Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2021. Т. 21, вып. 3. С. 408–418
Izvestiya of Saratov University. Mathematics. Mechanics. Informatics, 2021, vol. 21, iss. 3, pp. 408–418
https://mmi.sgu.ru https://doi.org/10.18500/1816-9791-2021-21-3-408-418

Научная статья
УДК 004.056.55

Протокол обмена ключами на основе некоммутативных элементов алгебры Клиффорда

С. Н. Чуканов

Институт математики им. С. Л. Соболева СО РАН, Омский филиал, Россия, 644043, г. Омск, ул. Певцова, д. 13

Чуканов Сергей Николаевич, доктор технических наук, профессор, ведущий научный сотрудник, ch_sn@mail.ru, https://orcid.org/0000-0002-8106-9813

Аннотация. Многие из протоколов асимметричной криптографии основаны на операциях, выполняемых в коммутативных алгебраических структурах, которые уязвимы для квантовых атак. Разработка алгоритмов в некоммутативных структурах позволяет усилить эти протоколы. Криптография — это раздел математики, в котором решается задача передачи информации через небезопасные каналы. Для этого информация шифруется. При шифрованном обмене данными выделяются подзадачи: безопасный обмен ключами, а затем шифрование/дешифрование сообщения. В задачах криптографии с открытым ключом применяется протокол обмена ключами Диффи – Хеллмана. В настоящее время возрос интерес к разработке альтернативных асимметричных криптосистем, устойчивых к атакам алгоритмов квантовых компьютеров. Большинство из этих схем являются алгоритмами некоммутативной криптографии, например схема, основанная на кольце матричных полиномов. Одна из задач для разработки криптографических схем — поиск сопряженности — может быть сформулирована над конечными некоммутативными группами. Безопасность передачи информации может быть построена на основе неразрешимости проблемы поиска сопряженности, которая определена над конечными некоммутативными группами. Целью настоящей работы является разработка модели протокола Диффи – Хеллмана с использованием алгебраической структуры алгебры Клиффорда (к которым относятся кватернионы) и структуры кольца многочленов. Обеспечение безопасности алгоритма с использованием алгебр Клиффорда основано на некоммутативной структуре этих алгебр и возможности работы в пространстве любой размерности $n \geqslant 1$. Группы алгебры Клиффорда являются некоммутативными структурами, так же как и матричные полиномы. Однако группы алгебры Клиффорда имеют более компактную запись, показывают меньшее время выполнения во многих сопоставимых операциях. Использование в качестве коэффициентов элементов алгебр Клиффорда и показателей степеней целых чисел позволяет понизить требование к регистрам процессоров (не использовать процессоры с плавающей запятой) и существенно повысить производительность формирования протокола Диффи – Хеллмана.

Ключевые слова: некоммутативная криптография, кватернионы, октонионы, алгебры Клиффорда

Благодарности: Работа выполнена при финансовой поддержке РФФИ (проекты № 18-07-00526, № 18-08-01284).

Для цитирования: *Чуканов С. Н.* Протокол обмена ключами на основе некоммутативных элементов алгебры Клиффорда // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2021. Т. 21, вып. 3. С. 408–418. https://doi.org/10.18500/1816-9791-2021-21-3-408-418

Article

The key exchange protocol based on non-commutative elements of Clifford algebra

S. N. Chukanov

Sobolev Institute of Mathematics, Siberian Branch of the Russian Academy of Sciences, Omsk Branch, 13 Pevtsova St., Omsk 644043, Russia
Sergei N. Chukanov, ch_sn@mail.ru, https://orcid.org/0000-0002-8106-9813

Abstract. Many of the asymmetric cryptography protocols are based on operations performed on commutative algebraic structures, which are vulnerable to quantum attacks. The development of algorithms in non-commutative structures makes it possible to strengthen these protocols. Cryptography is a branch of mathematics that solves the problem of transmitting information through unsafe channels. For this, information is encrypted, so it cannot be used without first decrypting it. In encrypted communication, subtasks are distinguished: secure key exchange, and then encryption/decryption of the message. Public key cryptography uses the Diffie – Hellman key exchange protocol. Since the beginning of this century, interest has increased in the development of alternative asymmetric cryptosystems that are resistant to attacks by quantum computer algorithms. Most of these schemes are non-commutative cryptography algorithms, such as a scheme of matrix polynomial ring. One of the tasks for the development of cryptographic schemes — the task of conjugacy search, can be formulated over finite non-commutative groups. The security of information transmission can be built based on the undecidability of the conjugacy search problem, which is defined over finite non-commutative groups. The aim of this work is to develop a model of the Diffie – Hellman protocol using the algebraic structure of the Clifford algebra (which includes the quaternions) and the structures of the polynomial ring. Safety ensuring of the algorithm using Clifford algebras is based on the non-commutative structure of these algebras and the ability to work in a space of any dimension $n \geqslant 1$. Clifford algebra groups are non-commutative structures, as are matrix polynomials and braid groups. However, Clifford algebra groups are more compact and show shorter execution times in many comparable operations. The use of elements of Clifford algebras and exponents of integers as coefficients allows us to reduce the requirement for processor registers (do not use floating-point processors) and significantly increase the performance of forming the Diffie – Hellman protocol.
Keywords: non-commutative cryptography, quaternions, octonions, Clifford algebra
Acknowledgements: This work was supported by the Russian Foundation for Basic Research (projects Nos. 18-07-00526, 18-08-01284).
For citation: Chukanov S. N. The key exchange protocol based on non-commutative elements of Clifford algebra. *Izvestiya of Saratov University. Mathematics. Mechanics. Informatics*, 2021, vol. 21, iss. 3, pp. 408–418 (in Russian). https://doi.org/10.18500/1816-9791-2021-21-3-408-418

Введение

Развитие криптографии с открытым ключом было революционной концепцией, возникшей в двадцатом веке. Первым исследованием криптографии с открытым ключом стала опубликованная в 1976 г. работа W. Diffie и M. E. Hellman, в которой была описана схема согласования ключей [1]. Безопасность криптосистемы Diffie – Hellman зависит от трудностей в решении задач теории чисел, например дискретных логарифмических задач (discrete logarithmic problems — DLP). Разработка криптосистем на основе неабелевых групп является одним из приоритетов исследования новых криптографических методов. Наиболее часто обсуждаемые неабелевы параметры включают группы матриц, группы кос, логарифмические сигнатуры.

Модель криптографической схемы с открытым ключом такова: предположим, что Alice хочет отправить сообщение M для Bob. Alice использует отображение f_{k_1} для шифрования сообщения $C = f_{k_1}(M)$, где f_{k_1} является односторонней функцией и является общедоступной. После получения кода C Bob использует отображение g_{k_2} для декодирования $g_{k_2}(f_{k_1}(M)) = M$, где g_{k_2} функция известна только Bob.

Протокол Diffie – Hellman (DH) работает следующим образом: пусть G — циклическая группа с генератором g. Предположим, что Alice и Bob формируют общий секретный ключ K. Alice случайным образом выбирает целое число $1 < a < o(g)$ и отправляет Bob код: $A = g^a$. Точно так же Bob случайным образом выбирает целое число $1 < b < o(g)$ и отправляет Alice: $B = g^b$. Alice вычисляет $K = B^a$, а Bob вычисляет $K = A^b$.

Задача 1 (Diffie – Hellman). *Пусть дана группа G. Для известных $g, g^x, g^y \in G$ найти g^{xy}.*

Задача 2 (DLP). *Пусть дана группа G. Если $h, g \in G$ таковы, что $h = g^x$ и h, g известны. Найти целое число x.*

Задача 3 (Conjugacy Search — поиска сопряжения). *Пусть дана неабелева группа G. Пусть $h, g \in G$ таковы, что $h = g^x$ для некоторого $x \in G$. Найти x. Здесь $g^x = x^{-1}gx$.*

Рассмотрим схему согласования ключей Anshel – Anshel – Goldfeld [2]. Пусть G — неабелева группа и $S_A = \langle a_1, \ldots, a_k \rangle \subseteq G, S_B = \langle b_1, \ldots, b_m \rangle \subseteq G$ — подгруппы.

Алгоритм AAG.

1. Alice выбирает случайный код $x = x(a_1, \ldots, a_k) \in G$ в качестве слова в S_A и отправляет Bob: $\{b_1^x, \ldots, b_m^x\} = \{x^{-1}b_1x, \ldots, x^{-1}b_mx\}$. Bob выбирает случайный код $y = y(b_1, \ldots, b_m) \in G$ в качестве слова в S_B и отправляет Alice: $\{a_1^y, \ldots, a_k^y\} = \{y^{-1}a_1y, \ldots, y^{-1}a_ky\}$.

2. Alice вычисляет $x(a_1^y, \ldots, a_k^y) = x^y = y^{-1}xy$ и $x^{-1}(y^{-1}xy) = x^{-1}y^{-1}xy = [x, y] = K$.

3. Bob вычисляет $y(b_1^x, \ldots, b_m^x) = y^x = x^{-1}yx$ и $(y^{-1}(x^{-1}yx))^{-1} = (y^{-1}x^{-1}yx)^{-1} = x^{-1}y^{-1}xy = [x, y] = K$.

В 2009 г. P. Hecht [3] представил модель обмена ключами на основе протокола Diffie – Hellman по некоммутативным кольцам с использованием матриц четвертого порядка с элементами Z_{256}, что особенно интересно для обеспечения криптографической защиты устройств с низкой вычислительной мощностью. В работе [4] построена схема шифрования с открытым ключом, основанная на проблеме сопряженности DH над группами кос [5]. В работе Kamlofsky [6] предложена

схема распределения ключей Diffie – Hellman, основанная на кольце кватернионных многочленов.

В настоящей работе разработана модель DH с использованием алгебраической структуры кватернионов, октонионов, алгебр Клиффорда и структуры кольца многочленов. Обеспечение безопасности алгоритма с использованием алгебр Клиффорда основано на некоммутативной структуре этих алгебр и возможности работы в пространстве любой размерности $n \geqslant 1$.

1. Кольцо многочленов

Для любого кольца $\mathbf{R}$ обозначим кольцо многочленов $\mathbf{R}[x]$ с формальными x и коэффициентами из кольца $\mathbf{R}$. Можно представить различные классы многочленов от переменной структуры (кватерниона, октониона) в зависимости от того, коммутирует ли переменная с коэффициентами многочлена или нет. Множество многочленов в $\mathbb{H}$, $\mathbb{O}$ или $G(p,q,r)$ [7, 8] является кольцом относительно операций сложения и умножения, определенными для многочленов $P(x) = \sum\limits_{i=0}^{n} a_i x^i$, $Q(x) = \sum\limits_{j=0}^{m} b_j x^j$: $P(x)+Q(x) = \sum\limits_{k=0}^{\max[m,n]} (a_k + b_k)\, x^k$, $P(x)Q(x) = \sum\limits_{k=0}^{m+n} \left(\sum\limits_{j=0}^{k} a_j b_{k-j} \right) x^k$. В качестве кольца многочленов $\mathbf{R}[x]$ для повышения производительности вычислительных операций можно выбрать кольцо многочленов $\mathbb{Z}[x]$.

Рассмотрим задачу двустороннего отображения в некоммутативных структурах: для трех заданных кватернионов (октонионов) M, L, S и другого кватерниона (октониона) Q найти два многочлена $V(x)$ и $W(x)$ таких, что $Q = V(M) \cdot L \cdot W(S)$. Кватернионом (октонионом) Q может быть открытый ключ Alice A или открытый ключ Bob B. Поскольку умножение кватернионов (октонионов) некоммутативно, то единственный способ, с помощью которого злоумышленник может решить эту проблему, — это найти методом исчерпывающего поиска два кватерниона (октониона) $V_1(M)$ и $W_1(M)$, таких что $Q = V_1(M) \cdot L \cdot W_1(S)$.

Рассмотрим задачу двустороннего отображения в некоммутативных структурах. Для трех заданных кватернионов (октонионов) M, L, S и еще одного кватерниона (октониона) Q найти такие два многочлена $V(x)$ и $W(x)$, где x — формальный параметр, что $Q = V(M) \cdot L \cdot W(S)$. Кватернион (октонион) Q может быть открытым ключом Alice A или открытым ключом Bob B. Поскольку умножение кватернионов (октонионов) некоммутативно, то единственный способ для злоумышленника решить задачу двустороннего отображения – это найти методом исчерпывающего поиска такие два кватерниона (октониона) $V_1(M)$ и $W_1(S)$, что $Q = V_1(M) \cdot L \cdot W_1(S)$.

Пусть Q принадлежит некоммутативным алгебраическим структурам $\mathbb{H}, \mathbb{O}$ или $G(p,q,r)$. Пусть $f(Q), h(Q) \in \mathbb{Z}^+(Q)$ — ненулевые многочлены с показателями и коэффициентами в $\mathbb{Z}^+$. Так как $q^s q^t = q^t q^s = q^{s+t}$, $\forall\ s,t \in \mathbb{Z}^+$, то

$$[f(Q)]^n \cdot [h(Q)]^m = [h(Q)]^m \cdot [f(Q)]^n, \quad \forall\ n,m \in \mathbb{Z}^+.$$

2. Протокол DH с некоммутативными алгебраическими структурами

Рассмотрим протокол DH с некоммутативными алгебраическими структурами (кватернионами, октонионами или алгебрами Клиффорда).

1. Alice выбирает два ненулевых элемента A, B (принадлежащие некоммутативной алгебраической структуре) с коэффициентами в $\mathbb{Z}_{256}$ и $m, n \in \mathbb{Z}_{16}$; $m \neq 0$,

$n \neq 0$. Alice рассчитывает $\tilde{A}$, $\tilde{B}$ нормализацией A, B соответственно: $\tilde{A} = A \cdot |A|^{-1}$, $\tilde{B} = B \cdot |B|^{-1}$.

2. Alice выбирает в качестве ключа целочисленный ненулевой многочлен $f(x) \in \mathbb{Z}_{16}(x)$ с показателями и коэффициентами в $\mathbb{Z}_{16}$, такой что $f(\tilde{A}) \neq 0$. Bob выбирает в качестве ключа целочисленный ненулевой многочлен $h(x) \in \mathbb{Z}_{16}(x)$ с показателями и коэффициентами в $\mathbb{Z}_{16}$, такой что $h(\tilde{A}) \neq 0$.

3. Alice отправляет Bob $\tilde{A}$, $\tilde{B}$, m, n по небезопасному каналу.

4. Alice рассчитывает символ $\tilde{f}(\tilde{A})$ нормализацией $f(\tilde{A})$ (при этом $r_A = \tilde{f}(\tilde{A})^m \cdot \tilde{B} \times$ $\times\, \tilde{f}(\tilde{A})^n$) и отправляет его Bob через небезопасный канал. Bob рассчитывает символ $\tilde{h}(\tilde{A})$ нормализацией $h(\tilde{A})$ (при этом $r_B = \tilde{h}(\tilde{A})^m \cdot \tilde{B} \cdot \tilde{h}(\tilde{A})^n$) и отправляет его Alice по небезопасному каналу.

5. Alice рассчитывает свой пароль: $k_A = \tilde{f}(\tilde{A})^m \cdot r_B \cdot \tilde{f}(\tilde{A})^n$. Bob рассчитывает свой пароль: $k_B = \tilde{h}(\tilde{A})^m \cdot r_A \cdot \tilde{h}(\tilde{A})^n$. Можно проверить:

$$k_A = \tilde{f}(\tilde{A})^m \times \tilde{h}(\tilde{A})^m \cdot \tilde{B} \cdot \tilde{f}(\tilde{A})^n \cdot \tilde{f}(\tilde{A})^n = \tilde{h}(\tilde{A})^m \cdot \tilde{f}(\tilde{A})^m \cdot \tilde{B} \cdot \tilde{f}(\tilde{A})^n \cdot \tilde{h}(\tilde{A})^n = k_B.$$

Alice рассчитывает: $K_A = (k_A \cdot 256) \,(\mathrm{mod}\, 256)$;
Bob рассчитывает: $K_B = (k_B \cdot 256)(\mathrm{mod}\, 256)$; $K_A = K_B$.

Протокол обмена ключами на основе кватернионов

Кватернионы были предложены У. Гамильтоном (W. R. Hamilton) в 1843 г. [9]. Описание кватернионов и бикватернионов можно найти в работах [10–13].

Гамильтон предположил, что существует три квадратных корня из -1 (мнимые кватернионные единицы): i, j, k с коммутационными соотношениями: $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$. Множество кватернионов обозначаются как $\mathbb{H}$. Они охватываются единичным элементом 1 и тремя мнимыми единицами, т. е. кватернион может быть представлен как четыре действительных числа: $q = q_1 + q_2 i + q_3 j + q_4 k$.

Кватернионы имеют более компактную запись и показывают меньшее время выполнения умножений во многих сопоставимых операциях по сравнению с умножениями матриц.

При исходных кватернионах

$$A = 15 + 157i + 200j + 46k, \quad B = 23 + 121i + 118j + 26k$$

и многочленах

$$f(x) = 13x^7 + 7x^4 + 11, \quad h(x) = 11x^7 + 5x^3 + 13$$

получим следующие результаты:

$$\tilde{A} = 0.058 + 0.607i + 0.773j + 0.178k, \quad \tilde{B} = 0.133 + 0.701i + 0.684j + 0.151k,$$
$$m = 4, \quad n = 3;$$
$$\tilde{f}(\tilde{A}) = 0.683 - 0.444i - 0.565j - 0.13k, \quad r_A = -0.402 + 0.626i + 0.625j + 0.238k,$$
$$\tilde{h}(\tilde{A}) = 0.46 - 0.539i - 0.687j - 0.158k, \quad r_B = 0.989 + 0.095i - 0.01j + 0.114k,$$
$$k_A = k_B = 0.805 + 0.321i + 0.442j + 0.231k,$$
$$(k_A \cdot 256)(\mathrm{mod}\, 256) = (k_B \cdot 256)(\mathrm{mod}\, 256) = 206 + 82i + 113j + 59k.$$

Протокол обмена ключами на основе октонионов

Октонионы были предложены Дж. Грейвсом (J. T. Graves) и А. Кейли (A. Cayley) в 1843 г. [14].

Для формирования октониона необходимо добавить еще один независимый квадратный корень из -1: $\mathfrak{l}$. Октонион x можно рассматривать как пару кватернионов (x_{1H}, x_{2H}), так что $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}\mathfrak{l}$. Будем обозначать произведение i и $\mathfrak{l}$ как $i\mathfrak{l}$; аналогично с j и k. Квадраты $i\mathfrak{l}$, $j\mathfrak{l}$, $k\mathfrak{l}$ также равны -1. Существует семь независимых мнимых единиц, и можно написать $x = x_0 + x_1 i + x_2 j + x_3 k + x_4 \mathfrak{l} + x_5 i\mathfrak{l} + x_6 j\mathfrak{l} + x_7 k\mathfrak{l}$, где $x_m \in \mathbb{R}$. Произведение октонионов является некоммутативным и неассоциативным. Символы октонионов $i, j, k, \mathfrak{l}$ могут быть заменены буквенными обозначениями: $e_1 = i$; $e_2 = j$; $e_3 = k$; $e_4 = \mathfrak{l} = l$; $e_5 = i\mathfrak{l} = m$; $e_6 = j\mathfrak{l} = n$; $e_7 = k\mathfrak{l} = o$. Для определения результатов умножения октонионов можно использовать таблицу Кэли:

$$\begin{array}{c} \\ 1 \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \end{array}
\begin{array}{c}
\begin{array}{cccccccc} 1 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\
\left[\begin{array}{cccccccc}
1 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \\
e_1 & -1 & e_3 & -e_2 & e_5 & -e_4 & -e_7 & e_6 \\
e_2 & -e_3 & -1 & e_1 & e_6 & -e_7 & -e_4 & -e_5 \\
e_3 & -e_2 & -e_1 & -1 & e_7 & -e_6 & -e_5 & -e_4 \\
e_4 & -e_5 & -e_6 & -e_7 & -1 & -e_1 & e_2 & e_3 \\
e_5 & -e_4 & -e_7 & e_6 & -e_1 & -1 & -e_3 & e_2 \\
e_6 & e_7 & e_4 & -e_5 & -e_2 & e_3 & -1 & -e_1 \\
e_7 & -e_6 & e_5 & e_4 & -e_3 & -e_2 & e_1 & -1
\end{array}\right]
\end{array}.$$

Результат умножения октонионов можно представить в виде

$$e_i e_j = \begin{cases} e_j, & \text{если } i = 0, \\ e_i, & \text{если } j = 0, \\ -\delta_{ij} e_0 + \varepsilon_{ijk} e_k, & \text{иначе,} \end{cases}$$

где δ_{ij} — символ Кронекера, ε_{ijk} — полностью антисимметричный тензор.

Октонионы имеют более компактную запись и показывают меньшее время выполнения умножений во многих сопоставимых операциях по сравнению с умножениями матриц.

При исходных октонионах

$$A = 15 + 57i + 93j + 137k + 172l + 202m + 231n + 250o,$$
$$B = 23 + 253i + 215j + 179k + 144l + 105m + 72n + 41o$$

и многочленах

$$f(x) = 13x^7 + 7x^4 + 11, \quad h(x) = 11x^7 + 5x^3 + 13$$

получим следующие результаты:

$$\tilde{A} = 0.032 + 0.122i + 0.2j + 0.294k + 0.37l + 0.434m + 0.496n + 0.537o,$$
$$\tilde{B} = 0.054 + 0.594i + 0.505j + 0.42k + 0.338l + 0.247m + 0.169n + 0.096o,$$
$$m = 4, \quad n = 3,$$

$$\tilde{f}(\tilde{A}) = 0.742 - 0.082i - 0.134j - 0.197k - 0.247l - 0.29m - 0.332n - 0.36o,$$
$$r_A = -0.582 + 0.472i + 0.39j + 0.365k - 0.241l + 0.167m + 0.254n - 0.052o,$$
$$\tilde{h}(\tilde{A}) = 0.54 - 0.103i - 0.168j - 0.248k - 0.311l - 0.365m - 0.418n - 0.452o,$$
$$r_B = 0.48 + 0.398i + 0.354j + 0.387k - 0.319l + 0.25m + 0.409n + 0.067o,$$
$$k_A = k_B = -0.222 + 0.069i + 0.136j + 0.3k - 0.415l + 0.363m + 0.65n + 0.332o,$$
$$(k_A \cdot 256)(\mathrm{mod}\,256) = (k_B \cdot 256)(\mathrm{mod}\,256) =$$
$$= -57 + 18i + 35j + 77k - 106l + 93m + 166n + 85o.$$

Протокол обмена ключами на основе элементов алгебр Клиффорда

Алгебры Клиффорда были предложены У. Клиффордом в 1878 г. [15, 16]. Описание алгебр Клиффорда можно найти в [7, 8].

Основные определения. Пусть V^n — векторное пространство размерности n. Сформируем геометрическую алгебру (вещественную алгебру Клиффорда) G_n. Пусть $\{e_1, e_2, \ldots, e_n\}$ набор ортонормированных базисных векторов в V^n. Геометрическая алгебра G_n снабжена квадратичной формой Q. Геометрическая алгебра $G\left(V^n, Q\right)$ порождается V^n при условии $v^2 = Q(v)$, $\forall\, v \in V^n$. Если характеристика основного поля F не равна 2, это условие можно переписать в следующем виде: $uv + vu = 2\left\langle u, v\right\rangle$, $\forall\ u, v \in V^n$, где $\left\langle u, v\right\rangle = \frac{1}{2}\left(Q\left(u + v\right) - Q\left(u\right) - Q\left(v\right)\right)$ — симметричная билинейная форма, связанная при заданной Q. Произведение ортонормированных базисных векторов антикоммутативно: $e_j e_k + e_k e_j = 2\left\langle e_j, e_k\right\rangle = 0 \to e_j e_k = -e_k e_j$, $\forall\ j \neq k$.

Скалярное умножение и сумма в G_n определяются аналогично векторному пространству. Геометрическое произведение базисных элементов в G_n будет обозначаться сопоставлением; из двух базисных векторов e_j и e_k получается новый элемент алгебры $e_j e_k = e_{jk}$. Существуют неотрицательные целые числа p, q, r, такие что $n = p + q + r$ и геометрическое произведение:

$$e_i e_i = e_i^2 = \begin{cases} +1, & \text{если } i = 1, \ldots, p, \\ -1, & \text{если } i = p+1, \ldots, p+q, \\ 0, & \text{если } i = p+q+1, \ldots, n, \end{cases}$$

при этом геометрическая алгебра Клиффорда обозначается $G(p, q, r)$. Квадратичная форма невырожденной геометрической алгебры $G(p, q, 0)$ может быть представлена в форме

$$Q\left(v\right) = v_1^2 + \ldots + v_p^2 - v_{p+1}^2 - \ldots - v_{p+q}^2,$$

где $n = p + q$ — размерность векторного пространства.

При известной квадратичной форме Q для алгебры $G(p, q, s)$ могут быть построены базисные элементы и соотношения для коммутаторов этих элементов при любых $p \geqslant 0, q \geqslant 0, r \geqslant 0$. Для определения результатов умножения элементов алгебры $G(p, q, s)$ можно использовать Clifford Multivector Toolbox [17–20].

Рассмотрим алгебру $G(3, 0, 0)$ с базисными элементами 1, e_1, e_2, e_3, e_{12}, e_{13}, e_{23}, $e_{123} \equiv I$, $I^2 = -1$. Приведем результаты геометрических произведений базисных

элементов алгебры $G(3,0,0)$, где $e_0 = 1$:

$$\begin{array}{c} \\ e_0 \\ e_1 \\ e_2 \\ e_3 \\ e_{12} \\ e_{13} \\ e_{23} \\ e_{123} \end{array} \begin{array}{c} \begin{array}{cccccccc} e_0 & e_1 & e_2 & e_3 & e_{12} & e_{13} & e_{23} & e_{123} \end{array} \\ \left[\begin{array}{cccccccc} e_0 & e_1 & e_2 & e_3 & e_{12} & e_{13} & e_{23} & e_{123} \\ e_1 & e_0 & e_{12} & e_{13} & e_2 & e_3 & e_{123} & e_{23} \\ e_2 & -e_{12} & e_0 & e_{23} & -e_1 & -e_{123} & e_3 & -e_{13} \\ e_3 & -e_{13} & -e_{23} & e_0 & e_{123} & -e_1 & -e_2 & e_{12} \\ e_{12} & -e_2 & e_1 & e_{123} & -e_0 & -e_{23} & e_{13} & -e_3 \\ e_{13} & -e_3 & -e_{123} & e_1 & e_{23} & -e_0 & -e_{12} & e_2 \\ e_{23} & e_{123} & -e_3 & e_2 & -e_{13} & e_{12} & -e_0 & -e_1 \\ e_{123} & e_{23} & -e_{13} & e_{12} & -e_3 & e_2 & -e_1 & -e_0 \end{array}\right] \end{array}.$$

Элементы алгебр Клиффорда имеют более компактную запись и показывают меньшее время выполнения умножений во многих сопоставимых операциях по сравнению с умножениями матриц. Число базисных элементов алгебры $G(p,q,s)$ равно $2^{(p+q+s)}$, а число элементов группы матриц $GL_n(\mathbb{R})$ равно n^2.

При исходных элементах алгебры $G(3,0,0)$

$$A = 15 + 57e_1 + 93e_2 + 137e_3 + 172e_{12} + 202e_{13} + 231e_{23} + 245e_{123},$$
$$B = 23 + 253e_1 + 215e_2 + 179e_3 + 144e_{12} + 105e_{13} + 72e_{23} + 41e_{123}$$

и многочленах

$$f(x) = 13x^7 + 7x^4 + 11, \quad h(x) = 11x^7 + 5x^3 + 13$$

получим следующие результаты:

$$\tilde{A} = 0.032e_0 + 0.123e_1 + 0.201e_2 + 0.296e_3 + 0.371e_{12} + 0.436e_{13} + 0.499e_{23} + 0.529e_{123},$$
$$\tilde{B} = 0.054e_0 + 0.594e_1 + 0.505_{e2} + 0.420_{e3} + 0.338e_{12} + 0.247e_{13} + 0.169e_{23} + 0.096e_{123},$$
$$m = 4, \quad n = 3,$$
$$\tilde{f}(\tilde{A}) = -0.057e_0 - 0.31e_1 - 0.006e_2 - 0.414e_3 - 0.215e_{12} - 0.471e_{13} - 0.398e_{23} - 0.551e_{123},$$
$$r_A = 0.678e_0 + 0.48e_1 - 0.602e_2 + 0.278e_3 - 0.553e_{12} - 0.002e_{13} - 0.443e_{23} - 0.542e_{123},$$
$$\tilde{h}(\tilde{A}) = -0.144e_0 - 0.406e_1 + 0.101e_2 - 0.47e_3 - 0.124e_{12} - 0.4808e_{13} - 0.3345e_{23} - 0.475e_{123},$$
$$r_B = -0.460e_0 - 0.382e_1 + 0.013e_2 - 0.429e_3 - 0.227e_{12} - 0.469e_{13} - 0.391e_{23} - 0.552e_{123},$$
$$k_A = k_B = -0.615e_0 - 0.457e_1 + 0.402e_2 - 0.338e_3 + 0.275e_{12} - 0.18e_{13} + 0.119e_{23} + 0.122e_{123},$$
$$(k_A \cdot 256) \pmod{256} = (k_B \cdot 256) \pmod{256} =$$
$$= -157 - 117e_1 + 103e_2 - 87e_3 + 70e_{12} - 46e_{13} + 30e_{23} + 31e_{123}.$$

Аналогичные модели протоколов DH могут быть построены для алгебр Клиффорда $G(p,q,s)$, $\forall\ p,q,s \in \mathbb{Z}^+$. Обеспечение безопасности алгоритма с использованием алгебр $G(p,q,s)$ основано на некоммутативной структуре этих алгебр и возможности работы при любых больших значениях $n = p + q + s$.

Заключение

В работе представлена модель протокола Диффи – Хеллмана с использованием алгебраической структуры алгебры Клиффорда, к которым относятся кватернионы,

и структуры кольца многочленов. Обеспечение безопасности алгоритма с использованием алгебр Клиффорда основано на некоммутативной структуре этих алгебр и возможности работы в пространстве любой размерности.

Так же как матричные полиномы и группы кос, группы алгебры Клиффорда обладают некоммутативными структурами. Однако группы алгебры Клиффорда, кватернионы и октонионы имеют более компактную запись и показывают меньшее время выполнения во многих сопоставимых операциях. Использование в качестве коэффициентов элементов алгебр Клиффорда и показателей степеней целых чисел $\mathbb{Z}^+$ (например, $\mathbb{Z}_{256}$) позволяет понизить требование к регистрам процессоров (не использовать процессоры с плавающей запятой) и повысить производительность формирования протокола.

Список литературы

1. *Diffie W., Hellman M. E.* New directions in cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22, № 6. P. 644–654. https://doi.org/10.1109/TIT.1976.1055638
2. *Anshel I., Anshel M., Goldfeld D.* An algebraic method for public-key cryptography // Mathematics Research Letter. 1999. Vol. 6, № 3. P. 287–291. http://dx.doi.org/10.4310/MRL.1999.v6.n3.a3
3. *Hecht P.* Un modelo compacto de criptografia asimetrica empleando anillos no conmutativos // Actas del V Congreso Iberoamericano de Seguridad Informatica CIBSI'09. 2009. P. 188–201.
4. *Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, Choonsik Park.* New public-key cryptosystem using braid group // Advances in Cryptology — CRYPTO 2000 / ed. M. Bellare. Berlin, Heidelberg : Springer, 2020. P. 166–183. (Lecture Notes in Computer Science, vol. 1880). https://doi.org/10.1007/3-540-44598-6_10
5. *Miasnikov A. G., Shpilrain V., Ushakov A.* Non-Commutative Cryptography and Complexity of Group-Theoretic Problems. AMS, 2011. 385 p. (Mathematical Surveys and Monographs, vol. 177).
6. *Kamlofsky J. A., Hecht J. P., Masih S., Izzi O.* A Diffie – Hellman compact model over non-commutative rings using quaternions // MEMORIAS CIBSI 2015 (VIII Congreso Iberoamericano de Seguridad Informatica). Quito, Ecuador, 2015. 6 p. https://doi.org/10.13140/RG.2.1.4063.1760
7. *Bayro-Corrochano E.* Geometric Algebra Applications : in 2 vols. Vol. 1 : Computer Vision, Graphics and Neurocomputing. Springer, 2020. 742 p. https://doi.org/10.1007/978-3-319-74830-6
8. *Bayro-Corrochano E.* Geometric Algebra Applications : in 2 vols. Vol. 2 : Robot Modelling and Control. Springer, 2020. 600 p. https://doi.org/10.1007/978-3-030-34978-3
9. *Hamilton W. R.* Elements of Quaternions. London, UK : Longmans, Green, & Co, 1866. 762 p.
10. *Бранец В. Н., Шмыглевский И. П.* Введение в теорию бесплатформенных инерциальных навигационных систем. Москва : Наука, 1992. 280 с.
11. *Челноков Ю. Н.* Кватернионная регуляризация в небесной механике и астродинамике и управление траекторным движением. I // Космические исследования. 2013. Т. 51, № 5. С. 389–401. https://doi.org/10.7868/S0023420613050026
12. *Челноков Ю. Н.* Кватернионная регуляризация в небесной механике и астродинамике и управление траекторным движением. II // Космические исследования. 2014. Т. 52, № 4. С. 322–336. https://doi.org/10.7868/S0023420614030029
13. *Челноков Ю. Н.* Кватернионная регуляризация в небесной механике и астродинамике и управление траекторным движением. III // Космические исследования. 2015. Т. 53, № 5. С. 430–446. https://doi.org/10.7868/S0023420615050040

14. *Baez J. C.* The octonions // Bulletin of the American Mathematical Society. 2002. Vol. 39, № 2. P. 145–205.
15. *Clifford W. K.* Applications of Grassmann's extensive algebra // American Journal of Mathematics. 1878. Vol. 1, № 4. P. 350–358. https://doi.org/10.2307/2369379
16. *Clifford W. K.* Preliminary sketch of biquaternions // Proceedings of the London Mathematical Society. 1873. Vol. s1-4, iss. 1. P. 381–395. https://doi.org/10.1112/plms/s1-4.1.381
17. Clifford Multivector Toolbox. URL: http://clifford-multivector-toolbox.sourceforge.net/ (дата обращения: 15.07.2020).
18. *Sangwine S. J., Hitzer E.* Clifford multivector toolbox (for MATLAB) // Advances in Applied Clifford Algebras. 2017. Vol. 27, iss. 1. P. 539–558. https://doi.org/10.1007/s00006-016-0666-x
19. *Mann S., Dorst L., Bouma T.* The making of GABLE: A geometric algebra package in Matlab // Geometric Algebra with Applications in Science and Engineering / eds. E. Bayro-Corrochano, G. Sobczyk. Boston : Birkhäuser, 2001. P. 491–511. https://doi.org/10.1007/978-1-4612-0159-5_24
20. *Ablamowicz R., Fauser B.* Clifford/Bigebra, a Maple package for Clifford (co)algebra computations. URL: http://www.math.tntech.edu/rafal/ (дата обращения: 15.07.2020).

References

1. Diffie W., Hellman M. E. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976, vol. 22, no. 6, pp. 644–654. https://doi.org/10.1109/ TIT.1976.1055638
2. Anshel I., Anshel M., Goldfeld D. An algebraic method for public-key cryptography. *Mathematics Research Letter*, 1999, vol. 6, no. 3, pp. 287–291. http://dx.doi.org/0.4310/MRL.1999.v6.n3.a3
3. Hecht P. Un modelo compacto de criptografia asimetrica empleando anillos no conmutativos. *Actas del V Congreso Iberoamericano de Seguridad Informatica CIBSI'09*, 2009. pp. 188–201.
4. Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, Choonsik Park. New public-key cryptosystem using braid group. In: M. Bellare, ed. *Advances in Cryptology — CRYPTO 2000*. (Lecture Notes in Computer Science, vol. 1880). Springer, Berlin, Heidelberg, 2020, pp. 166–183. https://doi.org/10.1007/3-540-44598-6_10
5. Miasnikov A. G., Shpilrain V., Ushakov A. *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*. (Mathematical Surveys and Monographs, vol. 177). AMS, 2011. 385 p.
6. Kamlofsky J. A., Hecht J. P., Masih S., Izzi O. A Diffie – Hellman compact model over non-commutative rings using quaternions. *MEMORIAS CIBSI 2015* (VIII Congreso Iberoamericano de Seguridad Informatica). Quito, Ecuador, 2015. 6 p. (in Spain). https://doi.org/10.13140/RG.2.1.4063.1760
7. Bayro-Corrochano E. *Geometric Algebra Applications. Vol. 1: Computer Vision, Graphics and Neurocomputing*. Springer, 2020. 742 p. https://doi.org/10.1007/978-3-319-74830-6
8. Bayro-Corrochano E. *Geometric Algebra Applications. Vol. 2: Robot Modelling and Control*. Springer, 2020. 600 p. https://doi.org/10.1007/978-3-030-34978-3
9. Hamilton W. R. *Elements of Quaternions*. London, UK, Longmans, Green, & Co, 1866. 762 p.
10. Branets V N., Shmyglevsky I. P. *Vvedenie v teoriiu besplatformennoi inertsial'noi navigatsionnoi sistemy* [Introduction to the Theory of Strapdown Inertial Navigation System]. Moscow, Nauka, 1992. 280 p. (in Russian).
11. Chelnokov Yu. N. Quaternion regularization in celestial mechanics and astrodynamics and trajectory motion control. I. *Cosmic Research*, 2013, vol. 51, iss. 5, pp. 350–361. https://doi.org/10.1134/S001095251305002X

12. Chelnokov Yu. N. Quaternion regularization in celestial mechanics and astrodynamics and trajectory motion control. II. *Cosmic Research*, 2014, vol. 52, iss. 4, pp. 304–317. https://doi.org/10.1134/S0010952514030022
13. Chelnokov Yu. N. Quaternion regularization in celestial mechanics and astrodynamics and trajectory motion control. III. *Cosmic Research*, 2015, vol. 53, iss. 5, pp. 394–4097. https://doi.org/10.1134/S0010952515050044
14. Baez J. C. The octonions. *Bulletin of the American Mathematical Society*, 2002, vol. 39, no. 2, pp. 145–205.
15. Clifford W. K. Applications of Grassmann's extensive algebra. *American Journal of Mathematics*, 1878, vol. 1, no. 4, pp. 350–358. https://doi.org/10.2307/2369379
16. Clifford W. K. Preliminary sketch of biquaternions. *Proceedings of the London Mathematical Society*, 1873, vol. s1-4, iss. 1, pp. 381–395. https://doi.org/10.1112/plms/s1-4.1.381
17. *Clifford Multivector Toolbox*. Available at: http://clifford-multivector-toolbox.sourceforge.net/ (accessed 15 July 2020).
18. Sangwine S. J., Hitzer E. Clifford multivector toolbox (for MATLAB). *Advances in Applied Clifford Algebras*, 2017, vol. 27, iss. 1. pp. 539–558. https://doi.org/10.1007/s00006-016-0666-x
19. Mann S., Dorst L., Bouma T. The making of GABLE: A geometric algebra package in Matlab. In: E. Bayro-Corrochano, G. Sobczyk, eds. *Geometric Algebra with Applications in Science and Engineering*. Boston, Birkhauser, 2001, pp. 491–511. https://doi.org/10.1007/978-1-4612-0159-5_24
20. Ablamowicz R., Fauser B. *Clifford/Bigebra, a Maple package for Clifford (co)algebra computations*. Available at: http://www.math.tntech.edu/rafal/ (accessed 15 July 2020).

Поступила в редакцию / Received 18.07.2020
Принята к публикации / Accepted 03.05.2021
Опубликована / Published 31.08.2021