ISSN 2658 – 7505
Выпуск №4, 2019
Электронный научный журнал «Вестник молодёжной науки России»

УДК 621.391.7

СПОСОБ МОДИФИКАЦИИ КРИПТОСИСТЕМЫ МАК-ЭЛИСА ДЛЯ ОБЕСПЕЧЕНИЯ СЕМАНТИЧЕСКОЙ СТОЙКОСТИ

Ю.В. Косолапов, *itaim@mail.ru*, ***О.Ю. Турченко,*** *olegmmcs@gmail.com,*
Южный Федеральный университет, г. Ростов-на-Дону

В связи с развитием квантовых вычислений актуальной является задача построения криптосистем с открытым ключом, не основанных на трудности решения задач дискретного логарифмирования и дискретной факторизации. Одним из возможных кандидатов является криптосистема Мак-Элиса, стойкость которой основана на трудности декодирования случайного кода. Однако, в исходном виде эта криптосистема не обладает семантической стойкостью, так как подвержена атакам на шифртекст. В настоящей работе предлагается и теоретически обосновывается способ модификации криптосистемы Мак-Элиса для обеспечения защиты от атак по подобранному открытому тексту. Построенная модификация рассматривается как основа при построении кодовой криптосистемы, устойчивой к атакам по подобранному шифртексту.

Ключевые слова: квантовые вычисления, криптосистема Мак-Элиса, защита от атак по подобранному открытому тексту.

A WAY OF SEMANTICALLY SECURE MODIFICATION OF THE MCELIECE CRYPTOSYSTEM

Y.V Kosolapov, O.Y. Turchenko
Southern Federal University, Rostov-on-Don

In connection with the development of quantum computing, an urgent task is to construct public-key cryptosystems that are not based on the integer factoring problem and the discrete logarithm problem. A possible candidate is the McEliece cryptosystem which is based on the problem of decoding a random code. However, in its original form, this cryptosystem is not semantically secure, as it is vulnerable to attacks on the ciphertext. The paper proposes and theoretically substantiates a way of modification the McEliece cryptosystem to provide indistinguishability under chosen plaintext attack. The constructed modification is considered as the basis for constructing a code cryptosystem that is indistinguishable under chosen ciphertext attack.

Keywords: quantum computing, McEliece cryptosystem, indistinguishability under chosen plaintext attack.

ВВЕДЕНИЕ

Многие криптосистемы с открытым ключом подвержены ряду атак на шифртекст: по выбранному открытому тексту, по информационным совокупностям на два сообщения, на зависимые открытые тексты, атака с контролируемым изменением открытого текста (*malleability attack*). Описание этих атак приведено в [1]. Семанически стойкие криптосистемы не подвержены большей части подобных атак. Понятие семантической стойкости было введено в [2] и означает, что шифртекст не дает противнику, при полиномиальных ограничениях на его вычислительные ресурсы, никакой информации об открытом тексте. Одним из способов построения таких криптосистем является использование недетерменированного шифрования. Так, например, М. Беллароом и П. Рогавеем [3] была предложена модификация OAEP широко используемой асимметричной криптосистемы RSA. Заметим, что стойкость используемых в настоящее время ассиметричных криптосистем основывается на задачах дискретного логарифмирования или дискретной факторизации. Данные задачи могут эффективно решаться с помощью алгоритма Шора [4] на квантовых компьютерах. Альтернативой таким криптосистемам может являться криптосистема Мак-Элиса [5], стойкость которой основана на задаче

ISSN 2658 – 7505
Выпуск №4, 2019
Электронный научный журнал «Вестник молодёжной науки России»

декодирования случайного кода. В исходном виде криптосистема Мак-Элиса не является семантически стойкой. Задача построения семантически стойкой криптосистемы типа Мак-Элиса является актуальной. В [1] построена модификация, обладающая на настоящий момент самым сильным свойством стойкости — свойством неотличимости при атаке на основе подобранного шифртекста (*IND-CCA2*). Однако, это свойство достигается только в рамках модели со случайным оракулом (*random oracle model*). Данная модель была впервые использована в [6] и означает, что участники протокола имеют доступ к некоторой теоретической функции (оракул), которая для любого уникального аргумента выдает истинно случайное значение, при этом, если аргумент повторяется, оракул повторяет соответствующий выход. В [7] построена модификация, обладающая свойством неразличимости при атаке на основе подобранного открытого текста (*IND-CPA*) без использования модели со случайным оракулом. В таком случае говорят, что используется стандартная модель (*standart model*). Эта модификация в дальнейшем была использована как базовая криптосистема в работе [8] для построения системы, обладающей свойством *IND-CCA2* в рамках стандартной модели. В этой работе одно сообщение шифруется l раз, что приводит к уменьшению скорости передачи информации, по меньшей мере, в l раз. Важно отметить, что l является длиной ключа подписи, а согласно [9], на настоящий момент для обеспечения высокой стойкости длина ключа асимметричной криптосистемы, лежащей в основе алгоритма цифровой подписи, должна быть не менее 256 бит. Таким образом, скорость передачи информации с помощью криптосистемы из [8] существенно мала. Следовательно, актуальна задача разработки криптосистем типа Мак-Элиса, одновременно обладающих свойством *IND-CCA2* и высокой скоростью передачи информации.

С этой целью в настоящей работе ставится задача построения базовой криптосистемы типа Мак-Элиса, одновременно обладающей свойством *IND-CPA* и позволяющей, основываясь на идеях [8], использовать эту базовую криптосистему для построения криптосистемы типа Мак-Элиса со свойством *IND-CCA2* и более высокой скоростью передачи информации.

Основные определения

Пусть F_q— поле Галуа мощности q, q — степень простого числа, $m = (m_1, \dots, m_n) \in F_q^n$. Носителем вектора m будем называть множество $supp(m) = \{i : m_i \neq 0\}$, а весом Хэмминга этого вектора — число $wt(m) = supp(m)$. Для вектора $m(\in F_q^n)$ и упорядоченного множества $\omega \subseteq \{1, \dots, n\}$ рассмотрим оператор проекции Π_ω: $F_q^n \to F_q^{|\omega|}$, действующий по правилу:

$$\Pi_\omega(m) = (m_{i_1}, \dots, m_{i_{|\omega|}}), i_j \in \omega, j = 1, \dots, |\omega|.$$

Пусть $x \in F_q^{n_1}$, $y \in F_q^{n_2}$, $z \in F_q^n$, $n_1 + n_2 = n$, $\omega \subset \{1, \dots, n\}$, $|\omega| = n_1$, тогда запись $z = x \parallel y$ будет означать конкатенацию векторов x и y, а запись $z = (x \parallel_\omega y)$ — конкатенацию этих векторов по упорядоченному множеству ω, то есть $\Pi_\omega(z) = x$ и $\Pi_{\{1,\dots,n\}\setminus\omega}(z) = y$.

Далее мы будем использовать стандартные обозначения для записи алгоритмов и экспериментов, описанные в [11].

ISSN 2658 – 7505
Выпуск №4, 2019
Электронный научный журнал «Вестник молодёжной науки России»

Известные криптосистемы типа Мак-Элиса

Рассмотрим базовую криптосистему Мак-Элиса [5] *McE* на линейном $[n, k, d]$-коде $C(\subseteq Fn)$, где n — его длина, k — размерность кода, а d — минимальное кодовое расстояние. Пусть G — порождающая матрица кода C, $t = \lfloor d - 1 \rfloor$. Секретным ключом sk системы *McE* является пара (S, P), где S — невырожденная $(k \times k)$ −матрица над полем F_q, а P — перестановочная $(n \times n)$-матрица. Публичным ключом pk является пара $(G = SGP, t)$. Зашифрование сообщения выполняется по правилу:

$$\{x\}_{pk}^{McE} = x\tilde{G} + e = y, x \in F_q^k, wt(e) \leq t.$$

Для расшифрования шифртекста y применяется эффективный декодер Dec: $F_q^n \to F_q^k$ кода C и секретный ключ sk:

$$\{y\}_{sk}^{McE} = Dec_c(yP^{-1})S^{-1}.$$

Стойкость к структурным атакам данной криптосистемы основана на следующем предположении.

Предположение 1. Не существует полиномиального алгоритма способного решить проблему синдромного декодировния.

Согласно работе [10], задача синдромного декодирования является *NP*-сложной. Таким образом, данное предположение справедливо.

Тем не менее, данная криптосистема уязвима к атакам на шифртекст. Поэтому, для того же кода C рассмотрим модификацию McE_l криптосистемы типа Мак-Элиса *McE* описанную в [7], в которой правило шифрования имеет вид:

$$\{x\}_{pk}^{McE_l} = \{x||v\}_{pk}^{McE} = y, x \in F_q^l, v \in_R F_q^{k-l},$$

где $a \in_R A$ — случайный и равновероятный выбор элемента a из множества A. Для расшифрования шифрограммы y достаточно применить правило (1.2) и отбросить крайние справа $k - l$ символов:

$$\{y\}_{pk}^{McE_l} = \{y\}_{sk}^{McE} \cdot (I_l \| O_{n-l})^T,$$

где I_l — единичная $(l \times l)$-матрица, O_{k-l} — нулевая $(k - l \times k - l)$ −матрица, а A^T — транспонированная матрица A.

Данная модификация обладает устойчивостью к атакам по подобранному открытому тексту. Другими словами, обладает *IND-CPA* свойством. Важно отметить, что в работе [7] для доказательства свойства *IND-CPA* данной модификации были использованы следующие два предположения:

Предположение 2. Не существует полиномиального алгоритма, способного отличить матрицу публичного ключа криптосистемы *McE* от случайной матрицы соответствующего размера с вероятностью, не являющейся пренебрежимо малой от n.

Предположение 3. Не существует полиномиального алгоритма способного решить задачу обучения с ошибками.

Основываясь на идеях данной модификации, а также её применении в работе [8], мы построим новую криптосистему типа Мак-Элиса.

Новая криптосистема типа Мак-Элиса

Рассмотрим такое множество перестановок $\Im_l \subseteq S_k$, действующих на элементах множества $\{1, \ldots, k\}$, что для любой $\pi \in \Im l$ выполняется условие $\pi(1) < \ldots < \pi(l)$. Множество $\{\pi(1), \ldots, \pi(l)\}$ обозначим ω_π. Заметим, что $|\Im_l| = C_k^l(\mathrm{k} - \mathrm{l})!$, так

ISSN 2658 – 7505
Выпуск №4, 2019
Электронный научный журнал «Вестник молодёжной науки России»

как всего C_k^l подмножеств мощности l во множестве из k элементов, и для каждого такого подмножества ω имеется класс $\Im_l(\omega)(\subseteq Sk)$ перестановок, $|\Im_l| = (k-l)!$, действующих тождественно на элементах из ω.

Каждой перестановке π из $\Im_l$ поставим в соответствие перестановочную $(k \times k)$ −матрицу R_π.

Теперь построим криптосистему $\omega 2McE_l$, в которой правило шифрования имеет вид:

$$\{x\}_{pk}^{\omega 2McE_l} = \{(x\|v_1)R_\pi\}_{pk}^{McE} \| \{(x\|v_2)R_\pi\}_{pk}^{McE} = y, x \in F_q^l, \pi \in_R \Im_l, \quad (1)$$

где $v_i \in_R F_q^{k-l}, i = 1,2, supp(v_1 - v_2) = \{1,\dots,k\}\backslash\omega_\pi$.

Отметим, что для расшифрования получателю не требуется матрица R_π. Для нахождения ω достаточно вычислить вектор

$$z = \{y \cdot (I_n\|O_n)^T\}_{sk}^{McE} - \{y \cdot (O_n\|I_n)^T\}_{sk}^{McE}$$

и найти его носитель $supp(z)$. Тогда,

$$\{y\}_{sk}^{\omega 2McE_l} = (z \cdot R_{\pi'}^{-1}) \cdot (I_l\|O_{k-l})^T, \pi' \in \Im_l(\omega), \omega = supp(z).$$

Далее формулируются предположения безопасности и теорема о семантической стойкости построенной криптосистемы.

Предположение 4. Не существует полиномиального алгоритма, который бы с не пренебрежимо малой вероятностью по одной паре сообщений мог бы определять принадлежность этих векторов коду.

Предположение основано на том, что на настоящий момент не существует таких полиномиальных алгоритмов. Так, например, в ряде недавних работ [11], [12], [13] все алгоритмы решающие поставленную задачу были не полиномиальными.

Предположение 5. Не существует распознавательного полиномиального алгоритма, который принимал бы на вход шифрограмму с базовой криптосистемы Мак-Элиса и ненулевое число l, а на выходе с вероятностью, не являющейся пренебрежимо малой по параметру безопасности n, выдавал бы 0, если данная шифрограмма с соответствует информационному сообщению веса меньшего, чем l и 1, если данная шифрограмма с соответствует информационному сообщению веса равного l.

Предположение основано на том, что существование подобного алгоритма существенно упрощало бы взлом криптосистемы Мак-Элиса и нахождение решения задачи обучения с ошибками. Это бы противоречило предыдущим предположениям.

Теорема. Криптосистема $\omega 2McE_l$ обладает свойством *IND-CPA*, если справедливы утверждения 1-5.

Доказательство данной теоремы будет представлено в следующей публикации.

Построенная криптосистема может быть использована как базовая в конструкции, описанной в [8]. А увеличение скорости может быть реализовано за счет возможности использования различных открытых сообщений в конструкции и одного общего множества ω. Также мы предлагаем способ независимого использования криптосистемы $\omega 2McE_l$.

ISSN 2658 – 7505
Выпуск №4, 2019
Электронный научный журнал «Вестник молодёжной науки России»

Положим, что отправителю необходимо передать пакет из N ($|N| = n$) информационных блоков, каждый из которых принадлежит F_q^l. Для передачи первого блока из N отправитель использует криптосистему $\omega 2McE_l$. Множество ω выбирается только при первой передаче и шифровании сообщения с помощью криптосистемы $\omega 2McE_l$. Это множество запоминается и не генерируется заново в рамках текущего пакета. При передаче последующих n − 1 блоков, блоки будут шифроваться следующим образом. Отправитель использует криптосистему McE_l, но перед шифрованием умножает информационное сообщение на перестановочную матрицу R_π из (1). То есть, отправитель формирует сообщение вида $c = \{(m \parallel v_1)R_\pi\}_{pk}^{McE}$. Для простоты понимания, можно сказать, что отправитель шифрует блок криптосистемой $\omega 2McE_l$ и отправляет только первую часть шифрограммы. Описанный протокол отправки блоков изображен ниже на рисунке 1.

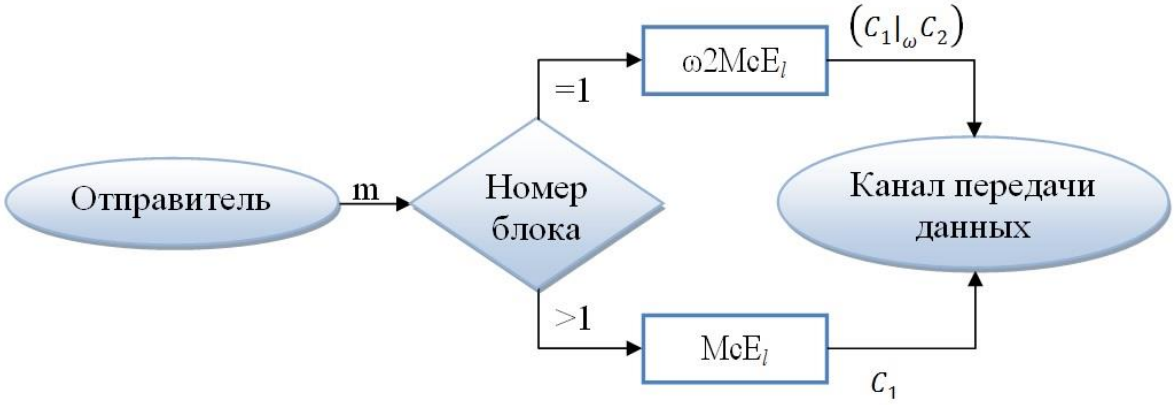

Рис. 1 – Протокол передачи

Получатель при первой передаче с помощью секретного ключа криптосистемы ω2McEl(C) расшифровывает информационный блок и получает множество ω. По множеству ω он строит матрицу R_π и расшифровывает последующие передачи.

Избыточность построенного протокола, относительно стандартного протокола базовой криптосистемы Мак-Элиса, будет равна $\frac{k(n+1)}{ln}$. Из формулы следует, что при большом количестве блоков в пакете избыточность стремится к $\frac{k}{l}$, что соответствует избыточности протокола с криптосистемой McE_l.

Список цитируемой литературы

1. Kobara K., Imai H. Semantically Secure McEliece Public-Key Cryptosystems Conversions for McEliece PKC // Public Key Cryptography. 2001. P. 19-35.
2. Goldwasser S., Micali S. Probabilistic Encryption // Journal of Computer and System Sciences. 1984. V. 38. №2. P. 270-299.
3. Bellare M., Rogaway P. Optimal Asymmetric Encryption - How to Encrypt with RSA // Advances in Cryptology EUROCRYPT'94. 1995. P. 92-111.
4. Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124- 134.
5. McEliece R. J. A Public-Key Cryptosystem Based On Algebraic Coding Theory // DSN Progress Report. 1978. V. 42. №44. P. 114-116.

6. Bellare M., Rogaway P. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols // CCS '93 Proceedings of the 1st ACM conference on Computer and communications security. 1993. P. 62-73.
7. Nojima R., Imai H., Kobara K., Morozov K. Semantic Security for the McEliece Cryptosystem without Random Oracles // Designs, Codes and Cryptography. 2008. V. 49. №1 3. P. 289-305.
8. Dottling N., Dowsley R., Muller-Quade J., Nascimento C. A. Anderson A CCA2 Secure Variant of the McEliece Cryptosystem // IEEE Transactions on Information Theory. 2012. V. 58. №10, P. 6672-6680.
9. Lenstra A. K., Verheul E. R. Selecting Cryptographic Key Sizes // Journal of Cryptology. 2001. V. 14. №4. P. 255-293.
10. Berlekamp E. R., McEliece R. J., Henk C. A. van Tilborg On the inherent intractability of certain coding problems // IEEE Trans. Inf. Theory / F. Kschischang — IEEE, 1978. V. 24, Iss. 3. P. 384–386.
11. Косолапов Ю.В., Турченко О.Ю. Применение одного метода распознавания линейного кода для канала с подслушиванием // ПДМ. 2017. №35.-с.76-88.
12. Chabot C. Recognition of a code in a noisy environment // Proceedings IEEE ISIT. 2007. P. 2211-2215.
13. Yardi A. D., Vijayakumaran S. Detecting linear block codes in noise using the GLRT // IEEE International Conference on Communications. 2013. P. 4895-4899.