

**ОПИСАНИЕ КЛАССОВ ЭКВИВАЛЕНТНОСТИ
СЕКРЕТНЫХ КЛЮЧЕЙ КРИПТОСИСТЕМЫ
МАК-ЭЛИСА–СИДЕЛЬНИКОВА С
ПРЕДСТАВИТЕЛЯМИ ОСОВОГО ВИДА**

Бусяк Мария Юрьевна

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: mbusyak@gmail.com

Криптосистема Мак-Элиса–Сидельникова — криптосистема с открытым ключом, основанная на декодировании кодов общего положения, является модификацией криптосистемы Мак-Элиса, использующей коды Рида-Маллера. Кодовые криптосистемы имеют особенность, отличающую их от других криптосистем: в них одному и тому же открытому ключу могут соответствовать несколько секретных ключей, то есть секретные ключи разбиваются на классы эквивалентности. Изучение таких классов существенно, так как возможность с некоторой достаточно большой вероятностью подобрать эквивалентный ключ снижает стойкость криптосистемы.

Пусть R есть стандартная порождающая матрица кода Рида-Маллера размера $(k \times n)$, H_1, H_2 — невырожденные матрицы размера $(k \times k)$, Γ — перестановочная матрица размера $(2n \times 2n)$. Тогда криптосистема Мак-Элиса–Сидельникова с параметром $u = 2$ описывается секретным ключом (H_1, H_2, Γ) и открытым ключом $(H_1 R || H_2 R) \Gamma$.

В [1] было доказано взаимно-однозначное соответствие между классом эквивалентности секретных ключей $[(H_1, H_2, \Gamma)]$ и множеством $\mathcal{G}(H_1, H_2)$, состоящим из подстановок Γ таких, что выполняется равенство: $(H_1 R || H_2 R) \Gamma = (H'_1 R || H'_2 R)$, где H'_1, H'_2 — невырожденные матрицы.

Наша задача — построить множество $\mathcal{G}(H_1, H_2)$, где $H_1 = E$ есть единичная матрица, H_2 обозначим как T . Для кода Рида-Маллера $RM(r, m) = RM(2, 6)$ нам бы пришлось перебирать все матрицы Γ и для каждой матрицы проверять, что в $(R || TR) \Gamma = (H'_1 R || H'_2 R)$ строки матриц H'_1, H'_2 принадлежат коду Рида-Маллера, что составляет $(2n)!$ вариантов. В случае $m = 6$ получаем $(2 \cdot 2^6)! \approx 10^{215}$ вариантов, что достаточно ресурсоемко. Наша задача — уменьшить мощность множества перебора.

Матрицу Γ можно представить в виде $\Gamma_0(\Gamma_1 || \Gamma_2)$, где Γ_1, Γ_2 суть перестановки столбцов внутри каждого блока, Γ_0 — перестановка столбцов между блоками. Тогда $(R || TR) \Gamma_0 = (H'_1 R \Gamma_1^{-1} || H'_2 R \Gamma_2^{-1})$.

Будем перебирать матрицы Γ_0 , и с помощью атаки Чижова-Бородина [2] искать матрицы Γ_1, Γ_2 . В случае успеха такой набор будет принадлежать множеству $\mathcal{G}(E, T)$.

Обозначим, через z вектор инцидентности переставляемых столбцов матрицы Γ_0 .

Теорема 1. *Если матрица Γ_0 задана вектором z , то*

$$1. z \in (RM(r, m)[T])^\perp$$

$$2. wt(z_l) = wt(z_r)$$

Теорема 2. *Если $(R||TR)\Gamma \subset RM(r, m) \times RM(r, m)$, то $((R||TR)^2)\Gamma \subset RM(2r, m) \times RM(2r, m)$*

Следовательно, нам достаточно перебрать все слова кода, дуального к $(RM(r, m)[T])^2$. Размерность такого кода не более, чем $k \cdot k = \left(1 + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{m-2r-1}\right) \left(1 + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{m-2r-1}\right)$.

Количество перебираемых слов не более $2^{k \cdot k}$. Для $m = 6, r = 2$ получаем $2^{\sum_{i=0}^{m-2r-1} \binom{m}{i} \sum_{i=0}^{m-2r-1} \binom{m}{i}} = 2^{\sum_{i=0}^1 \binom{6}{i} \sum_{i=0}^1 \binom{6}{i}} = 2^{49} \approx 10^{15}$.

Таким образом, мы получаем уменьшение множества перебора по меньшей мере в 10^{200} раз.

Литература

1. Чижов И. В. Пространство ключей криптосистемы Мак-Элиса-Сидельникова. Диссертация на соискание ученой степени кандидата физико-математических наук по специальности 05.13.19. МГУ им. М. В. Ломоносова, 2010.
2. Чижов И. В., Бородин М. А. Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида-Маллера. Дискретная математика, 2014, том 26, выпуск 1, 10–20.
3. McEliece R. J. A public-key cryptosystem based on algebraic coding theory. The Deep Space Network Progress Report, DSN PR 42-44, 1978, pp. 114-116.