УДК 519.151 + 519.725 Вестник УрФО № 4(18) / 2015, стр. 21–26

Медведев Н. В., Титов С. С.

ОБ ОДНОРОДНЫХ ИДЕАЛЬНЫХ СХЕМАХ РАЗДЕЛЕНИЯ СЕКРЕТА И МАТРОИДАХ КОРАНГА ТРИ

Работа посвящена вопросам, связанным с разграничением доступа посредством идеальных совершенных схем разделения секрета и матроидов. Рассматривается задача описания однородных схем разделения секрета, т. е. таких схем, в которых все разрешенные коалиции имеют одинаковую мощность. В соответствии с этим для матроидов, соответствующих идеальным схемам, предложен термин «однородный матроид», если все его циклы имеют одинаковую мощность. Решается задача описания однородных матроидов коранга три как частный случай таких схем разделения секрета. Доказано, что однородный разделяющий матроид с мощностью антициклов $m \geq 3$ является либо аффинной плоскостью порядка m, либо проективной плоскостью порядка $(m – 1)$ с прямыми линиями в качестве антициклов.

Ключевые слова: *однородные структуры доступа, схемы разделения секрета, матроиды, циклы.*

Medvedev N. V., Titov S. S.

ON HOMOGENEOUS IDEAL SECRET SHARING SCHEMES AND MATROIDS CORANK THREE

The work is dedicated to questions relating to the delimitation of access by the ideal perfect secret sharing schemes and matroids. The problem of describing homogeneous secret sharing schemes, with qualified coalition of the same capacity. Accordingly, for the matroid corresponding to the ideal scheme, proposed the term homogeneous matroid if all its circuits have the same capacity. It is proved that homogeneous separating matroid with capacity of co-hyperplanes $m \geq 3$ is either an affine plane of order m, or a projective plane of order $(m – 1)$ with straight lines as co-hyperplanes.

Keywords: *homogeneous access structure, secret sharing schemes, matroids, cycles.*

Введение

Основная идея разграничения доступа на основе схем разделения секрета (СРС) [1] состоит в раздаче долей секрета участникам таким образом, чтобы заранее заданные коалиции участников (разрешенные коалиции) могли однозначно восстановить секрет (совокупность этих множеств называется структурой доступа), а неразрешенные – 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, предоставляемый участнику, не больше размера секрета. При этом в качестве дилера (хранителя секрета) может выступать любой участник такой СРС. Если разрешенными коалициями являются любые множества из n или более элементов, то такие СРС называются пороговыми «n из N» СРС, где N – количество всех участников [2, 3, 4, 5].

Общая проблема описания матроидов, соответствующих СРС, пока не решена [2]. Поскольку эти проблемы признаны сложными, представляется естественным решать частные задачи, ведущие к решению общих проблем. Актуальной, сложной и до конца не решенной задачей является реализация сложных структур доступа в идеальных схемах. Ито М., Саито А., Нишизеки Т. доказали [6], что существуют схемы, реализующие произвольную структуру доступа, но они могут не быть идеальными. В связи с этим особый интерес вызывают однородные структуры доступа, т. е. такие, где мощность всех разрешенных коалиций n, но, возможно, не все n-элементные множества входят в структуру доступа СРС. При этом такие структуры доступа допускают идеальную реализацию [7]. Это направление исследований связано с известной гипотезой Г. А. Кабатянского о том, что степень неидеальности может расти экспоненциально [2, 3], как при неэффективной реализации пороговой СРС. Как известно [2, 8], разрешенные коалиции идеальной совершенной схемы разделения секрета определяются циклами некоторого связного матроида, изучение которого и дает структуру доступа.

Основные понятия и термины

Напомним [9], что на множестве M определен матроид, если некоторые его подмножества названы независимыми (остальные – зависимыми), причём удовлетворяются аксиомы матроида; так, в терминах циклов – минимальных (по включению) зависимых подмножеств из M – аксиом всего две: 1) нет цикла в цикле, т. е. если C, D – циклы, и $C \subset D$, то $C = D$; 2) если $C_1 \neq C_2$ – циклы, и $x \in C_1 \bigcap C_2$, то $C_1 \bigcup C_2 \setminus \{x\}$ содержит цикл. Под N будем понимать мощность матроида M, т. е. $N=|M|$. Любое максимальное независимое подмножество B, содержащееся в M, называется базой матроида M. Дополнение базы матроида будем называть кобазой $\overline{B} = M \setminus \{B\}$ и, аналогично, дополнение цикла матроида – антицикл (когиперплоскость) $\overline{C} = M \setminus C$. Из [10] известно, что аффинные и проективные пространства являются матроидами над $GF(q)$ с гиперпространствами в качестве антициклов. Рангом матроида M называется общая мощность всех баз. Ранговая функция двойственного матроида M^* называется коранговой функцией (корангом) матроида M [9]. Матроид называется связным, если для любых двух его элементов существует содержащий их цикл. Простым или комбинаторной геометрией называется матроид, в котором нет одноэлементных и двухэлементных циклов [9]. Под однородностью матроида понимается одинаковая мощность его циклов n, где, возможно, не все n-элементные множества – циклы. Ранее в [11] матроиды были названы почти пороговыми с близкой мощностью циклов, т. е. n или $n + 1$. Матроид, соответствующий СРС, является разделяющим тогда и только тогда, когда для любых $x \neq y$ существует разделяющий их цикл C, т. е. $x \notin C$, $y \in C$.

В структуре доступа СРС можно выделить три группы участников, а именно: незаменимые, неиспользуемые и эквивалентные.

Незаменимые участники входят в любую коалицию $A \in \Gamma$. Для идеальных СРС незаменимый участник p входит во все циклы, содержащие d (дилера). Отсюда следует, что матроид является разделяющим тогда и только тогда, когда нет незаменимых участников при любом выборе дилера.

Неиспользуемые участники не входят ни в одну коалицию из Γ_{min}; они исключаются из структуры доступа СРС, т. к. такие участники не входят ни в один цикл матроида (кроме одноэлементного себя). Остальные – существенные участники, т. е. если $d = x, y$ – существенный, то $\exists C : x \in C$ и $y \in C$. Отсутствие неиспользуемых участников при любом дилере равносильно тому, что матроид связан и нет одноэлементных циклов.

Для идеальных СРС эквивалентность участников (по [7]) $p, q \in P$ означает для матроида M, что: 1) не существует цикла, содержащего подмножества $\{d, p, q\}$, где $d = p_0$ – дилер; 2) Если $A \subset P \setminus \{p, q\}$, то $C = A \bigcup \{d, p\}$ есть цикл тогда и только тогда, когда $D = A \bigcup \{d, q\}$ является циклом. Отсутствие двухэлементных циклов в матроиде ведет к отсутствию эквивалентных участников в СРС. Следует отметить, что в рассматриваемых в работе СРС таких трех групп участников нет.

Утверждение 1. Любой элемент разделяющего (неодноэлементного) матроида принадлежит не менее чем двум разным антициклам, если антициклы неодноэлементны.

Доказательство. Пусть $a \in M$. Если a не принадлежит ни одному антициклу, то для любого цикла C элемент a ему принадлежит, и поэтому если M неодноэлементен, то для любого другого элемента $b \neq a$ не существует цикла B такого, что $b \in B$ и $a \notin B$. Если же а принадлежит только одному антициклу $U = C$, то при $U \geq 2$ для любого другого элемента $b \in U$, $b \neq a$, не существует цикла B такого, что $b \in B$ и $a \notin B$, т. к. антициклы C и B не существуют, что и требовалось доказать.

Утверждение 2. Любая пара элементов разделяющего неодноэлементного с неодноэлементными антициклами матроида лежит в некотором антицикле.

Доказательство. Пусть $a, b \in M$, $a \neq b$. По утверждению 1 существуют такие два разных антицикла $U \neq V$, что $a \in U$ и $a \in V$. Если $a \in V$ или $b \in V$, то нужный антицикл найден. Если же нет, то по второй аксиоме, т. к. $b \notin U \bigcup V$, существует такой антицикл W, что $\{b\} \bigcup (U \bigcap V) \subset W$, а поскольку $a \in U \bigcap V$, имеем $a \in W$, $b \in W$, что и требовалось доказать.

Примеры однородных матроидов

В работах [10, 11, 12] предложены серии однородных матроидов как проективных или аффинных пространств с гиперпространствами в качестве антициклов. Задача классификации таких матроидов предполагает их описание в терминах корангов. Ниже в данной работе рассмотрены значения корангов, равные один, два и три.

Так, циклы матроида ранга один двухэлементны, т. е. матроид является не простым и каждое двухэлементное множество является циклом.

Рассмотрим случай коранга два. Пусть $\{a,b\}$ кобаза и $M \setminus \{a,b\}$ база, тогда $\forall c \in M \setminus \{a,b\}$ существует единственный коцикл K такой, что $c \in K$, $(K \setminus \{c\}) \subset \{a,b\}$. Если $K = 2$, то СРС содержит незаменимых участников. Значит, $K = \{a,b,c\}$. Следовательно, любой коцикл трехэлементен, и поэтому любой цикл содержит $N - 1$ элементов, т. е. и в этом тривиальном случае матроид оказывается равномерным (пороговым).

Однородные матроиды коранга три

Следующий случай, когда коранг матроида равен трем, чему и посвящено основное содержание данной статьи. Рассмотрим матроид, в котором любой цикл содержит элементы либо a, либо b, либо c, либо пару их, либо все три. (Значит, $\{a,b,c\}$ – кобаза.) Из непороговости вытекает, что мощность m антициклов ≥ 3.

Пусть A_1, A_2 – циклы, такие, что $a \in A_1$, $a \in A_2$ ($b \notin A_1$, $c \notin A_1$). Тогда если $A_1 \neq A_2$, то в $(A_1 \bigcup A_2) \setminus \{a\}$ есть цикл A, причем $a \notin A$, $b \notin A$, $c \notin A$ (противоречие с вышеописанным предположением). Следовательно, существует единственный цикл A, такой что $a \in A$, $a \in A$, $c \notin C$. Аналогично – для элементов b, с матроида M и циклов B, C. Если a_1, a_2 таковы, что не существуют циклов, не содержащих $\{a_1,b,c\}$ или $\{a_2,b,c\}$, то A_i $(i = 1,2)$ – единственный цикл, такой, что $a_i \in A_i$, $b \notin A_i$, $c \notin A_i$ $(i = 1,2)$. Если $A_1 \bigcap A_2 \neq \varnothing$, то при $A_1 \neq A_2$ эта единственность нарушается для любого $a \in A_1 \bigcap A_2$ по второй аксиоме циклов. Если же $A_1 \bigcap A_2 = \varnothing$, то цикл A_1 не содержит $\{a_2,b,c\}$, и A_2 не содержит $\{a_1,b,c\}$ вопреки предположению. Итак, существует единственный цикл A, не содержащий ни b, ни c, и поэтому $bc = A$.

Определение линии bc: $x \in bc$ тогда и только тогда, когда во всех циклах, не содержащих ни b, ни c, нет и x. Поэтому $bc = A$, т. е. для каждой линии (вне которой есть хотя бы одна точка) существует единственный цикл, дополнением которой он является.

Утверждение 3. Вне каждой линии есть точка.

Доказательство. В противном случае не существовали бы три точки a, b, c.

Следствие 1. $N = |M| = n + |bc|$ для любых точек $b \neq c$ и определяемой ими линии bc.

Следствие 2. Если $w \in uv$, $u \neq v \neq w \neq u$, то $u \in vw$, $v \in uw$, как дополнение единственного цикла.

Итак, циклов (и антициклов) всего

$$\frac{\binom{N}{2}}{\binom{N-n}{2}} = \frac{C_N^2}{C_{N-n}^2} = \frac{N(N-1)}{(N-n)(N-n-1)}$$

Пусть $m = N - n$ есть мощность антициклов, т. е. количество точек на каждой линии. Тогда пары точек $u \neq v$ и $a \neq b$ определяют одну и ту же линию, когда они обе ей принадлежат, и таких пар на линии всего C_m^2. А всего пар различных элементов матроида – C_m^2. Поэтому количество всех линий как антициклов равно

$$\frac{\binom{N}{2}}{\binom{m}{2}} = \frac{C_N^2}{C_m^2} = \frac{N(N-1)}{m(m-1)} = \frac{N(N-1)}{(N-n)(N-n-1)}$$

Зафиксируем точку b и линию ac, $b \notin ac$. Тогда, поскольку для каждой точки x на линии ac получаем $(m-1)$ точку на линии ax (кроме b), итого получаем (поскольку все эти линии разные для разных x, т. к. иначе было бы $b \in ac = x_1x_2$) всего $m(m-1)+1$ точек. Если этими точками исчерпываются все элементы матроида, то $N = m^2 - m + 1$, и линий всего

$$\frac{(m^2 - m + 1)(m^2 - m)}{m(m-1)} = m^2 - m + 1$$

(«проективный случай» – проективная плоскость порядка ($m-1$)).

Если же есть точка y, отличная от уже таким образом построенных, то линия by не имеет общих точек с линией ac и, значит, для такого y имеется единственный цикл Y, такой, что $a \in Y$, $c \in Y$, $b \notin Y$, $y \notin Y$. Из единственности такого цикла Y вытекает, что любая другая линия by_1, не пересекающая ac, совпадает с линией by, т. е. $y_1 \in by$.

Допустим, есть две такие линии: by_1 и by_2. Из того, что $by_1 \neq by_2$, вытекает, что $by_1 = Y_1 \neq Y_2 = by_2$, $a \in Y_1$, $a \in Y_2$, $c \in Y_1$, $c \in Y_2$, $b \notin Y_i$, $y_1 \notin Y_i$, $y_2 \notin Y_i$ $(i = 1,2)$, $\{a,c\} \subset Y_1 \cap Y_2$.

По второй аксиоме циклов существует цикл $Y \subset (Y_1 \cup Y_2) \setminus \{a\}$ (т. е. не содержащий a), причем $b \notin Y_1 \cup Y_2$, и поэтому $b \notin Y$. По вышеописанному предположению должно быть $c \in Y$. По доказанному выше Y – единственный цикл, не содержащий ни a, ни b, $Y = ab$, и точки $y_1, y_2 \in Y = ab$, которая пересекается с линией ac в точке a – противоречие. Следовательно, имеется всего одна линия, проходящая через b и не пересекающая линию ac, и новых таких точек $y \neq b$ добавится еще $(m-1)$ штук. Итого получаем

$$N = (m(m-1)+1) + (m-1) =$$
$$= (m+1)(m-1) + 1 = (m^2 - 1) + 1 = m^2$$

(«аффинный случай» – аффинная плоскость порядка m), а линий всего

$$\frac{N(N-1)}{m(m-1)} = \frac{m^2(m^2-1)}{m(m-1)} = m(m+1)$$

Случай 1.

Далее произведем проверку аксиом проективной плоскости.

Аксиома 1. Две различные точки определяют единственную прямую.

Доказательство следует из разделимости матроида.

Аксиома 2. Две прямые пересекаются в единственной точке.

Пусть однородный матроид M мощности $|M| = N = m^2 - m + 1$, где m – мощность линий, и a, b, c – его элементы, не содержащиеся в одном антицикле. По описанному выше построению все точки (элементы матроида) исчерпываются точками линий, соединяющих точку b с точками ac.

Пусть $L_1 = \overline{C}_1$, $L_2 = \overline{C}_2$ – две разные линии, дополнения циклов C_1 и C_2, $C_1 \neq C_2$. Ясно, что если линии пересекутся в двух или более точках, то они совпадут (см. первую аксиому плоскости). Если же они не пересекутся, $L_1 \cap L = \varnothing$, то $C_1 \cup C_2 = M$.

Пусть $w \in M$ – любой элемент, C – цикл, содержащий w. Тогда линия $L = \overline{C}$ не проходит через w и содержит m точек. Линии, проходящие через w и через различные точки линии L, различны, и их всего m штук. Точек на всех этих линиях, как было вычислено выше, всего $N = m^2 - m + 1$. Следовательно, этими точками исчерпываются все элементы матроида, и других линий, проходящих через w, больше нет.

Итак, доказано: через любую точку w проходят ровно m линий.

Всего пар различных линий

$$C_N^2 = \binom{N}{2} = \frac{N(N-1)}{2} =$$
$$= \frac{(m^2 - m + 1)(m^2 - m)}{2} = \frac{(m^2 - m + 1)m(m-1)}{2}$$

Следовательно, количество пар различных линий, проходящих через любую данную точку, равно

$$C_m^2 = \binom{m}{2} = \frac{m(m-1)}{2}$$

Умножая это количество на мощность матроида, получаем количество всех пар линий, имеющих непустое пересечение, и поскольку это число совпадает с количеством всех вообще пар линий, делаем вывод, что непересекающихся линий нет.

Итак, доказано: в «проективном случае» каждая пара различных линий пересекается в единственной точке.

Аксиома 3. Существуют четыре точки, никакие три из которых не лежат на одной линии.

Итак, пусть $m \geq 3$, точки a, b, c не лежат на одной линии (антицикле). Возьмем, поскольку $m \geq 3$, третью точку x на линии ac, отличную от a и c. Соединим ее линией с b, и опять-таки пользуясь тем, что $m \geq 3$, третью точку d на линии bx, отличную от b и x. Из аксиомы 1 следует, что $d \notin ac$, $d \notin ab$, $d \notin bc$. По построению

$a \notin bc, b \notin ac, c \notin ab$. Так, что $a \notin dc, a \notin db, b \notin dc, c \notin ad, b \notin ad, c \notin bd$, действительно, никакие три не лежат на одной линии. Итак, в самом деле, в «проективном случае» получаем конечную проективную плоскость.

Случай 2.

Далее рассмотрим проверку аксиом аффинной плоскости.

Аксиома 1 совпадает с проективным случаем.

Аксиома 2. Через любую точку вне данной линии проходит единственная линия, не пересекающая данную (по книге Артина Э. [13]).

Пусть однородный матроид (в «аффинном случае») мощности $|M| = N = m^2$, где m – мощность антициклов, и a, b, c – его элементы, не содержащиеся в одном антицикле (как в вышеописанном построении). Все точки матроида исчерпываются точками линий, соединяющими точку b с точками ac и точками единственной линии, проходящей через b и не пересекающейся с ac. Таким образом, через точку b проходит всего $(m + 1)$ линий. Ясно, что через любую точку w проходит не более $(m + 1)$ линий, содержащих как раз $(m - 1)(m + 1) + 1 = (m^2 - 1) + 1 = m^2 = N$ точек. А так как через w и любую точку, отличную от w, можно провести единственную прямую, то, следовательно, через каждую точку проходят ровно $(m + 1)$ линий, и так можно получить все точки матроида. Поэтому среди этих $(m + 1)$ линий есть в точности одна, не пересекающая данную линию, в которой всего m точек.

Аксиома 3. Совпадает с проективным случаем.

Итак, доказано:

Утверждение 4. Однородный разделяющий матроид с мощностью антициклов $m \geq 3$, в котором есть три разные точки, не лежащие в одном антицикле, является либо аффинной плоскостью порядка m, либо проективной плоскостью порядка $(m - 1)$ с прямыми линиями в качестве антициклов.

В продолжение исследований необходимо сформулировать следующие гипотезы:

Гипотеза 1. Конечная плоскость определяет СРС, соответствующий построенному выше матроиду.

Гипотеза 2. Если коранг $r > 3$, то однородные матроиды исчерпываются аффинными и проективными пространствами размерности $r - 1$ с естественным образом [11] построенными СРС.

Первая гипотеза представляется естественной, т. к. хорошо известна связанная с конечной аффинной плоскостью схема разделения секрета Шамира [1] «два из N».

Заключение

Итак, в работе изложена общепринятая классификация участников идеальных СРС и выявлена связь однородных матроидов коранга три с конечными аффинными и проективными плоскостями, которые могут быть использованы в идеальных однородных СРС. Сформулированы гипотезы, необходимые для продолжения исследований однородных СРС.

Примечания

1. Shamir A. How to share a secret // Communications of the ACM. – 1979. – T. 22. – No11. – P. 612–613

2. Введение в криптографию / под общ. ред. В. В. Ященко. – СПб : Питер, 2001. – 288 с.

3. Блейкли Г. Р., Кабатянский Г. А. Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. – 1997. – Т. 33. – № 3. – С. 102–110.

4. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд. Урал. ун-та, 2003. – 328 с.

5. Болотова Е. А., Коновалова С. С., Титов С. С. Свойства решеток разграничения доступа, совершенные шифры и схемы разделения секрета // Проблемы безопасности и противод. терроризму : материалы IV междунар. науч. конф. М. : МЦНМО, 2009. – Т. 2. – С. 71–86.

6. Ito M., Saito A., Nishizeki T. Secret sharing scheme realizing any access structure. Proc. IEEE Globecom'87. – 1987. – P. 99–102.

7. Marti-Farre J., Padro C. Secret sharing schemes on sparse homogeneous access structures with rank three // Electronic Journal of Combinatorics 11(1). – 2004.

8. Welsh D. J. A. Matroid Theory. Academic press. – London, 1976.

9. Асанов М. О., Баранский В. А., Расин В. В. Дискретная математика: графы, матроиды, алгоритмы. – Ижевск : НИЦ «Регулярная и хаотическая динамика», 2001. – 288 с.

10. Медведев Н. В., Титов С. С. Проблемы почти пороговых схем разделения секрета // Прикладная дискретная математика. – 2012. – № 5 – С. 53–54.

11. Медведев Н. В., Титов С. С. О почти пороговых матроидах и схемах разделения секрета // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 1(3). – С. 31–36.

12. Медведев Н. В., Титов С. С. Бинарные почти пороговые матроиды // Научно-технический вестник Поволжья. – 2012. – № 4. – С. 136–142.

13. Артин Э. Геометрическая алгебра. – М.: Наука, 1969. – 239 с.

МЕДВЕДЕВ Никита Владимирович, старший преподаватель кафедры «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, канд. техн. наук. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: itcrypt@gmail.com

ТИТОВ Сергей Сергеевич, профессор кафедры «Высшая и прикладная математика» Уральского государственного университета путей сообщения, д-р физ.-мат. наук, профессор. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: sergey.titov@usaaa.ru

MEDVEDEV Nikita, senior lecturer of the department «Information Technologies and Information Security» Ural State University of Railway Transport, Ph.D. Bld. 66, Kolmogorova Str., Ekaterinburg, 620075. E-mail: itcrypt@gmail.com

TITOV Sergey, professor of department «Higher and Applied Mathematics» Ural State University of Railway Transport, Prof. Bld. 66, Kolmogorova Str., Ekaterinburg, 620075. E-mail: sergey.titov@usaaa.ru