ОТЗЫВ

на автореферат диссертации
Ахметзяновой Лилии Руслановны
«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»

Диссертация Л.Р. Ахметзяновой посвящена синтезу и анализу симметричных схем обеспечения конфиденциальности и целостности информации, использующих только один секретный параметр (AEAD-схем). Объектом исследования диссертации является та часть конструкции AEAD-схемы, независимая от базового примитива, которую принято называть AEAD-режимом. Тематика диссертационного исследования, связанная с развитием и совершенствованием математического аппарата для получения обоснованных оценок уровня информационной безопасности AEAD-режимов, актуальна как в теоретическом, так и в прикладном смысле.

К значимым результатам диссертации, имеющим научную новизну, можно отнести следующие:

1. построены новые математические методы получения обоснованных нижних оценок уровня стойкости для AEAD-режимов в базовых и расширенных моделях нарушителя;

2. построены методы получения обоснованных верхних оценок преобладаний нарушителей, определяемых базовыми и расширенными моделями для целостности и конфиденциальности;

3. разработаны новые AEAD-режимы с улучшенными комбинаторными свойствами и повышенным уровнем информационной безопасности по сравнению с существующими отечественными AEAD-режимами.

Теоретическая значимость полученных результатов характеризуется разработанными в диссертации методами оценки стойкости, имеющими математическую природу. Разработка методов проведена в рамках математических моделей, подробно описывающих возможности нарушителя и его цели. Автором успешно преодолен ряд существенных трудностей, возникающих на пути разработки данных методов.

Практическая ценность заключается в разработке новых конструкций, позволяющих эффективно решать задачу одновременного обеспечения конфиденциальности и целостности информации в прикладных системах.

Результаты позволяют сделать вывод, что цель диссертационной работы достигнута, а задачи, поставленные соискателем, выполнены.

Автореферат диссертации четко структурирован, достаточно полно

отражает результаты диссертации, опубликованные в 5 статьях, в том числе, в 3 статьях в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

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

Кандидат физико-математических наук,

Начальник отдела криптографического анал[redacted]

ООО «Код Безопасности» А.М. Коренева

Контактные данные:

тел.: +7 495 982 30 20, доб. 404, e-mail: a.koreneva@securitycode.ru

Адрес места работы:

115230, Москва, 1-й Нагатинский проезд, д.10, стр.1

Тел: +7 (495) 982-30-20 (многоканальный)

Я, Коренева Алиса Михайловна, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку.

«19» мая 2022 г.

Подпись Кореневой А.М. удостоверяю

[redacted]

Руководитель группы
[redacted]
ИВАНОВА