Криптография 2024

Разделение секрета

Разделение секрета

В протоколе разделения секрета имеются **n** участников $P_1,\ldots,P_n$, которых мы будем называть процессорами, и один выделенный участник **D**, называемый дилером. Протокол состоит из двух фаз:

1. На фазе разделения секрета дилер, знающий некоторый секрет **s**, генерирует **n** долей секрета $s_1,\ldots,s_n$ и посылает s_i процессору P_i по защищенному каналу связи.
2. На фазе восстановления секрета любое подмножество из не менее чем **t + 1** процессоров, где **t** - параметр протокола, однозначно восстанавливает секрет, обмениваясь сообщениями по защищенным каналам связи. А любое подмножество из не более чем **t** процессоров не может восстановить секрет.

Вопрос. Как можно защититься от нечестного дилера?

- Фаза разделения секрета начинается с того, что дилер публикует секрет **s** в «зашифрованном» виде. С помощью этой информации каждый процессор P_i может проверить, что значение s_i, полученное им от дилера, действительно является долей секрета **s**.
- Такой протокол называется протоколом проверяемого разделения секрета.
- От протокола требуется, чтобы честные участники, если их по крайней мере **t + 1**, всегда правильно восстанавливали значение **s**.

Разделение секрета

Рассмотрим конструкцию протокола, называемой схемой Шамира.

- Дилер выбирает случайный полином $\mathbf{Q(x) = a_0 + a_1x + ... + a_tx^t}$ степени **t**, где $\mathbf{a_0 = s}$
- Дилер вычисляет $\mathbf{r_i = g^{ai} (mod\ p)}$ ($\mathbf{i = 0,1,...,t}$) и публикует $\mathbf{r_0,...,r_t}$.
- Для всякого $\mathbf{j = 1,...,n}$ дилер вычисляет $\mathbf{s_j = Q(j)}$ и посылает это значение процессору $\mathbf{P_j}$ по защищенному каналу.
- Процессор $\mathbf{P_j}$, проверяя равенство $\mathbf{g^{sj} = r_0(r_1)^j...(r_t)^{j\wedge t}\ (mod\ p)}$ убеждается, что $\mathbf{s_j}$ - доля секрета **s**.($\mathbf{r_0(r_1)^j...(r_t)^{j\wedge t} = g^{a0}g^{a1j}...g^{atj\wedge t} = g^{a0+a1j+...+atj\wedge t} = g^{Q(x)}\ (mod\ p)}$)

Конструкцию протокола для фазы восстановления секрета рассмотрим в наиболее простом случае, когда дилер честный.

- Каждый процессор $\mathbf{P_j}$ посылает каждому другому процессору $\mathbf{P_i}$ свою долю $\mathbf{s_j}$.
- Всякий честный участник $\mathbf{P_i}$, получив некоторое значение $\mathbf{s_j}$ от $\mathbf{P_j}$, проверяет это значение, как описано выше, и отбрасывает все доли $\mathbf{s_j}$, не прошедшие проверку.
- Поскольку честных участников не менее $\mathbf{t + 1}$, $\mathbf{P_i}$ получит по крайней мере $\mathbf{t + 1}$ правильных долей секрета.
- Используя алгоритм восстановления секрета из схемы Шамира, $\mathbf{P_i}$ восстановит значение **s**.

Разделение секрета

Предположим, что с помощью описанной выше схемы разделены два секрета s_1 и s_2 и что оба эти секреты являются числами.

Теперь представим себе ситуацию, что после этого потребовалась разделить секрет $s = s_1 + s_2$.

Конечно, это может сделать дилер с помощью того же протокола.

А могут ли процессоры выполнить то же самое без участия дилера?

- Пусть $Q_1(x) = a_0 + a_1x + \ldots + a_tx^t$ и $Q_2(x) = b_0 + b_1x + \ldots + b_tx^t$ - полиномы, которые использовались для разделения секретов s_1 и s_2 соответственно.
- Пусть $r^1_1 = g^{ai} \pmod p$ и $r^2 = g^{bi} \pmod p$ для $i = 0,1\ldots,t$.
- Для любого $j = 1,\ldots,n$ пусть $s^1_j = Q_1(j)$ и $s^2_j = Q_2(j)$ - доли секретов s_1 и s_2, полученные процессором P_j.
- Ясно, что $Q(x) = Q_1(x) + Q_2(x)$ - также полином степени t и $Q(0) = s$.
- Поэтому каждый процессор P_j может вычислить долю s_j секрета s просто по формуле $s_j = s^1_j + s^2_j$.
- Эти доли проверяемы с помощью значений $r_i = r^1_i + r^2_i$.

Разделение секрета

Рабин и Бен-Ор показали, что процессоры могут вычислить любую функцию над конечным полем «проверяемым образом».

Области протоколов конфиденциального вычисления. Типичная задача: Требуется вычислить значение функции **f** на некотором наборе значений аргументов $y_1, \ldots, y_m$.

- С помощью схемы проверяемого разделения секрета вычисляются доли $x_1, \ldots, x_n$ этих значений.
- В начале выполнения протокола доля x_i известна процессору P_i и только ему.
- Протокол должен обеспечивать вычисление значения $f(x_1,\ldots,x_n) = f(y_1,\ldots,y_n)$ таким образом, чтобы для некоторого параметра **t**:
  - в результате выполнения протокола любое подмножество из не более чем **t** процессоров не получало никакой информации о значениях x_i других процессоров (кроме той, которая следует из известных им долей и значения функции $f(x_1,\ldots,x_n)$);
  - при любых действиях нечестных участников остальные участники вычисляют правильное значение $f(x_1,\ldots,x_n)$, если только количество нечестных участников не превосходит **t**.

Разделение секрета

Определение. Семейство подпространств $\{L_0,\dots,L_n\}$ конечномерного векторного пространства L над полем K удовлетворяет свойству «все или ничего», если для любого множества $A \subset \{1,\dots,n\}$ линейная оболочка подпространств $\{L_a: a \in A\}$ либо содержит подпространство L_0 целиком, либо пересекается с ним только по вектору 0.

Вопрос. Если поле K конечно ($|K| = q$) и все подпространства $\{L_0,\dots,L_n\}$ одномерны, то каково максимально возможное число участников n для линейных пороговых (n,k) - СРС ($k > 1$)?

Иначе говоря, каково максимально возможное число векторов $\{h_0,\dots,h_n\}$ таких, что любые k векторов, содержащие вектор h_0, линейно независимы, а любые $k + 1$ векторов, содержащие вектор h_0, линейно зависимы.

Это свойство эквивалентно следующему 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.

Гипотеза. 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 $N = q + 2$

Разделение секрета

Формальная математическая модель. Имеется **n + 1** множество $S_0,S_1,\ldots,S_n$ и (совместное) распределение вероятностей **P** на их декартовом произведении $S = S_0 \bullet \ldots \bullet S_n$. Соответствующие случайные величины обозначаются через S_i. Имеется также некоторое множество **Г** подмножеств множества **{1,…,n}**, называемое структурой доступа.

Определение 1. Пара **(P,S)** называется *совершенной вероятностной СРС*, реализующей структуру доступа **Г**, если

- $P(S_0 = c_0 \mid S_i = c_i, i \in A) \in \{0,1\}$ **для** $A \in$ **Г** (1)
- $P(S_0 = c_0 \mid S_i = c_i, i \in A) = P(S_0 = c_0)$ **для** $A \notin$ **Г** (2)

Другими словами.

- Имеется СРС, которая «распределяет» секрет s_0 между **n** участниками, посылая «проекции» $s_1,s_2,\ldots,s_n$ секрета с вероятностью $P_{s0}(s_1,\ldots,s_n)$.
- **i**-й участник получает свою «проекцию» $s_i \in S_i$ и не имеет информации о значениях других «проекций», но знает все множества S_i, а также оба распределения вероятностей $p(s_0)$ и $P_{s0}(s_1,\ldots,s_n)$.
- Эти два распределения могут быть эквивалентно заменены на одно: $P(s0,s1,\ldots,s_n) = p(s_0)\, P_{s0}(s_1,\ldots,s_n)$.
- Цель СРС состоит в том, чтобы:
  - **A** $\in$ **Г** вместе могли бы однозначно восстановить значение секрета.
  - **A** $\neq$ **Г** не могли бы получить дополнительную информацию об s_0, т.е., чтобы вероятность того, что значение секрета $S_0 = c_0$, не зависела от

Разделение секрета

Пример 1. Множество S_0 всех возможных секретов состоит из 0, 1 и 2, «представленных» соответственно:

- шаром
- кубом, ребра 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.

1. Первый участник получает в качестве своей «доли» секрета его проекцию на плоскость XY.
2. 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).

Разделение секрета

Замечание. Элемент (участник) $x \in \{1,\dots,n\}$ называется несущественным(относительно Г), если для любого неразрешенного множества **A** множество $A \cup x$ также неразрешенное.

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 **Г**, для которых все элементы являются существенными. Кроме того, естественно предполагать, что **Г** является монотонной структурой, т.е. из $A \subset B$, $A \in Г$ следует $B \in Г$.

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.

- Выбираем секрет, и его проекции из группы $\mathbb{Z}_q$, т.е. $S_0 = S_1 = \dots = S_n = \mathbb{Z}_q$.
- Дилер генерирует $n - 1$ независимых равномерно распределенных на $\mathbb{Z}_q$ случайных величин x_i и посылает i-му участнику $s_i = x_i$, а n-му участнику посылает $s_n = s_0 - (s_1 + \dots + s_{n-1})$.
- Выпишем распределение $P_{s0}(s_1,\dots,s_n)$, которое очевидно равно $1/q^{n-1}$, если $s_0 = s_1 + \dots + s_n$, и равно 0 - в остальных случаях.
- Легко проверяется и свойство (2), означающее в данном случае независимость случайной величины S_0 от случайных величин $\{S_i : i \in A\}$ при любом собственном подмножестве **A**.

Разделение секрета

Комбинаторный вариант. Произвольная **M•(n + 1)** - матрица **V**, строки которой имеют вид $\mathbf{v = (v_0,v_1,\ldots,v_n)}$, где $\mathbf{v_i \in S_i}$, называется матрицей комбинаторной СРС, а ее строки – «правилами» распределения секрета. Для заданного значения секрета $\mathbf{s_0}$ дилер СРС случайно и равновероятно выбирает строку **v** из тех строк матрицы **V**, для которых значение нулевой координаты равно $\mathbf{s_0}$.

Определение 2. Матрица **V** задает *совершенную комбинаторную СРС*, реализующую структуру доступа **Г**, если

1. Для любого множества $\mathbf{A \in Г}$ нулевая координата любой строки матрицы **V** однозначно определяется значениями ее координат из множества **A**.
2. Для любого множества $\mathbf{A \notin Г}$ 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,S)**, матрицу **V**, состоящую из строк $\mathbf{s \in S}$, 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.

Разделение секрета

Пример 2. (продолжение) Переформулируем данную выше конструкцию **(n,n)**-пороговой СРС на комбинаторном языке.

- Строками матрицы **V** являются все векторы **s** такие, что $-s_0 + s_1 + \ldots + s_n = 0$.
- Матрица **V** задает 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 $q^{n-1-|A|}$.

Простой схемы примера 2 оказывается достаточно, чтобы из нее построить совершенную СРС для произвольной структуры доступа.

- Для всех разрешенных 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 разрешенным множествам он принадлежит.

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 разрешенных множеств **A**, т.е. для $A \in \Gamma_{min}$, где Γ_{min} - совокупность минимальных (относительно включения) множеств из Γ.

Тем не менее, для пороговой **(n,n/2)** - СРС размер «проекции» будет в $C_n^{n/2} \sim 2^n/\sqrt{(2\pi n)}$ раз больше размера секрета (это наихудший случай для рассматриваемой конструкции).

Разделение секрета

Вопрос. Каково максимально возможное превышение размера «проекции» над размером секрета для наихудшей структуры доступа при наилучшей реализации.

Формально, **R(n) = max R(Г)**, где **max** берется по всем структурам доступа **Г** на **n** участниках, а **R(Г) = min max(log(|S_i|)/log(|S_0|))**, где **min** берется по всем СРС, реализующим данную структуру доступа **Г**, а **max** - по **i = 1,…,n**.

Приведенная конструкция показывает, что **R(n) ≤ $C_n^{n/2}$**.

С другой стороны доказано, что **R(n) ≥ n/log(n)**.

Такая огромная «щель» между верхней и нижней оценкой дает, по нашему мнению, достаточный простор для исследований.

Криптография 2024

Линейное разделение секрета

Линейное разделение секрета

Схема Шамира. Пусть $K = GF(q)$ конечное поле из $q > n$ элементов. Сопоставим участникам n различных ненулевых элементов поля $\{a_1, \dots, a_n\}$ и положим $a_0 = 0$.

- Дилер генерирует $k-1$ независимых равномерно распределенных на K случайных величин f_j $(j = 1, \dots, k-1)$ и посылает i -му участнику значение $s_i = f(a_i)$ многочлена $f(x) = f_0 + f_1 x + \cdots + f_{k-1} x^{k-1}$, где $f_0 = s_0$.
- Любые k участников вместе могут восстановить многочлен $f(x)$ и найти значение секрета как $s_0 = f(0)$.
- 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.
- Запишем систему в векторно-матричном виде: $s = fH$, где $s = (s_0, \dots, s_n), f = (f_0, \dots, f_{k-1}), H = (h_{ij}) = (a_i^{j-1})$ и $h_{00} = 1$.
  - Любые k столбцов этой матрицы линейно независимы
  - Максимально возможное число столбцов матрицы H равно q

Линейное разделение секрета

Определение. Пусть H произвольная $r\times(n+1)$ -матрицу с элементами из поля K. Соответствующую СРС будем называть одномерной линейной СРС.

- ОЛСРС является совершенной комбинаторной СРС со структурой доступа Γ, состоящей из множеств A таких, что вектор h_0 представим в виде линейной комбинации векторов $\{h_j: j \in A\}$, где h_j это j-ый столбец матрицы H.
- Строками матрицы V, соответствующей данной СРС являются линейные комбинации строк матрицы H.
- Перепишем $s = fH$ как $s_j = (f, h_j)$, где (f, h_j) - скалярное произведение векторов f и h_i.
  - Если $A \in \Gamma\ (h_0 = \sum \lambda_j h_j)$, то $s_0 = (f, h_0) = (f, \sum \lambda_j h_j) = \sum \lambda_j (f, h_j) = \sum \lambda_j s_j$ и, следовательно, значение секрета однозначно находится по его «проекциям».
  - Пусть h_0 не представим в виде линейной комбинации векторов $\{h_j: j \in A\}$. 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. (Указание: нужно рассмотреть $s = fH$ как систему линейных уравнений относительно неизвестных f_i).

Линейное разделение секрета

Определение. Общая линейная СРС.

- Пусть секрет и его «проекции» представляются как конечномерные векторы $s_i = (s_i^1, \dots, s_i^{m_i})$ и генерируются по формуле $s_i = fH_i$, где H_i - некоторые $r \times m_i$-матрицы.
- Сопоставим каждой матрице H_i линейное пространство L_i ее столбцов.
- Легко доказать, что данная конструкция дает совершенную СРС тогда и только тогда, когда семейство линейных подпространств $\{L_0, \dots, L_n\}$ конечномерного векторного пространства K^r удовлетворяет свойству «все или ничего».
- При этом множество $\mathbf{A}$ является разрешенным ($\mathbf{A} \in \Gamma$), если и только если линейная оболочка $\{L_a : a \in A\}$ содержит подпространство L_0 целиком.
- Множество $\mathbf{A}$ является неразрешенным ($\mathbf{A} \notin \Gamma$), если и только если линейная оболочка $\{L_a : a \in A\}$ пересекается с подпространством L_0 только по вектору 0.
- Если бы для некоторого $\mathbf{A}$ пересечение L_0 и линейной оболочки $\{L_a : a \in A\}$ было нетривиальным, то участники $\mathbf{A}$ не могли бы восстановить секрет однозначно, но получали бы некоторую информацию о нем, т.е. схема не была бы совершенной.

Линейное разделение секрета

Пример 3.

- Рассмотрим следующую структуру доступа для случая четырех участников, задаваемую $\boldsymbol{\Gamma_{min}} = \{\{\mathbf{1},\mathbf{2}\},\{\mathbf{2},\mathbf{3}\},\{\mathbf{3},\mathbf{4}\}\}$.
- Она известна как первый построенный пример структуры доступа, для которой не существует идеальной реализации.
- Для любой ее совершенной реализации $\boldsymbol{R(\Gamma)} \geq \mathbf{3/2}$.
- С другой стороны, непосредственная проверка показывает, что выбор матриц $\boldsymbol{H_0, H_1, \ldots, H_4}$, приведенных в табл. 1, дает совершенную линейную СРС с $\boldsymbol{R = 3/2}$, реализующую эту структуру, которая, следовательно, является и оптимальной СРС.

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

Криптография 2024

Идеальное разделение секрета и матроиды

Идеальное разделение секрета и матроиды

Для произвольного множества $B \subset \{0, 1, \dots, n\}$ 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 задает БД-совершенную СРС, реализующую структуру доступа Γ, если $\|V_{A \cup 0}\| = \|V_A\| \times \|V_0\|^{\delta_\Gamma(A)}$, где $\delta_\Gamma(A) = 0$, если $A \in \Gamma$, и $\delta_\Gamma(A) = 1$ в противном случае.

Это определение отличается от предыдущих определений тем, что на неразрешенные 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 или же «с априорной вероятностью» как в вероятностном определении).

Легко видеть, что матрица любой совершенной вероятностной СРС задает БД-совершенную СРС, но обратное неверно.

Идеальное разделение секрета и матроиды

Для комбинаторной СРС, задаваемой матрицей $\boldsymbol{V}$, определим на множествах $\boldsymbol{A} \subseteq \{\boldsymbol{0}, \boldsymbol{1}, \dots, \boldsymbol{n}\}$ функцию $\boldsymbol{h(A)} = \boldsymbol{log_a}\|\boldsymbol{V_A}\|$,где $\boldsymbol{a} = |\boldsymbol{S_0}|$. Легко проверить, что

$$\boldsymbol{max}\{\boldsymbol{h(A)}, \boldsymbol{h(B)}\} \leq \boldsymbol{h(A \cup B)} \leq \boldsymbol{h(A)} + \boldsymbol{h(B)}$$

для любых множеств $\boldsymbol{A}$ и $\boldsymbol{B}$, а условие $\|\boldsymbol{V_{A\cup 0}}\| = \|\boldsymbol{V_A}\| \times \|\boldsymbol{V_0}\|^{\boldsymbol{\delta_\Gamma(A)}}$ может быть переписано в виде $\boldsymbol{h_q(V_{A\cup 0})} = \boldsymbol{h_q(V_A)} + \boldsymbol{\delta_\Gamma(A)h_q(V_0)}$.

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

Доказательство. По условиям леммы

$$\boldsymbol{h(A \cup 0)} = \boldsymbol{h(A)} + \boldsymbol{h(0)} \text{ и } \boldsymbol{h(A \cup i \cup 0)} = \boldsymbol{h(A \cup i)}.$$

Следовательно,

$$\boldsymbol{h(A)} + \boldsymbol{h(i)} \geq \boldsymbol{h(A \cup i)} = \boldsymbol{h(A \cup i \cup 0)} \geq \boldsymbol{h(A \cup 0)} = \boldsymbol{h(A)} + \boldsymbol{h(0)}.$$

Мы предполагаем, что все точки $\boldsymbol{i} \in \{\boldsymbol{1}, \dots, \boldsymbol{n}\}$ существенные.

Следствие . Для БД-совершенной СРС $|\boldsymbol{S_i}| \geq |\boldsymbol{S_0}| \; \forall \; \boldsymbol{i} = \boldsymbol{1}, \dots, \boldsymbol{n}$.

Определение. БД-совершенная СРС называется идеальной, если $|\boldsymbol{S_i}| = |\boldsymbol{S_0}|$ для всех $\boldsymbol{i} = \boldsymbol{1}, \dots, \boldsymbol{n}$.

Замечание . Неравенство $|\boldsymbol{S_i}| \geq |\boldsymbol{S_0}|$ справедливо и для совершенных вероятностных СРС, поскольку их матрицы задают БД-совершенные СРС.

Идеальное разделение секрета и матроиды

Определение. Матроидом называется конечное множество $\boldsymbol{X}$ и семейство $\boldsymbol{I}$ его подмножеств, называемых независимыми (остальные множества называются зависимыми), если выполнены следующие свойства:

- $\emptyset \in \boldsymbol{I}$
- Если $\boldsymbol{A} \in \boldsymbol{I}$ и $\boldsymbol{B} \subset \boldsymbol{A}$, то $\boldsymbol{B} \in \boldsymbol{I}$
- Если $\boldsymbol{A}, \boldsymbol{B} \in \boldsymbol{I}$ и $|\boldsymbol{A}| = |\boldsymbol{B}| + \boldsymbol{1}$, то $\exists \boldsymbol{a} \in \boldsymbol{A} \backslash \boldsymbol{B}$ такое, что $\boldsymbol{a} \cup \boldsymbol{B} \in \boldsymbol{I}$

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

Определение. Ранговая функция $\boldsymbol{r}(\boldsymbol{A})$ матроида – максимальная мощность независимого подмножества $\boldsymbol{B} \subseteq \boldsymbol{A}$.

Очевидно, что независимые множества (и только они) задаются условием $\boldsymbol{r}(\boldsymbol{A}) = |\boldsymbol{A}|$.

Идеальное разделение секрета и матроиды

Ранговая функция матроида обладает свойствами

- $r(A) \in Z, r(\emptyset) = 0$
- $r(A) \leq r(A \cup b) \leq r(A) + 1$
- Если $r(A \cup b) = r(A \cup c) = r(A)$, то $r(A \cup b \cup c) = r(A)$.

Определение. Пусть некоторая функция $r(A)$ обладает перечисленными свойствами (6). Назовем независимыми те множества A, для которых $r(A) = |A|$.

Тогда эти множества задают матроид, а функция r является его ранговой функцией.

Определение. Минимальные зависимые множества, называются циклами.

Возможно также определить матроид через циклы.

Определение. Матроид называется связным, если для любых двух его точек существует содержащий их цикл.

Идеальное разделение секрета и матроиды

Теорема. Для любой БД-совершенной идеальной СРС, реализующей структуру доступа $\boldsymbol{\Gamma}$, независимые множества, определяемые условием $\boldsymbol{log_{|S_0|}\|V_A\| = |A|}$, задают связный матроид на множестве $\{\mathbf{0}, \mathbf{1}, \dots, \boldsymbol{n}\}$. Все циклы этого матроида, содержащие точку 0, имеют вид $\mathbf{0} \cup \boldsymbol{A}$, где $\boldsymbol{A} \in \boldsymbol{\Gamma_{min}}$.

Линейные матроиды есть ни что иное как идеальные одномерные линейные СРС.

Вопрос. Существует ли структура доступа $\boldsymbol{\Gamma}$, которую невозможно реализовать в виде идеальной одномерной линейной СРС, но можно в виде идеальной многомерной линейной СРС.

Такой пример был построен, значит, мы можем говорить о многомерных линейных матроидах как классе матроидов более общем, чем линейные.

Вывод. Идеальных СРС больше, чем линейных матроидов, но меньше, чем всех матроидов.