УДК 003.26

ПОСТКВАНТОВЫЙ АЛГОРИТМ КОММУТАТИВНОГО ШИФРОВАНИЯ НА ОСНОВЕ СКРЫТОЙ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ[1]

Костина А. А. – н.с. НИЛ КБ и ПКС СПИИРАН,
anna-kostina1805@mail.ru

Молдовян Д.Н. – к.т.н., с.н.с. НИЛ КБ и ПКС СПИИРАН,

mdn.spectr@mail.ru

Фахрутдинов Р.Ш. – к.т.н., зав. НИЛ КБ и ПКС СПИИРАН,

fahr@cobra.ru

Аннотация

Предложен постквантовый алгоритм коммутативного шифрования, обладающий стойкостью к атакам на основе известных исходных текстов. Алгоритм основан на вычислительной трудности скрытой задачи дискретного логарифмирования, заданной в новой форме. В качестве алгебраического носителя предложенного алгоритма могут быть использованы конечные некоммутативные ассоциативные алгебры, содержащие большое множество глобальных левосторонних единиц. Базовой процедурой шифрования является возведение сообщения в натуральную степень большой разрядности

Введение

Криптографические алгоритмы и протоколы с открытым ключом, основанные на вычислительной сложности задачи факторизации (ЗФ) и

[1] Санкт-Петербургский институт информатики и автоматизации Российской Академии Наук. Работа выполнена при частичной финансовой поддержке РФФИ (проект № 18-07-00932-а)

задачи дискретного логарифмирования (ЗДЛ) [1], нашли широкое практическое применение для обеспечения защиты информации. Специальные применения нашли протоколы бесключевого шифрования, основанные на коммутативном шифре Полига–Хеллмана [1], стойкость которого к атакам на основе известных текстов основана на вычислительной трудности ЗДЛ. Для квантовых компьютеров известны полиномиальные алгоритмы решения ЗФ и ЗДЛ [2,3], что обусловливает проблему разработки постквантовых криптосхем.

Предполагая, что квантовый компьютер, может появиться после 2025 г., НИСТ США в конце 2016 г. объявил международный конкурс на разработку постквантовых криптосхем с открытым ключом [4]. Аналогичную проблематику освещает ежегодная международная конференция «International Workshop on Post-Quantum Cryptography» [5].

Вопрос разработки постквантовых алгоритмов коммутативного шифрования актуален, поскольку взлом описанного в работе [6] коммутативного шифра, основанного на скрытой ЗДЛ (СЗДЛ), сводится к решению обычной ЗДЛ в конечном поле. В данной работе предложена усиленная форма СЗДЛ и постквантовый алгоритм коммутативного шифрования.

Обычная ЗДЛ задается как решение уравнения вида $W = G^x$, где Y и G – заданные элементы конечной циклической группы Г произвольной природы, x – неизвестное целочисленное значение. Скрытой ЗДЛ называется в случае, когда, по крайней мере, один из элементов W и G маскируется - вместо него задается некоторый другой элемент $Y \notin \Gamma$ алгебраической структуры, содержащей в себе циклическую группу Г [6,7]. Впервые СЗДЛ была задана в конечной алгебре кватернионов в форме, позволяющей построить протокол открытого согласования ключей и алгоритм коммутативного шифрования [8]. Новые формы СЗДЛ [9,10], отличаются усиленной маскировкой базовой циклической группы Г, однако ни одна из новых форм СЗДЛ не пригодна для разработки на ее основе алгоритмов коммутативного шифрования.

В настоящей статье предлагается новая форма задания СЗДЛ и постквантовый коммутативный шифр на ее основе.

Алгебраический носитель и его свойства

Пусть m-мерное векторное пространство задано над конечным полем $GF(p)$. Произвольный вектор A будем записывать в виде упорядоченного

набора его координат $A = (a_0, a_1, \ldots, a_{m-1})$ или в виде суммы его компонент $A = \sum_{i=0}^{m-1} a_i \mathrm{e}_i$, где $\mathbf{e}_i$ – базисные векторы; $a_i \in GF(p)$ – координаты вектора. Векторное пространство, в котором определена операция умножения произвольных двух векторов, дистрибутивная относительно операции сложения, называется алгеброй.

Операция умножения двух векторов $A = \sum_{i=0}^{m-1} a_i \mathrm{e}_i$ и $B = \sum_{j=0}^{m-1} b_j \mathrm{e}_j$ определяется по правилу перемножения каждой компоненты первого вектора с каждой компонентой второго вектора:

$$A \circ B = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j \left(\mathrm{e}_i \circ \mathrm{e}_j\right),$$

в котором каждое произведение вида $\mathrm{e}_i \circ \mathrm{e}_j$ заменяется на вектор $\lambda \mathbf{e}_k$, задаваемый таблицей умножения базисных векторов (ТУБВ). Значение λ называется структурным коэффициентом. Если $\lambda = 1$, то в таблице указывается базисный вектор $\mathbf{e}_k$. Левый множитель в произведении $\mathrm{e}_i \circ \mathrm{e}_j$ указывает строку, а правый – столбец, пересечение дает ячейку $\lambda \mathbf{e}_k$.

Для случая размерности $m = 4$ табл. 1 задает некоммутативную ассоциативную операцию умножения векторов, при которой для любой тройки векторов A, B, и C выполняется равенство

$$\left(A \circ B\right) \circ C = A \circ \left(B \circ C\right).$$

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mu\mathbf{e}_0$	$\mathbf{e}_3$	$\mu\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_1$	$\mu\mathbf{e}_0$	$\mathbf{e}_3$	$\mu\mathbf{e}_2$

Таблица 1. Строение ТУБВ для задания ассоциативной операции умножения четырехмерных векторов (μ – квадратичный невычет в $GF(p)$)

Рассматриваемая КНАА содержит большое подмножество элементов, которые играют роль глобальных левосторонних единиц. При этом в алгебре также содержится много различных локальных правосторонних единиц.

Рассмотрим векторное уравнение вида

$$X \circ A = A, \qquad (1)$$

где $X = (x_0, x_1, x_2, x_3)$ – неизвестное значение; A –заданный элемент алгебры. Решение этого уравнения сводится к решению системы из четырех линейных уравнений, что дает формулу, описывающую p^2 *глобальных* левосторонних единиц:

$$L = (l_0, l_1, l_2, l_3) = (x_0, x_1, 1 - x_0, - x_1), \qquad (2)$$

где $x_0, x_1 = 0, 1, \ldots. p - 1$. Для нахождения правосторонних единиц следует рассмотреть векторное уравнение вида

$$A \circ X = A, \qquad (3)$$

которое сводится к совместному решению следующих независимых систем из двух линейных уравнений:

$$\begin{cases} (a_0 + a_2)x_0 + \mu(a_1 + a_3)x_1 = a_0; \\ (a_1 + a_3)x_0 + (a_0 + a_2)x_1 = a_1; \end{cases} \qquad (4)$$

$$\begin{cases} (a_0 + a_2)x_2 + \mu(a_1 + a_3)x_3 = a_2; \\ (a_1 + a_3)x_2 + (a_0 + a_2)x_3 = a_3; \end{cases} \qquad (5)$$

Системы (4) и (5) имеют один и тот же главный детерминант Δ_A:

$$\Delta_A = (a_0 + a_2)^2 - \mu(a_1 + a_3)^2, \qquad (6)$$

С учетом того, что структурная константа μ является квадратичным невычетом в $GF(p)$, мы имеем только p^2 векторов A, для которых детерминант $\Delta_A = 0$. В алгоритме коммутативного шифрования мы будем представлять сообщение в виде 4-мерных векторов M, для которых с пренебрежимо малой вероятностью $p^2/p^4 = p^{-2}$ имеет место $\Delta_M = 0$. То есть практически мы всегда будем иметь случай $\Delta_M \neq 0$. Векторы, для которых главный определить систем (4) и (5) не равен нулю существует единственное решение векторного уравнения (3), которое дает единственную *локальную* правостороннюю единицу $R_A = (r_0, r_1, r_2, r_3)$, для координат которой легко могут быть получены следующие формулы:

$$r_0 = \frac{a_0(a_0 + a_2) - \mu a_1(a_1 + a_3)}{\Delta_A}; \qquad r_1 = \frac{a_1 a_2 - a_0 a_3}{\Delta_A}; \qquad (7)$$

$$r_2 = \frac{a_2(a_0 + a_2) - \mu a_3(a_1 + a_3)}{\Delta_A}; \qquad r_3 = \frac{a_0 a_3 - a_1 a_2}{\Delta_A}. \qquad (8)$$

В общем случае различным векторам A соответствуют различные правосторонние единицы, которые будем называть локальными, поскольку они действуют только в рамках некоторых подмножеств элементов рассматриваемой КНАА. Легко доказать следующие утверждения:

Утверждение 1. Правосторонняя локальная единица R_A, соответствующая некоторому вектору A, является одновременно локальной правосторонней единицей для вектора A^i при всех натуральных степенях i.

Утверждение 2. Пусть дан вектор A, такой, что $\Delta_A \neq 0$. Тогда для любого заданного вектора L из множества глобальных левосторонних единиц можно вычислить вектор B, для которого выполняется условие $A \circ B = L$.

Утверждение 3. Пусть дан вектор A, для которого выполняется условие $\Delta_A \neq 0$. Тогда при некотором минимальном значении ω_A имеет место $A^{\omega_A} = R_A$ и множество $\left\{A, A^2, ..., A^i, ..., A^{\omega_A}\right\}$ представляет собой конечную циклическую группу с единичным элементом R_A.

Утверждение 4. Пусть даны векторы A и B, такие, что выполняется условие $A \circ B = L$, где L – единица из множества (3). Тогда формула $\psi_L(X) = B \circ X \circ A$, где X пробегает все значения алгебры, задает гомоморфное отображение рассматриваемой четырехмерной КНАА.

Например для операции умножения имеем:

$$\psi_L(X_1 \circ X_2) = B \circ (X_1 \circ X_2) \circ A = B \circ X_1 \circ A \circ B \circ X_2 \circ A = \\ = \psi_L(X_1) \circ \psi_L(X_2).$$

Утверждение 5. Пусть даны векторы A и B, такие, что выполняется условие $A \circ B = L$. Тогда для любого натурального значения t выполняется условие $A^t \circ B^t = L$.

Утверждение 6. Пусть задана глобальная левосторонняя единица L. Тогда формула $\varphi_L(X) = X \circ L$, где X пробегает все значения алгебры, задает гомоморфное отображение рассматриваемой четырехмерной КНАА.

Постквантовый алгоритм коммутативного шифрования

Для разработки постквантового алгоритма коммутативного шифрования в данной работе предлагается использовать СЗДЛ, задаваемую в КНАА, рассмотренной в предыдущем разделе при размере простого числа p, равного 256–512 бит. Общими параметрами

постквантового алгоритма шифрования, представленного далее, являются значение p, значение структурной константы μ, левосторонняя единица L_0 и два вектора A и B, удовлетворяющие условию $A \circ B = L_0$.

Для шифрования сообщения M, оно представляется в виде четырехмерного вектора $M = (m_0, m_1, m_2, m_3)$. В качестве ключа шифрования формируется пара натуральных чисел e и d, таких, что выполняется соотношение $ed \equiv 1 \bmod (p^2 - 1)$, случайное натуральное число $t < p^2 - 1$ и случайная левосторонняя единица L из множества (2). Процедура зашифровывания включает выполнение следующих двух шагов:

1. По формулам (7) и (8) вычислить локальную правостороннюю единицу R_M, соответствующую вектору M.

2. Вычислить вектор C по формуле:

$$C = B^t \circ M^e \circ A^t \circ L. \qquad (9)$$

Выходным шифртекстом является пара векторов (R_M, C). Процедура расшифровывания шифртекста (R_M, C) выполняется по формуле:

$$M = A^t \circ C^d \circ B^t \circ R_M. \qquad (10)$$

Доказательство корректности работы предложенного алгоритма коммутативного шифрования выполняется следующим образом:

$$M' = A^t \circ C^d \circ B^t \circ R_M = A^t \circ \left(B^t \circ M^e \circ A^t \circ L\right)^d \circ B^t \circ R_M =$$
$$= A^t \circ B^t \circ M^{ed} \circ A^t \circ B^t \circ R_M = L_0 \circ M \circ L_0 \circ R_M = M.$$

Заметим, что при зашифровывании сообщения M на двух разных ключах первый элемент шифртекста вычисляется только в ходе первой процедуры зашифровывания. При выполнении второй процедуры зашифровывания выполняется только преобразование, задаваемое формулой (9). Также как и в случае экспоненциального шифра Полига–Хеллмана, основной вклад в стойкость описанного алгоритма коммутативного шифрования вносит операция возведения в степень большой разрядности, выполняемая над исходным сообщением. Однако, в предлагаемом алгоритме выполняются дополнительные операции гомоморфного отображения, что делает необходимым решать СЗДЛ при выполнении криптоанализа, за счет чего обеспечивается стойкость к атакам с использованием квантовых компьютеров.

По аналогии с предложенным алгоритмом могут быть реализованы

постквантовые алгоритмы с использованием КНАА содержащих большое множество правосторонних глобальных единиц. Значение размерности алгебры несущественно влияет на производительность алгоритма, поэтому в качестве алгебраических носителей алгоритма могут использоваться КНАА размерностей 4, 6 и 8. Самостоятельный интерес представляет построение постквантовых алгоритмов коммутативного шифрования с использованием КНАА, заданных над расширениями двоичного поля при степенях расширения 256 и более.

Заключение

Рассмотрено построение постквантового коммутативного шифра на основе новой формы СЗДЛ, в качестве алгебраического носителя которой использована четырехмерная КНАА, содержащая большое множество глобальных левосторонних единиц.

Литература

1. Menezes A.J., Van Oorschot P.C., and Vanstone S.A. Handbook of Applied Cryptography. – Boca Raton, FL: CRC Press, 1997. – 780 p.
2. Shor P.W. 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer. SIAM Journal of Computing. 26:1484–1509.
3. Yan S. Y. 2014. Quantum Attacks on Public-Key Cryptosystems . Springer US. 207 p.
4. Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf
5. Proceedings of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, February 24-26, 2016 // Lecture Notes in Computer Science (LNCS) series. Springer, 2016. Vol. 9606. - 270 p.
6. Post-Quantum Cryptography. 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings. // Lecture Notes in Computer Science series. Springer, 2018, vol. 10786

7. Moldovyan D.N., Moldovyan N.A. A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols // Springer Verlag LNCS. 2010. Vol. 6258. P. 183−194 / 5th Int. Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ANCS 2010 Proceedings. St.Petersburg, September 8−11, 2010.
8. Moldovyan D.N. Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. Vol. 18. P. 165−176.
9. Moldovyan N. A., Moldovyan A. A. Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem // Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS). 2019. Vol. 12. No. 1. P. 66–81.
10. Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science Journal of Moldova. 2018. Vol. 26. No. 3(78). P. 301–313.