Научная статья
Original article
УДК 004.453.2

КОДЫ QC-MDPC КАК ПОПЫТКА РЕШИТЬ ПРОБЛЕМУ ДЛИНЫ КЛЮЧА В КРИПТОСИСТЕМЕ МАК-ЭЛИСА

QC-MDPC CODES AS AN ATTEMPT TO SOLVE THE KEY LENGTH PROBLEM IN THE MC-ELIECE CRYPTOSYSTEM

Баев Дмитрий Александрович, Студент кафедры кибербезопасности информационных систем, ФГБОУ ВО «Донской государственный технический университет» (344003, ЮФО, Ростовская область, г.Ростов-на-Дону, пл. Гагарина, 1), тел. 8(968) 275-35-64, fantom-sj@yandex.ru

Dmitry A. Baev, Student of the Department of Cybersecurity of Information Systems, Federal State Budgetary Educational Institution of Higher Education "Don State Technical University" (344003, Southern Federal District, Rostov Region, Rostov-on-Don, Gagarina Square, 1), tel. 8 (968) 275-35-64, fantom-sj@yandex.ru

Аннотация. Данная статья рассматривает один из способов решения проблемы длины ключа в оригинальной криптосистеме Мак-Элиса, основанной на кодах Гоппа. В качестве её решения предлагается использование кодов более высокой плотности проверки на чётность QC-MDPC. В статье раскрывается понятие кодов QC-MDPC, а также приводится алгоритм построения порождающей и проверочной матриц данного семейства кодов. Помимо этого, были определены параметры криптосистемы Мак-Элиса с использованием кодов QC-MDPC для различных уровней защиты, а также был проведён сравнительный

анализ размеров ключа при их использовании по сравнению с кодами Гоппа. Также был описан алгоритм декодирования и его особенности, а также приведены необходимые изменения в алгоритм Мак-Элиса для внедрения данного семейства кодов.

Annotation. This article discusses one of the ways to solve the key length problem in the original McEliece cryptosystem based on Gopp codes. As a solution, it is proposed to use higher density parity codes QC-MDPC. The article reveals the concept of QC-MDPC codes, and also provides an algorithm for constructing the generating and parity matrices of this family of codes. In addition, the parameters of the McEliece cryptosystem were determined using the QC-MDPC codes for different levels of protection, and a comparative analysis of the key sizes when using them in comparison with the Gopp codes was carried out. The decoding algorithm and its features were also described, as well as the necessary changes to the McEliece algorithm for the introduction of this family of codes.

Ключевые слова: криптография, постквантовая криптография, асимметричная криптография, криптосистема Мак-Элиса, коды LDPC, коды QC-MDPC.

Keywords: cryptography, post-quantum cryptography, asymmetric cryptography, McEliece cryptosystem, LDPC codes, QC-MDPC codes.

Введение

Оригинальная реализация криптосистемы Мак-Элиса подразумевает использование кода Гоппа длиной n = 1024, размерностью k = 524 и минимальным кодовым расстоянием d не менее 101, которые могут исправить t = 50 ошибок. Однако его применение в реализации данной криптосистемы порождает существенный недостаток, связанный с чрезмерно большим объёмом открытого ключа, что мешает её широкому распространению [1]. Тем не менее, было предпринято несколько попыток уменьшения открытого ключа в исходной системе для устранения её недостатков, но принятие альтернативных семейств

кодов оказалось невозможным без ущерба для безопасности криптосистемы в целом [2].

Одной из таких попыток стало использование кодов проверки на четность с низкой плотностью или LDPC кодов [3]. Использование данного семейства кодов решает проблему длины открытого ключа, позволяя значительно её сократить. Также с применением данных кодов можно значительно ускорить процесс декодирования, так как коды LDPC обладают хорошей масштабируемостью в аппаратных реализациях, так как у них намного проще алгоритмы декодирования. Тем не менее, использование кодов LDPC в криптосистеме Мак-Элиса не считается таким же безопасным, как использование кодов Гоппа в оригинальной реализации [3].

Дальнейшее развитие данной идеи заключается в реализации криптосистемы Мак-Элиса на более компактных, но при этом достаточно безопасных кодах, которые основаны на кодах LDPC.

В работе [4] были предложены коды LDPC более высокой плотности, а именно квазициклические коды более высокой плотности проверки на чётность (QC-MDPC коды), которые обеспечивают быструю проверку на четность, а также позволяют с их помощью реализовывать эффективные криптосистемы, основанные на корректирующих кодах. При этом сохраняется полное число исправляемых ошибок, при значительном уменьшении открытого ключа, необходимого для осуществления криптографических преобразований.

Ход исследования

Коды QC-MDPC представляют из себя квазициклическую форму кодов MDPC, что показывается приставкой QC в их названии. При этом коды MDPC – это линейные коды длины n и размерности r, который допускает проверочную матрицу H принадлежащую полю $\mathbb{F}_2^{n\times r}$ с постоянным весом строки w [4].

Квазициклические коды – это линейный код с параметрами (n, r), такой, что существует целое число n_0, что каждый циклический сдвиг кодового слова на n_0 позиций порождает новое кодовое слово [5].

Тогда квазициклическим кодом MDPC называется код с параметром циклического сдвига n_0, размерности r, и длины $n = n_0 \cdot r$, при этом имеющий проверочную матрицу H с весом каждой строки равной w и имеющий вид [4]:

$$H = [H_0|H_1|\dots|H_{n_0-1}]$$

где H_i – это циркулянтный блок размера $r \times r$.

При этом для построения каждого циркулянтного блока матрицы H достаточно сгенерировать случайным образом первую стоку блока длиной в n бит, после чего все остальные $r - 1$ строк данного блока будут получены путём квазициклических сдвигов первой строки. При этом каждая строка будет иметь вес w рассчитывающийся по следующей формуле [4]:

$$w = \sum_{1}^{n_0} wi$$

Порождающая матрица кода G представляет собой структуру, построенную на основе блоков H_i матрицы H. При этом учитывая, что крайний правый блок H_{n_0-1} является невырожденным то, матрица G имеет следующий вид [4]:

$$G = \left[\begin{array}{c|c} I & \begin{matrix} \left(H_{n_0-1}^{-1} \cdot H_0\right)^T \\ \left(H_{n_0-1}^{-1} \cdot H_1\right)^T \\ \vdots \\ \left(H_{n_0-1}^{-1} \cdot H_{n_0-2}\right)^T \end{matrix} \end{array}\right]$$

где I – это единичная матрица размера $r \times r$.

Особенностью кодов QC-MDPC является тот факт, что декодирование данного класса кодов носит вероятностный характер отказоустойчивости [4]. Это означает, что алгоритм декодирования кодов QC-MDPC способен эффективно декодировать очередное кодовое слово с исправлением допущенных в нём ошибок с вероятностью < 1, что является недопустимым в криптографии, так как приводит к потере зашифрованной информации.

При этом для того, чтобы максимально снизить вероятность отказа при декодировании следует использовать такой декодер кодов QC-MDPC, который гарантирует отказ с вероятность не более 10^{-7} [6].

При этом, как отправитель сообщения, так и его получатель заранее знают параметры того кода, который будет использован в процессе шифрования. К таким параметрам относятся:

– r – длина исходного информационного вектора;

– n – длина кодового слова;

– t – количество ошибок, которые способен исправить данный код.

Помимо этого, получатель зашифрованной информации также знает некоторые параметры, которые относятся к используемому коду QC-MDPC, а именно:

– n_0 – циклический сдвиг для выбранного кода QC-MDPC;

– w – вес кодовых слов в проверочной матрице H.

Комбинация всех вышеперечисленных параметров позволяет задать определённый уровень защиты для выстраиваемой криптосистемы Мак-Элиса, который соответствовал бы уровню защиты аналогичных классических криптосистем с открытым ключом.

Так в работе [6] были предложены параметры для криптосистемы на основе QC-MDPC кодов, определённые в таблице 1.

Таблица 1. Параметры для построения криптосистемы Мак-Элиса

Уровень защиты	n_0	n	r	w	t	Размер ключа
80 бит	2	9600	4800	90	84	4800 бит
	3	10752	3584	153	53	7168 бит
	4	12288	3072	220	42	9216 бит

Продолжение таблице 1:

128 бит	2	19712	9856	142	134	9856 бит
	3	22272	7424	243	85	14848 бит
	4	27200	6800	340	68	20400 бит

256 бит	2	65536	32768	274	264	32768 бит
	3	67584	22528	465	167	45056 бит
	4	81920	20480	644	137	61440 бит

Учитывая размеры ключей для криптосистемы Мак-Элиса при использовании кодов Гоппа представленных в работе [7], проведём сравнение минимальных размеров ключа для каждого уровня защиты в криптосистеме Мак-Элиса на основе кодов Гоппа и кодов QC-MDPC. Результаты данного сравнения, представленные в таблице 2.

Таблица 2. Сравнения размеров ключей

Уровень защиты	QC-MDPC	Коды Гоппа
80 бит	4800 бит	460647 бит
128 бит	9856 бит	1537536 бит
256 бит	32768 бит	7667855 бит

Как можно заметить коды QC-MDPC дают значительно меньшие размеры открытого ключа, что делает их более привлекательными для реализации криптосистемы Мак-Элиса.

Как и многие другие линейные алгебраические коды, коды QC-MDPC кодируются достаточно просто, посредством умножение кодируемого вектора на порождающую матрицу кода. При этом процесс декодирования закодированного вектора является довольной сложной задачей и требует более одного шага для его осуществления [8]. Также процесс декодирования подвержен сбоям, что требует альтернативных путей его осуществления для успешного достижения результата декодирования.

В связи с этим, в алгоритме декодирования предлагается использовать сразу 3 метода нахождения очередного элемента, содержащего ошибку, внесённую в процессе шифрования. При этом алгоритм декодирования очередного кодового слова имеет следующий вид [9]:

1. Вычисление синдрома S для полученного кодового слова;

2. Вычисление веса синдрома S (количество не нулевых элементов в нём);
3. Вычисление значения изменения количества ошибок в синдроме, и далее определение в какой числовой промежуток попадает данное значение;
4. Определение порогового значения ошибки на основе её порога;
5. Выбор набольшего порогового значение между половиной веса для кода QC-MDPC и вычисленным пороговым значением на предыдущем этапе;
6. На основе вычисленного порогового значения, а также проверочной матрицы H и производится семплирование синдрома ошибок для нахождения ошибки в закодированном блоке;
7. Исправление найденной ошибки;
8. До тех пор, пока вес синдрома S больше 0 и не пройдено N итераций повторяем предыдущие 7 шагов.

После завершения процесса декодирования продолжается классический алгоритм расшифровывания зашифрованного блока в криптосистеме Мак-Элиса.

Отдельно стоит упомянуть процесс семплирования синдрома ошибки. Данный процесс заключается в нахождении позиции ошибки в кодовом слове на основе синдрома ошибок, как и для многих других алгебраических кодов [10]. Тем не менее данный процесс значительно отличается и для того чтобы определить в какой позиции кодового слова находится ошибка применятся один из трёх методов её поиска [11]:

Метод 1: Выбрать случайным образом среди возможных позиций ошибки, такую позицию для которого $\Sigma_j \geq T$, где Σ это вектор, вычисляемы следующим образом:

$$\Sigma = S \cdot H$$

Метод 2: Выбираем случайным образом неудовлетворённое уравнение, затем выбираем ненулевой бит этого уравнения циклически, до тех пор, пока j указывает на ненулевой бит, найденный исходя из $\Sigma_j \geq T$.

Метод 3: В качестве искомой позиции ошибки *j* возвращаем индекс максимального элемента в векторе Σ, при этом если найдено несколько индексов с максимальными одинаковыми значениям, то возвращаем любой из них.

Таким образом наличия трёх методов повышает вероятность нахождения позиции очередной ошибки в кодовом слове. Тем не менее каждый из предложенных методов может завершиться, не найдя ни одного подходящего под заданные условия элемента *j*.

Вывод

Реализация криптосистемы Мак-Элиса с применением компактных кодов QC-MDPC позволила достичь значительного уменьшения размера открытого ключа, при этом увеличив скорость работы алгоритма за счёт уменьшения необходимых вычислительных операций, при этом сохранив криптографическую стойкость данного алгоритма, что в конечном итоге позволяет решить одну из проблем, связанных с внедрением данной криптосистемы для повсеместного использования с целью замены существующих криптосистем с открытым ключом таких как RSA, подверженных атакам на квантовых вычисленных системах.

Так же использование разных алгоритмов при декодировании кодов данного класса, позволяет добиться значительного повышения вероятности успешного расшифровывания сообщения. Тем не менее вероятностный характер успешного декодирования кодов QC-MDPC не позволяет применять их на практике, что делает актуальным вопрос поиска алгоритма однозначного декодирования для кодов данного семейства.

Литература:

1. Баев, Д. А. Криптосистема Мак-Элиса и проблемы её внедрения / Д. А. Баев // StudNet. – 2021. – Т. 4. – № 3. – с. 71;
2. Бисвас Б. Внедрение криптосистемы Мак-Элиса: теория и практика / Б. Бисвас, Н. Сендриер // Исследовательский центр INRIA, Париж, Франция, PQCrypto, – 2008, – LNCS 5299, – с. 47-62;

3. Бранко П. Информационные науки / П. Бранко, П. Матеус, К. Салема, А. Соуто // – том 510, – 2020 г., – с. 243-255;
4. Мисоци Р. MDPC-МакЭлис: новые варианты Мак-Элиса из кодов проверки на четность средней плотности / Р. Мисоци, Дж. Тиллих, Н. Сендриер // Международный симпозиум IEEE по теории информации (ISIT2013), – Стамбул, – 2013, – с. 2069-2073;
5. Фуке П.А. Криптоанализ хеш-функции на основе квазициклических кодов / П.А. Фуке, Г. Лярент // – CT-RSA, – 2008, – т. 4964 – LNCS, – Springer, – с. 19–35;
6. Хейз С. Маленькие ключи для криптографии на основе кодов: реализация QC-MDPC Мак-Элиса на встроенных устройствах / С. Хейз, И. Маурих, Т. Гюнесу // – 2013, – с. 273-292, DOI: 10.1007 / 978-3-642-40349-1_16;
7. Бернштейн Д. Атака и защита криптосистемы Мак-Элиса / Д. Бернштейн, Дж. Бернштейн, Т. Ланге // материалы 2-го Международного семинара по постквантовой криптографии, – PQCrypto 2008, – Берлин, Гейдельберг, – Springer Verlag, – с 31-46;
8. Ромащенко А.Е. Заметки по теории кодирования. / А.Е. Ромащенко, А.Ю. Румянцев, А. Шень // 2-е изд., испр. и доп. М.: МЦНМО, – 2017. – 88 с.;
9. Ханада М. Цепь Маркова Монте-Карло для чайников / М. Ханада // – 2018, – 65 с.;
10. Деундяк В.М. Методы помехоустойчивой защиты данных: учебник / В.М. Деундяк, А.Э Маевский, Н.С. Могилевская // – Ростов н/Д: Издательство Южного федерального университета, – 2014. – 309 с.;
11. Асие А. Решение разреженных линейных систем уравнений над конечными полями с использованием алгоритма переворота битов / А. Асие, М. Садеги, Д. Панарио // Линейная алгебра и ее приложения, – 2013, – с. 1815-1824.

References

1. Baev, D.A. McEliece's cryptosystem and the problems of its implementation / D.A. Baev // StudNet. - 2021. - T. 4. - No. 3. - P. 71;
2. Bhaskar Biswas, Nicolas Sendrier. McEliece Cryptosystem Implementation: Theory and Practice., Centre de recherche INRIA Paris, France, PQCrypto 2008, LNCS 5299, pp. 47-62, 2008;
3. Pedro Branco, Paulo Mateus, Carlos Salema, Andre Souto., Information Sciences, Volume 510, February 2020, Pages 243-255;
4. Misoczki R. MDPC-McEliece: new McEliece variants from moderate density parity-check codes / R. Misoczki, J. Tillich, N. Sendrier // IEEE International Symposium on Information Theory (ISIT2013), – Istanbul, – 2013, – P. 2069-2073;
5. Fouque P.A. Cryptanalysis of a hash function based on quasi-cyclic codes / P.A. Fouque, G. Leurent // CT-RSA, – 2008, – vol. 4964 of LNCS, – Springer, – 2008, – P 19–35;
6. Heyse S. Smaller Keys for Code-Based Cryptography: QC-MDPC McEliece Implementations on Embedded Devices / S. Heyse, I. Maurich, T. Güneysu, – 2013, – m. 08, – P. 273-292, DOI: 10.1007/978-3-642-40349-1_16;
7. Bernstein D. Attacking and defending the McEliece cryptosystem / D. Bernstein, J. Bernstein, T. Lange // In Proceedings of the 2nd International Workshop on Post-Quantum Cryptography, – PQCrypto 2008, – Berlin, Heidelberg, – 2008, Springer Verlag, – P 31-46;
8. Romashchenko A.E. Notes on coding theory. / A.E. Romashchenko, A. Yu. Rumyantsev, A. Shen // 2nd ed., Rev. and add. M.: MTsNMO, 2017.88 p.;
9. Hanada M. Markov Chain Monte Carlo for Dummies / M. Hanada, – 2018, 65 p.;
10. Deundyak V.M. Anti-jamming data protection methods: textbook / V.M. Deundyak, A.E. Maevsky, N.S. Mogilevskaya. - Rostov n / a: Publishing house of the Southern Federal University, 2014. - 309 p .;

11. Asieh A. Solving sparse linear systems of equations over finite fields using bit-flipping algorithm / A. Asieh, M. Sadeghi, D. Panario // Linear Algebra and its Applications, – 2013, P. 1815-1824.

© Баев Д.А., 2021 Научно-образовательный журнал для студентов и преподавателей «StudNet» №9/2021.

Для цитирования: Баев Д.А. КОДЫ QC-MDPC КАК ПОПЫТКА РЕШИТЬ ПРОБЛЕМУ ДЛИНЫ КЛЮЧА В КРИПТОСИСТЕМЕ МАК-ЭЛИСА // образовательный журнал для студентов и преподавателей «StudNet» №9/2021.