Византийское соглашение и покер по телефону

Лекция N 2 курса “Современные задачи криптографии”

Юрий Лифшиц
yura@logic.pdmi.ras.ru

Мат-Мех СПбГУ — SPRINT Lab

Осень’2005

Однажды двоим чемпионам по “шахматам в слепую” надоела их игра:

— Давай для разнообразия сыграем в “покер в слепую”?
— Конечно! Только сдавать буду я.

Старый анекдот

План лекции

Автоматика и ошибки

По небу летит самолет. Им управляет автопилот.

Автопилот сломался ⇒ 
Решение 1: Два автопилота. Кто из них главный?
Решение 2: Три автопилота. Как выбрать решение?

Мысль: Контрольный центр проводит голосование.
Контрольный центр сломался ⇒ 

Вывод: Автопилоты должны договориться, не имея “главного автопилота”

Могут ли договориться три автопилота, один из которых сломался?

Покер по телефону

Два участника, общаясь между собой, должны выбрать себе карты:

- Раздача должна быть случайной
- Карты игроков не должны пересекаться
- Во время игры можно добирать карты из "колоды"
- В конце игры можно проверить честность противника

Покер: результаты

Раздача карт:

- Невозможна!
  - Мы это докажем
- Возможна!
  - Мы построим протокол для раздачи карт

План лекции

Византийские генералы

Общая картина:

- Пусть вокруг города расположено n византийских отрядов, каждым командует свой генерал
- У каждого генерала есть некоторая информация
- Генералы могут посылать сообщения другим генералам
- На основе общей информации нужно принять решение
- Среди генералов могут быть предатели

Требования:

А Все честные генералы принимают одинаковое решение

Б Малое количество предателей не способно заставить честных выбрать "плохой план"

План протокола

Фаза 1 Генералы делятся своими наблюдениями
Фаза 2 Генералы принимают решение

Требования к первой фазе:

1А Наблюдения честных генералов до других честных генералов дойдут неискаженными

1Б От нечестного генерала все честные генералы получат одинаковое наблюдение

Анализ плана:

Все честные генералы получат одинаковую сводку
Наблюдения всех честных генералов будут поняты правильно
Генералы смогут принять одинаковый и "хороший" план

Итоговая постановка

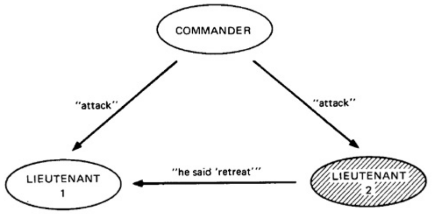
ЗАДАЧА О ВИЗАНТИЙСКИХ ГЕНЕРАЛАХ

Командир должен передать свой приказ $n-1$ лейтинанту так, чтобы были выполнены два свойства:

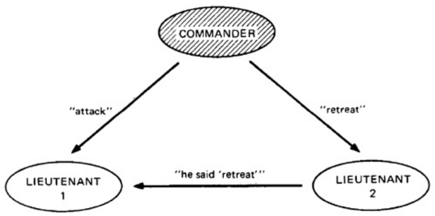
Согласованность	Все генералы получат одинаковый приказ
Исполнительность	Если командир честен, то приказ будет совпадать с исходным

Кстати, а почему генералы — византийские?

Невозможность "один из трех"



Пусть Командир честен и говорит "атакуй", а Лейтенант 2 ведет себя, как будто ему сказали "отступай".
Следуя **исполнительности**, Лейтенант 1 обязан атаковать



Пусть теперь Командир — предатель. Он говорит Лейтенанту 1 "атаковать", а Лейтенанту 2 "отступать".
С точки зрения Лейтенанта 2 эти ситуации не отличаются, так что он вынужден атаковать

Но Лейтенант 2 (из симметрии) будет отступать!
Противоречие с **согласованностью**.

Протокол "m из $3m+1$"

Протокол $BG(0)$:

1. Командир рассылает всем свой приказ
2. Лейтенанты принимают этот приказ в качестве окончательного

Протокол $BG(m)$:

1. Командир рассылает всем свой приказ
2. Для каждого i Лейтенант i рассылает остальным лейтенантам полученный им приказ с помощью $BG(m-1)$
3. В качестве окончательного решения лейтенанты выбирают наиболее частое значение среди своего командирского приказа и $n-2$ значений полученных с помощью $BG(m-1)$ от других лейтенантов

Каков порядок общего числа сообщений?

Лемма об исполнительности

Исполнительность: Командир честен $\Rightarrow$ получен исходный приказ

Лемма об исполнительности

Для всех k и m алгоритм $BG(m)$ обладает исполнительностью для хотя бы $2k+m+1$ генералов, среди которых не более k предателей.

Доказательство.

Индуция по m. При $m = 0$ верно!
Переход. Каждый честный генерал пользуется $BG(m-1)$ среди $\geq 2k+m-1$ генералов и не более k предателей. Т.е. по предположению "исполнительность" выполнена. Таким образом все честные генералы получат хотя бы $k+m$ копий верного приказа, а значит выполнят его. □

Согласованность

Корректность протокола

Протокол $BG(m)$ обладает исполнительностью и согласованностью для $\geq (3m+1)$ офицеров и $\leq m$ предателей.

Доказательство.

Исполнительность доказана в Лемме ($k := m$)
Индуция по m. База $m = 0$ верно!
Переход. Если командир не предатель, из исполнительности следует согласованность.

Пусть командир — предатель. Тогда по индукции $BG(m-1)$ обладает согласованностью (у нас $3m$ офицеров и не более $m-1$ предателя).

Следовательно все честные генералы получат одинаковые наборы из n значений, и сделают одинаковый окончательный выбор. Согласованность доказана. □

План лекции

Постановка задачи

Два участника, общаясь между собой, должны выбрать себе карты:

- Раздача должна быть случайной
- Карты игроков не должны пересекаться
- Во время игры можно добирать карты из "колоды"
- В конце игры можно проверить честность противника

Невозможность

Предположим:

В колоде 3 карты $\{X, Y, Z\}$
Каждому надо выдать по карте
Игроки обменялись сообщениями: $M_1, \ldots, M_n$
Алиса получила X, Боб получил Y

Могло ли так получится, что при тех же сообщениях Алиса получила бы Z?

Могло!

А могло ли так получится, что при тех же сообщениях Боб получил бы Z?

Тоже могло. Т.е. был шанс сдать одну карту обоим игрокам!

Задача про лодку

На одном берегу Алиса с навесным замком и алмазом, на другом Боб с еще одним навесным замком. Через реку ходит паром со встроенным сейфом.

Как надежно переправить алмаз от Алисы Бобу?

Коммутативное шифрование

Пусть есть две криптосистемы:

Шифрование E_1, дешифрование D_1
Шифрование E_2, дешифрование D_2

Эти системы называются коммутативными, если

$$E_1(E_2(X)) = E_2(E_1(X))$$

Пример: Криптосистема RSA

$$(x^{e_1})^{e_2} = x^{e_1 e_2} = (x^{e_2})^{e_1}$$

Протокол раздачи карт

Шаги:

1. Алиса шифрует своей системой все карты и в случайном порядке посылает их Бобу
2. Боб выбирает карты для Алисы и посылает их ей
3. Боб выбирает себе карты из оставшихся, шифрует их своей системой и посылает их Алисе
4. Алиса расшифровывает эти карты и возвращает их Бобу
5. Боб окончательно расшифровывает свои карты

При необходимости игроки и дальше могут вытягивать карты из оставшейся колоды

Анализ протокола

- Боб видит 52 случайных шифротекста, не зная где какая карта
- Боб случайно выбирает карты для Алисы. Он не знает, какие карты он ей отдал
- Боб случайно выбрал себе карты. Алиса не может узнать, что это за карты (она видела их только зашифрованными)
- Это рассуждение не является доказательством надежности!

Так раздача карт возможна или невозможна?

План лекции

1. Неформальные постановки
   - Автоматика и ошибки
   - Покер по телефону
2. Византийские генералы
   - Формализация задачи
   - Невозможность “один из трех”
   - Протокол “m среди $3m + 1$”
3. Покер по телефону
   - Невозможность честной раздачи
   - Протокол для честной раздачи
4. **Задача на дом**

Покер на троих

Придумайте протокол раздачи карт для трех игроков, не требующий вычислительной ограниченности участников (абсолютно стойкий)

Последний слайд

Если не запомните ничего другого:

- Задача о византийских генералах имеет решение только когда предателей строго меньше одной трети
- Покер по телефону возможен с криптографической стойкостью
- Задача на дом: покер на троих

Вопросы?