

ОТЗЫВ

на автореферат диссертационной работы Высоцкой Виктории Владимировны «Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки», представленной к защите на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность»

Диссертационное исследование Высоцкой Виктории Владимировны посвящено вопросам построения схемы цифровой подписи на основе кодов, исправляющих ошибки. Анализ стойкости теоретико-кодовых криптосистем во многих случаях опирается на изучение структурных свойств используемых кодов, что влечёт необходимость исследования соответствующих открытых вопросов. Также стоит отметить, что от выбранного класса кодов, как правило, существенно зависит не только стойкость, но и на эффективность реализации всей схемы. В ряде случаев с целью сокрытия структуры кода используется не код, а некоторый его подкод. Одним из связанных открытых вопросов является исследование стойкости криптосистем, основанных на подкодах кодов Рида–Маллера коразмерности больше 1.

К числу наиболее интересных результатов работы можно отнести описание структурных свойств подкодов кода Рида–Маллера второго порядка $RM(2, m)$, связанных со сведением к атаке на схему, построенную на полном коде Рида–Маллера, для которой в литературе известны эффективные структурные атаки. С целью описания подкодов, потенциально пригодных для использования в рассматриваемых в работе криптографических приложениях, вводятся новые термины - стабильные и нестабильные подкоды, при этом показано, что доля нестабильных подкодов кода Рида–Маллера порядка r $RM(r, m)$ с ростом m стремится к нулю. Введено понятие кода с разложимым и неразложимым квадратом и доказано, что любой линейный код обязан удовлетворять одному из этих определений. Также стоит отметить предложенные и проанализированные в работе алгоритмы построения невырожденных квазициклических матриц применительно к реализации одной из рассматриваемых схем цифровой подписи.

В качестве недостатков можно отметить следующие:

1. По тексту автореферата имеется некоторое количество опечаток, а также стилистических неточностей, например, “...сведения о этих кодах...” на стр. 13, “...векторов порядка r ...” на стр. 14, “маловероятно попасть в подкод” на стр. 16;
2. В тексте присутствует нестандартная терминология, например, “по внутреннему источнику случайности”, “сложность построения $\langle \dots \rangle$ становится запретительной”;

3. Не хватает содержательных выводов из оценок, представленных в Теоремах 3, 4, 7, 18, связанных, например, с исследованием асимптотического поведения представленных оценок.

Несмотря на представленные замечания, считаю, что диссертационная работа Высоцкой Виктории Владимировны «Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки» является завершённым научным исследованием, которое вполне соответствует всем требованиям «Положения о присуждении учёных степеней в МГУ имени М.В. Ломоносова», и рекомендую её к защите в диссертационном совете МГУ 012.3 на соискание учёной степени кандидата физико-математических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Старший преподаватель
кафедры теоретической кибернетики
механико-математического факультета
Новосибирского государственного университета,
кандидат физико-математических наук

А.В. Куценко

Куценко Александр Владимирович
630090, Новосибирск, ул. Пирогова, 1
ФГАОУ ВО «Новосибирский национальный
исследовательский государственный университет»
a.kutsenko@g.nsu.ru