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»

Важнейшим способом построения потоковых шифров является использование одного или нескольких регистров сдвига с линейной обратной связью и линейной преобразующей функции для получения псевдослучайной функции с большим периодом. Определение криптостойкости таких шифров сводится к исследованию свойств этой функции, которые выражаются в виде ограничений на те или иные их характеристики. В частности, для противостояния различным видам криптографических атак на шифры, среди которых выделяются корреляционные атаки, функция должна обладать уравновешенностью, корреляционной иммунностью достаточно большого порядка, большой нелинейностью, высокой алгебраической степенью, а также некоторыми другими свойствами. Эти критерии конфликтуют друг с другом, и рецензируемая диссертационная работа посвящена исследованию характеристик этих критериев, в первую очередь корреляционной иммунности, в том числе ее сочетанию с нелинейностью, а также разработке эффективных конструкций функций, сочетающих в себе указанные характеристики. Таким образом, тема диссертации Таранникова Ю.В. посвящена обеспечению стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности, является актуальной с позиции развития теории и практики методов защиты информации и информационной безопасности.

К достоинствам диссертации можно отнести следующее.

Во-первых, автор разработал серию последовательно углубляющихся методов построения m-устойчивых булевых функций от n переменных, нелинейность которых достигает верхней границы $2^{n-1}-2^{m+1}$, также установленной автором. До работ автора функции с такими параметрами были известны только для очень узкого диапазона пар значений (m,n). Автор также показал, что многие построенные им функции имеют низкую вычислительную сложность, что делает их эффективными для практической реализации.

Во-вторых, автор произвел анализ взаимосвязи корреляционной иммунности булевых функций не только с их нелинейностью, но и с другими криптографическими характеристиками булевых функций, важными при использовании булевой функции в качестве криптографического примитива в системах защиты информации.

В-третьих, автор развил технику спектрального анализа булевых функций, особенно в случаях разреженного носителя спектра булевых функций. Значительное место в диссертационной работе уделено изучению платовидных булевых функций, носитель спектра которых имеет специальный вид, способствующий наличию криптографически полезных свойств. Получены

результаты об аффинном ранге булевых функций. Также глубоко изучены разбиения пространства двоичных и q-ичных векторов на аффинные подпространства, что позволяет строить большое число криптографически сильных булевых функций.

В-четвертых, получены результаты о классах функций, близких к корреляционно-иммунным, но с немного ослабленными свойствами (l-уравновешенных функций), что позволяет расширить множество изучаемых функций новыми практически полезными конструкциями.

Эти и многие другие результаты составляют научную суть рецензируемой диссертации и являются серьезным продвижением в задаче обеспечения стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности.

Есть некоторое количество критических замечаний по содержанию автореферата, в частности, он содержит некоторое количество опечаток, а также используются без определений понятия, не являющиеся широко известными.

Эти замечания не затрагивают 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, содержит новые сильные научные результаты и является существенным продвижением в развитии теории и практики методов защиты информации.

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.

д.ф.-м.н., старший научный сотрудник ИПМ им. М.В. Келдыша РАН
Попков Кирилл Андреевич
125047, Москва, Миусская пл., д. 4
тел.: +79067838377
e-mail: kirill-formulist@mail.ru

Подпись Попкова К.А. заверяю: