ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Лелюка Евгения Андреевича на тему
«Синтез постквантовой схемы инкапсуляции сеансового ключа»,
представленную на соискание учёной степени кандидата технических наук
по специальности 2.3.6 «Методы и системы защиты информации,
информационная безопасность»

1. Актуальность темы диссертационного исследования

Стойкость применяемых в настоящее время на практике асимметричных криптосистем основана на сложности задач факторизации целых чисел или дискретного логарифмирования в конечной группе. Однако показано, что эти задачи могут быть решены за полиномиальное время на квантовом компьютере. Актуальной задачей криптографии в настоящее время является разработка криптосистем, стойких к атакам с использованием квантовых вычислений. Об этом свидетельствует проведение таких конкурсов, как NIST PQC (США), KpqC Competition (Южная Корея), а также работа рабочей группы ТК26 (Российская Федерация) по синтезу новой схемы инкапсуляции сеансового ключа, которая была бы стойкой против нарушителя, имеющего доступ к квантовому компьютеру достаточной мощности. Криптографические системы, в основе которых лежит применение помехоустойчивых кодов, рассматриваются как одна из альтернатив используемым в настоящее время асимметричным криптографическим системам.

Первой кодовой считается криптосистема, предложенная Робертом Мак-Элисом в 1978 году, в основе которой лежит использование кодов Гоппы (Original McEliece). На этой системе основан протокол инкапсуляции сеансового ключа NTS-KEM, участвовавший в конкурсе NIST PQC. Впоследствии этот проект был объединен с проектом Classic McEliece, входящим в число финалистов NIST PQC. Стойкость обеих систем, в частности, основана на сложности задачи декодирования случайного кода. Для этой задачи на текущий момент не найдено эффективного решения в модели квантовых вычислений. При этом, размер открытого ключа является недостатком систем на кодах Гоппы. Попытки использовать коды Рида-Соломона, коды Рида-Маллера, алгебро-геометрические коды, коды с низкой плотностью проверок на четность для уменьшения ключа не увенчались успехом, поскольку были найдены эффективные атаки на ключ (структурные атаки) для соответствующих криптосистем. Также стоит отметить, что коды Гоппы принадлежат классу альтернантных кодов. На текущий момент для некоторых классов кодов Гоппы также найдены структурные атаки на

соответствующие криптосистемы. Кроме того, была найдена эффективная атака для одного класса подпространственных подкодов кодов Рида-Соломона, которые также являются альтернантными. Эти результаты не исключают появления в будущем эффективных структурных атак на кодовые криптосистемы и на других классах кодов Гоппы. Поэтому, несмотря на имеющиеся стойкие схемы, актуальна задача поиска других эффективно декодируемых помехоустойчивых кодов, обеспечивающих высокую стойкость кодовых криптосистем типа Мак-Элиса при небольшом размере открытого ключа.

2. Оценка достоверности полученных результатов и новизны диссертационного исследования

Достоверность полученных результатов и обоснованность научных положений подтверждается корректностью математических выкладок и доказательств теорем, а также экспериментальными исследованиями.

Научная новизна состоит в следующем:

1. Разработаны и программно реализованы алгоритмы шифрования и расшифрования криптосистемы типа Мак-Элиса на основе D-кодов. В частности, разработаны и реализованы алгоритмическая модель декодирования с гарантированным исправлением ошибок для D-кодов, отличающаяся применением мажоритарного подхода к декодированию, и алгоритмы вероятностного декодирования D-кодов на основе кодов Рида-Маллера, отличающиеся декодированием ошибок в количестве, превышающем половину кодового расстояния, и позволяющие за счет этого сократить размер открытого ключа. Построенные алгоритмы обеспечивают эффективное расшифрование в криптосистеме типа Мак-Элиса.

2. Разработан и программно реализован алгоритм определения множества сильных и слабых ключей криптосистемы на D-кодах на основе кодов Рида-Маллера, отличающийся использованием найденных криптографических свойств разложимости степеней Шура-Адамара D-кодов на основе кодов Рида-Маллера в прямую сумму кодов Рида-Маллера, и позволяющий эффективно находить параметры стойких систем на D-кодах.

3. Разработан алгоритм комбинированной атаки для слабых ключей криптосистемы типа Мак-Элиса на основе D-кодов, отличающийся применением структурной атаки с частичным восстановлением секретного ключа для увеличения вероятности успеха атаки на шифрограмму. Теоретически показано и экспериментально подтверждено, что разработанный алгоритм позволяет для слабых ключей криптосистемы значительно упростить атаку на шифрограмму относительно классической атаки декодированием по информационным совокупностям.

4. На основе разработанных подходов к декодированию D-кодов на кодах Рида-Маллера, исследованных криптографических свойств этих кодов и результатов анализа стойкости построена новая криптосистема типа Мак-Элиса, отличающаяся применением конструкции D-кодов.

Теоретическая значимость. Теоретические результаты, полученные в данном исследовании, в частности, свойства произведения Шура-Адамара D-кодов и результаты анализа стойкости криптосистемы на этих кодах могут использоваться как при дальнейшем изучении криптосистем на D-кодах, например, для уточнения множеств сильных и слабых ключей построенной криптосистемы, так и при разработке новых кодовых криптосистем на основе подкодов прямой суммы кодов.

Практическая ценность работы. Построенная асимметричная кодовая криптосистема типа Мак-Элиса на D-кодах на основе кодов Рида-Маллера обладает либо большей стойкостью при сопоставимом размере ключа, либо меньшим размером ключа при сопоставимой стойкости, либо большей стойкостью при меньшем размере ключа по сравнению с системой Original McEliece. Это позволяет применять предложенную систему в схемах обеспечения конфиденциальности данных, например, для инкапсуляции сеансового ключа симметричной криптосистемы или для повышения защищенности данных, циркулирующих в информационных системах, за счет использования рандомизированного шифрования. Разработанный теоретико-графовый подход к декодированию D-кодов и, в частности, тензорного произведения кодов может применяться в задаче защиты от помех в каналах связи.

3. Оценка содержания диссертации, степени её завершённости, подтверждение публикаций автора

Содержание и структура диссертации Лелюка Е. А. соответствует теме, целям и задачам исследования. Диссертация написана на русском языке, состоит из введения, трех глав, заключения, списка используемой литературы из 85 наименований и двух приложений. Полный объем диссертации составляет 156 страниц (в том числе приложений 7 стр.), включая 10 рисунков и 14 таблиц. Структура диссертации логичная, рисунки и таблицы оформлены в соответствии со стандартами ГОСТ.

Во введении обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель, ставятся задачи работы, излагается научная новизна и практическая значимость представляемой работы, декларируются положения, выносимые на защиту,

область исследования и апробация полученных результатов, а также приведено краткое содержание каждой из глав.

В первой главе рассматриваются вопросы использования асимметричных криптосистем в протоколе инкапсуляции сеансового ключа, а также вопросы построения новых кодовых криптосистем для таких протоколов. Другими словами, рассматривается задача синтеза новой схемы инкапсуляции сеансового ключа, которая решается в последующих главах. Приводятся основные понятия теории кодирования, используемые в кодовой криптографии. Также в рамках задачи построения эффективных декодеров для применения в кодовой криптосистеме рассматривается концепция мажоритарного декодирования, на основе которой в следующей главе строится один из декодеров D-кодов: с гарантированным исправлением ошибок.

Вторая глава посвящена исследованию D-кодов. Именно, приводится определение D-кодов и исследуются их криптографические свойства. В частности, находятся условия разложимости степеней Шура-Адамара D-кодов на основе кодов Рида-Маллера в прямую сумму неразложимых кодов. Для эффективного расшифрования в главе строятся алгоритмические модели гарантированного и вероятностных декодеров для D-кодов. В качестве гарантированного строится мажоритарный декодер, а в качестве вероятностных – декодеры, использующие блочную структуру кодового слова D-кода. Для вероятностных декодеров приводятся результаты экспериментов, демонстрирующих их эффективность.

Третья глава посвящена синтезу схемы инкапсуляции сеансового ключа (KEM) на основе системы типа Мак-Элиса на D-кодах на основе кодов Рида-Маллера, а также исследованию ее стойкости. Именно, выделяются множества сильных и слабых ключей криптосистемы Мак-Элиса на D-кодах на основе кодов Рида-Маллера. Для слабых ключей криптосистемы строится комбинированная атака, позволяющая с помощью структурной атаки значительно повысить эффективность атаки на шифрограмму, и приводится оценка ее эффективности. Для сильных ключей криптосистемы подбираются параметры для возможности практического применения и проводится сравнение с оригинальной системой на кодах Гоппы при использовании разных подходов к декодированию D-кодов.

В заключении изложен основной научный результат диссертации, а также сформулированы теоретические и практические результаты, полученные в результате диссертационной работы.

В приложениях приводятся акты о внедрении результатов диссертационной работы, а также свидетельство о государственной регистрации программы для ЭВМ.

Диссертация является завершённым научно-исследовательским трудом. Задачи, поставленные автором, решены полностью, цель исследования достигнута.

Основные положения диссертации опубликованы в 9 научных печатных работах, в том числе: 3 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК (категории К1, RSCI), 2 – в научных рецензируемых журналах, индексируемых в базе Scopus (Q3, что соответствует категории ВАК К1), 4 – в материалах конференций и других изданиях. Получено свидетельство о государственной регистрации программы для ЭВМ. Результаты работы прошли апробацию на научных конференциях различного уровня.

4. Соответствие специальности

Диссертация соответствует паспорту научной специальности 2.3.6. – «Методы и системы защиты информации, информационная безопасность» и охватывает следующие области исследования, входящие в эту специальность: «Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов» (п. 19).

5. Замечания по диссертационной работе

- Автору следовало выделить больше места описанию D- кодов и подробнее расписать условия s1)-s3). Из приведенных автором определений, без использования исходных статей (Kasami, T. On the Construction of a Class of Majority–Logic Decodable Codes / T. Kasami, S. Lin // IEEE Transactions on Information Theory.1971.– Vol. IT-17, no. 5.– P. 600-610.)практически невозможно понять описание и свойства D-кодов. Из приведенных автором обозначений на стр.43 не ясно , что такое L(), какой величиной снизу ограничено значение dij . Из приведенного текста на стр. 43, 44 также не понятно, почему семейство кодов S1 , S2 не пустое. Кроме того на стр. 44 не определен параметр J. На странице 44 предлагается называть код $\overline{C(D)}$ двойственным, однако его ортогональность исходному коду C(D) нигде не доказывается.

  Надо отметить, что в дальнейшем , при рассмотрении D-кодов как семейств кодов Рида-Маллера, приведенные ранее определения, утверждения и свойства становятся понятны и в целом не требуют доказательств или дополнительных пояснений.

- Автор использует не совсем корректное сравнение алгоритмов типа Мак-Элиса на кодах Гоппы и D-кодах, разрешая последним при шифровании использовать вектора ошибок веса большего половины минимального расстояния и не рассматривая такую же возможность для кодов Гоппы, которые могут быть при этом nhодекодированы списочно (то есть, так же, как и в предлагаемом автором случае для D-кодов с некоторой заранее известной ошибкой правильного расшифрования), например, по алгоритму, предложенному в статье [Bezzateev S, Bossert M; A Unified View on Known Algebraic Decoding Algorithms and New Decoding Concepts, IEEE Transactions on Information Theory, 2013,Volume:59, Issue: 11, pp. 7320 – 7336].
- В работе имеются некоторые стилистические неточности и опечатки.

Однако, перечисленные выше недостатки не снижают высокого уровня представленной работы и позволяют говорить о выполнении автором всех требований, предъявляемых к квалификационной работе на соискание ученой степени кандидата технических наук.

6. Заключение

Диссертация Лелюка Е. А. представляет собой законченную научно-квалификационную работу, посвящённую решению актуальной задачи, имеющей важное значение в области информационной безопасности. Диссертация обладает научной новизной, имеет теоретическую значимость и практическую ценность. Полученные результаты в полной мере отражены в авторских публикациях. Автореферат полностью отражает содержание диссертации.

Диссертация отвечает требованиям, установленным Положением «О присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» (в действующей редакции) и предъявленным к диссертациям на соискание учёной степени кандидата наук, а автор, Лелюк Евгений Андреевич, заслуживает присвоения ему учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Официальный оппонент
Доктор технических наук (05.13.01 «Системный анализ, управление и обработка информации»), профессор, заведующий кафедрой

«Информационная безопасность», Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»,
Беззатеев Сергей Валентинович

190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А, ГУАП
Тел. служ.: +7 (812) 710-65-10, email: bsv@guap.ru

«01» 12 2025 г. _____/С. В. Беззатеев/

Подпись С. В. Беззатеева заверяю