екторий, соответствующих определенному сценарию, и осуществляет полный перебор возможных траекторий. Исходный код доступен по адресу http://www.proverif.ens.fr/.

УДК 519.725

ОБОБЩЕННЫЕ АВТОМОРФИЗМЫ КОДА РИДА–МАЛЛЕРА И КРИПТОСИСТЕМА МАК-ЭЛИСА–СИДЕЛЬНИКОВА

И. В. Чижов

Криптосистема Мак-Элиса–Сидельникова относится к классу кодовых криптосистем с открытым ключом. Криптосистема была предложена В. М. Сидельниковым в работе [1].

Кратко опишем устройство криптосистемы Мак-Элиса–Сидельникова. Пусть R — $(k \times n)$-порождающая матрица кода Рида–Маллера $RM(r, m)$. Секретным ключом криптосистемы является кортеж $(H_1, H_2, \ldots, H_u, \Gamma)$. Здесь $H_1, H_2, \ldots, H_u$ — невырожденные $k \times k$-матрицы над полем $F_2 = \{0, 1\}$, которые выбираются случайно и равновероятно из множества $GL_k(F_2)$ всех двоичных невырожденных $k \times k$-матриц над полем F_2. Матрица Γ — перестановочная $(u \cdot n \times u \cdot n)$-матрица.

Открытым ключом криптосистемы Мак-Элиса–Сидельникова является матрица $G' = (H_1R \| H_2R \| \ldots \| H_uR) \cdot \Gamma$, где символом $\|$ обозначена конкатенация матриц по столбцам. Алгоритмы шифрования и расшифрования подробно описаны в [1].

Два секретных ключа $(H_1, H_2, \ldots, H_u, \Gamma)$ и $(H'_1, H'_2, \ldots, H'_u, \Gamma')$ назовём *эквивалентными*, если соответствующие им открытые ключи совпадают, то есть выполняется соотношение $(H_1R \| H_2R \| \ldots \| H_uR) \cdot \Gamma = (H'_1R \| H'_2R \| \ldots \| H'_uR) \cdot \Gamma'$.

Рассмотрим множество $\mathcal{G}(H_1, H_2, \ldots, H_u)$, состоящее из перестановок $\Gamma \in S_{un}$, для которых существуют невырожденные двоичные матрицы H'_1, H'_2, …, H'_u, такие, что $(H_1R \| H_2R \| \ldots \| H_uR)\Gamma = (H'_1R \| H'_2R \| \ldots \| H'_uR)$. В работе такие множества называются множествами обобщённых автоморфизмов кода Рида–Маллера. Отметим, что эти множества, в отличие от множества обычных автоморфизмов, не всегда являются группами.

Вопрос изучения эквивалентных секретных ключей, а значит, и вопрос изучения множества открытых ключей, сводится к изучению множеств $\mathcal{G}(H_1, \ldots, H_u)$, то есть обобщённых автоморфизмов.

Обобщённые автоморфизмы и структура множества открытых ключей могут оказаться полезными для криптоанализа криптосистемы Мак-Элиса–Сидельникова. Так, знание некоторой структуры группы автоморфизмов обощённых кодов Рида–Соломона позволило В. М. Сидельникову и С. О. Шестакову [2] произвести взлом криптосистемы Мак-Элиса на основе этих кодов.

Перейдём к описанию множеств обобщённых автоморфизмов.

В случае произвольного u справедлива следующая теорема.

Теорема 1. Пусть для невырожденных матриц $D_1, D_2, \ldots, D_u$ существуют такие перестановки $P_i (1 \leqslant i \leqslant n)$ из S_n, что $D_1R = R \cdot P_1$, $D_2R = R \cdot P_2, \ldots, D_uR = R \cdot P_u$. Обозначим через $\mathcal{P}_1[1]$,$\mathcal{P}_2[2]$,…,$\mathcal{P}_u[u]$ перестановки из $\mathcal{A}_u(RM(r, m))$, соответствующие перестановкам $P_1, P_2 \ldots, P_u$. И пусть H — любая невырожденная матрица.

Тогда $\mathcal{G}(E, \ldots, E) = \mathcal{P}_1[1] \cdot \mathcal{P}_2[2] \ldots \mathcal{P}_u[u] \cdot \mathcal{G}(HD_1, \ldots, HD_u)$.

Описание множества $\mathcal{G}(E, \ldots, E)$ получено Г. А. Карпуниным [3].

Рассмотрим теперь случай $u = 2$.

Для некоторого вектора $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\alpha_i = 1$, рассмотрим матрицу $T^i_{\tilde{\alpha}}$ вида

$$T^i_{\tilde{\alpha}} = \begin{pmatrix} & & & & i & & \\ & & & & \downarrow & & \\ & 1 & 0 & \ldots & 0 & \ldots & 0 \\ & 0 & 1 & \ldots & 0 & \ldots & 0 \\ & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ i \to & \alpha_1 & \alpha_2 & \ldots & 1 & \ldots & \alpha_{k-1} \\ & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ & 0 & 0 & \ldots & 0 & \ldots & 1 \\ & & & & & & \end{pmatrix}.$$

Первый случай — $i = 1$. Справедлива теорема.

Теорема 2. Пусть $i = 1$, тогда

$$\mathcal{G}(E, T^1_{\tilde{\alpha}}) = \{\Gamma \in \mathcal{G}(E, E) | (0 \| (e^1 \oplus \tilde{\alpha})R)\Gamma \in RM(r, m) \times RM(r, m)\}.$$

Здесь символом e^1 обозначен вектор, у которого на первом месте стоит 1, а на всех остальных местах — 0.

При изучении обобщенных автоморфизмов в случае $i > 1$ возникает необходимость в исследовании эквивалентности некоторых специальных $(k-1)$-мерных подпространств кода Рида–Маллера $RM(r, m)$. В результате изучения подпространств кода Рида–Маллера получено описание множества $\mathcal{G}(E, T^i_{\tilde{\alpha}})$ для $i > 1$. Теорема 3 даёт это описание.

Теорема 3. Пусть $RM(r, m)$ — код Рида–Маллера, такой, что $2r \leqslant m$, $i > 1$, H — любая невырожденная двоичная матрица, α — произвольный двоичный вектор, у которого в координате с номером i стоит единица. Тогда множество $\mathcal{G}(H, HT^i_{\tilde{\alpha}})$ содержит те и только те перестановки Γ, которые могут быть представлены в виде $\Gamma = \Gamma' \cdot (\sigma_L \| \sigma_R)$, где σ_L, σ_R — автоморфизмы кода Рида–Маллера $RM(r, m)$, а для перестановки Γ' выполняются два условия:

1) если R' — $(k-1) \times n$-матрица, получающаяся выкидыванием строки с номером i из матрицы R, то $(R' \| R')\Gamma' = (R' \| R')$;
2) если r^i — строка матрицы R с номером i, то $(r^i \| \widetilde{\alpha} R)\Gamma' \in RM(r, m) \times RM(r, m)$.

ЛИТЕРАТУРА

1. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида–Маллера // Дискретная математика. 1998. Т. 6. № 3. 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. № 3. С. 57–63.
3. *Карпунин Г. А.* О ключевом пространстве криптосистемы Мак-Элиса на основе двоичных кодов Рида–Маллера // Дискретная математика. 2004. Т. 16. № 2. С. 79–84.
4. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory //The Deep Space Network Progress Report, DSN PR 42–44, January and February 1978. P. 114–116.
5. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.