В диссертационный совет МГУ.012.3 при Федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет имени М.В. Ломоносова».

ОТЗЫВ

официального оппонента на диссертацию

Давыдова Степана Андреевича

«Анализ и синтез некоторых классов линейных и нелинейных преобразований для использования в XSL-схемах», представленную на соискание учёной степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Диссертация С. А. Давыдова посвящена актуальным вопросам анализа и синтеза линейных и нелинейных преобразований, используемых в XSL-схемах при построении блочных шифров и хэш-функций.

Блочные шифры являются основным механизмом решения ряда задач защиты информации криптографическими методами, в том числе обеспечения конфиденциальности данных. На основе XSL-схем построены блочные шифрсистемы AES и DES (стандарты NIST, США), Кузнечик и Магма (стандарты Российской Федерации), SM4 (стандарт КНР), PRESENT (стандарт ISO) и др. Хэш-функции используются при вычислении контрольных сумм и имитовставок, при хранении и проверке паролей, при генерации и проверке электронных подписей, разработке постквантовых электронных подписей. На основе XSL-схем построены хэш-функции Стрибог (стандарт Российской Федерации), PHOTON и Whirlpool (стандарты ISO) и др.

Конструкция XSL-схем, предложенная более полувека назад, в настоящее время продолжает активно исследоваться. Одним из актуальных вопросов является разработка низкоресурсных блочных шифрсистем для реализации алгоритмов в RFID-метках, устройствах интернета вещей, а также серверах, обрабатывающих большие потоки данных, например, алгоритмы шифрования PRESENT, LED, GIFT, Skinny, Midory, Craft, ASCON и др. Для решения указанных задач также используются низкоресурсные реализации известных блочных шифрсистем.

XSL-схемы сконструированы из трех подсхем: подмешивание к данным бинарного ключа с помощью XOR-суммирования, нелинейное отображение S

и линейное преобразование L. Основное внимание диссертант уделил в работе исследованию реализации преобразования L и исследованию характеристик нелинейного отображения S. Важнейшими характеристиками этих функций являются дифференциальная равномерность соответствующей матрицы, нелинейность (расстояние по Хэммингу до класса аффинных функций) и алгебраическая степень.

Автором получен ряд теоретически значимых и практически важных результатов в указанной области.

В первой из четырех глав автор представил результаты исследования вопросов построения нелинейных преобразований с криптографическими характеристиками, близкими к оптимальным значениям. Доказаны теоремы о дифференциальной 4-равномерности подстановок, построенных при помощи предложенной конструкции и показана применимость конструкции к ряду практически важных преобразований.

Во второй главе доказана теорема 2.1 о минимальном числе слагаемых в разложении матрицы в сумму произведений диагональных матриц и матриц, реализуемых с помощью умножения на элемент кольца.

В третьей главе описаны все решения уравнения подобия для сопровождающей матрицы преобразования, а также разложения произвольной рекурсивной матрицы в произведение двух матриц, допускающих эффективную в определенном смысле реализацию.

В четвертой главе получен ряд важных свойств, относящихся к подобию матрицы-циркулянта верхнетреугольной матрице Тёплица, к инвариантным подпространствам матрицы-циркулянта и к максимально рассеивающим матрицам-циркулянтам.

Полученные результаты могут быть востребованы государственными организациями и коммерческими структурами, занимающимися анализом и синтезом блочных шифров на основе XSL-схем.

Работа написана на хорошем математическом уровне. Научные положения, выводы и рекомендации диссертационной работы обоснованы.

Основные результаты диссертации, вынесенные автором на защиту, являются новыми. Их достоверность подтверждается как приведенными в публикациях математическими доказательствами, так и выполненной автором апробацией результатов с помощью докладов на соответствующих данной тематике математических конференциях и семинарах.

Автореферат соответствует диссертации и достаточно полно отражает ее содержание. Вместе с тем, по диссертации и автореферату имеются замечания:

1) не представлен достаточно полный обзор известных результатов в той области, которой посвящены исследования диссертанта, что снижает точность позиционирования полученных в работе результатов в общей системе достигнутых знаний;

2) в исследованиях первой главы не уделено внимания вопросам вычислительной сложности построения нелинейных преобразований с криптографическими характеристиками, близкими к оптимальным значениям, что не позволяет сделать сравнение со сложностью построения аналогичных объектов другими известными методами;

3) в тексте диссертации на страницах 10, 77 использована неаккуратная формулировка про «подстановки с ***максимально известной*** нелинейностью»; по-видимому, имелись ввиду подстановки, нелинейность которых совпадает с максимальным среди известных значений нелинейности подстановок.

Данные замечания не снижают существенно в целом позитивного впечатления от выполненной диссертационной работы.

Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к работам подобного рода. Содержание диссертации соответствует специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (по физико-математическим наукам), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова. Диссертационное исследование оформлено согласно требованиям Положения о совете по защите диссертаций

на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Московского государственного университета имени М.В.Ломоносова. Таким образом, соискатель Давыдов Степан Андреевич заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Вывод: автором получены новые значимые результаты в области свойств нелинейных и линейных функций. Диссертационная работа Давыдова Степана Андреевича «Анализ и синтез линейных и нелинейных преобразований для использования в XSL-схемах» соответствует требованиям, предъявляемым к кандидатским диссертациям Положением о присуждении ученых степеней, утвержденным постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, а ее автор, Давыдов Степан Андреевич, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:
Профессор
Факультета физики, математики и естественных наук
Российского университета дружбы народов (РУДН) им. Патриса Лумумбы,
доктор физико-математических наук, профессор

Владимир Михайлович Фомичев

21 октября 2025 года

117198, Москва, ул. Миклухо-Маклая, 6
Тел.
E-mail:

Подпись Фомичева В.М. удостоверяю.

Ученый секретарь Ученого совета
факультета физико-математических и естественных наук
ФГАОУ ВО «Российский университет дружбы народов имени П. Лумумбы»

Зарядов Иван Сергеевич