Описание классов эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова

Кирюткина Виктория Владимировна

Студентка

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

E-mail: kiryutkina.v@gmail.com

Криптосистема Мак-Элиса–Сидельникова [1] является модификацией распространенной кодовой криптосистемы Мак-Элиса [4]. Кодовыми называются криптосистемы, основанные на задачах из теории кодов, исправляющих ошибки. Такие системы обладают одной отличительной особенностью: одному и тому же открытому ключу может соответствовать некоторое множество секретных ключей, поэтому секретные ключи могут быть разбиты на классы эквивалентности. Вопрос изучения этих классов важен, так как знание их структуры позволяет строить эффективные атаки на кодовые криптосистемы [2].

Секретным ключом криптосистемы Мак-Элиса–Сидельникова является кортеж (H_1, H_2, Γ). Здесь H_1, H_2, Γ — матрицы над полем $GF(2)$, причем H_1, H_2 — невырожденные, а Γ — перестановочная. Открытым ключом криптосистемы является матрица $G' = (H_1 R \,||\, H_2 R) \cdot \Gamma$, где символом $||$ обозначена конкатенация матриц по столбцам, а R — стандартная форма порождающей матрицы кода Рида–Маллера $RM(r, m)$.

В диссертации И. В. Чижова [3] была установлена связь между классом эквивалентности $[(H_1, H_2, \Gamma)]$ секретных ключей и множеством $\mathcal{G}(H_1, H_2)$, состоящим из подстановок Γ, для которых существуют невырожденные двоичные матрицы H_1', H_2' такие, что $(H_1 R \,||\, H_2 R) \cdot \Gamma = (H_1' R \,||\, H_2' R)$. Поэтому задача изучения классов эквивалентности секретных ключей свелась к задаче изучения структуры множества $\mathcal{G}$.

Обозначим за $\mathcal{C}$ код с порождающей матрицей $(R \,||\, HR)$, где $H = H_1^{-1} H_2$).

Утверждение. $\mathcal{C}^2 \subseteq RM(2r, m) \times RM(2r, m)$.

Теорема. Если $\mathcal{C}^2 = RM(2r, m) \times RM(2r, m)$, то $\mathcal{G} = \mathrm{Aut}(RM(r, m)) \times \mathrm{Aut}(RM(r, m))$.

Таким образом, для случая равенства можно получить описание классов эквивалентности.

В случае строгого вложения можно рассмотреть матрицу H специального вида такую, что в ней существует ортогональная подматрица $\hat{H}$, которая расположена с точностью до перестановки строк и столбцов следующим образом:

$$H = \left[\begin{array}{c|c} \hat{H} & H_1 \\ \hline 0 & H_2 \end{array}\right].$$

Для матрицы такого вида верны следующие факты.

Теорема. Если матрица H имеет специальный вид, то имеет место строгое вложение $\mathcal{C}^2 \subset RM(2r, m) \times RM(2r, m)$.

Теорема. Если выполнено строгое вложение $\mathcal{C}^2 \subset RM(2r, m) \times RM(2r, m)$, и подпространство, порожденное строками матрицы $(H^T \,|\, 0 \,||\, E \,|\, 0)$, пересекается с $(\mathcal{C}^2)^{\perp}$, то матрица H имеет специальный вид.

Утверждение. Доля матриц специального вида среди невырожденных матриц размера $k \times k$ есть $O(k^2 2^{-k})$.

Таким образом, доля матриц H специального вида мала, а значит, почти всегда известна структура множества $\mathcal{G}$ и можно описать классы эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова.

Литература

1. Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида-Маллера. // Дискретная математика. 1994. Т. 6, No. 2. С. 3–20.
2. Сидельников В. М., Шестаков С. О. О системе шифрования, построенной на основе обобщенных кодов Рида–Соломона. // Дискретная математика. 1992. Т. 4, No. 3. С. 57–63.
3. Чижов И. В. Пространство ключей криптосистемы Мак-Элиса–Сидельникова. // Диссертация на соискание ученой степени кандидата физико-математических наук по специальности 05.13.19. МГУ имени М. В. Ломоносова, 2010.
4. McEliece R. J. A public-key cryptosystem based on algebraic coding theory. // DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol. 1978, Vol. January. P. 114–116.