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

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

где $x, y \in \mathbb{F}_2^m$; $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$. Через функцию (1) условия 1 и 2 записываются следующим образом:

1') каждая точка $(u, v) \in \mathbb{F}_2^m \times \mathbb{F}_2^m$, не лежащая на кривой L, т. е. $v \neq f(u)$, может быть представлена в виде

$$\begin{cases} u = x_1 + x_2 + x_3, \\ v = f(x_1) + f(x_2) + f(x_3), \end{cases} \tag{2}$$

где $x_1 \neq x_2 \neq x_3 \neq x_1$ и знак «+» обозначает побитовое сложение в $\mathbb{F}_2^m$;

2') для всех $x_1 \neq x_2 \neq x_3 \neq x_1$ справедливо

$$f(x_1 + x_2 + x_3) \neq f(x_1) + f(x_2) + f(x_3). \tag{3}$$

Будем считать $\mathbb{F}_2^m$ полем Галуа $\mathrm{GF}(2^m)$ и строить f в виде многочлена. Возьмём f в виде

$$y = f(x) = x^3. \tag{4}$$

Проверяя 2', найдём

$$y = f(x_1 + x_2 + x_3) = (x_1 + x_2 + x_3)^3 = (x_1^3 + x_2^3 + x_3^3) + 3(x_1 + x_2)(x_1 + x_3)(x_2 + x_3). \tag{5}$$

Следовательно, равенство в (3) равносильно равенству $(x_1 + x_2)(x_1 + x_3)(x_2 + x_3) = 0$, что в поле характеристики два равносильно тому, что или $x_1 + x_2 = 0$, или $x_1 + x_3 = 0$, или $x_2 + x_3 = 0$. Это противоречит условию различности точек $x_1 \neq x_2 \neq x_3 \neq x_1$. Итак, функция (4) удовлетворяет условию 2'.

Приступим теперь к проверке условия 1'. Используя (5) в (2), получим в поле характеристики 2

$$0 \neq w = u^3 + v = (x_1 + x_2)(x_1 + x_3)(x_2 + x_3). \tag{6}$$

Значит, условие 1' сводится к условию

1'') для любых u, v, таких, что $u^3 + v \neq 0$ и $u = x_1 + x_2 + x_3$, существуют такие (все различные) x_1, x_2 и x_3, что справедливо (6).

Выразим x_3 из (2) $x_3 = u + x_1 + x_2$, подставим его в (6) и получим

$$\begin{gathered} 0 \neq w = u^3 + v = (x_1 + x_2)(u + x_2)(u + x_1) = \\ = [(x_1 + u) + (x_2 + u)](x_1 + u)(x_2 + u) = (x + y)xy, \end{gathered} \tag{7}$$

где обозначено $x = x_1 + u$, $y = x_2 + u$.

Пусть $w \in \mathrm{GF}(2^m)$ — произвольный отличный от нуля элемент поля. Если существуют такие элементы $x, y \in \mathrm{GF}(2^m)$, что $w = xy(x + y)$, то для любых u, v, таких, что $u^3 + v = w$, имеем при $x_1 = x + u$, $x_2 = y + u$, $x_3 = x + y + u$ равенства (2) и (7). При этом из (7) при $w \neq 0$ вытекает $x_1 \neq x_2 \neq x_3 \neq x_1$, и равенство (2) справедливо ввиду

$$v = u^3 + w = (x_1 + x_2 + x_3)^3 + (x_1 + x_2)(x_1 + x_3)(x_2 + x_3) = x_1^3 + x_2^3 + x_3^3.$$

Итак, функция (4) удовлетворяет условию 1' тогда и только тогда, когда

1''') для любого ненулевого $w \in \mathrm{GF}(2^m)$ существуют элементы $x, y \in \mathrm{GF}(2^m)$, удовлетворяющие уравнению (7).

Сведём уравнение (7) к квадратному. Вводя $\sigma = \sigma_1 = x+y$ и $\sigma_2 = xy = w/\sigma$, видим, что $\xi = x$ и $\xi = y$ — корни квадратного уравнения

$$\xi^2 + \sigma\xi + \frac{w}{\sigma} = 0. \tag{8}$$

Вводя вместо ξ новую неизвестную $\eta = \dfrac{\xi}{\sigma}$, из $\xi = \sigma\eta$ получим посредством (8) квадратное для η уравнение

$$\eta^2 + \eta + \frac{w}{\sigma^3} = 0.$$

Как известно [3 – 5], необходимым и достаточным условием существования решения уравнения (8) является равенство нулю следа свободного члена, т. е.

$$\operatorname{tr}\left(\frac{w}{\sigma^3}\right) = 0.$$

Заметим, что в качестве σ мы можем, для данного w, выбирать произвольный (ненулевой) элемент поля $\mathrm{GF}(2^m)$. При этом уравнение (7) есть частный случай уравнения (6) при $x_3 = u \neq 0$, $w = v \neq 0$. Следовательно, условия 1, 1', 1", 1"' равносильны следующему условию:

3) для любого ненулевого $w \in \mathrm{GF}(2^m)$ существует такой ненулевой $\sigma \in \mathrm{GF}(2^m)$, что (абсолютный) след элемента w/σ^3 равен нулю.

Проверка этого условия произведена в зависимости от $m \bmod 4$.

Суммируя результаты, получаем итоговое

Утверждение 1. При чётном $n = 2m$, $m \geqslant 3$, кубическая парабола

$$\bar{M} = L = \{(x, y) \in \mathbb{F}_2^n : y = x^3, x, y \in \mathrm{GF}(2^m)\}$$

удовлетворяет требованиям задачи 1, 2.

Таким образом, получена явная конструкция для решения задачи при чётной размерности.

ЛИТЕРАТУРА

1. `http://nsucrypto.nsu.ru`. International Students' Olympiad in Cryptography NSUCRYPTO.
2. *Agievich S., Gorodilova A., Idrisova V., et al.* Mathematical problems of the Second International Students' Olympiad in Cryptography // Cryptologia. 2017. `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1260666`.
3. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы. М.: КомКнига, 2006.
4. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006.
5. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.