ОТЗЫВ

на автореферат диссертации Таранникова Ю. В. на тему:
«Конструкции и свойства корреляционно-иммунных и платовидных булевых функций»
на соискание ученой степени доктора физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Булевы функции являются фундаментальными строительными блоками практически во всех симметричных криптографических алгоритмах. Существует ряд атак на такие алгоритмы, каждая из которых основана в конечном итоге на том, что булевы функции не обладают каким-либо свойством. Среди таких атак выделяются различные типы корреляционных атак. Для противодействия этим атакам к булевым функциям, использующимся в криптоалгоритмах, выработан большой набор требований, среди которых важную роль играют корреляционная иммунность, а также высокая нелинейность, низкие значения автокорреляционных характеристик и пр. Поэтому ключевое значение приобрела проблема анализа взаимосвязи разных криптографически важных характеристик булевых функций и разработки конструкций функций, одновременно сочетающих в себе несколько требуемых свойств.

В этой связи тема диссертации Таранникова Ю.В., посвящённая анализу и синтезу булевых функций для обеспечения стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности, является актуальной.

К достоинствам диссертации можно отнести следующее.

Во-первых, автор предложил новые оригинальные конструкции синтеза булевых функций, обладающих высоким порядком устойчивости и достигающих верхней оценки нелинейности, также доказанной автором в представленной диссертационной работе. При этом конструкция не только представляет собой результат существования, но автором предложены эффективные способы ее схемной и программной реализации.

Во-вторых, в работе представлено много новых оценок, связывающих криптографически важные параметры булевых функций. Эти оценки превосходят ранее имевшиеся результаты, а некоторые из них являются неулучшаемыми.

В-третьих, в диссертации получены результаты о классах булевых функций (платовидных, l-уравновешенных и других), дающие систематический взгляд на свойства и структуру булевых функций, а также результаты о вспомогательных объектах, таких как разбиение пространств над конечным полем на аффинные подпространства, которые как позволяют породить обширные классы криптографически важных булевых функций, так и представляют самостоятельный научный интерес.

Эти и другие результаты составляют научное содержание рецензируемой диссертации и являются существенным научным продвижением.

Вместе с тем, есть некоторые критические пожелания по содержанию автореферата, в частности имеется некоторое количество опечаток, не все употребляемые без определения понятия, являются широко известными.

Эти замечания не затрагивает научной сути диссертации, а скорее касаются способа изложения материалов диссертации в автореферате. В целом диссертация Таранникова Ю.В. на тему: «Конструкции и свойства корреляционно-иммунных и платовидных булевых функций» соответствует требованиям, предъявляемым к диссертациям на соискание учёной степени доктора физико-математических наук и является существенным продвижением в решении крупной научной проблемы обеспечения стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности.

Учитывая все вышеизложенное, считаю, что Таранников Ю.В. заслуживает присуждения ученой степени доктора физико-математических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Алексеев Евгений Константинович
к.ф.-м.н., ООО “КРИПТО-ПРО”, начальник отдела криптографических исследований
Email: alekseev@cryptopro.ru
+7 967 137-99-57
127018, г. Москва, ул. Сущевский Вал, дом 18, этаж 17