ОТЗЫВ

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

Исследование криптографических свойств математических преобразований, на основе которых строятся системы шифрования и функции хэширования, представляет собой важнейшую задачу в комплексе вопросов обеспечения безопасности информации.

Диссертация Давыдова Степана Андреевича посвящена вопросам анализа и синтеза линейных и нелинейных преобразований, используемых в XSL-схемах.

В автореферате диссертации, наряду с обсуждением актуальности темы диссертации, ее теоретической и практической значимости, новизны результатов, изложено содержание результатов диссертации.

XSL-схемы определяют признанный современный метод построения блочных шифрсистем и функций хэширования. На основе XSL-схем построены шифрсистемы: AES, Кузнечик, Магма, SM4, хэш-функции Стрибог, PHOTON, Whirlpool и многие другие.

К используемым в XSL-схемах преобразованиям предъявляются, с одной стороны, криптографические требования, выполнение которых позволяет противостоять атакам на системы защиты, и, с другой - эксплуатационные требования по производительности и простоте реализации.

Для стойкости схемы к дифференциальному и линейному криптоанализу нелинейные преобразования (S-блоки) должны обладать низким показателем дифференциальной равномерности и одновременно высокой нелинейностью. Автор диссертации (глава 1) построил S-блоки произвольной чётной размерности s с оптимальными из известных на текущий момент характеристиками: 4-равномерностью и нелинейностью $2^{s-1}-2^{s/2}$.

Вычислительными методами для размерности 8 получены значения алгебраической степени и графовой алгебраической иммунности построенных подстановок.

К линейным преобразованиям в XSL-схемах предъявляется требование обеспечения быстрого рассеивания активных S-блоков. В главах 2 и 3 диссертации, согласно автореферату, максимально рассеивающие матрицы исследуются на предмет эффективной программной реализации. Для рекурсивных матриц, т.е. степеней сопровождающих матриц некоторого многочлена, и циркулянтных матриц получены разложения, на основе которых предложены новые подходы к реализации соответствующих линейных преобразований. Результаты разложений подкреплены строгими математическими доказательствами. Для программных реализаций матрицы шифрсистемы Кузнечик проведены вычислительные эксперименты. Реализация 4 (стр. 18) может представлять интерес для использования в устройствах с ограниченным объёмом памяти.

Другим криптографическим требованием к преобразованиям XSL-схем является невозможность использованиях их инвариантных подпространств для нахождения инвариантов раундовой функции. В аспекте этого требования проведены исследования главы 4.

Для нелинейных преобразований описаны инвариантные подпространства в случае параллельного использования одинаковых S-блоков - наиболее распространенный на практике случай. Для циркулянтных матриц полностью описаны инвариантные подпространства в случае максимально рассеивающих матриц. Для рекурсивных матриц показано отсутствие инвариантных подпространств определенного вида. Результаты работы применимы к матрицам, используемым в шифрсистемах AES, Кузнечик и хэш-функции Whirlpool.

Результаты диссертации кратко и структурированно представлены в автореферате. Изложенные результаты представляют теоретический и практический интерес. Все представленные в диссертации результаты

опубликованы в рецензируемых научных изданиях, доложены на криптографических конференциях и семинарах. Результаты являются новыми.

По автореферату можно высказать некоторые замечания, связанные с удобством восприятия содержания и дополнительной информативностью автореферата:

- на стр. 11 приводится вполне традиционное определение функции-индикатора, но отсутствует более частное определение алгебраической иммунности;
- на стр. 12 используется, без его определения, понятие почти бент преобразования с формулировкой некоторого результата с этим понятием;
- в таблице 1 (стр. 18, Сравнение реализаций шифрсистемы Кузнечик) для известных реализаций было бы целесообразно указать авторство реализаций.

Указанные замечания не умаляют значимости диссертационного исследования.

Рассмотрение автореферата позволяет сделать вывод, что соискатель Давыдов Степан Андреевич заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Кандидат физико-математических наук,
Зам. начальника отдела ООО «КРИПТО-ПРО»
Ошкин Игорь Борисович

«07» 11 2025г.

27018, г. Москва, ул. Сущевский Вал, дом 18, +7(495) 995-48-20
oshkin@cryptopro.ru

Подпись Ошкина И.Б. удостоверяю

Начальник отдела кадров.
ООО «КРИПТО-ПРО» Н.В. Дыбова