incr}_{n-c}(I_{i-1})$

  $j \leftarrow \lceil q/l \rceil$

  $K^j \leftarrow ACPKM(K^{j-1})$

  $\Gamma_i \leftarrow E_{K^j}(I_i)$

$P \leftarrow C \oplus \mathrm{msb}_{|C|}(\Gamma_1 \| \ldots \| \Gamma_q)$

return P

Рис. 3.4. Определение алгоритмов Enc и Dec AEAD-режима GCM-ACPKM

Длина открытого текста в блоках ограничена значением $2^{n-c-1} - 2$. Данное ограничение и ограничение на вид констант $D_1, \ldots, D_s$ гарантируют, что блоки следующего секрета K^j никогда не будут среди блоков $E_{K^{j-1}}(I_i)$, где $1 \leqslant i \leqslant 2^{n-c-1} - 2$.

3.2.2. Конфиденциальность и целостность

В настоящем подразделе представлены результаты о стойкости режима с внутренним преобразованием секрета GCM-ACPKM. Полученные результаты показывают, что режим обеспечивает конфиденциальность и целостность в предположении стойкости базового блочного симметричного алгоритма и что преобразование секрета согласно процедуре ACPKM улучшает комбинаторные свойства режима GCM и позволяет обрабатывать большее количество данных.

Так как процедура преобразования открытого текста в режиме GCM-ACPKM аналогична процедуре в режиме CTR-ACPKM, введенного в работе [40], оценки уровня стойкости в модели IND-CPA могут быть получены аналогичным образом, как описано в работе [40]. Единственным отличием при доказательстве является учет влияния того, что у нарушителя дополнительно имеются значения имитовставки T. Напомним, что в режиме GCM-ACPKM маскирующие значения $E_K(I_0)$ и значение $H = E_K(0^n)$, используемые при формировании имитовставки, вычисляются с использованием начального секрета K первой секции. При этом, входные значения I_0 и 0^n для блочного симметричного алгоритма не совпадают со значениями, которые используются для формирования блоков Γ_i и блоков секрета K_2. Таким образом, при получении оценки для режима GCM-ACPKM необходимо дополнительно учитывать, что на первом секрете обрабатывается на $q + 1$ блоков больше, чем в режиме CTR-ACPKM.

Ниже представлена теорема для режима GCM-ACPKM, которая характеризует его стойкость в модели IND-CPA.

Теорема 3.2.1 (Смышляев С.В. [41]). *Для любого нарушителя $\mathcal{A}$ в модели IND-CPA с вычислительными ресурсами не более t, делающего не более q запросов, где максимальная длина открытого текста не превышает m блоков и суммарная длина открытых текстов во всех запросах не превышает σ блоков, существует нарушитель $\mathcal{A}'$, такой что*

$$\mathbf{Adv}^{\text{IND-CPA}}_{\text{GCM-ACPKM}[E,c,l]}(\mathcal{A}) \leqslant h \cdot \mathbf{Adv}^{\text{PRP-CPA}}_{E}(\mathcal{A}') + \frac{(\sigma_1 + q + s + 1)^2}{2^{n+1}} + \\ + \frac{(\sigma_2 + s)^2 + \ldots + (\sigma_{h-1} + s)^2 + (\sigma_h)^2}{2^{n+1}}, \quad (3.1)$$

где $s = \lceil k/n \rceil$, $h = \lceil m/l \rceil$, σ_j – это суммарное количество блоков, обработанных для q открытых текстов с помощью секционного секрета K^j, и $\sigma_1 + \ldots + \sigma_h = \sigma$. Нарушитель $\mathcal{A}'$ делает не более $\sigma_1 + q + s + 1$ запросов. При этом, вычислительные ресурсы $\mathcal{A}'$ не превышают $t + cn\sigma_A$, где σ_A – это суммарная длина всех запросов, c — константа, зависящая только от модели вычислений и способа кодирования.

Заметим, что режим будет являться стойким, если значение $s = \lceil k/n \rceil$ достаточно мало. Для ряда стандартных блочных симметричных алгоритмов (например, AES-256 и AES-128) данное условие выполнено: $s \in \{1, 2\}$. Данная оценка показывает, что верхняя оценка преобладаний нарушителей будет минимальной, если $\sigma_1 = \ldots = \sigma_h$, т.е. если все открытые тексты одной длины.

Теперь представим оценку для целостности.

Теорема 3.2.2 (Ахметзянова Л.Р.). *Для любого нарушителя $\mathcal{A}$ в модели INT-CTXT с вычислительными ресурсами не более t, делающего не более q запросов к оракулу Encrypt и не более q' запросов к оракулу*

Decrypt , где максимальная длина открытого/преобразованного текста и ассоциированных данных не превосходит m_A блоков и суммарная длина всех открытых текстов не более σ блоков, существует нарушитель $\mathcal{A}'$, такой что

$$\mathbf{Adv}^{\text{INT-CTXT}}_{\text{GCM-ACPKM}[E,c,l]}(\mathcal{A}) \leqslant \mathbf{Adv}^{\text{PRP-CPA}}_{E}(\mathcal{A}') + \\ + \left[\frac{q'(m_A+1)}{2^n}\right] \exp\left(\frac{4(\sigma_1+s)q}{2^n}\right), \quad (3.2)$$

где $s = \lceil k/n \rceil$, σ_1 – суммарное количество блоков, обработанных для q запросов с помощью изначального секрета $K = K^1$, и $\sigma_1 + s \leqslant 2^{n-1}$. Нарушитель $\mathcal{A}'$ делает не более $\sigma_1 + q + q' + s + 1$ запросов. Более того, вычислительные ресурсы $\mathcal{A}'$ не превышают $t + cn\sigma_A$, где σ_A – это суммарная длина всех запросов, c — константа, зависящая только от модели вычислений и способа кодирования.

Доказательство. Без ограничения общности будем считать, что длина секрета k кратна длине блока n, и $s = k/n$.

Сначала рассмотрим модификацию целевого режима – абстрактный режим GCM-ACPKM*. Отличие заключается в том, что вместо подстановки E_K со случайно равновероятно выбранным секретом K используется подстановка π, выбранная случайно равновероятно из множества $\mathcal{S}_{2^n}$. Данная подстановка используется для выработки

- значения $H = \pi(0^n)$,
- блоков второго секрета $\pi(D_1),\ \ldots,\ \pi(D_s)$, $K^2 = \pi(D_1)\| \ldots \|\pi(D_s)$,
- q значений $Z_i = \pi(N_i\|0^{n-c-1}1)$, $1 \leqslant i \leqslant q$,

- блоков для обработки первых секций q открытых текстов,т.е. $\Gamma_i^j = \pi(N_i \| \mathrm{str}_{n-c}(j+1))$, $1 \leqslant j \leqslant l_i \leqslant l$, $1 \leqslant i \leqslant q$ (заметим, что $l_1 + l_2 + \cdots + l_q = \sigma_1$).

Остальные секции обрабатываются с помощью E_{K^i}, где $K^2 = \pi(D_1) \| \ldots \| \pi(D_s)$ и $K^i = \mathrm{ACPKM}(K^{i-1})$, $i \geqslant 3$.

Путем построения сведения легко получить следующее соотношение:

$$\mathbf{Adv}^{\text{INT-CTXT}}_{\text{GCM-ACPKM}[E,c,l]}(\mathcal{A}) \leqslant \mathbf{Adv}^{\text{PRP-CPA}}_{E}(\mathcal{A}') + \mathbf{Adv}^{\text{INT-CTXT}}_{\text{GCM-ACPKM}^*_{c,l}}(\mathcal{A}),$$

где $\mathcal{A}'$ делает не более $\sigma_1 + q + s + 1$ запросов.

Теперь рассмотрим модификацию модели (INT-CTXT*): нарушитель в начале эксперимента дополнительное получает на вход блоки $\pi(D_1), \ldots, \pi(D_s)$. Заметим, что преобладание нарушителя в таком эксперименте не меньше преобладания нарушителя в исходном эксперименте модели INT-CTXT, так как в модели INT-CTXT* нарушителю дается больше информации. Поэтому

$$\mathbf{Adv}^{\text{INT-CTXT}}_{\text{GCM-ACPKM}^*_{c,l}}(\mathcal{A}) \leqslant \mathbf{Adv}^{\text{INT-CTXT}^*}_{\text{GCM-ACPKM}^*_{c,l}}(\mathcal{A}).$$

Для рассматриваемого режима GCM-ACPKM* доказательство оценки в модели INT-CTXT* аналогично доказательству оценки, представленной в Теореме 5 [27].

Без ограничения общности будем считать, что нарушитель $\mathcal{A}$ детерминированный, и значение нонса N' в запросе-подделке (N', A', C', T') совпало со значением нонса N_i из запроса к оракулу $Encrypt$ (N_i, A_i, P_i), в ответ на который вернулась пара (C_i, T_i) (иначе, можно показать, что

оценка будет меньше). Таким образом, вероятность подделки равна вероятности события, что выполнилось уравнение

$$\mathrm{GHASH}_H(A_i, C_i) \oplus \mathrm{GHASH}_H(A', C') = T_i \oplus T'.$$

Заметим, что при фиксации транскрипции взаимодействия между экспериментатором и нарушителей все случайные величины (кроме величины H) принимают фиксированные значения. Таким образом, для фиксированной транскрипции можно оценить вероятность искомого события как $\frac{m_A}{2^n}$, так как рассматриваемое уравнение относительно H имеет не более m_A решений в поле $GF(2^n)$ (не превышает степени полинома). Следующим шагом оценивается условная вероятность события, что реализуется фиксированная транскрипция (при условии $H = \pi(0^n)$). Легко заметить, что такая транскрипция однозначно определяется значениями T_i, Γ_i^j, K^2, которые в свою очередь определяются после фиксации $q+\sigma_1+s$ переходов в подстановке π. Поэтому требуемая условная вероятность вычисляется как $\frac{1}{(2^n-1)_{q+\sigma_1+s}}$, где $(a)_b = a \cdot (a-1) \cdots (a-b+1)$. Суммарная вероятность по всем транскрипциям T_i, Γ_i^j, K^2 оценивается в точности, как в работе [27] с использованием верхней оценки Бернштейна на вероятность интерполяций для случайной подстановки [34].

□

3.2.3. Сравнительный анализ оценок

Сравним полученные оценки стойкости для режимов GCM и GCM-ACPKM с БСА E, для которого $s = \lceil k/n \rceil = 2$.

Отметим, что известные оценки для режима GCM (см. [26, 27]) являются точными. В модели IND-CPA для режимов гаммирования это

является известным результатом, а в модели INT-CTXT это следует из результатов, полученных в работе [27].

IND-CPA. Для любого нарушителя $\mathcal{A}$ в модели IND-CPA, который делает не более q запросов с суммарной длиной всех открытых текстов не более σ и максимальной длиной открытого текста не более m блоков,

$$\mathbf{Adv}^{\text{IND-CPA}}_{\text{GCM}[E]}(\mathcal{A}) \approx \frac{(\sigma+q)^2}{2^{n+1}},$$
$$\mathbf{Adv}^{\text{IND-CPA}}_{\text{GCM-ACPKM}[E,c,l]}(\mathcal{A}) \approx \frac{(\sigma_1+q)^2+\sigma_2^2+\ldots+\sigma_{h-1}^2+\sigma_h^2}{2^{n+1}},$$

где $h = \lceil m/l \rceil$. Здесь и далее предполагается, что $\mathbf{Adv}^{\text{PRP-CPA}}_{E}(\mathcal{A}')$ является пренебрежимо малым в сравнении с указанными выше оценками.

Данные соотношения показывают, что гарантированный уровень стойкости в модели IND-CPA, обеспечиваемый режимом GCM-ACPKM, улучшен в сравнении с оригинальным режимом GCM для всех типичных случаев применения, так как $\sigma^2 \geqslant \sigma_1^2+\ldots+\sigma_h^2$ для любого $\sigma = \sigma_1+\ldots+\sigma_h$.

INT-CTXT. Для любого нарушителя $\mathcal{A}$ в модели INT-CTXT, который делает не более q запросов к оракулу *Encrypt* и не более q' запросов к оракулу *Decrypt* с суммарной длиной всех открытых текстов не более σ и максимальной суммарной длиной открытого/преобразованного текста и ассоциированных данных не более m_A блоков,

$$\mathbf{Adv}^{\text{INT-CTXT}}_{\text{GCM}[E]}(\mathcal{A}) \approx \frac{q'm_A}{2^n} \cdot \exp\left(\frac{4\sigma q}{2^n}\right),$$
$$\mathbf{Adv}^{\text{INT-CTXT}}_{\text{GCM-ACPKM}[E,c,l]}(\mathcal{A}) \approx \frac{q'm_A}{2^n} \cdot \exp\left(\frac{4\sigma_1 q}{2^n}\right).$$

Как видно из оценки, оценка уровня стойкости в части обеспечения

целостности также улучшена в сравнении с базовым режимом для всех типичных случаев применения, так как $\sigma_1 < \sigma$.

Замечание 3.2.1. *В работе [27] предлагается атака, в результате которой восстанавливается секретное значение H режима GCM с вероятностью не менее $\frac{1}{2}$ при $\sqrt{n/m} \cdot 2^{n/2}$ запросах к оракулу Encrypt, где m – блоковая длина открытых текстов в запросах. В случае режима* GCM-ACPKM *для такой атаки требуется $\sqrt{n/l} \cdot 2^{n/2}$ запросов к оракулу Encrypt для восстановления H, где l – размер секции.*

Рассматриваемые оценки также можно представить в терминах количества запросов q и длины открытых текстов в блоках m, используя соотношения $\sigma \leqslant qm$ и $\sigma_i \leqslant ql$ для всех i:

$$\mathbf{Adv}^{\text{IND-CPA}}_{\text{GCM}[E]}(\mathcal{A}) \approx \frac{(qm+q)^2}{2^{n+1}}, \quad \mathbf{Adv}^{\text{IND-CPA}}_{\text{GCM-ACPKM}[E,c,l]}(\mathcal{A}) \approx \frac{m}{l} \cdot \frac{(ql+q)^2}{2^{n+1}},$$
$$\mathbf{Adv}^{\text{INT-CTXT}}_{\text{GCM-ACPKM}[E,c,l]}(\mathcal{A}) \approx \frac{q' m_A}{2^n} \cdot \exp\left(\frac{4lq^2}{2^n}\right).$$

Зафиксируем ограничение на преобладание нарушителей. Пусть при таком ограничении с помощью режима GCM можно безопасно обработать q сообщений с одинаковой длиной открытых текстов m блоков. Заметим, что случай открытых текстов одинаковой длины является часто встречаемым на практике (см. [6]): сообщения часто дополняются до одной и той же длины для ее сокрытия. Согласно вышеприведенным оценкам длина сообщений может быть безопасно увеличена (то есть без потери стойкости) до длины $\min\left(\frac{m+1}{l+1} \cdot m,\ 2^{n-c-1} - 2\right)$ при применении внутреннего преобразования секрета. Более того, если длина ассоциированных данных достаточно мала в сравнении с длиной открытого текста

(например, являются заголовком к пакету), тогда вероятность подделки для $q' = 1$ будет все еще порядка $\frac{1}{2^c}$, пока $q \leqslant \frac{2^{n/2}-1}{\sqrt{l}}$.

Сравнение оценок. Рассмотрим режимы GCM и GCM-ACPKM при $n = 128$ и длиной секции $l = 2^6$. Технически, параметр l означает, что преобразование секрета будет происходить после обработки каждого килобайта открытого текста. Сравним оценки уровня стойкости в целевых моделях для данных режимов в рамках их применения в протоколе CMS [35], где на одном секрете обрабатывается только одно сообщение (т.е. $q = 1$).

Результаты сравнения представлены в Таблице 3.2, где в первой колонке содержатся значения длины m обрабатываемого открытого текста, а в последующих колонках содержатся соответствующие границы на успех нарушителя по нарушению конфиденциальности (δ_{priv}) или целостности (δ_{auth}). Данные вероятности были получены с учетом того, что $\exp(4x/2^{128}) \leqslant 2$ для $x \leqslant 2^{126}$.

Значительный рост стойкости благодаря использованию ACPKM обеспечивается в таких протоколах, как CMS, так как в рамках них могут обрабатываться длинные сообщения. Базовый режим GCM позволяет обрабатывать не более $2^{32} - 2$ блоков, обеспечивая достаточно высокий уровень безопасности. Режим GCM-ACPKM не имеет такого ограничения: выбирая подходящую длину нонса, мы можем увеличить максимальную длину открытого текста. Результаты в Таблице 3.2 показывают, что GCM-ACPKM позволяет обрабатывать сообщения длины 2^{64} блоков, обеспечивая высокий уровень стойкости в части обеспечения конфиденциальности (2^{-58}) и целостности (2^{-63}), а для режима GCM (с

m	GCM		GCM-ACPKM	
	δ_{priv}	δ_{auth}	δ_{priv}	δ_{auth}
$2^{32}-2$	2^{-64}	2^{-96}	2^{-91}	2^{-96}
2^{44}	$-/2^{-40}$	$-/2^{-83}$	2^{-78}	2^{-83}
2^{54}	$-/2^{-20}$	$-/2^{-73}$	2^{-68}	2^{-73}
2^{64}	$-/1$	$-/2^{-63}$	2^{-58}	2^{-63}

Таблица 3.2. Сравнительные оценки для режимов GCM и GCM-ACPKM с параметрами $n = 128$ бит, $l = 2^6$ блоков (1 килобайт) в протоколе CMS с количеством сообщений $q = 1$. Прочерк в столбце означает, что соответствующая длина открытого текста m не может обрабатываться в соответствующем режиме. Вероятность после знака косой черты соответствует модификации режима GCM, которая позволяет обрабатывать более длинные сообщений сообщения (за счет выбора длины нонса как в GCM-ACPKM, подробности см. в разделе 3.2.1).

увеличенной длиной сообщения так же, как в GCM-ACPKM) конфиденциальность будет полностью нарушена.

Выводы

На основе стандартного режима OMAC был разработан режим OMAC-ACPKM-Master, для которого удалось доказать оценки уровня стойкости в формальной модели нарушителя PRF. Путем сравнения полученных оценок с существующими оценками для оригинала было по-

казано, что внедрение преобразования секрета улучшает оценку уровня стойкости, что, в свою очередь, позволяет безопасно увеличить объем обрабатываемых данных. Отметим, что данный подход позволяет существенно увеличить именно длину обрабатываемых сообщений. Режим OMAC-ACPKM-Master наряду с режимом CTR-ACPKM был стандартизирован в Российской Федерации [25]

На основе стандартного режима GCM был разработан модифицированный режим GCM-ACPKM, в котором внутреннее преобразование секрета применено только к процедуре преобразования открытых текстов (аналогично режиму CTR-ACPKM), а процедура выработки имитовставки остается без изменений. Для нового режима доказана оценка уровня стойкости в модели INT-CTXT, и показано, что внутреннее преобразование секрета, примененное указанным выше образом, позволяет улучшить оценку уровня стойкости в части обеспечения не только конфиденциальности (т.е. в модели IND-CPA), но и целостности (т.е. в модели INT-CTXT) без существенного снижения производительности.

По результатам проведенных в настоящей диссертации исследований данный режим стал частью международного документа RFC 8645, разработанного исследовательской группой CFRG сообщества IETF, определяющей механизмы защиты информации в Интернете (см.[28]).

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 в модели INT-CTXT при обработке $2^{n/2}$ сообщений. Для режима MGM доказана 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 (в модели IND-CPA).

2) С целью улучшения свойств режима MGM разработана его модификация – режим MGM2. Для режима MGM2 доказаны 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.

3) На основе стандартизированных механизмов разработаны два ре-

жима 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 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 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.

Полученные в диссертации результаты могут быть использованы для развития и совершенствования математических моделей аппаратно-программных средств защиты информации, что будет способствовать повышению обоснованности методов оценки защищенности информации. Эти результаты могут найти применение также при разработке новых принципов создания аппаратно-программных средств защиты информации. В частности:

1) при синтезе и анализе систем обеспечения информационной безопасности на основе блочных симметричных алгоритмов;

2) в учебном процессе студентов-математиков, проходящих обучение в рамках специализации «Математические и программные методы обеспечения информационной безопасности»;

3) в научных центрах, проводящих исследования в области защиты информации.

Список литературы

1. Bellare M., Namprempre C. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm // Journal of Cryptology. 2008. Vol. 21. Pp. 469–491.
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. 2004. Vol. 7(2). Pp. 206–241.
3. Whiting D., Housley R., Ferguson. N. Counter with CBC-MAC (CCM) // RFC. 2003. Vol. 3610. Pp. 1–26.
4. Dworkin M. Recommendation for BlockCipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC // NIST Special Publication 800-38D. 2007.
5. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols // RFC. 2015. Vol. 7539. Pp. 1–45.
6. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3 // RFC. 2018. Vol. 8446. Pp. 1–160.
7. 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. 1997. Pp. 394–403.
8. Rogaway P. Nonce-Based Symmetric Encryption // In Proceedings of International Conference on Fast Software Encryption. 2004. Pp. 348-358.
9. Bellare M., Rogaway P. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs // Lecture Notes in Comput-

er Science. 2006. Vol. 4004. Pp. 409–426.

10. Competition for Authenticated Encryption: Security, Applicability, and Robustnes // NIST. https://competitions.cr.yp.to/caesar.html
11. 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). 2002. Pp. 62–75.
12. Andreeva E. et al. How to securely release unverified plaintext in authenticated encryption // Lecture Notes in Computer Science. 2014. Vol. 8873. Pp. 105–125.
13. Rogaway P., Shrimpton T. A provable-security treatment of the key-wrap problem // Lecture Notes in Computer Science. 2006. Vol. 4004. Pp. 373–390.
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). 2016. Pp. 456–467.
15. Hoang V., Krovetz T., Rogaway P. Robust Authenticated-Encryption AEZ and the Problem That It Solves // Lecture Notes in Computer Science. 2015. Vol. 9056. Pp. 15–44.
16. Gueron S., Lindell Y. GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte // In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). 2015. Pp. 109–119.
17. Ashur T., Dunkelman O., Luykx A. Boosting authenticated encryption robustness with minimal modifications // In Proceedings of Annual In-

ternational Cryptology Conference. 2017. Pp. 3–33.

18. Технический комитет 26 по стандартизации «Криптографическая защита информации» `https://tc26.ru`
19. Jonsson J. On the Security of CTR + CBC-MAC // Selected Areas in Cryptography. 2002.
20. 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). 2017.
21. 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. 2019.
22. Рекомендации по стандартизации Р 1323565.1.026-2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование» // Москва, Стандартинформ. 2019.
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). 2019.
25. Рекомендации по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования» // Москва, Стандартинформ. 2018.

26. Iwata, T., Ohashi, K., Minematsu K. Breaking and Repairing GCM Security Proofs // Lecture Notes in Computer Science. 2012. Vol. 7417. Pp. 31–49.
27. Nandi, M. Bernstein Bound on WCS is Tight Repairing Luykx-Preneel Optimal Forgeries // Lecture Notes in Computer Science. 2018. Vol. 10992.
28. Smyshlyaev S. Re-keying Mechanisms for Symmetric Keys // RFC. 2019. Vol. 8645. Pp. 1–69.
29. Goldreich O. Foundations of Cryptography: Volume 1 // Cambridge University Press. 2006.
30. Информационной ресурс «Математическая криптография». `https://cryptography.ru/ref/`модель_вычислений_однородная/
31. Shrimpton T. A Characterization of Authenticated-Encryption as a Form of Chosen-Ciphertext Security // In Cryptology ePrint Archive, Report 2004/272. 2004.
32. Chang D, Nandi M. A Short Proof of the PRP/PRF Switching Lemma // In Cryptology ePrint Archive, Report 2008/078. 2008.
33. ГОСТ Р 34.13–2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» // Москва, Стандартинформ. 2015.
34. Bernstein D. Stronger Security Bounds for Permutations // 2005.
35. Housley R. Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS) // RFC. 2007. Vol. 5084. Pp. 1–11.
36. Biham, E. How to Forge DES-Encrypted Messages in 2^{28} Steps // Technion Computer Science Department Technical Report CS0884. 1996.

37. Iwata T., Kurosawa K. Stronger Security Bounds for OMAC, TMAC and XCBC // Lecture Notes in Computer Science. 2003. Vol. 2904. Pp. 402–415.
38. Bernstein D. Stronger security bounds for wegman-carter-shoup authenticators. // In Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2005. Pp. 164–180.

Публикации в рецензируемых научных изданиях, индексируемых в базах данных Web of Science (WoS), Scopus, RSCI:

39. Ahmetzyanova L. R., Karpunin G. A., Sedov G. K. Near birthday attack on “8 bits” AEAD mode // Математические вопросы криптографии (RSCI WoS, ИФ РИНЦ 2020: 0,327). 2019. Т. 10(2). С. 47–60.
40. 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 (RSCI WoS, ИФ РИНЦ 2020: 0,327). 2019. Т. 10(2). С. 31–46.
41. Akhmetzyanova L. R., Alekseev E. K., Smyshlyaev S. V., Oshkin I. B. On Internal Re-keying // Lecture Notes in Computer Science (Scopus, ИФ SJR 2020: 0.249). 2020. Vol. 12529. Pp. 23–45.

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

42. Ахметзянова Л.Р., Алексеев Е.К., Бабуева А.А., Божко А.А., Смышляев С.В. MGM2: режим аутентифицированного шифрования, устой-

чивый к повтору вектора инициализации // International Journal of Open Information Technologies (ISSN: 2307-8162). 2022. Vol. 10(1). Pp. 6–14.

43. Ахметзянова Л.Р. О свойстве конфиденциальности AEAD-режима MGM // International Journal of Open Information Technologies (ISSN: 2307-8162). 2022. Vol. 10(3). Pp. 1–9.

Приложение

1. Оценка вероятности коллизий в атаке на режим «8 бит»

Лемма 1.1 (Г.К. Седов)**.** *Пусть* $x_1, \ldots, x_s$ *и* $y_1, \ldots, y_t$ *— различные элементы из* $\{0,1\}^n$*, отличные от* $0^n \in \{0,1\}^n$*;* β *— некоторый произвольный элемент из* $\{0,1\}^n$*; на множестве всех перестановок на* $\{0,1\}^n$ *задано равномерное распределение,* $K_1 \in Perm(n)$ *— произвольная функция. Тогда*

$$\Pr_{\pi\in Perm(n)}\left[\{\pi(x_m)\}_{m=1}^{s} \cap \{\pi(\pi(y_k) \oplus K_1(\pi(0^n)) \oplus \beta))\}_{k=1}^{t} \neq \varnothing\right] \geqslant$$
$$\geqslant 1 - \left(1 - \frac{s-1}{2^n}\right)^t \geqslant 1 - e^{-\frac{t(s-1)}{2^n}}.$$

Доказательство. Заметим, что для вероятности события, являющего отрицанием исходного события, верна следующая цепочка соотношений:

$$\Pr_{\pi\in Perm(n)}\left[\{\pi(x_m)\}_{m=1}^{s} \cap \{\pi(\pi(y_k) \oplus K_1(\pi(0^n)) \oplus \beta))\}_{k=1}^{t} = \varnothing\right] =$$
$$= \Pr_{\pi\in Perm(n)}\left[\{x_m\}_{m=1}^{s} \cap \{\pi(y_k) \oplus K_1(\pi(0^n)) \oplus \beta)\}_{k=1}^{t} = \varnothing\right] =$$
$$= \Pr_{\pi\in Perm(n)}\left[\{x_m \oplus K_1(\pi(0^n)) \oplus \beta\}_{m=1}^{s} \cap \{\pi(y_k)\}_{k=1}^{t} = \varnothing\right].$$

Поскольку рассматривается равновероятное распределение на множестве всех перестановок $Perm(n)$, то искомую вероятность можно пе-

реписать в комбинаторных терминах:

$$\begin{aligned}
&\Pr_{\pi\in Perm(n)}\left[\{x_m\oplus K_1(\pi(0^n))\oplus\beta\}_{m=1}^{s}\cap\{\pi(y_k)\}_{k=1}^{t}=\varnothing\right]=\\
&=\frac{\#\{\pi\in Perm(n)|\ \{x_m\oplus K_1(\pi(0^n))\oplus\beta\}_{m=1}^{s}\cap\{\pi(y_k)\}_{k=1}^{t}=\varnothing\}}{|Perm(n)|}=\\
&=\frac{1}{2^n!}\sum_{\alpha\in\{0,1\}^n}\#\left\{\pi\in Perm(n)|_{\{x_m\oplus K_1(\alpha)\oplus\beta\}_{m=1}^{s}\cap\{\pi(y_k)\}_{k=1}^{t}=\varnothing}^{\pi(0^n)=\alpha\text{ и }}\right\} \quad (3)
\end{aligned}$$

Для того чтобы вычислить число перестановок, стоящее под знаком суммы, заметим, что значение таких перестановок на входе 0^n зафиксировано величиной α, а на элементах $y_1,\ldots,y_t$ значения этих перестановок могут быть произвольными, не совпадающими с α и не входящими в s-элементное множество $S_\alpha=\{x_m\oplus K_1(\alpha)\oplus\beta\}_{m=1}^{s}$. Рассмотрим два варианта $\alpha\in S_\alpha$ и $\alpha\notin S_\alpha$. Для этих вариантов искомое число будет немного отличаться:

$$\begin{aligned}
&\#\{\pi\in Perm(n)|\ \pi(0^n)=\alpha\text{ и }S_\alpha\cap\{\pi(y_k)\}_{k=1}^{t}=\varnothing\}=\\
&=\begin{cases}(2^n-s)\cdot\ldots\cdot(2^n-s-(t-1))\cdot(2^n-(t+1))!, & \text{при }\alpha\in S_\alpha;\\ (2^n-s-1)\cdot\ldots\cdot(2^n-s-t)\cdot(2^n-(t+1))!, & \text{при }\alpha\notin S_\alpha.\end{cases} \quad (4)
\end{aligned}$$

С учетом (3) и (4) имеют место следующие неравенства:

$$\begin{aligned}
&\Pr_{\pi\in Perm(n)}\left[\{x_m\oplus K_1(\pi(0^n))\oplus\beta\}_{m=1}^{s}\cap\{\pi(y_k)\}_{k=1}^{t}=\varnothing\right]\leqslant\\
&\leqslant 2^n\cdot\frac{(2^n-s)\cdot\ldots\cdot(2^n-s-(t-1))\cdot(2^n-(t+1))!}{2^n!}=\\
&=\frac{2^n-s}{2^n-1}\cdot\ldots\cdot\frac{2^n-s-(t-1)}{2^n-t}\leqslant\left(\frac{2^n-(s-1)}{2^n}\right)^t=\\
&=\left(1-\frac{s-1}{2^n}\right)^t=e^{t\ln\left(1-\frac{s-1}{2^n}\right)}\leqslant e^{-\frac{t(s-1)}{2^n}}.
\end{aligned}$$

□