

Часть I

Как выдать по паролю президенту, премьер-министру и министру обороны так, чтобы каждый из них не получил никакой полезной информации, но любые двое смогли бы войти в систему управления ракетами?

План лекции

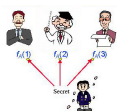
- 1 Разделение секрета
- 2 Полезные игры
- 3 Парадокс заключенного и пробки на дорогах

Разделение секрета

Общая картина — есть комната управления секретной ракетой, президент, премьер министр и министр обороны. Нужно сделать замок (систему замков) так, что:

- A Дверь может открыть каждый из трех
Решение: выдать каждому по ключу от замка
- B Дверь можно открыть только при согласии всех трех
Решение: сделать три разных замка
- B Если речь идет о пароле?
Простое решение: $p = \text{pas sword}$
Хитрое решение: $p = ((p_1 + p_2 + p_3) \bmod N)$
- Г Пароль могут восстановить любые два из трех?

Разделение секрета: постановка



Формализация

Разделить секрет $m \in [1..M]$ между n участниками
Любые t из них могут восстановить m
Любые $t - 1$ из них НИЧЕГО не могут узнать про m

Схема Шамира [1979]

Основная идея (из матана):

Зная значения многочлена степени $t - 1$ в t точках можно восстановить его значения во всех остальных (интерполяция)

Зная только $t - 1$ значения, невозможно предсказать остальные точки

Схема Шамира II

Подготовительный шаг

Раздающий выбирает простое p , которое больше всех возможных секретов

Кодирование секрета

Выбираем $s_1, s_{t-1} \stackrel{\text{ran}}{\in} \mathbb{Z}_p$
Устанавливаем $s(x) \stackrel{\text{def}}{=} m + s_1x + \dots + s_{t-1}x^{t-1}$

Раздача секрета

Для каждого $i = 1, 2, \dots, n$
посылаем участнику i пару чисел $(i, s(i))$

Восстановление секрета

Собрались t человек

Они знают t точек на графике многочлена:

$$(x_1, s(x_1)), \dots, (x_t, s(x_t))$$

Секрет — это значение в нуле: $m = s(0)$

Интерполяция Лагранжа:

$$s(x) = \sum_{i=1}^t s(x_i) \frac{\prod_{j \in [1..t], j \neq i} (x_j - x)}{\prod_{j \in [1..t], j \neq i} (x_j - x_i)}$$

Формула для ответа:

$$m = \sum_{i=1}^t s(x_i) \frac{\prod_{j \in [1..t], j \neq i} x_j}{\prod_{j \in [1..t], j \neq i} (x_j - x_i)}$$

Часть II

Как использовать умственные силы, которые тратят люди, играя в компьютерные игры?

9 / 22

Как использовать игроков?

Ваши идеи?

Luis von Ahn: надо пропагандировать **игры с полезной целью**

Задача, которую на могут решить **компьютеры:**

По картинке составить список изображенных на ней объектов

11 / 22

Результат ESP Game

Огромная база меток для изображений

Применение: поиск изображений

Другие игры:

Peekaboom
Verbose

13 / 22

Общая схема (2/2)

Пусть задача — это неизвестное соответствие **ответов** некоторым **входным данным**

Асимметричная игра

- Первый игрок получает вход
- Первый игрок посылает второму игроку возможные ответы
- Второй игрок должен угадать входные данные

15 / 22

Для сравнения

На игру в солитер человечество тратит **миллиард** человеко-часов в год

На постройку Панамского канала ушло **двадцать миллионов** человеко-часов

Панамский канал мог быть построен за 8 дней!

10 / 22

ESP Game

Правила:

- Это on-line игра (<http://www.espgame.org>)
- Игроки разбиваются на пары случайным образом
- Игрокам показывают картинки
- Цель раунда: как можно быстрее независимо напечатать общее слово
- Иногда, рядом с картинкой появляется список запрещенных слов. Нужно найти общее слово за пределами списка.

12 / 22

Общая схема (1/2)

Пусть задача — это неизвестное соответствие **ответов** некоторым **входным данным**

Симметричная игра

- Оба игрока получают входные данные
- Должны как можно быстрее набрать одинаковый ответ
- Возможно использование запрещенных ответов

14 / 22

Часть III

Две истории о том, к чему приводит эгоизм

16 / 22

Парадокс заключенного

Каждый из двух заключенных может или **дать показания** против напарника, или **промолчать**

Система наказаний:

- Оба дали показания: **пять лет каждому**
- Оба промолчали: **год каждому**
- Один дал показания: **его отпускают, второму дают пятнадцать лет**

Как бы вы поступили?

17 / 22

Пробки на дорогах (1/2)

Между A и B есть две дороги и 100 автомобилистов

- Первая дорога занимает час
- Вторая дорога занимает $\frac{x}{100}$ часов, где x — число автомобилей на второй дороге

Какую дорогу вы выбираете?

18 / 22

Пробки на дорогах (2/2)

Нужно проехать от A к B , есть промежуточные пункты C и D

- Дороги AC и DB занимают $\frac{x}{100}$
- Дороги AD и CB занимают 1 час
- Дорога CD занимает 0 секунд

Закрытие дороги CD уменьшает среднее время проезда!

19 / 22

Задача на дом

Вы хотите повесить несколько обычных замков и раздать ключи, чтобы было выполнено правило доступа "6 из 11".

Какое минимальное число замков вам понадобится?

20 / 22

Главные моменты

Сегодня мы узнали:

- Разделение секрета: используется интерполяция многочленов
- Игры с пользой: ESP Game
- Математическая модель эгоистического поведения: парадокс заключенного




Вопросы?

21 / 22

Источники

Домашняя страница <http://logic.pdmi.ras.ru/~yura>

Ссылки:

-  [Luis von Ahn](#)
-  [Adi Shamir](#)
-  [Tim Roughgarden](#)

22 / 22