ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.55 ISSN 1995-5499
DOI: https://doi.org/10.17308/sait.2020.3/3037
Поступила в редакцию 15.08.2020
Подписана в печать 30.09.2020

ПЕРЕДАЧА СИГНАЛОВ С ШИФРОВАНИЕМ МЕТОДОМ ГЕОМЕТРИЧЕСКОЙ АЛГЕБРЫ

© 2020 С. Н. Чуканов✉

Институт математики им. С. Л. Соболева СО РАН, Омский филиал
ул. Певцова, 13, 644043 Омск, Российская Федерация

Аннотация. ВВ криптографических системах шифрования информации используются гиперкомплексные числа: кватернионы и октонионы. В качестве ключа применяется кватернион, который производит вращения группы выборок информации. Кватернионы и бикватернионы являются частными случаями геометрической алгебры Клиффорда. Использование векторов и мультивекторов геометрической алгебры для шифрования информации позволяет расширить разнообразие этих векторов. Для шифрования информации, представленной совокупностью векторов геометрической алгебры, эти векторы умножаются на мультивектора, которые осуществляют операцию ротор (rotor). В качестве ключа используется мультивектор (ротор). Для дешифрования информации применяется операция, которая соответствует обратному ротору. Алгоритмы геометрической алгебры повышают безопасность шифрования информации за счет повышения размерности алгебры. Для повышения производительности шифрования предлагается коэффициенты информационного вектора и мультивектора вращения выбирать из поля Z_{256}. Предлагается вектор информации с коэффициентами из Z_{256} складывать со случайным вектором с коэффициентами из Z_{256} и считать эти коэффициенты ключами шифрования. Приведены базисные векторы применяемых геометрических алгебр и таблицы геометрических произведений базисных векторов.

Ключевые слова: шифрование информации, кватернион, алгебра Клиффорда, геометрическая алгебра, мультивектор.

ВВЕДЕНИЕ

В криптографических системах кодирования используются гиперкомплексные числа: кватернионы и октонионы [1–5]. В работе Кузнецовой К. С., Духнича Е. И. [6, 7] рассматривается аппаратная реализация алгоритма шифрования на основе кватернионов. В качестве ключа в этих алгоритмах применяется кватернион, который используется для вращения группы выборок информации для шифрования. Благодаря кватернионной алгебре шифрование осуществляется быстрее, чем шифрование на основе умножения матриц.

Алгебраическая форма кватерниона q имеет вид [8, 9]: $q = w + xi + yj + zk$. Векторная часть V кватерниона содержит три вектора (i, j, k), которые образуют ортонормированный базис в $\mathbb{R}^3$. Эти векторы имеют коммутационные соотношения: $i^2 = j^2 = k^2 = -1$; $ij = -ji = k$; $jk = -kj = i$; $ki = -ik = j$. Сопряженный кватерниону q кватернион: $\tilde{q} = (w, -x, -y, -z)$, квадрат нормы кватерниона: $\|q\|^2 = w^2 + x^2 + y^2 + z^2$; обратный кватернион: $q^{-1} = \tilde{q} \cdot \|q\|^{-2}$. Рассмотрим кватернион вращения (ключ) $q = w + xi + yj + zk$ и кватер-

✉ Чуканов Сергей Николаевич
e-mail: ch_sn@mail.ru

нион данных, которые требуется зашифровать $P = ai + bj + ck$. Полученный кватернион после шифрования (вращения) P_{rot} записывается как: $P_{rot} = q \cdot P \cdot q^{-1}$.

1. ГЕОМЕТРИЧЕСКАЯ АЛГЕБРА

Кватернионы и бикватернионы являются частными случаями геометрической алгебры Клиффорда [10–13]. Для проведения операции вращения векторов в геометрической алгебре существует операция ротор (rotor). Использование векторов и мультивекторов геометрической алгебры для шифрования информации позволяет расширить разнообразие этих векторов, так как геометрическая алгебра может иметь любую размерность, а не только 4. Использование алгоритмов геометрической алгебры повышает безопасность шифрования информации за счет повышения размерности алгебры.

Рассмотрим 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 $G_n\left(V^n, Q\right)$ порождается V^n при условии $v^2 = Q(v), \forall v \in V^n$, где Q — квадратичная форма алгебры G_n. Это условие можно переписать в следующем виде: $uv + vu = 2\langle u, v\rangle, \forall u, v \in V^n$, где

$$\langle u, v\rangle = \frac{1}{2}\left(Q(u+v) - Q(u) - Q(v)\right), \qquad (1)$$

симметричная билинейная форма, связанная с Q. Произведение ортонормированных базисных векторов антикоммутативно:

$$e_j e_k + e_k e_j = 2\langle e_j, e_k\rangle = 0 \to e_j e_k = -e_k e_j, \forall j \neq k.$$

Скалярное умножение и сумма в G_n определяются аналогично векторному пространству. Геометрическое произведение базисных 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 [12, 13]:

$$e_i e_i = e_i^2 = \begin{cases} +1; i = 1, \ldots, p, \\ -1; i = p+1, \ldots, p+q, \\ 0; i = p+q+1, \ldots, n, \end{cases} \qquad (2)$$

при этом геометрическая алгебра Клиффорда обозначается $G_{p,q,r}$. Квадратичная форма невырожденной геометрической алгебры $G_{p,q,0}$ может быть представлены в форме:

$$Q(v) = v_1^2 + \ldots + v_p^2 - v_{p+1}^2 - \ldots - v_{p+q}^2, \qquad (3)$$

где $n = p + q + s$ – размерность векторного пространства.

При известной квадратичной форме Q для алгебры $G_{p,q,r}$ могут быть построены базисные элементы и соотношения для коммутаторов этих элементов при любых $p \geq 0, q \geq 0, r \geq 0$. Число базисных элементов алгебры $G_{p,q,r}$ равно $2^n = 2^{p+q+s}$. Для определения результатов некоммутативного умножения элементов алгебры $G_{p,q,r}$ можно использовать Clifford Multivector Toolbox [14–17] (см. Приложение).

2. ОПЕРАЦИЯ РОТОР В ГЕОМЕТРИЧЕСКОЙ АЛГЕБРЕ

Построение роторов в алгебре $G_{0,3}$ (или $G_{3,0}$) основано на том факте, что для любого вектора:

$$v = \sum_{i=1}^{3} a_i e_i; a_i \in \mathbb{R}; e_i \in G_{0,3},$$

и бивектора:

$$w = \sum_{j,k=1; j\neq k}^{3} a_{jk} e_{jk}; a_{jk} \in \mathbb{R}; e_{jk} \in G_{0,3},$$

произведение: $v' = w \cdot v \cdot w^{-1} = w \cdot v \cdot \tilde{w} \cdot \|w\|^{-2} \in G_{0,3}$ является вектором [9], где $\tilde{w}$ — реверсия бивектора w. Формирование вектора $v' = w \cdot v \cdot w^{-1}$ на основе бивектора w соответствует вращению вектора v на основе бивектора w. Бивектор w по отношению к вектору v в алгебре $G_{0,3}$ называется ротором.

В случае алгебры $G_{0,q}, q \geq 3$ (или $G_{p,0}, p \geq 3$) для вектора:

$$v = \sum_{i=1}^{q} a_i e_i; a_i \in \mathbb{R}; e_i \in G_{0,q},$$

можно построить мультивектор степени $q-1$:

$$w = \sum_{j,\ldots,k=1; j\neq k\ldots}^{q} a_{j\ldots k} e_{j\ldots k}; a_{j\ldots k} \in \mathbb{R}; e_{j\ldots k} \in G_{0,q}.$$

Тогда произведение:

$$v' = w \cdot v \cdot w^{-1} = w \cdot v \cdot \tilde{w} \cdot \|w\|^{-2} \in G_{0,q}, \qquad (4)$$

является вектором, где $\tilde{w}$ – реверсия мультивектора w. Будем называть мультивектор w

по отношению к вектору v в алгебре $G_{0,q}$ ротором.

Действие мультивектора w реализует вращение (rotation) вектора v; компоненты мультивектора w являются ключом для шифрования вектора v.

Пример 1. Запишем для алгебры $G_{0,4}$ вектор $P = 211e_1 + 313e_2 + 47e_3 + 53e_4$ и тривектор (ротор) $q = 14e_{123} + 13e_{134} + 7e_{234}$. Нормализуем q к единичной норме: $\tilde{q} = q \cdot \|q\|^{-1}$: $\tilde{q} = 0.688e_{123} + 0.639e_{134} + 0.344e_{234}$, и найдем реверсивный вектор $\tilde{q}_{rev} = \tilde{q}^{-1} = -0.688e_{123} - 0.639e_{134} - 0.344e_{234}$.

Тогда:

$$P' = q \cdot P \cdot q^{-1} =$$

$$= -323.744e_1 - 103.618e_2 - 47e_3 + 172.488e_4,$$

является вектором алгебры $G_{0,4}$. □

Для повышения производительности нахождения шифрованного вектора $P_{rot} = q \cdot P \cdot q^{-1}$ предлагается коэффициенты вектора P и мультивектора q выбирать из поля $\mathbb{Z}^+$; например, $\mathbb{Z}_{256}$. Тогда вектор P_{rot} можно определить из соотношения:

$$P_{rot} = q \cdot P \cdot \tilde{q} \cdot \|q\|^{-2}, \qquad (5)$$

Расшифровывание вектора P_{rot} производится из соотношения:

$$P = \tilde{q} \cdot P_{rot} \cdot q \cdot \|q\|^{-2}. \qquad (6)$$

Пример 2. Запишем для алгебры $G_{0,4}$ вектор $P = 113e_1 + 211e_2 + 37e_3$ и тривектор (ротор) $q = 123e_{123} + 134e_{134} + 234e_{234}$. Получим реверсию тривектора q: $\tilde{q} = -123e_{123} - 134e_{134} - 234e_{234}$ и P_{rot}: $P_{rot} = -122.761e_1 - 205.411e_2 - 37e_3 + 5.131e_4$. Расшифровывание вектора P_{rot}: $\tilde{q} \cdot P_{rot} \cdot q \cdot \|q\|^{-2} = 113e_1 + 211e_2 + 37e_3$, то есть отсутствуют ошибки расшифровывания. □

Для повышения безопасности шифрования вектор P с коэффициентами из $\mathbb{Z}_{256}$ можно сложить со случайным вектором $RV \in G_{0,q}$ с коэффициентами из $\mathbb{Z}_{256}$ и считать эти коэффициенты ключами шифрования. После получения шифрования: $P_{rot} = q \cdot P \cdot \tilde{q} \cdot \|q\|^{-2}$ и дешифрования $P = \tilde{q} \cdot P_{rot} \cdot q \cdot \|q\|^{-2}$ результат необходимо сложить с вектором $\overline{RV} \in G_{0,q}$ по модулю 256. Коэффициенты вектора $\overline{RV}$: b_i, могут быть получены из коэффициентов a_i вектора RV по формуле $b_i = (256 - a_i) (\mathrm{mod}\ 256)$.

Пример 3. Сложим вектор $P = 113e_1 + 211e_2 + 37e_3 \in G_{0,4}$ со случайным вектором $RV = 31e_1 + 12e_2 + 73e_3 \in G_{0,4}$ (для которого $\overline{RV} = 225e_1 + 244e_2 + 183e_3$). В результате получим $PRV = P + RV = 144e_1 + 223e_2 + 110e_3$ и шифрование вектора имеет вид:

$$P_{rot} = q \cdot PRV \cdot \tilde{q} \cdot \|q\|^{-2} =$$

$$= -123.68e_1 - 234.636e_2 - 110e_3 - 10.681e_4,$$

при $q = 123e_{123} + 134e_{134} + 234e_{234} \in G_{0,4}$.

Расшифровывание вектора: $\tilde{q} \cdot P_{rot} \cdot q \cdot \|q\|^{-2} + \overline{RV} = 113e_1 + 211e_2 + 37e_3$, совпадает с исходным вектором P. □

ПРИЛОЖЕНИЕ

Для определения результатов некоммутативного умножения элементов алгебры $G_{p,q,r}$ можно использовать Clifford Multivector Toolbox [14–17].

Алгебра кватернионов. Коммутационные соотношения Гамильтона для базисных единичных векторов кватерниона i, j, k: $ij = k = -ji, jk = i = -kj, ki = j = -ik$. Для определения результатов умножения кватернионов можно использовать табл. 1.

Таблица 1. Результаты произведений базисных элементов кватерниона [Table 1. The results of products of basic elements of the quaternion]

	1	i	j	k
1	1	i	j	k
i	i	−1	k	$-j$
j	j	$-k$	−1	i
k	k	j	$-i$	−1

Геометрическая алгебра $G_{0,3,0}$ имеет $2^{0+3+0} = 8$ базисных элементов: $e_0 = 1,\ e_1, e_2, e_3,\ e_{12}, e_{13}, e_{23},\ e_{123} = I$. Результаты геометрических произведений базисных элементов алгебры $G_{0,3,0}$ приведены в табл. 2.

Геометрическая алгебра $G^+_{3,0,0}$ имеет 4 базисных элемента: $e_0 = 1,\ e_{12}, e_{13}, e_{23}$. Результаты геометрических произведений базисных элементов алгебры $G^+_{3,0,0}$ приведены в табл. 3.

Таблица 2. Результаты произведений базисных элементов алгебры $G_{0,3,0}$
[Table 2. The results of products of basic elements of algebra $G_{0,3,0}$]

	e_0	e_1	e_2	e_3	e_{12}	e_{13}	e_{23}	e_{123}
e_0	e_0	e_1	e_2	e_3	e_{12}	e_{13}	e_{23}	e_{123}
e_1	e_1	$-e_0$	e_{12}	e_{13}	$-e_2$	$-e_3$	e_{123}	$-e_{23}$
e_2	e_2	$-e_{12}$	$-e_0$	e_{23}	e_1	$-e_{123}$	$-e_3$	e_{13}
e_3	e_3	$-e_{13}$	$-e_{23}$	$-e_0$	e_{123}	e_1	e_2	$-e_{12}$
e_{12}	e_{12}	e_2	$-e_1$	e_{123}	$-e_0$	e_{23}	$-e_{13}$	$-e_3$
e_{13}	e_{13}	e_3	$-e_{123}$	$-e_1$	$-e_{23}$	$-e_0$	e_{12}	$-e_2$
e_{23}	e_{23}	e_{123}	e_3	$-e_2$	e_{13}	$-e_{12}$	$-e_0$	$-e_1$
e_{123}	e_{123}	$-e_{23}$	e_{13}	$-e_{12}$	$-e_3$	$-e_2$	$-e_1$	e_0

Таблица 3. Результаты произведений базисных элементов алгебры $G^+_{3,0,0}$
[Table 3. The results of products of basic elements of algebra $G^+_{3,0,0}$]

	e_0	e_{12}	e_{13}	e_{23}
e_0	e_0	e_{12}	e_{13}	e_{23}
e_{12}	e_{12}	$-e_0$	$-e_{23}$	e_{13}
e_{13}	e_{13}	e_{23}	$-e_0$	$-e_{12}$
e_{23}	e_{23}	$-e_{13}$	e_{12}	e_0

Вводя обозначения $i = Ie_1 = e_2e_3$, $j = -Ie_2 = e_1e_3$, $k = Ie_3 = e_1e_2$, где тривектор $I = e_1e_2e_3$ является псевдоскалярной единицей ($I^2 = -1$), получим коммутационные соотношения Гамильтона: $i^2 = j^2 = k^2 = ijk = -1$, то есть алгебра $G^+_{3,0,0}$ изоморфна алгебре кватернионов.

Геометрическая алгебра $G_{0,4,0}$ имеет $2^{0+4+0} = 16$ базисных элементов: $e_0 = 1$, e_1, e_2, e_3, e_4, $e_{12}, e_{13}, e_{14}, e_{23}, e_{24}, e_{34}$, $e_{123}, e_{124}, e_{134}, e_{234}$, $e_{1234} = I$. Результаты геометрических произведений базисных элементов алгебры $G_{0,4,0}$ приведены в табл. 4.

ЗАКЛЮЧЕНИЕ

В работе рассматривается использование геометрических алгебр Клиффорда в криптографических системах шифрования информации. Кватернионы и бикватернионы являются частными случаями геометрической алгебры Клиффорда. В качестве ключа применяется мультивектор геометрической алгебры, который производит вращения группы выборок информации. Использование векторов и мультивекторов геометрической алгебры для шифрования информации позволяет расширить разнообразие этих векторов, так как размерности мультивектора геометрической алгебры может быть любой. Для шифрования информации, представленной совокупностью векторов геометрической алгебры, эти векторы умножаются на мультивектора, которые осуществляют операцию ротор (rotor). В качестве ключа используется мультивектор-ротор. Для дешифрования информации применяется операция, которая соответствует обратному ротору.

Для повышения производительности шифрования предлагается коэффициенты информационного вектора и мультивектора вращения выбирать из поля $\mathbb{Z}_{256}$. Предлагается вектор информации складывать со случайным вектором с коэффициентами из $\mathbb{Z}_{256}$ и считать эти коэффициенты ключами шифрования.

Алгоритмы с применением геометрических алгебр Клиффорда в криптографических системах шифрования информации могут быть использованы при передаче мультимедийной информации, изображений, звука, сигналов любой физической природы.

БЛАГОДАРНОСТИ

Работа выполнена при поддержке комплексной программы фундаментальных научных исследований СО РАН I.5.1.7, проект 0314-2016-0020. Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (гранты № 18-07-00526 и № 18-08-01284).

Таблица 4. Результаты произведений базисных элементов алгебры $G_{0,4,0}$
[Таблица 4. The results of products of basic elements of algebra $G_{0,4,0}$]

	e_0	e_1	e_2	e_3	e_4	e_{12}	e_{13}	e_{14}	e_{23}	e_{24}	e_{34}	e_{123}	e_{124}	e_{134}	e_{234}	e_{1234}
e_0	e_0	e_1	e_2	e_3	e_4	e_{12}	e_{13}	e_{14}	e_{23}	e_{24}	e_{34}	e_{123}	e_{124}	e_{134}	e_{234}	e_{1234}
e_1	e_1	$-e_0$	e_{12}	e_{13}	e_{14}	$-e_2$	$-e_3$	$-e_4$	e_{123}	e_{124}	e_{134}	$-e_{23}$	$-e_{24}$	$-e_{34}$	e_{1234}	$-e_{234}$
e_2	e_2	$-e_{12}$	$-e_0$	e_{23}	e_{24}	e_1	$-e_{123}$	$-e_{124}$	$-e_3$	$-e_4$	e_{234}	e_{13}	e_{14}	$-e_{1234}$	$-e_{34}$	e_{134}
e_3	e_3	$-e_{13}$	$-e_{23}$	$-e_0$	e_{34}	e_{123}	e_1	$-e_{134}$	e_2	$-e_{234}$	$-e_4$	$-e_{12}$	e_{1234}	e_{14}	e_{24}	$-e_{124}$
e_4	e_4	$-e_{14}$	$-e_{24}$	$-e_{34}$	$-e_0$	e_{124}	e_{134}	e_1	e_{234}	e_2	e_3	$-e_{1234}$	$-e_{12}$	$-e_{13}$	$-e_{23}$	e_{123}
e_{12}	e_{12}	e_2	$-e_1$	e_{123}	e_{124}	$-e_0$	e_{23}	e_{24}	$-e_{13}$	$-e_{14}$	e_{1234}	$-e_3$	$-e_4$	e_{234}	$-e_{134}$	$-e_{34}$
e_{13}	e_{13}	e_3	$-e_{123}$	$-e_1$	e_{134}	$-e_{23}$	$-e_0$	e_{34}	e_{12}	$-e_{1234}$	$-e_{14}$	e_2	$-e_{234}$	$-e_4$	e_{124}	e_{24}
e_{14}	e_{14}	e_4	$-e_{124}$	$-e_{134}$	$-e_1$	$-e_{24}$	$-e_{34}$	$-e_0$	e_{1234}	e_{12}	$-e_{13}$	e_{234}	e_2	e_3	$-e_{123}$	$-e_{23}$
e_{23}	e_{23}	e_{123}	e_3	$-e_2$	e_{234}	e_{13}	$-e_{12}$	e_{1234}	$-e_0$	e_{34}	$-e_{24}$	$-e_1$	e_{134}	$-e_{124}$	$-e_4$	$-e_{14}$
e_{24}	e_{24}	e_{124}	e_4	$-e_{234}$	$-e_2$	e_{14}	$-e_{1234}$	$-e_{12}$	$-e_{34}$	$-e_0$	e_{23}	$-e_{134}$	$-e_1$	e_{123}	e_3	e_{13}
e_{34}	e_{34}	e_{134}	e_{234}	e_4	$-e_3$	e_{1234}	e_{14}	$-e_{13}$	e_{24}	$-e_{23}$	$-e_0$	e_{124}	$-e_{123}$	$-e_1$	$-e_2$	$-e_{12}$
e_{123}	e_{123}	$-e_{23}$	e_{13}	$-e_{12}$	e_{1234}	$-e_3$	e_2	$-e_{234}$	$-e_1$	e_{134}	$-e_{124}$	e_0	$-e_{34}$	e_{24}	$-e_{14}$	e_4
e_{124}	e_{124}	$-e_{24}$	e_{14}	$-e_{1234}$	$-e_{12}$	$-e_4$	e_{234}	e_2	$-e_{134}$	$-e_1$	e_{123}	e_{34}	e_0	$-e_{23}$	e_{13}	$-e_3$
e_{134}	e_{134}	$-e_{34}$	e_{1234}	e_{14}	$-e_{13}$	$-e_{234}$	$-e_4$	e_3	e_{124}	$-e_{123}$	$-e_1$	$-e_{24}$	e_{23}	e_0	$-e_{12}$	e_2
e_{234}	e_{234}	$-e_{1234}$	$-e_{34}$	e_{24}	$-e_{23}$	e_{134}	$-e_{124}$	e_{123}	$-e_4$	e_3	$-e_2$	e_{14}	$-e_{13}$	e_{12}	e_0	$-e_1$
e_{1234}	e_{1234}	e_{234}	$-e_{134}$	e_{124}	$-e_{123}$	$-e_{34}$	e_{24}	$-e_{23}$	$-e_{14}$	e_{13}	e_{12}	$-e_4$	e_3	$-e_2$	e_1	e_0

КОНФЛИКТ ИНТЕРЕСОВ

Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Nagase, T.* Secure signals transmission based on quaternion encryption scheme / T. Nagase, M. Komata, T. Araki // Proc. 18th Int. Conf., Advanced Information Networking and Application (AINA 2004), Fukuoka, Japan, 2004. – T. 2. – P. 35–38.

2. *Nagase, T.* A new Quadripartite Public-Key Cryptosystem / T. Nagase, R. Koide, T. Araki, Y. Hasegawa // International Symposium on Communications and Information Technologies 2004 (ISCIT 2004). – Sapporo, Japan, 2004. – P. 74–79.

3. *Nagase, T.* Dispersion of sequences for generating a robust enciphering system / T. Nagase, R. Koide, T. Araki, Y. Hasegawa // Computer and Information Theory, 2005. – T. 1, No. 1. – P. 9–14.

4. *Dzwonkowski, M.* Quaternion encryption method for image and video transmission / M. Dzwonkowski, R. Rykaczewski // Telecom. Overv.+Telecom. News, 2013. – T. 8–9. – P. 1216–1220.

5. *Czaplewski, B.* Joint fingerprinting and decryption method for color images based on quaternion rotation with cipher quaternion chaining // J. Visual Commun. Image Representation, 2016. – T. 40, Part A – P. 1–13.

6. *Кузнецова, К. С.* Повышение скорости шифрования в кватернионных криптосистемах / К. С. Кузнецова, Е. И. Духнич // Вестник государственного морского университета им. адмирала Ф. Ф. Ушакова, 2017. – Т. 20, № 3. – С. 52–58.

7. *Кузнецова К. С.* Аппаратурно-ориентированный алгоритм кватернионной криптосистемы / К. С. Кузнецова, Е. И. Духнич // Известия ЮФУ. Технические науки, 2018. – Т. 202, № 8. – С. 182–190.

8. *Hamilton, W. R.* Elements of Quaternions. Edited by W.E. Hamilton. – London, UK: Longmans, Green, & Co., 1866. – 762 p.

9. *Dixon, G. M.* Division Algebras: Octonions, Quaternions, Complex Numbers and the Algebraic Design of Physics. – Dordrecht: Kluwer, 1994. – 236 p.

10. *Clifford, W. K.* Applications of Grassmann's extensive algebra // Amer. J. Math, 1878. – V. 1. – P. 350–358.

11. *Clifford W. K.* Preliminary sketch of bi-quaternions // Proceedings of the London Mathematical Society, 1873. – V. 4. – P. 381–395.

12. *Bayro-Corrochano, E.* Geometric Algebra Applications. T. I. / E. Bayro-Corrochano – Springer, 2019. – 742 p.

13. *Bayro-Corrochano E.* Geometric Algebra Applications. T. II. / E. Bayro-Corrochano – Springer, 2020. – 600 p.

14. Clifford Multivector Toolbox. – Режим доступа: http://clifford-multivector-toolbox.sourceforge.net. – (Дата обращения: 15.07.2020).

15. *Sangwine, S. J.* Clifford multivector toolbox (for MATLAB) / S. J. Sangwine, E. Hitzer // Advances in Applied Clifford Algebras, 2017. – Т. 1. – P. 539–558.

16. *Mann, S.* The making of GABLE: a geometric algebra package in Matlab / S. Mann, L. Dorst, T. Bouma. In E. Bayro Corrochano and G. Sobczyk, editors,Geometric Algebra with Applications in Science and Engineering. – Birkhauser, Boston, 2001. – P. 491–511.

17. *Ablamowicz, R.* Clifford/bigebra, a Maple package for Clifford (co)algebra computations / R. Ablamowicz, B. Fauser. – Режим доступа: http://www.math.tntech.edu/rafal. – (Дата обращения: 15.07.2020).

Чуканов Сергей Николаевич — д-р техн. наук, проф., ведущий научный сотрудник Института математики им. С. Л. Соболева СО РАН (Омский филиал).
E-mail: ch_sn@mail.ru
ORCID iD: https://orcid.org/0000-0002-8106-9813

DOI: https://doi.org/10.17308/sait.2020.3/3037 ISSN 1995-5499
Received 15.08.2020
Accepted 30.09.2020

TRANSMISSION OF GEOMETRIC ALGEBRA ENCRYPTED SIGNALS

© 2020 S. N. Chukanov✉

Sobolev Institute of Mathematics of the Siberian Branch of Russian Academy of Sciences, Omsk branch
13, Pevtsova Street, 644043 Omsk, Russian Federation

Annotation. Cryptographic systems of information encryption use hypercomplex numbers: quaternions and octonions. A quaternion is used as a key, which rotates a group of information samples. Quaternions and biquaternions are special cases of Clifford's geometric algebra. Using vectors and multivectors of geometric algebra to encrypt information allows us to expand the diversity of these vectors. To encrypt information represented by a set of geometric algebra vectors, these vectors are multiplied by multivectors that perform the rotor operation. A multivector (rotor) is used as a key. An operation corresponding to the reverse rotor is used to decrypt the information. Geometric algebra algorithms increase the security of information encryption by increasing the dimension of the algebra. To improve the encryption performance, it is proposed to select the coefficients of the information vector and the multivector of rotation from field Z_{256}. It is proposed to add a vector of information with coefficients from Z_{256} to a random vector with coefficients from Z_{256} and consider these coefficients as encryption keys. The article presents reference vectors of the applied geometric algebras and tables of geometric products of reference vectors.
Keywords: information encryption, quaternion, Clifford algebra, geometric algebra, multivector.

✉ Chukanov Sergey N.
e-mail: ch_sn@mail.ru

CONFLICT OF INTEREST

The author declare the absence of obvious and potential conflicts of interest related to the publication of this article.

REFERENCES

1. *Nagase T., Komata M., Araki T.* Secure signals transmission based on quaternion encryption scheme. Proc. 18th Int. Conf., Advanced Information Networking and Application (AINA 2004), Fukuoka, Japan. 2004. Vol. 2. P. 35–38.

2. *Nagase T., Koide R., Araki T., Hasegawa Y.* A new Quadripartite Public-Key Cryptosystem. International Symposium on Communications and Information Technologies 2004 (ISCIT 2004). Sapporo, Japan. 2004. P. 74–79.

3. *Nagase T., Koide R., Araki T., Hasegawa Y.* Dispersion of sequences for generating a robust enciphering system. Computer and Information Theory. 2005. 1(1). P. 9–14. DOI 10.37936/ecti-cit.200511.51826

4. *Dzwonkowski M., Rykaczewski R.* Quaternion encryption method for image and video transmission. Telecom. Overv.+Telecom. News. 2013. Vol. 8–9. P. 1216–1220.

5. *Czaplewski B.* Joint fingerprinting and decryption method for color images based on quaternion rotation with cipher quaternion chaining. J. Visual Commun. Image Representation. 2016. Vol. 40, Part A. 1–13. DOI 10.1016/j.jvcir.2016.06.006

6. *Kuznetsova K. S. , Dukhnich E. I.* Increasing the speed of encryption in quaternionic cryptosystems. Vestnik of Admiral Ushakov State Maritime University. 2017. 20(3). 52–58. (in Russian).

7. *Kuznetsova K. S., Dukhnich E. I.* Hardware-oriented algorithm of a quaternion cryptosystem. IZVESTIYA SFedU. ENGINEERING SCIENCES. 2018. 202(8). P. 182–190. (in Russian). DOI 10.23683/2311-3103-2018-8-182-190

8. *Hamilton W. R.* Elements of Quaternions. Edited by W.E. Hamilton. London, UK: Longmans, Green, & Co. 1866. 762 p.

9. *Dixon G. M.* Division Algebras: Octonions, Quaternions, Complex Numbers and the Algebraic Design of Physics. Kluwer, Dordrecht. 1994. 236 p.

10. *Clifford W. K.* Applications of Grassmann's extensive algebra. Amer. J. Math. 1878. Vol. 1. P. 350–358.

11. *Clifford W. K.* Preliminary sketch of bi-quaternions // Proceedings of the London Mathematical Society. 1873. V. 4. P. 381–395.

12. *Bayro-Corrochano E.* Geometric Algebra Applications. Vol. I. Springer. 2019. 742 p.

13. *Bayro-Corrochano E.* Geometric Algebra Applications. Vol. II. Springer. 2020. – 600 p.

14. Clifford Multivector Toolbox. Available at: http://clifford-multivector-toolbox.sourceforge.net. (Accessed 15, July, 2020).

15. *Sangwine S. J., Hitzer E.* Clifford multivector toolbox (for MATLAB). Advances in Applied Clifford Algebras 27. 2017. Vol. 1. P. 539–558.

16. *Mann S., Dorst L., Bouma T.* The making of GABLE: a geometric algebra package in Matlab. In E. Bayro Corrochano and G. Sobczyk, editors, Geometric Algebra with Applications in Science and Engineering. Birkhauser, Boston. 2001. P. 491–511.

17. *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).

Chukanov Sergey N. — DSc in Technical Sciences, Professor, leading researcher, Sobolev Institute of Mathematics of the Siberian Branch of Russian Academy of Sciences (Omsk branch).
E-mail: ch_sn@mail.ru
ORCID iD: https://orcid.org/0000-0002-8106-9813