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

Носов Андрей БПИ-232

18 ноября 2024 г.

Определение

- Схема разделения секрета (СРС) — это криптографический протокол, позволяющий разделить секрет S на n долей $S_1, S_2, \ldots, S_n$, так что:
  - Любая подгруппа участников размером k или более может восстановить секрет.
  - Любая подгруппа из менее чем k участников ничего не знает о секрете.

Участники и дилер

- **Дилер** — доверенное лицо, которое:
  - Генерирует секрет S.
  - Вычисляет n долей $S_1, S_2, \ldots, S_n$.
  - Передаёт доли участникам.
- **Участники** — лица, получающие доли секрета. Они объединяются для восстановления секрета.

Функции разделения и восстановления секрета

- **Функция разделения**:

$$\text{Share}(S) \rightarrow \{S_1, S_2, \ldots, S_n\}$$

Разбивает секрет S на n долей.

- **Функция восстановления**:

$$\text{Reconstruct}(\{S_1, S_2, \ldots, S_k\}) \rightarrow S$$

Объединяет k долей для получения оригинального секрета.

Определение идеальной СРС

- Идеальная схема разделения секрета:
  - Доля каждого участника имеет тот же размер, что и секрет S.
  - Участники не обладают избыточной информацией.

Определение

- Совершенная СРС:

$$P(S|\text{меньше чем } k \text{ долей}) = P(S)$$

- Свойство «всё или ничего»:
  - Меньше k долей — нет информации о секрете.
  - k или больше долей — секрет полностью восстанавливается.

Определение

- (n, k)-пороговая схема:
  - Секрет делится между n участниками.
  - Для восстановления секрета требуется k участников ($k \leq n$).

Пример

- Секрет делится на n долей, каждая из которых равна S.
- Доказательство:
  - n участников объединяются и полностью восстанавливают секрет.
  - Менее n участников ничего не знают о секрете.

Восстановление по k точкам

- Полином степени $k-1$:

$$f(x) = \sum_{i=1}^{k} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

- Используется для восстановления секрета $f(0)$ по k точкам.

Описание

- Генерация случайного полинома степени $k-1$:

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$$

  где a_0 — секрет.
- Доли: точки $(x_i, f(x_i))$, $x_i \neq 0$.
- Доказательства:
  - Совершенность: $k-1$ долей не дают информацию о a_0.
  - Идеальность: размер долей равен размеру секрета.

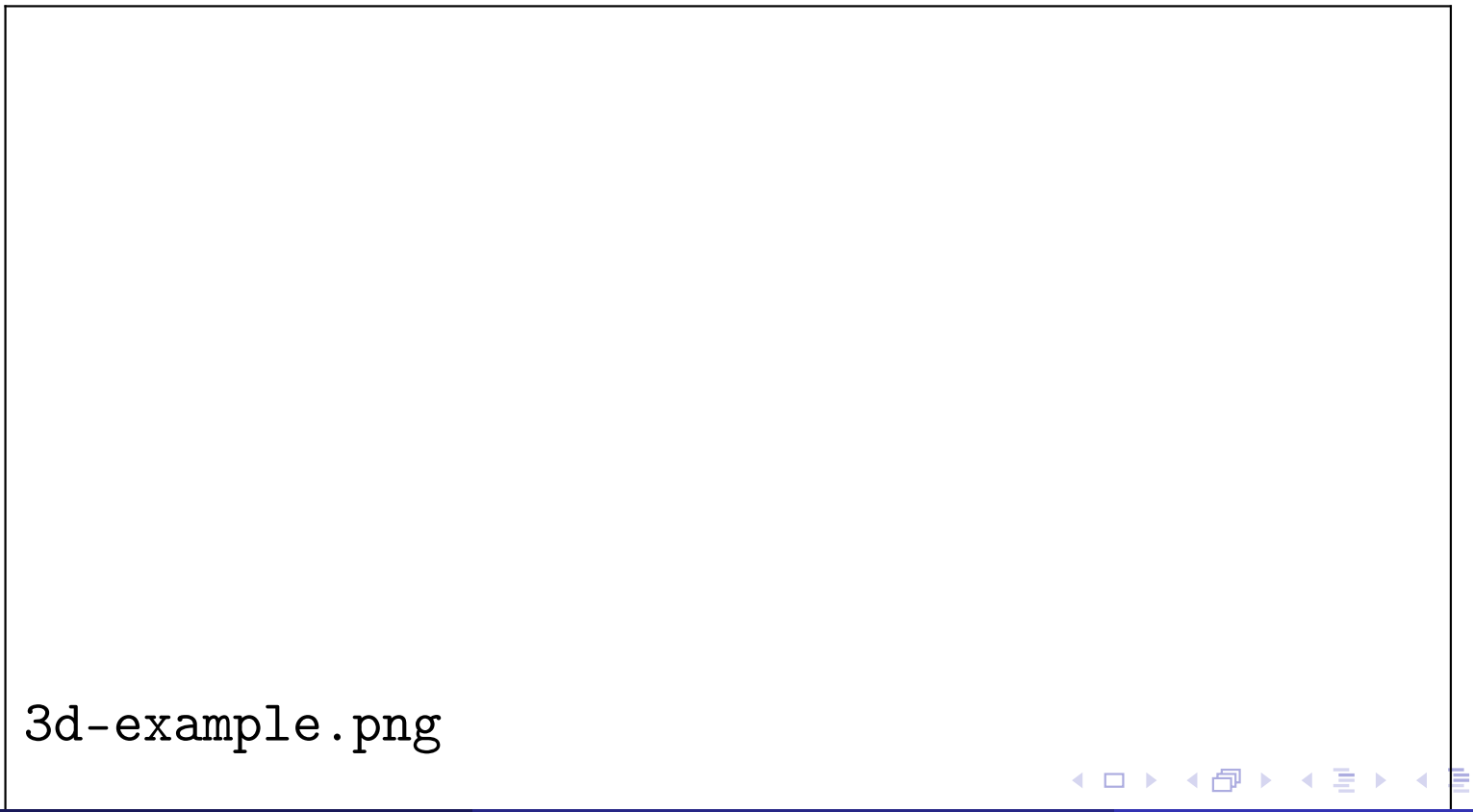
Описание

- Использует систему линейных уравнений:

$$A \cdot X = B$$

где A — матрица коэффициентов, X — вектор секретов, B — вектор долей.

- Пример для 3D:



Заключение

- СРС — важный инструмент для безопасного хранения данных.
- Различные схемы применяются в зависимости от задач.
- Перспективы: улучшение устойчивости и эффективность вычислений.

Спасибо за внимание!