2. *Feistel H.* Cryptography and Computer Privacy // Scientific American. 1973. V. 228. No. 5. P. 15–23.
3. http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf — NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, revision 1.

УДК 003.26.09

СВЯЗЬ СТРУКТУРЫ МНОЖЕСТВА ОТКРЫТЫХ КЛЮЧЕЙ СО СТОЙКОСТЬЮ КРИПТОСИСТЕМЫ МАК-ЭЛИСА–СИДЕЛЬНИКОВА

И. В. Чижов

Криптосистема Мак-Элиса — одна из старейших криптосистем с открытым ключом. Она была предложена в 1978 г. Р. Дж. Мак-Элисом [1]. Эта криптосистема основывается на $\mathbb{NP}$-трудной проблеме в теории кодирования. В. М. Сидельников в работе [2] предложил использовать для построения криптосистемы Мак-Элиса коды Рида–Маллера $RM(r, m)$, однако, проведя криптоанализ, В. М. Сидельников пришёл к выводу, что на сегодняшний день такая криптосистема не обеспечивает должного уровня стойкости, и в той же работе предложил усиленную модификацию криптосистемы Мак-Элиса на основе РМ-кодов — криптосистему Мак-Элиса–Сидельникова.

Рассмотрим оригинальную криптосистему Мак-Элиса, построенную на кодах Рида–Маллера $RM(r, m)$. При этом предполагается, что выполнено неравенство $2r \leqslant m$, так как именно при таких ограничениях на m и r обеспечивается эффективность алгоритмов декодирования РМ-кода. Будем понимать под взломом как оригинальной криптосистемы Мак-Элиса, так и модифицированной (криптосистемы Мак-Элиса–Сидельникова) восстановление компонентов секретного ключа по открытому ключу. Легко видеть, что в этом случае стойкость оригинальной криптосистемы Мак-Элиса определяется сложностью задачи mcRM (см. далее). Другими словами, если злоумышленник научится эффективно решать задачу mcRM, то он тем самым сможет взломать оригинальную криптосистему Мак-Элиса, построенную на основе РМ-кодов.

Задача mcRM

Вход: матрица $G = H \cdot R \cdot \gamma$, где H — невырожденная двоичная $(k \times k)$-матрица; R — порождающая $(k \times n)$-матрица кода Рида–Маллера $RM(r, m)$; γ — перестановочная $(n \times n)$-матрица.

Найти: невырожденную матрицу H' размера $(k \times k)$ и перестановочную $(n \times n)$-матрицу γ', такие, что $H' \cdot G \cdot \gamma'$ — порождающая матрица кода Рида–Маллера $RM(r, m)$, то есть найдётся невырожденная $(k \times k)$-матрица M, что выполнено равенство $H' \cdot G \cdot \gamma' = M \cdot R$.

Введем в рассмотрение семейство mcRMi задач для $1 \leqslant i \leqslant k$.

Задача mcRMi

Вход: матрица $G = H' \cdot R' \cdot \gamma'$, где H' — невырожденная двоичная $(k-1) \times (k-1)$-матрица; R' — $((k-1) \times n)$-матрица, получающаяся из порождающей матрицы R кода Рида–Маллера $RM(r, m)$ выкидыванием строки с номером i; γ' — перестановочная $(n \times n)$-матрица.

Найти: невырожденную матрицу M' размера $(k-1)\times(k-1)$ и перестановочную $(n\times n)$-матрицу σ', такие, что $M' \cdot G \cdot \sigma'$ — порождающая матрица кода $\mathcal{R}'$, порождаемого матрицей R', то есть найдётся невырожденная $((k-1) \times (k-1))$-матрица L', что выполнено равенство $M' \cdot G \cdot \sigma' = L' \cdot R'$.

Построение этого семейства полностью продиктовано результатами работы [3], в которой получено описание ряда классов эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова.

Рассмотрим теперь задачу, связанную со стойкостью криптосистемы Мак-Элиса–Сидельникова. Однако здесь криптосистема Мак-Элиса–Сидельникова рассматривается не на всём ключевом пространстве, а только на полностью описанных в [3] классах эквивалентности.

Задача mcSRM

Вход: матрица $G = (H_1 \cdot R \| H_2 \cdot R) \cdot \Delta$, где H_1 и H_2 — невырожденные двоичные $(k \times k)$-матрицы, принадлежащие классу эквивалентности $[(H, HT^i_{\widetilde{\alpha}}, \Gamma)]$ для некоторой невырожденной $(k \times k)$-матрицы H, некоторой перестановочной $(2n \times 2n)$-матрицы Γ, некоторого числа $1 \leqslant i \leqslant k$ и некоторого вектора $\widetilde{\alpha}$; R — порождающая $(k \times n)$-матрица кода Рида–Маллера $RM(r, m)$; Δ — перестановочная $(2n \times 2n)$-матрица.

Найти: невырожденные матрицы H'_1 и H'_2 размера $(k \times k)$ и перестановочную $(2n \times 2n)$-матрицу Δ', такие, что $G \cdot \Delta' = (H'_1 R \| H'_2 R)$.

Справедливы следующие теоремы.

Теорема 1. Пусть существует набор машин Тьюринга $MTmcRMi$, каждая из которых решает соответствующую задачу mcRMi за полиномиальное время. Тогда существует машина Тьюринга $MTmcSRM$, которая решает задачу mcSRM за полиномиальное время.

Теорема 2. Пусть существует машина Тьюринга $MTmcRM$, которая решает задачу mcRM за полиномиальное время. Тогда существует семейство машин Тьюринга $MTmcRMi$, которые соответственно решают задачи mcRMi за полиномиальное время.

Теорема 3. Пусть существует машина Тьюринга $MTmcRM$, которая решает задачу mcRM за полиномиальное время. Тогда существует машина Тьюринга $MTmcSRM$, которая решает задачу mcSRM за полиномиальное время.

ЛИТЕРАТУРА

1. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol. 1978. P. 114–116.
2. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида-Маллера // Дискретная математика. 1994. № 6(2). С. 3–20.
3. *Чижов И. В.* Ключевое пространство криптосистемы Мак-Элиса-Сидельникова // Дискретная математика. 2009. № 21(3). С. 132–158.

УДК 681.3

МОДЕЛЬ СИММЕТРИЧНОГО ШИФРА НА ОСНОВЕ НЕКОММУТАТИВНОЙ АЛГЕБРЫ ПОЛИНОМОВ

И. В. Широков

Пусть $\mathbb{F}$ — некоторое поле, $f(x), g(x)$ — элементы кольца $\mathbb{F}[x]$, $(f \circ g)(x) \equiv f(g(x))$ — композиция полиномов. Кольцо $\mathbb{F}[x]$ с дополнительной операцией композиции является некоммутативной алгеброй полиномов с тремя бинарными операциями $\{+, \cdot, \circ\}$.

Решение уравнения

$$(f \circ g)(x) = r(x) \bmod h(x), \quad f, g, h, r \in \mathbb{F}[x], \tag{1}$$