Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 514.14 DOI 10.17223/2226308X/12/1

О БЛОКИРОВКЕ ДВУМЕРНЫХ АФФИННЫХ МНОГООБРАЗИЙ

К. Л. Геут, С. С. Титов

Рассмотрена проблема блокировки семейств подмножеств и предложена конструкция расширения блокирующих множеств семейства двумерных аффинных многообразий в пространстве битовых строк при увеличении его размерности. Рассмотрены приложения этой конструкции к решению задачи «A secret sharing» олимпиады NSUCRYPTO не только для чётной, но и для нечётной размерности пространства. Приведены примеры и вычислены мощности дополнений блокирующих множеств этого семейства многообразий для высоких нечётных размерностей.

Ключевые слова: *аффинные многообразия, блокирующее множество, NSUCRYPTO.*

При построении отображений конечных полей, обладающих хорошими криптографическими свойствами, в том числе при разделении секрета, построении APN-функций и т. п., естественным образом возникает подзадача блокировки семейств подмножеств, т. е. задача построения блокирующего множества — такого, что в каждом подмножестве блокируемого семейства найдётся элемент этого множества. Эта задача аналогична классической задаче нахождения трансверсали — системы различных представителей. Так, задачу «A secret sharing» олимпиады по криптографии NSUCRYPTO-2015 [1] можно трактовать как задачу блокировки двумерных аффинных многообразий над полем GF(2). Эта задача частично решена [2, 3], а именно: предложена конструкция дополнения L блокирующего множества M для чётной размерности пространства над полем GF(2). В данной работе для полного решения задачи предлагается конструкция дополнения блокирующего множества, пригодная и для нечётных размерностей пространства, на основе построения расширения множества L при увеличении размерности на единицу.

Под задачей блокировки семейства S подмножеств T множества E понимается задача построения такого минимального по включению подмножества M, что любое подмножество T из семейства S имеет непустое пересечение с подмножеством M. Каждое такое подмножество M называется блокирующим множеством семейства S, а подмножество $L = E \setminus M$ — дополнением блокирующего множества. Так, если E — множество точек конечной плоскости, семейство S включает в себя все прямые линии T на этой плоскости, то известная задача блокировки прямых [4, 5] состоит в построении минимального нетривиального множества M точек, такого, что в каждой прямой найдётся хотя бы одна точка из M. Таким образом, блокирующее множество на плоскости — это множество точек, пересекающих множество линий. Блокирующее множество называется тривиальным, если оно содержит линию. Семейство прямых в конечной плоско-

сти естественным образом связано с $O(2)$-стойкими шифрами [6, 7], являясь при этом семейством гиперплоскостей однозначно определённого матроида, элементы которого (точки) могут быть интерпретированы как участники некоторой идеальной схемы разделения секрета [8].

В задаче «A secret sharing» E есть множество битовых строк длины n, семейство S включает в себя все двумерные аффинные многообразия над $\mathrm{GF}(2)$, т. е. такие четырёхэлементные подмножества $T = \{x_1, x_2, x_3, x_4\}$ множества E, что $x_1+x_2+x_3+x_4 = 0$, и требуется предложить конструкцию блокирующего множества M (или, что равносильно, его дополнения L). В информационной безопасности, если пользоваться метафорой семейства S множеств как семейства контролируемых пространств или возможных траекторий движения злоумышленника, то элементы блокирующего множества M представляют собой в этой метафоре [9] блок-посты или контролирующие устройства (типа датчиков движения, камер видеонаблюдения и т. п.); так что если эти семейства и множества имеют конкретную математическую (в частности, геометрическую) природу, то можно ставить соответствующие математические задачи блокировки.

Пусть $L = \bar{M}$ даёт решение задачи блокировки двумерных аффинных многообразий в $\mathbb{F}_2^n$. Можно ли включить L в множество L^+, дающее решение этой задачи в пространстве $\mathbb{F}_2^{n+1}$?

Если $L^+ = L \cup L'$, $L' \subset \mathbb{F}_2^{n+1} \setminus \mathbb{F}_2^n$, то $L' = \{f + t : t \in T\}$, где f — фиксированный элемент $f \in \mathbb{F}_2^{n+1} \setminus \mathbb{F}_2^n$, $T \subset \mathbb{F}_2^n$. Необходимым и достаточным условием того, что L^+ даёт решение, является $|L^+ \oplus L^+ \setminus \{0\}| = \mathrm{C}^2_{l^+}$ (где $l^+ = |L^+|$) при максимальном L^+ (по включению) с таким равенством.

Утверждение 1. Подмножество $L = \bar{M}$ даёт решение задачи блокировки двумерных аффинных многообразий в $\mathbb{F}_2^n$ тогда и только тогда, когда L — максимальное по включению подмножество, такое, что $|L \oplus L\setminus\{0\}| = \mathrm{C}^2_l$, где $l = |L|$.

Это свойство равносильно тому, что для любых двух различных пар $\{u, v\} \neq \{w, t\}$, $u \neq v$, $w \neq t$, $\{u, v, w, t\} \subset L$, имеем $u \oplus v \neq w \oplus t$.

Утверждение 2. Если множество $L = \bar{M}$, дающее решение задачи блокировки двумерных аффинных многообразий в $\mathbb{F}_2^n$, можно включить в множество L^+, дающее решение этой задачи в пространстве $\mathbb{F}_2^{n+1}$, то найдётся такое подмножество $T \subset \mathbb{F}_2^n$, что $(L \oplus L) \cap (T \oplus T) = \{0\}$ и $|(T \oplus T) \setminus \{0\}| = \mathrm{C}^2_{|T|}$.

При этом если T — максимальное по включению такое подмножество, то множество $L^+ = L \cup \{f \oplus t : t \in T\} = L \cup (\{f\} \oplus T)$, где f — произвольный элемент в $\mathbb{F}_2^{n+1} \setminus \mathbb{F}_2^n$, даёт решение этой задачи.

Конструкция.

Пусть $n = 2m$. Тогда $\mathbb{F}_2^n = \mathbb{F}_2^m \times \mathbb{F}_2^m$, имеется конструкция [3] множества L в виде $L = \{(x, x^3) : x \in \mathrm{GF}(2^m)\}$. Пусть L^- есть дополнение блокирующего множества в $\mathbb{F}_2^m = \mathrm{GF}(2^m)$.

Положим $T = \{(0, t) : t \in L^-\}$ для любого m, так что условие инъективности выполняется.

Проверяя условие отсутствия общих ненулевых сумм, видим, что если $(x_1, x_3) + (x_2, x_2^3) = (0, t_1) + (0, t_2)$, то $x_1 + x_2 = 0$, откуда $x_1 = x_2$, и поэтому $x_1^3 + x_2^3 = 0 = t_1 + t_2$, откуда $t_1 = t_2$. Следовательно, $(L \oplus L) \cap (T \oplus T) = \{(0, 0)\}$ и для решения задачи блокировки в $\mathbb{F}_2^{n+1}$ требуется установить только максимальность T.

Возьмём без ограничения общности $f = (0, \ldots, 0, 1) \in \mathbb{F}_2^{n+1} \setminus \mathbb{F}_2^n$, так что $L' = \{f + t : t \in L^-\}$ удовлетворяет условию инъективности. Будем представлять эле-

менты из $\mathbb{F}_2^{n+1} = \mathbb{F}_2^{2m+1}$ в виде троек (x, y, z), где $x \in \mathbb{F}_2^m = \mathrm{GF}(2^m)$, $y \in \mathbb{F}_2^m = \mathrm{GF}(2^m)$, $z \in \mathbb{F}_2$. Тогда $L = \{(x, x^3, 0) : x \in \mathrm{GF}(2^m)\}$, $L' = \{(0, t, 1) : t \in L^-\}$ и $L^+ = L \cup L'$ удовлетворяет условию инъективности.

Для проверки условия максимальности возьмём элемент $e = (a, b, c) \in \mathbb{F}_2^{n+1}$.

Если $c = 0$, то либо $e \in L$, либо e представим в виде суммы трёх различных элементов из L по построению. Если же $c = 1$, то при $a = 0$ либо $e \in L'$, либо e представим в виде суммы трёх различных элементов из L' согласно выбору L^-, поскольку $1 \oplus 1 \oplus 1 = 1$.

Пусть, наконец, $c = 1$ и $a \neq 0$. Тогда при $b = a^3$ имеем $e = (a, a^3, 0) + (0, 0, 0) + (0, 0, 1)$, где первые два слагаемых принадлежат L, а третье — L' (предполагается, без ограничения общности, что $0 \in L^-$). При $b \neq a^3$ положим $b = a^3 + d$. Здесь $a \neq 0$, $d \neq 0$, так что единственный возможный вариант представления e в виде суммы трёх элементов из L^+ — взять два слагаемых из L и одно из L'. Будем искать представление e в виде

$$e = (a, b, 1) = (x_1, x_1^3, 0) + (x_2, x_2^3, 0) + (0, t, 1). \tag{1}$$

Это даёт систему уравнений $x_1 + x_2 = a$, $x_1^3 + x_2^3 + t = b$. Обозначим $x_1 = x$, тогда $x_2 = x + a$ и последнее уравнение принимает вид $x^3 + (a + x)^3 + t = a^3 + d$. Раскрывая скобки и приводя подобные, получим $ax^2 + a^2x + t = d$. Деля на $a^3 \neq 0$, приходим к уравнению $y^2 + y = (t' + d')$ для $y = x/a$, где обозначено $t' = t/a^3$, $d' = d/a^3$. Как известно [10], решение y существует тогда и только тогда, когда (абсолютный) след правой части равен нулю, т. е. $\mathrm{Tr}(t' + d') = 0$. Итак, наличие представления (1) равносильно возможности подбора для данного d такого $t \in L^-$, что $\mathrm{Tr}(t') = \mathrm{Tr}(d')$. Поскольку областью значений функции следа является двухэлементное поле $\mathbb{F}_2 = \{0, 1\}$, для существования такого t при любом d достаточно, чтобы в L^-/a^3 имелись как элементы с нулевым, так и элементы с единичным следом. Докажем две леммы.

Лемма 1. Пусть L — дополнение блокирующего множества в $\mathbb{F}_2^k = \mathrm{GF}(2^k)$. Тогда для любого ненулевого $h \in \mathrm{GF}(2^k)$ множество $L^* = hL$ также является дополнением блокирующего множества.

Доказательство. Если $l_i^* \in L^*$ $(i = 1, \ldots, 4)$ различны и $l_1^* + l_2^* + l_3^* + l_4^* = 0$, то $l_i^* = hl_i$, $i = 1, \ldots, 4$, причём $l_1 + l_2 + l_3 + l_4 = 0$ и все l_i тоже различны, что невозможно. Если $m^* \notin L^*$, то $m^* = hm$, где $m \notin L$, так что имеется представление m в виде суммы трёх различных элементов из L, т. е. $m = l_1 + l_2 + l_3$, $l_i \in L$ $(i = 1, 2, 3)$. Однако тогда имеется и представление для m^*, так как $m^* = hl_1 + hl_2 + hl_3 = l_1^* + l_2^* + l_3^*$, где l_1^*, l_2^*, l_3^* — три различных элемента из L^*. ■

Лемма 2. Пусть L — дополнение блокирующего множества в $\mathbb{F}_2^k = \mathrm{GF}(2^k)$. Тогда в L есть элемент с нулевым следом и есть элемент с единичным следом.

Доказательство. Пусть, от противного, в L нет ни одного элемента с нулевым следом. Значит, все элементы в L имеют след равный единице. Следовательно, все суммы троек элементов из L имеют след, тоже равный единице, так как $1 \oplus 1 \oplus 1 = 1$, что противоречит представимости элементов дополнения L, содержащего элементы и с нулевым следом, в виде сумм троек элементов из L. Аналогично — для L без элементов с единичным следом. ■

Применяя эти леммы, получаем при $k = m$ и $h = 1/a^3$

Утверждение 3. Для произвольного L^-, являющегося дополнением блокирующего множества в $\mathbb{F}_2^m$ (без ограничения общности содержащего нуль), предложенная

конструкция даёт множество L^+, являющееся дополнением блокирующего множества в $\mathbb{F}_2^{2m+1}$.

Таким образом, для решения задачи «A secret sharing» предложена конструкция множества, блокирующего двумерные многообразия, не только для чётной, но и для нечётной размерности. Необходимо применить описанную процедуру расширения конечное число раз в зависимости от числа n — размерности пространства. Если n чётно, то имеем конструкцию работы [3]. Если $n = 2k + 1$ и множество L_k известно (например, если k чётно), то применяем процедуру расширения, получив $|L_n| = 2^k + |L_k|$. Если $n = 4k - 1$, то, в случае необходимости, можно применить процедуру ещё один раз, при этом мощность дополнения L_n блокирующего множества равна $|L_n| = 2^{2k} + 2^k$. Так, из того, что $|L_5| = 7$, находим $|L_{11}| = 2^5 + 7 = 39$, а из $|L_3| = 4$ находим $|L_7| = 2^3 + 4 = 12$. Поэтому множества L_{23} и L_{15} находятся «в два действия», т. е. повторным применением описанной процедуры, при этом получается $|L_{23}| = 2^{11} + 2^5 + 7 = 2087$, $|L_{15}| = 2^7 + 2^3 + 4 = 2^7 + 12 = 140$. В три действия находим, например, $|L_{47}| = 2^{23} + |L_{23}| = 8390695$. Очевидно, что для любого n число процедур расширения не превосходит $\log_2 n$, оно достигает максимума s для $n = 2^s - 1$. Например, при $s = 5$ имеем, применяя процедуру четыре раза, $|L_{31}| = 2^{15} + |L_{15}| = 32908$, а при $s = 8$ имеем, применяя процедуру семь раз, $|L_{255}| = 2^{127} + 2^{63} + 2^{31} + 2^{15} + 2^7 + 2^3 + 4$. Этот метод может быть применён и к другим криптографическим задачам [11].

ЛИТЕРАТУРА

1. Сайт олимпиады NSUCRYPTO. `http://nsucrypto.nsu.ru/`
2. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems from the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58.
3. *Геут К. Л., Кириенко К. А., Садков П. О. и др.* О явных конструкциях для решения задачи "A secret sharing" // Прикладная дискретная математика. Приложение. 2017. № 10. С. 68–70.
4. *Szonyi T.* Blocking sets in desarguesian affine and projective planes // Finite Fields and their Appl. 1997. V. 3. Iss. 3. P. 187–202.
5. *Polverino O.* Linear sets in finite projective spaces // Discrete Mathematics. 2010. V. 310. Iss. 22. P. 3096–3107.
6. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
7. *Болотова Е. А., Коновалова С. С., Титов С. С.* Свойства решёток разграничения доступа, совершенные шифры и схемы разделения секрета // Проблемы безопасности и противодействия терроризму. Материалы IV Междунар. науч. конф. М.: МЦНМО, 2009. Т. 2. С. 71–86.
8. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2(2). С. 50–57.
9. *Башуров В. В., Филимоненкова Т. И.* Математические модели безопасности. Новосибирск: Наука, 2009. 87 с.
10. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Книга по Требованию, 2013. Т. 1–2. 812 с.
11. *Городилова А. А.* От криптоанализа щифра к криптографическому свойству булевой функции // Прикладная дискретная математика. 2016. № 3(33). С. 16–44.