Математика разделенного секрета: Пороговые (n,k)-схемы доступа, схема Шамира и схема Блэкли

Носов Андрей БПИ-232

Схема разделения секрета

Пусть есть секрет и группа людей, между которыми нужно распределить этот секрет. Задача состоит в следующем. Нужно придумать, какую информацию предоставить каждому человеку, чтобы только «разрешенные» подгруппы могли восстановить секрет.

Определение

Схема разделения секрета (СРС) *— способ распределения секрета среди группы участников, в котором*

- *каждому из участников достается своя некая* ***доля****;*
- *только разрешенные подмножества группы участников могут восстановить секрет.*

Участники и дилер

Определение

В СРС выделяются следующие роли:

- ***Дилер*** *— доверенное лицо, которое*
    - *Знает секрет* s_0;
    - *Вычисляет* n *долей* $s_1, s_2, \ldots, s_n$;
    - *Передает доли участникам.*
- ***Участники*** *— лица, получающие доли секрета. Они объединяются для восстановления секрета.*

Математическая модель

Зададим модель СРС следующим набором:

- Множества $S_0, S_1, \ldots, S_n$.
  S_0 — множество секретов.
  S_i $(i = \overline{1, n})$ — множество долей i-го участника.
- Распределение вероятностей P на их декартовом произведении $S = S_0 \times S_1 \times \cdots \times S_n$.
  Соответствующие случайные величины обозначим ξ_i.
- Множество $\mathcal{A} \subseteq 2^{\underline{n}}$, называемое структурой доступа.
  Тогда любое множество $A \in \mathcal{A}$ задает разрешенное подмножество группы участников.

Замечания

Определение

Участник $x \in \{1, \ldots, n\}$ *называется* **несущественным** *для структуры доступа* $\mathcal{A}$, *если*

- $\forall A \notin \mathcal{A} \Longrightarrow A \cup x \notin \mathcal{A}$.

Замечание

Очевидно, что несущественные участники настолько несущественны для разделения секрета, что им просто не нужно посылать никакой информации. Поэтому можно рассматривать только такие структуры доступа $\mathcal{A}$, *для которых все элементы являются существенными.*

Замечание

Естественно полагать, что $\mathcal{A}$ *является монотонной структурой, т. е.*

$$\left.\begin{array}{l} A \subseteq B \\ A \in \mathcal{A} \end{array}\right\} \Longrightarrow B \in \mathcal{A}$$

Функции разделения и восстановления секрета

В такой математической модели можно легко задать функции разделения и восстановления секрета.

Определение

Функция разделения:

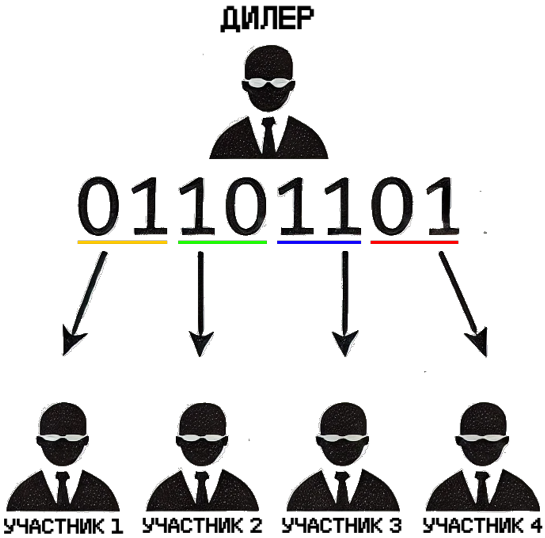
$$Share: \; S_0 \to (S_1 \times \cdots \times S_n)$$

Определение

Функция восстановления:

$$Reconstruct: \; (S_{i_1} \times \cdots \times S_{i_m}) \to S_0$$

Примитивная идея



Совершенная СРС

Определение

СРС, реализующая структуру доступа $\mathcal{A}$, называется ***совершенной****, если*

- $P(\xi_0 = x \,|\, \xi_i = s_i, i \in A) \in \{0, 1\}$ *для* $A \in \mathcal{A}$
- $P(\xi_0 = x \,|\, \xi_i = s_i, i \in A) = P(\xi_0 = x)$ *для* $A \notin \mathcal{A}$

Это определение можно понять следующим образом:

- участники из разрешенного множества A ($A \in \mathcal{A}$) вместе могут однозначно восстановить значение секрета;
- участники, образующие неразрешенное множество A ($A \notin \mathcal{A}$),не получают никакой дополнительной информации о секрете. Т. е. вероятность того, что значение секрета $\xi_0 = x$, не зависит от значений долей $\xi_i, i \in A$.

Особый интерес с точки зрения безопасности вызывают СРС, обладающие данным свойством. Поэтому далее будем рассматривать только их.

Идеальная СРС

Определение

Идеальная СРС *— это схема, в которой доля каждого участника имеет тот же размер, что и секрет:*

$$|S_i| = |S_0|, \ \forall i = \overline{1, n}$$

Простейшая структура доступа

Рассмотрим такую СРС, что только все участники вместе могут восстановить секрет, т. е. $\mathcal{A} = \{\{1, \ldots, n\}\}$.
Пусть $S_0 = S_1 = \cdots = S_n = \mathbb{Z}_p$.

- Share:
  Дилер генерирует значения долей для первых $n-1$ участников: $s_1, \ldots, s_{n-1}$.
  s_n вычисляется: $s_n = s_0 - s_1 - \cdots - s_{n-1}$.
- Reconstruct:
  $s_0 = s_1 + \cdots + s_{n-1} + s_n$

Простейшая структура доступа

Утверждение

Описанная СРС является идеальной и совершенной.

Доказательство: Идеальность очевидна, т. к. $S_0 = S_1 = \dots = S_n = \mathbb{Z}_p$
Докажем совершенность. Нужно:

- $P(\xi_0 = x \mid \xi_1 = s_1,\ \xi_2 = s_2, \dots, \xi_n = s_n) \in \{0, 1\}$
- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \dots, \xi_{i_k} = s_{i_k}) = P(\xi_0 = X)$ при $k < n$

Простейшая структура доступа

- $P(\xi_0 = x \,|\, \xi_1 = s_1,\ \xi_2 = s_2, \ldots, \xi_n = s_n) \in \{0, 1\}$

Доказательство:

$$P(\xi_0 = x \,|\, \xi_1 = s_1,\ \xi_2 = s_2, \ldots, \xi_n = s_n) =$$

$$= P(\xi_0 = x \,|\, \xi_1 = s_1,\ \xi_2 = s_2, \ldots, \xi_0 - \xi_1 - \cdots - \xi_{n-1} = s_n) =$$

$$= P(x - s_1 - \cdots - s_{n-1} = s_n) = P(x = s_1 + \cdots + s_n)$$

Если $s_1 + \cdots + s_n = x$, то $P = 1$;
Если $s_1 + \cdots + s_n \neq x$, то $P = 0$.

Простейшая структура доступа

- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_k} = s_{i_k}) = P(\xi_0 = x)$ при $k < n$

Доказательство: Для этого докажем, что $P(\xi_i = x) = \frac{1}{p}, \ \forall i = \overline{0, n}$.
Очевидно, что $P(\xi_i = x) = \frac{1}{p}, \ \forall i = \overline{0, n-1}$.
Для ξ_n:

$$P(\xi_n = x) = P(\xi_0 - \xi_1 - \cdots - \xi_n = x) = P(\xi_0 = \xi_1 + \cdots + \xi_{n-1} + x) =$$

$$= \sum_{s_i \in \mathbb{Z}_p} P(\xi_1 = s_1, \ldots, \xi_{n-1} = s_{n-1}, \ \xi_0 = s_1 + \cdots + s_{n-1} + x) =$$

$$= \sum_{s_i \in \mathbb{Z}_p} P(\xi_1 = s_1, \ldots, \xi_{n-1} = s_{n-1}) P(\xi_0 = s_1 + \cdots + s_{n-1} + x) =$$

$$= \frac{1}{p} \sum_{s_i \in \mathbb{Z}_p} P(\xi_1 = s_1, \ldots, \xi_{n-1} = s_{n-1}) = \frac{1}{p} \cdot 1 = \frac{1}{p}$$

Простейшая структура доступа

Теперь нужно доказать, что $\forall i = \overline{1, n}$ $\xi_0, \xi_1, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_n$ независимы в совокупности.

Очевидно, что $\xi_0, \xi_1, \ldots, \xi_{n-1}$ независимы по построению.

Необходимо доказать, что $\forall i = \overline{1, n-1}$ $\xi_0, \xi_1, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_n$ независимы.

$$P(\xi_0 = s_0, \xi_1 = s_1, \ldots, \xi_{i-1} = s_{i-1}, \xi_{i+1} = s_{i+1}, \ldots, \xi_n = s_n) =$$

$$= P(\ldots, \xi_0 - \xi_1 - \cdots - \xi_{i-1} - \xi_i - \xi_{i+1} - \cdots - \xi_{n-1} = s_n) =$$

$$= P(\ldots, s_0 - s_1 - \cdots - s_{i-1} - \xi_i - s_{i+1} - \cdots - s_{n-1} = s_n) =$$

$$= P(\ldots, \xi_i = s_0 - s_1 - \cdots - s_{i-1} - s_{i+1} - \cdots - s_n) = \left(\frac{1}{p}\right)^n =$$

$$= P(\xi_0 = s_0)P(\xi_1 = s_1)\ldots P(\xi_{i-1} = s_{i-1})P(\xi_{i+1} = s_{i+1})\ldots P(\xi_n = s_n)$$

Простейшая структура доступа

Так как $\forall i = \overline{1, n}$ $\xi_0, \xi_1, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_n$ независимы, то при $k < n$

$$P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_k} = s_{i_k}) = P(\xi_0 = x)$$

(n,k)-пороговая СРС

Определение

(n, k)-пороговая схема разделения секрета:

- *n участников;*
- $\mathcal{A} = \{K \subseteq \{1, \ldots, n\} \mid |K| \geq k\}$.

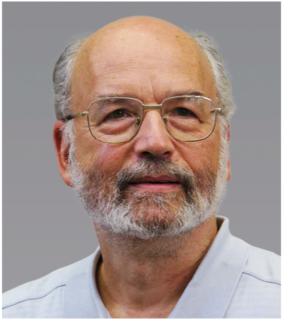
То есть любые k участников, собравшись вместе, могут восстановить секрет, а любые $k - 1$ участников не получат никакой дополнительной информации о секрете.

Замечание

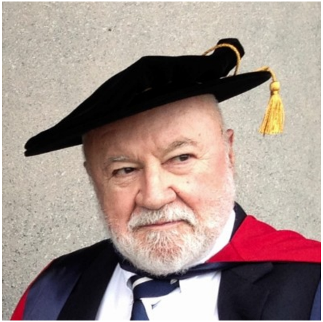
Описанная ранее простейшая структура доступа соответствует (n, n)-пороговой СРС.

Начало

- История СРС начинается с 1979 года, когда Ади Шамир и Джордж Блэкли независимо друг от друга предложили методы того, как составлять (n,k)-пороговые СРС.



Ади Шамир



Джордж Блэкли

Схема Шамира

Ади Шамир предложил следующую СРС.
Сопоставим участникам n различных чисел $x_1, \ldots, x_n \in \mathbb{F}_q$ и положим $x_0 = 0$.

- Share:
  Дилер генерирует $k-1$ чисел $a_i, i = \overline{1, k-1}$. a_0 полагается равным s_0. Составляет многочлен:
  $$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$$
  И посылает i-му участнику его долю $s_i = f(x_i)$.
- Reconstruct:
  Любые k участников собираются вместе и по k точкам восстанавливают многочлен $f(x)$, т. к. $\deg(f) = k-1$.
  Например, через интерполяционный многочлен Лагранжа или через решение СЛАУ.
  Затем находят $s_0 = f(0)$.

Схема Шамира

Визуализация для $k = 4$:

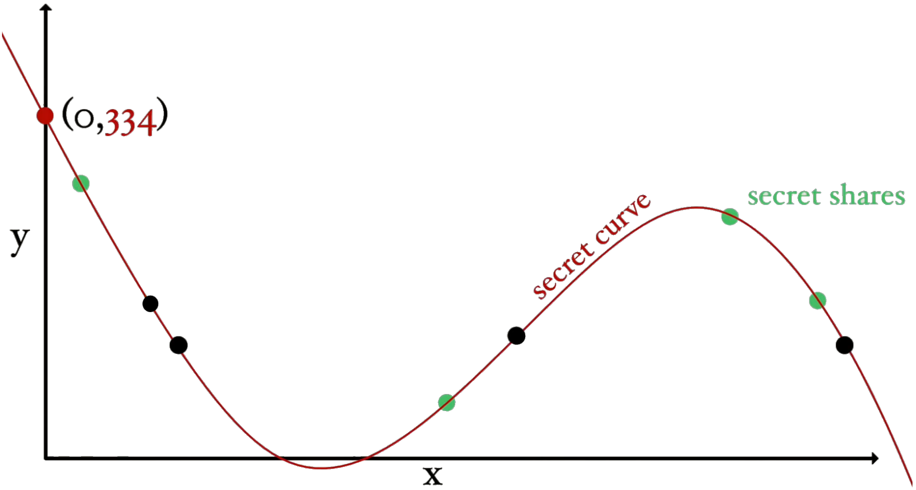


Схема Шамира. Пример

Интерполяционный многочлен Лагранжа степени не больше n по $n+1$ точкам:

$$L_n(x) = \sum_{i=0}^{n} y_i \left(\prod_{j=0, j\neq i}^{n} \frac{x - x_j}{x_i - x_j} \right)$$

Пример восстановления секрета:
Реализована $(n, 3)$-пороговая СРС Шамира.
Алисе соответсвует число 1, Бобу — 2, Еве — 3.
Доля Алисы — 2, доля Боба — 3, доля Евы — 5.
Восстановление многочлена:

$$L_2(x) = 2 \cdot \frac{x-2}{1-2} \cdot \frac{x-3}{1-3} + 3 \cdot \frac{x-1}{2-1} \cdot \frac{x-3}{2-3} + 5 \cdot \frac{x-1}{3-1} \cdot \frac{x-2}{3-2}$$

Найдем секрет:

$$L_2(0) = 2 \cdot \frac{-2}{-1} \cdot \frac{-3}{-2} + 3 \cdot \frac{-1}{1} \cdot \frac{-3}{-1} + 5 \cdot \frac{-1}{2} \cdot \frac{-2}{1} = 2$$

Схема Шамира

Утверждение

Схема Шамира является идеальной СРС.

Доказательство: $\forall i = \overline{1, n}\ |S_i| = |\mathbb{F}_q| = |S_0|$.

Схема Шамира

Утверждение

Схема Шамира является совершенной СРС.

Доказательство: Нужно

- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_k} = s_{i_k}) \in \{0, 1\}$;
- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_t} = s_{i_t}) = P(\xi_0 = x)$ при $t < k$.

Схема Шамира

- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_k} = s_{i_k}) \in \{0, 1\}$

Запишем систему уравнений относительно неизвестных $a_0, \ldots, a_{k-1}$:

$$\begin{cases} s_{i_1} = a_0 + a_1 x_{i_1} + \cdots + a_{k-1} x_{i_1}^{k-1} \\ \vdots \\ s_{i_k} = a_0 + a_1 x_{i_k} + \cdots + a_{k-1} x_{i_k}^{k-1} \end{cases}$$

Перепишем в матричном виде:

$$\begin{pmatrix} s_{i_1} \\ \vdots \\ s_{i_k} \end{pmatrix} = \begin{pmatrix} 1 & x_{i_1} & \ldots & x_{i_1}^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_k} & \ldots & x_{i_k}^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix}$$

- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \dots, \xi_{i_k} = s_{i_k}) \in \{0, 1\}$

$$\begin{pmatrix} s_{i_1} \\ \vdots \\ s_{i_k} \end{pmatrix} = \begin{pmatrix} 1 & x_{i_1} & \dots & x_{i_1}^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_k} & \dots & x_{i_k}^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix}$$

Определитель матрицы Вандермонда не равен 0 $\Longrightarrow$ есть единственное решение $\Longrightarrow$ можем найти это единственной решение $(a_0, \dots, a_{k-1})^T \Longrightarrow$ можем найти секрет $s_0 = a_0$.
Тогда для рассматриваемой вероятности будет верно:

$$P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \dots, \xi_{i_k} = s_{i_k}) = P(\xi_0 = x \mid \xi_0 = s_0) =$$

$$= P(x = s_0) \in \{0, 1\}$$

Схема Шамира

- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_t} = s_{i_t}) = P(\xi_0 = x)$ при $t < k$.

Докажем, что $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_{k-1}} = s_{i_{k-1}}) = P(\xi_0 = x)$.

Зная $k-1$ точек $(x_{i_1}, s_{i_1}), \ldots, (x_{i_{k-1}}, s_{i_{k-1}})$, через которые проходит многочлен $f(x)$ степени $k-1$, можно для каждого значения секрета $s_0 = f(0)$ построить ровно один многочлен $f(x)$.
Значит даже зная, что $\xi_{i_j} = s_{i_j}$, СВ ξ_0 распределена равномерно на всем поле $\mathbb{F}_q$.

Схема Блэкли

Джордж Блэкли предложил следующую СРС.

- Share: Дилер генерирует $k-1$ число $b_1, \ldots, b_{k-1} \in \mathbb{F}_q$ и задает точку в k-мерном пространстве с координатами $(s_0, b_1, \ldots, b_{k-1})$. Для каждого участника он составляет уравнение гиперплоскости, которая проходит через заданную точку. Для этого дилер для i-го участника генерирует k чисел $a_{i_1}, \ldots, a_{i_k} \in \mathbb{F}_q$. Так как уравнение плоскости имеет вид $a_{i_1}x_1 + a_{i_2}x_2 + \cdots + a_{i_k}x_k + d_i = 0$, то для каждого участника необходимо еще вычислить d_i:

$$\begin{gathered} d_1 = -(a_{1_1}s_0 + a_{1_2}b_1 + \cdots + a_{1_k}b_{k-1}) \\ \vdots \\ d_i = -(a_{i_1}s_0 + a_{i_2}b_1 + \cdots + a_{i_k}b_{k-1}) \\ \vdots \\ d_n = -(a_{n_1}s_0 + a_{n_2}b_1 + \cdots + a_{n_k}b_{k-1}) \end{gathered}$$

Доля i-го участника задается вектором $s_i = (a_{i_1}, \ldots, a_{i_k}, d_i)$.

- Reconstruct:
  Любые k участников собираются вместе и по уравнениям k плоскостей однозначно восстанавливают точку, которая принадлежит всем плоскостям.
  Первая координата точки — секрет.

Визуализация для $k = 3$:

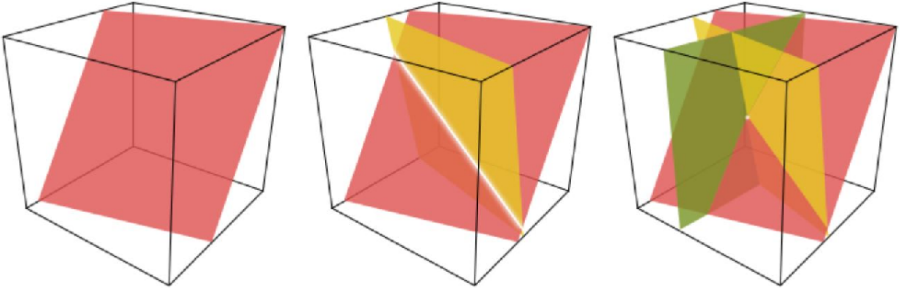


Схема Блэкли. Пример

Реализована $(n, 3)$- пороговая СРС Блэкли.
Уравнение Алисы: $2x + 3y + z - 17 = 0$
Уравнение Боба: $x - y + 4z - 15 = 0$
Уравнение Евы: $5x + 2y - z - 12 = 0$
Восстановление точки:

$$\begin{cases} 2x + 3y + z - 17 = 0 \\ x - y + 4z - 15 = 0 \\ 5x + 2y - z - 12 = 0 \end{cases} \longrightarrow \left(\begin{array}{ccc|c} 2 & 3 & 1 & 17 \\ 1 & -1 & 4 & 15 \\ 5 & 2 & -1 & 12 \end{array}\right) \longrightarrow$$

$$\longrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 4 \end{array}\right)$$

Секрет — первая координата точки, т. е. 2.

Схема Блэкли

Замечание

Схема Блэкли не является идеальной СРС, так как $\forall i = \overline{1, n} \;\; |S_i| = |\mathbb{F}_q|^{k+1} \neq |\mathbb{F}_q| = |S_0|$.

Схэма Блэкли

Обозначим $h_0 = (1, \dots, 0) \in \mathbb{F}_q^k$, $h_i = (a_{i_1}, \dots, a_{i_k})$ $i = \overline{1, n}$.

Для того, чтобы СРС была совершенной дилер должен следить за следующими условиями:

- Любые k векторов $h_{i_i}, \dots, h_{i_k}$ должны быть ЛНЗ.
  Необходимо для того, чтобы по любым k восстановить секрет.
- Для любых $k-1$ векторов $h_{i_i}, \dots, h_{i_{k-1}}$ вектор h_0 не должен лежать в $\langle h_{i_i}, \dots, h_{i_{k-1}} \rangle$.
  Необходимо для того, чтобы любые $k-1$ участников не получали никакой дополнительной информации о секрете.

Схема Блэкли

Утверждение

Схэма Блэкли является совершенной СРС.

- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_k} = s_{i_k}) \in \{0, 1\}$;
- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_t} = s_{i_t}) = P(\xi_0 = x)$ при $t < k$.

Схема Блэкли

- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_k} = s_{i_k}) \in \{0, 1\}$.

Запишем СЛАУ:

$$\begin{cases} a_{i_1 1} x_1 + a_{i_1 2} x_2 + \cdots + a_{i_1 k} x_k + d_{i_1} = 0 \\ \vdots \\ a_{i_k 1} x_1 + a_{i_k 2} x_2 + \cdots + a_{i_k k} x_k + d_{i_k} = 0 \end{cases}$$

Так как все строки ЛНЗ, то существует решение и ровно одно. Это решение $(s_0, b_1, \ldots, b_{k-1})$. Тогда

$$P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_k} = s_{i_k}) = P(\xi_o = x \mid \xi_0 = s_0) =$$

$$= P(x = s_0) \in \{0, 1\}$$

Схема Блэкли

- $P(\xi_0 = x \mid \xi_{i_1} = s_{i_1}, \ldots, \xi_{i_t} = s_{i_t}) = P(\xi_0 = x)$ при $t < k$.

Запишем СЛАУ в матричном виде:

$$\begin{pmatrix} h_{i_1} \\ \vdots \\ h_{i_t} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} -d_{i_1} \\ \vdots \\ -d_{i_k} \end{pmatrix}$$

Допишем уравнение для h_0 с соответствующим значением x:

$$\begin{pmatrix} h_0 \\ h_{i_1} \\ \vdots \\ h_{i_t} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} x \\ -d_{i_1} \\ \vdots \\ -d_{i_k} \end{pmatrix}$$

$$\begin{pmatrix} \boxed{\quad h_0 \quad} \\ \boxed{\quad h_{i_1} \quad} \\ \vdots \\ \boxed{\quad h_{i_t} \quad} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} x \\ -d_{i_1} \\ \vdots \\ -d_{i_k} \end{pmatrix}$$

Так как $(h_0, h_{i_1}, \ldots, h_{i_t})$ — ЛНЗ, то система совместна для любого x. При этом для любого x количество решений неоднородной СЛАУ равно количеству решений ОСЛАУ, то есть не зависит от x. То есть распределение секрета не изменилось.

Обобщение

Выпишем в матричном виде системы для схемы Шамира
и для схемы Блэкли:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 1 & x_1 & \dots & x_1^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} s_0 \\ \vdots \\ s_n \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & \dots & 0 \\ a_{1_1} & a_{1_2} & \dots & a_{1_k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_1} & a_{n_2} & \dots & a_{n_k} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} s_0 \\ -d_{1_1} \\ \vdots \\ -d_{n_k} \end{pmatrix}$$

Видно, что во многом эти схемы схожи, у них отличается только матрица.
Давайте обозначим матрицу H с векторами строками $h_0, h_1, \dots, h_n$,
неизвестный вектор столбец – x,
известный вектор столбец – s.
Тогда оба этих уравнения переписываются в виде $Hx = s$.

Линейная СРС

$Hx = s$

А что будет, если в качестве матрицы H взять какую-то случайную?

Определение

Получим ***линейную СРС****. В ней:*

- *множество индексов* $\{i_1, \ldots, i_m\} \in \mathcal{A}$ *(является разрешенным), если* $h_0 \in \langle h_{i_1}, \ldots, h_{i_m} \rangle$;
- *множество индексов* $\{i_1, \ldots, i_l\} \notin \mathcal{A}$ *(не является разрешенным), если* $h_0 \notin \langle h_{i_1}, \ldots, h_{i_m} \rangle$;
- s_i *— доля* i*-го участника;*
- $s_i = (h_0, x)$ *— секрет.*

Замечание

Доказательство совершенности схемы Блэкли обобщается на случай линейной СРС. Таким образом все линейные СРС совершенны.

Вариант 1

1. Выступая в роли дилера, разделите секрет $s_0 = 22$ в $\mathbb{F}_{29}$, реализовав $(5, 3)$-пороговую СРС с помощью
    1. алгоритма Шамира
    2. алгоритма Блэкли
2. Реализована $(n, 3)$-пороговая СРС Шамира в $\mathbb{F}_{29}$.
   Алисе соответсвует число 1, Бобу — 2, Еве — 3.
   Доля Алисы — 7, доля Боба — 26, доля Евы — 11.
   Воспроизведите процесс восстановления секрета Алисой, Бобом и Евой.

Вариант 2

1. Выступая в роли дилера, разделите секрет $s_0 = 7$ в $\mathbb{F}_{29}$, реализовав $(5, 3)$-пороговую СРС с помощью
   1. алгоритма Шамира
   2. алгоритма Блэкли
2. Реализована $(n, 3)$-пороговая СРС Шамира в $\mathbb{F}_{29}$.
   Алисе соответсвует число 1, Бобу — 2, Еве — 3.
   Доля Алисы — 9, доля Боба — 3, доля Евы — 23.
   Воспроизведите процесс восстановления секрета Алисой, Бобом и Евой.

Спасибо за внимание!