УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2022 Том 22 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2022 Vol. 22 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2022-22-2-324-331
УДК 004.056.55

Современные вариации криптосистем Мак-Элиса и Нидеррайтера

Вадим Валерьевич Давыдов[1]✉, Владислав Владиславович Беляев[2], Елизар Филаретович Кустов[3], Антон Георгиевич Леевик[4], Сергей Валентинович Беззатеев[5]

[1,2,3,4,5] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[5] Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация

[1] vvdavydov@itmo.ru✉, https://orcid.org/0000-0002-5544-2434
[2] v.beliaev@niuitmo.ru, https://orcid.org/0000-0002-1067-7483
[3] efkustov@itmo.ru, https://orcid.org/0000-0002-0191-1178
[4] agleevik@niuitmo.ru, https://orcid.org/0000-0003-1823-7877
[5] bsv@aanet.ru, https://orcid.org/0000-0002-0924-6221

Аннотация

Предмет исследования. Исследованы классические криптосистемы, предложенные Робертом Мак-Элисом в 1978 году и Гарольдом Нидеррайтером в 1986 году и их современные вариации. **Метод.** Выполнен детальный обзор пяти кодовых криптосистем с открытым ключом. **Основные результаты.** Показано, что некоторые из современных интерпретаций классических систем Мак-Элиса и Нидеррайтера имеют значительные недостатки. Установлено, что допущен ряд неточностей в описании криптосистемы XGRS на расширенных кодах Рида–Соломона, которая не обеспечивает заявленного уровня безопасности к атаке по информационным совокупностям. Продемонстрировано, что время генерации ключей и время расшифрования в современных кодовых криптосистемах достаточно велико, а открытый и секретный ключи занимают большой объем памяти. **Практическая значимость.** Выявленные неточности в рассмотренных схемах могут быть учтены при их улучшении и коррекции, а также при построении более точной оценки их уровня безопасности и эффективности. Представленные в работе кодовые криптосистемы могут рассматриваться как стандарты постквантовой криптографии и использоваться для защиты данных после появления мощного квантового компьютера.

Ключевые слова

постквантовая криптография, криптосистема Мак-Элиса, криптосистема Нидеррайтера, двоичные коды Гоппы, расширенные коды Рида–Соломона

Благодарности

Работа выполнена в рамках НИР № 620164 Университета ИТМО. Работа частично финансировалась Федеральной программой академического лидерства Приоритет 2030. Выражается благодарность Жан-Мишелю Дакуо за помощь в программной реализации.

Ссылка для цитирования: Давыдов В.В., Беляев В.В., Кустов Е.Ф., Леевик А.Г., Беззатеев С.В. Современные вариации криптосистем Мак-Элиса и Нидеррайтера // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 2. С. 324–331. doi: 10.17586/2226-1494-2022-22-2-324-331

Modern variations of McEliece and Niederreiter cryptosystems

Vadim V. Davydov[1]✉, Vladislav V. Beliaev[2], Elizar F. Kustov[3], Anton G. Leevik[4], Sergey V. Bezzateev[5]

[1,2,3,4,5] ITMO University, Saint Petersburg, 197101, Russian Federation
[5] Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, 190000, Russian Federation

[1] vvdavydov@itmo.ru✉, https://orcid.org/0000-0002-5544-2434
[2] v.beliaev@niuitmo.ru, https://orcid.org/0000-0002-1067-7483
[3] efkustov@itmo.ru, https://orcid.org/0000-0002-0191-1178
[4] agleevik@niuitmo.ru, https://orcid.org/0000-0003-1823-7877
[5] bsv@aanet.ru, https://orcid.org/0000-0002-0924-6221

Abstract
Classical cryptosystems proposed by Robert McEliece (1978) and Harold Niederreiter (1986) and their modern variations are studied. A detailed review of five code-based public key cryptosystems has been presented. It is shown that some of the modern interpretations of the classical McEliece and Niederreiter cryptosystems have significant issues. In particular, it has been established that the XGRS cryptosystem based on extended Reed-Solomon codes does not provide the declared level of security against the information set decoding attack, and also has a number of inaccuracies. It is shown that the time of key generation and decryption in modern cryptosystems is quite large, and the public and private keys take up a large amount of memory. The inaccuracies of the considered schemes revealed in this work can be used to improve and adjust the systems, as well as to build a more accurate assessment of their security level and efficiency. The presented cryptosystems can be considered as standards for post-quantum cryptography and can be used to protect data after development of powerful quantum computers.

Keywords
post-quantum cryptography, McEliece cryptosystem, Niederreiter cryptosystem, binary Goppa codes, generalized Reed-Solomon codes

Aknowledgements
The work is made as a part of research work no. 620164 at ITMO University. This project has received financial support from the Priority 2030 Federal Academic Leadership Program. We thank Jean-Michelle Dakuo for his help in programming implementation.

For citation: Davydov V.V., Beliaev V.V., Kustov E.F., Leevik A.G., Bezzateev S.V. Modern variations of McEliece and Niederreiter cryptosystems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 2, pp. 324–331 (in Russian). doi: 10.17586/2226-1494-2022-22-2-324-331

Введение

В настоящее время ведется активная разработка систем постквантовой криптографии. Это связано с появлением квантового компьютера и изобретением Питером Шором квантового алгоритма [1], позволяющего решать задачи факторизации и дискретного логарифмирования за полиномиальное время. Одним из разделов постквантовой криптографии в целом является криптография, основанная на кодах, исправляющих ошибки. Впервые такая система была построена Робертом Мак-Элисом в 1978 году [2] на основе нового класса двоичных кодов, предложенных В.Д. Гоппой в 1971 году [3]. Через 8 лет, в 1986 году, Гарольд Нидеррайтер [4] предложил одноименную криптосистему, построенную на обобщенных кодах Рида–Соломона [5]. В 1992 году В.М. Сидельников и С.О. Шестаков [6] опубликовали атаку на криптосистему Нидеррайтера, приводящую к вскрытию данной системы.

Впоследствии исследователи занимались разработкой различных модификаций схем, использующих помехоустойчивые коды. Сегодня также продолжаются исследования, связанные с поисками улучшений в оригинальных системах Мак-Элиса и Нидеррайтера. Основные идеи состоят в снятии ограничения на вес вектора ошибки, использование кодов, отличных от кодов Гоппы, а также увеличение стойкости системы к различным атакам, в частности к атаке по информационным совокупностям («information set decoding») [7].

В последних опубликованных работах описаны новые криптосистемы, основанные на оригинальных идеях Мак-Элиса и Нидеррайтера, однако все они были успешно вскрыты. В 1994 году В.М. Сидельниковым была предложена криптосистема, основанная на кодах Рида–Маллера [8], однако в 2007 году был представлен ее криптоанализ, показывающий вскрытие системы за полиномиальное время [9]. В 1995 году представлена криптосистема на кодах ранговой метрики Э.М. Габидулина [10], которая была взломана в 2008 году в работе [11]. В 2007 году предложена криптосистема на кодах с малой плотностью проверок (Low-Density Parity-Check, LDPC-кодах) [12], а в 2008 году в [13] — взлом системы. Использование алгебро-геометрических кодов также оказалось ненадежным [14, 15]. Попытки модифицировать криптосистему Мак-Элиса с тем, чтобы сделать ее более стойкой к различным атакам, также не увенчались успехом [16, 17].

Из представленного обзора видно, что оригинальные идеи Мак-Элиса и Нидеррайтера на сегодняшний день являются наиболее актуальными, а код, который до сих пор оказался устойчивым к различного вида атакам, — двоичный код Гоппы [18].

Постановка задачи

Рассмотрим три новые криптосистемы, на примере которых продемонстрированы существующие подходы и актуальное состояние постквантовой криптографии, использующей помехоустойчивые коды. Криптосистема «Classic McEliece» [19] была предложена международной группой авторов и приняла участие в конкурсе NIST (National Institute of Standards and Technology) на включение в стандарт постквантовой криптографии.

В схеме XGRS (eXtended Generalized Reed-Solomon), опубликованной в 2021 году [20], использованы расширенные коды Рида–Соломона [21]. По мнению авторов, данная схема устойчива к атакам Сидельникова–Шестакова и к атаке по информационным совокупностям. В настоящей работе выполнен подробный анализ безопасности и эффективности схемы XGRS. Впервые продемонстрирована ее неустойчивость к атаке по информационным совокупностям и доказано, что уровень ее безопасности к данной атаке не соответствует заявленному авторами оригинальной работы.

На примере схемы IKKR (Ivanov–Kabatiansky–Krouk–Rumenko), предложенной в [22] и основанной на результатах работы [23], продемонстрирована неэффективность идеи увеличения маскирующего векто-

ра за счет использования дополнительного случайного кодового слова.

В результате анализа представленных криптосистем выполнена оценка размеров ключей и выделена система, имеющая ключи минимального размера. Приведены результаты моделирования рассмотренных систем, позволяющие провести их численное сравнение.

Классические криптосистемы Мак-Элиса и Нидеррайтера

В 1978 году в работе [2] была предложена Робертом Мак-Элисом криптосистема, где в качестве кодов, исправляющих ошибки, выбраны двоичные коды Гоппы [3]. Также Гарольд Нидеррайтер в 1984 году в работе [6] предложил использовать обобщенные коды Рида–Соломона.

Данные криптосистемы являются классическими, так как впервые для шифрования были использованы идеи применения NP-полной задачи синдромного декодирования, сложность которой была доказана в работе [23]. Несмотря на то, что работа Нидеррайтера вышла через 8 лет после публикации Мак-Элиса, в ней использована более простая идея — математическая проблема синдромного декодирования случайного кода. Основным отличием криптосистем является случайность шифрования. В криптосистеме Мак-Элиса шифрование зависит от вектора ошибки, который выбирается случайным образом, в то время как в криптосистеме Нидеррайтера целенаправленно выбирается сообщение с определенными ограничениями.

Атакующий, стремясь взломать криптосистему Мак-Элиса или Нидеррайтера, должен решить NP-полную задачу синдромного декодирования [24], найти ближайшее кодовое слово линейного кода C к вектору в окружении пространства C, зная, что такое слово единственно. Злоумышленник не знает секретного кода, поэтому должен решать задачу для случайного кода без какой-либо специальной структуры.

В настоящее время существует несколько типов атак на системы, использующие помехоустойчивые коды.

Одна из них — атака полным перебором, которая для кодов большой размерности и избыточности становится невозможной из-за большого числа операций и соответственно времени их выполнения.

Для многих кодов из-за их структуры основной является атака Сидельникова–Шестакова. В 1992 году В.М. Сидельников и С.О. Шестаков показали возможность вскрытия системы Нидеррайтера из-за особенностей обобщенного кода Рида–Соломона [6]. Как утверждали авторы, их атака может быть применена и к двоичным кодам Гоппы. Впоследствии оказалось, что это не так, и система, построенная на двоичных кодах Гоппы, устойчива к данной атаке. В то же время структура обобщенного кода Рида–Соломона позволяет эффективно, за полиномиальное время, решить для них задачу синдромного декодирования, что делает невозможным их применение в системах шифрования с открытым ключом. Отметим, что идея Нидеррайтера нашла свое применение практически во всех современных криптосистемах, участвующих в конкурсе на стандартизацию, проводимом NIST. В частности, система «Classic McEliece» использует идею Нидеррайтера, но названа в честь Роберта Мак-Элиса из-за использования двоичных кодов Гоппы, устойчивых к атаке Сидельникова–Шестакова.

Самой опасной и универсальной является атака по информационным совокупностям, описанная в работах [7, 25].

Во многих современных научных работах данные системы шифрования модифицированы, использованы иные подходы к шифрованию и расшифрованию. Но все построенные системы сводятся к базовым идеям классических схем [2, 4]. Рассмотрим подробнее три системы, которые наиболее полно отражают текущее положение дел в области кодовой криптографии и дают представление о попытках улучшить системы Мак-Элиса и Нидеррайтера путем снятия некоторых ограничений (например, увеличение веса вектора ошибки).

Современный вариант криптосистемы Мак-Элиса на кодах Гоппы

Криптосистема на кодах Гоппы «Classic McEliece» представлена в работе [19]. В отличие от классической системы Нидеррайтера, где открытый ключ получается перемножением матриц, в современном варианте криптосистемы открытый ключ определяется представлением проверочной матрицы $\hat{\mathbf{H}}$ в систематическом виде. Поскольку такое представление матрицы является односторонней функцией, т. е. нельзя произвести обратную операцию перевода матрицы из систематического вида к исходному, матрицу $\mathbf{T}$, которая является урезанной версией матрицы $\hat{\mathbf{H}}$ без единичной матрицы слева, используют как открытый ключ. Умножение матрицы $\hat{\mathbf{H}}$ на дополнительные матрицы не требуется, так как это увеличивает время выполнения процедур шифрования и расшифрования, а также увеличивается размер ключей, а выигрыш в стойкости алгоритма совсем невелик. Отметим, что получение из матрицы $\hat{\mathbf{H}}$, приведенной к систематическому виду, секретных параметров кода Гоппы является сложной задачей, и на данный момент не существует таких алгоритмов, которые делали бы это за полиномиальное время.

Криптосистема XGRS на расширенных кодах Рида–Соломона

Криптосистема XGRS на расширенных кодах Рида–Соломона представлена в работе [20], где авторам удалось уменьшить размер открытого ключа по сравнению с криптосистемой в [19] и сохранить требуемый уровень безопасности к атаке по информационным совокупностям. Также авторы утверждают, что данная криптосистема устойчива к атаке Сидельникова–Шестакова и к атаке на основе произведения Шура [26] благодаря расширению и последующему за ним выкалыванию позиций исходного кода, которое приводит к изменению его структуры.

Заметим, что в [20] присутствуют некоторые неточности. В частности, на этапе генерации ключа нет информации о том, что результирующая матрица при-

водится к систематическому виду, однако, в процессе подсчета размеров ключей логически понятно, что часть матрицы «выбрасывается», что отображено в расчетных формулах. Также обнаружены неточности подсчета размеров ключей из-за неправильного округления величины $\log_2 q$.

Авторы работы [20] утверждают, что при параметрах кода Рида–Соломона над конечным полем F_{q^m} при $q = 13$, $m = 3$, где q — характеристика поля, m — степень расширения и, соответственно, длиной кода $n = 1258$ и числом информационных символов $k = 1031$ достигается 256-битный уровень безопасности к атаке по информационным совокупностям.

Такой же уровень достигается для двоичных кодов Гоппы в криптосистеме «Classic McEliece» с параметрами $n = 6960$, $k = 5413$, $q = 2$, $m = 13$ [19, 20]. Для проверки этого утверждения был выполнен пересчет вероятности успешной атаки при использовании кодов Рида–Соломона в криптосистеме XGRS [20] и двоичных кодов Гоппы в криптосистеме «Classic McEliece» по следующей формуле:

$$P_{\text{успеха}} = \frac{C_{n-t}^{k}}{C_{n}^{k}}, \qquad (1)$$

где C_n^k — биномиальный коэффициент из n по k; t — количество ошибок, исправляемых кодом.

Отметим, что полученные результаты дают грубую наглядную и вычислительно простую оценку вероятности реализации атаки по информационным совокупностям, поскольку в настоящей работе задачей является сравнительная оценка соотношения уровня безопасности системы «Classic McEliece» и системы на кодах Рида–Соломона [20]. Более точные формулы для оценки вероятности реализации атаки по информационным совокупностям представлены в работе [27]. Так как в криптосистеме XGRS на кодах Рида–Соломона шифрование ведется поблочно, рассчитаем общее количество блоков на длине кода (n), число информационных блоков (k) и кодовое расстояние (d).

Избыточность кода Рида–Соломона с параметрами $n = 1258$ и $k = 1031$ равна: $r = n - k = 227$. Получим минимальное расстояние такого кода $d = r + 1 = 228$, а число исправляемых ошибок кодом: $t = \left\lfloor \frac{d-1}{2} \right\rfloor = 113$.

Вычислим количество информационных блоков длины λ для расширенного кода Рида–Соломона [20]:

$$k' = \frac{mk - (m-\lambda)n}{\lambda} = \frac{3 \cdot 1031 - 1258}{2} = 611.$$

Общее количество блоков длины λ на длине $n = 2516$ расширенного кода совпадает с длиной кода и равно 1258. Для таких параметров вероятность успешной атаки по информационным совокупностям для криптосистемы на кодах Рида–Соломона приблизительно равна $5{,}9 \times 10^{-36}$. Воспользуемся параметрами для кода Гоппы [20] для «Classic McEliece» с 256-битным уровнем безопасности: $n = 6960$, $k = 5413$, $t = 119$. В соответствии с формулой (1), получим, что вероятность успешной атаки приблизительно равна $4{,}9 \times 10^{-80}$, что примерно соответствует 256-битному уровню безопасности.

Таким образом, очевидна неточность в расчетах безопасности системы, изложенная авторами в [20], и, соответственно, утверждение о выигрыше представленной системы по размеру открытого ключа в сравнении с «Classic McEliece» неверно.

Несмотря на то, что рассматриваемая система [20] на кодах Рида–Соломона не может быть вскрыта с помощью атаки Сидельникова–Шестакова, она неустойчива к атаке по информационным совокупностям и не может быть использована на практике в текущей редакции. Важно отметить, что использование кодов Рида–Соломона без их расширения также невозможно, так как в этом случае система становится уязвимой к атаке Сидельникова–Шестакова.

Криптосистема IKKR, использующая маскирующие вектора большого веса

Модификация современной криптосистемы Мак-Элиса на кодах Гоппы представлена в работе [22]. В работе рассмотрено повышение стойкости криптосистемы путем исключения обязательного ограничения на вес вектора ошибки. В отличие от оригинальной системы, где вес вектора обязательно должен быть меньше либо равен значению количества ошибок, исправляемых кодом, в системе [22] данное ограничение нивелируется применением линейных преобразований к вектору ошибки и введением кодовых слов в качестве «засаливающих» элементов.

В криптосистеме IKKR акцент сделан на увеличение веса вектора ошибок **e**, что может улучшить криптостойкость системы к атакам по информационным совокупностям. В криптосистеме вектор **e** умножен на матрицу

$$\mathbf{E}_{\text{pub}} = \mathbf{W} \times \mathbf{D} \times (\mathbf{C}_n + \mathbf{P}) \times \mathbf{M},$$

где **W**, **M** — случайные невырожденные матрицы размера $n \times n$; **P** — перестановочная матрица размера $n \times n$; **D** — диагональная матрица с t ненулевыми элементами на диагонали; $\mathbf{C}_n$ — матрица кодовых слов; $\mathbf{E}_{\text{pub}}$ — открытый ключ.

После расчета получим:

$$\mathbf{e} \times \mathbf{E}_{\text{pub}} = \mathbf{e} \times \mathbf{W} \times \mathbf{D} \times (\mathbf{C}_n + \mathbf{P}) \times \mathbf{M} = \\ = (\mathbf{e} \times \mathbf{W} \times \mathbf{D} \times \mathbf{C}_n + \mathbf{e} \times \mathbf{W} \times \mathbf{D} \times \mathbf{P}) \times \mathbf{M}.$$

Первое слагаемое — кодовое слово, так как матрица $\mathbf{C}_n$ — матрица, строки в которой — это кодовые слова. Второе слагаемое — вектор ошибки веса не более t. Данное условие получается из-за умножения на матрицу **D**. При умножении на данную матрицу ненулевыми остаются только те позиции вектора, которые соответствуют ненулевым ее столбцам. В итоге шифртекст будет представлять некое кодовое слово с ошибкой, но, в отличие от современной криптосистемы Мак-Элиса, если злоумышленник найдет алгоритм, по которому он правильно произведет декодирование, то он не сможет найти открытый текст, не зная остальных частей закрытого ключа.

Несмотря на устойчивость к атаке по информационным совокупностям, криптосистема IKKR оказалась

подвержена другим атакам. Криптоанализ системы описан в работе [28]. В работе показан алгоритм атаки, работающий за полиномиальное время, который позволяет найти открытый текст на основе шифртекста, а также приведена ссылка на программную реализацию данной атаки с помощью системы компьютерной алгебры Sagemath. Атака использует факт линейности шифрования в системе и строится на решении системы линейных уравнений, которая имеет решение, эквивалентное открытому тексту. Кроме того, время работы алгоритма атаки меньше времени, требуемого на сам процесс расшифрования.

Заметим, что данная атака является частной для криптосистемы IKKR и не применима для систем, рассмотренных выше.

Параметры криптосистем

На сегодняшний день одной из проблем, почему алгоритмы кодовой криптографии сложно использовать в практических системах, является проблема больших размеров ключей. Отметим, что под «большими» размерами понимается использование кодов огромной длины для достижения стойкости к атакам, описанным выше — это происходит из-за того, что приходится хранить элементы кода, такие как порождающая матрица, порождающий многочлен, множество нумераторов и т. д.

Оценим размеры ключей для рассмотренных криптосистем: оригинальной системы Мак-Элиса, «Classic McEliece» и XGRS на расширенных кодах Рида–Соломона. Допустим, что один элемент матрицы представляет один бит (за основу взяты двоичные коды).

Для оригинальной системы Мак-Элиса и системы «Classic McEliece» примем за основу код Гоппы с параметрами $m = 13$, $n = 6960$, $k = 5413$, $t = 119$. Для криптосистемы XGRS на расширенных кодах Рида–Соломона параметры кода: $q = 13$, $n_{RS} = 1258$, $k_{RS} = 1031$, $t_{RS} = 114$, а также дополнительные параметры $\lambda = 2$, $m_{RS} = 3$.

Результаты расчетов представлены в табл. 1.

В табл. 1 используются следующие обозначения: $\mathbf{S}(k \times k)$ — случайная невырожденная матрица; $\mathbf{G}(k \times n)$ — порождающая матрица кода Гоппы; $\mathbf{P}(n \times n)$ — случайная перестановочная матрица; $\hat{\mathbf{G}}(k \times n)$ — произведение матриц $\mathbf{S} \times \mathbf{G} \times \mathbf{P}$; $\mathbf{T}(mt \times k)$ — матрица-открытый ключ для системы «Classic McEliece»; $\mathbf{s}(n)$ — случайная строка длины n; $\mathbf{L}(n)$ — множество локаторов для кода Гоппы; $\mathbf{H}'(m_{RS} \times (n_{RS} - k_{RS}) \times \lambda n_{RS}) \times [\log_2 q]$ — матрица-открытый ключ для системы XGRS; $\mathbf{H}((n_{RS} - k_{RS}) \times n_{RS}) \times [\log_2 q^{m_{RS}}]$ — порождающая матрица для расширенного кода Рида–Соломона; $\mathbf{Q}(n_{RS}\lambda \times n_{RS}\lambda) \times [\log_2 q]$ — матрица-секретный ключ для криптосистемы XGRS; γ — примитивный элемент поля F_{q^m}.

Из полученных результатов (табл. 1) видно, что оптимальным решением с точки зрения памяти является криптосистема XGRS на расширенных кодах Рида–Соломона. Однако, из-за наличия выявленных в настоящей работе проблем устойчивости криптосистемы XGRS к атаке по информационным совокупностям, использовать ее не рекомендуется. Из рассмотренных систем наиболее приближенная к оптимальной для использования – криптосистема «Classic McEliece».

Моделирование криптосистем

Для моделирования рассмотренных криптосистем разработаны программы на языке программирования Python с использованием программного обеспечения SAGE на персональном компьютере со следующими характеристиками: процессор Intel Core i5-8300H CPU 2.30 GHz, оперативная память 8 GB 2667 MHz.

Для каждой криптосистемы проведено измерение значения времени выполнения процессов генерации ключей *tGen*, шифрования *tEnc* и расшифрования *tDec*. Для криптосистем Мак-Элиса и «Classic McEliece» использован алгоритм декодирования Паттерсона [29], для криптосистемы XGRS — алгоритм декодирования Берлекэмпа–Месси [30].

Входные параметры для моделирования криптосистем: n — длина кода, k — длина кодируемого сообщения, t — количество исправляемых ошибок.

Заметим, что при моделировании криптосистемы XGRS на обобщенных кодах Рида–Соломона исполь-

Таблица 1. Оценка размеров ключей криптосистем

Table 1. Cryptosystems key sizes estimation

Криптосистема	Вид ключа		Размер открытого ключа, бит	Размер секретного ключа, бит	Приблизительный общий размер ключей, МБ
	Открытый	Секретный			
Оригинальная система Мак-Элиса	$\hat{\mathbf{G}}(k \times n)$ t	$\mathbf{S}(k \times k)$ $\mathbf{G}(k \times n)$ $\mathbf{P}(n \times n)$	$3{,}77 \cdot 10^7$	$1{,}15 \cdot 10^8$	18
«Classic McEliece»	$\mathbf{T}(mt \times k)$	$\mathbf{s}(n)$ $\mathbf{G}(k \times n)$ $\mathbf{L}(n)$	$8{,}37 \cdot 10^6$	$3{,}77 \cdot 10^7$	5,5
XGRS на расширенных кодах Рида–Соломона	$\mathbf{H}'(m_{RS}(n_{RS} - k_{RS}) \times \times \lambda n_{RS}) \times \lceil \log_2 q \rceil$ t_{RS} λ	$\mathbf{H}((n_{RS} - k_{RS}) \times \times n_{RS}) \times \lceil \log_2 q^{m_{RS}} \rceil$ $\mathbf{Q}(n_{RS}\lambda \times n_{RS}\lambda) \times \times \lceil \log_2 q \rceil$ γ	$6{,}85 \cdot 10^6$	$2{,}87 \cdot 10^7$	4,2

Таблица 2. Экспериментальные значения исследуемых параметров рассмотренных криптосистем
Table 2. Experimental values of the studied parameters of the considered cryptosystems

Параметры								
q	*n*	*k*	*t*	*m*	λ	*tGen*, отн. ед.	*tEnc*, отн. ед.	*tDec*, отн. ед.
Оригинальной криптосистемы Мак-Элиса								
—	2304	1280	64	—	—	1	0,00026	0,347
—	3584	1536	128	—	—	2,06	0,00026	0,784
—	4096	2048	128	—	—	3,73	0,00026	1,390
—	6912	2816	256	—	—	3,94	0,00035	4,070
Криптосистемы «Classic McEliece»								
—	2304	1280	64	—	—	12,07	0,066	0,790
—	3584	1536	128	—	—	49,71	0,214	2,523
—	4096	2048	128	—	—	67,11	0,237	3,091
—	6912	2816	256	—	—	484,07	0,842	12,301
Криптосистемы XGRS на обобщенных кодах Рида–Соломона								
13	1258	1031	113	3	2	17,24	0,00023	20,470
13	1382	829	276	3	2	38,21	0,00065	25,390
7	1770	1539	115	4	2	36,94	0,00051	55,570
7	2024	1841	91	4	2	38,40	0,00034	87,750

зованы следующие дополнительные параметры: q — характеристика поля, m — расширение поля, λ — коэффициент сокращения.

Результаты моделирования представлены в табл. 2.

Для оценки параметров целесообразно использовать относительные единицы, так как на устройствах с разными мощностями возможен большой разброс полученных результатов. Примем за относительную единицу по времени время генерации ключей для оригинальной системы Мак-Элиса с параметрами $n = 2304$, $k = 1280$, $t = 64$.

Как видно из представленных результатов, наиболее трудозатратной операцией в большинстве случаев является генерация ключей.

В криптосистеме «Classic McEliece» время генерации увеличивается по сравнению с оригинальной системой из-за расширения проверочной матрицы кода и последующего ее приведения к систематическому виду.

При рассмотрении криптосистемы XGRS на обобщенных кодах Рида–Соломона наиболее трудозатратной операцией является расшифрование, поскольку применяется отличный от предыдущих систем алгоритм расшифрования из-за использования другого класса кодов.

Заключение

В работе выполнен обзор оригинальных криптосистем Мак-Элиса и Нидеррайтера и их современных модификаций. Рассмотрены пять различных криптосистем, для трех из которых было проведено моделирование. Продемонстрировано, что попытки улучшения кодовых схем с открытым ключом путем использования других классов кодов (не двоичных кодов Гоппы) и снятия ограничений на вес вектора ошибки не увенчались успехом. Получены важные теоретические и практические результаты. В рассмотренной криптосистеме XGRS было выявлено несоответствие реального уровня безопасности к атаке по информационным совокупностям заявленному авторами, что делает ее неприменимой с учетом современных реалий, а также отмечены неточности при подсчете размеров ключей. Сравнительный анализ представленных криптосистем показал, что криптосистема «Classic McEliece» на сегодняшний день является наиболее приближенной к оптимальному решению по уровню безопасности и производительности среди рассмотренных в работе криптосистем. Оценка результатов моделирования трех представленных криптосистем показала, что, помимо больших размеров ключей, процессы генерации ключа и декодирования на компьютере со средними характеристиками занимают достаточно большое время — их уменьшение остается на сегодняшний момент актуальной задачей для дальнейших исследований.

Литература

1. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proc. of the 35th IEEE Annual Symposium on Foundations of Computer Science (FOCS). 1994. P. 124–134. https://doi.org/10.1109/SFCS.1994.365700
2. McEliece R.J. A public-key cryptosystem based on algebraic coding theory // DSN Progress Report 42-44, 1978. P. 114–116.
3. Гоппа В.Д. Рациональное представление кодов и (L,g)-коды // Проблемы передачи информации. 1971. Т. 7. № 3. С. 41–49.
4. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problems of Control and Information Theory. 1986. V. 15. N 2. P. 159–166.
5. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. М.: Связь, 1979. С. 506–507.
6. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида–Соломона // Дискретная математика. 1992. Т. 4. № 3. С. 57–63.
7. Peters C. Information-set decoding for linear codes over Fq // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2010. V. 6061. P. 81–94. https://doi.org/10.1007/978-3-642-12929-2_7
8. Sidelnikov V.M. A public-key cryptosystem based on binary Reed-Muller codes // Discrete Mathematics and Applications. 1994. V. 4. N 3. P. 191–207. https://doi.org/10.1515/dma.1994.4.3.191
9. Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov cryptosystem // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2007. V. 4515. P. 347–360. https://doi.org/10.1007/978-3-540-72540-4_20
10. Gabidulin E.M. Public-key cryptosystems based on linear codes: Report 95-30 / Delft University of Technology, Faculty of Technical Mathematics and Informatics, 1995. P. 17–31.
11. Overbeck R. Structural attacks for public key cryptosystems based on Gabidulin codes // Journal of Cryptology. 2008. V. 21. N 2. P. 280–301. https://doi.org/10.1007/s00145-007-9003-9
12. Baldi M., Chiaraluce F. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes // Proc. of the IEEE International Symposium on Information Theory (ISIT). 2007. P. 2591–2595. https://doi.org/10.1109/ISIT.2007.4557609
13. Otmani A., Tillich J.P., Dallot L. Cryptanalysis of McEliece cryptosystem based on quasi-cyclic LDPC codes // Proc. of the First International Conference on Symbolic Computation and Cryptography. LMIB Beihang University, 2008. P. 69–81.
14. Janwa H., Moreno O. McEliece public key cryptosystems using algebraic-geometric codes // Designs, Codes and Cryptography. 1996. V. 8. N 3. P. 293–307. https://doi.org/10.1023/A:1027351723034
15. Faure C., Minder L. Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes // Proc. of the 11th International Workshop on Algebraic and Combinatorial Coding Theory. 2008. P. 99–107.
16. Loidreau P. Strengthening McEliece cryptosystem // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2000. V. 1976. P. 585–598. https://doi.org/10.1007/3-540-44448-3_45
17. Kobara K., Imai H. On the one-wayness against chosen-plaintext attacks of the Loidreau's modified McEliece PKC // IEEE Transactions on Information Theory. 2003. V. 49. N 12. P. 3160–3168. https://doi.org/10.1109/TIT.2003.820016
18. Bernstein D.J., Lange T., Peters C. Attacking and defending the McEliece cryptosystem // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2008. V. 5299. P. 31–46. https://doi.org/10.1007/978-3-540-88403-3_3
19. Bernstein D.J. et al. Classic McEliece: conservative code-based cryptography / NIST. 2017.
20. Khathuria K., Rosenthal J., Weger V. Encryption scheme based on expanded reed-solomon codes // Advances in Mathematics of Communications. 2021. V. 15. N 2. P. 207–218. https://doi.org/10.3934/amc.2020053
21. Reed I.S., Solomon G. Polynomial codes over certain finite fields // Journal of the Society for Industrial and Applied Mathematics. 1960. V. 8. N 2. P. 300–304. https://doi.org/10.1137/0108018
22. Ivanov F., Kabatiansky G., Krouk E., Rumenko N. A new code-based cryptosystem // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes

References

1. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring. *Proc. of the 35th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, 1994, pp. 124–134. https://doi.org/10.1109/SFCS.1994.365700
2. McEliece R.J. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report 42–44*, 1978, pp. 114–116.
3. Goppa V.D. A Rational Representation of Codes and (L,g)-Codes. *Problems Information Transmission*, 1971, vol. 7, no.3. pp. 223–229.
4. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 1986, vol. 15, no. 2, pp. 159–166.
5. Mac Williams F.J., Sloane N.J.A. *The theory of Error-Correcting Codes*. Amsterdam, 1977.
6. Sidel'nikov V.M., Shestakov S.O. On an encoding system constructed on the basis of generalized Reed–Solomon codes. *Discrete Mathematics and Applications*, 1992, vol. 2, no. 4, pp. 439–444.
7. Peters C. Information-set decoding for linear codes over Fq. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6061, pp. 81–94. https://doi.org/10.1007/978-3-642-12929-2_7
8. Sidelnikov V.M. A public-key cryptosystem based on binary Reed-Muller codes. *Discrete Mathematics and Applications*, 1994, vol. 4, no. 3, pp. 191–207. https://doi.org/10.1515/dma.1994.4.3.191
9. Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov cryptosystem. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2007, vol. 4515, pp. 347–360. https://doi.org/10.1007/978-3-540-72540-4_20
10. Gabidulin E.M. Public-key cryptosystems based on linear codes. Report 95-30. *Delft University of Technology, Faculty of Technical Mathematics and Informatics*, 1995, pp. 17–31.
11. Overbeck R. Structural attacks for public key cryptosystems based on Gabidulin codes. *Journal of Cryptology*, 2008, vol. 21, no. 2, pp. 280–301. https://doi.org/10.1007/s00145-007-9003-9
12. Baldi M., Chiaraluce F. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. *Proc. of the IEEE International Symposium on Information Theory (ISIT)*, 2007, pp. 2591–2595. https://doi.org/10.1109/ISIT.2007.4557609
13. Otmani A., Tillich J.P., Dallot L. Cryptanalysis of McEliece cryptosystem based on quasi-cyclic LDPC codes. *Proc. of the First International Conference on Symbolic Computation and Cryptography*. LMIB Beihang University, 2008, pp. 69–81.
14. Janwa H., Moreno O. McEliece public key cryptosystems using algebraic-geometric codes. *Designs, Codes and Cryptography*, 1996, vol. 8, no. 3, pp. 293–307. https://doi.org/10.1023/A:1027351723034
15. Faure C., Minder L. Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes. *Proc. of the 11th International Workshop on Algebraic and Combinatorial Coding Theory*, 2008, P. 99–107.
16. Loidreau P. Strengthening McEliece cryptosystem. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2000, vol. 1976, pp. 585–598. https://doi.org/10.1007/3-540-44448-3_45
17. Kobara K., Imai H. On the one-wayness against chosen-plaintext attacks of the Loidreau's modified McEliece PKC. *IEEE Transactions on Information Theory*, 2003, vol. 49, no. 12, pp. 3160–3168. https://doi.org/10.1109/TIT.2003.820016
18. Bernstein D.J., Lange T., Peters C. Attacking and defending the McEliece cryptosystem. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2008, vol. 5299, pp. 31–46. https://doi.org/10.1007/978-3-540-88403-3_3
19. Bernstein D.J. et al. *Classic McEliece: conservative code-based cryptography*. NIST, 2017.
20. Khathuria K., Rosenthal J., Weger V. Encryption scheme based on expanded reed-solomon codes. *Advances in Mathematics of Communications*, 2021, vol. 15, no. 2, pp. 207–218. https://doi.org/10.3934/amc.2020053
21. Reed I.S., Solomon G. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 1960, vol. 8, no. 2, pp. 300–304. https://doi.org/10.1137/0108018
22. Ivanov F., Kabatiansky G., Krouk E., Rumenko N. A new code-based cryptosystem. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes*

in Bioinformatics). 2020. V. 12087. P. 41–49. https://doi.org/10.1007/978-3-030-54074-6_3
23. Berlekamp E., McEliece R., Van Tilborg H. On the inherent intractability of certain coding problems (corresp.) // IEEE Transactions on Information Theory. 1978. V. 24. N 3. P. 384–386. https://doi.org/10.1109/TIT.1978.1055873
24. Augot D., Finiasz M., Sendrier N. A family of fast syndrome based cryptographic hash functions // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2005. V. 3715. P. 64–83. https://doi.org/10.1007/11554868_6
25. Azouaoui A., Chana I., Belkasmi M. Efficient information set decoding based on genetic algorithms // International Journal of Communications, Network and System Sciences. 2012. V. 5. N 7. P. 423–429. https://doi.org/10.4236/ijcns.2012.57052
26. Gauthier V., Otmani A., Tillich J.P. A Distinguisher-based attack on a variant of McEliece's cryptosystem based on Reed-Solomon codes // arXiv.org. 2012. arXiv:1204.6459. https://doi.org/10.48550/arXiv.1204.6459
27. Torres R.C., Sendrier N. Analysis of information set decoding for a sub-linear error weight // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2016. V. 9606. P. 144–161. https://doi.org/10.1007/978-3-319-29360-8_10
28. Lee Y., Cho J., Kim Y.-S., No J.-S. Cryptanalysis of the Ivanov-Kabatiansky-Krouk-Rumenko cryptosystems // IEEE Communications Letters. 2020. V. 24. N 12. P. 2678–2681. https://doi.org/10.1109/LCOMM.2020.3019054
29. Patterson N. The algebraic decoding of Goppa codes // IEEE Transactions on Information Theory. 1975. V. 21. N 2. P. 203–207. https://doi.org/10.1109/TIT.1975.1055350
30. Berlekamp E.R. Non-binary BCH decoding. North Carolina State University. Dept. of Statistics, 1966.

in Bioinformatics), 2020, vol. 12087, pp. 41–49. https://doi.org/10.1007/978-3-030-54074-6_3
23. Berlekamp E., McEliece R., Van Tilborg H. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory*, 1978, vol. 24, no. 3, pp. 384–386. https://doi.org/10.1109/TIT.1978.1055873
24. Augot D., Finiasz M., Sendrier N. A family of fast syndrome based cryptographic hash functions. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2005, vol. 3715, pp. 64–83. https://doi.org/10.1007/11554868_6
25. Azouaoui A., Chana I., Belkasmi M. Efficient information set decoding based on genetic algorithms. *International Journal of Communications, Network and System Sciences*, 2012, vol. 5, no. 7, pp. 423–429. https://doi.org/10.4236/ijcns.2012.57052
26. Gauthier V., Otmani A., Tillich J.P. A Distinguisher-based attack on a variant of McEliece's cryptosystem based on Reed-Solomon codes. *arXiv.org*, 2012, arXiv:1204.6459. https://doi.org/10.48550/arXiv.1204.6459
27. Torres R.C., Sendrier N. Analysis of information set decoding for a sub-linear error weight. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, vol. 9606, pp. 144–161. https://doi.org/10.1007/978-3-319-29360-8_10
28. Lee Y., Cho J., Kim Y.-S., No J.-S. Cryptanalysis of the Ivanov-Kabatiansky-Krouk-Rumenko cryptosystems. *IEEE Communications Letters*, 2020, vol. 24, no. 12, pp. 2678–2681. https://doi.org/10.1109/LCOMM.2020.3019054
29. Patterson N. The algebraic decoding of Goppa codes. *IEEE Transactions on Information Theory*, 1975, vol. 21, no. 2, pp. 203–207. https://doi.org/10.1109/TIT.1975.1055350
30. Berlekamp E.R. *Non-binary BCH decoding*. North Carolina State University. Dept. of Statistics, 1966.

Авторы

Давыдов Вадим Валерьевич — преподаватель, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57203909696, https://orcid.org/0000-0002-5544-2434, vvdavydov@itmo.ru
Беляев Владислав Владиславович — лаборант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57217737570, https://orcid.org/0000-0002-1067-7483, v.beliaev@niuitmo.ru
Кустов Елизар Филаретович – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0002-0191-1178, efkustov@itmo.ru
Леевик Антон Георгиевич — инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57219714571, https://orcid.org/0000-0003-1823-7877, agleevik@niuitmo.ru
Беззатеев Сергей Валентинович — доктор технических наук, доцент, профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация; заведующий кафедрой, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация, SC 6602425996, https://orcid.org/0000-0002-0924-6221, bsv@aanet.ru

Authors

Vadim V. Davydov — Lecturer, ITMO University, 197101, Saint Petersburg, Russian Federation, SC 57203909696, https://orcid.org/0000-0002-5544-2434, vvdavydov@itmo.ru
Vladislav V. Beliaev — Laboratory Assistant, ITMO University, 197101, Saint Petersburg, Russian Federation, SC 57217737570, https://orcid.org/0000-0002-1067-7483, v.beliaev@niuitmo.ru

Elizar F. Kustov – PhD Student, ITMO University, 197101, Saint Petersburg, Russian Federation, https://orcid.org/0000-0002-0191-1178, efkustov@itmo.ru
Anton G. Leevik — Engineer, ITMO University, 197101, Saint Petersburg, Russian Federation, SC 57219714571, https://orcid.org/0000-0003-1823-7877, agleevik@niuitmo.ru
Sergey V. Bezzateev — D. Sc., Full Professor, Associate Professor, ITMO University, 197101, Saint Petersburg, Russian Federation; Saint-Petersburg State University of Aerospace Instrumentation, Head of department, 190000, Saint Petersburg, Russian Federation, SC 6602425996, https://orcid.org/0000-0002-0924-6221, bsv@aanet.ru

Статья поступила в редакцию 12.02.2022
Одобрена после рецензирования 05.03.2022
Принята к печати 31.03.2022

Received 12.02.2022
Approved after reviewing 05.03.2022
Accepted 31.03.2022