Значения δ_{ij} можно найти как решение соответствующей системы линейных уравнений, например методом Гаусса. После этого, подставив в правую часть вместо матрицы G матрицу B', Джон получит сформированный ключ K и сможет читать все сообщения, которые отправляют Алиса и Боб между собой:

$$\sum_{i,j=1}^{8} \delta_{ij}(PE_iP^{-1})B'(PE_jP^{-1}) = \sum_{i,j=1}^{8} \delta_{ij}(PE_iP^{-1})(PD_B^{r_1}P^{-1})G(PD_B^{r_2}P^{-1})(PE_jP^{-1}) =$$

$$= \sum_{i,j=1}^{8} (PD_B^{r_1}P^{-1}) \left(\delta_{ij}(PE_iP^{-1})G(PE_jP^{-1})\right) (PD_B^{r_2}P^{-1}) =$$

$$= (PD_B^{r_1}P^{-1}) \left(\sum_{i,j=1}^{8} \delta_{ij}(PE_iP^{-1})G(PE_jP^{-1}) \right) (PD_B^{r_2}P^{-1}) =$$

$$= B^{r_1} \left(\sum_{i,j=1}^{8} \delta_{ij}(PE_iP^{-1})G(PE_jP^{-1}) \right) B^{r_2} = B^{r_1}A'B^{r_2} = K.$$

Заключение

Данная атака основана на методе линейной разложимости [3]. Для её осуществления достаточно, чтобы протокол строился на линейной группе. Необходимые вычисления выполняются методом Гаусса, который квадратичен по числу уравнений и линеен по числу неизвестных. Заметим, что достаточно найти любое частное решение соответствующей системы линейных уравнений. Уравнений в данном случае 64 (число элементов в матрице), неизвестных 64 (коэффициенты в разложении). При атаке «грубой силой» пришлось бы подбирать параметры k_1, k_2, r_1 и r_2. Этот перебор может быть ограничен, но ограничение не может быть меньше, чем порядок мультипликативной группы поля для каждого из этих параметров. Кроме того, пришлось бы подбирать ненулевые элементы поля $\alpha_1, \ldots, \alpha_8, \beta_1, \ldots, \beta_8$. Размер этого ключевого пространства 250^{16}. Атака методом линейного разложения на рассматриваемый протокол является не только эффективной, но и практически реализуемой. От общей схемы атаки методом линейного разложения на протокол Шпильрайна — Ушакова [3] рассматриваемая атака отличается тем, что для неё нет необходимости строить базисы линейных подпространств, без чего не обойтись в общем случае.

ЛИТЕРАТУРА

1. *Hecht P.* Post-Quantum Cryptography (PQC): Generalized ElGamal Cipher over GF(251^8). arXiv:1702.03587v1 [cs.CR], 12 Feb 2017. 6 p.
2. *Shpilrain V. and Ushakov A.* Thompson's group and public key cryptography // LNCS. 2005. V. 3531. P. 151–164.
3. *Романьков В. А.* Алгебраическая криптография. Омск : Изд-во Ом. ун-та, 2013. 135 с.

УДК 003.26, 519.725 DOI 10.17223/2226308X/10/28

КВАДРАТ КОДА РИДА — МАЛЛЕРА И КЛАССЫ ЭКВИВАЛЕНТНОСТИ СЕКРЕТНЫХ КЛЮЧЕЙ КРИПТОСИСТЕМЫ МАК-ЭЛИСА — СИДЕЛЬНИКОВА

В. В. Высоцкая

Исследован вид классов эквивалентности секретных ключей криптосистемы Мак-Элиса — Сидельникова. Найден вид этих классов в случае, когда квадрат кода

с порождающей матрицей $(R|HR)$, где R — порождающая матрица кода Рида — Маллера порядка r и длины 2^m (то есть $\mathrm{RM}(r,m)$), равен декартову квадрату кода порядка $2r$ той же длины. В данном случае существует взаимно однозначное соответствие класса эквивалентности и декартова квадрата группы автоморфизмов кодов $\mathrm{RM}(r,m)$. Показано, что доля остальных случаев стремится к нулю при стремлении размерности кода к бесконечности.

Ключевые слова: *криптосистема Мак-Элиса — Сидельникова, код Рида — Маллера, квадрат кода, классы эквивалентности.*

Криптосистема Мак-Элиса — Сидельникова [1] является модификацией распространённой кодовой криптосистемы Мак-Элиса [2]. 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 актуален, так как знание их структуры позволяет строить эффективные атаки на кодовые криптосистемы [3].

Секретным ключом криптосистемы Мак-Элиса — Сидельникова является кортеж (H_1, H_2, Γ), где H_1, H_2, Γ — матрицы над полем $\mathrm{GF}(2)$, причём 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; R — стандартная форма порождающей матрицы кода Рида — Маллера $\mathrm{RM}(r,m)$.

В [4] установлена связь между классом эквивалентности $[(H_1, H_2, \Gamma)]$ секретных ключей и множеством $\mathcal{G}(H_1, H_2)$ 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 $\mathcal{G}$.

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

Утверждение 1. $\mathcal{C}^2 \subseteq \mathrm{RM}(2r,m) \times \mathrm{RM}(2r,m)$.

Теорема 1. Если $\mathcal{C}^2 = \mathrm{RM}(2r,m) \times \mathrm{RM}(2r,m)$, то

$$\mathcal{G} = \mathrm{Aut}(\mathrm{RM}(r,m)) \times \mathrm{Aut}(\mathrm{RM}(r,m)).$$

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:

$$H = \left[\begin{array}{c|c} \hat{H} & H_1 \\ \hline 0 & H_2 \end{array}\right]. \tag{1}$$

Для матрицы вида (1) верны следующие факты.

Теорема 2. Если матрица H имеет вид (1), то имеет место строгое вложение $\mathcal{C}^2 \subset \mathrm{RM}(2r,m) \times \mathrm{RM}(2r,m)$.

Теорема 3. Если выполнено строгое вложение $\mathcal{C}^2 \subset \mathrm{RM}(2r,m) \times \mathrm{RM}(2r,m)$ и подпространство, порождённое строками матрицы $(H^T \,|\, 0 \,||\, E \,|\, 0)$, пересекается с $(\mathcal{C}^2)^\perp$, то матрица H имеет вид (1).

Утверждение 2. Доля матриц вида (1) среди невырожденных матриц размера $k \times k$ есть $O(k^2 2^{-k})$.

Таким образом, доля матриц H вида (1) 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. № 2. С. 3–20.
2. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Progress Report. 1978. V. 42–44. P. 114–116.
3. *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.
4. *Чижов И. В.* Пространство ключей криптосистемы Мак-Элиса — Сидельникова: дис. ... канд. физ.-мат. наук. М.: МГУ, 2010.

УДК 512.6: 003.26 DOI 10.17223/2226308X/10/29

О ЯВНЫХ КОНСТРУКЦИЯХ ДЛЯ РЕШЕНИЯ ЗАДАЧИ “A SECRET SHARING”

К. Л. Геут, К. А. Кириенко, П. О. Садков, Р. И. Таскин, С. С. Титов

Рассматривается следующая задача: построить подмножество $M \subset \mathbb{F}_2^n$, удовлетворяющее двум условиям: 1) каждый элемент $u \in M$ может быть представлен в виде суммы трёх различных элементов множества $\overline{M} = \mathbb{F}_2^n \setminus M$; 2) сумма любых трёх различных элементов из $\overline{M}$ принадлежит M. Излагаются подходы к решению этой проблемы, в частности, для чётной размерности предложена явная конструкция искомого множества на основе кубической параболы.

Ключевые слова: *NSUCRYPTO-2015, поле Галуа, кривая, разделение секрета.*

Во втором раунде олимпиады по криптографии NSUCRYPTO-2015 [1] была предложена задача на специальный приз программного комитета Problem 1 “A secret sharing”, в ноябре 2016 г. отмеченная как все ещё не решённая [2].

Постановка задачи требует предложить для каждого натурального $n \in \mathbb{N}$ явную конструкцию подмножества M множества $\mathbb{F}_2^n$ всех битовых строк длины n, удовлетворяющего следующим двум условиям:

1) каждый элемент $u \in M$ может быть представлен в виде $u = x \oplus y \oplus z$, где x, y, z — различные элементы множества $\overline{M} = \mathbb{F}_2^n \setminus M$;
2) для всех различных $x, y, z \in \overline{M}$ справедливо $x \oplus y \oplus z \in M$.

Обозначая $L = \overline{M}$, можем переписать условия 1 и 2 для L. Как показывают вычислительные эксперименты, $|L| \approx 2^{n/2}$. Это оправдывает подход к построению L в виде кривой при чётном $n = 2m$.

Пусть $n = 2m$ ($m \in \mathbb{N}$); представим $\mathbb{F}_2^n$ в виде декартова произведения $\mathbb{F}_2^n = \mathbb{F}_2^m \times \mathbb{F}_2^m$, а множество L — в виде кривой, состоящей из точек (x, y) этой плоскости, удовлетворяющих уравнению $F(x, y) = 0$ ($x, y \in \mathbb{F}_2^m$). Будем искать уравнение кривой L в явном виде

$$y = f(x), \tag{1}$$