УДК 519.6

ХАРАКТЕРИСТИЧЕСКИЕ МНОЖЕСТВА ИДЕАЛЬНЫХ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА

Ю.П. Москалева, И.Г. Фомина

Таврический национальный университет им. В.И. Вернадского
факультет математики и информатики
пр-т Вернадского, 4, г. Симферополь, 95007, Украина
e-mail: *YulMosk@mail.ru*

Abstract

The secret sharing scheme with Γ аз the access structure is a method for the distribution of the information between the participant of set P so that a subset of participants can determine the key if and only if that subset is in Γ. In this paper the access structure of ideal secret sharing scheme in the rank 2 case is described in terms of group theory.

Введение

Первые задачи криптографического разделения секрета для случая пороговой структуры доступа, были независимо сформулиронаны и решены Шамиром (A. Shamir) [1] и Блэкли (G.Rr Blakley) [2]. За два десятилетия сущесвования. задача разделения секрета превратилась в активно развивающуюся область современной криптографии. Наиболее полные современные обзоры математики разделения секрета можно найти в учебниках [3], [4], [5].

Анализ последних достижений в области описания структур доступа идеальных схем разделения секрета [3], [6], [7] позволяет сделать вывод, что наиболее общим направлением исследовании в этой области является изучение специальным образом построенных матроидов [8]. Следует отметить, что переход от исследования структуры доступа идеальной схемы разделения секрета к матроидам не упрощает практический анализ структур доступа. В связи с этим *важной и актуальной проблемой* является поиск новых путей решения задачи описания структур доступа идеальных слей разделения секрета, позволяющих упростить *решение вопроса существования идеальных схем разделения секрета* для той или иной структуры доступа.

Целью настоящей работы является описание структуры доступа идеальных схем разделения секрета в терминах теории групп для случая ранга 2.

1. Постановка задачи

Пусть P $= \{p_1, ..., \mathrm{p}_n\}$.P будем называть *множеством участников схемы разделения секрета* (СРС). Обозначим M — конечную матрицу с количеством столбцов $n+1$. Пометим меткой p_0 первый столбец матрицы M и метками $p_1, ..., \mathrm{p}_n$ остальные столбцы. Произвольное подмножество $\Gamma : \Gamma \subset \mathcal{B}(P)$, где $\mathcal{B}(P)$ — булеан множества

P, будем называть *структурой доступа*, а произвольное $A \in \Gamma$ *допустимым множеством.*

Пусть $P_0 = \{p_0, p_1, ..., \mathrm{p}_n\}$. Обозначим $M(r, A)$ — r-ую строку матрицы, полученную из M удалением столбцов, метки которых не принадлежат множеству A. Рассмотрим $A \subset P_0$ и $b \in P_0$.

Определение 1. Будем говорить, что A знает b (и обозначать $A \Rightarrow b$) если из того, что r_1 и $r_2 : \mathrm{M}(r_1, \mathrm{A}) = M(r_2, \mathrm{A})$ следует $\mathrm{M}(r_1, b) = \mathrm{M}(r_2, b)$.

Соответственно A не знает b ($A \not\Rightarrow b$) если найдутся строчки r_1 и $r_2 : \mathrm{M}(r_1, A) = \mathrm{M}(r_2, \mathrm{A})$ и $\mathrm{M}(r_1, b) \neq M(r_2, b)$.

Обозначим через $S(A)$ множество различных $\mathrm{M}(r, \mathrm{A})$ и через $\sharp\mathrm{A}$ мощность множества $S(A)$.

Определение 2. Будем говорить, что A не имеет информации о b (и обозначать $bA \nrightarrow b$), если $\forall \alpha, \beta : \alpha \in S(A)$ и $\beta \in S(b) \exists r : M(r, A) = \alpha$ и $M(r, b) = \beta$.

Соответственно A имеет информации о $b(\mathrm{A} \to b)$, если $\exists \alpha, \beta : \alpha \in S(A)$ и $\beta \in S(b)$ и при этом не $\exists r : \mathrm{M}(r, \mathrm{A}) = \alpha$ и $\mathrm{M}(r, \mathrm{Ь}) = \beta$.

Определение 3. Матрица M называется *совершенной* СРС со структурой доступа Γ, если

1) $A \Rightarrow p_0 \quad \forall A \in \Gamma$,
2) $A \nrightarrow p_0 \quad \forall A \notin \Gamma$.

Из определений 1- 3 следуют свойства:

1. Если $A \Rightarrow b$, то $A \to b$.
2. Если $A \nrightarrow b$, то $A \not\Rightarrow b$
3. Если M совершенная СРС, то из того, что $\mathrm{A} \to p_0$, следует $\mathrm{A} \Rightarrow p_0$.
4. Если M совершенная СРС, то из того, что $A \not\Rightarrow p_0$, следует $\mathrm{A} \nrightarrow p_0$.

Определение 4. Матрица M называется *идеальной* СРС если

1) M — совершенная СРС,
2) $\sharp p_0 = \sharp p_i \quad \forall i = \overline{1, n}$.

Если СРС является идеальной, то, не ограничивая общности будем считать, что $S(p_0) = S(p_1) = \ldots = S(p_n) = S$. Обозначим $|S| = q$. Каждая строка r совершенной СРС M со структурой доступа Γ является методом разделения секрета $M(r, \mathrm{p}_0)$ между участниками множества P. Каждый элемент $M(r, \mathrm{p}_i)$ строки r — это *часть секрета* участника p_i. Предполагается, что каждый участник p_i знает только свою часть секрета. Матрица M считается общеизвестной. Из определения совершенной СРС следует, что участники допустимого множества A по $M(r, \mathrm{A})$ могут восстановить секрет $M(r, p_0)$, участники множества A не из Γ, зная $M(r, \mathrm{A})$ не получают никакой дополнительной информации о значении секрета.

Естественными свойствами,вытекающими из постановки задачи разделения секрета являются: монотонность структуры доступа и связность СРС. Множество подмножеств Γ называется *монотонным*, если из того, что B ∈ Γ и B ⊂ C следует что C ∈ Γ. Обозначим Γ_m множество минимальных элементов Γ. СРС со структурой доступа Γ называется *связной*, если $\forall p \in P \exists A \in \Gamma_m : p \in A$, то есть каждый участник входит хотя бы в одно минимальное допустимое множество.

Для всякой совершенной СРС $\sharp p \geqslant \sharp p_0 \ \forall p \in P$ [3], поэтому идеальные СРС, для которых $\sharp p = \sharp p_0 \ \forall p \in P$, представляют особый интерес, как случай минимально возможных размеров частей секрета. В связи с этим важной является *задача описания структур доступа, для которые существуют идеальные* СРС.

2. Идеальные СРС ранга 2

Определение 5. Идеальная СРС имеет ранг 2, если

1. $\exists A \in \Gamma_m : |A| = 2$;
2. $\forall A \in \Gamma_m : |A| = 1 \vee |A| = 2$;
3. $\sharp P_0 = q^2$.

Пусть $D(M) = \{A \subseteq P | \exists y \in A : \frac{A}{y} \Rightarrow y\}$. Тогда для случая идеальных СРС ранга 2 имеют место следующие теоремы.

Теорема 1. [6] *Пусть* M *— связная идеальная СРС ранга 2. Тогда* $D(M)$ *— зависимые множества связного матроида.*

Теорема 2. [6] *Пусть* $T = (V, I)$ *— связный матроид ранга 2. Пусть* $v_0 \in V$. *Тогда* $\exists M$ *— связная идеальная СРС такая, что* $p_0 = v_0$, $P_0 = V$ *и* $D(M)$ *— зависимые множества* T.

Рассмотрим вспомогательные утверждения.

Лемма 1. [6] *Пусть* $A \subseteq P_0 ub \in P_0$. *Если* $A \Rightarrow b$, *то* $\sharp A = \sharp(A \bigcup b)$.

Лемма 2. *Пусть* M *— идеальная СРС ранга два. Тогда следующие утверждения эквивалентны:*

1) $\{a, b\} \notin \Gamma$;
2) $a \Rightarrow bu\{a\} \notin \Gamma$

Доказательство. Пусть $\{a, b\} \notin \Gamma$. Так как M — совершенная СРС, то $\{a, b\} \nrightarrow p_0$, тогда $\sharp\{a, b, p_0\} = \sharp\{a, b\} \cdot q$. Так как M — идеальная СРС ранга два, то $\sharp P_0 = q^2$, тогда

$$\sharp\{a, b\} \cdot q = \sharp\{a, b, p_0\} \leqslant q^2.$$

Откуда получаем, что $\sharp\{a, b\} \leqslant q$. С другой стороны $\sharp a = q$.Тогда

$$q = \sharp a \leqslant \sharp\{a, b\} \leqslant q$$

и следовательно, $\sharp\{a,b\}=q$. Так как $\sharp b=q$, то $a\Rightarrow b$.

В другую сторону. Пусть $a\Rightarrow b$. Предположим, что $\{\mathrm{a},b\}\in\Gamma$. Если $\{\mathrm{a},b\}\in\Gamma$, то $\{\mathrm{a}\}\in\Gamma$. Действительно, если $a\Rightarrow b$, то по Свойству 1 $a\to b$, тогда

$$\sharp\{a,b\}<\sharp\{a\}\cdot q.$$

По лемме 1, из того, что $\{\mathrm{a},b\}\in\Gamma$, следует что $\sharp\{a,b\}=\sharp\{a,b,p_0\}$. Далее,

$$\sharp\{a,p_0\}\leqslant\sharp\{a,b,p_0\}=\sharp\{a,b\}<\sharp\{a\}\cdot q.$$

Строгое неравенство $\sharp\{a,p_0\}<\sharp\{a\}\cdot q$ означает, что $a\to p_0$, так как M — совершенная СРС, то $a\Rightarrow p_0$ и следовательно $\{a\}\in\Gamma$. Получили противоречие, значит $\{a,b\}\in\Gamma$.

В настоящей работе описание структур доступа идеальных СРС ранга 2 проводится в терминах множества характеристических векторов допустимых множеств мощности 2.

3. Характеристические множества идеальных схем ранга 2

Обозначим $B^n=\{\gamma=(\gamma_1,\ldots,\gamma_n)|\gamma_i\in\{0,1\}\}$. B^n — группа относительно операции $\gamma+\delta=(\gamma_1\oplus\delta_1,\ldots,\gamma_n\oplus\delta_n)$ и линейное нормированное пространство с операцией сложения как задано выше, операцией умножения на число из поля $\{0,1\}$ и нормой $\|\gamma\|=\sum\limits_{i=1}^{n}\gamma_i$. Через B^n_k будем обозначать множество векторов из B^n нормы k. Введем в рассмотрение произведение $k(k\geqslant 2)$ элементов из B^n по следующему правилу

$$(\gamma^1,\ldots,\gamma^k)=\sum_{i=1}^{n}\gamma^1_i\ldots\gamma^k_i.$$

Теорема 3. *Пусть $\gamma^1,\ldots,\gamma^k\in B^n$. Тогда имеет место формула*

$$\|\gamma^1+\ldots+\gamma^k\|=\sum_{i=1}^{k}\|\gamma^i\|-2\sum_{1\leqslant i_1<i_2\leqslant k}(\gamma^{i_1},\gamma^{i_2})+2^2\sum_{1\leqslant i_1<i_2<i_3\leqslant k}(\gamma^{i_1},\gamma^{i_2},\gamma^{i_3})+\ldots$$
$$+(-1)^{l-1}2^{l-1}\sum_{1\leqslant i_1<i_2\ldots<i_l\leqslant k}(\gamma^{i_1},\ldots,\gamma^{i_l})+\ldots+(-1)^{k-1}2^{k-1}(\gamma^{i_1},\ldots,\gamma^{i_k}).\quad(1)$$

Доказательство. Рассмотрим бинарную матрицу со строками $\gamma^1,\ldots,\gamma^k$. Зафиксируем произвольный столбец. Пусть l — количество единиц в столбце. Если l четное, то этому столбцу в левой части формулы соответствует нулевая координата, если l нечетное, то единичная. Рассмотрим правую часть

$$l-2C^2_l+2C^3_l+\ldots+(-1)^{l-1}2^{l-1}C^l_l=1/2(2l-2^2C^2_l+2^3C^3_l+\ldots+(-1)^{l-1}2^lC^l_l)=$$
$$=1/2(1-(1-2l+2^2C^2_l-2^3C^3_l+\ldots+(-1)^l2^lC^l_l))=$$
$$=1/2(1-(-1)^l)=\begin{cases}1, & \text{если } l \text{ нечетно},\\ 0, & \text{если } l \text{ четно}.\end{cases}$$

Следствие 1. *Если* $\gamma, \delta \in B^n$ *такие, что* $\|\gamma\| = \|\delta\| = 2$, *то* $\|\gamma + \delta\| = 2$ *тогда и только тогда, когда* $(\gamma, \delta) = 1$.

Определение 6. Характеристическим множеством СРС ранга два будем называть (и обозначать $\mathcal{S}(M)$) множество характеристических векторов $A \in \Gamma_m : |A| = 2$.

Теорема 4. *Пусть* M *идеальная СРС ранга два и* $\gamma, \delta \in B_2^n \backslash \mathcal{S}(M)$. *Тогда* $\gamma + \delta \notin \mathcal{S}(M)$.

Доказательство. Так как $\mathcal{S}(M)$ строится по $A \in \Gamma_m : |A| = 2$, то $\mathcal{S}(M) \subset B_2^n$. По формуле (1) при $k = 2$ имеем $\|\gamma + \delta\| = \|\gamma\| + \|\delta\| - 2(\gamma, \delta)$. Если $(\gamma, \delta) = 2$, то есть $\gamma = \delta$, то $\|\gamma + \delta\| = 0$ и значит $\gamma + \delta \notin \mathcal{S}(M)$. Еслп $(\gamma, \delta) = 0$, то $\|\gamma + \delta\| = 4$ и значит $\gamma + \delta \notin \mathcal{S}(M)$. Рассмотрим случай когда $(\gamma, \delta) = 1$, то есть γ и δ совпадают по одной единичной координате. Пусть $\gamma : \gamma_i = \gamma_j = 1$ и $\delta : \delta_j = \delta_k = 1$, тогда $\{p_i, p_j\} \notin \Gamma$ и $\{p_j, p_k\} \notin \Gamma$. По Лемме 2 это означает, что $p_i \Rightarrow p_j$ и $p_j \Rightarrow p_k$, но тогда $p_i \Rightarrow p_k$, так как $\{p_i\} \notin \Gamma$, то еще раз используя Лемму 2 получим $\{p_j, p_k\} \notin \Gamma$ и значит $\gamma + \delta \notin \mathcal{S}(M)$.

Теорема 5. *Пусть* $\mathcal{S} \subset B_2^n$ *такое что для всяких* $\gamma, \delta \in B_2^n \backslash \mathcal{S}$ *выполняется условие* $\gamma + \delta \notin \mathcal{S}$. *Тогда существует матрица* M *— идеальная СРС ранга два такая, что* $\mathcal{S}(M) = \mathcal{S}$.

Доказательство. Во множестве участников введем отношение R : pRpR и $p_i R p_j$ при $i \neq j$ если характеристический вектор множества $\{p_i, p_j\}$ не принадлежит $\mathcal{S}$. Отношение R рефлексивно и симметрично. Покажем, что R транзитивно. Пусть $p_i R p_j$ и $p_j R p_k$, тогда характеристические векторы γ, δ множеств $\{p_i, p_j\}$, $\{p_j, p_k\}$ не принадлежат $\mathcal{S}$ и по условию теоремы $\gamma + \delta \notin \mathcal{S}$, но $\gamma + \delta$ — характеристический вектор $\{p_j, p_k\}$, откуда следует, что $p_i R p_k$. Таким образом отношение R является отношением эквивалентности. Обозначим $l = |P|_R|$ и построим $(l, 2)$-пороговую схему Шамира [1] с $q > l$. Определим матрицу M размера $q \times (n+1)$ каждый столбец которой совпадает со столбцом соответствующего класса эквивалентности схемы Шамира. Непосредственной проверкой получаем, что M — идеальная СРС ранга 2 с $\mathcal{S}(M) = \mathcal{S}$.

4. Классификация идеальных СРС ранга 2 в терминах теории групп

Теорема 6. *Пусть* M *идеальная СРС ранга два. Тогда* $H \cap \mathcal{S}(M) = \varnothing$, *где* H *— подгруппа группы* B^n *с системой образующих* $B_2^n \backslash \mathcal{S}(M)$.

Доказательство. Так как $\forall \gamma \in B^n \quad 2\gamma = 0$, то всякий $h \in H$ представим в виде $h = \gamma^1 + \ldots + \gamma^k$ — суммы различных векторов из системы образующих подгруппы. Рассмотрим $h \in H : \|h\| = 2$. Для доказательства теоремы достаточно показать, что $h \notin \mathcal{S}(M)$. При $k = 1$ $h \notin \mathcal{S}(M)$ по построению подгруппы. Для случая $k = 2$ $h \notin \mathcal{S}(M)$ по Теореме 4. Пусть теперь $k = 3$. Тогда $h = \gamma + \delta + d$ и $\|h\| = 2$. Так как $\|\gamma + \delta + d\| = 2$, то найдется хотя бы одна пара векторов, совпадающих ровно по одной единичной координате. Иначе по формуле (1) $\|\gamma + \delta + d\| = 6$. Пусть γ, δ

— векторы, совпадающие ровно по одной единичной координате. По Следствию из Теоремы 3 $\|\gamma + \delta\| = 2$ и по Теореме 4 $\gamma + \delta \notin \mathcal{S}(M)$. Обозначим $\eta = \gamma + \delta$, тогда $\eta, d \in B_2^n \backslash \mathcal{S}(M)$ и по Теореме 4 $h = \eta + d \notin \mathcal{S}(M)$. Аналогично для $h = \gamma^1 + \ldots + \gamma^k$ получаем, что h сумма $k-1$ или $k-3$ различных векторов из системы образующих $B_2^n \backslash \mathcal{S}(M)$. Тогда по индукции $h = \gamma^1 + \ldots + \gamma^k \notin \mathcal{S}(M)$.

Теорема 7. *Пусть $S \subset B_2^n$ такое, что $H \cap \mathcal{S} = \emptyset$, где H — подгруппа группы B^n с системой образующих $B_2^n \backslash \mathcal{S}$. Тогда существует матрица* M *— идеальная СРС ранга два такая, что $\mathcal{S}(M) = \mathcal{S}$.*

Доказательство. Иэ того, что $H \cap \mathcal{S} = \emptyset$ следует, что для всяких $\gamma, \delta \in B_2^n \backslash \mathcal{S}$ выполняется условие $\gamma + \delta \notin \mathcal{S}$ и по Теореме 5 утверждение Теоремы 7.

Подмножество абелевой группы называется свободным от сумм, если сумма двух любых элементов подмножества не принадлежит подмножеству. Отметим, для случая $|P|_R| = 2$ справедливость следующей теоремы.

Теорема 8. *Пусть* M *идеальная СРС ранга два и $|P|_R| = 2$. Тогда $\mathcal{S}(M)$ максимальное в B_2^n множество свободное от сумм.*

Заключение

Основным результатом настоящей работы являются Теоремы 4-7 В терминах характеристических множеств схем разделения секрета получены необходимые и достаточные условия существования идеальных схем разделения секрета для заданных структур доступа для случая ранга 2.

Перспективным представляется описание структур доступа идеальных СРС в терминах теории групп для идеальных СРС произвольного ранга

Список литературы

1. Shamir A. How to share a secret // Com. of the ACM. - 1979. - Vol. 22, №11. - P.612-613.
2. Blakley G.R. Safeguarding cryptographic keys // Proc. of AFIPS Nasiona1 Computer Conference. - 1979. - 48. - P.313-317.
3. Ященко В.В. Введение в криптографию. - Санкт-Петербург: МЦНМО, 2001. - 237 с.
4. Шнайер Б. Приклдная криптография. - М.: Изд-во Триумф, 2003. - 816 с.
5. Чмора А. Современная прикладная криптография. - М.: Гелиос АРВ, 2001. - 244 с.
6. Brickell E.F., Davenport D.M. On the Classification of Ideal Secret Sharing Schemes // J. Criptology. - 1991. - Vol. 4(2). - P.123-134.
7. Блейкли Г.Р., Кабатянский Г.А. Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи ннформации. - 1997. - Т. 33, вып. 3. - С. 102-110.
8. Емеличев В.А., Мельников О И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. - М.: Наука, 1990. - 384с.