Keywords: *Neural network, cyberattacks, model, efficiency, concept.*

УДК 004.942

Бояринова Ю.Є.
кандидат технических наук, старший научный сотрудник, доцент кафедры системного программирования и специализированных компьютерных систем НТУУ «КПИ» им. И.Сикорского

Калиновський Я.О.
доктор технических наук, старший научный сотрудник института проблем регистрации информации НАН Украины

Хицко Я.В.
кандидат технических наук, старший преподаватель кафедры системного программирования и специализированных компьютерных систем НТУУ «КПИ» им. И.Сикорского

ИСПОЛЬЗОВАНИЕ НЕКАНОНИЧЕСКИХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЛОВЫХ СИСТЕМ ДЛЯ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ

Аннотация. *Предложена модификация модулярной задачи разделения секрета, которая отличается от существующих представлением информации остатками в неканонических гиперкомплексных числових системах по совокупности неканонических гиперкомплексных модулей. Показано, что при использовании неканонической гиперкомплексной числовой системы размерности 4 для обеспечения такой же криптостойкости как и для канонической гиперкомплексной числовой системы размерности 6, количество необходимых вичислений уменьшается.*

Ключевые слова: *гиперкомплексная числовая система, неканоническая система, схема разделения секрета, криптостойкость*

Введение

Расширение круга задач в науке и технике требует развития и совершенствования методов математического моделирования, одним из

важных компонентов которого является форма представления информации и обработки данных.

Выбор формы представления данных оказывает существенное влияние на быстродействие алгоритмов. В свою очередь, вопрос быстродействия алгоритмов, работающих с большими объемами данных актуален и теперь. Для больших объемов информации, как правило, используют структурные формы представления массивов данных, которые для представления каждого элемента такого массива могут использовать любую форму. Существуют такие структурные формы представления данных как: векторно-матричная, полиномиальная, системы остаточных классов, а также гиперкомплексная [1-4].

Переход от вещественных параметров моделей к различным гиперкомплексным числовым системам является одним из методов повышения эффективности алгоритмов математического моделирования. Методы представления и обработки данных в гиперкомплексных числовых системах (ГЧС) дают преимущества, которые позволяют значительно повысить эффективность моделирования задач электротехники, аэродинамики, навигации, квантовой механики, теории колебаний, криптографии, обработки сигналов и многих других[5-8].

Анализ литературных данных и постановка проблемы

Примеры применения известных и широко используемых в теории гиперкомплексных числовых систем комплексных, двойных, дуальных чисел, кватернионов и др. для повышения эффективности алгоритмов в совершенно различных областях науки и техники известны достаточно давно. Среди них:

1. Для моделирования вращения и перемещения используются дуальные числа, бикватернионы и двойные кватернионы, которые нашли широкое применение в задачах моделирования и управления плоскими механизмами **[9-11 46-48]**, роботами и манипуляторами с многими степенями свободы **[12-14 49-51]** и даже моделировании скелета человека **[15 52]**.

Кватернионы эффективно используются в задачах управления ориентации твердого тела **[7 53]**. Вышеперечисленные преимущества позволяют использовать кватернионы для решения задач компьютерной графики и создания эффектов анимации **[16 56]**, обработки цветного изображения **[17 57]**. В таких работах, как **[18,19 58-59]** исследованы задачи деформации упругих и эластичных конструкций с использованием кватернионов.

2. Еще одной областью эффективного применения гиперкомплексной формы представления данных является криптография. Например, наряду с полиномиальной формой остаточных классов, может использоваться гиперкомплексная форма, в алгоритмах шифрования с открытым ключом. Таким образом, используя изоморфные переходы из вещественной системы в гиперкомплексную, можно строить в последней систему остаточных классов, и строить алгоритмы, которые будут обладать более высокой стойкостью.

Необходимо отметить, что гиперкомплексные числовые системы больших порядков, а особенно неканонические гиперкомплексные числовые системы, усложняют вычисления, как и сложный алгоритм изоморфного перехода из одной системы в другую. Поэтому ключевым моментом является выбор конкретной гиперкомплексной числовой системы, с представлением данных в которой, можно будет как существенно усилить криптографический алгоритм, так и минимизировать дополнительные затраты, связанные на его реализацию в гиперкомплексной числовой системе **[7,8, 16,17, 20 53-57].**

3. Широко применяются гиперкомплексные числа и для повышения эффективности цифровой обработки сигналов. Традиционно, в быстрых алгоритмах обработки сигналов могут использоваться комплексные коэффициенты для минимизации элементарных операций. Например, в работах **[21-24 65-74]** рассмотрены фильтры с гиперкомплексными коэффициентами, которые при равных условиях, обеспечивают работу фильтра на значительно высшей тактовой частоте, по сравнению с фильтром с вещественными коэффициентами.

Цель и задачи исследований

На протяжение многих лет исследовались канонические гиперкомплексные числовые системы. Так применение канонических ГЧС в задаче разделения секрета позволило значительно улучшить криптостойкость алгоритма (оценка криптостойкости зависит от размерности и вида числовой системы) **[25 34]**. Однако следует отметить, что увеличение криптостойкости задачи разделения секрета напрямую связано с увеличением размерности гиперкомплексной числовой системы, что увеличивает количество элементарных операций при реализации данной модели.

Поэтому актуальным является представление исходных данных в неканонических ГЧС и модификация модели разделения секрета, что может позволить увеличить криптостойкость алгоритма без наращивания размерности такой системы.

Сведения о гиперкомплексных числовых системах

Наряду с вышеупомянутыми структурными формами представления информации, особый интерес представляет гиперкомплексная форма представления данных.

С алгебраической точки зрения гиперкомплексная числовая система – это кольцо со структурой векторного пространства, то есть, гиперкомплексной числовой системой размерности n называется множество чисел такого вида:

$$A = a_1 E_1 + a_2 E_2 + .. + a_n E_n , \qquad (1)$$

с определенными правилами выполнения операций сложения и умножения.

Совокупность элементов

$$\{E_1, E_2, ..., E_n\} \tag{2}$$

называется базисом гиперкомплексной числовой системы или системы ее образующих.

Коэффициенты $A = a_1, a_2, ..., a_n$ могут принадлежать системам вещественных, комплексных или других гиперкомплексных чисел, в том числе и рассматриваемой гиперкомплексной числовой системе. В этом случае считается, что гиперкомплексная числовая система задана над соответствующей системой вещественных, комплексных чисел или другой числовой системой.

Для определения правил выполнения операции умножения, и, соответственно, полного задания гиперкомплексной числовой системы необходимо задать правила умножения элементов базиса (2), такие чтобы числовая система должна быть замкнута относительно этой операции.

В общем виде произведение двух базисных элементов из-за замкнутости системы относительно операции умножения должно представлять собой число такой же гиперкомплексной числовой системы вида (1):

$$E_i E_j = \sum_{k=1}^{n} \gamma_{ij}^k E_k \tag{3}$$

Коэффициенты γ_{ij}^k, которые называют структурными константами, являются вещественными числами: $\gamma_{ij}^k \in R$. При таком представлении для полного определения гиперкомплексной числовой системы необходимо задать n^3 структурных констант.

Простейшие операции в гиперкомплексной числовой системе это сложение и умножение. Сложение производится покомпонентно:

$$A + B = \sum_{i=1}^{n} (a_i + b_i) E_i. \tag{4}$$

В том случае, если в базисе присутствует единичный элемент системы, которым без ограничения общности можно считать элемент E_1.

Умножение гиперкомплексных чисел производится путем их перемножения как полиномов, подстановкой произведения базисных элементов по заданным правилам (1.3). В общем виде, произведение будет иметь вид:

$$A \cdot B = \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=1}^{n} a_i b_j \gamma_{ij}^k E_k. \tag{5}$$

При этом норма гиперкомплексного числа *a* определяется за формулой:

$$N(a) = \left\| (N(a))_{j,k} = \sum_{i=1}^{n} \gamma_{ij}^k a_i \right\|_{j,k=1...n} \tag{6}$$

Обозначим сопряженные гиперкомплексного числа как $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{n-1}}$, а их произведение как $\overline{a}$. В общем случае для сопряженных $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{n-1}}$ должно выполняться уравнение:

$$a \cdot \overline{a_1} \cdot \overline{a_2} \cdot \ldots \cdot \overline{a_{n-1}} = N(a) \cdot \xi, \tag{7}$$

где ξ – единичный элемент гиперкомплексной числовой системы. Или

$$a \cdot \overline{a} = N(a) \cdot \xi. \tag{8}$$

Допустим, что

$$\overline{a_k} = x_{1k} e_1 + x_{2k} e_2 + \ldots + x_{nk} e_n \tag{9}$$

Если приравнять выражения при одинаковых базисных элементах, получим систему из $(n\text{-}1)$ уравнений от $n(n\text{-}1)$ неизвестных **[26 76-81]**. Решить такую систему, не зная особенностей каждой конкретной числовой системы достаточно проблематично. Поэтому, если неизвестен вид сопряженных и система уравнений не имеет решения в действительных числах, можно найти, с учетом (7), произведение сопряженных

$$\overline{a} = x_1 E_1 + x_2 E_2 + \ldots + x_n E_n, \tag{10}$$

которое в основном и используется для вычислений.

Деление двух гиперкомплексных чисел производится с помощью формулы:

$$C = \frac{A}{B} = \frac{\sum_{i=1}^{n} a_i E_i}{\sum_{j=1}^{n} b_j E_j} = \frac{A \cdot \overline{B}}{B \cdot \overline{B}} = \frac{A \cdot \overline{B}}{N(B)}, \tag{11}$$

где $N(B)$ - норма знаменателя, а $\overline{B}$ - сопряженный знаменателю элемент.

Делителем нуля в неканонической гиперкомплексной числовой системе является число a, обладающее такими свойствами **[27 96]**:

- это число отлично от нуля: $a \neq 0$;
- существует такое отличное от нуля число b с этой же гиперкомплексной числовой системы Q, что произведение чисел a и b равняется нулю: $a \cdot b = 0; \quad a,b \neq 0; \quad a,b \in Q$.
- если a - делитель нуля, $\alpha \in \boldsymbol{R}$, то и αa также является делителем нуля.

В соответствии с теоремой Фробениуса **[4]**, поле вещественных чисел и поле комплексных чисел являются единственными конечномерными ассоциативно-коммутативными алгебрами без делителей нуля, тело кватернионов является единственной конечномерной ассоциативной, но не коммутативной алгеброй без делителей нуля, алгебра Кэли является единственной конечномерной альтернативной, но не ассоциативной алгеброй без делителей нуля.

Очевидно **[28 109]**, что норма делителя нуля равна нулю:

$$N(a \cdot b) = 0, \tag{12}$$

Таким образом, чтобы найти делителей нуля необходимо решить уравнение:

$$\left\| \sum_{i=1}^{n} \gamma_{ij}^{k} a_i \right\| = 0 . \tag{13}$$

В зависимости от свойств закона композиции, то есть операции умножения, множество гиперкомплексных чисел распадается на ряд классов **[1-2]**. Например, это класс коммутативных, некоммутативных и антикоммутативных гиперкомплексных числовых систем, для которых выполняется, соответственно:

$$\begin{aligned} &ab = ba, \quad && a,b \in \Gamma, \\ &ab \neq ba, \quad && a,b \in \Gamma, \\ &ab = -ba, \quad && a,b \in \Gamma . \end{aligned} \tag{14}$$

Перечисление неканонических гиперкомплексных числовых систем отличается от перечисления канонических систем. В каждой ячейке перебираются суммы структурных элементов, путем перебора коэффициентов при этих элементах **[29]**.

$E_{111} + E_{112} + \\ + \ldots + E_{11n}$	$E_{121} + E_{122} + \\ + \ldots + E_{12n}$	$\cdots$	$E_{1n1} + E_{1n2} + \\ + \ldots + E_{1nn}$
$E_{211} + E_{212} + \\ + \ldots + E_{21n}$	$E_{221} + E_{222} + \\ + \ldots + E_{22n}$	$\cdots$	$E_{2n1} + E_{2n2} + \\ + \ldots + E_{2nn}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$E_{n11} + E_{n12} + \\ + \ldots + E_{n1n}$	$E_{n21} + E_{n22} + \\ + \ldots + E_{n2n}$	$\cdots$	$E_{nn1} + E_{nn2} + \\ + \ldots + E_{nnn}$

где $E_{ijk} = C_{ij} \cdot E_k$, $C_{ij} \in \{-1,0,1\}$. Таким образом получаем 3^{n^3} числовых систем, $(2n+1)^{n^2}$ из которых являются каноническими.

Схема разделения секрета с представлением данных гиперкомплексными числами

Схема разделения секрета является методом, близким к криптографии с открытым ключом, который сводится к задаче модулярного разделения секрета. Суть этой задачи состоит в том, как сохранить секрет, разделив его на составные части между несколькими законными пользователями. Исходная постановка задачи и ее решение были предложены в 80-х годах прошлого

столетия Ч.Асмусом и Л.Блюмом **[30-32]**. Поскольку разделение секрета в неканонических ГЧС базируется на исходном алгоритме для вещественных чисел, приведем его в начальном виде.

Будем говорить, что n участников (законных пользователей) A_i, $i=1...n$ осуществляют k-хранение секрета C, $1<k\le K_n$, если выполняются следующие три условия.

1. Каждый A_i знает некоторую информацию a_i, неизвестную любому другому участнику.

2. Секрет C может быть легко вычислен на основе любых k секретов a_i.

3. Знание любых $k-1$ частичных секретов a_i не дает возможности восстановить информацию.

Множество $\{a_1...a_n\}$, удовлетворяющее этим условиям называется (n,k) пороговой схемой.

Пусть $m_1, m_2, ..., m_n$ – система попарно взаимно простых натуральных модулей. Предположим, что они упорядочены $m_1 < m_2 < ... < m_n$ и выполнено условие

$$M_2 = m_1 m_2 .. m_k > m_{n-k+1} m_{n-k+2} .. m_n = M_1 , \qquad (15)$$

а секрет взят из промежутка (M_1, M_2). Тогда часть секрета i-го участника a_i определяется наименьшим неотрицательным вычетом секрета x по модулю m_i. Получаем систему сравнений

$$x \equiv a_i (\mathrm{mod}\, m_i), i = 1..n. \qquad (16)$$

Любая подсистема из k сравнений данной системы имеет единственное решение в промежутке (M_1, M_2). Это решение можно найти, исходя из китайской теоремы об остатках или с помощью алгоритма, основанного на кодах со смешанными основаниями **[33]**.

Рассмотрим восстановление с помощью китайской теоремы, которая состоит в следующем **[34,35]**.

Выберем совокупность попарно взаимно простых модулей m_i, $i=1..n$. Имеем a_i, $i=1..n$ – произвольные целые числа, удовлетворяющие условиям $1 \le a_i < m_i$.

Обозначим через M произведение всех модулей m_i, $i=1..n$. Пусть далее

$$M_i = M / m_i . \qquad (17)$$

Обозначим через N_i-число, обратное M_i по модулю m_i, $i=1..n$.

Таким образом,

$$M_i N_i = 1 \pmod{m_i} . \qquad (18)$$

Система сравнений

$$x \equiv a_i (\mathrm{mod}\, m_i), \; i = 1...n \qquad (19)$$

обладает единственным решением по модулю M, которое можно найти следующим образом:

$$x = \sum_{i=1}^{n} a_i M_i N_i \,. \tag{20}$$

Пусть теперь k фиксировано, $1 < k \le n$. Обозначим через M_1 наименьшее произведение k различных модулей. Разместив модули в порядке возрастания, получим $M_1 = m_1 \times ... \times m_k$.

Обозначим через M_2 наибольшее произведение $k-1$ модулей. Модули следует выбирать так, чтобы разность $M_1 - M_2$ была велика:

$$M_1 - M_2 \ge 3M_2 \,. \tag{21}$$

Далее требуется, чтобы $M_2 < c < M_1$. В качестве секретов участников a_i возьмем наименьшие неотрицательные вычеты секрета c по модулю m_i, так что

$$a_i \equiv c \,(\mathrm{mod}\, m_i), i = 1,..., n \,. \tag{22}$$

Можно утверждать, что множество $a_1,\ldots, a_t$ есть (n,k)-пороговая схема для секрета C.

Доказательством этому является следующее. Пусть, например, известны $a_1,\ldots, a_k$. Далее вычислим $M' = m_1 \times ... \times m_k$, $M'_i = M'/m_i, i = 1...k$ и тогда N'_i обратно к M_i по модулю m_i. Тогда можно вычислить

$$y = \sum_{i=1}^{k} a_i M'_i N'_i \,. \tag{23}$$

В соответствии с китайской теоремой об остатках

$$y \equiv c \,(\mathrm{mod}\, M') \,. \tag{24}$$

по имеющейся совокупности линейных сравнений может быть определена искомая величина.

Так как $M' \ge M_1 > C$, то C равно наименьшему неотрицательному вычету y по модулю M', что дает способ вычисления, исходя из $a_1,\ldots, a_k$.

Теперь предположим, что известны лишь $a_1,\ldots, a_{k-1}$. Тогда

$$y \equiv c \,(\mathrm{mod}\, m_1 \times ... \times m_{k-1}). \tag{25}$$

Но это оставляет много возможностей для выбора C. Таким образом, необходимо k секретов для полного восстановления исходной информации.

Схема разделения секрета в неканонической гиперкомплексной числовой системе

Пусть задана неканоническая гиперкомплексная числовая система 3-й размерности.

E_1	E_2	E_3
E_2	$-E_1 - 2E_2$	$E_1 + E_2 - E_3$

(26)

E_3	$E_1 + E_2 - E_3$	$-E_1 + 2E_3$

Секрет *C* имеет вид :

$$C = -47E_1 - 19E_2 + 53E_3 .$$

Выберем три взимнопростых модуля, т.е. такие модули, нормы которых являются взаимно простыми.

$$\begin{aligned} m_1 &= E_1 - 2E_2 ,\ N(m_{1)}) = 27, \\ m_3 &= -3E_2 + E_3 ,\ N(m_{3)}) = 64, \\ m_2 &= 5E_3 ,\ \ N(m_{2)}) = 125. \end{aligned} \qquad (27)$$

Покажем область представимости секрета. В гиперкомплексных числовых системах область представимости секрета определяется как диапазон $0...N(M)$, где $N(M)$ – норма величины *M*, а *M* в свою очередь определяется соотношением:

$$M = \prod_{i=1}^{n} m_i . \qquad (28)$$

При этом должно выполняться условие $0 < N(C) < N(M)$.

Соответственно, для данной системы, секрета и выбранных модулей:

$$M = -100E_1 - 85E_2 + 75E_3 ,\ N(M) = 216000,$$
$$N(C) = 15625.$$

Как видим, заданный секрет может быть представлен совокупностью вычетов по выбранным модулям. Вычеты в свою очередь будут равны:

$$\begin{aligned} a_1 &\equiv (-47E_1 - 19E_2 + 53E_3)(\mathrm{mod} E_1 - 2E_2) = -E_1 + 2E_3 , \\ a_2 &\equiv (-47E_1 - 19E_2 + 53E_3)(\mathrm{mod} - 3E_2 + E_3) = -3E_1 - 4E_2 + 4E_3 , \\ a_3 &\equiv (-47E_1 - 19E_2 + 53E_3)(\mathrm{mod} 5E_3) = -2E_1 + E_2 + 3E_3 . \end{aligned} \qquad (29)$$

Таким образом секрет *C*, представленный в неканонической гиперкомплексной числовой системе может быть представлен совокупностью вычетов (29) по модулям (27).

Восстановим секрет с помощью китайской теоремы об остатках. Вычислим систему сравнений:

$$\begin{aligned} M_1 N_1 &\equiv 1(\mathrm{mod} m_1) , \\ M_2 N_2 &\equiv 1(\mathrm{mod} m_2) , \\ &\cdots \\ M_n N_n &\equiv 1(\mathrm{mod} m_n) , \end{aligned}$$

где $M_i = M / m_i$, N_i – искомые числа, обратные M_i по модулю m_i, $i = 1...n$.

Для вычисления числа N_i в области вещественных чисел можно использовать функцию Эйлера :

$$N_i = M_i^{\varphi(m_i)-1} (\mathrm{mod} m_i) ,$$

которая рассмотрена только для поля вещественных чисел.

Для определения N_i наряду с применением функции Эйлера можно использовать и другие подходы. Это восстановление с использованием изоморфного перехода на основе фундаментальной теоремы Гаусса и ее модификациях , а также с применением алгоритма Евклида, который был описан ранее.

Итак, для выбранных модулей, система сравнений будет иметь вид:

$$\begin{aligned}(-20E_1-15E_2+25E_3)N_1 &\equiv E_1(\mathrm{mod}\,E_1-2E_2),\\ (-10E_1-10E_2+15E_3)N_2 &\equiv E_1(\mathrm{mod}-3E_2+E_3),\\ (-8E_1-17E_2+3E_3)N_3 &\equiv E_1(\mathrm{mod}5E_3).\end{aligned} \qquad (30)$$

Выполняем последовательно шаги алгоритма Евклида для каждого из сравнений:

1) $(-20E_1-15E_2+25E_3)N_1 \equiv E_1(\mathrm{mod}\,E_1-2E_2)$,

Инициализируем начальные значения:

$r_0=-20E_1-15E_2+25E_3$, $x_0=E_1$, $y_0=0$,

$r_1=E_1-2E_2$, $x_1=0$, $y_1=E_1$.

Находим промежуточные значения:

$$\frac{r_0}{r_1}=\frac{-20E_1-15E_2+25E_3}{E_1-2E_2}=\frac{-60E_1-15E_2+225E_3}{27},$$

$-60\mathrm{mod}(27)\equiv -6$, $-15\mathrm{mod}(27)\equiv 12$, $225\mathrm{mod}(27)\equiv 9$,

$$=> r_2=\frac{(-6E_1+12E_2+9E_3)(E_1-2E_1)}{27}=2E_2+E_3,$$

$$q_1=\frac{-20E_1-17E_2+24E_3}{E_1-2E_1}=-2E_1-E_2+8E_3,$$

$x_2=x_0-q_1x_1=E_1-(-2E_1-E_2+8E_3)*0=E_1$,

$N(r_2)=-1$,

$N_1=X=x_2/(2E_2+E_3)=-2E_1-2E_2-E_3$.

2) $(-10E_1-10E_2+15E_3)N_2 \equiv E_1(\mathrm{mod}-3E_2+E_3)$,

Инициализируем начальные значения:

$r_0=-10E_1-10E_2+15E_3$, $x_0=E_1$, $y_0=0$,

$r_1=-3E_2+E_3$, $x_1=0$, $y_1=E_1$.

Находим промежуточные значения:

$$\frac{r_0}{r_1}=\frac{-10E_1-10E_2+15E_3}{-3E_2+E_3}=\frac{80E_1+20E_2+180E_3}{64},$$

$80\mathrm{mod}(64)\equiv 16$, $20\mathrm{mod}(64)\equiv 20$, $180\mathrm{mod}(64)\equiv 52$,

$$=> r_2=\frac{(16E_1+20E_2+52E_3)(-3E_2+E_3)}{64}=-2E_1-E_2+4E_3,$$

$$q_1=\frac{-8E_1-9E_2+11E_3}{-3E_2+E_3}=E_1+2E_3,$$

$x_2=x_0-q_1x_1=E_1-(E_1+2E_3)\cdot 0=E_1$,

$$\frac{r_1}{r_2}=\frac{-3E_2+E_3}{-2E_1-E_2+4E_3}=\frac{60E_1-15E_2-39E_3}{27}$$

$60\bmod(27)\equiv 6,\quad -15\bmod(27)\equiv 12,\quad -39\bmod(27)\equiv -12,$

$$\Rightarrow r_3=\frac{(6E_1+12E_2-12E_3)(-2E_1-E_2+4E_3)}{27}=4E_1+2E_2-4E_3,$$

$$q_2=\frac{-4E_1-5E_2+5E_3}{-2E_1-E_2+4E_3}=2E_1-E_2-E_3,$$

$$x_3=x_1-q_2x_2=0-(2E_1-E_2-E_3)*E_1=-2E_1+E_2+E_3,$$

$$\frac{r_2}{r_3}=\frac{-2E_1-E_2+4E_3}{4E_1+2E_2-4E_3}=\frac{28E_1+8E_2-8E_3}{-8},$$

$28\bmod(-8)\equiv 4,\quad 8\bmod(-8)\equiv 0,\quad -8\bmod(-8)\equiv 0,$

$$\Rightarrow r_4=\frac{(4E_1)(4E_1+2E_2-4E_3)}{-8}=-2E_1-E_2+2E_3,$$

$$q_3=\frac{-6E_1-E_2+4E_3}{4E_1+2E_2-4E_3}=-3E_1-E_2+E_3,$$

$$x_4=x_2-q_3x_3=-2E_1-E_2+4E_3-$$

$$-(-3E_1-E_2+E_3)(-2E_1+E_2+E_3)=-8E_1-2E_2+5E_3,$$

$N(r_4)=1,$

$N_2=X=x_4/(-2E_1-E_2+2E_3)=-8E_1-2E_2+5E_3.$

3) $(-8E_1-17E_2+3E_3)N_3\equiv E_1(\bmod 5E_3),$

Инициализируем начальные значения:

$r_0=-8E_1-17E_2+3E_3,\qquad x_0=E_1,\qquad y_0=0,$

$r_1=5E_3,\qquad x_1=0,\qquad y_1=E_1.$

Находим промежуточные значения:

$$\frac{r_0}{r_1}=\frac{-8E_1-17E_2+3E_3}{5E_3}=\frac{100E_1-425E_2-225E_3}{125}$$

$100\bmod(125)\equiv 25,\quad -425\bmod(125)\equiv 75,\quad -225\bmod(125)\equiv 25,$

$$\Rightarrow r_2=\frac{(25E_1+75E_2+25E_3)(5E_3)}{125}=2E_1+3E_2+3E_3,$$

$$q_1=\frac{-10E_1-20E_2}{5E_3}=-4E_2-2E_3,$$

$$x_2=x_0-q_1x_1=E_1-(-4E_2-2E_3)\cdot 0=E_1,$$

$$\frac{r_1}{r_2}=\frac{5E_3}{2E_1+3E_2+3E_3}=\frac{-30E_2-10E_3}{8}$$

$-30\bmod(8)\equiv 2,\quad -10\bmod(8)\equiv -2,$

$$\Rightarrow r_2=\frac{(2E_2-2E_3)(2E_1+3E_2+3E_3)}{8}=-E_2-2E_3,$$

$N(r_2)=-1,$

$x_2=x_0-qx_1=E_1-(-E_2-2E_3)\cdot 0=E_1,$

$N_3 = X = x_2 /(-E_2 - 2E_3) = 3E_1 - 7E_2 - 7E_3$.

$Y = a_1 M_1 N_1 + a_2 M_2 N_2 + a_3 M_3 N_3 = -387E_1 - 29E_2 + 263E_3$.

Тогда секрет C будет равен:

$$C \equiv Y(\mathrm{mod} M) = (-387E_1 - 29E_2 + 263E_3)(\mathrm{mod} -100E_1 - 85E_2 + 75E_3) =$$
$$= -47E_1 - 19E_2 + 53E_3$$

Определение вычислительную сложность задачи разделения секрета с гиперкомплексными числами

Рассмотрим вычислительную сложность задачи разделения секрета для канонической гиперкомплексной числовой системы размерности n и $n+1$, а также неканонической гиперкомплексной числовой системы размерности n с одной составной и $(n-1)^2$ составными ячейками. При этом предполагается, что у данных систем единичный элемент в базисе.

Таблица 1

Вычислительная сложность задачи разделения секрета в ГЧС

Вид ГЧС	Разделение секрета (вычисление вычета)	Восстановление секрета с помощью алгоритма Евклида
Каноническая ГЧС размерности n	$O(4n^2 + n \cdot n!)$	$O(7n^2 + n + n \cdot n! + Ln(m(4n^2 + 4n + n \cdot n!)))$
Каноническая ГЧС размерности $n+1$	$O(4n^2 + 4n + 4 + (n+1)(n+1)!)$	$O(7n^2 + 15n + 8 + (n+1)(n+1)! + Ln(m(4n^2 + 12n + 8 + (n+1) \cdot (n+1)!)))$
Неканоническая ГЧС размерности n с одной составной ячейкой	$O(4n^2 + 4n - 4 + n \cdot n!)$	$O(7n^2 + 8n - 7 + n \cdot n! + Ln(m(5n^2 + 9n - 5 + n \cdot n!)))$
Неканоническая ГЧС размерности n с $(n-1)^2$ составных ячеек	$O(4n^3 - 8n^2 + 8n - 2 + n \cdot n!)$	$O(7n^3 - 14n^2 + 18n - 5 + n \cdot n! + Ln(m(5n^3 - 10n^2 + 15n - -3 + n \cdot n!)))$

Очевидно, что вычислительная процедура разделения секрета в неканонической гиперкомплексной числовой системе размерности n с $(n-1)$ составных ячеек, сложнее чем аналогичная процедура в канонической гиперкомплексной числовой системе размерности $n+1$. Тоже самое можно сказать и про процедуру восстановления секрета.

Для усиления задачи разделения секрета при работе с каноническими гиперкомплексными числами необходимо было повышать размерность гиперкомплексной числовой системы. Учитывая вышесказанное, можно сделать вывод, что для усиления задачи разделения секрета целесообразно

представлять данные в неканонических гиперкомплексных числовых системах той же размерности, с более сложной структурой таблицы умножения.

Покажем вычислительные сложности подбора гиперкомплексной числовой системы злоумышленником, - а фактически, процедуры перебора гиперкомплексных числовых систем с единицей в базисе.

Таблица 2

Вычислительная сложность подбора числовых систем злоумышленником.

Каноническая ГЧС размерности *n*	$O(2n^3-3n^2+1)$
Каноническая ГЧС размерности *n+1*	$O(2n^3+3n^2)$
Неканоническая ГЧС размерности *n* с одной составной ячейкой	$O(3n+((n-1)^2-1)(2n+1))=$ $=O(2n^3-3n^2+3n)$
Неканоническая ГЧС размерности *n* с $(n-1)^2$ составных ячеек	$O(3n(n-1)^2)=$ $=O(3n^3-6n^2+3n)$
Неканоническая ГЧС размерности *n* с $(n-1)^2$ составных ячеек с целыми коэффициентами при базисных элементах из диапазона $\{-t,0,t\}$	$O((2t+1)n(n-1)^2)=$ $=O((2t+1)(n^3-2n^2+n))$

Можно утверждать, что сложность подборов канонической гиперкомплексной числовой системы размерности *n+1* и неканонической гиперкомплексной числовой системы размерности *n* практически одинаковы. Но, если учитывать, что коэффициентами при структурных элементах могут быть целые числа из диапазона $\{-t,0,t\}$, вычислительная сложность значительно возрастает, что подтверждает вывод о целесообразности и эффективности использования неканононических гиперкомплексных чисел в задаче разделения секрета.

Выводы

Использование неканонической гиперкомплексной числовой системы размерности 3 для того, чтобы обеспечить такую же криптостойкость, как и при использовании канонической ГЧС размерности 4, не дает нужного эффекта по минимизации вычислений, так как количество умножений увеличивается в среднем на 92%. Но при использовании неканонической ГЧС размерности 4 с 9 составными ячейками в таблице умножения с коэффициентами из диапазона {-4,4}, для обеспечения такой же криптостойкости, как и при использовании канонической ГЧС размерности 6, количество требуемых вычислений уменшается в среднем на 44%.

Список литературы

1. *Общая алгебра / Мельников О.В., Ремесленников В.Н., Романьков В.А., Скорняков Л.А., Шестаков И.П. // М.: Наука, 1990. —Т.1. —591с.*
2. *Приходовский М.А. Применение многомерных матриц для исследования гиперкомплексных чисел и конечномерных алгебр [Электронный ресурс] / Приходовский М.А.. // Режим доступа: physics.nad.ru/ matboard/themes/16127.htm.C.4.*
3. *Акушский И.Я. Машинная арифметика в остаточных классах / Акушский И.Я., Юдицкий Д.И. // – М.: Сов. Радио,1968. – 440 с.*
4. *И. Л. Кантор. Гиперкомплексные числа / И. Л. Кантор, А. С. Солодовников // М.: Наука, 1973. – 144с.*
5. *Розвиток гіперкомплексного представлення інформації та її застосування / М.В. Синьков, Ю.Є. Боярінова, О.В.Федоренко, Т.Г. Постнікова, Т.В. Синькова // Реєстрація, зберігання і обробка даних. —2007. — Т. 9, № 4. — С.28—48.*
6. *Федоренко О.В. Модель цифрового фільтра з гіперкомплексними коефіцієнтами / Федоренко О.В. // Системний аналіз та інформаційні технології: матеріали X Міжн. наук.-техн. конф. – К. : НТУУ „КПІ”, 2008. – С. 413.*
7. *Бранец В.Н. Применение кватернионов в задачах ориентации твердого тела / Бранец В.Н., Шмыглевский И.П. // М.: Наука,1973. — 319с.*
8. *Синьков М.В. Конечномерные гиперкомплексные числовые системы. Основы теории. Применения / Синьков М.В., Калиновский Я.А., Бояринова Ю.Е. // К.: Инфодрук, 2010.- 388с.*
9. *Hestenes D., Fasse E. Modeling Elastically Coupled Rigid Bodies with Geometric Algebra(2001).Preprint. P.13. // Online: http://modelingnts.la. asu. edu /pdf/ElasticModeling.pdf*
10. *Cheng H. H., Thompson S. Dual Polynomials and complex dual Numbers for analysis of spatial Mechanisms (1996) Proceedings of The 1996 ASME Design Engineering Technical Conference and Computers in Engineering Conference. P. 1-12.*
11. *Cheng H. Programming with Dual Numbers and its Applications in Mechanisms Design (1994) Engineering with Computers. Vol. 10, No.4. P.212-229.*
12. *McCarthy J, Ahlers S. Dimensional Synthesis Robots using a Double Quaternion Formulation of the Workspace (2000) Robotics Research: The Ninth International Symposium. P. 3-8.*
13. *Perez A., McCarthy J.M. Dual Quaternion Synthesis of a Parallel 2-TRP Robot (2004) Proc. of the Workshop on Fundamental Issues and Future Research Directions for Parallel Mechanisms and Manipulators, Quebec City. Mech. Des 125(4), P.709-716*
14. *Doik Kim, Wan Kyun Chung. Analytic Formulation of Reciprocal Screws and Its Application to Nonredundant Robot Manipulators (2003). Journal of Mechanical Design. Vol.125, No. 1. P.158-164.*

15. *Ning Ying, Wangdo Kim .Use of Dual euler Angles to describe general spatial Movements of human Joints(2001). Online: asme.pinetec.com/bio2001/data/pdfs/a0014419.pdf.*
16. *Shoemake K. Animation with quaternions (1987). ACM SIGGRAPH course notes 10, Computer animation: 3D Motion, Specification and Control. Proc ComputerAnimation CG 87, P.27–37*
17. *Sangwine S.J. Colour in image processing (2000). Electronics & Communication Engineering Jour. Vol. 12, No. 5, P. 211-219.*
18. *Mukundan R. Quaternions: From Classical Mechanics to Computer Graphics, and Beyond (2002). Proceedings of the 7th Asian Technology Conference in Mathematics. P.97-106.*
19. *Samareh J. A. Application of Quaternions for Mesh Deformation(2002). 8-th International Conference on Numerical Grid Generation in Computational Field Simulations . Honolulu (Hawaii). NASA/TM-2002-211646*
20. *Калиновский Я.В. Высокоразмерные изоморфные гиперкомплексные числовые системы и их использование для повышения эффективности вычислений / Калиновский Я.В., Бояринова Ю.Е. //К: Инфодрук, 2012.-183с.*
21. *Toyoshima H. Design of Hypercomplex All-Pass Filters to Realize Complex Transfer Functions(1999) Proc. Second Int. Conf. Information, Communications and Signal Processing. #2B3.4. P.1-5.*
22. *Toyoshima H. Computationally Efficient Implementation of Hypercomplex Digital Filters(2002). IEICE Trans. Fundamentals. E85-A, 8. P.1870-1876.*
23. *Toyoshima H. Computationally Efficient Implementation of Hypercomplex Digital Filters(1998). Proc. Int. Conf. Acoustics, Speech, and Signal processing. Vol. 3. P.1761-1764. (m5May 1998.)*
24. *Toyoshima H. Computationally Efficient Bicomplex Multipliers for Digital Signal Processing (1998). IEICE Trans. Inf. & Syst. E81-D, 2. P.236-238.*
25. *Алексейчук А.Н. Модулярная схема разделения секрета над кольцом целых гауссовых чисел / Алексейчук А.Н., Бояринова Ю.Е. // Реєстрація, зберігання і оброб. даних. — 2007. — Т. 9, № 1. — С. 87–99.*
26. *Изучение построений сопряжённых элементов в гиперкомплексных числовых системах. Ч.2 / Синьков М. В., Калиновский Я.А., Постникова Т. Г., Синькова Т.В. // Реєстрація, зберігання і обробка даних. — 2002. — Т. 4, №2. — С. 11-15.*
27. *Nobauer C. The number of isomorphism classes of d.g. near-rings on the generalized quaternion groups (2001). Proceedings of the Conference on Near-Rings and Near-Fields, Stellenbosch, South Africa. P. 133 – 137*
28. *Калиновский Я.А. Построение норм и сопряженных чисел в изоморфных гиперкомплексных числовых системах / Калиновский Я.А. // Реєстрація, зберігання і обробка даних. — 2011. — Т. 13, №3. — С. 17-29.*
29. *Одарич Я.В. Процедура перечисления гиперкомплексных числовых систем методом линейных преобразований / Одарич Я.В. // Реєстрація, зберігання і обробка даних—2008. —Т. 6, № 2—С.107-112.*

30. *Asmuth C.A., Blum J. A modular approach to key safeguarding(1983). IEEE Transactions on Information Theory, (5: IEE-83a), P. 23-**30**.*
31. *Blakley G.R. Safeguarding cryptographic keys(1979). In Proceedings AFIPS 1979, Nat. Computer Conf. V.48, P.313-317.*
32. *Мао Венбо. Современная криптография: теория и практика./ Мао Венбо. Пер. с англ. — М. : Издательский дом "Вильямс", 2005. — 768с.*
33. *Бояринова Ю.Е. Разработка алгоритмов восстановления информации в задаче разделения секрета / Бояринова Ю.Е., Одарич Я.В., Трубников П.В. // Реєстрація, зберігання і оброб. даних. — 2004. — Т. 6, № 4. — С. 107–112.*
34. *Виноградов И.М. Основы теории чисел / Виноградов И.М. – М.:Л., Гостехиздат, 1952— 180 с.*
35. *Синьков М.В. Непозиционные представления в многомерных числовых системах / Синьков М.В., Губарени Н.М. – К.: Наукова думка, 1979. – 140с.*

Боярінова Ю.Є.
кандидат технічних наук, старший науковий співробітник, доцент кафедри системного програмування і спеціалізованих комп'ютерних систем НТУУ «КПІ» ім. И.Сікорського

Каліновський Я.О.
доктор технічних наук, старший науковий співробітник інституту проблем реєєстрації інформації НАН України

Хіцко Я.В.
кандидат технічних наук, старший викладач кафедри системного програмування і спеціалізованих комп'ютерних систем НТУУ «КПІ» ім. И.Сікорського

ВИКОРИСТАННЯ НЕКАНОНІЧНИХ ГІПЕРКОМПЛЕКСНИХ ЧИСЛОВИХ СИСТЕМ ДЛЯ ПІДВИЩЕННЯ КРИПТОСТІЙКОСТІ

***Анотація**. Запропоновано модифікацію модулярної задачі розділення секрету, яка відрізняється від існуючої представленням інформації лишками в неканонічних гіперкомплексних числових систем за сукупністю неканонічних гіперкомплексних модулів. Показано, що при використанні неканонічної гіперкомплексної числової системи вимірності 4 для забезпечення такої ж криптостійкості, як і для канонічної гіперкомплексної числової системи вимірності 6, кількість потрібних обчислень зменшується.*

Ключові слова: *гіперкомплексна числова система, неканонічна система, схема розділення секрету, криптостійкість.*

Boyarinova J.E.
candidate of technical sciences, senior researcher, associate professor of system programming and specialized computer systems NTU "KPI" them. Y.Sikorskoho

Kalinowski Y.O.
doctor of technical sciences, senior researcher Institute for Information Sciences of Ukraine reyeyestratsiyi

Hitsko Y.V.
candidate of technical sciences, senior lecturer in system programming and specialized computer systems NTU "KPI" them. Y.Sikorskoho

USE NONCANONICAL HYPERCOMPLEX NUMERICAL SYSTEMS TO ENHANCE CRYPTOGRAPHIC RESISTANCE

Abstract. *Development of information systems and perfection of mathematical modeling methods demands new approaches and realizations for field expansion of solved applied problems.Choosing of data representation methods and effective data processing play an important role at construction of various type of information systems.*

Traditional and nonconventional methods of data representation are considered in work. Each of these forms of data representation has the own features and the most effective scopes. The carried out work and the analysis of these systems allows to make a conclusion, that hypercomplex numerical systems are effective for use in practical problems of mechanics, electrodynamics, radio electronics and many others.

It has offered to formulate a secret sharing problem in one of the big set of hypercomplex number systems - noncanonical number system. It has been shown that when using the noncanonical dimension hypercomplex number system 4 to provide the same as for the reliability of the canonical hypercomplex numerical systems by dimension 6, the number of required calculating decreases.

Keywords: *hypercomplex number system, noncanonical number system, modulo arithmetic, residual representations, secret sharing task, cryptographic resistance.*