Московский государственный университет имени М. В. Ломоносова
Факультет вычислительной математики и кибернетики
Кафедра информационной безопасности

Линь Пэйфэн

Свойства произведения Адамара констациклических линейных кодов

Выпускная квалификационная работа

Научный руководитель:
доцент, к.ф.-м.н.
Чижов Иван Владимирович

Москва, 2022

Оглавление

Введение

Констациклические коды являются обобщением известных циклических и негациклических кодов. Их алгебраическая структура обеспечивает эффективность кодирования и декодирования с помощью регистров линейого сдвига. Произведение Адамара это покомпонентное умножение. Его применение к подпространству векторного W пространства V_n является одним из способов построения подпространств пространства. Для заданного кода, исследования влияния повторного применения умножения Адамара к коду на изменение параметров размерности k, кодового расстояния d и порождающего полинома $g(x)$ широко заинтересованы. Для констациклических кодов, еще один важный введенный в [1] параметр полином-образец. Он помогает исследовать порождающий многочлен кода, иногда они даже равны.

В этой работе исследуется замыкание кода. Понятие замыкания кода ведено в [2]. В той работе полностью описав замыкание кода Рида-Маллера, И. Чижов и М. Бородин упростили атаку на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера. Замыкание кода C по сути является множеством тех кодов, которые могут получены применением операции умножения Адамара кода на код C и взятия дуального кода. В этой работе собраны теории, которые помогают исследовать криптосистему Мак-Элиса, построенной на основе констациклических кодов. В этой работе описал группу автоморфизмов и замыкание констациклических кодов, которые имеют базис с непересекающимися носителями. И уменьшил объем перебора ключей криптосистемы Мак-Элиса, построенной на основе констациклических кодов, чьи последовательности размерностей до длины n не достигается.

1. Основные определения и теории

Все объекты рассматриваются над полем F_q. Через I_n обозначим множество $\{1, 2, \ldots, n\}$.

Определение 1.1. [3] Линейный код C длины n — это линейное подпространство векторного пространства F_q^n.

Определение 1.2. [3] Кодовыми словами называются векторы линейного кода C.

Определение 1.3. [3] Размерностью $k = k_C$ кода C называется его размерность как векторного пространства

$$k = k_C = \dim C$$

Определение 1.4. [3] Весом Хемминга $\mathrm{wt}(x)$ вектора $x = (x_1, x_2, \ldots, x_n) \in F_q^n$ называется число ненулевых компонент вектора x.

Определение 1.5. [4] Для произвольного вектора $x \in F_q^n$ множество

$$\mathrm{supp}(x) = \{i \in I_n \mid x_i \neq 0\}$$

называется носителем вектора x.

Определение 1.6. [3] Расстоянием Хемминга $\mathrm{dist}(x', x'')$ между двумя векторами $x', x'' \in F_q^n$ называется число координат, в которых они отличаются.

Определение 1.7. [3] Минимальным расстоянием $d_{min} = d_{min}(C)$ кода C называется минимальное расстояние Хемминга между его кодовыми словами

$$d_{min}(C) = \min\{\mathrm{dist}(c, c') \mid c, c' \in C, c \neq c'\}$$

Поскольку код C является векторным подпространством, то его минимальное расстояние удовлетворяет следующему равенству

$$d_{min}(C) = \min\{\mathrm{wt}(c) \mid c \in C, c \neq 0\}$$

Определение 1.8. [1] Произведением Адамара двух векторов $c = (c_1, c_2, \ldots, c_n)$, $d = (d_1, d_2, \ldots, d_n) \in F_q^n$ называется вектор $(c_1 \cdot d_1, c_2 \cdot d_2, \ldots, c_n \cdot d_n)$, обозначают его через $c \odot d$.
Степени Адамара $c^{\langle i \rangle}$ вектора c определяются как $\underbrace{c \odot c \odot \cdots \odot c}_{i}$

Определение 1.9. [1] Произведением Адамара кодов C_1 и C_2 называется множество всевозможных произведений Адамара кодовых слов двух кодов.

$$C_1 \odot C_2 = \{c_1 \odot c_2 \mid c_1 \in C_1, c_2 \in C_2\}$$

Степени Адамара $C^{\langle i \rangle}$ кода C при $i \geqslant 1$ определяются как

$$C^{\langle i \rangle} = \underbrace{C \odot C \odot \cdots \odot C}_{i}$$

Через $C^{\langle 0 \rangle}$ обозначается одномерное пространство, базисом которого является вектор 1^n.

Определение 1.10. [1] Пусть $f(x) = x^n - a$ и $p(x) = \sum\limits_{i=0}^{n-1} c_i x^i \in F_q[x]/f(x)$.

$p(x)$ обозначается вектором $\text{coeff}(p(x)) = (c_0, \cdots, c_{n-1}) \in F_q^n$.

Аналогично, каждому вектору $c = (c_0, \ldots, c_{n-1}) \in F_q^n$ соответствует полином $\text{poly}(c) = \sum\limits_{i=0}^{n-1} c_i x^i$.

Определение 1.11. [1] Пусть полиномы $r(x)$ и $s(x)$ имеют одинаковую степень.

Произведением Адамара полиномов $r(x)$ и $s(x)$ называется

$$r(x) \odot s(x) = \text{poly}\left(\text{coeff}\left(r\left(x\right)\right) \odot \text{coeff}\left(s\left(x\right)\right)\right)$$

Степени Адамара $r^{\langle i \rangle}$ полинома $r(x)$ определяются как

$$r^{\langle i \rangle} = \text{poly}\left(\left(\text{coeff}\left(r\left(x\right)\right)\right)^{\langle i \rangle}\right)$$

Определение 1.12. [5] Пусть $f(x) = a_0 + a_1 x + \cdots + a_r x^r$. $f^*(x) = a_r + a_{r-1}x + \cdots + a_0 x^r$ называется его обратным полиномом.

Определение 1.13. [1] Для любого ненулевого элемента a поля F, минимальное число l_a такое, что $a^{l_a} = 1$ называется порядком элемента a в поле F.

Определение 1.14. [1] Пусть $C \subseteq F^n$ линейный код. Последовательность $\dim\left(C^{\langle i \rangle}\right), i \geqslant 0$ называется последовательностью размерностей кода C.

Утверждение 1.1. *[4] Для любого линейного кода $C \subseteq F^n$ и $i \geqslant 0$*

$$\dim\left(C^{\langle i+1 \rangle}\right) \geqslant \dim\left(C^{\langle i \rangle}\right)$$

и

$$d_{min}\left(C^{\langle i+1 \rangle}\right) \leqslant d_{min}\left(C^{\langle i \rangle}\right)$$

Потому что последовательность размерностей кода монотонно неубывает и ограничена сверху длиной кода, то эта последовательность имеет предел.

Определение 1.15. [4] Минимальное положительное цилое число $r = r(C)$ такое, что для любого целого неотрицательного числа i выполняется равенство

$$\dim\left(C^{\langle r\rangle}\right) = \dim\left(C^{\langle r+i\rangle}\right)$$

называется регулярностью Кастельнуово-Мумфорда линейного кода C.

Утверждение 1.2. *[4]*
Для кода C и числа $i \in \{1, \ldots, r(C) - 1\}$

$$\dim\left(C^{\langle i+1\rangle}\right) > \dim\left(C^{\langle i\rangle}\right)$$

Утверждение 1.3. *[4] Пусть $C \subseteq F^n$ линейный код и t неотрицательное целое число. Тогда следующие условия эквивалентны.*

1) $t \geqslant r\,(C)$

2) $C^{\langle t\rangle}$ *имеет базис с непересекающимися носителями*

3) $\left(C^{\langle t\rangle}\right)^{\perp}$ *имеет базис, в котором веса всех векторов небольше двух.*

Через S_n далее обозначим группу перестановок на множестве I_n. Пусть $\sigma \in S_n$, C код длины n и $c = (c_1, c_2, \cdots, c_n)$ вектор длины n. То $c^{\sigma} = \left(c_{\sigma(1)}, c_{\sigma(2)}, \cdots, c_{\sigma(n)}\right)$, $C^{\sigma} = \{c^{\sigma} | c \in C\}$.

Определение 1.16. [6] Множество перестановок компонент кодовых слов кода C, переводящих каждое кодовое слово в кодовое слово, называется группой автоморфизмов кода C и обозначается $\mathrm{Aut}\,(C) = \{\sigma \in S_n | C^{\sigma} = C\}$

Группа автоморфизмов имеет очевидное свойство:

$$\forall i \geqslant 1, \mathrm{Aut}\,(C) \subseteq \mathrm{Aut}\left(C^{\langle i\rangle}\right)$$

Утверждение 1.4. *[7] Линейный код C и дуальный к нему код $C^{\perp}$ имеют одну и ту же группу автоморфизмов.*

Определение 1.17. [2] Пусть $U = \{x \odot y, x^{\perp}\}$. Множество формул над U описывается следующщии условиями:

1) Элемент $u \in U$ является формулой над U глубины 1

2) Пусть $v\left(x_1, x_2, \ldots, x_p\right)$ - формула над U глубины s. Тогда $x_{p+1} \odot v$ и $v^{\perp}$, где $x_{p+1}-$ символ переменной, являются формулами над U глубины $s+1$.

3) Других формул нет.

Определение 1.18. [2] Замыканием $[C]$ кода C называется множество всех кодов C', которые могут быть представлены в виде

$$C' = v\left(C, C, \ldots, C\right),$$

где $v\left(x_1, \ldots, x_p\right)$ - формула над U.

Утверждение 1.5. *[1] Пусть даны базисы двух линейных кодов C_1 и C_2, можно найти базис кода $C_1 \odot C_2$ за $O\left(n^4\right)$ операций.*

Лемма 1.1. *[8] Зная порождающую матрицу кода C, можно построить $C^{\langle h \rangle}$,где $r\left(C\right) \leqslant h \leqslant n$ за $O\left(n^4 log\left(n\right)\right)$ операций.*

Следствие 1.1. *Зная порождающую матрицу кода C, можно построить $C^{\langle w(r(C),\ell_\alpha)\rangle}$, где*

$$w\left(r\left(C\right), \ell_\alpha\right) = \begin{cases} \ell_\alpha + 1 \text{ при } r\left(C\right) \leqslant \ell_\alpha + 1 \\ m\ell_\alpha + 1 \text{ при } r\left(C\right) > \ell_\alpha + 1 \text{ где } m \text{ минимальное число такое,} \\ \text{что } m\ell_\alpha + 1 \geqslant r\left(C\right) \end{cases}$$

за $O\left(n^4 log\left(qn\right)\right)$ операций.

2. Свойства констациклических кодов

Определение 2.1. [1] Пусть $f(x) \in F[x]$–полином степени n. То для любого делителя $g(x)$ полинома $f(x)$ определяется множество

$$C = \{\text{coeff}(g(x) \cdot h(x) \mod f(x)) \mid h(x) \in F[x]/f(x)\} \subset F_q^n$$

Оно является линейным подпространством пространства F_q^n и называется кодом C, построенным на основе идеалов колец, который порождается $g(x)$. При этом $g(x)$ называется порождающим полиномом кода C.

Определение 2.2. [1] Код, построенный на основе идеалов колец по модулю $f(x) = x^n - a$ называется констациклическим линейным.
Через $C_{const}(g, n, a, q)$ далее обозначим констациклический линейный код C, порожденный полиномом $g(x)$ по модулю $f(x) = x^n - a \in F_q[x]$.

Определение 2.3. [1] Пусть $C = C_{const}(g, n, a, q)$,$c = \text{coeff}\,(h(x)\, g(x) \bmod f(x)) \in C$ кодовое слово для некоторого полинома $h\,(x) \in F_q[x]/f(x)$.

$$s_a^{(i)} c = \text{coeff}\left(x^i g(x)\, h(x) \mod f(x)\right)$$

Например, для кодового слова $c = (c_1, \ldots, c_n)$ $s_a^{(1)} c = (a \cdot c_n, c_1, c_2, \ldots, c_{n-1})$

Утверждение 2.1. *[1] Линейный код $C \subseteq F^n$ является констациклическим по модулю $x^n - a$ тогда и только тогда, когда он замкнут относительно констациклического сдвига:*

$$(c_1, \ldots, c_n) \mapsto (a \cdot c_n, c_0, \ldots, c_{n-1})$$

Утверждение 2.2. *[8] Для любого констациклического кода $C = C_{const}(g, n, a, q)$ размерности k, множество*

$$\left\{\text{coeff}\left(x^i g(x)\right) \mid 0 \leqslant i < k\right\}$$

образует базис кода C.
Матрица G_C размера $k \times n$, чья i-я строка равна $\text{coeff}(x^{i-1} g(x))$ *является порождающей матрицей констациклического кода C.*

$$G_C = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & c_0 & c_1 & \cdots & c_{n-k-1} & c_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & c_0 & \cdots & c_{n-k-2} & c_{n-k-1} & c_{n-k} & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \\ 0 & \cdots & 0 & 0 & c_0 & \cdots & c_{n-k-2} & c_{n-k-1} & c_{n-k} \end{bmatrix}$$

Утверждение 2.3. *[1] Применяя метод Гаусса к порождающей матрице G_C в 2.2, получают порождающую матрицу в систематическом виде, которая имеет вид $G_C^E = (E_k \mid P)$, где E_k единичная матрица размера $(k \times k)$, P некоторая матрица размера $(k \times (n-k))$.*

Утверждение 2.4. *[8] Пусть $C \subseteq F^n$ является констациклическим кодом размерности k. Кодовое слово $c \in C$ имеет k подряд нулей тогда и только тогда, когда $c = 0^n$.*

Утверждение 2.5. *[8] Любой констациклический код длины n размерности k имеет минимальное расстояние $d_{min} \geqslant \frac{n}{k}$. Если кодовое слово c имеет вес $\mathrm{wt}(c) = \frac{n}{k}$ и p – первая позиция ,где стоит ненулевой элемент, то кодовое слово c имеет носитель*

$$\mathrm{supp}(c) = \left\{p + z \cdot k, 0 \leqslant z < \frac{n}{k}\right\}$$

Замечание 2.1. $1 \leqslant p \leqslant k$, если $p > k$, то по лемме 2.4 $c = 0^n$.

Утверждение 2.6. *[8] Для любого констациклического кода $C \subseteq F^n$ размерности k даны j кодовых слов кода C, среди которых существуют k линейно независимых кодовых слов. Тогда можно найти порождающий многочлен $g_0(x)$ кода C за $O(j \cdot k \cdot n)$операций.*

Утверждение 2.7. *[8] Пусть $C \subseteq F^n$ является констациклическим кодом размерности k. Если $k > n/2$, то* $\dim(C^{\langle \ell_a+1 \rangle}) = \dim(C)$ *или* $\dim(C^{\langle \ell_a+1 \rangle}) = n$

Определение 2.4. [8] Пусть $C = C_{const}(g, n, a, q)$ и $g(0) = 1$.
Полином $p(x)$, который имеет возможную высшую степень $n - v$, где $v|n$, $p(0) = 1$, $p(x)|g(x)$ и носители $\left\{\mathrm{coeff}\left(x^i p(x)\right) \mid 0 \leqslant i < v\right\}$ непересекаются, называется полиномом-образцом порождающего полинома $g(x)$.

Замечание 2.2. Для любого порождающего полинома $g(x)$ его полином-образец всегда существует, так как $p(x) = 1$ удовлетворяет всем требованиям к полиному-образцу.

Утверждение 2.8. *[8] Пусть $C = C_{const}(g, n, a, q)$. Можно найти полином-образец $p(x)$ за $O\left(n^2\right)$ операций.*

Утверждение 2.9. *[1] Пусть $C = C_{const}(g_1, n, a, q)$ и $g_1(x)$ имеет полином-образец $p_1(x)$. Тогда для $z \geqslant r(C)$, порождающие полиномы $g_z(x)$ кодов $C^{\langle z \rangle}$ находятся по формуле $g_z(x) = p_1(x)^{\langle z \rangle}$.*

Лемма 2.1. *Пусть* $C = C_{const}\left(g\left(x\right), n, a, q\right)$.
$C^{\perp} = C_{const}\left(\left(\frac{f(x)}{g(x)}\right)^{*}, n, a^{-1}, q\right)$

Доказательство. Доказательство аналогично доказательству для циклических кодов в [9]. □

Лемма 2.2. *Пусть* $C_1 = C_{const}(g_1, n, a_1, q)$, $C_2 = C_{const}(g_2, n, a_2, q)$.
$C_1 \odot C_2 = C_{const}(g_3, n, a_1 \cdot a_2, q)$

Доказательство. Доказательство аналогично доказательству для констациклических кодов в [1],где $a_1 = a_2$. □

Лемма 2.3. *[1] Пусть* $C = C_{const}\left(g, n, a, q\right)$, $\dim\left(C\right) = k$.
Носители $\operatorname{supp}\left(x^i \cdot g\left(x\right)\right), 0 \leqslant i < k$ *непересекаются тогда и только тогда, когда* $g = \lambda \cdot \sum\limits_{i=0}^{\frac{n}{k}-1} \alpha^i x^{k \cdot i}$, *где* λ *обратим и* $\alpha^{\frac{n}{k}} = a^{-1}$.

Через $I_{n,\delta,i}$ далее обозначим множество $\left\{i, i+\delta, i+2\delta, i+\left(\frac{n}{\delta}-1\right)\delta\right\}$, где $\delta \mid n$ и i-ю строку матрицы A через $A[i]$.

Опишем группу автоморфизмов констациклических кодов, имеющих непересекающиеся носители.
Пусть Код C имеет базис с непересекающимися носителями. Тогда по лемме 2.3 порождающий полиномом $g\left(x\right) = \lambda \cdot \sum\limits_{i=0}^{\frac{n}{k}-1} \alpha^i x^{k \cdot i}$, где λ обратим и $\alpha^{\frac{n}{k}} = a^{-1}$. Тогда по утверждению 2.3 код C имеет порождающую матрицу G_C^E в систематическом виде, чья i-я строка равна $\operatorname{coeff}\left(x^{i-1} \sum\limits_{i=0}^{\frac{n}{k}-1} \alpha^i x^{k \cdot i}\right)$.

Заметим, что

- $\operatorname{supp}\left(G_C^E[i]\right) = I_{n,k,i}$
- $\forall \sigma \in \operatorname{Aut}\left(C\right), \sigma\left(\operatorname{supp}\left(G_C^E[i]\right)\right) = I_{n,k,j}$
- $\forall \sigma \in \operatorname{Aut}\left(C\right), \sigma\left(G_C^E[i]\right) = \lambda_i G_C^E[j]$

Замечание 2.3. Во втором пункте если $G_C^E[i]$ не переставляется в $I_{n,k,j}$, то в вектор, у которого есть k подряд 0, потому что по лемме 2.4 $\sigma\left(G_C^E[i]\right) = 0^n$.

Всего 4 случаев:

1) $\ell_\alpha > \frac{n}{k}$

2) $\ell_\alpha = \frac{n}{k}$

3) $\ell_\alpha < \frac{n}{k}$ и $\ell_\alpha \mid \frac{n}{k}$

4) $\ell_\alpha < \frac{n}{k}$ и $\ell_\alpha \nmid \frac{n}{k}$

Все числа ниже небольше n, если результат вычисления больше n, то вычитаем из него n. Пусть строки матрицы G_C^E имеют вид $c = (c_1, c_2, \ldots, c_n)$, тогда у них очевидное свойство $c_i = \alpha c_{i-k}$ для $\forall i > k$.

В первом случае:

В каждой строке среди всех ненулевых элементов можно взять только первый ненулевой элемент в качестве первого ненулевого элемента переставимой строки. То есть $\forall i \in I_k$, $\sigma(i) \in I_k$ и $\forall i \neq j \in I_k$, $\sigma(i) \neq \sigma(j)$.

Определив места первых ненулевых элементов всех строк, остальные ненулевые элементы располагаются единственным образом по свойству $c_i = \alpha c_{i-k}$ для $\forall i > k$.

Тогда $\forall \sigma \in \mathrm{Aut}(C)$ имеет вид

$$\forall 0 \leqslant i < \frac{n}{k},\ 1 \leqslant j \leqslant k,\ \sigma(i \cdot k + j) = i \cdot k + \mu_j,$$

где $\sigma(\{1, 2, ..., k\}) = \{\mu_1, \mu_2, ..., \mu_k\} = \{1, 2, ..., k\}$.

Всего $A_k^k = k!$ таких перестановок.

Во втором случае:

В каждой строке среди всех ненулевых элементов можно взять любой ненулевой элемент в качестве первого ненулевого элемента переставимой строки. То есть $\forall i \in I_k$, $\sigma(i) \in I_{n,k,\gamma_i}$ и $\forall i \neq j \in I_k$, $\gamma_i \neq \gamma_j$.

Определив места первых ненулевых элементов всех строк, остальные ненулевые элементы располагаются единственным образом по свойству $c_i = \alpha c_{i-k}$ для $\forall i > k$.

Тогда $\forall \sigma \in \mathrm{Aut}(C)$ имеет вид

$$\forall 0 \leqslant i < \frac{n}{k},\ 1 \leqslant j \leqslant k,\ \sigma(i \cdot k + j) = i \cdot k + \mu_j,$$

где $\mu_j \in I_{n,k,\gamma_j}$, $\{\gamma_1, ..., \gamma_k\} = I_k$

Всего $k!\left(\frac{n}{k}\right)^k$ таких перестановок.

В третьем случае:

В каждой строке среди всех ненулевых элементов можно взять любой ненулевой элемент в качестве первого ненулевого элемента переставимой строки.

Пусть $\frac{n}{k}/\ell_\alpha = \beta$.
$\forall\sigma \in \mathrm{Aut}\,(C)$ имеет вид

$$\sigma\,(j + (x\ell_\alpha + y)\,k) = \mu_j + (x'\ell_\alpha + y)\,k,$$

где $1 \leqslant j \leqslant k, 0 \leqslant x \leqslant \beta - 1, 0 \leqslant y \leqslant \ell_\alpha - 1$, $\mu_j \in I_{n,k,\gamma_j}$,
$\{\gamma_1, ..., \gamma_k\} = \{1, ..., k\}$ и для каждой пары (j, y)

$$\sigma\,(\{j+(x\ell_\alpha + y)\,k \,|\, x \in \{0, 1, \ldots, \beta - 1\}\}) = \left\{\mu_j+(x'\ell_\alpha + y)\,k \,|\, x' \in \{0, 1, \ldots, \beta - 1\}\right\}$$

Всего $k!{\ell_\alpha}^k(\beta!)^{k\ell_\alpha} = k!{\ell_\alpha}^k\left(\left(\frac{\frac{n}{k}}{\ell_\alpha}\right)!\right)^{k\ell_\alpha}$ таких перестановок.

В четвёртом случае:
В каждой строке среди всех ненулевых элементов можно взять любой ненулевой элемент в качестве первого ненулевого элемента переставимой строки.
Пусть $\frac{n}{k} \equiv \gamma\,(\mathrm{mod}\ell_\alpha)$ и $\left(\frac{n}{k} - \gamma\right)/\ell_\alpha = \beta$.
В каждой строке матрицы G_C^E γ ненулевых элементов появляются $\beta + 1$ раз и $(\ell_\alpha - \gamma)$ ненулевых элементов появляются β раз. $\forall\sigma \in \mathrm{Aut}\,(C)$ имеет вид

$$\sigma\,(j + (x\ell_\alpha + y)\,k) = \mu_j + (x'\ell_\alpha + y)\,k,$$

где $1 \leqslant j \leqslant k, 0 \leqslant x \leqslant \beta, 0 \leqslant y \leqslant \ell_\alpha - 1$, $\mu_j \in I_{n,k,\gamma_j}, \{\gamma_1, ..., \gamma_k\} = \{1, ..., k\}$

Замечание 2.4. При $x = \beta$, $0 \leqslant y \leqslant \gamma - 1$.

Для каждой пары (j, y), где $0 \leqslant y \leqslant \gamma - 1$

$$\sigma\,(\{j+(x\ell_\alpha + y)\,k \,|\, x \in \{0, 1, \ldots, \beta\}\}) = \left\{\mu_j+(x'\ell_\alpha + y)\,k \,|\, x' \in \{0, 1, \ldots, \beta\}\right\}$$

Для каждой пары (j, y), где $\gamma \leqslant y \leqslant \ell_\alpha - 1$

$$\sigma\,(\{j+(x\ell_\alpha + y)\,k \,|\, x \in \{0, 1, \ldots, \beta - 1\}\}) = \left\{\mu_j+(x'\ell_\alpha + y)\,k \,|\, x' \in \{0, 1, \ldots, \beta - 1\}\right\}$$

Всего $k!\left(\ell_\alpha((\beta + 1)!)^\gamma(\beta!)^{\ell_\alpha - \gamma}\right)^k = k!\left(\ell_\alpha(\beta!)^{\ell_\alpha}(\beta + 1)^\gamma\right)^k$ таких перестановок.

Утверждение 2.10. $x^t - b | x^n - a \Leftrightarrow t | n, b^{n/t} = a$

Доказательство. Необходимость. Пишем деление $x^n - a$ на $x^t - b$ столбиком, получим $t | n, b^{\frac{n}{t}} = a$.
Достаточность. Пусть $t | n, b^{n/t} = a$. Очевидно.

$$\sum_{i=0}^{\frac{n}{t}-1} b^{-i}x^{t\cdot i} = \frac{\left(x^t \cdot b^{-1}\right)^{\frac{n}{t}} - 1}{x^t \cdot b^{-1} - 1} = \frac{x^n \cdot b^{-\frac{n}{t}} - 1}{x^t \cdot b^{-1} - 1} = \frac{x^n \cdot a^{-1} - 1}{x^t \cdot b^{-1} - 1} = \frac{x^n - a}{x^t - b} \cdot \frac{b}{a}$$

□

Утверждение 2.11. *Замыкание констациклического кода* $C = C_{const}\,(x^t - b, n, a, q)$ *имеет вид*

$$[C] = \{F^n, \{0^n\}\} \cup \left\{\left(\left(C^{\perp}\right)^{\langle i\rangle}\right)^{\perp} \mid 1 \leqslant i \leqslant u\right\} \cup \left\{\left(C^{\perp}\right)^{\langle i\rangle} \mid 1 \leqslant i \leqslant u\right\} =$$

$$= \{F^n, \{0^n\}\} \cup \left\{C_{const}\left(g_i, n, a^i, q\right) \mid 1 \leqslant i \leqslant u\right\} \cup \left\{C_{const}\left(g_i', n, a^{-i}, q\right) \mid 1 \leqslant i \leqslant u\right\},$$

где $g_i(x) = x^t - b^i$, $g_i'(x) = \sum\limits_{j=0}^{\frac{n}{t}-1} b^{i\cdot j} x^{j\cdot t}$, $u = HOK(\ell_a, \ell_b)$.

Доказательство. Обозначим коды $(C^{\perp})^{\langle i\rangle}$ через C_i', $\left((C^{\perp})^{\langle i\rangle}\right)^{\perp}$ через C_i.
Вычисляем квадрат Адамара кода C, заметим, что $C^{\langle 2\rangle} = F^n$. Очевидно дуальный код к F_n это $\{0^n\}$.
Ищем дуальный код $C^{\perp}$. По лемме 2.1

$$C^{\perp} = C_{const}\left(\left(\frac{x^n - a}{x^t - b}\right)^*, n, a^{-1}, q\right) = C_{const}\left(g_1', n, a^{-1}, q\right)$$

Ищем степени Адамара кода C_1'. Он имеет базис с непересекающимися носителями, так что его степени Адамара легко находятся. Порождающий полином степени Адамара кода C_1' – это соотвествующая степень Адамара порождающего полинома кода C_1'. Получим

$$C_i' = C_1'^{\langle i\rangle} = C_{const}\left(g_i', n, a^{-i}, q\right)$$

Заметим, что $\forall i, j \geqslant 1, i \equiv j \pmod{u}$ тогда и только тогда, когда $C_i' = C_j'$.
Т.е. код имеет всего u разных степеней Адамара.
Для C_i' ищем дуальный к нему код C_i. По лемме 2.1

$$C_i = C_i'^{\perp} = C_{const}\left(\left(\frac{x^n - a^{-i}}{g_i'}\right)^*, n, a^i, q\right) = C_{const}\left(g_i, n, a^i, q\right)$$

Как степени Адамара кода C_1', число степеней Адамара кода C_1 тоже u:
$\forall i, j \geqslant 1, i \equiv j \pmod{u}$ тогда и только тогда, когда $C_i = C_j$.
Докажем, что в замыкании кода C других кодов нет.
Дуальный код любого кода замыкания кода C тоже принадлежит этому замыканию.
Произведение Адамара F^n и любого другого кода C'' – это C''.
Произведение Адамара $\{0^n\}$ и любого другого кода C'' – это $\{0^n\}$.
Произведение Адамара C_i и C_j – это C_{i+j}.

Произведение Адамара C'_i и C'_j – это C'_{i+j}.
Произведение Адамара C_i и C'_j – это F^n.
Всевозможные произведения Адамара и дуальные коды кодов искомого множества принадлежат искомому множеству. Это означает, что искомое множество является замыканием кода C. □

3. Криптосистема Мак-Элиса

Роберт Мак-Элиса в 1978 году [10]разработал криптосистему с открытым ключом на основе теории алгебраического кодирования. Эта криптосистема является одним из кандидатов для постквантовой криптографии, так как она устойчива к атаке с использованием алгоритма Шора.
Оригинальная криптосистема строится на основе двоичных кодов Гоппа, она достаточно безопасна, но при этом размер открытого ключа очень большой. Поэтому появляются другие варианты, которые построены на основе других линейных кодов, чтобы уменьшить размер открытого ключа и сохранить безопасность этой криптосистемы.
В этой криптосистеме выбирается некоторый линейный код, который имеет эффективные алгоритмы декодирования и порождающая матрица максированного кода берется в качестве открытый ключ. Его стойкость основана на сложности декодирования кода общего положения, которая является $\mathbb{NP}-$сложной задачей.

Пусть криптосистема строится на основе линейного кода с параметрами (n, k, d).

алгоритм генерации ключей

Вход: Порождающая матрица G_C кода C, где G_C имеет размер $k \times n$.

- Выбирается рандомно невырожденная матрица H размера $k \times k$.
- Выбирается рандомно перестановка σ на множестве I_n и его матрица P_σ размера $n \times n$.
- Вычислить открытый ключ $G'_C = H \cdot G_C \cdot P_\sigma$

Выход: Открытый ключ $\left(G_C, G'_C\right)$ и секретный ключ (H, P_σ)

алгоритм зашифрования

Вход: открытое сообщение m длины k

- Вычислить $x = m \cdot G'_C$.
- Выбрать вектор e длины n с весом не больше $\left\lfloor \frac{d-1}{2} \right\rfloor$.
- Вычислить $y = x + e$.

Выход: зашифрованное сообщение y.

алгоритм расшифрования

Вход: зашифрованное сообщение y.

- Вычислить $y' = y \cdot P_\sigma^{-1} = x \cdot P_\sigma^{-1} + e \cdot P_\sigma^{-1} = m \cdot H \cdot G + e^{\sigma^{-1}}$.
- Восстановить y' в кодовое слово x' кода C.
- Декодировать кодовое слово x' по порождающей матрице G, получить сообщение m'.
- Умножать сообщение m' справа на H^{-1}, получить открытое сообщение m.

Выход: открытое сообщение m

Определение 3.1. [11] Для заданного линейного кода C, два секретных ключа (H_1, P_{σ_1}) и (H_2, P_{σ_2}) называются эквивалентными, если и только если выполняется соотношение

$$H_1 \cdot G_C \cdot P_{\sigma_1} = H_2 \cdot G_C \cdot P_{\sigma_2}$$

то есть порождаемые ими открытые ключи совпадают.

Умножение матрицы G слева на невырожденную матрицу H – это по сути получение другой порождающей матрицы одного и того же кода. Умножение матрицы G справа на матрицу перестановки – это по сути получение порождающей матрицы кода C^σ.

М. А. Бородин, И. В. Чижов [2] построили эффективную атаку на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера. Она имеет полиномиальную сложность когда НОД$(r, m-1) = 1$. Идея атака состоится в находжения быстрого способа построения $RM^\sigma(1, m)$ с $RM^\sigma(r, m)$. В этой работе полностью описали замыкание $[RM(r, m)]$ кода $RM(r, m)$ и заметили, что если НОД$(r, m-1) = 1$ то $RM^\sigma(1, m) \in [RM^\sigma(r, m)]$.
Получив $RM^\sigma(1, m)$ лекго найти такую перестанову σ', что $\sigma \cdot \sigma' \in \mathrm{Aut}(RM(1, m))$. По свойству группах автоморфизмов замечаем, что $\sigma \cdot \sigma' \in \mathrm{Aut}\left(RM(1, m)^{\langle r \rangle}\right) = \mathrm{Aut}(RM(r, m))$. Иными словами, нашли перестановку σ', которая восстанавляет $RM^\sigma(r, m)$ в $RM(r, m)$.
Найдя σ', то можно решить уравнение $G'_C = H' G P_{\sigma'}$ за $O\left(n^3\right)$ операции.
То получили эквивалентный закрытому ключ $\left(H', \sigma'^{-1}\right)$.

Утверждение 3.1. *Пусть дан открытый ключ криптосистемы Мак-Элиса, построенной на основе констациклического кода C, который имеет базис с непересекающимися носителями. Тогда можно за* $O\left(q + n^3\right)$ *операций найти все перестановки, которые восстанавливают* C^σ *в* C.

Доказательство. Пусть $\dim(C) = v$, по лемме 2.3 $g(x) = \sum_{i=0}^{\frac{n}{v}-1} \alpha^i x^{v \cdot i}$

Применяя метод Гаусса к матрице G'_C, получаем матрицу $\left(G_C^E\right)^\sigma$, чьи строки имеют одинаковый вес $\frac{n}{v}$, причем их носители непересекаются. В этом процессе требуется $O\left(v^2 n\right)$ операций.

Дальше определяем порядок ℓ_α элемента α за $O(q)$ операций.

Рассматриваем 2 случая:

1) $\ell_\alpha > \frac{n}{v}$

2) $\ell_\alpha \leqslant \frac{n}{v}$

Считаем, что $\sigma\left(\operatorname{supp}\left(\left(G_C^E\right)^\sigma[i]\right)\right) = I_{n,v,i}$.

В первом случае:

Пусть $M_i = \left\{u_1, u_1\alpha, \ldots, u_1\alpha^{\frac{n}{v}-1}\right\}$ множество всех ненулевых элементов i-й строки матрицы $\left(G_C^E\right)^\sigma$ Для i-й строке матрицы $\left(G_C^E\right)^\sigma$, первый шаг это найти элемент, который переставляется в i-ю координату. Берем любой элемент w множества M_i и постепенно умножаем на его α^{-1} до тех пор, пока новое значение не принадлежит множеству M_i. То предпоследний получившийся в процессе число имено то что мы ищем.

Переставляем координату, где стоит u_i в i-ю координату и координаты, где стоят $u_i\alpha^j$ в $i + jv$-ые координаты. В этом процессе требуется $O\left(\frac{n}{v}v\right) = O(n)$ операций.

Во втором случае:

Для i-й строке, выбираем любой ненулевой элемент w и переставляем его координату в i-ю координату. Дальше переставляем координаты, где стоят ws^j в $i + jv$-ые координаты. В этом процессе тоже требуется $O\left(\frac{n}{v}v\right) = O(n)$ операций.

Тогда за $O\left(q+n^3\right)$ можно получить одну перестановку σ′, которая восстанавливает C^{σ} в C.

Множество всех таких перестановок, это σ′ Aut (C).

□

Алгоритм поиска эквивалентных открытых ключей криптосистемы Мак-Элиса, построенной на основе некоторых констациклических кодов

1) Определить точную верхнюю грань последовательности размерностей кода:
   По алгоритму в 2.8 лекго найти полином-образец $p(x)$ степени $n-v$ порождающего полинома $g(x)$.
   Где v означает точную верхнюю грань последовательности размерностей кода. То есть подтвердить, что полином-образец порождающего полинома не 1. Если он равен 1, то работа завершается.

2) По алгоритму в 1.1 построить код $(C^{\sigma})^{<w(r(C),\ell_{\alpha})>}$ по открытому ключу со сложностью $O(n^4 log(n))$.

3) По алгоритму в 3.1 найти все потенциальные ключи со сложностью $O\left(q+n^3\right)$.

4) Проверить, выполняется ли условие $\ell_{\alpha} > \frac{n}{v}$. Если да, то продолжить работу.

5) Перебирать всего $v!$ потенциальных ключей. Если по какому-то потенциальному ключу матрица H' находится, то эквивалентный ключ нашли.

В наилучшей ситуации, когда $\ell_{\alpha} > \frac{n}{v}$, алгоритм имеет сложность $O\left(n^4 log\,(n)+v!n^3\right)$.

4. Практика

Пусть дан открытый ключ G_C^σ криптосистемы Мак-Элиса, построенной на основе констациклического кода $C = C_{const}\,(x^t - b, n, a, q)$. По утверждению 1.4, можем найти σ' для $G_{C^\perp}^\sigma$, которая тоже восстанавляет G_C^σ в G_C. Причем $G_{C^\perp}^\sigma$ лекго восстанавляется в $G_{C^\perp}$, потому что он имеет базис с непересекающимися носителями.

Пример1 Пусть $q = 7$, $n = 8$, $a = 4$, $b = 3$, $t = 2$, $m := n/t = 4$. $f(x) = x^8 - 4$, $g(x) = x^2 - 3$. Причем $b^{n/t} = 3^4 = 81 \equiv 4 \,(\mod q = 7) = a \Leftrightarrow g(x)|f(x)$

$\alpha = 3$, $\ell_\alpha = 6 > \frac{n}{t} = 4$ $\frac{f(x)}{g(x)} = \sum\limits_{i=0}^{m-1} b^{m-1-i}x^{i\cdot t} = \sum\limits_{i=0}^{3} 3^{3-i}x^{2\cdot i} = x^6 + 3x^4 + 2x^2 + 6$

$p(x) = (\frac{f(x)}{g(x)})^* = \sum\limits_{i=0}^{m-1} b^{+i}x^{i\cdot t} = 6x^6 + 2x^4 + 3x^2 + 1$

$C = C_{const}(x^2 - 3, 8, 4, 7), C^\perp = C_{const}(6x^6 + 2x^4 + 3x^2 + 1, 8, 2, 7)$

$$G_C = \begin{pmatrix} 4 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 & 1 \end{pmatrix}$$

Произвольно выбираем невырожденную матрицу $H = \begin{pmatrix} 0 & 3 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 6 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$

Произвольно выбираем перестановку на I_n : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 1 & 3 & 7 & 5 & 6 & 8 \end{pmatrix}$

$$G_{C^\sigma} = G' = H \cdot G_C \cdot P_\sigma = \begin{pmatrix} 0 & 5 & 3 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 4 & 1 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 4 & 0 & 1 & 6 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 \end{pmatrix}$$

$$G_{C^{\sigma\perp}} = G_{C^{\perp\sigma}} = \begin{pmatrix} 1 & 0 & 0 & 5 & 0 & 2 & 3 & 0 \\ 0 & 1 & 3 & 0 & 2 & 0 & 0 & 6 \end{pmatrix}$$

$$G^E_{C^\perp} = \begin{pmatrix} 1 & 0 & 3 & 0 & 2 & 0 & 6 & 0 \\ 0 & 1 & 0 & 3 & 0 & 2 & 0 & 6 \end{pmatrix}$$

Сдесь $(\dim(C^\perp))! = 2! = 2$ варианта:

$\mathrm{supp}(G_{C^\perp\sigma}[1])\ I_{8,2,1}$

1) $\mathrm{supp}(G_{C^\perp\sigma}[1])$ переставляется в $I_{8,2,1}$
   $\mathrm{supp}(G_{C^\perp\sigma}[2])$ переставляется в$I_{8,2,2}$

2) $\mathrm{supp}(G_{C^\perp\sigma}[1])$ переставляется в $I_{8,2,2}$
   $\mathrm{supp}(G_{C^\perp\sigma}[2])$ переставляется в $I_{8,2,1}$

В первом случае множество M_1 ненулевых элементов первой строки матрицы $G_{C^\perp\sigma}$ – это $\{1, 5, 2, 3\}$. Берем его любой элемент, допускаем, чсило 1 выбрано. Умножаем его на α^{-1}: $1 * 5 = 5 \in M_1$. Умножаем 5 на α^{-1}: $5 * 5 = 4 \notin M_1$.

Тогда координата, где стоит элемент 5, переставляется в 1-ю координату. То есть $\sigma_1(4) = 1$

Координата, где стоит элемент $5 * \alpha = 1$, переставляется в $(1 + 2)$-ю координату. То есть $\sigma_1(1) = 3$.

Координата, где стоит элемент $1 * \alpha = 3$, переставляется в $(1 + 2 + 2)$-ю координату. То есть $\sigma_1(7) = 5$.

Координата, где стоит элемент $3 * \alpha = 2$, переставляется в $(1 + 2 + 2 + 2)$-ю координату. То есть $\sigma_1(6) = 7$.

$M_2 = \{1, 3, 2, 6\}$. Допускаем, что число 3 выбрано. Умножаем его на α^{-1}: $3 * 5 = 1 \in M_2$. Умножаем 1 на α^{-1}: $1 * 5 = 1 \notin M_2$.

Тогда координата, где стоит элемент 1, переставляется в 2-ю координату. То есть $\sigma_1(2) = 2$

Координата, где стоит элемент $1 * \alpha = 3$, переставляется в $(2 + 2)$-ю координату. То есть $\sigma_1(3) = 4$.

Координата, где стоит элемент $3 * \alpha = 2$, переставляется в $(2 + 2 + 2)$-ю координату. То есть $\sigma_1(5) = 6$.

Координата, где стоит элемент $2 * \alpha = 6$, переставляется в $(2 + 2 + 2 + 2)$-ю координату. То есть $\sigma_1(8) = 8$.

Получим $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 6 & 7 & 5 & 8 \end{pmatrix}$. Аналогично $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 3 & 2 & 5 & 8 & 6 & 7 \end{pmatrix}$

Теперь должны восстановить $G' \cdot P_{\sigma_i}$ в матрицу G путем решения системы линейных алгебраических уравнений $H_i G'_C P_{\sigma_i} = G_C$.

Получим: $H_1 = H^{-1} = \begin{pmatrix} 0 & 4 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$, $H_2 = \begin{pmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 4 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$

Пусть зашифруем сообщение $m = (1, 0, 1, 0, 0, 2)$

зашифрованное сообщение $x = m \cdot G' = (4, 6, 5, 0, 2, 0, 1, 4)$

В первом случае:

$x^{\sigma_1} = (0, 6, 4, 5, 1, 2, 0, 4)$

Декодируем этот кодовое слово, получаем $c_1 = (0, 5, 1, 0, 0, 4)$

Умножаем это кодовое слово справа на H_1 : $m = c_1 \cdot H_1 = (1, 0, 1, 0, 0, 2)$.

Во втором случае:

$x^{\sigma_2} = (6, 0, 5, 4, 2, 1, 4, 0)$

Декодируем этот кодовое слово, получаем $c_2 = (5, 0, 0, 1, 4, 0)$

Умножаем это кодовое слово справа на H_1 : $m = c_2 \cdot H_2 = (1, 0, 1, 0, 0, 2)$.

Пример2 Сравним $n!$ и $S = |\operatorname{Aut}(C^{\langle w(r(C),\ell_\alpha)\rangle})|$ тех констациклических кодов, которые предлагали в [1].

q	n	a	g	α	v	ℓ_α	$\frac{n}{v}$	$\ell_\alpha > \frac{n}{v}$?	$lg(n!)$	$lg\,(S)$	$lg(n!)/lg\,(S)$
7	18	-1	g_1	1	6	2	3	нет	15.8	6.5	2.4
7	12	-1	g_2	-1	6	2	2	нет	8.7	4.7	1.9
7	16	-1	g_3	-1	8	2	2	нет	13.3	7.0	1.9
7	20	-1	g_4	-1	5	2	4	нет	18.4	6.6	2.8
3	7	-1	g_5	-1	1	2	7	нет	3.7	2.5	1.5
3	20	-1	g_6	-1	4	2	5	нет	18.4	6.9	2.7
3	20	-1	g_7	-1	4	2	5	нет	18.4	6.9	2.7
3	25	-1	g_8	-1	5	2	5	нет	25.2	9.0	2.8
5	12	-2	g_9	-2	4	4	3	да	8.7	1.4	6.2
5	18	-2	g_{10}	-2	6	4	3	да	15.8	2.9	5.4
5	21	-2	g_{11}	-2	3	4	7	нет	19.7	5.3	3.7
5	21	-2	g_{12}	-2	7	4	3	да	19.7	3.7	5.3

$g_1(x)$	$x^{12} + x^6 + 1$
$g_2(x)$	$-x^8 - x^6 + x^2 + 1$
$g_3(x)$	$x^{14} + 3x^{13} + 3x^{12} - 2x^{11} - 3x^{10} + 3x^9 - x^8$ $-x^6 - 3x^5 - 3x^4 + 2x^3 + 3x^2 + 4x + 1$
$g_4(x)$	$-x^{16} - x^{15} + x^{11} + x^{10} - x^6 - x^5 + x + 1$
$g_5(x)$	$x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$
$g_6(x)$	$-x^{18} + x^{17} + x^{16} + x^{14} - x^{13} - x^{12} - x^{10}$ $+x^9 + x^8 + x^6 - x^5 - x^4 - x^2 + x + 1$
$g_7(x)$	$-x^{18} - x^{17} + x^{16} + x^{14} + x^{13} - x^{12} - x^{10}$ $-x^9 + x^8 + x^6 + x^5 - x^4 - x^2 - x + 1$
$g_8(x)$	$x^{21} + x^{20} + 2x^{16} + 2x^{15} + x^{11} + x^{10}$ $+2x^6 + 2x^5 + x + 1$
$g_9(x)$	$-x^8 - 2x^4 + 1$
$g_{10}(x)$	$x^{16} + x^{15} - x^{14} + 2x^{13} - x^{12} + 2x^{10} + 2x^9$ $-2x^8 - x^7 - 2x^6 - x^4 - x^3 + x^2 - 2x + 1$
$g_{11}(x)$	$2x^{19} - x^{18} - x^{16} - 2x^{15} - 2x^{13} + x^{12} + x^{10}$ $+2x^9 + 2x^7 - x^6 - x^4 - 2x^3 - 2x + 1$
$g_{12}(x)$	$2x^{15} - x^{14} - x^8 - 2x^7 - 2x + 1$

Замечание 4.1. Заметим, что по полиному-образцу неоднозначно определяется порождающий полином. Порождающие полиномы g_6 и g_7 имеют одинаковый полином-образец, который не 1.

5. Заключение и будущие направления

Заметили, что если последовательность размерностей кода не достигается до его длины n, то можно сузить пространство потенциальных ключей. В этом случае если порядок элемента α большой и точная верхняя грань последовательности размерностей мала, то пространство потенциальных ключей не так большое, стоит все потенциальные ключи перебрать.

Для некоторых кодов, чьи последовательности размерностей достигаются до n, их некоторые степени Адамара порождаются полиномами вида $x^t - b$, которые эквивалентные случаям, когда строится код с базисом с непересекающимися носителями. Можно как-то их отличить?

Существует ли метод, который не пытаясь решить алгебраические системы, быстро проверяет являются ли потенциальные ключи эквивалентными ключами?

Список литературы

1. *Falk B. H.*, *Heninger N.*, *Rudow M.* Properties of constacyclic codes under the Schur product // Designs, Codes and Cryptography. — 2020. — Т. 88, № 6. — С. 993—1021.
2. *Бородин М. А. Ч. И. В.* Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера // Дискретная математика. — 2014. — Т. 26. — С. 10—20. — DOI: 10.4213/dm1264.
3. *Mirandola D.* Schur products of linear codes: a study of parameters. — 2012.
4. *Hugues R.* On products and powers of linear codes under componentwise multiplication // Contemporary Mathematics. — 2013. — DOI: 10.1090/conm/637/12749.
5. *Martin A.* A course in enumeration //. Т. 238. — 2007. — С. 94. — DOI: 10.1007/978-3-540-39035-0.
6. *Логачёв О. А.* Криптографические свойства булевых функций. — 2011.
7. *ARF E.* Automorphism groups of cyclic codes. — 2009. — DOI: 10.13140/RG.2.1.4898.3528.
8. *Michael R.* Properties of Quasi-Cyclic Codes Under the Schur Product. — 2017.
9. *Мак-Вильямс Ф. Д.*, *Слоэн Н. Д. А.* Теория кодов, исправляющих ошибки. — Связь, 1979.
10. *Mceliece R.* A Public-Key Cryptosystem Based on Algebraic Coding Theory // JPL DSN Progress Report. — 1978. — Т. 44. — С. 123—125.
11. *Чижов И. В.* Ключевое пространство криптосистемы Мак-Элиса - Сидельникова // Дискретная математика. — 2009. — Т. 21. — С. 132—159. — DOI: 10.4213/dm1066.