v. 2.0

Криптография

Лекция 7. Алгоритмы разделения секрета.

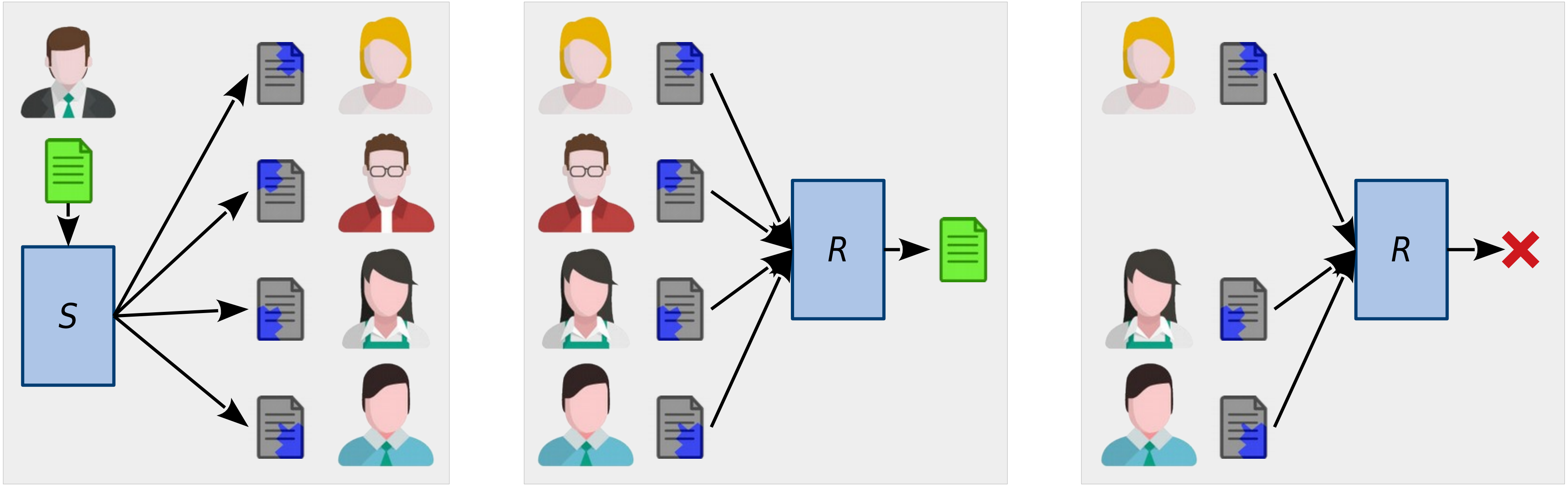
Дмитрий Яхонтов

“Кочерга”, 2019

Что такое разделение секрета
(Secret Sharing)

- Распределение информации (секрета) среди группы участников так, что каждый получает свою долю.
  Секрет может восстановить только группа совместно.

- Неполная группа не может получить никакой информации.



Простейшая схема

$$S = S_1 \oplus S_2 \oplus S_3 \oplus \ldots \oplus S_n$$

S — секрет

$S_1 \ldots S_n$ — доли участников

$S_1 \ldots S_{n-1}$ — случайные

$S_n = S \oplus S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1}$

Потеря одной доли ведёт к потере всего секрета.

Решение — пороговые схемы (k из n)

Схема Блэкли

- Секрет — координата точки в k-мерном пространстве
- Доля — уравнение (k–1)-мерной плоскости
- Для восстановления секрета требуются любые k долей
- Все операции в поле целых чисел по модулю p

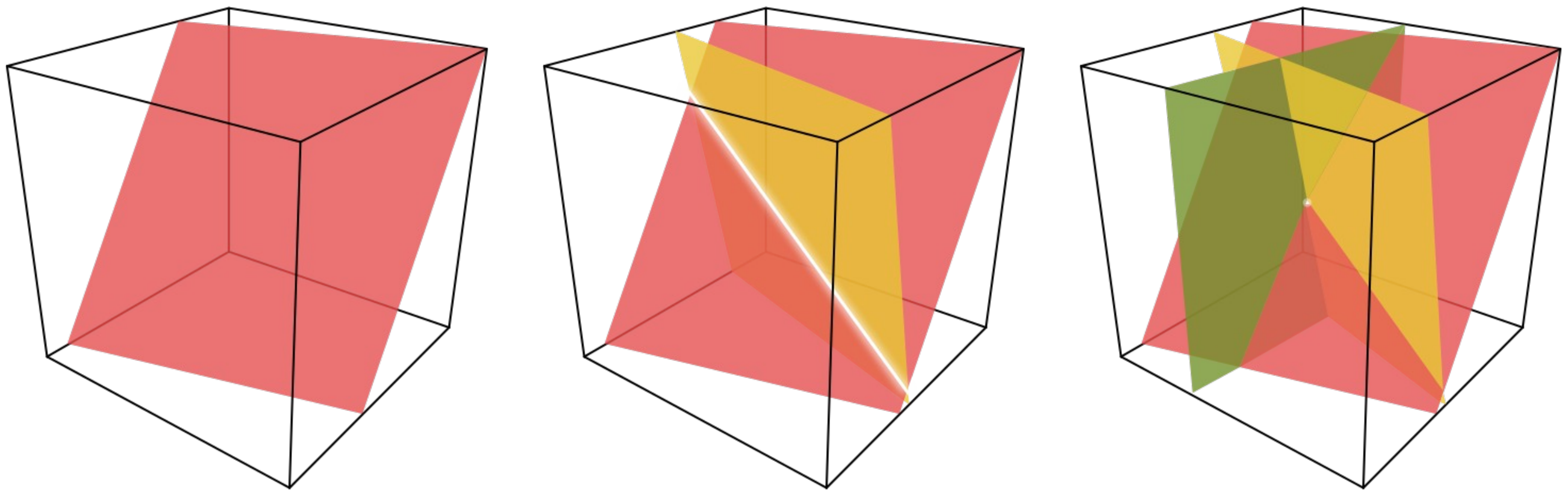


Схема Карнина–Грина–Хеллмана

- Выбирается n+2 векторов U, V_0, V_1, V_2 ... V_n размерности k
- Секрет — скалярное произведение $(U \bullet V_0)$
- Доля — скалярное произведение $(U \bullet V_i)$
- Вектора V_0, V_1, V_2 ... V_n — открытые
- Для восстановления секрета необходимо решить систему из k уравнений:

$$\begin{cases} u_1 v_{1,1} + u_2 v_{1,2} + u_3 v_{1,3} + \ldots + u_k v_{1,k} = (U \bullet V_1) \\ u_1 v_{2,1} + u_2 v_{2,2} + u_3 v_{2,3} + \ldots + u_k v_{2,k} = (U \bullet V_2) \\ \quad \ldots \\ u_1 v_{k,1} + u_2 v_{k,2} + u_3 v_{k,3} + \ldots + u_k v_{k,k} = (U \bullet V_k) \end{cases}$$

и найти $(u_1, u_2, u_3 \ldots u_k)$ — координаты вектора U, затем вычислить $(U \bullet V_0)$

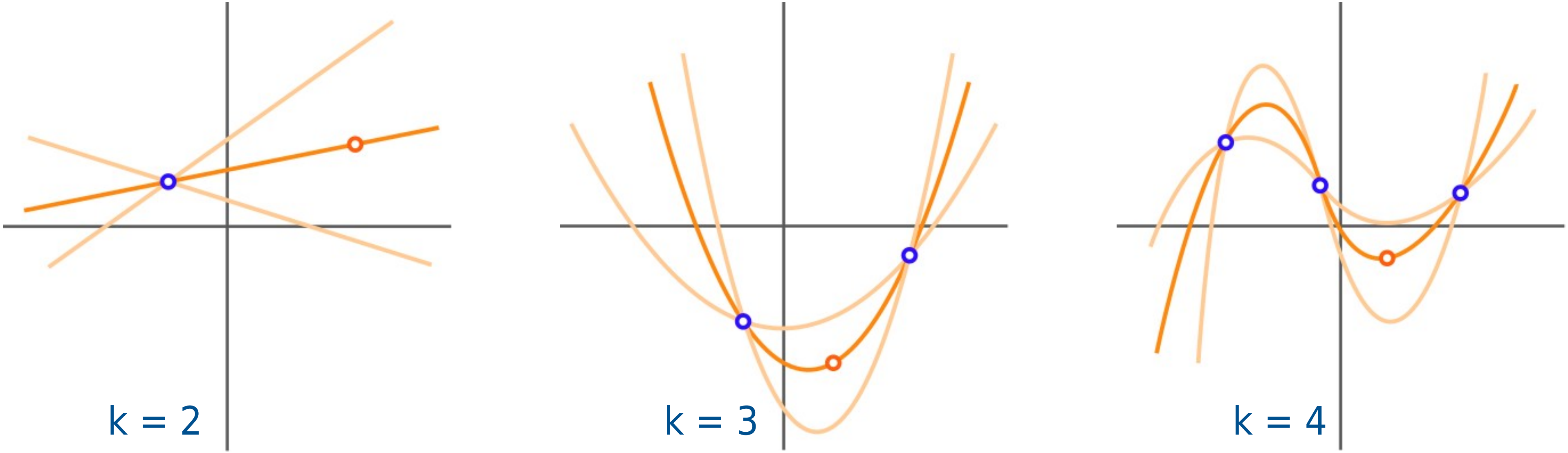
Схема Шамира

- Секрет — свободный коэффициент M полинома (k–1)-ой степени

  $$F(x) = (a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_2x^2 + a_1x + M) \bmod p$$

- Доля — значение полинома в некоторой точке $F(x_i)$

- Для восстановления секрета необходимо интерполировать полином и восстановить его коэффициенты. Для этого необходимы k точек.



Расширенные протоколы разделения секрета

- Проверяемое разделение

  Участники могут убедиться, что их доли совместны друг с другом.
- Без раздающего

  Участники совместно генерируют секрет и распределяют его доли так, что никто не знает секрет целиком, пока он не будет восстановлен.
- Без раскрытия долей

  Ни один из участников не может узнать доли других участников даже после восстановления секрета. Возможность повторно использовать секрет без нового разделения.
- С голосованием “против”

  Каждый получает “положительную” и “отрицательную” доли секрета. Восстановление возможно, если предъявлено не менее k положительных и не более m отрицательных долей.
- С возможностью отзыва

  Протокол позволяет отозвать долю, например, в случае компрометации.

Проверяемое разделение секрета
(на основе схемы Шамира)

- Секрет — свободный коэффициент M полинома
  $$F(x) = (a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_2x^2 + a_1x + M) \bmod p$$
- Маскирующий полином
  $$E(x) = (b_{k-1}x^{k-1} + b_{k-2}x^{k-2} + \ldots + b_2x^2 + b_1x + R) \bmod p$$
- Открытые основания g и h
- Открытые проверочные коэффициенты
  $$A_0 = g^M h^R \bmod p, \quad A_1 = g^{a1}h^{b1} \bmod p, \quad A_2 = g^{a2}h^{b2} \bmod p \ldots$$
- Доля — значения полиномов в точке: $F(x_i)$, $E(x_i)$
- Проверка доли:
  $$g^{F(x)}h^{E(x)} \bmod p = A_0 \cdot (A_1)\hat{}x \cdot (A_2)\hat{}x^2 \cdot \ldots \cdot (A_{t-2})\hat{}x^{(k-2)} \cdot (A_{t-1})\hat{}x^{(k-1)} \bmod p$$

Практическое применение

- Хранение закрытого ключа удостоверяющего центра

  Для использования ключа нужны совместные действия нескольких ответственных лиц. Существуют алгоритмы пороговой подписи.

- Протоколы электронного голосования

  В подсчете голосов участвуют N независимых наблюдателей.
  Избиратель распределяет доли своего голоса среди всех наблюдателей.
  Для восстановления результатов голосования требуется коалиция из K < N наблюдателей. Операции восстановления секрета и суммирования голосов должны быть коммутативны друг по отношению к другу.
  Для защиты от мошенничества избирателя используется схема с проверяемым разделением.

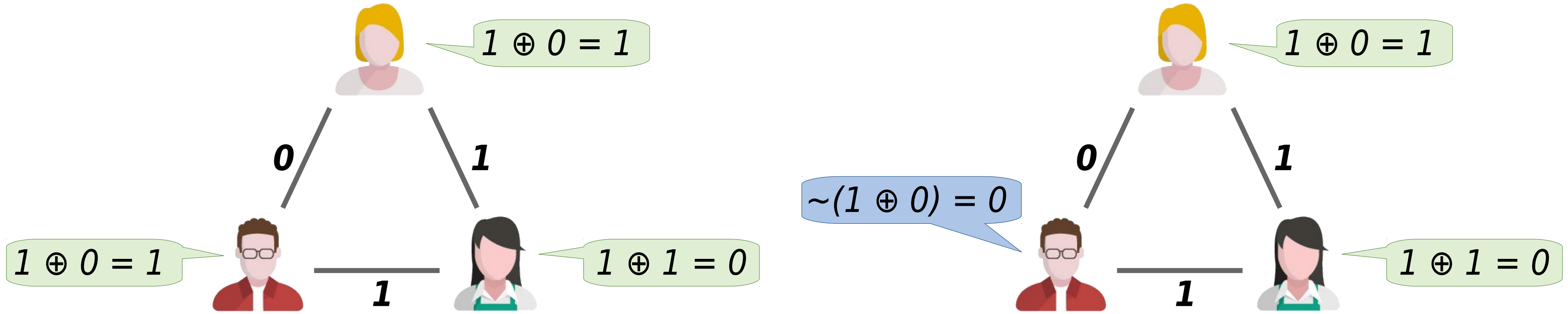
- Анонимная широковещательная передача

  Узлы сети создают разделяемые секреты друг с другом. Каждый узел публикует линейную комбинацию долей секретов, которые он разделил с разными соседями. Узел, желающий передать данные, инвертирует определенные биты в этой комбинации.
  Иллюстрация — “задача об обедающих криптографах”.

Задача об обедающих криптографах

Три криптографа обедают в ресторане. Официант сообщает им, что их обед кем-то оплачен. Оплатить мог анонимно один из криптографов (и он об этом знает), либо обед оплатило АНБ.

Криптографы хотят узнать, причастно ли АНБ, но не хотят раскрывать анонимность своих платежей.



- Каждые два криптографа создают общий 1-битный секрет.
- Каждый публикует бит, равный XOR от секретов, полученных с каждым из своих соседей. Если он платил за еду, то дополнительно инвертирует бит.
- Вычисляется XOR всех опубликованных бит. Если результат 0, значит никто из сидящих за столом не платил.

Задачи

1. Ключ запуска ядерных ракет разделяется между президентом и 8 генералами. Предложите схему разделения, при которой запустить ракеты могут либо президент вместе с четырьмя генералами, либо 7 генералов без президента.

2. Капитан Флинт закопал на острове клад и собирается сообщить его координаты двум своим помощникам, но так, чтобы найти клад они могли только вместе.

   Флинт хотел дать первому помощнику значение широты, а второму — долготы, но услышал о существовании металлоискателя, с которым можно обнаружить клад на любой траектории конечной длины.

   Предложите максимально простую схему разделения секрета, устойчивую к атаке с металлоискателем.

Ссылки

- Обратная связь:
  android.ruberoid@gmail.com
  @androidruberoid
- Анонсы:
  facebook.com/kocherga.club
  vk.com/kocherga_club
  vk.com/kocherga_prog
- Материалы лекций:
  github.com/notOcelot/Kocherga_crypto
- Видео:
  youtube.com/channel/UCeLSDFOndl4eKFutg3oowHg