ОТЗЫВ

на автореферат диссертации
Ахметзяновой Лилии Руслановой
«Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации», представленной на соискание ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

AEAD-схемы, одновременно обеспечивающие аутентификацию и шифрование данных, находят широкое практическое применение при разработке протоколов передачи информации (например, протокола защиты транспортного уровня TLS 1.3), использующих наряду с зашифрованными данными некоторой, как правило, открытой служебной информации (заголовков, адресов, портов, версий протоколов, данных для принятия решения о том, как должен обрабатываться или пересылаться зашифрованный текст). Вообще говоря, реализовать указанный функционал представляется возможным за счет совместного использования отдельных стандартизированных механизмов обеспечения конфиденциальности и аутентификации информации. Однако, как показали время и практика, такие синтезные решения существенно ухудшают эксплуатационные характеристики соответствующих протоколов, в том числе за счет предъявления дополнительных требований к сторонам информационного взаимодействия. Но что самое главное, при таком построении схем существенно усложняется анализ их информационной безопасности. С учетом изложенного, разработка и исследование математических моделей безопасности AEAD-схем, а также методов их анализа являются значимыми и актуальными задачами в области защиты информации.

Согласно представленному тексту автореферата диссертация Лилии Руслановой Ахметзяновой посвящена построению новых математических методов получения обоснованных оценок уровня информационной безопасности существующих AEAD-режимов в целевых моделях нарушителя.

С использованием математического аппарата комбинаторной теории вероятностей, теории сложности вычислений и теории алгоритмов автором

диссертации разработаны:

– 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;

– модификация MGM2 AEAD-режима MGM, позволившая исправить недостаток режима MGM, заключающийся в возможности возникновения «опасных» коллизий между любыми возможными значениями входов в блочном симметричном алгоритме;

– метод получения обоснованных нижних оценок уровня стойкости MGM2 в расширенных моделях нарушителя для конфиденциальности и целостности;

– методы модификации режима выработки имитовставки OMAC и AEAD-режима GCM с применением внутреннего преобразования секрета;

– методы получения обоснованных нижних оценок уровня стойкости модифицированных режимов выработки имитовставки OMAC и AEAD-режима GCM в целевых моделях нарушителя.

Следует отметить, что результаты диссертации существенно использованы при стандартизации в Российской Федерации режима MGM, а разработанный в рамках диссертации режим OMAC-ACPKM-Master стандартизирован в Российской Федерации и стал частью международного документа RFC 8645.

Автореферат диссертации четко структурирован, полностью отражает результаты диссертации, опубликованные в 5 научных трудах, 3 из которых представлены в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Основные результаты диссертации, докладывались на международных и всероссийских конференциях и семинарах.

Судя по автореферату и публикациям, диссертационная работа Лилии Руслановой Ахметзяновой по уровню выполнения, новизне и актуальности полностью соответствует критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова, а ее автор заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Старший преподаватель
кафедры Компьютерная безопасность
МИЭМ НИУ ВШЭ
к.ф.-м.н. [redacted] В.О. Миронкин

Контактные данные:
Тел.: [redacted]
e-mail: mironkin.v@mail.ru.
Адрес места работы: г. Москва, ул. Таллинская, д. 34.

Я, Миронкин Владимир Олегович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку.

«23» мая 2022 года

[redacted]

Подпись заверяю
[redacted]
23.05.2022