2008 Математические методы криптографии № 2(2)
DOI 10.17223/20710410/2/11
УДК 519.7

СОВЕРШЕННЫЕ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

Н.Г. Парватов

Томский государственный университет

E-mail: parvatov@mail.tsu.ru

В статье излагаются некоторые известные результаты теории разделения секрета.

***Ключевые слова*:** *совершенная схема разделения секрета*, *структура доступа*, *идеальное разделение секрета*, *полиматроид*, *матроид.*

В теории разделения секрета рассматривается задача, которую неформально можно поставить следующим образом. Требуется разделить значение секрета из некоторого множества секретов между участниками из некоторого множества участников, выдав каждому участнику его долю секрета так, чтобы заранее определённые, авторизованные, множества участников могли, соединив свои доли, вычислить истинное значение секрета, а участники остальных, неавторизованных, множеств не могли бы этого сделать. Иногда требуется, чтобы участники неавторизованных множеств, пытаясь восстановить истинное значение секрета, не могли бы исключить ни одного значения из множества секретов, или даже не получили бы никакой дополнительной информации о секрете. Данная задача может возникнуть при разделении доступа между группой лиц, не доверяющих друг другу, а также при хранении конфиденциальной информации, разделённой на части. Несмотря на то, что в настоящее время имеется довольно обширный перечень публикаций по разделению секрета, некоторые ключевые статьи достать довольно трудно. Столкнувшись с этой трудностью, автор вынужден был самостоятельно восстанавливать систему первоначальных понятий теории разделения секрета и получать некоторые основные результаты этой теории. О некоторых из этих результатов и пойдёт речь далее.

Структура доступа

Структурой доступа (сд) на множестве Q станем называть всякое подмножество G системы $B(Q)$ всех подмножеств множества Q, обладающее свойством монотонности:

«если часть множества $A \subseteq Q$ принадлежит G, то и само A принадлежит G».

Множества, принадлежащие сд, станем называть *авторизованными* в ней. Система всех минимальных по включению авторизованных множеств сд G называется её *базисом* и обозначается G_0. Элементы множества Q называются *участниками* сд G. Участники, принадлежащие базисным множествам из G_0, называются *существенными*. Пользуясь случаем, введём несколько важных операций над сд. Во-первых, заметим, что для любого множества U из $B(Q)$ множество $B(Q\backslash U)\cap G$ является сд на множестве участников $Q\backslash U$; эту сд станем обозначать через $G_{Q\backslash U}$. Множество всех подмножеств V из $B(Q)$, таких, что $U\cup V$ авторизованно в G, образует сд на Q. Эту сд обозначим через $G^{(U)}$. Наконец, через $G^{Q\backslash U}$ станем обозначать сд $G^{(U)}{}_{Q\backslash U}$, полученную повторным применением первых двух операций. Из данных трёх операций первая и последняя имеют особое значение и называются операциями *взятия миноров*. Сд, возникающие из данной сд G в результате (возможно, неоднократного) применения подобных операций, называются *минорами* G. Отметим, что многократное взятие миноров можно всегда заменить равносильным не более, чем двукратным применением подобных операций. Если все участники, принадлежащие множеству U, несущественны в сд G, то миноры $G_{Q\backslash U}$ и $G^{Q\backslash U}$ совпадают. В этой ситуации будем говорить, что сд G получена из сд $G_{Q\backslash U}$ (равносильно из $G^{Q\backslash U}$) путём *введения* несущественных участников, а сд $G_{Q\backslash U}$ (равносильно сд $G^{Q\backslash U}$) получена из сд G путём *удаления* несущественных участников. Классы сд, замкнутые операциями взятия миноров, а также операциями введения и удаления несущественных участников, станем называть *инвариантными*. Далее, для сд G на множестве Q через G^* принято обозначать определённую на том же множестве Q сд, в которой авторизованными являются всевозможные дополнения неавторизованных в G множеств. Ясно, что $G^{**}=G$. Сд G и G^* по отношению друг к другу принято называть *двойственными*.

В дальнейшем полезно иметь в виду, что существует взаимно однозначное соответствие

$$x \mapsto U(x)$$

между булевыми векторами $x = (x_1, ..., x_n)$ длины n и всевозможными подмножествами $U(x)$ n-элементного множества $Q = \{p_1, ..., p_n\}$, при котором $U(x) = \{p_i \mid x_i = 1\}$. Данный факт влечёт существование (обратных по отношению друг к другу) взаимно однозначных соответствий

$$f \mapsto G(f),\ G \mapsto f(G)$$

между булевыми функциями f, зависящими от n аргументов $x_1, ..., x_n$, и всевозможными системами G подмножеств множества Q. При этом система $G(f)$ состоит из всевозможных таких подмножеств $U(x)$, для которых $f(x) = 1$, а булева функция $f(G)$ принимает значение 1 на наборе x, если $U(x)$ принадлежит G. Данные соответствия, в свою очередь, индуцируют взаимно однозначное соответствие между монотонными булевыми функциями от n аргументов и структурами доступа на n-элементном множестве. Отметим, что существенность участника p_i из Q в структуре доступа G равносильна тому, что функция $f(G)$ зависит от переменной x_i существенно. Отметим также, что функции $f(G_{Q\setminus U})$ и $f(G^{Q\setminus U})$ могут быть получены из функции $f(G)$ подстановкой константы 0 и 1 соответственно на места переменных x_i, $p_i \in U$. В свете сказанного легко понятна связь между инвариантными классами структур доступа и инвариантными классами булевых функций (замкнутыми операциями перестановки переменных, операциями введения и удаления фиктивных переменных, а также операциями подстановки 0 и 1 на места переменных [1]).

Схема разделения секрета

Договоримся обозначать через A^Q множество всевозможных функций $s{:}Q\to A$. Всякую такую функцию будем называть также набором, а её значение $s(q)$ будем также обозначать через s_q и называть значением q-координаты набора s. Для любого множества U из $B(Q)$ через s_U станем обозначать ограничение $s_U{:}U\to A$, такое, что $s_U(q) = s(q)$ для всех q из U. В дальнейшем нас будут интересовать подмножества множества A^Q. Для всякого такого подмножества S станем обозначать через S_q множество всех q-координат s_q и через S_U множество всех ограничений s_U для всевозможных наборов s из S. Для набора y из S_U через S^y обозначим множество всех таких наборов s из S, что $s_U = y$. Пусть $Q = P \cup \{D\}$ и элемент D не принадлежит множеству P. Набор (S, P, D), где S – непустое подмножество множества A^Q, называется *схемой разделения секрета* (*срс*). При этом множество Q называется *множеством участников* данной срс. Участник D называется *дилером*. Множество S_D называется *множеством секретов*, число $|S_D|$ его элементов называется *порядком* срс. Множество S_q называется *множеством долей* участника q из P. Наборы из S называются *правилами разделения секрета*. Так, s из S – это правило разделения секрета s_D, а s_q – принадлежащая участнику q доля секрета s_D, разделённого по правилу s. Несложно понять, что всевозможные множества U из $B(P)$, для которых выполняется равенство

$$|S_U \cup {}_{\{D\}}| = |S_U|,$$

образуют сд, обозначим её через $G(S, P)$, на множестве P. Это – сд, *реализуемая* срс S. В соответствии с определением для любого авторизованного в $G(S, P)$ множества U и любого правила s из S значение s_D однозначно определяется ограничением s_U. Это свойство позволяет использовать срс для решения описанной во введении задачи разделения секрета. Именно для того, чтобы разделить значение секрета из множества S_D между участниками из множества P так, чтобы авторизованные в $G(S, P)$ множества участников могли восстановить секрет, нужно прибегнуть к помощи ещё одного участника, пользующегося всеобщим доверием. Этот участник выбирает наугад (или в соответствии с некоторым распределением) правило s из S и каждому участнику q из P в тайне от остальных передаёт долю s_q. Отметим, что в описанной ситуации доли участников из неавторизованного множества могут содержать некоторую (возможно, значительную или даже полную) информацию о секрете. Чтобы избавить срс от этого нежелательного свойства, понадобятся более сложные определения, которые будут сделаны далее.

Энтропийная функция

Для непустого подмножества S множества A^Q функцию $h{:}B(Q)\to[0,+\infty)$ будем называть *энтропийной*, если выполнены условия:

1) $h(\varnothing) = 0$;

2) $h(U) \le h(V)$, если $U \subseteq V \subseteq Q$;

3) $h(U \cup V) + h(U \cap V) \le h(U) + h(V)$ для любых подмножеств U и V множества Q;

4) если $h(U) = h(V)$ и $U \subseteq V \subseteq Q$, то $|S_U| = |S_V|$.

В частности, равенства $h(U) = 0$ и $|S_U| = 1$ равносильны. Если говорить неформально, то величина $h(U)$ (*энтропия* множества U) призвана задавать степень неопределённости, возникающую при попытках угадать зафиксированный элемент из S_U. Примером энтропийной функции на S может служить *комбинаторная энтропия*, определённая для всех U из $B(Q)$ как

$$h(U) = \log|S_U|,$$

(логарифмы берутся по фиксированному основанию $k > 1$), а также *энтропия Шеннона* (см. [2]), определённая для всех U из $B(Q)$ как

$$h(U) = -\Sigma P_U(x_U)\log P_U(x_U).$$

Во втором случае предполагается, что на множестве S определено распределение $P(x)$ (ненулевых) вероятностей случайной величины X, которое индуцирует распределение $P_U(x_U)$ случайной величины X_U на множестве S_U, а суммирование ведётся по всем x_U из S_U; при этом величину $h(U)$ принято называть *вероят-*

ностной энтропией, или *энтропией Шеннона*, случайной величины X_U. В обоих случаях все четыре свойства очевидны, известны или легко проверяются. В первом свойстве предполагается, что множество S_U при пустом U само не пусто, а состоит из единственного пустого набора (см. [2]). Вполне возможно, что имеют смысл и другие способы определения энтропийной функции, но перечисленные два являются основными. Имеет смысл при $U \subseteq V$ разность $h(V) - h(U)$ обозначать через $h(V|U)$ и называть *условной энтропией* множества V при известном U. Эта величина задаёт остаточную неопределённость вектора s_V при известном ограничении s_U (и известном S) и может принимать значения от 0 (когда s_V однозначно восстанавливается по известному s_U и S) до $h(V\setminus U)$. Отметим, что как комбинаторная, так и вероятностная энтропия h обладает ещё одним свойством:

5) если $h(U \cup V) + h(U \cap V) = h(U) + h(V)$, то $|S_{U\cup V}||S_{U\cap V}| = |S_U||S_V|$,

из которого следует, что при пустом пересечении $U \cap V$ равенство $h(U \cup V) = h(U) + h(V)$ влечёт $|S_{U\cup V}|=|S_U||S_V|$. Последнее означает, что компоненты s_U и s_V в наборе $s_{U\cup V}$ принимают все возможные значения из множеств S_U и S_V.

Совершенная срс

Пусть теперь $Q = P \cup \{D\}$, $D \notin P$ и h − энтропийная функция на непустом множестве $S \subseteq A^Q$. Набор (S, P, D, h) будем называть *совершенной срс*, если для каждого подмножества $U \subseteq P$ выполняется

$$h(U, D) = h(U) \text{ или } h(U, D) = h(U) + h(D).$$

(Здесь и далее из соображений краткости под знаком функции h опускаются знаки объединения и фигурные скобки; вместо них используются запятые.) В случае комбинаторной или вероятностной энтропии h будем говорить соответственно о *комбинаторной* или *вероятностной срс*. Те подмножества U, для которых выполняется первое условие, составляют сд $G(S, P)$, реализуемую данной срс. Как уже отмечалось, для таких подмножеств U имеется возможность для любого правила s из S определить значение s_D по проекции s_U. В это же время для неавторизованных в $G(S, P)$ подмножеств U выполняется второе условие, означающее, что участники этого множества при любом s из S, пытаясь угадать s_D по s_U, сталкиваются с максимально возможной неопределённостью. В случае комбинаторной срс это означает, что для любого набора y из S_U найдётся правило s в S такое, что $s_U = y$, обладающее любым наперёд заданным значением s_D из S_D. А в случае вероятностной срс это означает, что для любого правила s из S проекция s_U не несёт никакой информации о значении секрета s_D.

Скорость срс

В силу вышесказанного об энтропийной функции h возможность эффективного использования срс в значительной степени определяется величинами $h(p)$ для p из P. Чем они больше, тем больше требуется затрат для передачи, хранения и обработки долей. Вместе с тем без ущерба для разделения и восстановления секрета несущественным участникам можно не передавать их долей. В связи с этим эффективность совершенной срс (S, P, D, h), реализующей сд G, можно охарактеризовать величиной

$$r(S, P, D, h) = \min(h(p)/h(D)),$$

где min вычисляется по всевозможным существенным участникам p из $\cup G_0$. Эта величина называется *скоростью* срс (S, P, D, h). Имеет место

Теорема 1. Пусть совершенная срс (S, P, D, h) реализует сд G. Тогда для любого существенного в G участника p из P имеет место неравенство $h(p) \le h(D)$.

Доказательство. Так как участник p существенный в G, то для некоторого неавторизованного в G множества U множество $U \cup \{p\}$ авторизованно в G. Тогда $h(U) + h(p) \ge h(U, p) = h(U, p, D) \ge h(U, D) = h(U) + h(D)$. Отсюда $h(p) \ge h(D)$. Теорема доказана.

Из доказанной теоремы следует, что скорость определена корректно и принимает значения из отрезка [0, 1], если имеется хотя бы один существенный участник (то есть когда сд G не тривиальна − не пуста и отличается от $B(P)$). Если существенных участников нет, то скорость срс будем считать бесконечной и будем обозначать её знаком $+\infty$. Срс, имеющие скорость, равную 1 или $+\infty$, называются *идеальными*.

Одной из основных задач теории разделения секрета является задача создания (синтеза) срс для заданной сд. При этом требуется в некотором классе найти срс, реализующую заданную сд и имеющую по возможности максимальную скорость. Этим оправдывается введение для заданного класса C схем разделения секрета и заданной сд G на множестве P величины

$$r(C, G) = \sup r(S, P, D, h),$$

где sup берётся по всевозможным срс (S, P, D, h) из класса C, реализующим сд G. Данная величина носит название *скорости* сд G *в классе* C. Отметим, что скорость $r(C, G)$ данной сд G в классе C не обязана достигаться на некоторой срс из C, но может достигаться на некоторой последовательности срс. В частности, автор не исключает возможности существования сд, имеющей в некотором классе скорость, равную 1, но не имеющей в этом классе идеальной реализации.

Вычислительная эффективность срс

Введённая выше скорость схем разделения секрета в большей степени характеризует их коммуникационную (связанную с затратами при передаче и хранении долей секрета), нежели вычислительную эффективность. Последняя определяется вычислительными затратами, необходимыми для разделения и восстановления секрета. Эти затраты могут быть значительными вне зависимости от энтропии долей. Более прямо вычислительную эффективность срс (S, P, D, h) характеризует максимальная схемная сложность $l(S, P, D, h)$ функции

$$S_U \to S_D,$$

определённой для каждого авторизованного множества U следующим образом:

$$x \mapsto y, \text{ если } x = s_U \text{ и } y = s_D \text{ для некоторого } s \text{ из } S.$$

Естественно назвать эту величину *сложностью* срс (S, P, D, h). В связи с этим представляет интерес задача нахождения для заданной сд реализующей её срс, принадлежащей заданному классу и имеющей по возможности минимальную сложность. К сожалению, в известных автору работах данная задача не рассматривалась.

Срс, связанные с группами

Пусть $S \subseteq A^Q$, и для любого элемента q из Q пусть S_q – аддитивная (но не обязательно абелева) группа с множеством операторов K, действующих левым умножением [3, 4]. Через $\Pi_Q S_q$ обозначается прямое произведение этих групп, состоящее из всевозможных таких наборов s из A^Q, что $s_q \in S_q$ для любого q из Q, и являющееся группой с множеством операторов K, в которой

$$(s + w)_q = s_q + w_q, \ (cs)_q = cs_q$$

для любых s и w из $\Pi_Q S_q$ и любого c из K. Пусть также множество S является подгруппой группы $\Pi_Q S_q$ (и тогда подпрямым произведением групп S_q). В этой ситуации полезно иметь в виду, что для любого подмножества $U \subseteq Q$ и для нулевого набора 0 из $S_{Q\setminus U}$ каждое из множеств S_U и S^0 является (K-операторной) подгруппой группы $\Pi_U S_q$, а для любого набора y из $S_{Q\setminus U}$ множество S^y является смежным классом группы $S_{Q\setminus U}$ по подгруппе S^0. Пусть, наконец, $Q = P \cup \{D\}$ и для любого подмножества $U \subseteq P$ верно

$$|S_{U\cup\{D\}}| = |S_U| \text{ или } |S_{U\cup\{D\}}| = |S_U||S_{\{D\}}|. \qquad (1)$$

Тогда можно определить совершенную комбинаторную срс (S, P, D, h) с ранговой функцией h, такой, что $h(U) = log_{|S(D)|} S(U)$. Эта срс является одновременно и вероятностной для равномерного распределения вероятностей на S. В некоторых случаях условие (1) выполняется автоматически. Так происходит, например, когда группа S_D простая относительно множества операторов K, то есть имеет ровно две допустимые относительно K подгруппы (именно тривиальные подгруппы). В частности, именно этот случай имеет место, когда все S_q являются одномерными векторными пространствами над конечным полем K; в данном случае срс называется *векторной*, или *линейной одномерной*, или *срс Брикелла*. Если все S_q являются векторными пространствами над конечным полем K, но не обязательно одномерными, то срс называется *линейной*. Срс Брикелла представляют особый интерес в связи с их высокой эффективностью (они идеальны и обладают простыми алгоритмами разделения и восстановления секрета). В меньшей степени это относится к линейным срс (которые могут быть неидеальными). В ещё меньшей степени это относится к срс, связанным с группами. Последние не обязаны быть идеальными и для них не известны хорошие алгоритмы разделения и восстановления секрета.

Инвариантные классы сд

Введённые ранее операции взятия миноров над сд связаны с некоторыми операциями над срс. С этой целью рассмотрим энтропийную функцию h непустого подмножества $S \subseteq A^Q$ и для подмножества $U \subseteq Q$ определим функции

$$h_{Q\setminus U}: B(Q\setminus U) \to [0,+\infty), \ h^{(U)}: B(Q) \to [0,+\infty) \text{ и } h^{Q\setminus U}: B(Q\setminus U) \to [0,+\infty),$$

положив $h_{Q\setminus U}(V) = h(V)$ для $V \subseteq Q\setminus U$, $h^{(U)}(V) = h(U \cup V)$ для $V \subseteq Q$ и $h^{Q\setminus U} = h^{(U)}{}_{Q\setminus U}$. Несложно понять, что данные функции являются энтропийными для соответствующих множеств $S_{Q\setminus U}$, S^y и $S^y{}_{Q\setminus U}$, где набор y выбран произвольно из множества S_U. В действительности, имеет место

Теорема 2. Пусть (S, P, D, h) – совершенная срс, реализующая сд G, и $Q = P \cup \{D\}$. Тогда для любого подмножества $U \subseteq P$ и любого набора y из S_U верно:

1) набор $(S_{Q\setminus U}, P\setminus U, D, h_{Q\setminus U})$ является срс, реализующей сд $G_{P\setminus U}$;
2) набор $(S^y, P\setminus U, D, h^{(U)})$ является срс, реализующей сд $G^{(U)}$;
3) набор $(S^y{}_{Q\setminus U}, P\setminus U, D, h^{Q\setminus U})$ является срс, реализующей сд $G^{P\setminus U}$.

Следствие 1. Для любого r из $[0, 1] \cup \{+\infty\}$ класс C_r всех сд, чья скорость в классе всех срс не меньше r, инвариантен. В частности, инвариантен класс всех идеальных срс.

Отметим, что инвариантность того или иного класса сд позволяет охарактеризовать этот класс посредством запрещающего множества миноров, подобно тому, как это делается для наследственных классов графов [5]. Помимо класса C_r имеются и другие важные для приложений инвариантные классы сд, такие, как классы сд, имеющих векторную (или линейную) реализацию над заданным (или произвольным) конечным полем, класс групповых сд, класс совершенных вероятностных (или комбинаторных) сд, класс сд, имеющих реализацию порядка, равного заданной величине k или 1. Очевидно, при помощи операций пересечения и объединения из перечисленных классов снова получаются инвариантные классы. Отметим ещё одно

Следствие 2. Если существует реализующая сд G срс с энтропийной функцией h, то существует реализующая G срс с энтропийной функцией H, такой, что $H(p) \le h(p)$ для любого участника p сд G и $H(p) = 0$ для любого несущественного в G участника p.

Идеальный матроид

Для заданного класса C совершенных срс, представляющих практический интерес, имеет смысл задача конструктивного описания всех сд, имеющих реализацию в классе C. В частности, данная задача имеет смысл для класса всех идеальных совершенных срс. В настоящее время данная задача не решена, а наилучшие из известных условий связаны с понятием матроида. Напомним, что *полиматроидом* на множестве Q называется пара (Q, h), где h: $B(Q)\to[0, +\infty)$ – функция, обладающая свойствами (1) – (3) из определения энтропийной функции. В частности, энтропийная функция непустого подмножества $S \subseteq A^Q$ определяет полиматроид на множестве Q. Полиматроид (Q, h) называется *матроидом*, если дополнительно выполнено свойство

1) $h(U) \in \{0, ..., |U|\}$ для любого U из $B(Q)$.

При этом элементы множества Q называются *точками* матроида. Функция h называется *ранговой* функцией матроида. Её значение $h(U)$ называется *рангом* множества $U \in B(Q)$. Множества, чья мощность совпадает с рангом, называются *независимыми*, в отличие от остальных, *зависимых* множеств матроида. Минимальные по включению зависимые множества матроида называются его *циклами*. Матроид называется *связным*, если любые две его точки попадают в некоторый цикл. Известно, что матроид однозначно определяется всеми своими циклами, проходящими через любую его заданную точку. Имеет место следующая теорема

Теорема 3 (Брикелл, Дэвенпорт). Пусть (S, P, Q, H) – идеальная совершенная срс, реализующая сд G, не имеющую несущественных участников. Пусть также $H(D) = 1$. Тогда (Q, H) – матроид, циклами которого, проходящими через точку D, являются всевозможные множества $U \cup \{D\}$, $U \in G_0$.

Замечание. Требование $H(D) = 1$ не умаляет общности теоремы. Энтропийную функцию H совершенной срс с этим свойством всегда можно найти, разделив все значения произвольной энтропийной функции h на $h(D)$, то есть положив $H = h/(h(D))$.

Вариант доказательства данной теоремы можно найти в [6]. Без доказательства данная теорема приводится в [7]. В [6, 7] можно найти ссылки на оригинальную работу Дэвенпорта и Брикелла, содержащую доказательства данной теоремы. Ещё один вариант доказательства будет приведён далее. Для доказательства понадобятся вспомогательные леммы 1 и 2.

Лемма 1. Пусть в условиях теоремы 3 $V \in B(P)\backslash G$ и множество $U \in B(P)$ минимальное по включению, для которого выполняется условие $V \cup U \in G$. Тогда $H(U, V) = H(V) + |U|$. В частности, для базисного множества $U \in G_0$ верно $H(U) = |U|$.

***Доказательство леммы* 1.** Пусть множество U n-элементное, состоит из элементов $p_1, ..., p_n$. Тогда для любого m, $1 \le m \le n$, верно: $H(V, U, D) = H(V, U) \le H(V, U\setminus\{p_m\}) + H(p_m) = H(V, U\setminus\{p_m\}) + H(D) = H(V, U\setminus\{p_m\}, D) \le H(V, U, D)$. Очевидно, что здесь везде равенства. Учитывая это и используя свойства (2) и (3) из определения энтропийной функции, получаем $H(p_m) = H(V, U) - H(V, U\setminus\{p_m\}) \le H(V, p_1, ..., p_m) - H(V, p_1, ..., p_{m-1}) \le H(p_m) = H(D) = 1$. Очевидно, что и здесь равенства. Используя их при $m = 1, ..., n$, получаем, что $H(V, p_1) = H(V) + H(D) = H(V) + 1$ и $H(V, p_1, p_2) = H(V, p_1) + H(p_2) = H(V, p_1) + 1 = H(V) + 2$, ..., $h(V, U) = h(V) + |U|$. Что и требовалось доказать.

Лемма 2. Пусть в условиях теоремы 3 $p \in U$ и $U \in G_0$. Тогда для любого $V \in B(P)$, такого, что $U \subseteq V$, верно: $H(V\setminus\{p\}, D) = H(V, D) = H(V)$.

***Доказательство леммы* 2.** Легко понять, что $H(D) + H(U\setminus\{p\}) = H(p) + H(U\setminus\{p\}) \ge H(U) = H(U, D) \ge H(U\setminus\{p\}, D) = H(U\setminus\{p\}) + H(D)$. Отсюда следует, что $H(U\setminus\{p\}, D) = H(U, D) = H(U)$. В силу третьего свойства в определении энтропийной функции H данные равенства будут выполняться и после замены U на V. Лемма доказана.

***Доказательство теоремы* 3.** Прежде всего докажем, что (Q, H) – матроид. Для этого достаточно проверить целочисленность функции H. Более того, достаточно проверить целочисленность значений $H(U)$ лишь для авторизованных в G множеств U. Это следует из того, что не авторизованное множество V можно дополнить до авторизованного множества $U = V \cup W$ минимальным по включению множеством W, тогда по лемме 1 $H(U) = H(V, W) = H(V) + |W|$ и из целочисленности $H(U)$ следует целочисленность $H(V)$. Итак, будем

доказывать для авторизованного в G множества U, что значение $H(U)$ – целое. Назовём множество U m-множеством, если $U = U_1 \cup U_2$ для некоторого m-элементного множества U_1 и для некоторого не пересекающегося с ним базисного множества U_2. Ясно, что всякое авторизованное множество является m-множеством для некоторого натурального m. Индукцией по m покажем, что $H(U)$ – целое для m-множества U. Данное утверждение является следствием леммы 1 при $m = 0$, так как 0-множествами являются базисные множества. Пусть $M > 0$, и утверждение имеет место при всех $m < M$. Докажем его при $m = M$. Рассмотрим m-множество $U = U_1 \cup U_2$, где $|U_1| = m$ и U_2 из G_0. Предположим сначала, что U_2 – единственное базисное множество, включённое в U. Тогда по лемме 1 $H(U) = H(U_1) + |U_2|$ и нужно убедиться, что $H(U_1)$ – целое. Поскольку элементы множества U_1 существенны в P, найдётся базисное множество, имеющее непустое пересечение с U_1. Выберем некоторое такое базисное множество U_3 с минимальной по включению разностью $U_3 \backslash U_1$. Тогда множество $U_1 \cup U_3$ является m'-множеством для некоторого $m' < m$ (именно для $m' = |U_1 \backslash U_3|$) и по предположению $H(U_1, U_3)$ – целое. Так как в силу минимальности U_3 по лемме 1 $H(U_1, U_3) = H(U_1) + |U_3 \backslash U_1|$, то и значение $H(U_1)$ – целое. Возвращаясь назад, заключаем, что в рассмотренном случае $H(U)$ – целое. Осталось рассмотреть случай, когда U включает отличное от U_2 базисное множество, содержащее некоторый элемент p из U_1. Так как множество $U \backslash \{p\}$ авторизовано (ибо оно включает U_2), то $H(U \backslash \{p\}, D) = H(U)$. По лемме 2 заключаем, что $H(U \backslash \{p\}) = H(U)$. Поскольку $U \backslash \{p\} = (U_1 \backslash \{p\}) \cup U_2$, множество $U \backslash \{p\}$ является $(m-1)$-множеством. По предположению индукции значение $H(U) = H(U \backslash \{p\})$ – целое. Итак, доказано, что пара (Q, H) является матроидом. Обратим своё внимание на циклы данного матроида. Прежде всего отметим, что циклами матроида являются такие множества точек, чей ранг на 1 меньше мощности и чьё любое собственное подмножество имеет ранг, совпадающий с мощностью. В силу этого для любого цикла $U \cup \{D\}$, где $D \notin U$, верно, что $|U| = H(U, D) = H(U) = H(U \backslash \{p\}, D) = H(U \backslash \{p\}) + 1$ для любого p из U. Это означает, что U – минимальное авторизованное в G, то есть принадлежит G_0. Обратно, если U из G_0, то, учитывая леммы 1 и 2, имеем $|U| = H(U) = H(U, D) = H(U \backslash \{p\}, D)$ для всех p из U. Следовательно, $U \cup \{D\}$ – цикл. Теорема доказана.

Итак, теорема 3 показывает, что энтропийная функция совершенной идеальной срс является ранговой функцией матроида. Матроиды, получающиеся таким путём, называются *идеальными*. В настоящее время известны неидеальные матроиды [7]. В [7] указывается, что матроид, отвечающий совершенной комбинаторной срс, связный.

Срс и сд Брикелла

Рассмотрим срс Брикелла над конечным полем K и реализуемые ими сд. Такие сд называются *сд Брикелла* над полем K. Установим необходимые и достаточные условия того, что заданная сд является сд Брикелла над заданным конечным полем. Итак, пусть (S, P, Q, h) – срс Брикелла над конечным полем K, реализующая сд G. Выберем в векторном пространстве S порождающий его набор R векторов $r_1, ..., r_m$, линейная оболочка $<r_1, ..., r_m>$ которых совпадает с S. Для любого q из Q через $R(q)$ обозначим набор $(r_{1q}, ..., r_{mq})$ и для любого U из $B(Q)$ через $R(U)$ обозначим множество наборов $R(q)$ для всевозможных q из U. Возникшее таким образом отображение

$$R: Q \to K^m,\ R: q \mapsto R(q)$$

называется *реализацией Брикелла* срс (S, P, Q, h) и сд G. Отметим пару свойств реализации R, имеющих место для любого подмножества U из $B(P)$.

Свойство 1. Множество U тогда и только тогда авторизовано в G, когда вектор $R(D)$ принадлежит линейной оболочке $<R(U)>$. Это следует из того, что $\operatorname{rank} S_V = \operatorname{rank} <R(V)>$ для любого V из $B(Q)$, что в свою очередь, является простой переформулировкой следующего известного свойства из [3]: строчный ранг матрицы над полем совпадает с её столбцовым рангом.

Свойство 2. Множество U тогда и только тогда не авторизовано в G, когда существует вектор $v(U)$ в K^m, такой, что $v(U) \bullet R(D) = 1$ (здесь и далее точкой обозначаем скалярное произведение) и $v(U) \bullet B(p) = 0$ для любого p из U. Действительно, в силу предыдущего свойства $U \in G \Leftrightarrow <R(D)> \subseteq <R(U)> \Leftrightarrow <R(U)>\perp \subseteq <R(D)>\perp$ (в последнем выражении речь идёт об ортогональном дополнении). Следовательно, условие $U \in G$ равносильно существованию вектора $v(U)$ в $<R(U)>\perp \backslash <R(D)>\perp$. Иными словами, вектор $v(U)$ ортогонален всем векторам $R(p)$, таким, что $p \in U$, и не ортогонален вектору $B(D)$. Очевидно, вектор $v(U)$ можно выбрать так, что $v(U) \bullet R(D) = 1$. Тем самым свойство 2 доказано. Имеет место

Теорема 4. Пусть G – сд с множеством участников P. Если G – сд Брикелла над конечным полем K, то существует пара функций

$$d: G_0 \times P \to K \text{ и } d^*: G^*_0 \times P \to K,$$

обладающих следующими свойствами:

1) $d(U, p) \neq 0$ и $d^*(V, q) \neq 0$, если $p \in U \in G_0$ и $q \in V \in G^*_0$;

2) $d(U, p) = 0$ и $d^*(V, q) = 0$, если $p \notin U \in G_0$ и $q \notin V \in G^*_0$;

3) $\Sigma d(U, p) d^*(V, p) = 1$ для любых $U \in G_0$ и $V \in G^*_0$, где суммирование ведётся в K по всевозможным p из P.

Обратно, если существуют функции d и d^*, обладающие свойствами 2) и 3), то сд G является сд Брикелла над K.

Доказательство. Необходимость. Пусть G – сд Брикелла над конечным полем K с реализацией R: $Q \to K^m$. Пусть V – множество из G^*_0. Тогда $P \setminus V$ – максимальное неавторизованное в G. В силу второго свойства существует вектор $v = v(P \setminus V)$ в K^m, такой, что $v \bullet R(D) = 1$ и $v \bullet R(p) = 0$ для любого $p \in P \setminus V$. Отметим, что в силу максимальности множества $P \setminus V$ скалярные произведения $v \bullet R(p)$ при $p \in V$ не равны нулю. Пусть также U – минимальное авторизованное в G множество из G_0. Тогда в силу первого свойства вектор $R(D)$ выражается линейно через вектора $B(p)$, где p из U, с ненулевыми (в силу минимальности U) коэффициентами. Обозначим эти коэффициенты через $d(U, p)$ так, что $B(D) = \Sigma d(U, p) R(p)$, и положим $d(U, p) = 0$ для всех p из $P \setminus U$. Тогда $1 = v \bullet R(D) = v \bullet \Sigma d(U, p) R(p) = \Sigma d(U, p)(v \bullet R(p))$. Остаётся положить $d^*(V, p) = v \bullet R(p)$. Докажем достаточность. С этой целью будем считать заданными величины $d(U, p)$ и $d^*(V, p)$, обладающие вторым и третьим свойствами. Пусть множество G^*_0 состоит из множеств $V_1, ..., V_m$. Зададим функцию R: $Q \to K^m$ так, что $R(D) = (1, ..., 1)$ и $R(p) = (d^*(V_1, p), ..., d^*(V_m, p))$ для всех p из P. Легко понять, что для любого U из G_0 вектор $R(D)$ выражается линейно через вектора $R(p)$, p из U с коэффициентами $d(U, p)$; это следует из второго и третьего свойств. Если же U – максимальное не авторизованное в G множество, то разность $P \setminus U$ совпадает с некоторым множеством V_i. Тогда всякий вектор $R(p)$, где p из U, имеет 0 в i-й координате, а значит, вектор $R(D) = (1, ..., 1)$ нельзя выразить линейной комбинацией этих векторов. Отмеченные свойства функции R говорят о том, что она является реализацией Брикелла сд G. Теорема доказана. Непосредственно из теоремы получаем

Следствие 3. Сд G на множестве P тогда и только тогда является сд Брикелла над конечным полем K, когда над этим полем относительно переменных $d(U, p)$ и $d^*(V, q)$, где $p \in U \in G_0$ и $q \in V \in G^*_0$, разрешима система уравнений $\Sigma d(U, p) d^*(V, p) = 1$ (сумма по всем p из $U \cap V$) для всевозможных значений $U \in G_0$ и $V \in G^*_0$.

В случае двухэлементного поля $K = Z_2$ получаем

Следствие 4 [10]. Сд G тогда и только тогда является сд Брикелла над полем Z_2, когда для любого множества U из G и любого множества V из G^*_0 пересечение $U \cap V$ содержит нечётное число элементов.

Данное следствие было опубликовано с доказательством в [6]. Теорема 4 является непосредственным обобщением этого результата.

Замечание. Следствие 3 сводит вопрос о существовании реализации Брикелла над полем K для заданной сд G к разрешимости над K некоторой системы уравнений. Причём, как видно из доказательства теоремы 4, решение данной системы даёт реализацию Брикелла данной сд, впрочем, возможно неэффективную (с большим m). В [9] описывается алгоритм, распознающий совместность системы полиномиальных уравнений над алгебраически замкнутым полем. В соответствии с этим алгоритмом нужно найти редуцированный базис Грёбнера идеала, порождённого системой многочленов (определяющих систему уравнений). Тогда система оказывается совместной, если редуцированный базис не состоит из одного единичного многочлена. При нахождении редуцированного базиса методом Бухбергера из [9] все вычисления происходят в кольце многочленов над фиксированным полем. В частности, если коэффициенты системы целочисленные (как в нашем случае), то все вычисления будут происходить в простом поле заданной характеристики. Это приводит ещё к одному интересному следствию.

Следствие 5. Для любого простого p существует алгоритм, распознающий для произвольной заданной сд свойство иметь реализацию Брикелла над конечным полем характеристики p.

Замечание. Отметим ещё одно свойство системы из следствия 3. Оказывается, переменные $d(U, p)$ можно выразить через переменные $d^*(V, q)$, поскольку для любого U из G_0 и p из U в G^*_0 найдётся такое V, что в системе имеется уравнение $d(U, p) d^*(V, p) = 1$. Аналогично, переменные $d^*(V, q)$ выражаются через переменные $d(U, q)$. Указанные возможности следуют из леммы 3.

Лемма 3. Для любой сд G, любого множества U из G_0 и любого p из U найдётся такое множество V в G^*_0, что $U \cap V = \{p\}$.

Доказательство. Обязательно найдётся максимальное по включению неавторизованное в G множество W, такое, что $U \setminus \{p\} \subseteq W \subseteq P \setminus \{p\}$. Так как дополнение $V = P \setminus W$ принадлежит G^*_0 и $U \cap V = \{p\}$, лемма доказана.

Нижние оценки порядка реализации

Предположим, что сд G является сд Брикелла над некоторым конечным полем K, содержащим q элементов. Представляется интересной задача нахождения наименьшего такого значения q для заданной сд G. Также имеет смысл задача нахождения нижней оценки для q. При решении данных задач может оказаться полезной следующая лемма. Далее будет показано, как этой леммой следует пользоваться.

Лемма 4. Пусть G – сд Брикелла над полем порядка q на множестве участников $P = A \cup \{a_1, ..., a_r\}$, где элементы $a_1, ..., a_r$ все различные из $P \setminus A$ и для любого i из $\{1, ..., r\}$ существует множество A_i в G_0, такое, что $a_i \in A_i$ и $A_i \subseteq A \cup \{a_1, ..., a_i\}$. Тогда для любого элемента a_0 из A число таких множеств B в G^*_0, что пересечение $B \cap (A \setminus \{a_0\})$ пусто, не превосходит q.

Доказательство. В системе уравнений из теоремы 4 в этом случае для всякого множества B из G^*_0 будут присутствовать уравнения:

$$d(A_1, a_0)d^*(B, a_0) + d(A_1, a_1)d^*(B, a_1) = 1,\ \ d(A_2, a_0)d^*(B, a_0) + d(A_2, a_1)d^*(B, a_1) + d(A_2, a_2)d^*(B, a_2) = 1, ...$$

Отсюда видно, что значение $d^*(B, a_0)$ однозначно определяет все значения $d^*(B, a)$ для всевозможных a из P и таким образом однозначно определяет само множество B. Следовательно, имеется не более q возможностей для выбора B. Лемма доказана.

Пороговая сд

Рассмотрим пример использования леммы 4.

Структура доступа G на n-элементном множестве P называется (n, k)-*пороговой*, если её базис, множество G_0, состоит из всевозможных k-элементных подмножеств множества P. Хорошо известно, что для любых целых k и n, таких, что $1 \le k \le n$, (n, k)-пороговая сд является сд Брикелла над некоторым конечным полем. Об этом можно прочитать, например, в [7, 10]. Несложно понять, что для заданных целого положительного k и целого положительного q, являющегося степенью простого числа, существует наибольшее n, при котором существует сд Брикелла над q-элементным полем, реализующая (n, k)-пороговую сд. Для такого наибольшего n положим $m(k, q) = n + 1$. Несложно понять, что $m(k, q)$ – это наибольшее число векторов в векторном пространстве над q-элементным полем, из которых любые k линейно независимы и любые $k + 1$ линейно зависимы. В некоторых случаях значение $m(k, q)$ найти несложно. Так, величина $m(1, q)$ совпадает с длиной кода Хэмминга над q-элементным полем и, следовательно, равняется $q + 1$. Определение точного вида функции $m(k, q)$ в общем случае является давней комбинаторной задачей, не решённой и по сей день [7, 11]. Предполагается, что $m(k, q) = q + 1$ за исключением случая $m(3, q) = (q - 1, q) = q + 2$ при чётном q. Следующая теорема даёт нижнюю оценку порядка реализации Брикелла для (n, k)-пороговой сд и одновременно даёт верхнюю оценку $m(k, q) \le q + k - 1$ для величины $m(k, q)$, лишь на 1 худшую, чем оценка теоремы 11 из [11].

Теорема 5. Если над q-элементным полем существует реализация Брикелла (n, k)-пороговой сд и $k \ge 2$, то $n \le q + k - 2$.

Доказательство данной теоремы опирается на лемму 4. Пусть G – (n, k)-пороговая сд на n-элементном множестве P. Тогда G_0 состоит из всевозможных k-элементных подмножеств множества P и G^*_0 состоит из всевозможных $(n - k + 1)$-элементных подмножеств. Это позволяет в условиях леммы 4 выбрать $(k–1)$-элементное множество A. Тогда, с одной стороны, число подмножеств B, о которых идёт речь в лемме, равно $n - k + 2$. С другой стороны, это число по лемме 4 не превосходит q. Таким образом получаем неравенство $n - k + 2 \le q$. Теорема доказана.

ЛИТЕРАТУРА

1. *Яблонский С.В.* О классах функций алгебры логики, допускающих простую схемную реализацию // УМН. 1957. Т. XII. Вып. 6 (78). С. 189 – 196.
2. *Алон Н.*, *Спенсер Д.Ж.* Вероятностный метод. М.: Бином. Лаборатория знаний, 2007. 320 с.
3. *Ван дер Варден Б.Л.* Алгебра. Определения, теоремы, формулы. 3-е изд., стер. – СПб.: Лань, 2004. 624 с.
4. *Каргаполов М.И.*, *Мерзляков Ю.И.* Основы теории групп. М.: Наука, 1972. 240 с.
5. *Дистель Р.* Теория графов. Новосибирск: Изд-во Ин-та математики, 2002. 336 с.
6. *Marti-Ferre J.*, *Padro C.* On secret sharing schemes, matroids and polymatroids // Cryptology ePrint Archive, Report 2006/077, http://eprint.iacr.org/2006/077.
7. *Введение* в криптографию / Под общ. ред. В.В. Ященко. 3-е изд., доп. М.: МЦНМО «ЧеРо», 2000. 288 с.
8. *Marti-Ferre J.*, *Padro C.* Secret sharing schemes on sparse homogeneous access structures with rank three // The electronic journal of combinatorics 11 (2004), Research papper 72, 16 p. (electronic).
9. *Кокс Д.*, *Литтл Дж.*, *О'Ши Д.* Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. М.: Мир, 2000. 687 с.
10. *Агибалов Г.П.* Избранные теоремы начального курса криптографии. Томск: Изд-во НТЛ, 2005. 116 с.
11. *Мак-Вильямс Ф. Дж.*, *Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.