УДК 519.151, 519.725, 519.165 DOI 10.17223/2226308X/12/34

ОДНОРОДНЫЕ МАТРОИДЫ И БЛОК-СХЕМЫ

Н. В. Медведев, С. С. Титов

Работа посвящена исследованию однородных матроидов, т. е. таких, все циклы которых имеют одинаковую мощность. Эта задача связана с задачей описания идеальных однородных схем разделения секрета, т. е. таких схем, в которых все разрешённые коалиции имеют одинаковую мощность, а также с задачей описания матроидов, соответствующих идеальным совершенным схемам разделения секрета. Изучается возможность представления семейства когиперплоскостей однородного матроида как блоков блок-схемы $D(v, b, r, k, \lambda)$ с некоторым набором параметров, в том числе соответствующих системе троек Штейнера. Установлена взаимосвязь однородных матроидов с системой троек Штейнера. Доказано, что разделяющий матроид является однородным матроидом с трёхэлементными когиперплоскостями тогда и только тогда, когда его когиперплоскости образуют систему троек Штейнера, т. е. $k = 3$ и $\lambda = 1$.

Ключевые слова: *схемы разделения секрета, однородные матроиды, блок-схемы, циклы, системы троек Штейнера.*

Схема разделения секрета (СРС) — это система разраничения доступа, при которой участникам раздаются доли секрета таким образом, чтобы заранее заданные коалиции участников (разрешённые коалиции) могли однозначно восстановить секрет (совокупность этих множеств называется структурой доступа), а неразрешённые не получали никакой дополнительной информации, к имеющейся априорной, о возможном значении секрета. Такие СРС называются совершенными. Особый интерес вызывают идеальные СРС, т. е. такие, где размер доли секрета, предоставляемой участнику, не больше размера секрета. При этом разрешённые коалиции идеальной совершенной схемы разделения секрета определяются циклами некоторого связного матроида, изучение которого и даёт структуру доступа [1 – 4].

Актуальной задачей является описание однородных СРС [5 – 7], т. е. таких, где мощность всех разрешённых коалиций равна k, но, возможно, не все k-элементные множества входят в структуру доступа СРС. Под однородностью матроида понимается одинаковость мощностей его циклов, равная n, где, возможно, не все n-элементные множества — циклы; таким образом, для матроида однородной СРС справедливо равенство $n = k + 1$. При этом если все его n-элементные подмножества — циклы, то такой матроид называется пороговым (равномерным). Матроид называется связным, если для любых двух его элементов существует содержащий их цикл. Для исключения незаменимых участников идеальной СРС имеет смысл рассматривать только разделяющие матроиды. Матроид разделяющий тогда и только тогда, когда для любых $x \neq y$ существует разделяющий их цикл C, т. е. $x \notin C$, $y \in C$.

Будем понимать под блок-схемой $D(v, b, r, k, \lambda)$, согласно [8], такое размещение v различных элементов по b блокам, что каждый блок содержит точно k различных элементов, каждый элемент появляется точно в r различных блоках и каждая пара различных элементов появляется в λ блоках.

Согласно [8], блок-схема с $k = 3$ вполне естественно называется системой троек. При этом параметры должны удовлетворять аксиомам $3b = rv$, $2r = \lambda(v - 1)$. Система троек с $\lambda = 1$ называется системой троек Штейнера. Условие $v \equiv 1, 3 \pmod 6$ необходимо и достаточно для существования штейнеровской системы троек.

В [9] выдвинута гипотеза о том, что однородный матроид определяется некоторой блок-схемой. В данной работе рассматривается связь однородных матроидов с частным случаем блок-схем — системами троек Штейнера.

Пусть все когиперплоскости (дополнения циклов) однородного матроида $M = (E, \mathcal{C})$, где E — носитель, а $\mathcal{C}$ — семейство циклов с мощностью n, трехэлементны, т. е. $|E| = n + 3 = n + k$. Пусть F — максимальное по включению подмножество носителя E этого матроида, такое, что каждое его n-элементное подмножество является циклом. Поскольку, очевидно, F является плоскостью матроида M, имеем $n \leqslant |F| \leqslant |E| - 2 = n + 1$, если M не является равномерным, и при $|F| = n + 1$ имеем $|E \setminus F| = 2$, так что множество $E \setminus F = \{a, b\}$ двухэлементно, а любой цикл, не содержащийся в F, содержит $\{a, b\}$ (иначе F было бы незамкнутым). Это противоречит тому, что M — разделяющий. Следовательно, $|F| = n$ и F есть цикл.

Пусть $G^* = \{a, b, c\}$ и $H^* = \{a, b, d\}$ — две когиперплоскости, пересекающиеся по двухэлементному подмножеству $\{a, b\}$. Тогда симметрическая разность дополнений G^* и H^* равна $\{c, d\}$, т. е. двухэлементна, и поэтому в объединении дополнений G^* и H^*, мощность которого равна $(n + 1)$, каждое его n-элементное подмножество является циклом, что противоречит доказанному выше. Следовательно, любые две когиперплоскости матроида M пересекаются не более чем по одноэлементному множеству.

Из свойства матроида быть разделяющим в терминах когиперплоскостей следует, что каждый элемент лежит хотя бы в одной когиперплоскости. Связность равносильна тому, что любая пара элементов лежит вне некоторой когиперплоскости. Из доказанного выше вытекает, что любая пара элементов лежит не более чем в одной когиперплоскости.

Докажем, что любая пара $\{a, b\}$ элементов, $a \neq b$, лежит в единственно определённой когиперплоскости. Поскольку матроид M является разделяющим, существуют когиперплоскости H_a и H_b, такие, что a принадлежит H_a, но не принадлежит H_b, и b принадлежит H_b, но не принадлежит H_a. Пусть элемент c принадлежит H_a, но $a \neq c$. Тогда из того, что матроид M является разделяющим, вытекает, что существуют когиперплоскости H_c и H, такие, что c принадлежит H_c, но не принадлежит H, и a принадлежит H, но не принадлежит H_c. Отсюда $H \neq H_a$, так что элемент a принадлежит не менее чем двум различным когиперплоскостям. Если и b принадлежит H, то всё доказано. Если же нет, то, поскольку b не принадлежит ни когиперплоскости H, ни когиперплоскости H_a, причём $H \neq H_a$, по второй аксиоме гиперплоскостей должна существовать когиперплоскость, содержащая b и пересечение $H \cap H_a = \{a\}$, что и требовалось доказать.

Покажем, что семейство когиперплоскостей рассматриваемого матроида есть блок-схема $D(v, b, r, k, \lambda)$ с набором параметров, соответствующих системе троек Штейнера.

Из трёхэлементности когиперплоскостей следует, что $k = 3$. Из того, что каждая пара элементов лежит в единственной когиперплоскости, следует, что $\lambda = 1$. Из предположения однородности матроида следует, что $v = |E| = n + 3$, и так как каждая пара определяет единственным образом тройку, а в тройке таких пар три, получаем $b = (v(v - 1)/2)/3 = v(v - 1)/6$. Поскольку пересекающиеся когиперплоскости имеют одноэлементное пересечение, для каждого элемента e множество $E \setminus \{e\}$ разбивается на двухэлементные подмножества когиперплоскостями, проходящими через e, поэтому $r = (v - 1)/2$.

Таким образом, доказано

Утверждение 1. Разделяющий матроид является однородным матроидом с трёхэлементными когиперплоскостями тогда и только тогда, когда его когиперплоскости образуют систему троек Штейнера, т. е. $k = 3$ и $\lambda = 1$.

Итак, в работе показана связь однородных матроидов с тройками Штейнера. Описанный метод может быть применён к решению более сложных задач обобщения связи матроидов с блок-схемами с $\lambda = 1$, согласно выдвинутой ранее гипотезе.

ЛИТЕРАТУРА

1. Введение в криптографию / под общ. ред. В. В. Ященко. СПб.: Питер, 2001.
2. *Блейкли Г. Р., Кабатянский Г. А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. 1997. Т. 33. № 3. С. 102–110.
3. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. №2 (2). С. 50–57.
4. *Welsh D. J. A.* Matroid Theory. Academic Press, 1976.
5. *Marti-Farre J. and Padro C.* Secret sharing schemes on sparse homogeneous access structures with rank three // Electronic J. Combinatorics. 2004. No. 1 (1). Research Paper 72. 16 p.
6. *Алексейчук А. Н.* Совершенные схемы разделения секрета и конечные универсальные алгебры // Реєстрація, зберігання і оброб. даних. 2005. Т. 7. № 2. С. 55–65.
7. *Alekseychuk A. N.* Lattice-Theoretic Characterization of Secret Sharing Representable Connected Matroids. Cryptology ePrint Archive: Report 2010/348.
8. *Холл М.* Комбинаторика. М.: Мир, 1970.
9. *Медведев Н. В., Титов С. С.* Об однородных матроидах и блок-схемах // Прикладная дискретная математика. Приложение. 2017. № 10. С. 21–23.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/12/35

ГЕОМЕТРИЧЕСКАЯ МОДЕЛЬ СОВЕРШЕННЫХ ШИФРОВ С ТРЕМЯ ШИФРВЕЛИЧИНАМИ

Н. В. Медведева, С. С. Титов

Рассматривается проблема описания совершенных по Шеннону (абсолютно стойких к атаке по шифртексту) шифров с мощностью шифрвеличин равной трём. Показано, что не существует минимальных по включению совершенных шифров с четырьмя шифробозначениями и пятью или шестью ключами зашифрования. Определено количество минимальных по включению совершенных шифров, содержащих семь ключей зашифрования, а также количество совершенных шифров с числом ключей равным восьми. Построены примеры минимальных по включению совершенных шифров.

Ключевые слова: *совершенные шифры, эндоморфные шифры, неэндоморфные шифры.*

Рассмотрим вероятностную модель Σ_B шифра [1 – 3]. Пусть X, Y — конечные множества соответственно шифрвеличин и шифробозначений, с которыми оперирует некоторый шифр замены; K — множество ключей, причём $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\lambda > 1$, $\mu \geqslant \lambda$. Это означает, что открытые и шифрованные тексты представляются словами (ℓ-граммами, $\ell \geqslant 1$) в алфавитах X и Y соответственно. Согласно [2, 3], под *шифром* Σ_B будем понимать совокупность множеств правил зашифрования и правил