ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА МГУ.05.01
ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

Решение диссертационного совета от «01» июня 2022 г. № 15
о присуждении Ахметзяновой Лилии Руслановне,
гражданке Российской Федерации,
ученой степени кандидата физико-математических наук

Диссертация **«Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации»** по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите диссертационным советом 27 апреля 2022 г., протокол № 12.

Соискатель **Ахметзянова Лилия Руслановна** 1994 года рождения

в 2016 году окончила бакалавриат ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», факультет вычислительной математики и кибернетики, кафедра информационной безопасности (направление 01.03.02 «Прикладная математика и информатика», квалификация «Бакалавр», диплом ААН 1507126);

в 2018 году с отличием окончила магистратуру ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», факультет вычислительной математики и кибернетики, кафедра информационной безопасности (направление 01.04.02 «Прикладная математика и информатика», квалификация «Магистр», диплом ААА 2602354).

В 2018 году соискатель поступила в аспирантуру ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», факультет вычислительной математики и кибернетики, кафедра информационной безопасности (по состоянию на 01 июня 2022 г. соискатель продолжает обучение в аспирантуре, справка о сдаче кандидатских экзаменов выдана 5 апреля 2022 года).

Соискатель работает в должности заместителя начальника отдела криптографических исследований ООО «КРИПТО-ПРО», г. Москва.

Диссертация выполнена в ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», факультет вычислительной математики и кибернетики, кафедра информационной безопасности.

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

Официальные оппоненты:

Запечников Сергей Владимирович – доктор технических наук, доцент, профессор отделения интеллектуальных кибернетических систем офиса образовательных программ ФГБОУ ВО «Национальный исследовательский ядерный университет «МИФИ»;

Захаров Владимир Анатольевич – доктор физико-математических наук, профессор кафедры математической кибернетики факультета вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова»;

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

дали **положительные отзывы** на диссертацию.

Выбор официальных оппонентов обосновывался их высокой профессиональной квалификацией, наличием научных публикаций по направлениям, тесно связанным с темой диссертации, а также их соответствием критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова.

Соискатель имеет 15 опубликованных работ, в том числе по теме диссертации 5 работ, включая 3 публикации в рецензируемых научных изданиях, индексируемых в Web of Science, Scopus, RSCI, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

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

1) 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. /
2) Ahmetzyanova L.R. Practical significance of security bounds for standardized internally re-keyed block cipher modes / Ahmetzyanova L.R., Alekseev E.K., Sedov G.K., Smyshlyaeva E.S., Smyshlyaev S.V. // Математические вопросы криптографии. 2019. Т. 10. № 2. С. 31-46 (RSCI WoS, ИФ РИНЦ 2020: 0,327). / Ахметзяновой Л.Р. принадлежит синтез режима OMAC-ACPKM-Master и его анализ (доказательство утверждения Теоремы 2 по тексту статьи). Остальные результаты статьи получены соавторами. /
3) Akhmetzyanova L. On Internal Re-keying / Akhmetzyanova L., Alekseev E., Smyshlyaev S., Oshkin I. // Lecture Notes in Computer Science. 2020. Vol. 12529. Pp. 23-45 (Scopus, ИФ SJR 2020: 0.249). / Ахметзяновой Л.Р. принадлежит конструкция режима GCM-ACPKM, доказательство утверждения Теоремы 2 (по тексту статьи), выводы о защищенности режима GCM-ACPKM в части обеспечения целостности, сравнение с базовым режимом GCM. Остальные результаты статьи получены соавторами. /

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

4) Ахметзянова Л.Р. MGM2: режим аутентифицированного шифрования, устойчивый к повтору вектора инициализации / Ахметзянова Л.Р., Алексеев Е.К., Бабуева А.А., Божко А.А., Смышляев С.В. // International Journal of Open Information Technologies. ISSN: 2307-8162. 2022. Т. 10. № 1. С. 6-14. / Соавторам принадлежит постановка задачи и сравнение режима MGM2 с оригинальным режимом. Остальные результаты статьи получены Ахметзяновой Л.Р. /
5) Ахметзянова Л.Р. О свойстве конфиденциальности AEAD-режима MGM // International Journal of Open Information Technologies. ISSN: 2307-8162. 2022. Т. 10. № 3. С. 1-9.

На автореферат поступили **5 дополнительных отзывов, все они положительные**.

Диссертационный совет отмечает, что **диссертация** Л.Р. Ахметзяновой, представленная на соискание ученой степени кандидата физико-математических наук, является научно-квалификационной работой, в которой на основании выполненных автором исследований **получено решение научной задачи** разработки симметричных схем аутентифицированного шифрования, предназначенных для одновременного обеспечения конфиденциальности и целостности информации с помощью единственного секрета (AEAD-схемы), и оценки уровня их стойкости в релевантных математических моделях нарушителя, формально описывающих его возможности и цели. Данные схемы применяются во многих значимых протоколах защиты информации, таких как протокол TLS, широко используемый для защиты соединений в сети Интернет.

В результате диссертационного исследования построены новые математические методы получения обоснованных оценок уровня стойкости в целевых моделях нарушителя

для существующих AEAD-схем на основе блочных симметричных алгоритмов (AEAD-режимы) и разработаны новые AEAD-режимы с целью улучшения комбинаторных свойств и достижения новых свойств безопасности.

Диссертация представляет собой **самостоятельное законченное исследование, обладающее внутренним единством**. Положения, выносимые на защиту, содержат обоснование актуальности темы исследования, описание научной и практической значимости работы, а также перечисленные далее новые научные результаты, которые свидетельствуют о личном вкладе автора в науку.

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.
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 режима работы блочного симметричного алгоритма с внутренним преобразованием секрета с целью увеличения объема безопасно обрабатываемых данных. На основе стандартизированного в Российской Федерации режима выработки имитовставки OMAC разработан режим OMAC-ACPKM-Master. Для данного режима доказана верхняя оценка преобладаний нарушителей, определяемых моделью PRF (неотличимость от случайной функции). 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.

Результаты диссертации базируются на известных теоретических положениях комбинаторной теории вероятностей, теории алгоритмов и теории сложности вычислений.

Достоверность результатов исследования гарантируется следующими факторами:

- все результаты диссертации имеют законченный характер и снабжены строгими математическими доказательствами;
- установлено, что все результаты диссертации являются новыми, а результаты других авторов, упомянутые в диссертации, отмечены соответствующими ссылками;
- результаты диссертации прошли апробацию на международных и всероссийских конференциях и на научных семинарах.

Полученные результаты вносят существенный вклад в развитие математических методов синтеза и анализа стойких и эффективных AEAD-схем, а 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.

На заседании 1 июня 2022 года диссертационный совет принял решение присудить Ахметзяновой Л.Р. ученую степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 22 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 30 человек, входящих в состав совета, проголосовали: за - 22, против - 0, недействительных бюллетеней - 0.

Заместитель председателя
диссертационного совета МГУ.05.01,
доктор физико-математических наук, профессор Г.М. Кобельков

Ученый секретарь
диссертационного совета МГУ.05.01,
кандидат физико-математических наук М.А. Кривчиков

«01» июня 2022 г.