УДК 621.391

В.Г. Лабунец [1], В.П. Часовских[1], Е. Остхаймер[2]
V.G. Labunets[1], V.P. Chasovskikh[1], E. Ostheimer[2]

[1]Ural State Forest Engineering University, Yekaterinburg
[2]Capricat LLC 1340 S. Ocean Blvd., Suite 209 Pompano Beach, 33062 Florida, USA

КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ, ОСНОВАННЫЕ НА ЛИНЕЙНЫХ КОДАХ НАД НЕКОММУТАТИВНЫМИ АЛГЕБРАМИ

PUBLIC KEY CRYPTOSYSTEMS BASED ON LINEAR CODES OVER NONCOMMUTATIVE ALGEBRAS

Ключевые слова: *открытый ключ, линейный код, алгебра Клиффорда, преобразование Фурье-Клиффорда Галуа*

Цель статьи – ввести новые криптосистемы, основанные на линейных кодах над алгебрами Клиффорда с быстрой процедурой кодирования/декодирования, использующей быстрое преобразование Фурье-Клиффорда-Галуа.

Keywords: *public key, linear code, Clifford algebra, Fourier-Clifford-Galois transforms.*

The purpose of this paper is to introduce new cryptosystems based on linear codes over Clifford algebras with fast code and encode procedures based on fast Fourier-Clifford-Galois transforms.

Введение

Популярным классом ассиметричных криптосистем являются системы, основанные на линейных кодах. Впервые такая система была предложенная в работе (McEliece, 1978). Позже было установлено, что задача декодирования произвольного двоичного линейного кода является NP-полной задачей (Berlekamp et al., 1978). Преимуществом таких систем является их высокое быстродействие и возможность исправлять ошибки при доставке шифротекста законному пользователю. Недостаток этих систем – большой объем открытого ключа. Для того, чтобы семейство линейных кодов можно было использовать для построения системы открытого шифрования необходимо, чтобы это семейство удовлетворяло следующим требованиям: 1) семейство содержит достаточно большое число кодов с одинаковыми параметрами, с тем чтобы избежать атаки путем полного перебора всех возможных кодов, 2) каждый код семейства обладает простыми процедурами кодирования и декодирования при условии, что известно полное описание кода, и 3) получение полного описания кода из открытого ключа должно представлять собой трудную задачу.

В работе (McEliece, 1978) использовано семейство двоичных кодов Гоппы, причем открытым ключом является скремблированная порождающая матрица выбранного кода. Известны несколько более или менее безуспешных атак на эту систему (Heiman, Shamir, 1987; Adams, Meijer, 1987). Система Нидерратера (Niederreiter, 1986), основанная на обобщенных кодах Рида-Соломона (ОРС-кодах), использует в качестве открытого ключа скремблированную проверочную матрицу кода. Как показано в работах В.М. Сидельникова и С.О. Шестакова (1992а,б), эта система и некоторые ее варианты могут быть взломаны за полиномиальное время, что является следствием малочисленности семейства ОРС-кодов по сравнению со всем семейством линейных кодов. В этой работе

мы предлагаем в существенной мере расширить класс ОРС-кодов за счет использования некоммутативных алгебр Клиффорда $Clif_n\{\mathbf{GF}(p)\}$ над простыми полями Галуа $\mathbf{GF}(p)$ вместо расширенных полей Галуа $\mathbf{GF}(p^n)$.

Объект изучения

Пусть $\mathbf{T}=\{t\}$ - множество открытых секретных текстов, $\mathbf{C}=\{c\}$ - множество шифрограмм (зашифрованных секретных сообщений), $\mathbf{K}^{\text{op}}=\{k^{\text{op}}\}$ - множество открытых ключей (набор данных, позволяющих зашифровывать секретные сообщения, превратив их в шифрограмму), $\mathbf{K}^{\text{sec}}=\{k^{\text{sec}}\}$ - множество секретных ключей (набор данных, позволяющих расшифровывать шифрограмму, т.е. извлечь из нее секретный текст). Процедуру шифрования можно описать в виде взаимнооднозначного отображения

$$E:\ \mathbf{T}\times\mathbf{K}^{\text{op}}\to\ \mathbf{C},\quad c=E\left(t,k^{\text{op}}\right), \tag{1}$$

которое преобразует секретный текст t в шифрограмму c с использованием открытого ключа k^{op}. Аналогично, дешифрирование представляется отображением, обратным к E:

$$D:\ \mathbf{C}\times\mathbf{K}^{\text{sec}}\to\ \mathbf{T},\quad t=D\left(c,k^{\text{sec}}\right), \tag{2}$$

позволяющим по имеющейся шифрограмме c и при наличии секретного ключа k^{sec} извлечь из шифрограммы c секретное сообщение t. Пусть $t,c,k^{\text{op}},k^{\text{sec}}$ - последовательности длины не более n над некоторым конечным алфавитом. Определим вычислительную сложность шифрования $W\left(E\,|\,k^{\text{op}}\right)$ как число арифметических операций, необходимых для получения шифрограммы c из секретного текста t при заданном ключе k^{op}. Сложность шифрования должна представляться полиномом невысокой степени от n: $W\left(E\,|\,k^{\text{op}}\right)=\text{Pol}(n)$. Аналогично определяется сложность дешифрования $W\left(D\,|\,k^{\text{sec}}\right)$. Она также должна представляться полиномом невысокой степени от n: $W\left(D\,|\,k^{\text{sec}}\right)=\text{Pol}(n)$ при известном секретном ключе k^{sec}. С другой стороны, если ключ k^{sec} неизвестен (такой ключ будем обозначать символом $k^{\text{sec-?}}$), то дешифрирование должно быть гораздо сложнее. Обычно желательно, чтобы она носила экспоненциальный характер $W\left(D\,|\,k^{\text{sec-?}}\right)=\text{Exp}(n)$ или чтобы задача дешифрования относилась к так называемым трудным NP-полным задачам. В этом случае говорят, что криптосистема является криптостойкой. Итак, если два пользователя (А и В) хотят установить секретную связь, то они могут выбрать один ключ $k=k^{\text{op}}=k^{\text{sec}}$ и хранить его в секрете. С его помощью они могут легко шифровать и расшифровывать сообщения. Криптосистемы, использующие секретный ключ, называются симметричными шифрами. За последние годы было предложено много подобных криптосистем.

В 1976 г. Даффи и Хеллманом впервые была выдвинута новая криптографическая концепция – концепция открытого шифрования (цит. по: McEliece, 1978). Основная идея заключалась в том, чтобы ключ шифрования k^{op} и алгоритм шифрования $c=E\left(t,k^{\text{op}}\right)$ сделать доступными всем желающим. Однако, ключ дешифрования k^{sec} непосредственно не задается, а вычисляется по ключу k^{op} с помощью некоторой функции $k^{\text{sec}}=S\left(k^{\text{op}}\right)$, которая должна быть трудно вычислимой с вычислительной сложностью порядка $\text{Exp}(n)$. В этом случае отображение S называется *секретом* (*отмычкой*, *потайным ходом*). Понятно, что сложность дешифрования $W\left(D\,|\,k^{\text{sec}}\right)=W\left(D\,|\,S\left(k^{\text{op}}\right)\right)$ становится экспоненциальной для взломщика, если он не знает секрета S, а знает

только шифрограмму c и открытый ключ k^{op}. Говорят, что k^{op} определяет *асимметричный шифр*, если трудоемкость $W\left(E|k^{\text{op}}\right)$ полиномиальна по n, а трудоемкость $W\left(D|S\left(k^{\text{op}}\right)\right)$ - экпоненциальна по n даже при известном k^{op} (но неизвестном секрете S).

В данной работе мы предлагаем в качестве открытого ключа использовать порождающую матрицу ОРС-кода в виде дискретного преобразования Фурье-Клиффорда над некоммутативной алгеброй Клиффорда $Clif_n\{\mathbf{GF}(p)\}$.

Методы

Алгебраическое кодирование над некоммутативными телами. Все до сих пор рассматриваемые асимметричные криптосистемы используют коды над конечными полями Галуа. Пусть $\mathbf{GF}(q)$ - конечное поле из q элементов, где q степень простого числа p. Рассмотрим n- мерное пространство $\mathbf{V}_n\left[\mathbf{GF}(q)\right]=\mathbf{GF}^n(q)$ над полем $\mathbf{GF}(q)$, содержащее q^n векторов длины n с компонентами из $\mathbf{GF}(q)$. Если $\mathbf{x}=\left(x_1,x_2,...,x_n\right)\in\mathbf{GF}^n(q)$ вектор из $\mathbf{V}_n\left[\mathbf{GF}(q)\right]$, то в $\mathbf{V}_n\left[\mathbf{GF}(q)\right]$ определено умножение векторов $\mathbf{x}=\left(x_1,x_2,...,x_n\right)$ на скаляры $\lambda\in\mathbf{GF}(q)$:

$$\lambda\mathbf{x}:=\lambda\left(x_1,x_2,...,x_n\right)=\left(\lambda x_1,\lambda x_2,...,\lambda x_n\right). \qquad (3)$$

Ситуация меняется, если рассматривается n-мерное пространство $\mathbf{V}_n\left[\mathbf{K}\right]=\mathbf{K}^n$ над некоторым конечным некоммутативным кольцом $\mathbf{K}$. В силу некоммутативности умножения в кольце $\mathbf{K}$ можно ввести правое и левой умножения в $\mathbf{V}_n\left[\mathbf{K}\right]$:

$$\lambda\mathbf{x}:=\lambda\left(x_1,x_2,...,x_n\right)=\left(\lambda x_1,\lambda x_2,...,\lambda x_n\right),\ \ \mathbf{x}\lambda:=\left(x_1,x_2,...,x_n\right)\lambda=\left(x_1\lambda,x_2\lambda,...,x_n\lambda\right).$$

Причем, $\lambda\mathbf{x}\neq\mathbf{x}\lambda$. Поэтому в некоммутативном случае необходимо вводить в рассмотрение не одно, а два n-мерных векторных пространства: правое $\mathbf{V}_n^R\left[\mathbf{K}\right]={}^R\mathbf{K}^n$ и левое $\mathbf{V}_n^L\left[\mathbf{K}\right]={}^L\mathbf{K}^n$. В действительности же возможностей здесь значительно больше. Пусть каждая компонента вектора $\mathbf{x}=\left(x_1,x_2,...,x_n\right)\in\mathbf{K}^n$ оснащена бинарным указателем σ, показывающим, с какой стороны скаляру разрешено умножать компоненту вектора:

$$\lambda x^{\sigma}=\begin{cases}\lambda x, & \sigma=1,\\ x\lambda, & \sigma=0.\end{cases} \qquad (4)$$

Поэтому сам вектор $\mathbf{x}=\left(x_1,x_2,...,x_n\right)\in\mathbf{K}^n$ должен быть оснащен набором из n бинарных указателей: $\mathbf{x}^{\boldsymbol{\sigma}}=\left(x_1^{\sigma_1},x_2^{\sigma_2},...,x_n^{\sigma_n}\right)$, где $\boldsymbol{\sigma}=\left(\sigma_1,\sigma_2,...,\sigma_n\right)\in\mathbf{B}_2^n$ - n-мерный булев вектор. Этот набор назовем *секретом* вектора $\mathbf{x}=\left(x_1,x_2,...,x_n\right)\in\mathbf{K}^n$. Определим теперь в пространстве $\mathbf{K}^n$ новое умножение на скаляр по правилу

$$\lambda\mathbf{x}^{\sigma}:=\lambda\left(x_1^{\sigma_1},x_2^{\sigma_2},...,x_n^{\sigma_n}\right)=\left(\lambda x_1^{\sigma_1},\lambda x_2^{\sigma_2},...,\lambda x_n^{\sigma_n}\right). \qquad (5)$$

Определение 1. Линейное векторное пространство $\mathbf{K}^n$, оснащенное умножением на скаляр по правилу (5), назовем векторным пространством с *секретом, отмычкой*, или с *потайным ходом* $\boldsymbol{\sigma}=\left(\sigma_1,\sigma_2,...,\sigma_n\right)\in\mathbf{B}_2^n$ и обозначим символом $\mathbf{K}^n\left(\boldsymbol{\sigma}\right)$.

Левое и правое векторные пространства имеют ФМ-отмычки $\sigma=\left(1,1,...,1\right)\in\mathbf{B}_2^n$ и $\sigma=\left(0,0,...,0\right)\in\mathbf{B}_2^n$, соответственно. Очевидно, что существует целое семейство

$\left\{\mathbf{K}^n(\boldsymbol{\sigma})\right\}_{\boldsymbol{\sigma}\in\mathbf{B}_2^n}$ из 2^n различных векторных пространств $\mathbf{K}^n(\boldsymbol{\sigma})$, для $\langle\boldsymbol{\sigma}\rangle_{10}=0,1,...,2^n-1$, где $\langle\boldsymbol{\sigma}\rangle_{10}$ - десятичный эквивалент бинарного числа $\sigma=(\sigma_1,\sigma_2,...,\sigma_n)\in\mathbf{B}_2^n$.

Алгебры Клиффорда. Положим, $N=2^m$. Пусть «малое» mD пространство $\mathbf{GF}^m(p)$ натянуто на m ортонормированных пространственных *гипермнимых единиц* I_i, $i=1,2,\ldots,m$. Мы предполагаем, что

$$I_i^2=\begin{cases}+1 & \text{for } i=1,2,\ldots,p,\\ -1 & \text{for } i=p+1,2,\ldots,p+q,\\ 0 & \text{for } i=p+q+1,2,\ldots,p+q+r=m,\end{cases} \tag{6}$$

и $I_iI_j=-I_jI_i$. Теперь можно сконструировать «большое» 2^m-мерное гиперкомплексное пространство $\mathbf{GF}^{2^m}(p)$ как прямую сумму подпространств следующих размерностей $C_m^0,C_m^1,C_m^2,...,C_m^m$:

$$\begin{aligned}&\mathbf{GF}^{2^m}(p)=\sum_{s=0}^{m}\mathbf{GF}^{C_m^s}(p)=\\ &=\mathbf{GF}^{C_m^0}(p)\oplus\mathbf{GF}^{C_m^1}(p)\oplus\mathbf{GF}^{C_m^2}(p)\oplus...\oplus\mathbf{GF}^{C_m^s}(p)\oplus...\oplus\mathbf{GF}^{C_m^{m-1}}(p)\oplus\mathbf{GF}^{C_m^m}(p),\end{aligned} \tag{7}$$

где подпространства $\mathbf{GF}^{C_m^s}(p)$, $s=0,1,2,...,m$ натянуты на s–кратные произведения гипермнимых единиц $I_{k_1}I_{k_2}...I_{k_s}$ $(k_1<k_2<...<k_s)$. По определению мы полагаем, что $I_0\equiv1$ - есть обычная вещественная единица так, что

$$\begin{aligned}&\mathbf{GF}^{C_m^0}(p)=\left\{x_0I_0\middle|x_0\in\mathbf{GF}(p)\right\},\\ &\mathbf{GF}^{C_m^1}(p)=\left\{x_1I_1+x_2I_2+...+x_mI_m\middle|x_1,x_2,...,x_m\in\mathbf{GF}(p)\right\},\\ &\mathbf{GF}^{C_m^2}(p)=\left\{x_{12}I_1I_2+x_{13}I_1I_3+...+x_{m-1m}I_{m-1}I_m\middle|x_{12},x_{13},...,x_{m-1m}\in\mathbf{GF}(p)\right\},\\ &\mathbf{GF}^{C_m^3}(p)=\left\{x_{123}I_1I_2I_3+x_{124}I_1I_2I_4+...+x_{m-2m-1m}I_{m-2}I_{m-1}I_m\middle|x_{123},x_{124},...,x_{m-2m-1m}\in\mathbf{GF}(p)\right\},\\ &.....,\\ &\mathbf{GF}^{C_m^m}(p)=\left\{x_{123...m}I_1I_2I_3...I_m\middle|x_{123...\mathrm{m}}\in\mathbf{GF}(p)\right\}.\end{aligned} \tag{8}$$

Пример 1. Пусть «малые» пространства суть $\mathbf{GF}^1(p),\mathbf{GF}^2(p),\mathbf{GF}^3(p)$. Тогда соответствующими «большими» пространствами будут

$$\begin{aligned}&\mathbf{GF}^{2^1}(p)=\mathbf{GF}^2(p)=\mathbf{GF}^1(p)\oplus\mathbf{GF}^1(p)=\mathbf{GF}(p)\cdot I_0\oplus\mathbf{GF}(p)\cdot I_1,\\ &\mathbf{GF}^{2^2}(p)=\mathbf{GF}^4(p)=\mathbf{GF}^1(p)\oplus\mathbf{GF}^2(p)\oplus\mathbf{GF}^1(p)\\ &\quad=\mathbf{GF}(p)\cdot I_0\oplus\left\{\mathbf{GF}(p)\cdot I_1\oplus\mathbf{GF}(p)\cdot I_2\right\}\oplus\left\{\mathbf{GF}(p)\cdot I_1I_2\right\},\\ &\mathbf{GF}^{2^3}(p)=\mathbf{GF}^8(p)=\mathbf{GF}^1(p)\oplus\mathbf{GF}^3(p)\oplus\mathbf{GF}^3(p)\oplus\mathbf{GF}^1(p)=\\ &\quad=\mathbf{GF}(p)\cdot I_0\oplus\left\{\mathbf{GF}(p)\cdot I_1\oplus\mathbf{GF}(p)\cdot I_2\oplus\mathbf{GF}(p)\cdot I_3\right\}\oplus\\ &\quad\oplus\left\{\mathbf{GF}(p)\cdot I_1I_2\oplus\mathbf{GF}(p)\cdot I_1I_3\oplus\mathbf{GF}(p)\cdot I_2I_3\right\}\oplus\mathbf{GF}(p)\cdot I_1I_2I_3.\end{aligned} \tag{9}$$

В $\mathbf{GF}^{2^1}(p)$ “живут” обобщенные комплексные модулярные числа, в $\mathbf{GF}^{2^2}(p)$-модулярные кватернионы и в $\mathbf{GF}^{2^3}(p)$ - октонионы. Каждый элемент из $\mathbf{GF}^{2^m}(p)$ может иметь следующее представление. Пусть $\mathbf{b}=(b_1,b_2,...,b_m)\in\mathbf{B}_2^m$ будет произвольным n-битовым числом, где $b_i\in\mathbf{B}_2=\{0,1\}$ и $\mathbf{B}_2^m$ - mD Булев куб. Введем следующие обозна-

чения $I^{\mathbf{b}} := I_1^{b_1} I_2^{b_2} \ldots I_m^{b_m}$. Тогда 2^m элементов $\left\{I^{\mathbf{b}}\right\}_{\mathbf{b}\in\mathbf{B}_2^m}$ формируют базис 2^mD пространства:

$$\begin{aligned} Q &= \sum_{\mathbf{b}\in\mathbf{B}_2^m} x_{\mathbf{b}} I_{\mathbf{b}} = \sum_{s=0}^{m} \sum_{w(\mathbf{b})=s} x_{\mathbf{b}} I_{\mathbf{b}} = \sum_{w(\mathbf{b})=0} x_{\mathbf{b}} I_{\mathbf{b}} + \left(\sum_{w(\mathbf{b})=1} x_{\mathbf{b}} I_{\mathbf{b}} + \sum_{w(\mathbf{b})=2} x_{\mathbf{b}} I_{\mathbf{b}} + \ldots + \sum_{w(\mathbf{b})=s} x_{\mathbf{b}} I_{\mathbf{b}} + \ldots + \sum_{w(\mathbf{b})=m} x_{\mathbf{b}} I_{\mathbf{b}} \right) = \\ &= \mathbf{Sc}(Q) + \left(\mathbf{Vec}^1(Q) + \mathbf{Vec}^2(Q) + \ldots + \mathbf{Vec}^s(Q) + \ldots + \mathbf{Vec}^m(Q) \right) = \\ &= \mathbf{Sc}(Q) + \mathbf{Vec}(Q) = \mathbf{Sc}(Q) + \mathbf{Vec}^1(Q) + \mathbf{Vec}^{>1}(Q) = Q_0 + \vec{\mathbf{x}} + Q^{>1}, \end{aligned} \tag{10}$$

где

$$\mathbf{Sc}(Q) = \sum_{w(\mathbf{b})=0} x_{\mathbf{b}} I_{\mathbf{b}} \tag{11}$$

- суть скалярная часть Клиффордовского числа и

$$\mathbf{Vec}(Q) = \left(\mathbf{Vec}^1(Q) + \mathbf{Vec}^2(Q) + \ldots + \mathbf{Vec}^s(Q) + \ldots + \mathbf{Vec}^m(Q) \right) \tag{12}$$

- есть его общая векторная часть, $Vec^1(Q) = \sum_{w(\mathbf{b})=1} x_{\mathbf{b}} I_{\mathbf{b}}$ - чисто векторная часть, $Vec^2(Q) = \sum_{w(\mathbf{b})=2} x_{\mathbf{b}} I_{\mathbf{b}}$ - бивекторная часть, …, $Vec^s(Q) = \sum_{w(\mathbf{b})=s} x_{\mathbf{b}} I_{\mathbf{b}}$ - s-векторная часть,…, и, наконец, $Vec^m(Q) = \sum_{w(\mathbf{b})=m} x_{\mathbf{b}} I_{\mathbf{b}}$ - есть m–векторная часть. По определению полагаем

$$\mathbf{Vec}^{>1}(Q) := \left(\mathbf{Vec}^2(Q) + \ldots + \mathbf{Vec}^s(Q) + \ldots + \mathbf{Vec}^m(Q) \right) \tag{13}$$

Если $Q_1, Q_2 \in \mathbf{GF}^{2^m}(p)$, то можно определить произведение двух чисел Клиффорда $Q_1 \cdot Q_2$

$$S = Q_1 Q_2 := \left(\sum_{\mathbf{b}\in\mathbf{B}_2^m} x_{\mathbf{b}} I_{\mathbf{b}} \right) \cdot \left(\sum_{\mathbf{c}\in\mathbf{B}_2^m} y_{\mathbf{c}} I_{\mathbf{c}} \right) = \sum_{\mathbf{d}\in\mathbf{B}_2^m} z_{\mathbf{d}} I_{\mathbf{d}} \tag{14}$$

Существует 3^n возможностей для всех $I_k^2 = +1, 0, -1, \ \forall i = 1, 2, \ldots, m$. Каждая возможность генерирует вполне определенную алгебру. Следовательно, пространство $\mathbf{GF}^{2^m}(p)$, оснащенное 3^m правилами умножения 3^m различных 2^mD алгебр, которые называются пространственными алгебрами Клиффорда. Обозначим их символами $\mathrm{A}_{2^m}^{(p,q,r)}\left(\mathbf{GF}(p)|1, I_1, \ldots, I_n\right)$ или $Clif\left\{\mathbf{GF}(p)\right\}$, если $I_1, \ldots, I_m$, p, q, r фиксированы.

Пусть $\mathbf{G}^{\boldsymbol{\sigma}} = [w_{ik}^{\sigma_{ik}}]_{i,k=1}^{N}$ - $(N \times N)$-матрица над некоммутативной алгеброй Клиффорда $Clif\left\{\mathbf{GF}(p)\right\}$, каждый матричный элемент $w_{ik}^{\sigma_{ik}}$ которой оснащен меткой σ_{ik}, которая показывает, с какой стороны компонента $w_{ik}^{\sigma_{ik}}$ умножает компоненту x_k вектора $\mathbf{x} = (x_1, x_2, ..., x_N)$, где $x_k \in Clif\left\{\mathbf{GF}(p)\right\}$, при действии $y_i^{\boldsymbol{\sigma}} = \sum_{k=1}^{n} w_{ik}^{\sigma_{ik}} x_k$:

$$w_{ik}^{\sigma_{ik}} x_k = \begin{cases} w_{ik} x_k, & \sigma = 1, \\ x_k w_{ik}, & \sigma = 0. \end{cases} \tag{15}$$

Все метки σ_{ik} формируют бинарную матрицу $\boldsymbol{\sigma} = \left[\sigma_{ik}\right]$.

Определение 2. Пространство $Mat_{M\times N}^{\boldsymbol{\sigma}}\left[Clif\left\{\mathbf{GF}(p)\right\}\right]$, оснащенное матричной меткой $\boldsymbol{\sigma} = \left[\sigma_{ik}\right]$, назовем пространством с *секретом, с отмычкой* или с *потайным ходом* $\boldsymbol{\sigma} = \left[\sigma_{ik}\right]$.

Очевидно, что существует целое семейство $\left\{Mat^{\boldsymbol{\sigma}}_{M\times N}\left[Clif\left\{\mathbf{GF}(p)\right\}\right]\right\}_{\boldsymbol{\sigma}\in\mathbf{B}_2^{M\times N}}$ из $2^{M\times N}$ различных пространств. Для $M=N=16$ это число громадно $2^{16\times 16}=2^{256}=64\cdot 10^{25}$!

Пусть $\mathbf{G}^{\boldsymbol{\sigma}}=[w_{kj}^{\sigma_{kj}}]_{k,j=1}^{M,N}$ и $\mathbf{H}^{\boldsymbol{\alpha}}=[v_{ik}^{\alpha_{ik}}]_{i,k=1}^{N,M}$ - две произвольные матрицы (генерирующая и проверочная) размеров $(M\times N)$ и $(N\times M)$, матричные элементы которых состоят из унимодулярных чисел. Тогда для $\mathbf{y}={}^2\mathbf{H}^{\boldsymbol{\alpha}}\cdot{}^1\mathbf{G}^{\boldsymbol{\sigma}}\cdot\mathbf{x}$ имеем $y_i=\sum_{j=1}^{N}\left(\sum_{k=1}^{M}{}^2v_{ik}^{\alpha_{ik}}\cdot{}^1w_{kj}^{\sigma_{kj}}\cdot x_j\right)$, где левые верхние индексы обозначают порядок воздействия матриц на вектор. Произведение ${}^2v_{ik}^{\alpha_{ik}}\cdot{}^1w_{kj}^{\sigma_{kj}}\cdot x_j$ в зависимости от значений бинарных меток может быть записано в четырех формах

$$
{}^2v_{ik}^{\alpha_{ik}}\cdot{}^1w_{kj}^{\alpha_{kj}}\cdot x_j=\begin{cases}{}^2v_{ik}\cdot{}^1w_{kj}\cdot x_j, & (\alpha_{ik}=1)\&(\sigma_{kj}=1),\\ {}^2v_{ik}\cdot x_j\cdot{}^1w_{kj}, & (\alpha_{ik}=1)\&(\sigma_{kj}=1),\\ {}^1w_{kj}\cdot x_j\cdot{}^2v_{ik}, & (\alpha_{ik}=1)\&(\sigma_{kj}=1),\\ x_j\cdot{}^2v_{ik}\cdot{}^1w_{kj}, & (\alpha_{ik}=1)\&(\sigma_{kj}=1),\end{cases}
\tag{16}
$$

Так как числа по предположению унимодулярные, то $v_{ik}\cdot w_{kj}\cdot x_j$, $v_{ik}\cdot x_j\cdot w_{kj}$, $w_{kj}\cdot x_j\cdot v_{ik}$ и $x_j\cdot v_{ik}\cdot w_{kj}$ суть вращения многомерного числа Клиффорда x_j и четыре выше приведенных выражения можно записать в векторно-матричной форме

$$
v_{ik}^{\alpha_{ik}}\cdot w_{kj}^{\alpha_{kj}}\cdot x_j=\begin{cases}R^l(v_{ik})\cdot R^l(w_{ik})\cdot\vec{x}_j, & (\alpha_{ik}=1)\&(\sigma_{kj}=1),\\ R^l(v_{ik})\cdot R^r(w_{ik})\cdot\vec{x}_j, & (\alpha_{ik}=1)\&(\sigma_{kj}=1),\\ R^r(v_{ik})\cdot R^l(w_{ik})\cdot\vec{x}_j, & (\alpha_{ik}=1)\&(\sigma_{kj}=1),\\ R^l(v_{ik})\cdot R^r(w_{ik})\cdot\vec{x}_j, & (\alpha_{ik}=1)\&(\sigma_{kj}=1),\end{cases}
\tag{17}
$$

где $R^l(w_{ik}),R^r(w_{ik})$ и $R^l(v_{ik}),R^r(v_{ik})$ - левые и правые вращательные представления чисел Клиффорда v_{ik} и w_{ik}. Следовательно, имеем

$$
\vec{y}_i=\sum_{j=1}^{N}\left(\sum_{k=1}^{M}R\left(v_{ik}^{\alpha_{ik}}\right)\cdot R\left(w_{kj}^{\sigma_{kj}}\right)\cdot\vec{x}_j\right)=\sum_{j=1}^{N}\left(\sum_{k=1}^{M}R\left(v_{ik}^{\alpha_{ik}}\right)\cdot R\left(w_{kj}^{\sigma_{kj}}\right)\right)\cdot\vec{x}_j,
\tag{18}
$$

где $\vec{x}_j,\vec{y}_i$ - векторные представления многомерных чисел Клиффорда x_j,y_i. Пара матриц $\mathbf{G}^{\boldsymbol{\sigma}}=[w_{ik}^{\sigma_{ik}}]_{i,k=1}^{N}$ и $\mathbf{H}^{\boldsymbol{\alpha}}=[v_{ik}^{\alpha_{ik}}]_{i,k=1}^{N}$ будет взаимообратной, если выполнится равенство $\sum_{k=1}^{M}R\left(v_{ik}^{\alpha_{ik}}\right)\cdot R\left(w_{kj}^{\sigma_{kj}}\right)=I_{ij}$.

Определение 3. Для каждой фиксированной отмычки $\boldsymbol{\sigma}\in\mathbf{B}_2^{M\times N}$ множество всех векторов $\mathbf{y}^{\boldsymbol{\sigma}}=\mathbf{G}^{\boldsymbol{\sigma}}\mathbf{x}$ назовем линейным кодом с порождающей матрицей $\mathbf{G}^{\boldsymbol{\sigma}}$.

Определение 4. Если $\mathbf{G}^{\boldsymbol{\sigma}}$ является преобразованием Фурье-Клиффорда-Галуа и спектр $\mathbf{y}^{\boldsymbol{\sigma}}=\mathbf{G}^{\boldsymbol{\sigma}}\mathbf{x}$ имеет нулевые компоненты $y_b,y_{b+1},...,y_{b+\delta-2}$ для некоторых b,δ, то такой линейный код назывем БЧХ-кодом над алгеброй Клиффорда.

Определение 5. Если $\mathbf{G}^{\boldsymbol{\sigma}}$ является преобразованием Фурье-Клиффорда-Галуа и спектр $\mathbf{y}^{\boldsymbol{\sigma}}=\mathbf{G}^{\boldsymbol{\sigma}}\mathbf{x}$ имеет нулевые компоненты $y_b,y_{b+1},...,y_{b+\delta-2}$ для некоторых b,δ, а длина кода равна $p-1$, то такой БЧХ-код назовем кодом Рида-Соломона алгеброй Клиффорда.

Наличие процедур быстрого преобразования Фурье-Клиффорда-Галуа делает введенные коды эффективным средством одновременного избыточного кодирования и шифрования данных.

Заключение

Впервые введены в рассмотрение криптосистемы, основанные на линейных кодах Рида-Соломона-Клиффорда с повышенной криптостойкостью и обладающие быстрыми процедурами кодирования и декодирования в виде быстрых дискретных преобразований Фурье-Клиффорда-Галуа.

Работа выполнена при финансовой поддержке РФФИ в рамках грантов РФФИ-а № 17-07-00886, РФФИ-офи-м № 17-29-03369.

Список использованной литературы

Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // Дискрет. Мат. 1992а. Т. 3. № 3. С. 57-63.

Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // Перспективные средства телекоммуникации и интегрированные системы связи / Под ред. В.В. Зяблова. М.: ИППИ, РАН, 1992б. С. 48-61.

Adams C.M. Meijer H. Security-Related Comments Regarding McEliece Public Key Cryptosystem // Advances in Cryptology – EUROCRYPT'87 / D. Chaum, W.L. Price (eds.). Proc. Workshop on the Theory and Application of Cryptographic Techniques. Amsterdam, The Netherlands, April 13-15, 1987.

Berlekamp E.R., McEliece R.J., van Tilborg H.C.A. On inherent intractability of certain coding problems // IEEE Trans. Inf. Theory. 1978. Vol. IT-24. No. 4. P. 384-386.

Heiman R., Shamir A. On the Security of Cryptosystem Based on Linear Error Correcting Codes // Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel, 1987.

McEliece R.J. A Public Key Cryptosystem Based on Algebraic Coding Theory // JPL DSN Progress Rep. 42-44. 1978, Jan.-Feb. P.114-116.

Niederreiter H. Knapsack-Type Cryptosystem and Algebraic Coding Theory // Probl. Control and Inform. Theory. 1986. Vol.13. No. 2. P. 159-16.

Рецензент статьи: доктор технических наук, профессор Института радиоэлектроники и информационных технологий Уральского федерального университета Л.Г. Доросинский.