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 решению важной задачи разработки схем одновременного обеспечения конфиденциальности и целостности информации (AEAD-схем) и оценки их уровня стойкости в релевантных моделях нарушителя. Автором доказаны оценки уровня стойкости для существующих AEAD-схем на основе блочных симметричных алгоритмов, рассматриваемых в рамках процесса стандартизации схем указанного типа в России, а также разработаны новые конструкции, для которых удалось обосновать улучшенные оценки уровня стойкости с применением подходов теории вероятностей и теории сложности алгоритмов.

Совокупность полученных в диссертационной работе Л.Р. Ахметзяновой результатов позволяет констатировать успешное решение рассматриваемой задачи.

Считаю важным отдельно отметить разработанный автором режим аутентифицированного шифрования MGM2, а также оценки его уровня стойкости. Указанный режим может быть задействован в тех случаях, когда не удается обеспечить уникальность вектора инициализации, что нередко случается в практических приложениях. Например, в широко используемом протоколе построения частных виртуальных сетей WireGuard для защиты от атак типа «отказ в обслуживании» каждый раз вырабатывается случайный вектор инициализации. Таким образом, обладая формальным обоснованием стойкости, разработанный Л.Р. Ахметзяновой режим MGM2 может рассматриваться в качестве решения актуальных задач информационной безопасности.

Результаты диссертации опубликованы в 5 работах, из них 3 – в рецензируемых изданиях, индексируемых Scopus, Web Of Science, RSCI, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации,

информационная безопасность. Полученные в диссертации результаты апробированы на международных конференциях, научных семинарах.

Содержание автореферата диссертации соответствует паспорту специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Считаю, что диссертация Ахметзяновой Л.Р. «Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации» отвечает всем требованиям, изложенным в «Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова» для кандидатских диссертаций, 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,
Старший специалист-исследователь
Лаборатории криптографии
АО "НПК "Криптонит" [redacted] М.В. Николаев

«23» мая 2022 г.

Подпись Николаева М.В. удостоверяю
Генеральный директор
АО "НПК "Криптонит" [redacted] В.М. Хачатуров