

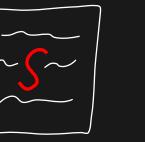
# РАЗДЕЛЕНИЕ СЕКРЕТА

# ПЛАН

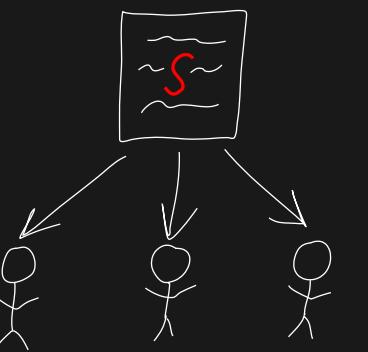
1. Введение
2.  $(n, n)$ -схема
3. Схема Блэкли
4. Многочлен Лагранжа ( $\star$ )
5. Схема Шамира
6. Атаки ( $\star$ )
7. Реализация простых структур доступа
8. Связь с теорией матроидов
9. Реализация произвольных структур доступа ( $\star$ )

# ЗАЧЕМ ЭТО НАДО?

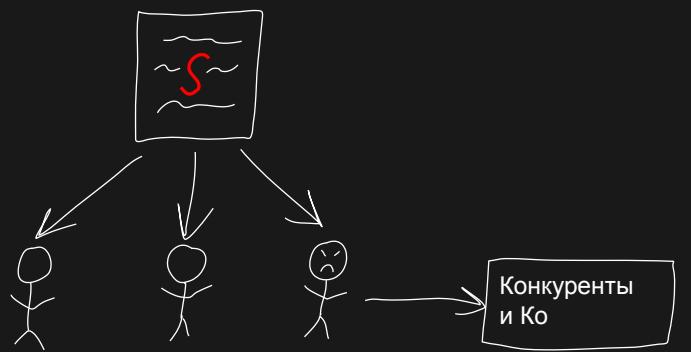
# ЗАЧЕМ ЭТО НАДО?



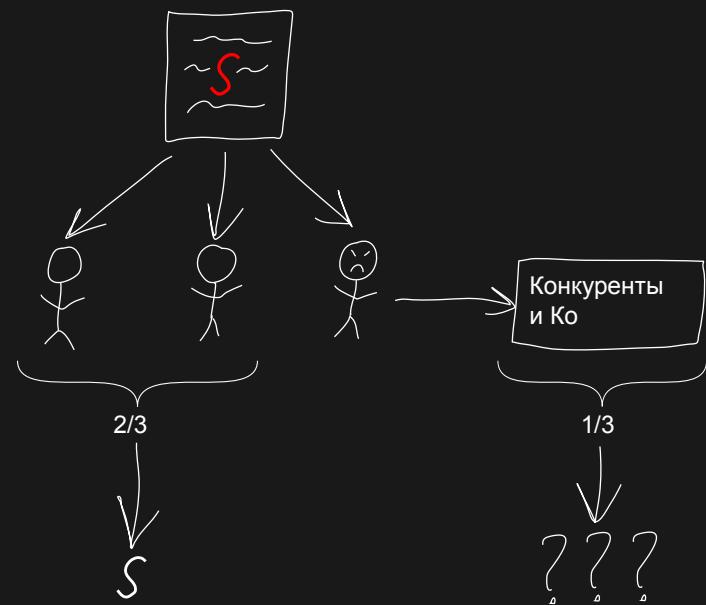
# ЗАЧЕМ ЭТО НАДО?



# ЗАЧЕМ ЭТО НАДО?



# ЗАЧЕМ ЭТО НАДО?

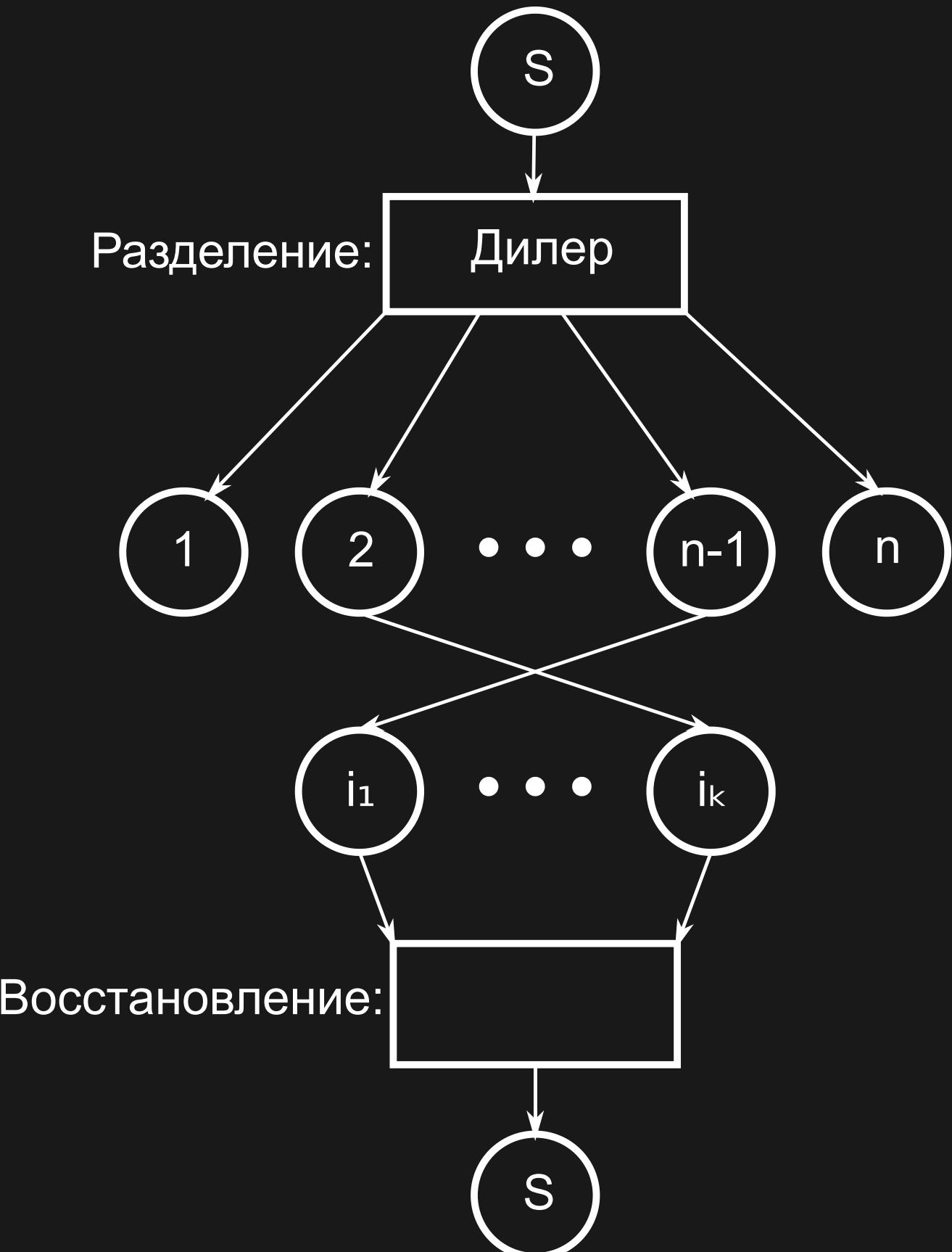


# СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА

Схема разделения секрета (CPC) разделяет секрет  $s$  между  $n$  участниками.

1. Дилер берёт секрет и делит его на доли
2. Они раздаются участникам –  $n$  штук
3. Затем какое-то подмножество участников собираются вместе
4. И они вместе восстанавливают секрет обратно

Две важные фазы: разделение и восстановление



# КРАТКО ОБ ОПРЕДЕЛЕНИЯХ

1. Разрешенное множество — те участники, которые могут восстановить секрет.
2. Структура доступа — совокупность всех разрешенных множеств. Должна быть монотонной.
3. Секрет разделяется на доли.
4. Схема называется **совершенной**, если недостаточное число долей (не входящие ни в одно разрешенное множество) не дают **никакой** информации о секрете.
5. Схема называется **идеальной**, если каждая доля содержит не больше информации, чем содержится в секрете.

# ПОРОГОВАЯ $(n, k)$ -СХЕМА

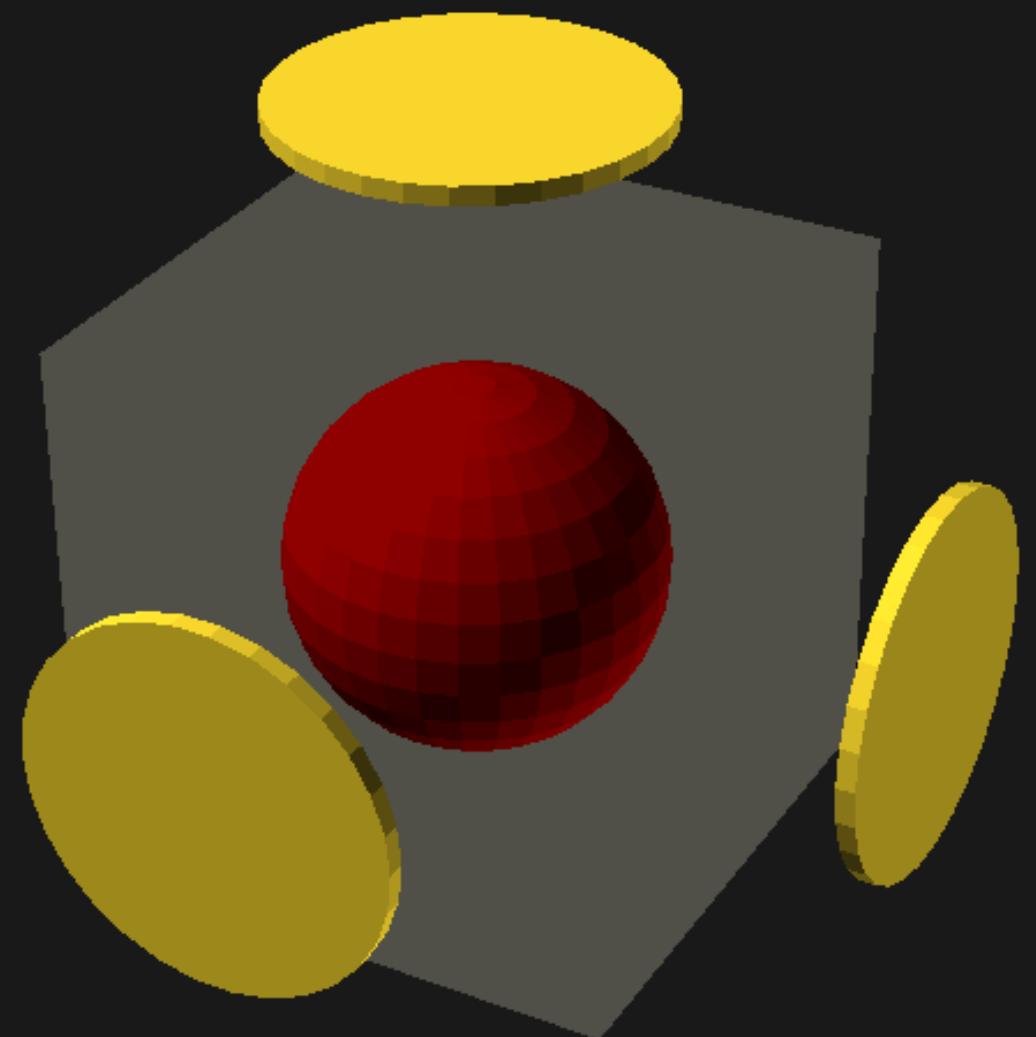
Это такая схема разделения доступа, что любые  $k$  участников из  $n$  могут восстановить секрет.

Другими словами, чтобы получить секрет, нужно хотя бы  $k$  участников.

Множество разрешенное, если в нём не меньше  $k$  участников.

# ПРИМЕР

Разделим между **тремя** участниками, чтобы только вместе они могли восстановить



- **Секрет**  $\in \{ \text{Шар}, \text{Куб}, \text{Цилиндр} \}$
- **Доля**  $\in \{ \text{Круг}, \text{Квадрат} \}$

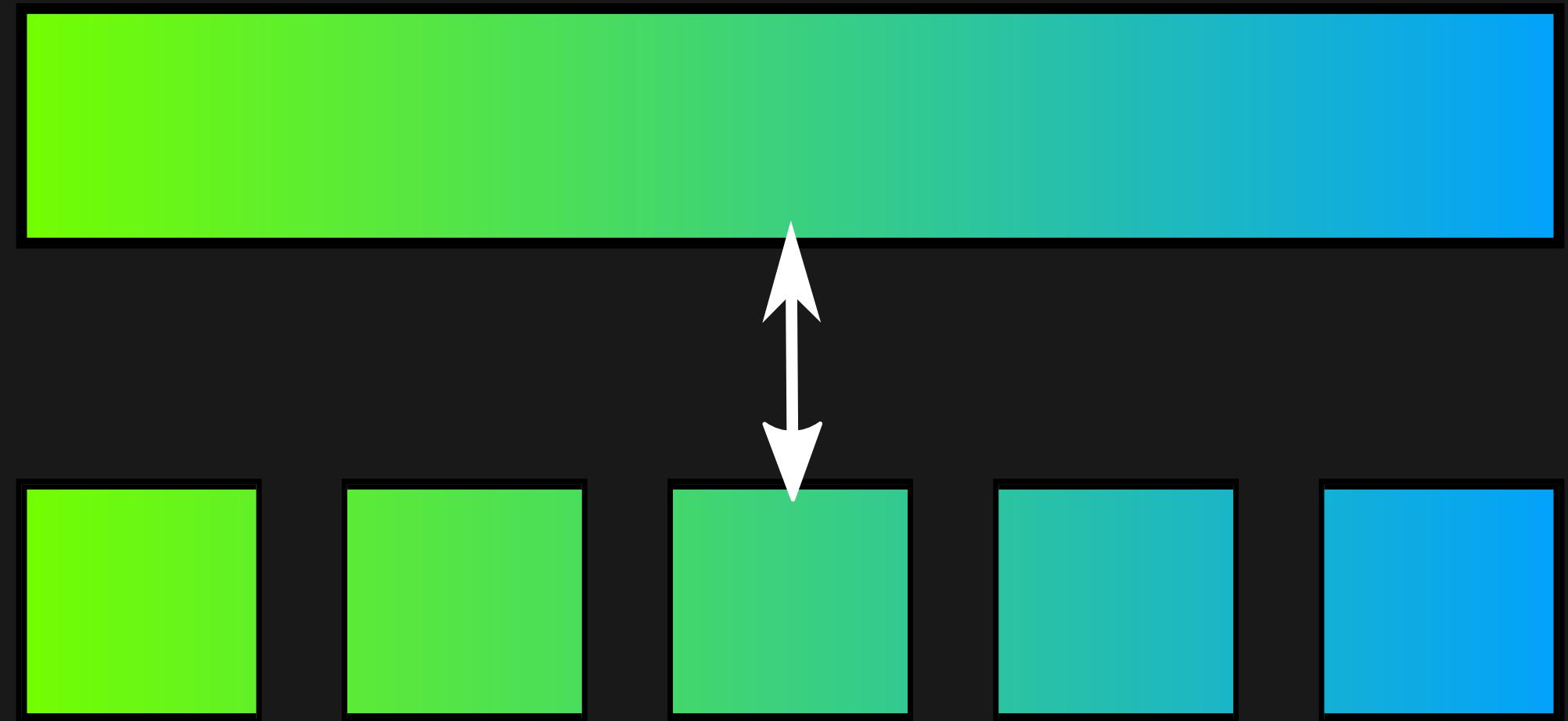
Любых двух проекций недостаточно, чтобы восстановить секрет

Это  $(3, 3)$ -схема.  $n = k = 3$

# $(n, n)$ -СХЕМА

$k = n$ . То есть  $n$  участников только **все вместе** могут получить секрет.

- Идея 1: нарезать секрет на доли.
- Недостаток: конкуренты легко взломают перебором
- Никогда такую схему использовать не будем



# СОВЕРШЕННОСТЬ

Хотим, чтобы конкуренты ничего не знали о секрете. Даже если знают  $k - 1$  долю.

# СОВЕРШЕННОСТЬ

Хотим, чтобы конкуренты ничего не знали о секрете. Даже если знают  $k - 1$  долю.

По-другому: знание  $k - 1$  долей ничего не даёт

# СОВЕРШЕННОСТЬ

Хотим, чтобы конкуренты ничего не знали о секрете. Даже если знают  $k - 1$  долю.

По-другому: знание  $k - 1$  долей ничего не даёт

- $s$  — секрет

# СОВЕРШЕННОСТЬ

Хотим, чтобы конкуренты ничего не знали о секрете. Даже если знают  $k - 1$  долю.

По-другому: знание  $k - 1$  долей ничего не даёт

- $s$  — секрет
- $v_i$  — доля секрета ( $i = 0 \dots n$ )

# СОВЕРШЕННОСТЬ

Хотим, чтобы конкуренты ничего не знали о секрете. Даже если знают  $k - 1$  долю.

По-другому: знание  $k - 1$  долей ничего не даёт

- $s$  — секрет
- $v_i$  — доля секрета ( $i = 0 \dots n$ )
- $H(s \mid v_{i_1}, v_{i_2}, \dots, v_{i_m})$  — сколько энтропии в  $s$ , если знаем эти доли

# СОВЕРШЕННОСТЬ

Хотим, чтобы конкуренты ничего не знали о секрете. Даже если знают  $k - 1$  долю.

По-другому: знание  $k - 1$  долей ничего не даёт

- $s$  — секрет
- $v_i$  — доля секрета ( $i = 0 \dots n$ )
- $H(s | v_{i_1}, v_{i_2}, \dots, v_{i_m})$  — сколько энтропии в  $s$ , если знаем эти доли
- $H(s)$  — сколько энтропии в секрете, если мы совсем ничего про него не знаем

# СОВЕРШЕННОСТЬ

Хотим, чтобы конкуренты ничего не знали о секрете. Даже если знают  $k - 1$  долю.

По-другому: знание  $k - 1$  долей ничего не даёт

- $s$  — секрет
- $v_i$  — доля секрета ( $i = 0 \dots n$ )
- $H(s | v_{i_1}, v_{i_2}, \dots, v_{i_m})$  — сколько энтропии в  $s$ , если знаем эти доли
- $H(s)$  — сколько энтропии в секрете, если мы совсем ничего про него не знаем

Хотим:

$$H(s | v_{i_1}, v_{i_2}, \dots, v_{i_m}) = H(s), \quad \text{при } m < k$$
$$H(s | v_{i_1}, v_{i_2}, \dots, v_{i_m}) = 0, \quad \text{при } m \geq k$$

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

Алгоритм: 0. Пусть  $s \in \mathbb{F}$

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

Алгоритм:

0. Пусть  $s \in \mathbb{F}$
1. Генерируем совершенно случайные  $v_2, \dots, v_n$  тоже из  $\mathbb{F}$ .

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

Алгоритм:

0. Пусть  $s \in \mathbb{F}$
1. Генерируем совершенно случайные  $v_2, \dots, v_n$  тоже из  $\mathbb{F}$ .
2. Находим  $v_1 = s - v_2 - \dots - v_n$

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

Алгоритм:

0. Пусть  $s \in \mathbb{F}$
1. Генерируем совершенно случайные  $v_2, \dots, v_n$  тоже из  $\mathbb{F}$ .
2. Находим  $v_1 = s - v_2 - \dots - v_n$
3. Раздаём эти доли участникам

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

Алгоритм:

0. Пусть  $s \in \mathbb{F}$
1. Генерируем совершенно случайные  $v_2, \dots, v_n$  тоже из  $\mathbb{F}$ .
2. Находим  $v_1 = s - v_2 - \dots - v_n$
3. Раздаём эти доли участникам

**Почему она совершенная?**

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

Алгоритм:

0. Пусть  $s \in \mathbb{F}$
1. Генерируем совершенно случайные  $v_2, \dots, v_n$  тоже из  $\mathbb{F}$ .
2. Находим  $v_1 = s - v_2 - \dots - v_n$
3. Раздаём эти доли участникам

**Почему она совершенная?**

Допустим: знаем  $v_1, \dots, v_{n-1}$  — все кроме (без потери общности) последнего.

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

Алгоритм:

0. Пусть  $s \in \mathbb{F}$
1. Генерируем совершенно случайные  $v_2, \dots, v_n$  тоже из  $\mathbb{F}$ .
2. Находим  $v_1 = s - v_2 - \dots - v_n$
3. Раздаём эти доли участникам

**Почему она совершенная?**

Допустим: знаем  $v_1, \dots, v_{n-1}$  — все кроме (без потери общности) последнего.

Тогда:

1. Есть  $|\mathbb{F}|$  вариантов для последней доли.

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

Алгоритм: 0. Пусть  $s \in \mathbb{F}$

1. Генерируем совершенно случайные  $v_2, \dots, v_n$  тоже из  $\mathbb{F}$ .
2. Находим  $v_1 = s - v_2 - \dots - v_n$
3. Раздаём эти доли участникам

## Почему она совершенная?

Допустим: знаем  $v_1, \dots, v_{n-1}$  — все кроме (без потери общности) последнего.

Тогда:

1. Есть  $|\mathbb{F}|$  вариантов для последней доли.
2. Каждый вариант даёт свой уникальный  $s$ .

# НАСТОЯЩАЯ $(n, n)$ -СХЕМА

Идея:  $s = v_1 + v_2 + \dots + v_n$

Алгоритм: 0. Пусть  $s \in \mathbb{F}$

1. Генерируем совершенно случайные  $v_2, \dots, v_n$  тоже из  $\mathbb{F}$ .
2. Находим  $v_1 = s - v_2 - \dots - v_n$
3. Раздаём эти доли участникам

## Почему она совершенная?

Допустим: знаем  $v_1, \dots, v_{n-1}$  — все кроме (без потери общности) последнего.

Тогда: 1. Есть  $|\mathbb{F}|$  вариантов для последней доли.

2. Каждый вариант даёт свой уникальный  $s$ .

3. Угадать значение доли из  $|\mathbb{F}|$  также сложно, как угадать секрет (тоже из  $\mathbb{F}$ ).

Теперь и секрет, и доли из одного поля, т.е. они содержат одинаково информации (если они выбраны случайно). Это интересно.

Теперь и секрет, и доли из одного поля, т.е. они содержат одинаково информации (если они выбраны случайно). Это интересно.

## ТЕОРЕМА

Пусть схема совершенная, а  $v_i \in V$  – доля секрета  $s \in S$ .  
Тогда  $H(v_i) \geq H(s)$ .

Теперь и секрет, и доли из одного поля, т.е. они содержат одинаково информации (если они выбраны случайно). Это интересно.

# ТЕОРЕМА

Пусть схема совершенная, а  $v_i \in V$  – доля секрета  $s \in S$ .

Тогда  $H(v_i) \geq H(s)$ .

**Следствие:** Если секрет и доли выбираются случайно, то  $|V| \geq |S|$ .

теперь и секрет, и доли из одного поля, т.е. они содержат одинаково информации (если они выбраны случайно). Это интересно.

# ТЕОРЕМА

Пусть схема совершенная, а  $v_i \in V$  – доля секрета  $s \in S$ .

Тогда  $H(v_i) \geq H(s)$ .

**Следствие:** Если секрет и доли выбираются случайно, то  $|V| \geq |S|$ .

## Доказательство следствия

1. Известно, что знание  $k - 1$  доли не даёт никакой информации о секрете
2. Также известно, что зная  $k$  долей можно единственным образом восстановить секрет.
3. Если  $|V| < |S|$ , то зная  $k - 1$  долей, мы можем получить лишь  $|V|$  значений секрета, по одному на каждое возможное значение доли.

# СХЕМА БЛЭКЛИ

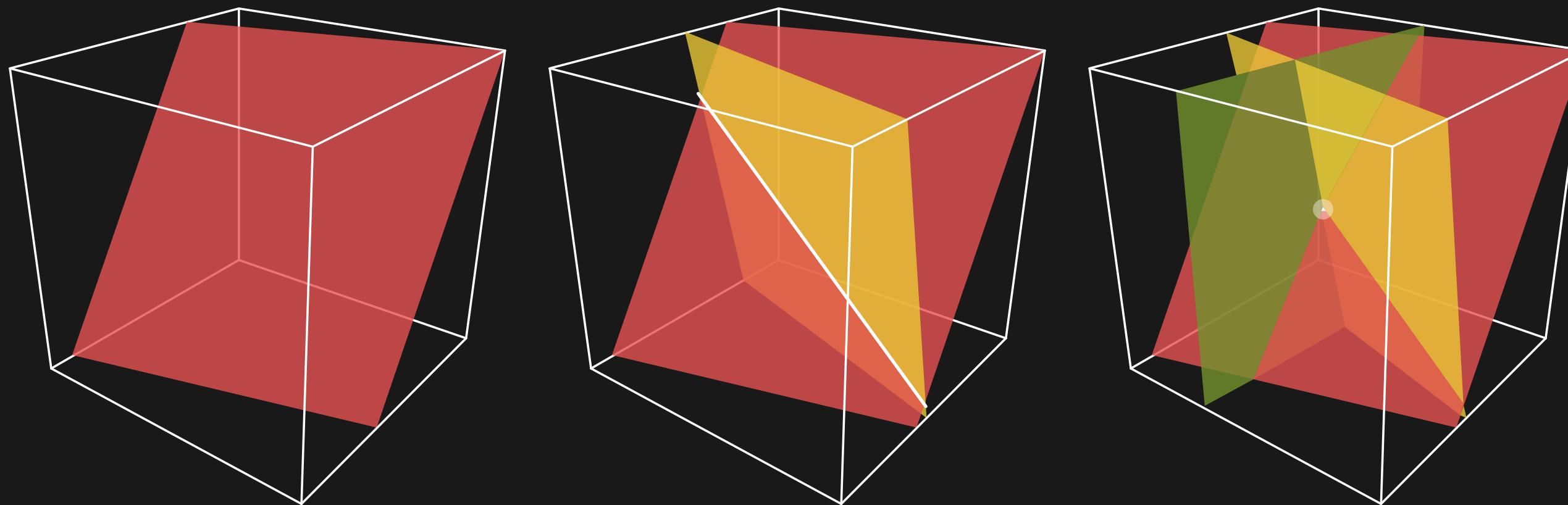
Это  $(n, k)$ -схема. Из  $n$  участников  
достаточно только  $k$ .

Описана Джорджем Блэкли в начале июня  
1979 года.



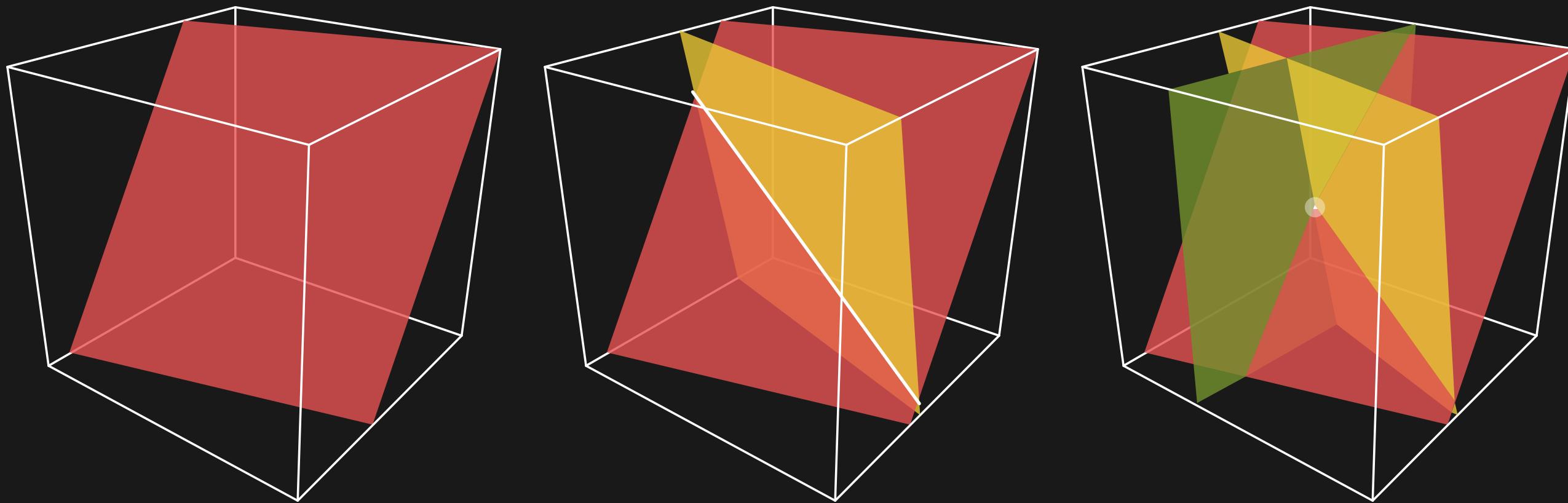
# СХЕМА БЛЭКЛИ

Идея:  $k$  гиперплоскостей пересекаются в  $k$ -мерном пространстве в точке.



# СХЕМА БЛЭКЛИ

Идея:  $k$  гиперплоскостей пересекаются в  $k$ -мерном пространстве в точке.

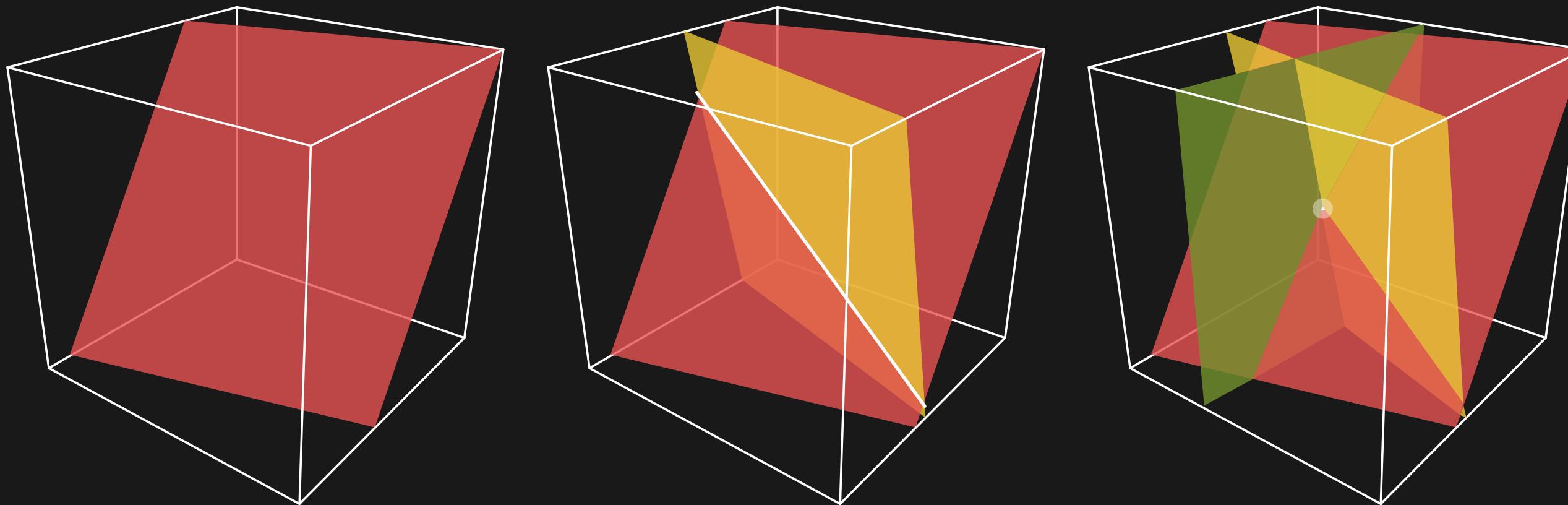


Алгоритм:

0. Секрет  $s \in \mathbb{F}$ .

# СХЕМА БЛЭКЛИ

Идея:  $k$  гиперплоскостей пересекаются в  $k$ -мерном пространстве в точке.

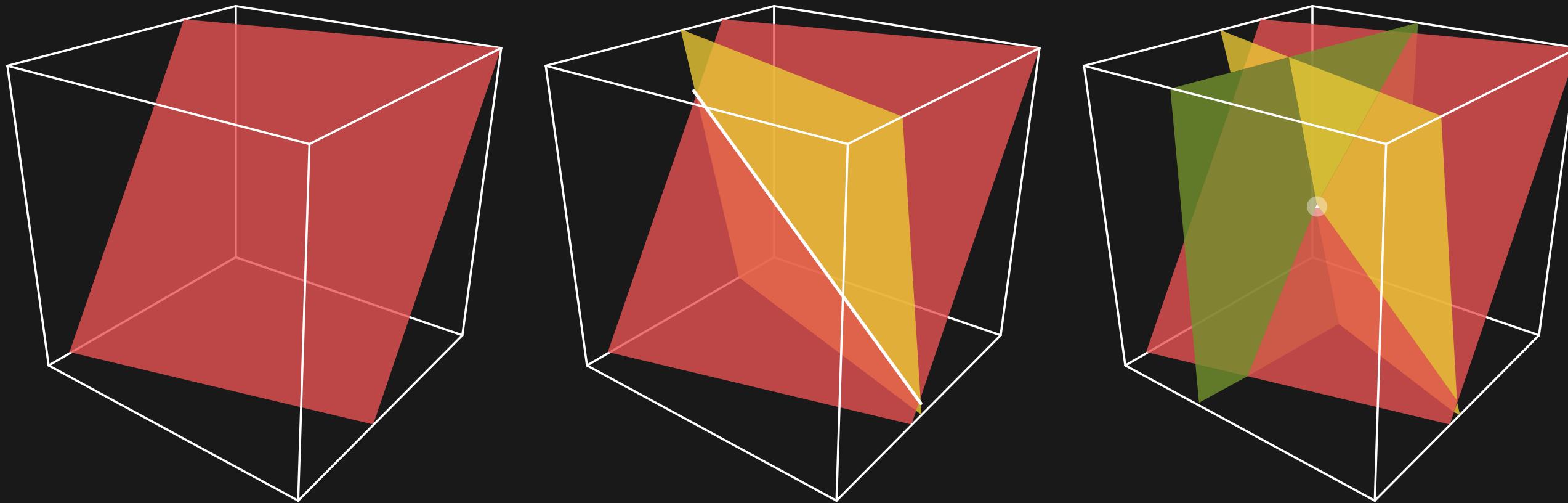


Алгоритм:

0. Секрет  $s \in \mathbb{F}$ . Возьмём пространство  $\mathbb{F}^k$

# СХЕМА БЛЭКЛИ

Идея:  $k$  гиперплоскостей пересекаются в  $k$ -мерном пространстве в точке.

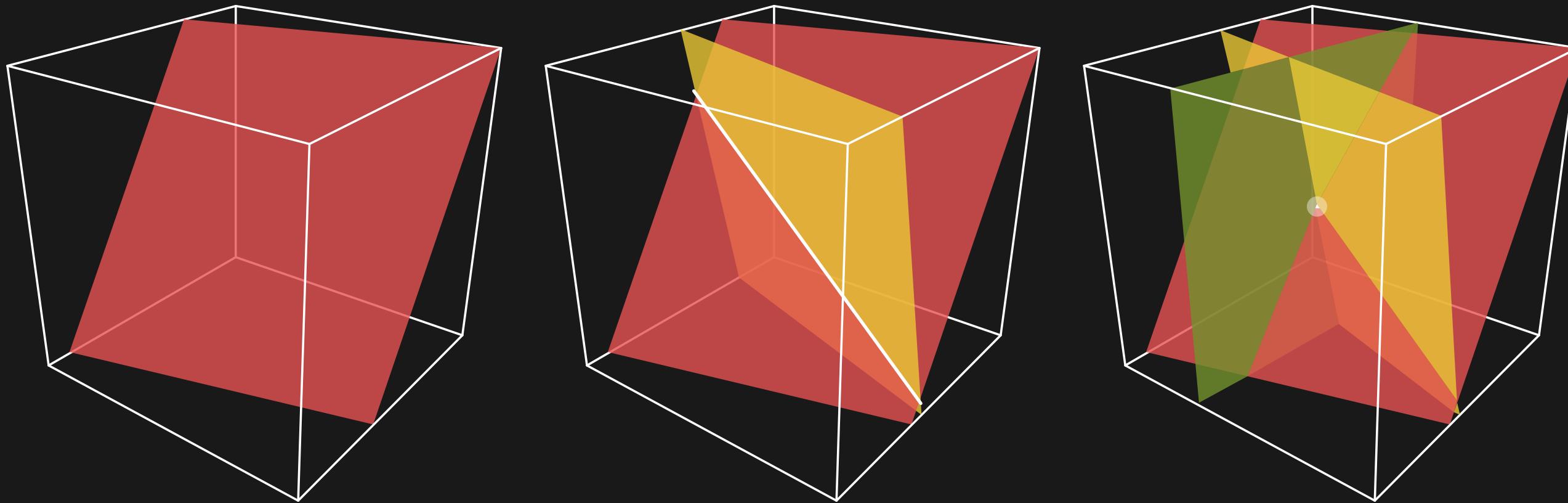


Алгоритм:

0. Секрет  $s \in \mathbb{F}$ . Возьмём пространство  $\mathbb{F}^k$
1. Выберем случайные и независимые  $x_2, x_3, \dots, x_k$

# СХЕМА БЛЭКЛИ

Идея:  $k$  гиперплоскостей пересекаются в  $k$ -мерном пространстве в точке.

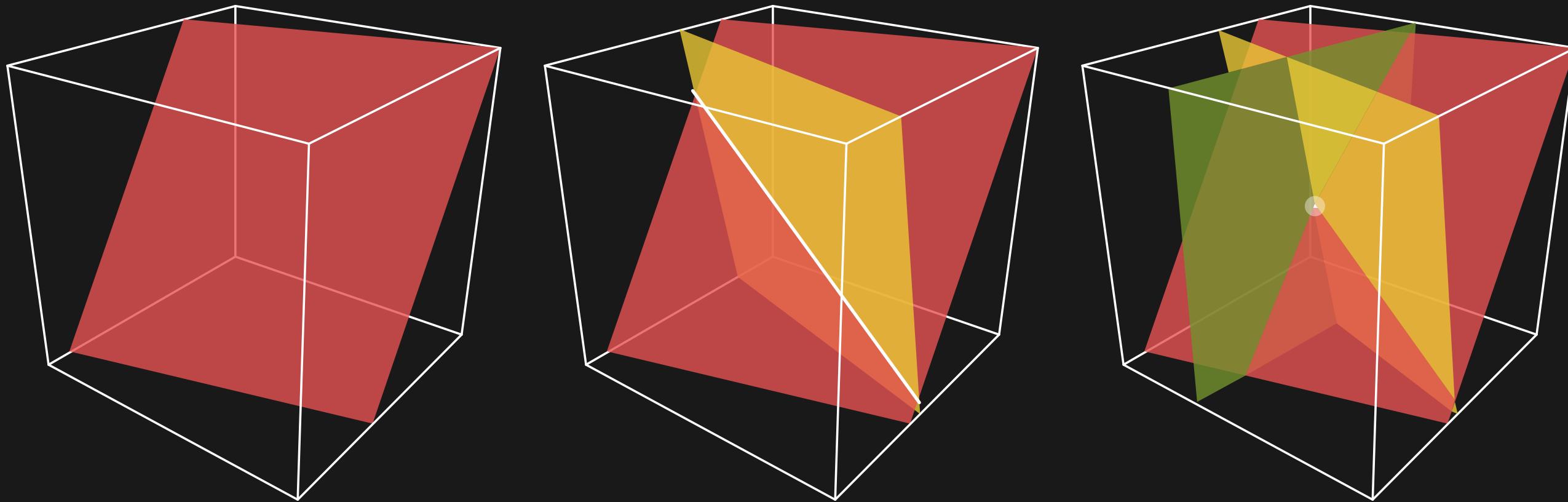


Алгоритм:

0. Секрет  $s \in \mathbb{F}$ . Возьмём пространство  $\mathbb{F}^k$
1. Выберем случайные и независимые  $x_2, x_3, \dots, x_k$
2. Секретная точка:  $(s, x_2, x_3, \dots, x_k)$

# СХЕМА БЛЭКЛИ

**Идея:**  $k$  гиперплоскостей пересекаются в  $k$ -мерном пространстве в точке.



**Алгоритм:**

0. Секрет  $s \in \mathbb{F}$ . Возьмём пространство  $\mathbb{F}^k$
1. Выберем случайные и независимые  $x_2, x_3, \dots, x_k$
2. Секретная точка:  $(s, x_2, x_3, \dots, x_k)$
3. Провести через неё  $n$  случайных гиперплоскостей и раздать их участникам.

# ПРИМЕР

- Секрет из поля  $\mathbb{Z}_{23}$  будет  $s = 18$
- Действуем в пространстве  $\mathbb{Z}_{23}^3$  — три участника могут восстановить
- Выберем случайную точку  $(18, 7, 20)$  — секрет в первой координате
- Проведём плоскости через эту точку:
  - $21x_1 + x_2 + 15x_3 = 18$
  - $11x_1 + 9x_2 + x_3 = 5$
  - $3x_1 + 6x_2 + 8x_3 = 3$

Именно этой информацией обладают участники — каждый знает ровно одну плоскость.

- Выберем случайную точку  $(18, 7, 20)$  — секрет в первой координате
- Проведём плоскости через эту точку:
  - $21x_1 + x_2 + 15x_3 = 18$
  - $11x_1 + 9x_2 + x_3 = 5$
  - $3x_1 + 6x_2 + 8x_3 = 3$

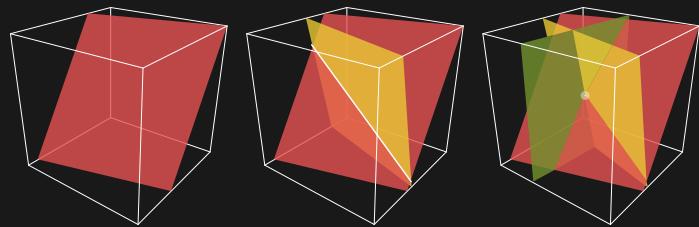
Именно этой информацией обладают участники — каждый знает ровно одну плоскость.

- Пересечём их:

$$\begin{pmatrix} 21 & 1 & 15 \\ 11 & 9 & 1 \\ 3 & 6 & 8 \end{pmatrix} \vec{x} = \begin{pmatrix} 18 \\ 5 \\ 3 \end{pmatrix}$$

# СХЕМА БЛЭКЛИ: СОВЕРШЕННОСТЬ

- Даны  $k - 1$  плоскости, пересекаются по прямой ( $\cong \mathbb{F}$ )



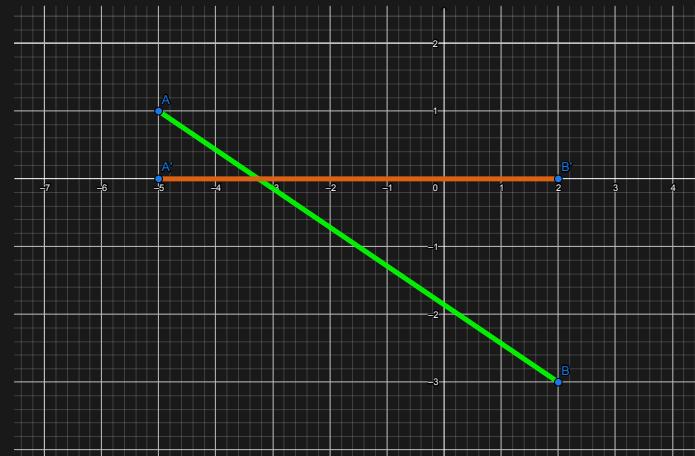
# СХЕМА БЛЭКЛИ: СОВЕРШЕННОСТЬ

- Даны  $k - 1$  плоскости, пересекаются по прямой ( $\cong \mathbb{F}$ )
- Но нас интересует только одна координата



# СХЕМА БЛЭКЛИ: СОВЕРШЕННОСТЬ

- Даны  $k - 1$  плоскости, пересекаются по прямой ( $\cong \mathbb{F}$ )
- Но нас интересует только одна координата



- На прямой столько же точек, сколько и значений секрета!

# СХЕМА БЛЭКЛИ

**Секрет:**  $s \in \mathbb{F}$ .

**Доля:**  $k$ -мерная плоскость

# СХЕМА БЛЭКЛИ

**Секрет:**  $s \in \mathbb{F}$ .

**Доля:**  $k$ -мерная плоскость

$$A_1x_1 + A_2x_2 + \dots + A_kx_k + A_0 = 0$$

# СХЕМА БЛЭКЛИ

**Секрет:**  $s \in \mathbb{F}$ .

**Доля:**  $k$ -мерная плоскость

$$A_1x_1 + A_2x_2 + \dots + A_kx_k + A_0 = 0$$

**Плоскость:** набор  $(A_1, A_2, \dots, A_k) \in \mathbb{F}^{k+1}$

Но секрет-то только из  $\mathbb{F}$ ! Доля в  $k + 1$  раз больше.

# ИДЕАЛЬНОСТЬ

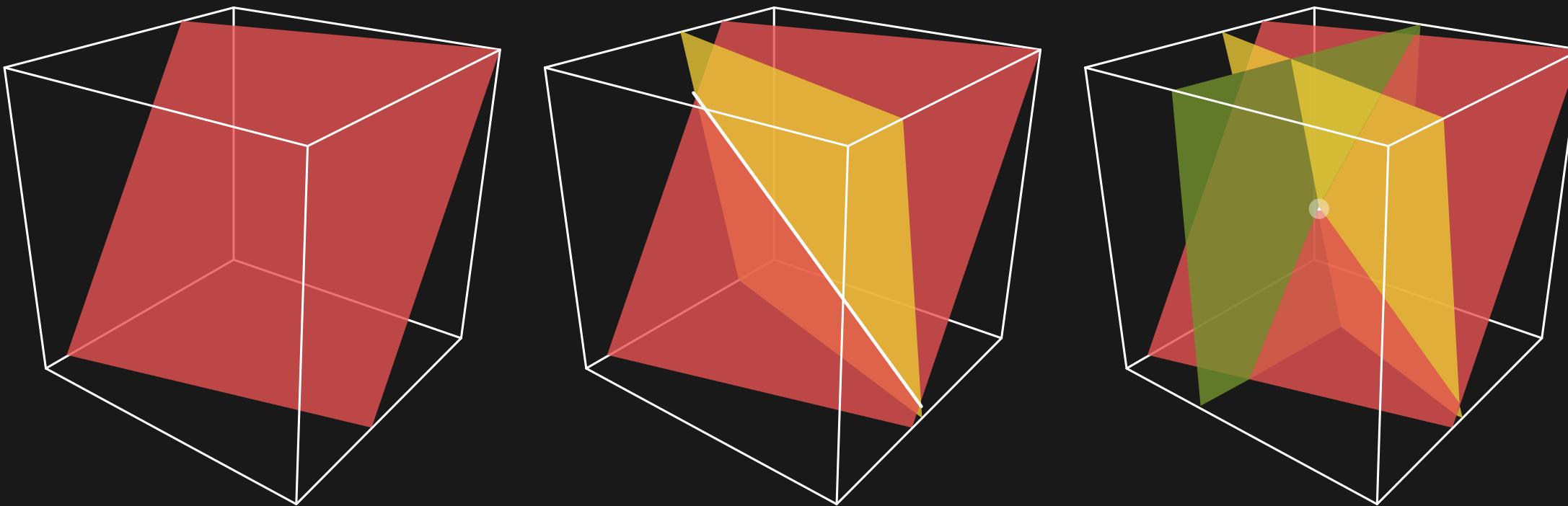
Секрет  $s \in S$ , доля  $v_i \in V$ .

- Из теоремы:  $H(v_i) \geq H(s)$
- Если  $H(v_i) = H(s)$ , то схема идеальна

Схема идеальна тогда, когда доля содержит ровно столько же информации, сколько и секрет.

# НЕПРАВИЛЬНАЯ СХЕМА

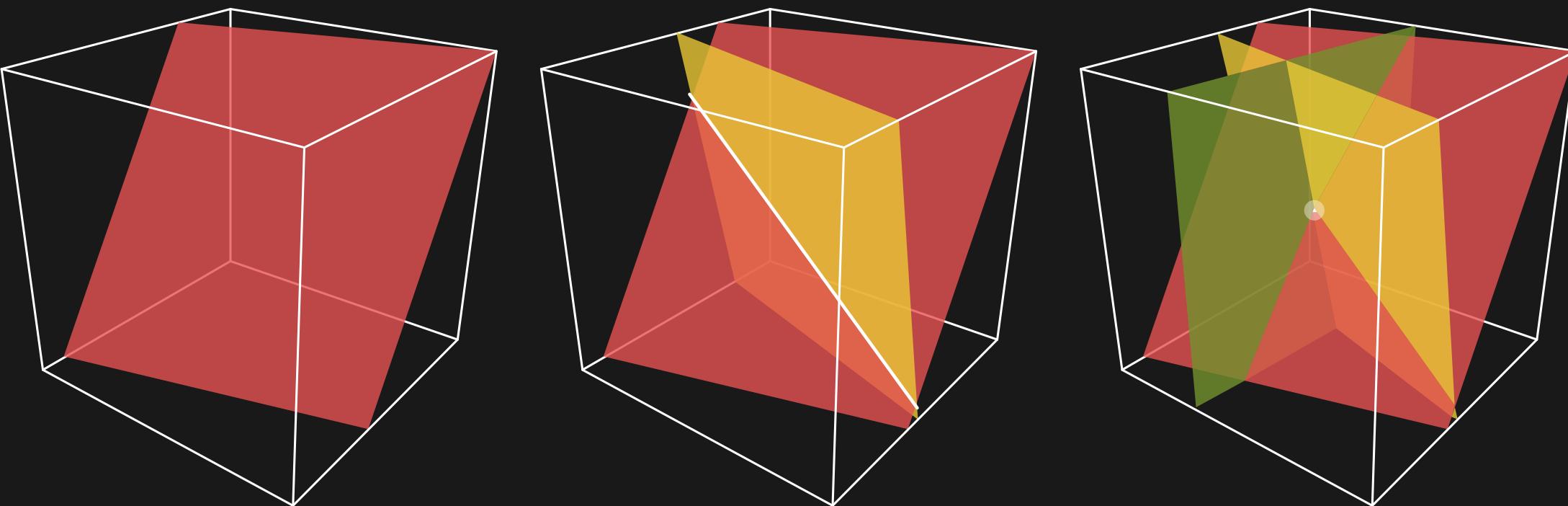
Хотим сделать схему Блэкли её идеальной.



# НЕПРАВИЛЬНАЯ СХЕМА

Хотим сделать схему Блэкли её идеальной.

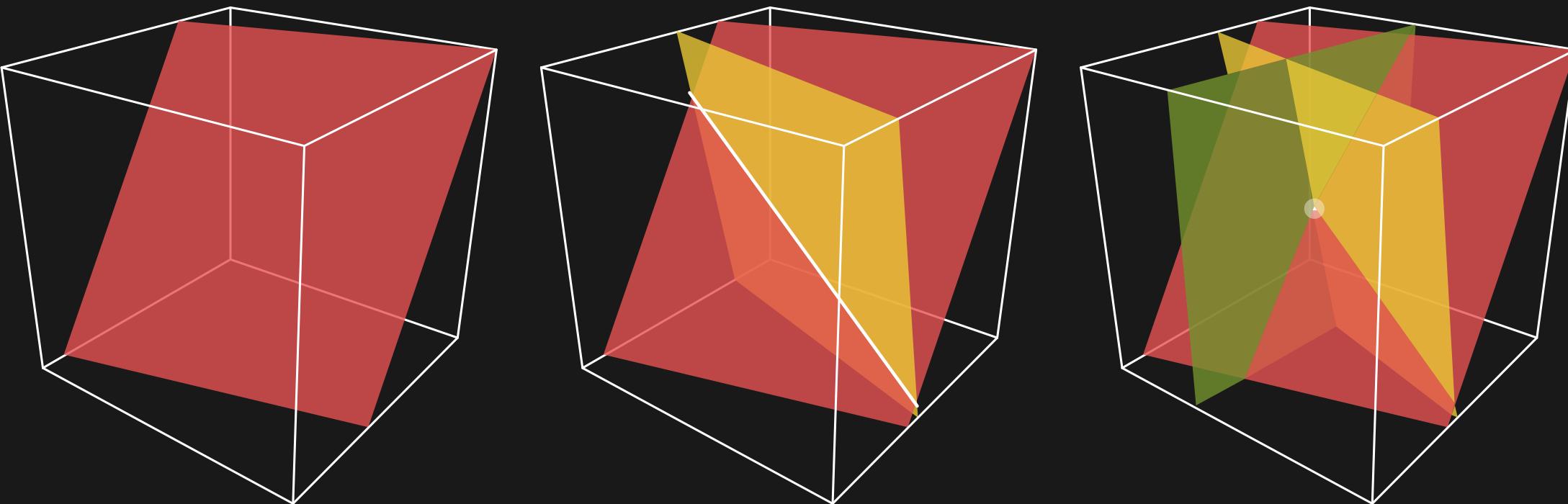
- Секрет хранится только в одной координате.
  - $s \in \mathbb{F}$



# НЕПРАВИЛЬНАЯ СХЕМА

Хотим сделать схему Блэкли её идеальной.

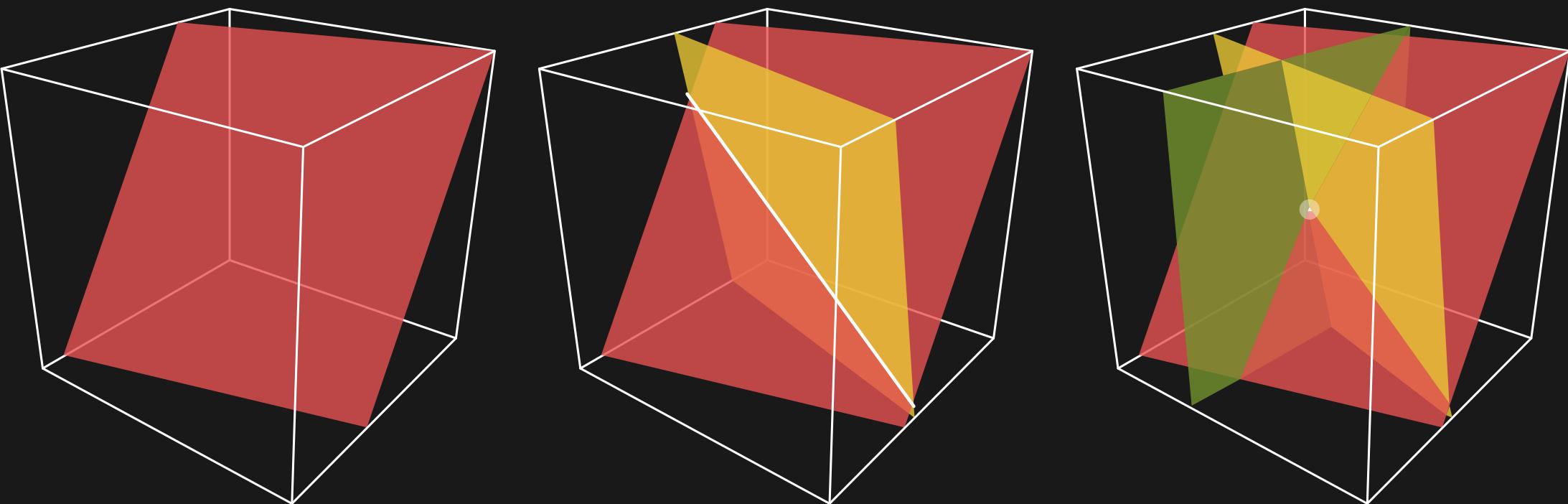
- Секрет хранится только в одной координате.
  - $s \in \mathbb{F}$
- А доля гораздо больше
  - $v_i \in \mathbb{F}^k$



# НЕПРАВИЛЬНАЯ СХЕМА

Хотим сделать схему Блэкли её идеальной.

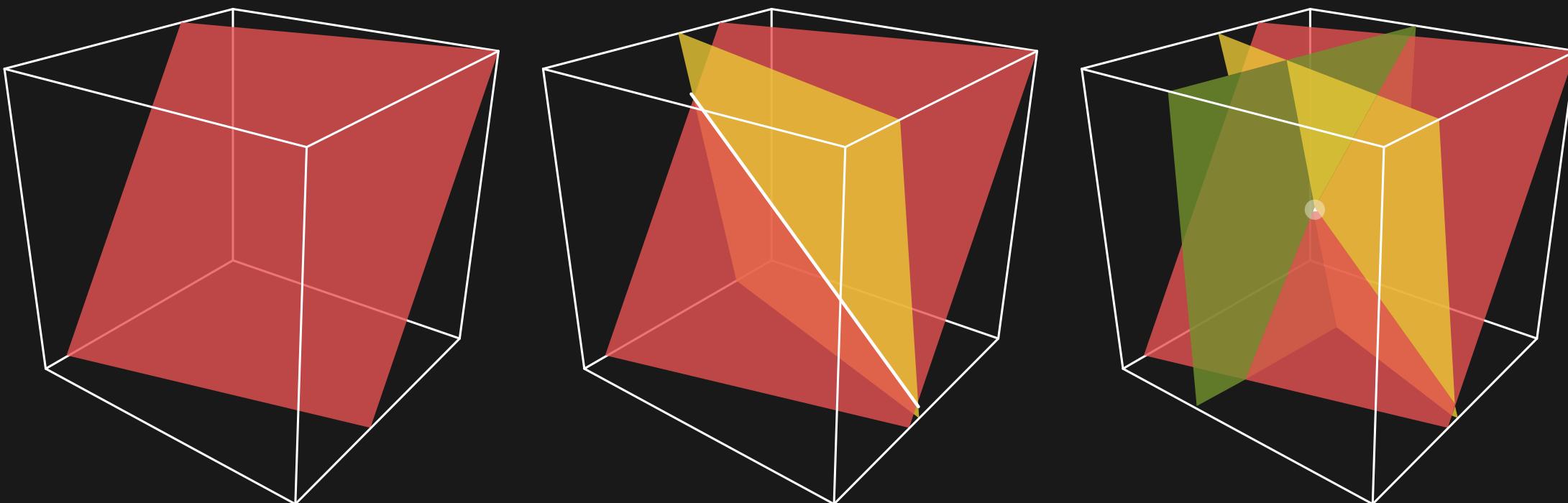
- Секрет хранится только в одной координате.
  - $s \in \mathbb{F}$
- А доля гораздо больше
  - $v_i \in \mathbb{F}^k$
- Идея: распределить секрет по всем координатам:  $s \in \mathbb{F}^k$



# НЕПРАВИЛЬНАЯ СХЕМА

Хотим сделать схему Блэкли её идеальной.

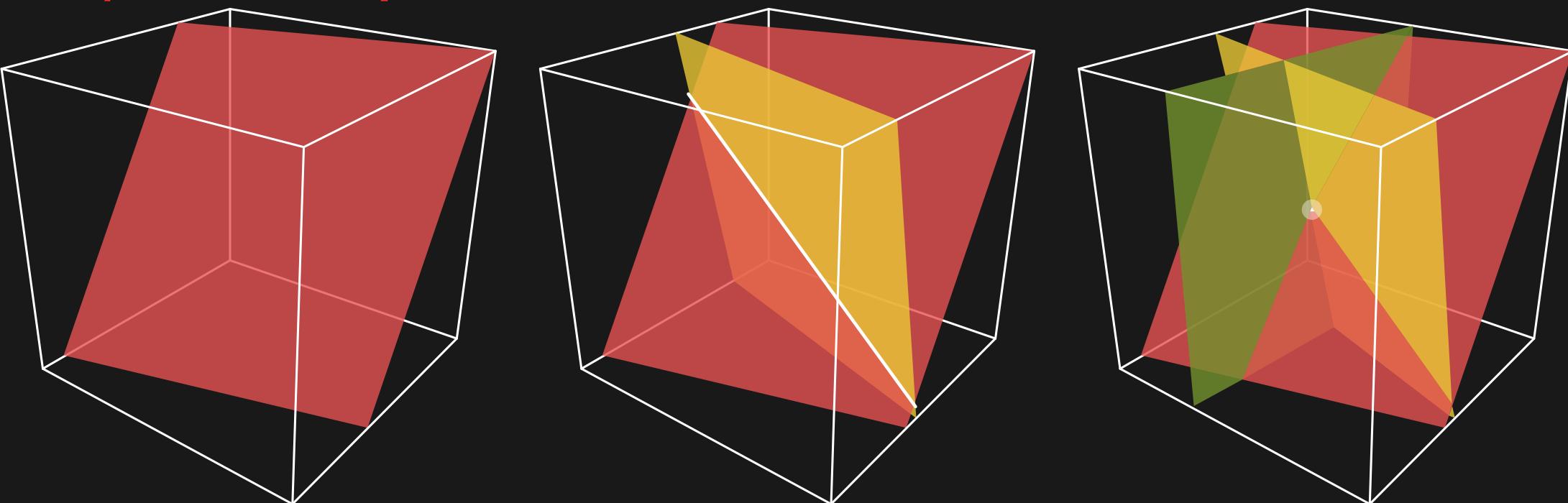
- Секрет хранится только в одной координате.
  - $s \in \mathbb{F}$
- А доля гораздо больше
  - $v_i \in \mathbb{F}^k$
- Идея: распределить секрет по всем координатам:  $s \in \mathbb{F}^k$ 
  - Нельзя: на прямой всего лишь  $|\mathbb{F}|$  точек, хотя вариантов секрета  $|\mathbb{F}|^k$



# НЕПРАВИЛЬНАЯ СХЕМА

Хотим сделать схему Блэкли её идеальной.

- Секрет хранится только в одной координате.
  - $s \in \mathbb{F}$
- А доля гораздо больше
  - $v_i \in \mathbb{F}^k$
- Идея: распределить секрет по всем координатам:  $s \in \mathbb{F}^k$ 
  - Нельзя: на прямой всего лишь  $|\mathbb{F}|$  точек, хотя вариантов секрета  $|\mathbb{F}|^k$
  - Такая схема **не будет совершенной!**



# МНОГОЧЛЕН ЛАГРАНЖА

# МНОГОЧЛЕН ЛАГРАНЖА

**Хотим:** провести многочлен не более  $n - 1$  степени через  $n$  точек

Например, **прямая** — многочлен первой степени — легко строится по **двум** точкам.

**Дано:** точки  $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ .

# МНОГОЧЛЕН ЛАГРАНЖА

**Хотим:** провести многочлен не более  $n - 1$  степени через  $n$  точек

Например, **прямая** — многочлен первой степени — легко строится по **двум** точкам.

**Дано:** точки  $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ .

**Очень простая идея:**

Можно составить СЛАУ на  $c_i$ , подставив точки в  $c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}$ .

Здесь  $n$  неизвестных,  $n$  уравнений, а следовательно решение единствено.

# МНОГОЧЛЕН ЛАГРАНЖА

**Хотим:** провести многочлен не более  $n - 1$  степени через  $n$  точек

Например, **прямая** — многочлен первой степени — легко строится по **двум** точкам.

**Дано:** точки  $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ .

**Очень простая идея:**

Можно составить СЛАУ на  $c_i$ , подставив точки в  $c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}$ .

Здесь  $n$  неизвестных,  $n$  уравнений, а следовательно решение единствено.

Но есть явная формула:  $f(\textcolor{red}{x}) = \sum_{j=1}^n y_j \prod_{\substack{i=0 \\ i \neq j}}^n \frac{\textcolor{red}{x} - x_i}{x_j - x_i}$  — многочлен Лагранжа

# ОЧЕВИДНОЕ РЕШЕНИЕ

Просто скажем следующее:

$$f(x) = \begin{cases} y_1, & x = x_1 \\ y_2, & x = x_2 \\ \dots \\ y_n, & x = x_n \\ \text{что-нибудь,} & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$$

# ОЧЕВИДНОЕ РЕШЕНИЕ

Просто скажем следующее:

$$f(x) = \begin{cases} y_1, & x = x_1 \\ y_2, & x = x_2 \\ \dots \\ y_n, & x = x_n \\ \text{что-нибудь}, & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$$

И если бы у нас была такая функция:

$$\ell_j(x) = \begin{cases} 1, & x = x_i, i = j \\ 0, & x = x_i, i \neq j \\ \text{что-нибудь} & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$$

# ОЧЕВИДНОЕ РЕШЕНИЕ

Просто скажем следующее:

$$f(x) = \begin{cases} y_1, & x = x_1 \\ y_2, & x = x_2 \\ \dots \\ y_n, & x = x_n \\ \text{что-нибудь}, & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$$

И если бы у нас была такая функция:

$$\ell_j(x) = \begin{cases} 1, & x = x_i, i = j \\ 0, & x = x_i, i \neq j \\ \text{что-нибудь} & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$$

Тогда бы мы разбили на сумму:

$$f(x) = y_1 \ell_1(x) + y_2 \ell_2(x) + \dots + y_n \ell_n(x)$$

# ТАКАЯ ФУНКЦИЯ ЕСТЬ!

Напомню:  $\ell_j(x) = \begin{cases} 1, & x = x_j \\ 0, & x = x_i, i \neq j \\ \text{что-нибудь}, & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$

# ТАКАЯ ФУНКЦИЯ ЕСТЬ!

Напомню:  $\ell_j(x) = \begin{cases} 1, & x = x_j \\ 0, & x = x_i, i \neq j \\ \text{что-нибудь}, & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$

Выглядит она как произведение дробей:

$$\ell_j(\textcolor{red}{x}) = \prod_{\substack{i=0 \\ i \neq j}}^{} \frac{\textcolor{red}{x} - x_i}{x_j - x_i}$$

# ТАКАЯ ФУНКЦИЯ ЕСТЬ!

Напомню:  $\ell_j(x) = \begin{cases} 1, & x = x_j \\ 0, & x = x_i, i \neq j \\ \text{что-нибудь}, & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$

Выглядит она как произведение дробей:

$$\ell_j(\textcolor{red}{x}) = \prod_{\substack{i=0 \\ i \neq j}}^{} \frac{\textcolor{red}{x} - x_i}{x_j - x_i}$$

- Если  $x = x_j$ , то каждая дробь равна 1, и вся функция тоже.

# ТАКАЯ ФУНКЦИЯ ЕСТЬ!

Напомню:  $\ell_j(x) = \begin{cases} 1, & x = x_j \\ 0, & x = x_i, i \neq j \\ \text{что-нибудь}, & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$

Выглядит она как произведение дробей:

$$\ell_j(\textcolor{red}{x}) = \prod_{\substack{i=0 \\ i \neq j}}^{} \frac{\textcolor{red}{x} - x_i}{x_j - x_i}$$

- Если  $x = x_j$ , то каждая дробь равна 1, и вся функция тоже.
- Если  $x = x_i, i \neq j$ , то найдётся  $i$ , такой что  $x_i = x$ . А значит один из числителей будет таким:  $x_i - x_i = 0$ . И всё произведение обнулится.

# ТАКАЯ ФУНКЦИЯ ЕСТЬ!

Напомню:  $\ell_j(x) = \begin{cases} 1, & x = x_i, i = j \\ 0, & x = x_i, i \neq j \\ \text{что-нибудь}, & x \notin \{x_1, x_2, \dots, x_n\} \end{cases}$

Выглядит она как произведение дробей:

$$\ell_j(\textcolor{red}{x}) = \prod_{\substack{i=0 \\ i \neq j}}^{} \frac{\textcolor{red}{x} - x_i}{x_j - x_i}$$

- Если  $x = x_j$ , то каждая дробь равна 1, и вся функция тоже.
- Если  $x = x_i, i \neq j$ , то найдётся  $i$ , такой что  $x_i = x$ . А значит один из числителей будет таким:  $x_i - x_i = 0$ . И всё произведение обнулится.
- Все точки различны и  $j \neq i$ , а значит мы не делим на ноль.

# ИТОГ

Интерполяционный многочлен Лагранжа:

$$f(\textcolor{red}{x}) = \sum_{j=1}^n y_j \prod_{\substack{i=0 \\ i \neq j}}^n \frac{\textcolor{red}{x} - x_i}{x_j - x_i}$$

- Проходит через точки  $(x_1, y_1), \dots, (x_n, y_n)$
- Степень не больше  $n$

# ЕДИНСТВЕННОСТЬ

*Через  $p$  точек проходит единственный многочлен степени не больше  $n - 1$ .*

**Доказательство:**

- Пусть  $f(x)$  и  $q(x)$  – два многочлена, оба проходят через одинаковые  $p$  точек
- Тогда  $f(x) - q(x)$  имеет не меньше  $p$  нулей – в точках через которые они проходят.
- А ещё  $f(x) - q(x)$  тоже степени не больше  $n - 1$ .
- Но  $f(x) - q(x)$  не может иметь  $p$  нулей! Это же больше его степени.
- А значит  $f(x) - q(x) = 0$  ■

# СХЕМА ШАМИРА

Опубликована в ноябре 1979 года, всего  
через полгода после схемы Блэкли.

**Идея:** через  $k$  точек можно провести  
единственный многочлен. Пусть  $s = f(0)$ .

Доли — точки на многочлене. Секрет — его  
значение в нуле.



# РЕАЛИЗАЦИЯ

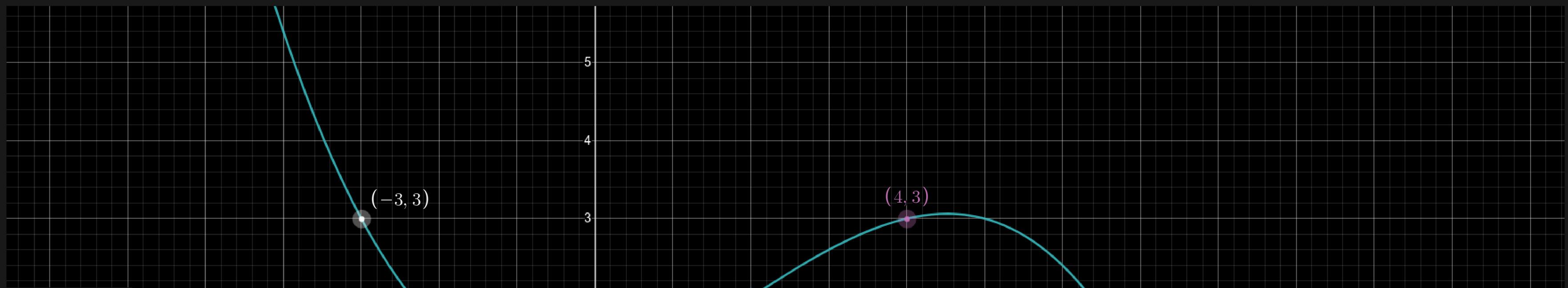
1. Выбрать достаточно большое поле (секрет должен поместиться).
2. Сгенерировать случайный многочлен степени  $k - 1$

$$f(x) = c_1x^{k-1} + c_2x^{k-2} + \dots + c_{k-2}x^2 + c_{k-1}x + s$$

Свободный член равен  $s$ , благодаря чему  $f(0) = s$

3. Посчитать значения в точках  $1, 2, 3, \dots, n$  и раздать их. То есть  $v_i = f(i)$ .  
Координата  $x$  точек — публичная информация.
4. По  $k$  любых из этих  $n$  точек можно построить  $f$  обратно. Тогда  $s = f(0)$ .

3. Посчитать значения в точках  $1, 2, 3, \dots, n$  и раздать их. То есть  $v_i = f(i)$ . Координата  $x$  точек — публичная информация.
4. По  $k$  любых из этих  $n$  точек можно построить  $f$  обратно. Тогда  $s = f(0)$ .



# ПРИМЕР

- Из поля  $\mathbb{Z}_{13}$  выбрали секрет  $s = 4$ .
- Три участника могут восстановить секрет. Используем многочлен второй степени.
- Сгенерируем такой:  $f(x) = 5x^2 + 11x + 4$ ; здесь  $s = f(0)$
- Посчитаем точки (над полем!):
  1.  $f(1) = 7$
  2.  $f(2) = 7$
  3.  $f(3) = 4$

Именно этой информацией обладают участники.

- Посчитаем точки (над полем!):

$$1. f(1) = 7$$

$$2. f(2) = 7$$

$$3. f(3) = 4$$

Именно этой информацией обладают участники.

- Восстановим многочлен (вычисления по модулю 13):

$$\begin{aligned} f(x) &= y_1 \frac{x - x_2}{x_1 - x_2} \frac{x - x_3}{x_1 - x_3} + y_2 \frac{x - x_1}{x_2 - x_1} \frac{x - x_3}{x_2 - x_3} + y_3 \frac{x - x_1}{x_3 - x_1} \frac{x - x_2}{x_3 - x_2} = \\ &= 7 \frac{x - 2}{1 - 2} \frac{x - 3}{1 - 3} + 7 \frac{x - 1}{2 - 1} \frac{x - 3}{2 - 3} + 4 \frac{x - 1}{3 - 1} \frac{x - 2}{3 - 2} = \\ &= \frac{7}{2}(x - 2)(x - 3) + \frac{7}{-1}(x - 1)(x - 3) + \frac{4}{2}(x - 1)(x - 2) = \end{aligned}$$

# СОВЕРШЕННОСТЬ

*For example, a polynomial of degree  $b$  can be reconstructed from its values at  $b + 1$  points. But already its values at any  $b$  points tell a lot about it. It can also be reconstructed from the values of its 0th through  $b$ th Taylor coefficients at a point. But already the values of any  $b$  of these  $b + 1$  numbers tell a lot about it.*

— Блэкли о многочленах

# СОВЕРШЕННОСТЬ

Мы знаем  $k - 1$  долей. Хотим узнать какой может быть секрет.

- Не используя знания долей, можем перебрать все секреты: их  $|\mathbb{F}|$  штук.
- Перебор вариантов последнего долей не легче: тоже  $|\mathbb{F}|$  вариантов.

# СОВЕРШЕННОСТЬ

Мы знаем  $k - 1$  долей. Хотим узнать какой может быть секрет.

- Не используя знания долей, можем перебрать все секреты: их  $|\mathbb{F}|$  штук.
- Перебор вариантов последнего долей не легче: тоже  $|\mathbb{F}|$  вариантов.
- Правда ли, что все секреты возможны?

# СОВЕРШЕННОСТЬ

Мы знаем  $k - 1$  долей. Хотим узнать какой может быть секрет.

- Не используя знания долей, можем перебрать все секреты: их  $|\mathbb{F}|$  штук.
- Перебор вариантов последнего долей не легче: тоже  $|\mathbb{F}|$  вариантов.
- Правда ли, что все секреты возможны?
- Можем ли построить многочлен степени  $k - 1$ , проходящий через всякий секрет и через известные  $k - 1$  точек?

# СОВЕРШЕННОСТЬ

Мы знаем  $k - 1$  долей. Хотим узнать какой может быть секрет.

- Не используя знания долей, можем перебрать все секреты: их  $|\mathbb{F}|$  штук.
- Перебор вариантов последнего долей не легче: тоже  $|\mathbb{F}|$  вариантов.
- Правда ли, что все секреты возможны?
- Можем ли построить многочлен степени  $k - 1$ , проходящий через всякий секрет и через известные  $k - 1$  точек?
- Конечно можем! Даны  $k$  точек, надо многочлен степени  $k - 1$ . Это легко и всегда возможно.

# СОВЕРШЕННОСТЬ

Мы знаем  $k - 1$  долей. Хотим узнать какой может быть секрет.

- Не используя знания долей, можем перебрать все секреты: их  $|\mathbb{F}|$  штук.
- Перебор вариантов последнего долей не легче: тоже  $|\mathbb{F}|$  вариантов.
- Правда ли, что все секреты возможны?
- Можем ли построить многочлен степени  $k - 1$ , проходящий через всякий секрет и через известные  $k - 1$  точек?
- Конечно можем! Даны  $k$  точек, надо многочлен степени  $k - 1$ . Это легко и всегда возможно.

Значит схема совершенна!

# ИДЕАЛЬНОСТЬ

- Размер доли равен размеру секрета?
- Конечно!  $f(0) \in \mathbb{F}$  и  $f(i) \in \mathbb{F}$
- Значит схема идеальна.

# О СОВЕРШЕННОСТИ

**Совершена ли следующая схема?**

1. Дан секрет  $0 \leq s \leq 100$
2. Генерируем  $k - 1$  случайный коэффициент  $c_i \in \mathbb{Z}_{100}$  и многочлен
$$f(x) = c_1x^{k-1} + c_2x^{k-2} + \dots + c_{k-2}x^2 + c_{k-1}x + s$$
3. ...

# О СОВЕРШЕННОСТИ

**Совершена ли следующая схема?**

1. Дан секрет  $0 \leq s \leq 100$
2. Генерируем  $k - 1$  случайный коэффициент  $c_i \in \mathbb{Z}_{100}$  и многочлен
$$f(x) = c_1x^{k-1} + c_2x^{k-2} + \dots + c_{k-2}x^2 + c_{k-1}x + s$$
3. ...

**Правильная и совершенная схема Шамира:**

1. Выбрать достаточно большое поле (секрет должен поместиться).
2. Сгенерировать случайный многочлен степени  $k - 1$ 
$$f(x) = c_1x^{k-1} + c_2x^{k-2} + \dots + c_{k-2}x^2 + c_{k-1}x + s$$
3. ...

# О СОВЕРШЕННОСТИ

**Совершена ли следующая схема?**

1. Дан секрет  $0 \leq s \leq 100$
2. Генерируем  $k - 1$  случайный коэффициент  $c_i \in \mathbb{Z}_{100}$  и многочлен
$$f(x) = c_1x^{k-1} + c_2x^{k-2} + \dots + c_{k-2}x^2 + c_{k-1}x + s$$
3. ...

**Правильная и совершенная схема Шамира:**

1. Выбрать достаточно большое **поле** (секрет должен поместиться).
2. Сгенерировать случайный многочлен степени  $k - 1$ 
$$f(x) = c_1x^{k-1} + c_2x^{k-2} + \dots + c_{k-2}x^2 + c_{k-1}x + s$$
3. ...

# АТАКА НА НЕ-ПОЛЕ

Известно кольцо:  $\mathbb{Z}_{30}$ .

В нём многочлен:  $y = c_0 + c_1x + c_2x^2 + c_3x^3$

Знаем три точки (из четырёх):

1.  $(1, 18)$
2.  $(2, 24)$
3.  $(3, 10)$
4.  $(4, y_4)$

Что мы знаем о секрете?

Подставим точки:  $(1, 18)$ ,  $(2, 24)$ ,  $(3, 10)$ ,  $(4, y_4)$  в уравнение  $y = c_0 + c_1x + c_2x^2 + c_3x^3$ , получим СЛАУ на коэффициенты:

$$\begin{cases} 18 = c_0 + c_1 \cdot 1 + c_2 \cdot 1 + c_3 \cdot 1 \\ 24 = c_0 + c_1 \cdot 2 + c_2 \cdot 4 + c_3 \cdot 8 \\ 10 = c_0 + c_1 \cdot 3 + c_2 \cdot 9 + c_3 \cdot 27 \\ y_4 = c_0 + c_1 \cdot 4 + c_2 \cdot 16 + c_3 \cdot 64 \end{cases}$$

Подставим точки:  $(1, 18)$ ,  $(2, 24)$ ,  $(3, 10)$ ,  $(4, y_4)$  в уравнение  $y = c_0 + c_1x + c_2x^2 + c_3x^3$ , получим СЛАУ на коэффициенты:

$$\begin{cases} 18 = c_0 + c_1 \cdot 1 + c_2 \cdot 1 + c_3 \cdot 1 \\ 24 = c_0 + c_1 \cdot 2 + c_2 \cdot 4 + c_3 \cdot 8 \\ 10 = c_0 + c_1 \cdot 3 + c_2 \cdot 9 + c_3 \cdot 27 \\ y_4 = c_0 + c_1 \cdot 4 + c_2 \cdot 16 + c_3 \cdot 64 \end{cases}$$

Решение:

$$c_0 = -y_4 - 32; \quad c_1 = \frac{11}{6}y_4 + 80; \quad c_2 = -y_4 - 34; \quad c_3 = \frac{1}{6}y_4 + 4$$

Подставим точки:  $(1, 18), (2, 24), (3, 10), (4, y_4)$  в уравнение  $y = c_0 + c_1x + c_2x^2 + c_3x^3$ , получим СЛАУ на коэффициенты:

$$\begin{cases} 18 = c_0 + c_1 \cdot 1 + c_2 \cdot 1 + c_3 \cdot 1 \\ 24 = c_0 + c_1 \cdot 2 + c_2 \cdot 4 + c_3 \cdot 8 \\ 10 = c_0 + c_1 \cdot 3 + c_2 \cdot 9 + c_3 \cdot 27 \\ y_4 = c_0 + c_1 \cdot 4 + c_2 \cdot 16 + c_3 \cdot 64 \end{cases}$$

Решение:

$$c_0 = -y_4 - 32; \quad c_1 = \frac{11}{6}y_4 + 80; \quad c_2 = -y_4 - 34; \quad c_3 = \frac{1}{6}y_4 + 4$$

В кольце  $\mathbb{Z}_{30}$  **можем** делить на: 1, 7, 11, 13, 17, 19, 23, 29.

Подставим точки:  $(1, 18), (2, 24), (3, 10), (4, y_4)$  в уравнение  $y = c_0 + c_1x + c_2x^2 + c_3x^3$ , получим СЛАУ на коэффициенты:

$$\begin{cases} 18 = c_0 + c_1 \cdot 1 + c_2 \cdot 1 + c_3 \cdot 1 \\ 24 = c_0 + c_1 \cdot 2 + c_2 \cdot 4 + c_3 \cdot 8 \\ 10 = c_0 + c_1 \cdot 3 + c_2 \cdot 9 + c_3 \cdot 27 \\ y_4 = c_0 + c_1 \cdot 4 + c_2 \cdot 16 + c_3 \cdot 64 \end{cases}$$

Решение:

$$c_0 = -y_4 - 32; \quad c_1 = \frac{11}{6}y_4 + 80; \quad c_2 = -y_4 - 34; \quad c_3 = \frac{1}{6}y_4 + 4$$

В кольце  $\mathbb{Z}_{30}$  **можем** делить на: 1, 7, 11, 13, 17, 19, 23, 29.

На **6 не можем**.

Значит  $y_4$  делится на 6. Значит  $y_4 \in \{0, 6, 12, 18, 24\}$ .

Всего 5 значений вместо 30!

# ЕЩЁ ПРО НЕ-ПОЛЕ

Интересный пример:

Используется  $\mathbb{Z}_{15}$ . Тогда:

1.  $f(x) = x^2 - 1$
2.  $g(x) = x^2 - 5x + 4$

у них разные секреты:  $f(0) = -1$ , но  $g(0) = 4$ .

# ЕЩЁ ПРО НЕ-ПОЛЕ

Интересный пример:

Используется  $\mathbb{Z}_{15}$ . Тогда:

1.  $f(x) = x^2 - 1$
2.  $g(x) = x^2 - 5x + 4$

у них разные секреты:  $f(0) = -1$ , но  $g(0) = 4$ .

Для восстановления обоих достаточно трёх участников. Выберем  $x = 1, x = 4, x = 7$ :

1.  $f(1) = 0, g(1) \equiv 0$
2.  $f(4) = 0, g(4) = 0$
3.  $f(7) \equiv 3, g(7) \equiv 3$

Получается, что **конкретно эти три** участника не способны восстановить секрет!

# АТАКИ

С внешними врагами разобрались, как делать схемы совершенными теперь знаем.

Но схемы разделения применяются когда нет доверия даже участникам!

Участники могут назвать вместо настоящей доли что-то своё. И никто не узнает!

А если сговорилось  $k - 1$  участников...

# АТАКА НА СХЕМУ ШАМИРА

**Имеется:** один участник — заговорщик

**Хочется:** узнать секрет одному, так чтобы другие его не знали

**Можем:** назвать другое число в качестве своей доли

**Знаем:** координаты  $x$  других участников

Как?

# АТАКА НА СХЕМУ ШАМИРА

**Имеется:** один участник — заговорщик

**Хочется:** узнать секрет одному, так чтобы другие его не знали

**Можем:** назвать другое число в качестве своей доли

**Знаем:** координаты  $x$  других участников

Как?

**Идея:** сдвинуть свою долю так, чтобы секрет от этого **предсказуемо сдвинулся**

# РЕАЛИЗАЦИЯ АТАКИ

## Обозначения:

- $(x_1, y_1)$  — «своя» точка (без потери общности первая).
- $t$  — насколько мы хотим изменить секрет.  $s' = s + t$
- $f$  — «настоящий» многочлен, проходит через  $(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)$ .
- $y'_1$  — поправленное значение «своей» доли. Хотим его найти.
- $f'$  — «ложный» многочлен, проходит через ложную точку  $(x_1, y'_1)$ .
- $s = f(0)$  и  $s' = f'(0) = s + t$  — восстановленные секреты: «настоящий» и «ложный» соответственно

**Атака:** Проводим многочлен  $g(x)$  через  $(0, t), (x_2, 0), (x_3, 0), \dots, (x_k, 0)$ . Тогда  $y'_1 = y_1 + g(x_1)$ .

То есть многочлен в нуле (где секрет) равен  $t$ , а в точках других участников равен нулю. Тогда  $y'_1 = y_1 + g(x_1) = f(x_1) + g(x_1)$

$g(x)$  проходит через  $(\mathbf{0}, t), (x_2, 0), (x_3, 0), \dots, (x_k, 0)$ . Тогда  $y'_1 = y_1 + g(x_1)$

Используем формулу Лагранжа:  $g(\textcolor{red}{x}) = \sum_{j=1}^n y_j \prod_{\substack{i=1 \\ i \neq j}}^k \frac{\textcolor{red}{x} - x_i}{x_j - x_i}$

Здесь из-за  $y_j = 0$  обнуляется всё кроме  $g(\textcolor{red}{x}) = t \prod_{i=2}^k \frac{\textcolor{red}{x} - x_i}{\mathbf{0} - x_i}$

Тогда  $g(x_1) = t \prod_{i=2}^k \frac{x_1 - x_i}{\mathbf{0} - x_i}$

Теперь в  $f(\textcolor{red}{x}) = \sum_{j=1}^n y_j \prod_{\substack{i=1 \\ i \neq j}}^k \frac{\textcolor{red}{x} - x_i}{x_j - x_i}$  вместо  $y_1$  поставим  $y'_1 = y_1 + g(x_1)$

Используем формулу Лагранжа:  $g(\textcolor{red}{x}) = \sum_{j=1}^n y_j \prod_{\substack{i=1 \\ i \neq j}}^{k-1} \frac{x - x_i}{x_j - x_i}$

Здесь из-за  $y_j = 0$  обнуляется всё кроме  $g(\textcolor{red}{x}) = t \prod_{i=2}^k \frac{\textcolor{red}{x} - x_i}{\textcolor{blue}{0} - x_i}$

Тогда  $g(x_1) = t \prod_{i=2}^k \frac{x_1 - x_i}{\textcolor{blue}{0} - x_i}$

Теперь в  $f(\textcolor{red}{x}) = \sum_{j=1}^n y_j \prod_{\substack{i=1 \\ i \neq j}}^{k-1} \frac{\textcolor{red}{x} - x_i}{x_j - x_i}$  вместо  $y_1$  поставим  $y'_1 = y_1 + g(x_1)$

$$f(\textcolor{red}{x}) = \left( \sum_{j=1}^n y_j \prod_{i=1}^{k-1} \frac{\textcolor{red}{x} - x_i}{x_j - x_i} \right) + \underbrace{\left( \sum_{i=2}^k \frac{y'_1 + g(x_1)}{x_1 - x_i} \right)}_{g(x_1)} \left( \prod_{i=2}^k \frac{\textcolor{blue}{0} - x_i}{x_1 - x_i} \right)$$

# ЗАЩИТА ОТ ЭТОЙ АТАКИ

Очень просто:

1. Выбирать  $x_i$  для долей случайно среди всех возможных.
2. Сделать эту информацию секретной.

Тогда доля содержит всю пару  $(x, y)$  и схема больше не идеальна.

# СТРУКТУРЫ ДОСТУПА

- Множество всех долей:  $P = \{p_1, p_2, \dots, p_n\}$ 
  - Число долей может не совпадать с числом участников
- Структура доступа:  $\Gamma \subseteq \mathcal{P}(P)$
- Секрет могут получить только те подмножества, которые лежат в  $\Gamma$ .
- Пороговая схема — любые  $k$  могут получить секрет
- $\Gamma$  — монотонная структура: если  $A \in \Gamma$  и  $A \subset B$ , то  $B \in \Gamma$ 
  - Эквивалентно,  $A \in \Gamma \rightarrow \forall i(A \cup \{p_i\}) \in \Gamma$

# ПРОСТЫЕ СТРУКТУРЫ ДОСТУПА

**Задача:** разделить секрет так, чтобы:

1. CEO и CTO компании могли вдвоём восстановить секрет
2. ... или три бухгалтера
3. ... или же пять обычных сотрудников

# ПРОСТЫЕ СТРУКТУРЫ ДОСТУПА

**Задача:** разделить секрет так, чтобы:

1. CEO и CTO компании могли вдвоём восстановить секрет
2. ... или три бухгалтера
3. ... или же пять обычных сотрудников

**Сделаем так:**

- CEO и CTO получат по 15 долей
- Каждый бухгалтер получит 10 долей
- Каждый сотрудник получит 6 долей

И тогда получим пороговую схему с  $k = 30$

**Задача:** разделить секрет так, чтобы:

1. CEO и CTO компании могли вдвоём восстановить секрет
2. ... или три бухгалтера
3. ... или же пять обычных сотрудников

**Сделаем так:**

- CEO и CTO получат по 15 долей
- Каждый бухгалтер получит 10 долей
- Каждый сотрудник получит 6 долей

И тогда получим пороговую схему с  $k = 30$

**Откуда числа?**

- $k = \text{НОК}(2, 3, 5) = 30$
- CEO и CTO:  $\frac{30}{2} = 15$
- Бухгалтеры:  $\frac{30}{3} = 10$

# МАТРОИДЫ

**Определение:** это пара из двух множеств –  $\langle X, I \rangle$ :

- $X$  – «носитель матроида», произвольное множество
- $I$  – «независимые подмножества»  $X$ . Т.е.  $I \subseteq \mathcal{P}(X)$

Такие что:

1.  $\emptyset \in I$  (т.е.  $I$  не пусто)
2. Если  $A \in I$  и  $B \subset A$ , то  $B \in I$
3. Если  $A, B \in I$  и  $|B| < |A|$ , то  $\exists x \in A \setminus B : A \cup \{x\} \in I$ 
  - Можем расширить  $B$  новым элементом из  $A$

**Соглашение:** Если  $A \in I$ , то говорим, что  $A$  независимо (и наоборот).

# УНИВЕРСАЛЬНЫЙ МАТРОИД

- $X$  – произвольное множество
  - $V$  – все подмножества, мощности не больше некоторого  $k \in \mathbb{N}$ 
    1. Поскольку  $|\emptyset| \leq k$ , то  $\emptyset \in V$
    2. Если  $A \in I$ , то  $|A| \leq k$ . Если  $B \subset A$ , то  $|B| < k$ , а значит  $B \in I$ .
    3. Если  $A \in I$ , то  $|A| \leq k$ . Если  $|B| < |A|$ , то  $|B| < k$ . Отсюда  $|B \cup \{x\}| \leq k$ , а значит  $B \cup \{x\} \in I$
- 

Матроид это...

такие  $\langle X, I \rangle$ , что:

1.  $\emptyset \in I$
2. Если  $A \in I$  и  $B \subset A$ , то  $B \in I$
3. Если  $A, B \in I$  и  $|B| < |A|$ , то  $\exists x \in A \setminus B : A \cup \{x\} \in I$

# ЦВЕТНОЙ МАТРОИД

- $X$  – элементы, каждый раскрашен в какой-то цвет
- $V$  – все подмножества  $X$ , в которых все элементы разных цветов

Тогда:

1. В пустом множестве все элементы разных цветов (vacuous truth)
2. Если в  $A$  элементы разных цветов, то и во всяком его подмножестве  $B$  они тоже разных цветов.
3. И в  $A$ , и в  $B$  все элементы разных цветов. Т.к.  $|A| > |B|$ , то в  $A$  больше цветов, чем в  $B$ . Значит найдётся  $x \in A \setminus B$  такого цвета, которого нет в  $B$ . И тогда  $B \cup x \in I$

---

Матроид это...

1.  $\emptyset \in I$

такие  $\langle X, I \rangle$ , что:

2. Если  $A \in I$  и  $B \subset A$ , то  $B \in I$

3. Если  $A, B \in I$  и  $|B| < |A|$ , то  $\exists x \in A \setminus B : A \cup \{x\} \in I$

# ЛИНЕЙНЫЙ МАТРОИД

- $X$  – вектора из какого-то линейного пространства
- $V$  – все подмножества  $X$ , в которых вектора линейно независимы

Тогда:

1. В пустом множестве все вектора л.н.з. (vacuous truth)
2. Если в  $A$  вектора л.н.з., то и во всяком его подмножестве  $B$  они тоже раных цветов.
3. Вектора в  $B$  л.н.з., значит  $\dim L(B) = |B|$ . Поскольку  $|A| > |B|$ , то в  $A$  найдется вектор  $x$ , не входящий в линейную оболочку  $L(B)$ . Тогда он будет л.н.з. с векторами из  $B$ . Т.е.  $B \cup x \in I$ .

---

Матроид это...

такие  $\langle X, I \rangle$ , что:

$$1. \emptyset \in I$$

$$2. \text{Если } A \in I \text{ и } B \subset A, \text{ то } B \in I$$

$$3. \text{Если } A, B \in I \text{ и } |B| < |A|, \text{ то } \exists x \in A \setminus B : A \cup \{x\} \in I$$

# МАТРОИД ВАМОСА

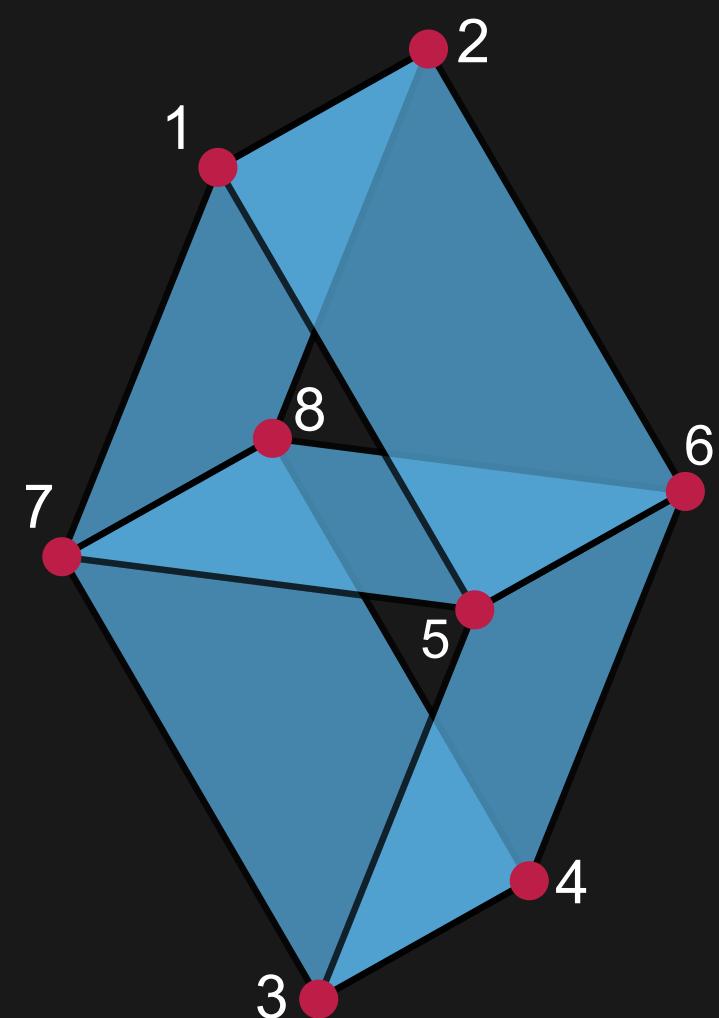
- $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$
- Подмножество  $A$  **независимо**, если и только если  $A \leq 4$  и его нет на картинке.

Известно, что **этот матроид не является линейным**.

Другое (но равносильное) определение:

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.



Например,  $\{1, 2, 5, 6\} \notin V$  — оно зависимо, а  $\{1, 2, 3, 4\} \in V$  — независимо.

# СВЯЗЬ СХЕМ РАЗДЕЛЕНИЯ И МАТРОИДОВ

- Носитель матроида ( $X$ ) — участники схемы
- Зависимые подмножества ( $\mathcal{P}(X) \setminus V$ ) — подмножества участников, могущие восстановить секрет

Например, универсальный матроид (где  $A \in V \Leftrightarrow |A| < k$ ) соответствует  $(n, k)$  схеме

Тогда верны следующие утверждения:

1. Не любой матроид может быть реализован как **идеальная** СРС (например, матроид Вamosа)
2. Но всякий **линейный** матроид (над полем) реализуется как **идеальная** СРС
3. Любой идеальной СРС соответствует матроид (не обязательно линейный)
4. Не всякая структура доступа может быть реализована идеально
5. (★) Однако для любой структуры доступа можно построить **совершенную** СРС
6. Идеальных СРС больше, чем линейных матроидов (и меньше, чем всех матроидов)

\**CPC* — схема разделения секрета

# СЛОЖНЫЕ СТРУКТУРЫ ДОСТУПА

Участники:

- Алиса ( $a$ ) и Берта ( $b$ )
- Степан ( $c$ ) и Денис ( $d$ )

Хотим:

- Алиса и Берта вместе могут восстановить секрет
- Степан и Денис тоже могут
- Но чтобы никак по-другому было нельзя!

Например, Алиса и Степан не могли восстановить секрет.

Структура доступа:  $\Gamma = \{\{a, b\}, \{c, d\}, \dots\}$

# СЛОЖНЫЕ СТРУКТУРЫ ДОСТУПА

Участники:

- Алиса ( $a$ ) и Берта ( $b$ )
- Степан ( $c$ ) и Денис ( $d$ )

Хотим:

- Алиса и Берта вместе могут восстановить секрет
- Степан и Денис тоже могут
- Но чтобы никак по-другому было нельзя!

Например, Алиса и Степан не могли восстановить секрет.

Структура доступа:  $\Gamma = \{\{a, b\}, \{c, d\}, \dots\}$

Проблема: пороговая схема это не позволяет.

Хотим:

- Алиса и Берта вместе могут восстановить секрет
- Степан и Денис тоже могут
- Но чтобы никак по-другому было нельзя!

Например, Алиса и Степан не могли восстановить секрет.

Структура доступа:  $\Gamma = \{\{a, b\}, \{c, d\}, \dots\}$

Проблема: пороговая схема это не позволяет.

**Доказательство:**

1. Участники  $a, b, c, d$  получат каждый по  $w_a, w_b, w_c, w_d$  долей, соответственно.
2.  $a$  и  $b$  могут восстановить секрет:  $w_a + w_b \geq k$
3. Скажем, что  $w_a \geq w_b$  (и  $w_c \geq w_d$ )
4. Тогда  $w_a \geq w_b \implies w_a + w_a \geq w_a + w_b \geq k \implies w_a \geq k/2$
5. Аналогично с другой парой:  $w_c + w_d \geq k$  и  $w_c \geq k/2$
6. Теперь рассмотрим пару  $a$  и  $c$ . Получаем  $w_a + w_c \geq k/2 + k/2 = k$

Значит  $a$  и  $c$  смогут восстановить секрет. Противоречие.

# БУЛЕВЫ ФУНКЦИИ

Структура доступа:  $\Gamma = \{\{a, b\}, \{c, d\}, \dots\}$

Соответствующая функция:  $f(a, b, c, d) = (a \wedge b) \vee (c \wedge d)$

Хотим:  $f(v_1, v_2, \dots, v_k) \leftrightarrow (\{v_1, v_2, \dots, v_k\} \in \Gamma)$  для всяких  $v_1, \dots, v_k$



# РЕШЕНИЕ ПРИМЕРА

Как разделить секрет в соответствии с  $f(a, b, c, d) = (a \wedge b) \vee (c \wedge d)$ ?

1. Разделить секрет между  $a$  и  $b$
2. Снова разделить тот же секрет между  $c$  и  $d$

Получим две раздельные схемы для одного секрета.

# В ОБЩЕМ СЛУЧАЕ

Хотим разделить секрет  $s$  в соответствии с формулой  $F$ .

Обозначим это как  $\$(s; F)$ , где  $\$(s; F)$  — множество пар: какой участник какой долей владеет.

# В ОБЩЕМ СЛУЧАЕ

Хотим разделить секрет  $s$  в соответствии с формулой  $F$ .

Обозначим это как  $\$(s; F)$ , где  $\$(s; F)$  — множество пар: какой участник какой долей владеет.

Пусть  $v_1, \dots, v_n$  — участники. Тогда зададим  $\$(s; F)$  рекуррентно:

1.  $\$(s; v_i) = \{(v_i, s)\}$  — просто передать участнику эту долю (или весь секрет)
2.  $\$(s; f \vee g) = \$(s; f) \cup \$(s; g)$  — если надо чтобы и  $f$ , и  $g$  могли восстановить секрет, то разделить его между ними по отдельности
3.  $\$(s; f \wedge g) = \$(s_1; f) \cup \$(s_2; g)$ , где  $s = s_1 + s_2$  — если надо чтобы  $f$  и  $g$  только вместе могли восстановить секрет, то разделить его на сумму и раздать слагаемые (вспомните самую первую  $(n, n)$ -схему)

# В ОБЩЕМ СЛУЧАЕ

Хотим разделить секрет  $s$  в соответствии с формулой  $F$ .

Обозначим это как  $\$(s; F)$ , где  $\$(s; F)$  — множество пар: какой участник какой долей владеет.

Пусть  $v_1, \dots, v_n$  — участники. Тогда зададим  $\$(s; F)$  рекуррентно:

1.  $\$(s; v_i) = \{(v_i, s)\}$  — просто передать участнику эту долю (или весь секрет)
2.  $\$(s; f \vee g) = \$(s; f) \cup \$(s; g)$  — если надо чтобы и  $f$ , и  $g$  могли восстановить секрет, то разделить его между ними по отдельности
3.  $\$(s; f \wedge g) = \$(s_1; f) \cup \$(s_2; g)$ , где  $s = s_1 + s_2$  — если надо чтобы  $f$  и  $g$  только вместе могли восстановить секрет, то разделить его на сумму и раздать слагаемые (вспомните самую первую  $(n, n)$ -схему)

# В ОБЩЕМ СЛУЧАЕ

Хотим разделить секрет  $s$  в соответствии с формулой  $F$ .

Обозначим это как  $\$(s; F)$ , где  $\$(s; F)$  — множество пар: какой участник какой долей владеет.

Пусть  $v_1, \dots, v_n$  — участники. Тогда зададим  $\$(s; F)$  рекуррентно:

1.  $\$(s; v_i) = \{(v_i, s)\}$  — просто передать участнику эту долю (или весь секрет)
2.  $\$(s; f \vee g) = \$(s; f) \cup \$(s; g)$  — если надо чтобы и  $f$ , и  $g$  могли восстановить секрет, то разделить его между ними по отдельности
3.  $\$(s; f \wedge g) = \$(s_1; f) \cup \$(s_2; g)$ , где  $s = s_1 + s_2$  — если надо чтобы  $f$  и  $g$  только вместе могли восстановить секрет, то разделить его на сумму и раздать слагаемые (вспомните самую первую  $(n, n)$ -схему)

# В ОБЩЕМ СЛУЧАЕ

Хотим разделить секрет  $s$  в соответствии с формулой  $F$ .

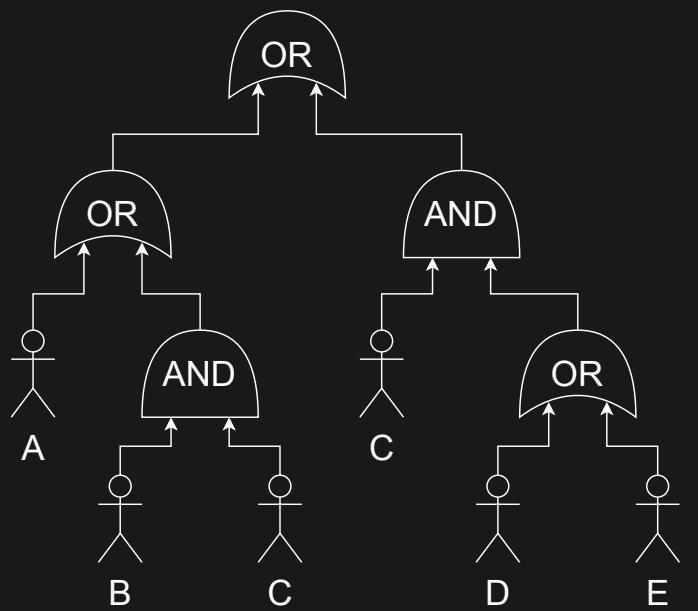
Обозначим это как  $\$(s; F)$ , где  $\$(s; F)$  — множество пар: какой участник какой долей владеет.

Пусть  $v_1, \dots, v_n$  — участники. Тогда зададим  $\$(s; F)$  рекуррентно:

1.  $\$(s; v_i) = \{(v_i, s)\}$  — просто передать участнику эту долю (или весь секрет)
2.  $\$(s; f \vee g) = \$(s; f) \cup \$(s; g)$  — если надо чтобы и  $f$ , и  $g$  могли восстановить секрет, то разделить его между ними по отдельности
3.  $\$(s; f \wedge g) = \$(s_1; f) \cup \$(s_2; g)$ , где  $s = s_1 + s_2$  — если надо чтобы  $f$  и  $g$  только вместе могли восстановить секрет, то разделить его на сумму и раздать слагаемые (вспомните самую первую  $(n, n)$ -схему)

# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

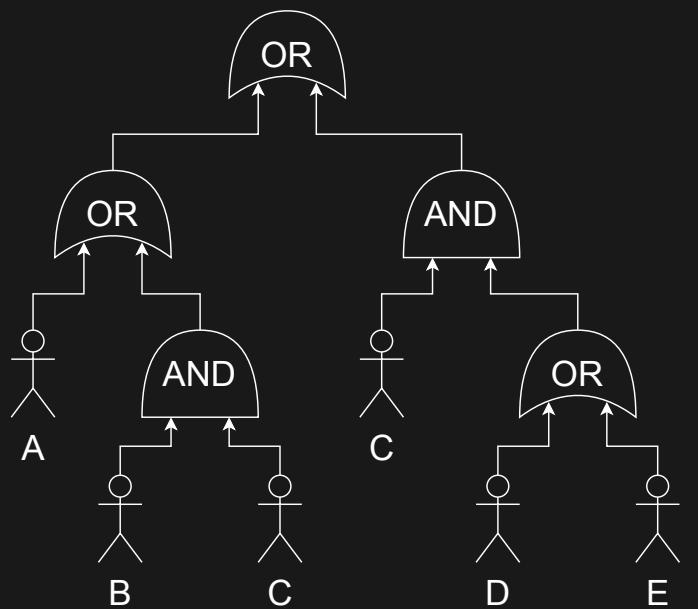
Формула:  $F(a, b, c, d, e) = (a \vee (b \wedge c)) \vee (c \wedge (d \vee e))$ . Надо разделить секрет  $s$ .



# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

Формула:  $F(a, b, c, d, e) = (a \vee (b \wedge c)) \vee (c \wedge (d \vee e))$ . Надо разделить секрет  $s$ .

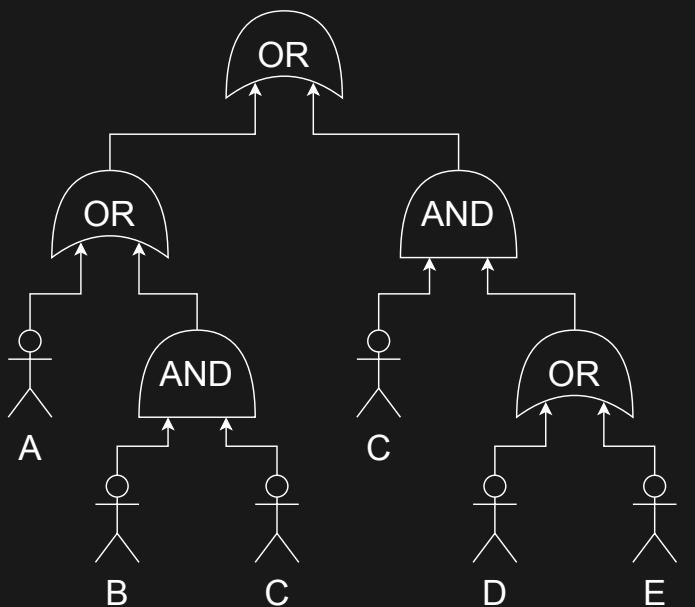
1.  $\$(s; F) = \$s; a \vee (b \wedge c) \cup \$s; c \wedge (d \vee e)$



# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

Формула:  $F(a, b, c, d, e) = (\underline{a \vee (b \wedge c)}) \vee (c \wedge (d \vee e))$ . Надо разделить секрет  $s$ .

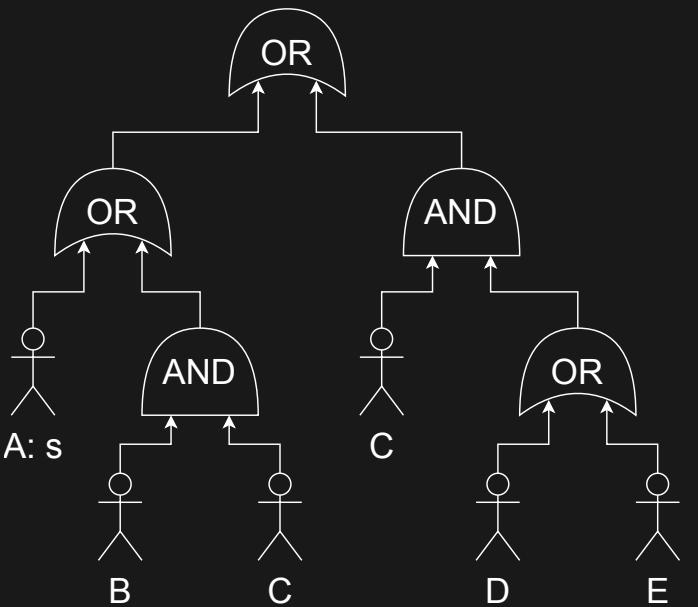
1.  $\$(s; F) = \$\underline{(s; a \vee (b \wedge c))} \cup \$\underline{(s; c \wedge (d \vee e))}$
2.  $\$(s; a \vee (b \wedge c)) = \$\underline{(s; a)} \cup \$\underline{(s; b \wedge c)}$



# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

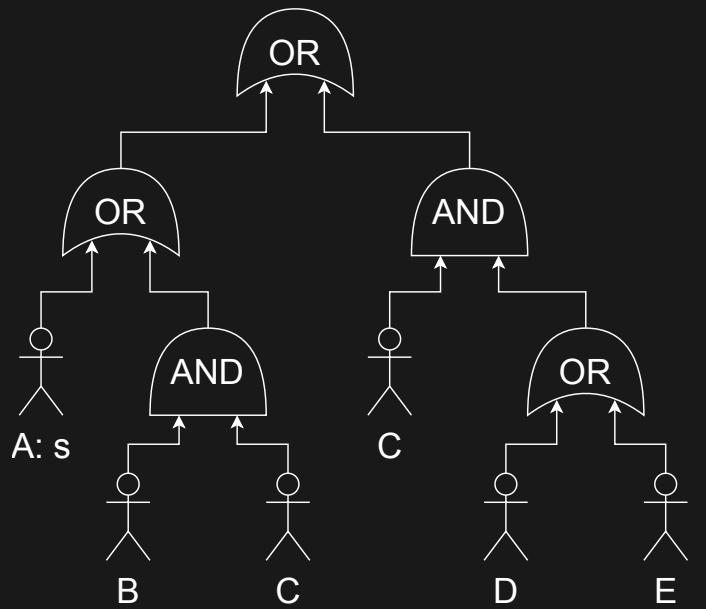
Формула:  $F(a, b, c, d, e) = (\underline{a} \vee (b \wedge c)) \vee (c \wedge (d \vee e))$ . Надо разделить секрет  $s$ .

1.  $\$(s; F) = \$\underline{(s; a \vee (b \wedge c)) \vee (c \wedge (d \vee e))}$
2.  $\$(s; a \vee (b \wedge c)) = \$\underline{(s; a) \cup (s; b \wedge c)}$
3.  $\$(s; \underline{a}) = \{(a, s)\}$



# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

Формула:  $F(a, b, c, d, e) = (a \vee (\underline{b \wedge c})) \vee (c \wedge (d \vee e))$ . Надо разделить секрет  $s$ .

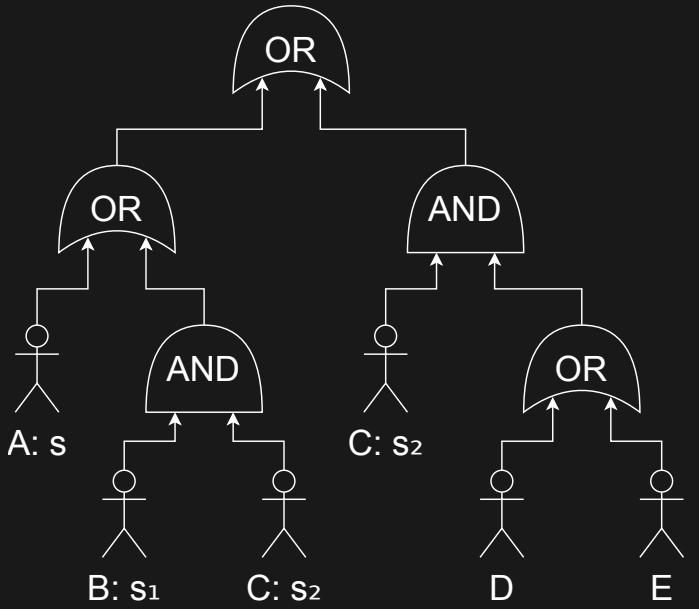


1.  $\$(s; F) = \$(s; a \vee (\underline{b \wedge c})) \cup \$(s; c \wedge (d \vee e))$
2.  $\$(s; a \vee (\underline{b \wedge c})) = \$(s; a) \cup \$(s; \underline{b \wedge c})$
3.  $\$(s; \underline{a}) = \{(a, s)\}$
4.  $\$(s; \underline{b \wedge c}) = \$(s_1; \underline{b}) \cup \$(s_2; \underline{c}),$   
где  $s = s_1 + s_2$

$$s_1 + s_2 = s$$

# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

Формула:  $F(a, b, c, d, e) = (a \vee (\underline{b} \wedge \underline{c})) \vee (c \wedge (d \vee e))$ . Надо разделить секрет  $s$ .

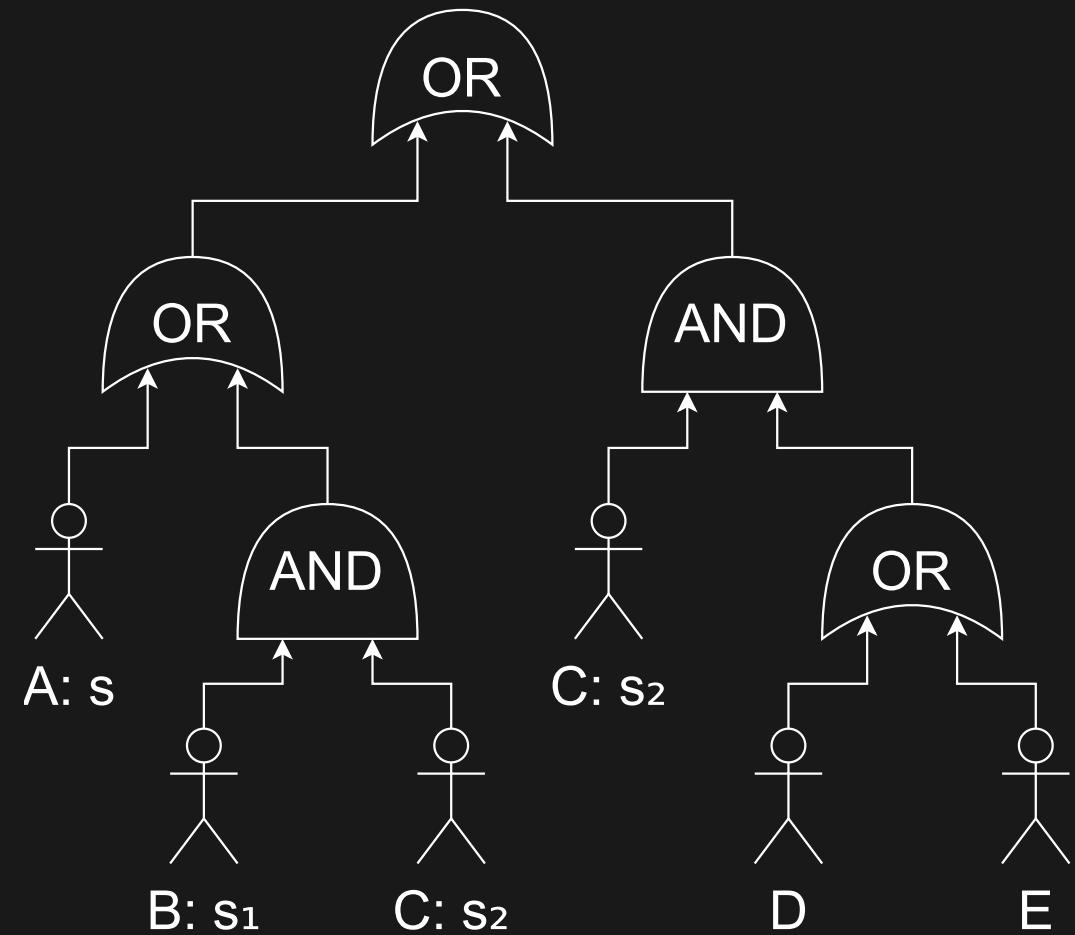


1.  $\$(s; F) = \$\!(s; \textcolor{green}{a} \vee (\textcolor{brown}{b} \wedge \textcolor{brown}{c})) \cup \$\!(s; \textcolor{brown}{c} \wedge (\textcolor{brown}{d} \vee \textcolor{brown}{e}))$
2.  $\$(s; a \vee (\underline{b} \wedge \underline{c})) = \$\!(s; \textcolor{green}{a}) \cup \$\!(s; \textcolor{brown}{b} \wedge \textcolor{brown}{c})$
3.  $\$(s; \underline{a}) = \{(a, s)\}$
4.  $\$(s; \underline{b} \wedge \underline{c}) = \$\!(s_1; \textcolor{green}{b}) \cup \$\!(s_2; \textcolor{brown}{c}),$   
где  $s = s_1 + s_2$
5.  $\$(s_1; \underline{b}) = \{(b, s_1)\}$  и  $\$(s_2; \underline{c}) = \{(c, s_2)\}$

$$s_1 + s_2 = s$$

# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

Формула:  $F(a, b, c, d, e) = (a \vee (b \wedge c)) \vee (\underline{c} \wedge (\underline{d} \vee e))$ . Надо разделить секрет  $s$ .

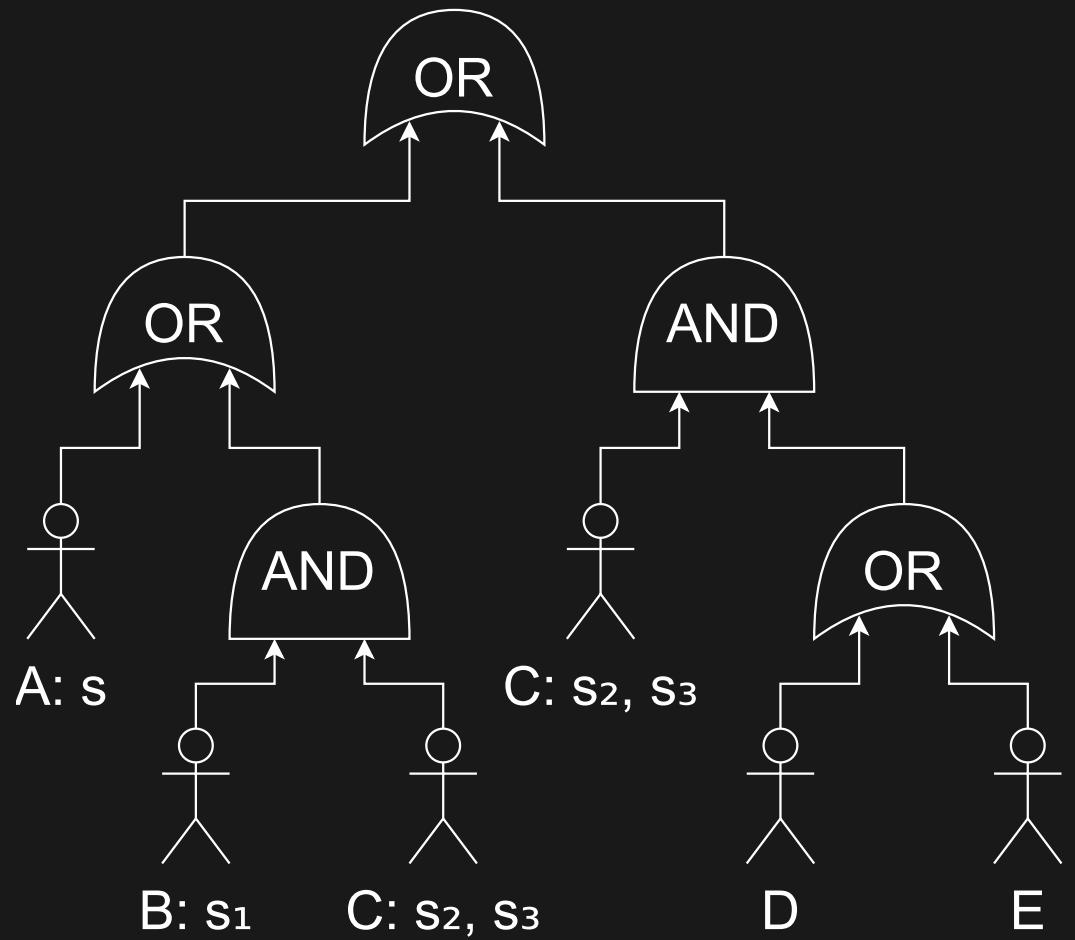


1.  $\$(s; F) = \$(s; \underline{a} \vee (\underline{b} \wedge \underline{c})) \cup \$(s; \underline{c} \wedge (\underline{d} \vee \underline{e}))$
2.  $\$(s; \underline{a} \vee (\underline{b} \wedge \underline{c})) = \$(s; \underline{a}) \cup \$(s; \underline{b} \wedge \underline{c})$
3.  $\$(s; \underline{a}) = \{(a, s)\}$
4.  $\$(s; \underline{b} \wedge \underline{c}) = \$(s_1; \underline{b}) \cup \$(s_2; \underline{c}),$   
где  $s = s_1 + s_2$
5.  $\$(s_1; \underline{b}) = \{(b, s_1)\}$  и  $\$(s_2; \underline{c}) = \{(c, s_2)\}$
6.  $\$(s; \underline{c} \wedge (\underline{d} \vee \underline{e})) = \$(s_3; \underline{c}) \cup \$(s_4; \underline{d} \vee \underline{e}),$   
где  $s = s_3 + s_4$

$$s_1 + s_2 = s; \quad s_3 + s_4 = s$$

# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

Формула:  $F(a, b, c, d, e) = (a \vee (b \wedge c)) \vee (\underline{c} \wedge (d \vee e))$ . Надо разделить секрет  $s$ .

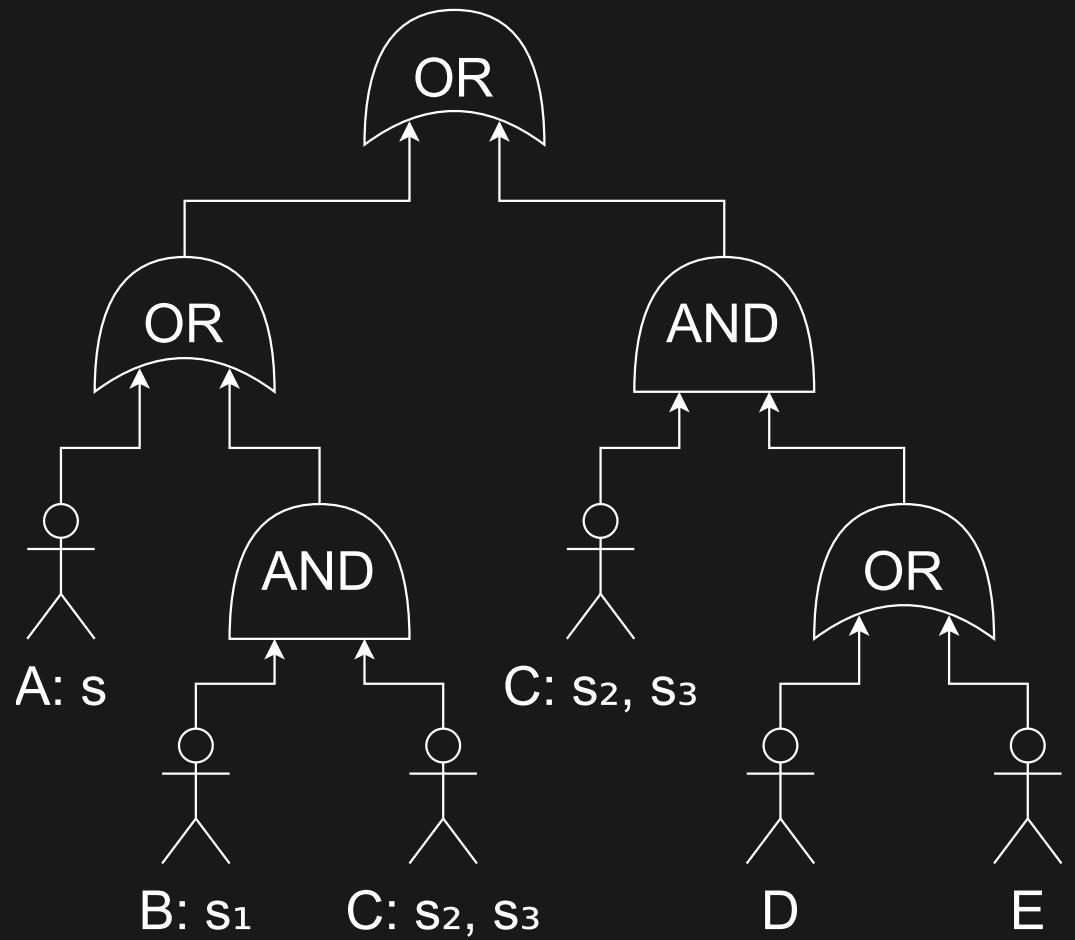


$$s_1 + s_2 = s; \quad s_3 + s_4 = s$$

1.  $\$(s; F) = \$\underbrace{(s; a \vee (b \wedge c))}_{\$s; a} \cup \$\underbrace{(s; c \wedge (d \vee e))}_{\$s; c}$
2.  $\$(s; a \vee (b \wedge c)) = \$\underbrace{(s; a)}_{\$s; a} \cup \$\underbrace{(s; b \wedge c)}_{\$s; b \wedge c}$
3.  $\$(s; \underline{a}) = \{(a, s)\}$
4.  $\$(s; \underline{b \wedge c}) = \$\underbrace{(s_1; b)}_{\$s_1; b} \cup \$\underbrace{(s_2; c)}_{\$s_2; c}$ ,  
где  $s = s_1 + s_2$
5.  $\$(s_1; \underline{b}) = \{(b, s_1)\}$  и  $\$(s_2; \underline{c}) = \{(c, s_2)\}$
6.  $\$(s; \underline{c \wedge (d \vee e)}) = \$\underbrace{(s_3; c)}_{\$s_3; c} \cup \$\underbrace{(s_4; d \vee e)}_{\$s_4; d \vee e}$ ,  
где  $s = s_3 + s_4$
7.  $\$(s_3; \underline{c}) = \{(c, s_3)\}$

# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

Формула:  $F(a, b, c, d, e) = (a \vee (b \wedge c)) \vee (c \wedge (\underline{d} \vee \underline{e}))$ . Надо разделить секрет  $s$ .

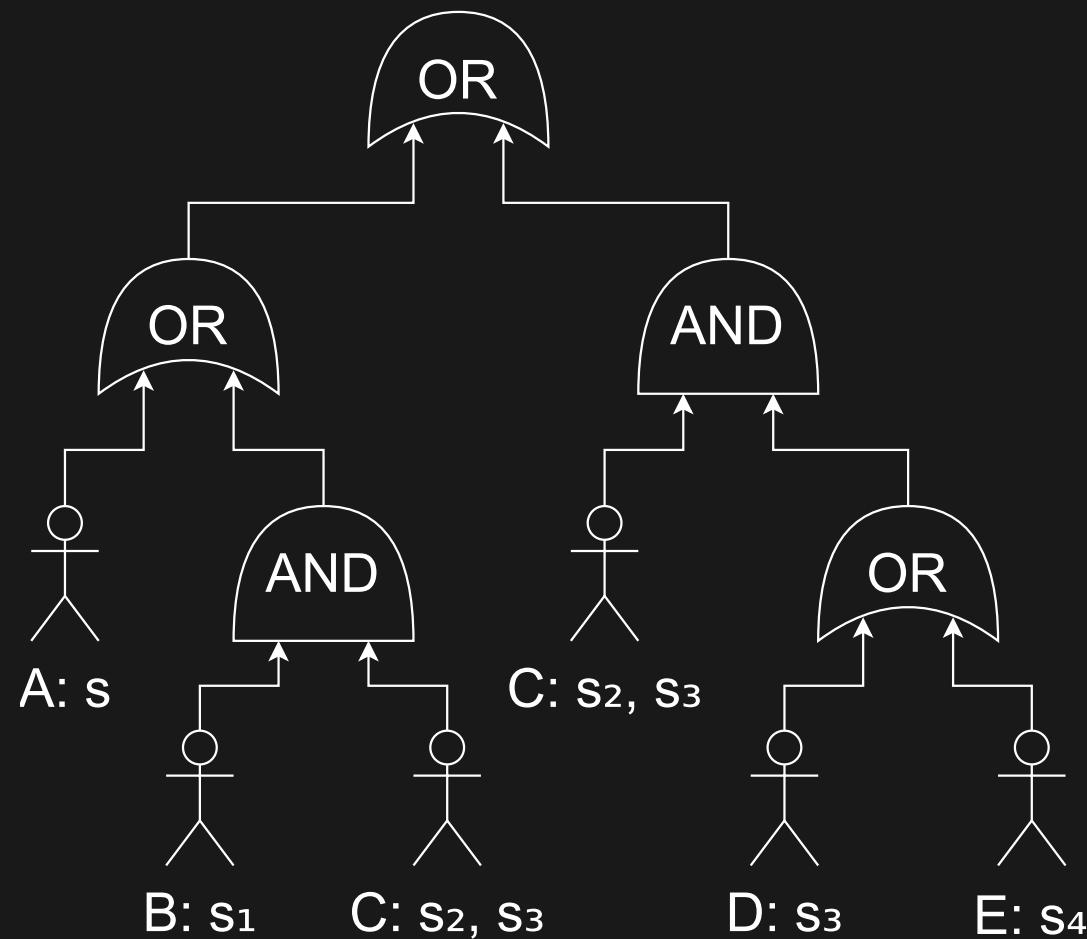


$$s_1 + s_2 = s; \quad s_3 + s_4 = s$$

1.  $\$(s; F) = \$\$(s; a \vee (b \wedge c)) \cup \$\$(s; c \wedge (\underline{d} \vee \underline{e}))$
2.  $\$(s; a \vee (b \wedge c)) = \$\$(s; a) \cup \$\$(s; b \wedge c)$
3.  $\$(s; \underline{a}) = \{(a, s)\}$
4.  $\$(s; \underline{b} \wedge c) = \$\$(s_1; b) \cup \$\$(s_2; c)$ ,  
где  $s = s_1 + s_2$
5.  $\$(s_1; \underline{b}) = \{(b, s_1)\}$  и  $\$(s_2; \underline{c}) = \{(c, s_2)\}$
6.  $\$(s; c \wedge (\underline{d} \vee \underline{e})) = \$\$(s_3; c) \cup \$\$(s_4; d \vee e)$ ,  
где  $s = s_3 + s_4$
7.  $\$(s_3; \underline{c}) = \{(c, s_3)\}$
8.  $\$(s_4; \underline{d} \vee e) = \$\$(s_4; d) \cup \$\$(s_4; e)$

# ПРИМЕР СЛОЖНОГО РАЗДЕЛЕНИЯ

Формула:  $F(a, b, c, d, e) = (a \vee (b \wedge c)) \vee (c \wedge (\underline{d} \vee \underline{e}))$ . Надо разделить секрет  $s$ .



$$s_1 + s_2 = s; \quad s_3 + s_4 = s$$

1.  $\$(s; F) = \$\$(s; a \vee (b \wedge c)) \cup \$\$(s; c \wedge (\underline{d} \vee \underline{e}))$
2.  $\$(s; a \vee (b \wedge c)) = \$\$(s; a) \cup \$\$(s; b \wedge c)$
3.  $\$(s; \underline{a}) = \{(a, s)\}$
4.  $\$(s; \underline{b} \wedge c) = \$\$(s_1; b) \cup \$\$(s_2; c)$ ,  
где  $s = s_1 + s_2$
5.  $\$(s_1; \underline{b}) = \{(b, s_1)\}$  и  $\$(s_2; \underline{c}) = \{(c, s_2)\}$
6.  $\$(s; c \wedge (\underline{d} \vee \underline{e})) = \$\$(s_3; c) \cup \$\$(s_4; d \vee e)$ ,  
где  $s = s_3 + s_4$
7.  $\$(s_3; \underline{c}) = \{(c, s_3)\}$
8.  $\$(s_4; \underline{d} \vee e) = \$\$(s_4; d) \cup \$\$(s_4; e)$
9.  $\$(s_4; \underline{d}) = \{(d, s_4)\}$  и  $\$(s_4; \underline{e}) = \{(e, s_4)\}$

# ОПТИМИЗИРУЕМ

Хотим разделить секрет, чтобы любые 3 из 5 могли его восстановить.

- Легко при помощи пороговых  $(n, k)$  схем ( $n = 5, k = 3$ )
- Сложно через функции:  $F(a, b, c, d, e) = (a \wedge b \wedge c) \vee (a \wedge b \wedge e) \vee \dots \vee (c \wedge d \wedge e)$  – всего  $C_n^k = 10$  слагаемых

Это плохо.

# ОПТИМИЗИРУЕМ

Хотим разделить секрет, чтобы любые 3 из 5 могли его восстановить.

- Легко при помощи пороговых  $(n, k)$  схем ( $n = 5, k = 3$ )
- Сложно через функции:  $F(a, b, c, d, e) = (a \wedge b \wedge c) \vee (a \wedge b \wedge e) \vee \dots \vee (c \wedge d \wedge e)$  – всего  $C_n^k = 10$  слагаемых

Это плохо.

Дополнительно к  $\wedge$  и  $\vee$  добавим оператор:  $\text{THRESHOLD}_k(F_1, F_2, \dots, F_n)$  – это выражение истинно тогда и только тогда, когда не меньше  $k$  аргументов истинны.

Тогда:  $\$(s; \text{THRESHOLD}_k(F_1, \dots, F_n)) = \bigcup_{1 \leq i \leq n} \$(s_i; F_i)$ , где  $s_i$  – доли, полученные при помощи эффективной пороговой схемы.

Т.е. чтобы вычислить  $\$(s; \text{THRESHOLD}_k(F_1, \dots, F_n))$  нужно

1. Разделить  $s$  при помощи пороговой схемы и получить  $s_1, s_2, \dots, s_n$
2. Каждую долю распределить между соответствующей группой:  $\$(s_1; F_1)$

# ИСТОЧНИКИ

1. Введение в криптографию. Под редакцией В.В.Ященко
2. “Safeguarding cryptographic keys”, G. R. Blakley, 1979
3. “On secret sharing systems”, E. Karnin, J. Greene and M. Hellman, 1983
4. “Generalized secret sharing and monotone functions.”, Benaloh, Josh, and Jerry Leichter, 1988
5. “How to share a secret with cheaters.”, Tompa, Martin, and Heather Woll., 1989

# СПАСИБО ЗА ВНИМАНИЕ

- Презентация с комментариями
- Варианты ДЗ
- Калькулятор СЛАУ

<https://secret-sharing.sldr.xyz>

