ЛИТЕРАТУРА

1. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.

УДК 519.151, 519.725, 519.165 DOI 10.17223/2226308X/12/29

БЛОКИРОВКА ЛИНЕЙНЫХ МНОГООБРАЗИЙ И ТРОЙКИ ШТЕЙНЕРА

М. В. Ведунова, А. О. Игнатова, К. Л. Геут

Рассматриваются задачи блокировки троек Штейнера, применимые в схемах разделения секрета. Описан метод построения блокирующего множества минимальной и максимальной мощности. Для дополнительного множества найден метод оценки минимальной мощности дополнения как в линейных, так и в нелинейных системах троек Штейнера. Для соответствующих матроидов реализованы идеальные схемы разделения секрета на основе интерполяционных многочленов с нулевым следом. В нелинейной системе троек Штейнера с 13 элементами найдены максимальные и минимальные мощности дополнения блокирующего множества.

Ключевые слова: *системы троек Штейнера, схемы разделения секрета, блокирующие множества.*

Во втором раунде международной интернет-олимпиады по криптографии NSUCRYPTO-2015 [1] была предложена задача на специальный приз программного комитета «A secret sharing», в 2016 и 2017 гг. отмеченная как всё ещё не решённая [2, 3]. Решение этой задачи рассматривается с точки зрения блокировки двумерных аффинных многообразий над полем GF(2). Здесь 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 M. Каждое такое подмножество M называется блокирующим множеством семейства S, а подмножество $L = E \setminus M$ — дополнением блокирующего множества. Задача блокировки троек Штейнера может трактоваться как вспомогательная при решении исходной задачи NSUCRYPTO, поскольку каждое такое многообразие является сдвигом однозначно определённого двумерного линейного многообразия, соответствующего линейной тройке Штейнера [4]. Проблеме вложимости произвольной системы троек Штейнера в совершенный двоичный код посвящена работа [5]. Проблеме реализации связи блок-схем с семейством троек Штейнера, где однородный матроид, когиперплоскости которого — это тройки Штейнера, соответствует идеальной схеме разделения секрета, посвящена работа [6]. Линейные системы троек Штейнера S_n — системы с $v = 2^n - 1$ элементами — ненулевыми битовыми строками длины n, $n \geqslant 3$, в которых бинарная операция квазигруппы Штейнера есть побитовое сложение по модулю два. Для матроидов линейных троек Штейнера ниже построены соответствующие им схемы разделения секрета [7, 8], а также рассмотрены методы построения блокирующих множеств минимальной и максимальной мощности.

Утверждение 1. Мощность l дополнения L блокирующего множества удовлетворяет неравенству $l(l+1)/2 \geqslant v$.

Используя данное неравенство, получим, что для нелинейной тройки Штейнера при $v = 13$ минимальная мощность дополнения $l = 5$, а для $v = 31$ не может быть меньше восьми.

Линейные системы троек Штейнера можно трактовать как систему предписанных соотношений в конечных бинарных полях. В зависимости от их интерпретации задачу блокировки можно рассматривать в связи с реализацией схем разделения секрета (СРС) в конечных полях. Так, проблема «A secret sharing» как проблема блокировки аффинных многообразий приводит к задаче реализации СРС, сохраняющих предписанные соотношения в виде семейства H_4 четвёрок в $\mathrm{GF}(2^n)$, таких, что $X_1+X_2+X_3+X_4=0$, а проблема блокировки линейных троек Штейнера приводит к задаче реализации СРС, сохраняющих предписанные соотношения в виде семейства H_3 троек в $\mathrm{GF}(2^n)$, таких, что $X_1+X_2+X_3=0$. Эти зависимости можно трактовать как циклы [9] в некоторых матроидах.

Утверждение 2. Семейство H_4 с добавлением пятиэлементных подмножеств, никакие четыре элемента которых не дают в сумме нуль, удовлетворяет аксиомам циклов матроида.

Утверждение 3. Семейство H_3 с добавлением четырёхэлементных подмножеств, никакие три элемента которых не дают в сумме нуль, удовлетворяет аксиомам циклов матроида.

Оказывается, эти матроиды являются матроидами идеальных СРС, реализация которых аналогична реализации схемы Шамира и основывается на интерполяционных многочленах с нулевым следом.

Утверждение 4. Классом многочленов, разделяющих секрет посредством циклов семейства H_4 построенного матроида, является класс многочленов вида $f(x)=ax^4+bx^2+cx+d$, где a, b, c, d — произвольные элементы поля $\mathrm{GF}(2^n)$.

Утверждение 5. Классом многочленов, разделяющих секрет посредством циклов семейства H_3 построенного матроида, является класс многочленов вида $f(x)=ax^3+bx+c$, где a, b, c — произвольные элементы поля $\mathrm{GF}(2^n)$.

Для нелинейных троек Штейнера мощность блокирующего множества может быть получена только полным перебором, например:

Утверждение 6. Для $v=13$ максимальные и минимальные мощности дополнительного множества равны $|L|_{\min}=5$, $|L|_{\max}=6$.

Система троек, построенная на тринадцати элементах, не относится к линейным. Рекуррентная конструкция блокирующего множества M и его дополнения L такова:

Утверждение 7. Для любого дополнительного множества L существует L_k в S_k (при $k>n$, k — мощность множества битовых строк, в которых первые n битов равны нулю), имеющее мощность $|L_k|=|L|\cdot 2^{k-n}$.

Максимальность такого L вытекает из условия, что для любого элемента из тройки $u\in M$ существуют $x_1,x_2\in L$, что $u=x_1\oplus x_2$ и L не включает в себя ни одной тройки с нулевой суммой.

Конструкция минимального блокирующего множества M и его дополнения L такова: $G=M\cup\{0\}$ есть подгруппа группы $(\mathbb{F}_2^n;\oplus)$ индекса два (линейное пространство), а $L=G\oplus h$ $(h\notin G)$ — её смежный класс (аффинное пространство). Эта конструкция, очевидно, даёт решение задачи блокировки в общем случае линейной тройки Штейнера при $n\geqslant 3$, при этом $|L|=2^{n-1}$, $|M|=2^{n-1}-1$.

Итак, предложены конструкции блокирующих множеств троек Штейнера и оценки возможных значений их мощности.

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. *Холл М.* Комбинаторика: пер. с англ. М.: Мир, 1970. 424 с.
5. *Ковалевская Д. И., Соловьева Ф. И., Филимонова Е. С.* О системах троек Штейнера малого ранга, вложимых в совершенные двоичные коды // Дискретный анализ и исследование операций. 2013. Т. 20. № 3(111). С. 3–25.
6. *Медведев Н. В., Титов С. С.* Об однородных матроидах и блок-схемах // Прикладная дискретная математика. Приложение. 2017. № 10. С. 21–23.
7. *Shamir A.* How to share a secret // Commun. ACM. 1979. No. 22. P. 612–613.
8. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2(2). С. 50–57.
9. *Асанов М. О., Баранский В. А., Расин В. В.* Дискретная математика: графы, матроиды, алгоритмы. Ижевск: НИЦ Регулярная и хаотическая динамика, 2001. 288 с.

УДК 519.7 DOI 10.17223/2226308X/12/30

ОБ АРГУМЕНТАЦИИ ОТСУТСТВИЯ СВОЙСТВ СЛУЧАЙНОГО ОРАКУЛА У НЕКОТОРЫХ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ[1]

И. А. Грибанова, А. А. Семёнов

Представлены новые алгебраические атаки на хеш-функции вида MD4-k, где k — число шагов базового алгоритма MD4, $39 \leqslant k \leqslant 48$. Для решения алгебраических уравнений используются SAT-решатели. Представленные атаки демонстрируют отсутствие свойств случайного оракула у рассматриваемых хеш-функций. Более точно, мы строим оценки доли легко обратимых выходов этих функций и показываем, что даже для полнораундовой функции MD4 эта доля весьма высока. Для построения оценок с каждой функцией вида MD4-k связывается специальная функция, длина входа которой существенно меньше 512. Показано, что любое значение такой функции является значением MD4-k. Задача обращения специальной функции, как правило, существенно проще, чем задача обращения MD4-k. Оценка доли векторов в $\{0,1\}^{128}$, являющихся значениями специальной функции, даёт оценку доли легко обратимых значений исходной функции MD4-k.

Ключевые слова: *криптографические хеш-функции, поиск прообразов хеш-функций, MD4, MD4-39, SAT.*

Случайный оракул — это гипотетический объект, обладающий рядом привлекательных с точки зрения криптографии свойств. Строго (см., например, [1]) случайный оракул определяется как отображение вида $O : \{0,1\}^* \to \{0,1\}^\infty$, которое произвольному конечному двоичному слову сопоставляет слово, являющееся бесконечной

[1]Работа выполнена при финансовой поддержке Российского научного фонда, проект № 16-11-10046. Грибанова И. А. поддержана стипендией Президента РФ СП-3545.2019.5.