Математика разделения секрета

Г. А. Кабатянский*

1. Введение

Рассмотрим следующую, в наше время вполне реальную ситуацию. Два совладельца драгоценности хотят положить её на хранение в сейф. Сейф современный, с цифровым замком на 16 цифр. Так как совладельцы не доверяют друг другу, то они хотят закрыть сейф таким образом, чтобы они могли открыть его вместе, но никак не порознь. Для этого они приглашают третье лицо, называемое дилером, которому они оба доверяют (например, потому что оно не получит больше доступ к сейфу). Дилер случайно выбирает 16 цифр в качестве «ключа», чтобы закрыть сейф, и затем сообщает первому совладельцу втайне от второго первые 8 цифр «ключа», а второму совладельцу втайне от первого — последние 8 цифр «ключа». Такой способ представляется с точки здравого смысла оптимальным, ведь каждый из совладельцев получил «полключа» и что может быть лучше?! Недостатком данного примера является то, что любой из совладельцев, оставшись наедине с сейфом, может за пару минут найти недостающие «полключа» с помошью несложного устройства, перебирающего ключи со скоростью 1 МГц. Кажется, что единственный выход — в увеличении размера «ключа», скажем, вдвое. Но есть другой, математический выход, опровергающий (в данном случае — к счастью) соображения здравого смысла. А именно, дилер независимо выбирает две случайные последовательности по 16 цифр в каждой, сообщает каждому из совладельцев втайне от другого «его» последовательность, а в качестве «ключа», чтобы закрыть сейф, использует последовательность, полученную сложением по модулю 10 соответствуюших цифр двух выбранных последовательностей. Довольно очевидно (и ниже мы это докажем), что для каждого из совладельцев все 10^{16} возможных «ключей» одинаково вероятны и остается только перебирать их, что потребует в среднем более полутора лет для устройства, перебирающего ключи со скоростью 100 МГц.

*Работа поддержана Российским фондом фундаментальных исследований (проект №96-01-00884).

И с математической, и с практической точки зрения неинтересно останавливаться на случае двух участников и следует рассмотреть общую ситуацию. Неформально говоря, «схема, разделяюшая секрет» (СРС) позволяет «распределить» секрет между n участниками таким образом, чтобы заранее заданные разрешённые множества участников могли однозначно восстановить секрет (совокупность этих множеств называется структурой доступа), а неразрешённые — не получали никакой дополнительной к имеющейся априорной информации о возможном значении секрета. СРС с последним свойством называются совершенными (и только они, как правило, рассматриваются в этой статье).

История СРС начинается с 1979 года, когда эта проблема была поставлена и во многом решена Г. Блейкли [1] и А. Шамиром [2] для случая пороговых (n,k)-СРС (т. е. разрешёнными множествами являются любые множества из k или более элементов). Особый интерес вызвали так называемые идеальные СРС, т. е. такие, где «размер» информации, предоставляемой участнику, не больше «размера» секрета (а меньше, как было показано, он и не может быть). Оказалось [3], что любой такой СРС соответствует матроид (определение, что это такое, см. в п. 4) и, следовательно, не для любой структуры доступа возможно идеальное разделение секрета. С другой стороны, было показано, что для любого набора разрешённых множеств можно построить совершенную СРС, однако известные построения весьма «неэкономны». В данной статье рассматриваются алгебро-геометрические и комбинаторные задачи, возникающие при математическом анализе «схем, разделяющих секрет». Вот пример одной из таких задач.

Будем говорить, что семейство линейных подпространств $\{L_0,\ldots,L_n\}$ конечномерного векторного пространства L над полем K удовлетворяет свойству «всё или ничего», если для любого множества $A\subset\{1,\ldots,n\}$ линейная оболочка подпространств $\{L_a : a\in A\}$ либо содержит подпространство L_0 целиком, либо пересекается с ним только по вектору $\mathbf{0}$. В п. 3 мы увидим, что такое семейство задаёт «линейную» СРС, у которой множество $A\subset\{1,\ldots,n\}$ является разрешённым, если и только если линейная оболочка подпространств $\{L_a : a\in A\}$ содержит подпространство L_0 целиком. В связи с этим понятием возникает ряд вопросов. Например, если поле K конечно ($|K|=q$) и все подпространства $\{L_0,\ldots,L_n\}$ одномерны, то каково максимально возможное число участников n для линейных пороговых (n,k)-СРС ($k>1$)? Иначе говоря, каково максимально возможное число векторов $\{h_0,\ldots,h_n\}$ таких, что любые k векторов, содержащие вектор h_0, линейно независимы, а любые $k+1$ векторов, содержащие вектор h_0, линейно зависимы. Оказывается, что это свойство

эквивалентно следующему, на первый взгляд более сильному, свойству: любые k векторов линейно независимы, а любые $k+1$ — линейно зависимы. Такие системы векторов изучались в геометрии как N-множества ($N = n+1$) в конечной проективной геометрии $PG(k-1, q)$, в комбинаторике как ортогональные таблицы силы k и индекса $\lambda = 1$, в теории кодирования как проверочные матрицы МДР кодов (подробнее см. [4]). В п. 3 мы приведем известную конструкцию таких множеств с $N = q+1$, а довольно старая гипотеза состоит в том, что это и есть максимально возможное N, за исключением двух случаев: случая $q < k$, когда $N = k+1$, и случая $q = 2^m$, $k = 3$ или $k = q-1$, когда $N = q+2$.

2. Разделение секрета для произвольных структур доступа

Начнем с формальной математической модели. Имеется $n+1$ множество $\mathcal{S}_0, \mathcal{S}_1, \ldots, \mathcal{S}_n$ и (совместное) распределение вероятностей P на их декартовом произведении $\mathcal{S} = \mathcal{S}_0 \times \cdots \times \mathcal{S}_n$. Соответствующие случайные величины обозначаются через S_i. Имеется также некоторое множество Γ подмножеств множества $\{1, \ldots, n\}$, называемое структурой доступа.

Определение 1. Пара $(P, \mathcal{S})$ называется *совершенной вероятностной СРС*, реализующей структуру доступа Γ, если

$$P(S_0 = c_0 | S_i = c_i, i \in A) \in \{0, 1\} \text{ для } A \in \Gamma, \tag{1}$$

$$P(S_0 = c_0 | S_i = c_i, i \in A) = P(S_0 = c_0) \text{ для } A \notin \Gamma. \tag{2}$$

Это определение можно истолковать следующим образом. Имеется множество $\mathcal{S}_0$ всех возможных секретов, из которого секрет s_0 выбирается с вероятностью $p(s_0)$, и имеется СРС, которая «распределяет» секрет s_0 между n участниками, посылая «проекции» $s_1, \ldots, s_n$ секрета с вероятностью $P_{s_0}(s_1, \ldots, s_n)$. Отметим, что i-й участник получает свою «проекцию» $s_i \in \mathcal{S}_i$ и не имеет информации о значениях других «проекций», однако знает все множества $\mathcal{S}_i$, а также оба распределения вероятностей $p(s_0)$ и $P_{s_0}(s_1, \ldots, s_n)$. Эти два распределения могут быть эквивалентно заменены на одно: $P(s_0, s_1, \ldots, s_n) = p(s_0) P_{s_0}(s_1, \ldots, s_n)$, что и было сделано выше. Цель СРС, как указывалось во введении, состоит в том, чтобы:
а) участники из разрешённого множества A (т. е. $A \in \Gamma$) вместе могли бы однозначно восстановить значение секрета — это отражено в свойстве (1);
б) участники, образующие неразрешённое множество A ($A \notin \Gamma$), не могли бы получить дополнительную информацию об s_0, т. е., чтобы вероятность того, что значение секрета $S_0 = c_0$, не зависела от значений «проекций» S_i при $i \in A$ — это свойство (2).

Замечание о терминологии. В англоязычной литературе для обозначения «порции» информации, посылаемой участнику СРС, были введены термины «share» (А. Шамир) и «shadow» (Г. Блейкли). Первый термин оказался наиболее популярным и автор долго боролся с соблазном привлечь массового читателя, постоянно используя в качестве его перевода слово «акция». Неадекватная (во всех смыслах) замена «акции» на «проекцию» может быть несколько оправдана следующим примером.

Пример 1. Множество $\mathcal{S}_0$ всех возможных секретов состоит из 0, 1 и 2, «представленных» соответственно: шаром; кубом, рёбра которого параллельны осям координат; цилиндром, образующие которого параллельны оси Z. При этом диаметры шара и основания цилиндра, и длины ребра куба и образующей цилиндра, равны. Первый участник получает в качестве своей «доли» секрета его проекцию на плоскость XY, а второй — на плоскость XZ. Ясно, что вместе они однозначно восстановят секрет, а порознь — не могут. Однако, эта СРС не является совершенной, так как любой из участников получает информацию о секрете, оставляя только два значения секрета как возможные при данной проекции (например, если проекция — квадрат, то шар невозможен).

Еще одно замечание. Элемент (участник) $x \in \{1, \ldots, n\}$ называется несущественным (относительно Γ), если для любого неразрешённого множества A множество $A \cup x$ также неразрешённое. Очевидно, что несущественные участники настолько несущественны для разделения секрета, что им просто не нужно посылать никакой информации. Поэтому далее, без ограничения общности, рассматриваются только такие структуры доступа Γ, для которых все элементы являются существенными. Кроме того, естественно предполагать, что Γ является монотонной структурой, т. е. из $A \subset B, A \in \Gamma$ следует $B \in \Gamma$.

Пример 2. Рассмотрим простейшую структуру доступа — (n, n)-пороговую схему, т. е. все участники вместе могут восстановить секрет, а любое подмножество участников не может получить дополнительной информации о секрете. Будем строить идеальную СРС, выбирая и секрет, и его проекции из группы Z_q вычетов по модулю q, т. е. $\mathcal{S}_0 = \mathcal{S}_1 = \ldots = \mathcal{S}_n = Z_q$. Дилер генерирует $n-1$ независимых равномерно распределённых на Z_q случайных величин x_i и посылает i-му участнику $(i = 1, \ldots, n-1)$ его «проекцию» $s_i = x_i$, а n-му участнику посылает $s_n = s_0 - (s_1 + \cdots + s_{n-1})$. Кажущееся «неравноправие» n-ого участника тут же исчезает, если мы выпишем распределение $P_{s_0}(s_1, \ldots, s_n)$, которое очевидно равно $1/q^{n-1}$, если $s_0 = s_1 + \cdots + s_n$, и равно 0 — в остальных случаях. Теперь легко проверяется и свойство (2), означающее в дан-

ном случае независимость случайной величины S_0 от случайных величин $\{S_i : i \in A\}$ при любом собственном подмножестве A.

Данное выше определение СРС, оперирующее словами «распределение вероятностей», ниже переведено, почти без потери общности, на комбинаторный язык, который представляется автору более простым для понимания. Произвольная $M \times (n+1)$-матрица V, строки которой имеют вид $\mathbf{v} = (v_0, v_1, \ldots, v_n)$, где $v_i \in \mathcal{S}_i$, называется матрицей комбинаторной СРС, а её строки — «правилами» распределения секрета. Для заданного значения секрета s_0 дилер СРС случайно и равновероятно выбирает строку $\mathbf{v}$ из тех строк матрицы V, для которых значение нулевой координаты равно s_0.

Определение 2. Матрица V задаёт *совершенную комбинаторную СРС*, реализующую структуру доступа Γ, если, во-первых, для любого множества $A \in \Gamma$ нулевая координата любой строки матрицы V однозначно определяется значениями её координат из множества A, и, во-вторых, для любого множества $A \notin \Gamma$ и любых заданных значений координат из множества A число строк матрицы V с данным значением α нулевой координаты не зависит от α.

Сопоставим совершенной вероятностной СРС, задаваемой парой $(P, \mathcal{S})$, матрицу V, состоящую из строк $s \in \mathcal{S}$, таких что $P(s) > 0$. Заметим, что если в определении 1 положить все ненулевые значения P одинаковыми, а условия (1) и (2) переформулировать на комбинаторном языке, то получится определение 2. Это комбинаторное определение несколько обобщается, если допустить в матрице V повторяющиеся строки, что эквивалентно вероятностному определению 1, когда значения вероятностей $P(s)$ — рациональные числа.

Пример 2 (продолжение). Переформулируем данную выше конструкцию (n, n)-пороговой СРС на комбинаторном языке. Строками матрицы V являются все векторы $\mathbf{s}$ такие, что $-s_0 + s_1 + \cdots + s_n = 0$. Очевидно, что V задаёт совершенную комбинаторную СРС для $\Gamma = \{1, \ldots, n\}$, так как для любого собственного подмножества $A \subset \{1, \ldots, n\}$ и любых заданных значений координат из множества A число строк матрицы V с данным значением нулевой координаты равно $q^{n-1-|A|}$.

Удивительно, но простой схемы примера 2 оказывается достаточно, чтобы из неё, как из кирпичиков, построить совершенную СРС для произвольной структуры доступа. А именно, для всех разрешённых множеств, т. е. для $A \in \Gamma$, независимо реализуем описанную только что пороговую $(|A|, |A|)$-СРС, послав тем самым i-му участнику столько «проекций» s_i^A,

скольким разрешённым множествам он принадлежит. Это словесное описание несложно перевести на комбинаторный язык свойств матрицы V и убедиться, что эта СРС совершенна. Как это часто бывает, «совершенная» не значит «экономная», и у данной СРС размер «проекции» оказывается, как правило, во много раз больше, чем размер секрета. Эту схему можно сделать более экономной, так как достаточно реализовать пороговые $(|A|, |A|)$-СРС только для минимальных разрешённых множеств A, т. е. для $A \in \Gamma_{\min}$, где $\Gamma_{\min}$ — совокупность минимальных (относительно включения) множеств из Γ. Тем не менее, для пороговой $(n, n/2)$-СРС размер «проекции» (измеренный, например, в битах) будет в $C_n^{n/2} \sim 2^n/\sqrt{2\pi n}$ раз больше размера секрета (это наихудший случай для рассматриваемой конструкции). С другой стороны, как мы убедимся чуть позже, любая пороговая структура доступа может быть реализована идеально, т. е. при совпадающих размерах «проекции» и секрета. Поэтому естественно возникает вопрос о том, каково максимально возможное превышение размера «проекции» над размером секрета для наихудшей структуры доступа при наилучшей реализации. Формально, $R(n) = \max R(\Gamma)$, где max берётся по всем структурам доступа Γ на n участниках, а $R(\Gamma) = \min \max \frac{\log|S_i|}{\log|S_0|}$, где min берётся по всем СРС, реализующим данную структуру доступа Γ, а max — по $i = 1, \ldots, n$. Приведенная конструкция показывает, что $R(n) \leqslant C_n^{n/2}$. С другой стороны, как было доказано лишь недавно [5], $R(n) \geqslant n/\log n$. Такая огромная «щель» между верхней и нижней оценкой даёт, по нашему мнению, достаточный простор для исследований (автор предполагает, что $R(n)$ растет экспоненциально от n).

3. Линейное разделение секрета.

Начнем с предложенной А. Шамиром [2] элегантной схемы разделения секрета для пороговых структур доступа. Пусть $K = GF(q)$ конечное поле из q элементов (например, $q = p$ — простое число и $K = Z_p$) и $q > n$. Сопоставим участникам n различных ненулевых элементов поля $\{a_1, \ldots, a_n\}$ и положим $a_0 = 0$. При распределении секрета s_0 дилер СРС генерирует $k-1$ независимых равномерно распределённых на $GF(q)$ случайных величин f_j $(j = 1, \ldots, k-1)$ и посылает i-му участнику $(i = 1, \ldots, n)$ «его» значение $s_i = f(a_i)$ многочлена $f(x) = f_0 + f_1 x + \cdots + f_{k-1}x^{k-1}$, где $f_0 = s_0$. Поскольку любой многочлен степени $k-1$ однозначно восстанавливается по его значениям в произвольных k точках (например, по интерполяционной формуле Лагранжа), то любые k участников вместе могут восстановить многочлен $f(x)$ и, следовательно, найти значение секрета как $s_0 = f(0)$. По этой же причине для любых $k-1$ участников,

любых полученных ими значений проекций s_i и любого значения секрета s_0 существует ровно один «соответствующий» им многочлен, т. е. такой, что $s_i = f(a_i)$ и $s_0 = f(0)$. Следовательно, эта схема является совершенной в соответствии с определением 2. «Линейность» данной схемы становится ясна, если записать «разделение секрета» в векторно-матричном виде:

$$\mathbf{s} = \mathbf{f}H, \tag{3}$$

где $\mathbf{s} = (s_0, \ldots, s_n), \mathbf{f} = (f_0, \ldots, f_{k-1})$, $k \times (n+1)$-матрица $H = (h_{ij}) = (a_i^{j-1})$ и $h_{00} = 1$. Заметим, что любые k столбцов этой матрицы линейно независимы, а максимально возможное число столбцов матрицы H равно q, и чтобы добиться обещанного в п. 1 значения $q+1$ надо добавить столбец, соответствующий точке «бесконечность».

Упражнение. *Придумайте сами, как это сделать.*

Возьмём в (3) в качестве H произвольную $r \times (n+1)$-матрицу с элементами из поля K. Получаемую СРС будем называть одномерной линейной СРС. Она является совершенной комбинаторной СРС со структурой доступа Γ, состоящей из множеств A таких, что вектор $\mathbf{h}_0$ представим в виде линейной комбинации векторов $\{\mathbf{h}_j : j \in A\}$, где $\mathbf{h}_j$ это j-ый столбец матрицы H. Строками матрицы V, соответствующей данной СРС являются, как видно из (3), линейные комбинации строк матрицы H. Перепишем (3) в следующем виде

$$s_j = (\mathbf{f}, \mathbf{h}_j) \text{ для } j = 0, 1, \ldots, n,$$

где $(\mathbf{f}, \mathbf{h}_j)$ — скалярное произведение векторов $\mathbf{f}$ и $\mathbf{h}_j$. Если $A \in \Gamma$, т. е. если $\mathbf{h}_0 = \sum \lambda_j \mathbf{h}_j$, то

$$s_0 = (\mathbf{f}, \mathbf{h}_0) = (\mathbf{f}, \sum \lambda_j \mathbf{h}_j) = \sum \lambda_j (\mathbf{f}, \mathbf{h}_j) = \sum \lambda_j s_j$$

и, следовательно, значение секрета однозначно находится по его «проекциям». Рассмотрим теперь случай, когда вектор $\mathbf{h}_0$ не представим в виде линейной комбинации векторов $\{\mathbf{h}_j : j \in A\}$. Нам нужно показать, что в этом случае для любых заданных значений координат из множества A число строк матрицы V с данным значением нулевой координаты не зависит от этого значения. В этом нетрудно убедиться, рассмотрев (3) как систему линейных уравнений относительно неизвестных f_i и воспользовавшись тем, что система совместна тогда и только тогда, когда ранг матрицы коэффициентов равен рангу расширенной матрицы, а число решений у совместных систем одинаково и равно числу решений однородной системы.

Указание. Рассмотрите две системы: без «нулевого» уравнения (т. е. со свободным членом) и с ним. Так как вектор $\mathbf{h}_0$ не представим в виде линейной комбинации векторов $\{\mathbf{h}_j : j \in A\}$, то ранг матрицы коэффициентов второй системы на 1 больше ранга матрицы коэффициентов первой системы. Отсюда немедленно следует, что если первая система совместна, то совместна и вторая при любом s_0.

Эта конструкция подводит нас к определению общей линейной СРС. Пусть секрет и его «проекции» представляются как конечномерные векторы $\mathbf{s}_i = (s_i^1, \ldots, s_i^{m_i})$ и генерируются по формуле $\mathbf{s}_i = \mathbf{f}H_i$, где H_i — некоторые $r \times m_i$-матрицы. Сопоставим каждой матрице H_i линейное пространство L_i её столбцов (т. е. состоящее из всех линейных комбинаций вектор-столбцов матрицы H_i). Несложные рассуждения, аналогичные приведённым выше для одномерного случая (все $m_i = 1$), показывают, что данная конструкция даёт совершенную СРС тогда и только тогда, когда семейство линейных подпространств $\{L_0, \ldots, L_n\}$ конечномерного векторного пространства K^r удовлетворяет упомянутому во введении свойству «всё или ничего». При этом множество A является разрешённым ($A \in \Gamma$), если и только если линейная оболочка подпространств $\{L_a : a \in A\}$ содержит подпространство L_0 целиком. С другой стороны, множество A является неразрешённым ($A \notin \Gamma$), если и только если линейная оболочка подпространств $\{L_a : a \in A\}$ пересекается с подпространством L_0 только по вектору $\mathbf{0}$. Отметим, что если бы для некоторого A пересечение L_0 и линейной оболочки $\{L_a : a \in A\}$ было нетривиальным, то участники A не могли бы восстановить секрет однозначно, но получали бы некоторую информацию о нем, т. е. схема не была бы совершенной.

Пример 3. Рассмотрим следующую структуру доступа для случая четырёх участников, задаваемую $\Gamma_{\min} = \{\{1,2\},\{2,3\},\{3,4\}\}$. Она известна как первый построенный пример структуры доступа, для которой не

Таб. 1.

$$H_0 = \begin{bmatrix} 1\,0 \\ 0\,1 \\ 0\,0 \\ 0\,0 \\ 0\,0 \\ 0\,0 \end{bmatrix},\ H_1 = \begin{bmatrix} 0\,0 \\ 0\,0 \\ 1\,0 \\ 0\,1 \\ 0\,0 \\ 0\,0 \end{bmatrix},\ H_2 = \begin{bmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \\ 0\,0\,0 \end{bmatrix},\ H_3 = \begin{bmatrix} 0\,0\,1 \\ 0\,0\,0 \\ 0\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \\ 1\,0\,0 \end{bmatrix},\ H_4 = \begin{bmatrix} 0\,0 \\ 0\,1 \\ 0\,0 \\ 0\,0 \\ 1\,0 \\ 0\,1 \end{bmatrix}.$$

существует идеальной реализации. Более того, было доказано, что для любой её совершенной реализации $R(\Gamma) \geqslant 3/2$. С другой стороны, непосредственная проверка показывает, что выбор матриц $H_0, H_1, \ldots, H_4$, приведенных в таб. 1, даёт совершенную линейную СРС с $R = 3/2$, реализующую эту структуру, которая, следовательно, является и оптимальной (наиболее экономной) СРС.

4. Идеальное разделение секрета и матроиды

Начнем с определения идеальных СРС. Для этого вернемся к комбинаторному определению совершенной СРС. Следующее определение совершенной СРС [3] является даже более общим, чем вероятностное определение 1, поскольку условие (2) заменено в нем на более слабое.

Для произвольного множества $B \subseteq \{0, 1, \ldots, n\}$ обозначим через V_B $M \times |B|$-матрицу, полученную из матрицы V удалением столбцов, номера которых не принадлежат множеству B. Пусть $||W||$ обозначает число различных строк в матрице W.

Определение 3. Матрица V задаёт БД-совершенную СРС, реализующую структуру доступа Γ, если

$$||V_{A\cup 0}|| = ||V_A|| \times ||V_0||^{\delta_\Gamma(A)}, \tag{4}$$

где $\delta_\Gamma(A) = 0$, если $A \in \Gamma$, и $\delta_\Gamma(A) = 1$ в противном случае.

Это определение отличается от определений 1 и 2 тем, что на неразрешённые множества A накладывается довольно слабое условие, а именно, если множество строк V с данными значениями координат из множества A непусто, то все возможные значения секрета встречаются в нулевой координате этих строк (без требований «одинаково часто» как в комбинаторном определении 2 или же «с априорной вероятностью» как в вероятностном определении 1). Легко видеть, что матрица любой совершенной вероятностной СРС задаёт БД-совершенную СРС, но обратное неверно.

Для произвольной комбинаторной СРС, задаваемой матрицей V, определим на множествах $A \subseteq \{0, 1, \ldots, n\}$ функцию $h(A) = \log_q ||V_A||$, где $q = |\mathcal{S}_0|$. Легко проверить, что $\max\{h(A), h(B)\} \leqslant h(A \cup B) \leqslant h(A) + h(B)$ для любых множеств A и B, а условие (4) может быть переписано в виде

$$h_q(V_{A\cup 0}) = h_q(V_A) + \delta_\Gamma(A) h_q(V_0),$$

Лемма. *Для любой БД-совершенной СРС если* $A \notin \Gamma$ *и* $\{A \cup i\} \in \Gamma$, *то* $h(i) \geqslant h(0)$.

Доказательство. По условиям леммы $h(A \cup 0) = h(A) + h(0)$ и $h(A \cup i \cup 0) = h(A \cup i)$. Следовательно,

$$h(A) + h(i) \geqslant h(A \cup i) = h(A \cup i \cup 0) \geqslant h(A \cup 0) = h(A) + h(0). \quad \blacksquare$$

Так как мы предполагаем, что все точки $i \in \{1, \ldots, n\}$ существенные, т. е. для любого i найдётся подмножество A такое, что $A \notin \Gamma$ и $\{A \cup i\} \in \Gamma$, то из леммы вытекает

Следствие. *Для любой БД-совершенной СРС* $|\mathcal{S}_i| \geqslant |\mathcal{S}_0|$ *для всех* $i = 1, \ldots, n$.

Следствие означает, как мы и предупреждали в начале статьи, что для совершенных СРС «размер» проекции не может быть меньше «размера» секрета. Поэтому БД-совершенная СРС называется идеальной, если $|\mathcal{S}_i| = |\mathcal{S}_0|$ для всех $i = 1, \ldots, n$.

Замечание. Неравенство $|\mathcal{S}_i| \geqslant |\mathcal{S}_0|$ справедливо и для совершенных вероятностных СРС, поскольку их матрицы задают БД-совершенные СРС.

Естественный вопрос состоит в том, для каких структур доступа Γ существуют реализующие их идеальные (вероятностные или комбинаторные) СРС. Как уже отмечалось во введении, наилучший на сегодняшний день ответ использует слово «матроид». Напомним определение матроидов и некоторые их основные свойства (см. [6]).

Матроидом называется конечное множество X и семейство I его подмножеств, называемых независимыми (остальные множества называются зависимыми), если выполнены следующие свойства:

$$\varnothing \in I; \tag{5.1}$$

$$\text{Если } A \in I \text{ и } B \subset A, \text{ то } B \in I; \tag{5.2}$$

$$\text{Если } A, B \in I \text{ и } |A| = |B| + 1,$$
$$\text{то существует } a \in A \backslash B \text{ такое, что } a \cup B \in I. \tag{5.3}$$

Пример 4. Множество X — это множество векторов в некотором линейном векторном пространстве, а независимые подмножества — это линейно независимые подмножества векторов.

Собственно с этого примера и началась теория матроидов, вначале как попытка дать аксиоматическое определение линейной независимости векторов через «внутренние свойства», т. е. не апеллируя к понятию вектора. К счастью, попытка не удалась, так как нашлись матроиды, не представимые как линейные (т. е. как системы векторов), а сама теория матроидов разрослась далеко за пределы «линейной алгебры» (см. [6]).

Пример 5 (матроид Вамоса). Рассмотрим множество $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ и положим $a = \{1,2\}$, $b = \{3,4\}$, $c = \{5,6\}$ и $d = \{7,8\}$. Матроид Вамоса определяется как матроид, в котором множества $a \cup c$, $a \cup d$, $b \cup c$, $b \cup d$, $c \cup d$, а также все подмножества из пяти или более элементов являются зависимыми. Известно, что этот матроид не является линейным.

Матроид также можно определить через так называемую ранговую функцию $r(A)$ матроида, определяемую как максимальная мощность независимого подмножества $B \subseteq A$. Очевидно, что независимые множества (и только они) задаются условием $r(A) = |A|$. Ранговая функция матроида обладает свойствами

$$r(A) \in Z,\ r(\varnothing) = 0; \tag{6.1}$$

$$r(A) \leqslant r(A \cup b) \leqslant r(A) + 1; \tag{6.2}$$

$$\text{Если } r(A \cup b) = r(A \cup c) = r(A), \text{ то } r(A \cup b \cup c) = r(A). \tag{6.3}$$

Обратно, пусть некоторая функция $r(A)$ обладает свойствами (6). Назовем независимыми те множества A, для которых $r(A) = |A|$. Тогда эти множества задают матроид, а функция r является его ранговой функцией. Возможно также определить матроид через минимальные зависимые множества, называемые циклами. Матроид называется связным, если для любых двух его точек существует содержаший их цикл.

Теперь мы можем сформулировать основной результат.

Теорема ([3]). *Для любой БД-совершенной идеальной СРС, реализующей структуру доступа* Γ, *независимые множества, определяемые условием* $\log_{|\mathcal{S}_0|} ||V_A|| = |A|$, *задают связный матроид на множестве* $\{0, 1, \ldots, n\}$. *Все циклы этого матроида, содержащие точку* 0, *имеют вид* $0 \cup A$, *где* $A \in \Gamma_{min}$.

Главным в доказательстве теоремы является «проверка» целочисленности функции $h(A)$. В самом деле, $h(\cdot)$ очевидно обладает остальными свойствами (6) и, следовательно, при условии целочисленности является ранговой функцией и задаёт матроид. Доказательство этой теоремы и несколько более общих утверждений можно найти в [7].

Отметим, что из второй части утверждения теоремы следует, что разным идеальным СРС, реализуюшим данную структуру доступа Γ, всегда соответствует один и тот же матроид, поскольку матроид однозначно определяется всеми циклами, проходящими через фиксированную точку (см. [6]). Тем самым, каждой идеально реализуемой структуре доступа соответствует однозначно определённый матроид.

В связи с теоремой возникает несколько естественных вопросов. Прежде всего, не порождают ли идеальные СРС все матроиды? Нет, например, матроид Вамоса не может быть получен как матроид идеальной СРС [8]. С другой стороны, линейные матроиды есть ни что иное как рассмотренные в п. 3 идеальные одномерные линейные СРС. В связи с этим возникает вопрос о существовании структуры доступа Г, которую невозможно реализовать в виде идеальной одномерной линейной СРС, но можно в виде идеальной многомерной линейной СРС. Недавно такой пример был построен [9], и, значит, мы можем говорить о многомерных линейных матроидах как классе матроидов более общем, чем линейные.

Итак, идеальных СРС больше, чем линейных матроидов, но меньше, чем всех матроидов. Уточнить, «насколько больше», представляется довольно сложной задачей. В частности, существует ли идеально реализуемая структура доступа Г, которую невозможно реализовать как идеальную линейную многомерную СРС?

Список литературы

[1] *Blakley G. R.* Safeguarding cryptographic keys // Proc. AFIPS 1979 National Computer Conference. V. 48. N. Y., 1979. P. 313–317.

[2] *Shamir A. How to Share a Secret* // Comm. ACM. V. 22, No 1, 1979. P. 612–613.

[3] *Brickell E. F., Davenport D. M.* On the classification of Ideal Secret Sharing Schemes. // J. Cryptology. V. 4, 1991. P. 123–134.

[4] *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки.* М.: Связь, 1979.

[5] *Csirmaz L.* The size of a share must be large // J. Cryptology. V. 10, No 4, 1997. P. 223–232.

[6] *Welsh D. J. A.* Matroid Theory. Academic Press, 1976.

[7] *Блейкли Г. Р., Кабатянский Г. А.* Обобщённые идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. Т. 33, вып. 3, 1997. С. 102–110.

[8] *Seymour P. O.* On Secret-Sharing Matroids. // J. Comb. Theory. Ser. B. V. 56, 1992. P. 69–73.

[9] *Ashihmin A., Simonis J.* Almost Affine codes. // Designs, codes and cryptography. (В печати.)