НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«LOCKER - LOw rank parity ChecK codes EncRyption»

Виконали:
студенти V курсу, групи ФІ-32мн
Володимир Карловський
Дар'я Коваленко

Київ — 2023

1.1 Базові означення

Означення 1.1. Показник рангу над $F_{q^m}^n$ $x = (x_1, ..., x_n)$ - вектор в $F_{q^m}^n$ і $(\beta_1, ..., \beta_n)$ - базис в $F_{q^m}^m$.

Кожна координата x_j є вектором в F_q^m $x_j = \sum_{i=1}^m m_{ij}\beta_i$, де m_{ij} - елемент матриці $M(x)$

Тоді:

$$||x|| = RankM(x) \tag{1.1}$$

відстань між x та y $d(x, y) = ||x - y||$

Означення 1.2. F_{q^m} Лінійний код C розмірності k і довжини n це підпростір розмірності k простору $F_{q^m}^n$ вбудований з метрикою рангу.

Позначається $[n, k]_{q^m}$

C можна виразити двома способами

1) Через породжуючу матрицю $H \in F_{q^m}^{kn}$, кожен рядок матриці G елемент базису C:

$$C = \{xG, x \in F_{q^m}^k\} \tag{1.2}$$

2) Через матриця перевірки парності $H \in F_{q^m}^{(n-k)n}$ кожен рядок H визначає перевірку парності рівняння, перевірене елементами C:

$$C = \{x \in F_{q^m}^k, Hx^T = 0\} \tag{1.3}$$

Ми говоримо, що G (відповідно H) має систематичний вигляд, якщо він має форму $(I_k|A)$ (відповідно $(I_{n-k}|B)$).

Означення 1.3. (Підтримка слова) $x = (x_1, ..., x_n) \in F_{q^m}^n$.

Підтримка E з x, позначається $Supp(x)$, є F_q-підпростором F_{q^m}, породженим координатами x:

$$E =< x_1,...,x_n > F_q \tag{1.4}$$

$dimE = ||x||$.

Кількість опор розмірності w з F_{q^m} позначається коефіцієнтом Гауса

$$[\frac{m}{w}] = \prod_{i=0}^{w-1} \frac{q^m - q^i}{q^w - q^i} \tag{1.5}$$

1.2 Подвійний циркулянт і ідеальні коди

Щоб описати $[n,k]_{q^m}$ лінійний код, ми можемо дати його систематичну генераторну матрицю або його систематичну матрицю перевірки парності. В обох випадках кількість бітів, необхідних для

представлення такої матриці, дорівнює $k(n-k)m\log_2 q$. Щоб зменшити розмір подання коду, ми вводимо подвійні циркулянтні коди.

Спочатку нам потрібно визначити циркулянтні матриці.

Означення 1.4. (Циркулянтна матриця). Квадратна матриця M розміром $n \times n$ називається циркулянтом, якщо вона має форму:

$$M = \begin{bmatrix} m_0 & m_1 & m_2 & \dots & m_{n-1} \\ m_{n-1} & m_0 & m_1 & \dots & m_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ m_1 & m_2 & m_3 & \dots & m_0 \end{bmatrix} \tag{1.6}$$

Позначимо $M_n(F_{q^m})$ множину циркулянтних матриць розміру $n \times n$ над F_{q^m}. Наступне твердження визначає важливу властивість циркулянтних матриць.

Твердження 1.1. *$M_n(F_{q^m})$ є F_{q^m} -алгеброю, ізоморфною $F_{q^m}[X]/(X^n-1)$, тобто набору поліномів із коефіцієнтами у F_{q^m} за модулем (X^n-1). Канонічний ізоморфізм задано формулою*

$$\phi : F_{q^m}[X]/(X^n-1) \to M_n(F_{q^m}) \tag{1.7}$$

$$\sum_{i=0}^{n-1} m_i X^i \to \begin{bmatrix} m_0 & m_1 & m_2 & \dots & m_{n-1} \\ m_{n-1} & m_0 & m_1 & \dots & m_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ m_1 & m_2 & m_3 & \dots & m_0 \end{bmatrix} \tag{1.8}$$

Далі, щоб спростити позначення, ми будемо ідентифікувати поліном $G(X) = \sum_{i=0}^{n-1} g_i X^i \in F_{q^m}[X]$ з вектором $g = (g_0,...,g_{n-1}) \in F_{q^m}^n$.

Позначимо $ugmodP$ вектор коефіцієнтів полінома $(\sum_{j=0}^{n-1} u_j X^j)(\sum_{i=0}^{n-1} g_i X^i) mod P$ або просто ug, якщо немає неоднозначності у виборі полінома P.

Означення 1.5. (Подвійні циркулянтні коди) Лінійний код $[2n,n]_{q^m}C$ називається подвійним циркулянтом, якщо він має генеруючу матрицю G у вигляді $G = (A|B)$, де A і B є двома циркулянтними матрицями розміру n.

З попередніми позначеннями маємо $C = \{(xa,xb), x \in F_{q^m}\}$. Якщо a оборотне в $F_{q^m}[X]/(X^n-1)$

тоді $C = \{(x,xg), x \in F_{q^m}\}$, де $g = a^{-1}b$. У цьому випадку C породжується $g(modX^n-1)$. Таким чином, нам потрібно лише $nm\log_2 q$ бітів для опису $[2n,n]_{q^m}$ подвійного циркулянтного коду.

Ми можемо узагальнити подвійні циркулянтні коди, вибравши інший поліном P для визначення факторкільця $F_{q^m}[X]/(P)$.

Означення 1.6. (Ідеальні коди). Нехай $P(X) \in F_q[X]$ — поліном ступеня n і $g_1,g_2 \in F_{q^m}$. Нехай $G_1(X) = \sum_{i=0}^{n-1} g_{1i} X^i$, $G_2(X) = \sum_{j=0}^{n-1} g_{1j} X^j$ поліноми, асоційовані відповідно з g_1 і g_2.

За визначенням, $[2n,n]_{q^m}$ ідеальний код C генератора (g_1,g_2) є кодом з генераторною матрицею

$$G = \begin{bmatrix} G_1(X)modP & G_2(X)modP \\ XG_1(X)modP & XG_2(X)modP \\ \cdots & \cdots \\ X^{n-1}G_1(X)modP & X^{n-1}G_2(X)modP \end{bmatrix} \tag{1.9}$$

1.3 Складні задачі в ранговій метриці

У цьому розділі представляємо складні проблеми, на яких базується криптосистема.

Задача 1.1. (Розшифровка рангового синдрому) Дано матрицю повного рангу $H \in F_{q^m}^{(n-k)\times n}$ синдрому σ і ваги w, важко взяти вектор $x \in F_{q^m}$ ваги меншої за w так, що $Hx^T = \sigma^T$.

Проблема RSD нещодавно була доведена важкою для ймовірнісної редукції.

Задача 1.2. (Розшифровка синдрому ідеального рангу)
Заданий вектор $h \in F_{q^m}^n$ поліном P ступеня n, синдром σ і вага w, важко взяти вектор $x = (x_1, x_2)F_{q^m}^{2n}$ ваги меншої за w, так що $x_1 + x_2h = \sigma modP$

Оскільки h і P визначають систематичну матрицю перевірки парності ідеального коду $[2n,n]_{q^m}$, I-RSD Проблема є окремим випадком задачі RSD.

Задача 1.3. (Відновлення підтримки ідеального рангу) Дано вектор $h \in F_{q^m}$, поліном $P \in F_q[X]$ ступеня n, синдрому σ і ваги w, важко відновити опору E розмірності, нижчої за w, так що $e_1 + e_2h = \sigma modP$, де вектори e_1 і e_2 були відібрані з E.

Проблема I-RSR тривіально зводиться до задачі I-RSD. Дійсно, щоб відновити опору E екземпляра проблеми I-RSD із розв'язку x проблеми I-RSD, нам просто потрібно обчислити опору x. Відповідно, проблему I-RSD також можна звести до задачі I-RSR. Припустимо, що нам відомий носій E розв'язку задачі I-RSR для ваги w. Ми хочемо знайти $x = (x1,x2)$ ваги, меншої за w, щоб $x_1 + x_2h = \sigma modP$.

1.4 LOCKER IND-CPA PKE на основі метрики рангу

1.4.1 Визначення та модель безпеки

Схема шифрування з відкритим ключем (PKE - Public Key Encryption) визначається трьома алгоритмами: алгоритмом генерації ключів KeyGen, який приймає на вході параметр безпеки λ і виводить пару відкритих і закритих ключів (pk,sk); алгоритм шифрування

$Enc(pk,M)$, який виводить зашифрований текст C, що відповідає повідомленню M, і алгоритм дешифрування $Dec(sk,C)$, який виводить відкритий текст M. Схема PKE містить хеш-функцію G.

1) $KeyGen(1^\lambda)$:

а) виберемо незвідний поліном $P \in F_q[X]$ ступеня n.

б) вибрати рівномірно навмання підпростір F у F_{q^m} розмірності d і вибірку a пара векторів (x, y) $F^n \times F^n$ таких, що x є оборотним за модулем P, $Supp(x, y) = F$.

в) обчислити $h = x^{-1}ymodP$.

г) визначимо $pk = (h,P)$ і $sk = (x,y)$.

2) $Enc(pk,M)$:

а) вибрати рівномірно навмання підпростір E у F_{q^m} розмірності r і вибираємо пару векторів (e_1, e_2) $E_n \times E_n$, $Supp(e_1, e_2) = E$.

б) обчислити $c = e_1 + e_2hmodP$ і $\tilde{C} = M \oplus G(E)$.

в) вивести зашифрований текст $C = (c, \tilde{C})$.

3) $Dec(sk,C)$:

а) обчислити $xc = xe_1 + ye_2modP$ і відновити E за допомогою алгоритму відновлення підтримки.

б) результат $M = \tilde{C} \oplus G(E)$.

Коректність: оскільки P знаходиться у $F_q[X]$, xc має підтримку в просторі продукту $< E.F >$, отже, знаючи F, можна застосувати алгоритм RS-Recover з попереднього розділу, який відновлює E.

Обчислювальна вартість: Вартість $Encaps$ відповідає поліноміальній інверсії $modP$ у F_{q^m}, для вартості множення елементів F_{q^m} у $m\log(m)\log(\log(m))$, ми отримуємо складність шифрування в $O(n^2\log(n)m\log(m)\log(\log(m)))$. Вартість $Decaps$ — це матриця-вектор множення вартості $O(n^2m\log(m)\log(\log(m)))$ плюс вартість декодування алгоритму RS-Recover (перетинів підпросторів розмірності rd у F_{q^m}) у $O((rd)^2m)$.