

Криптография

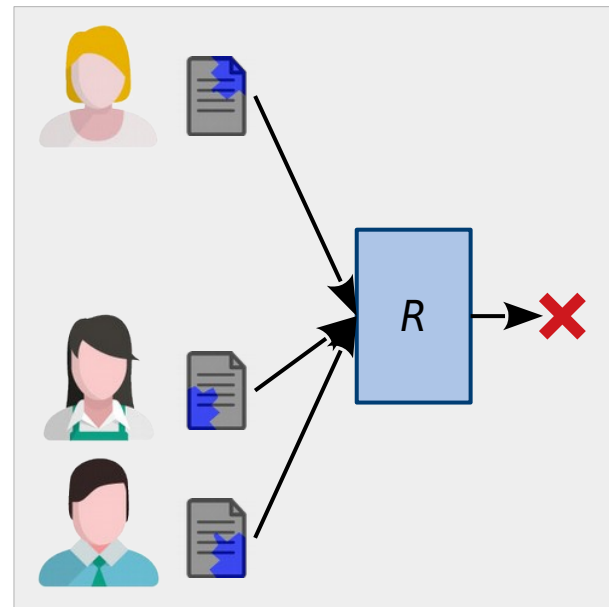
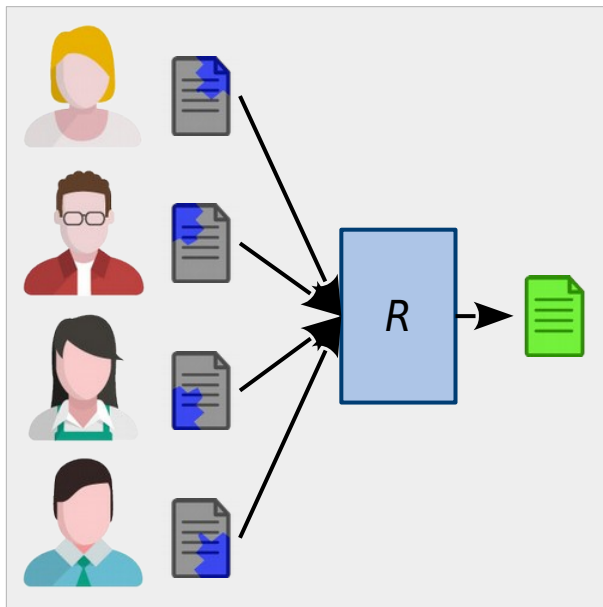
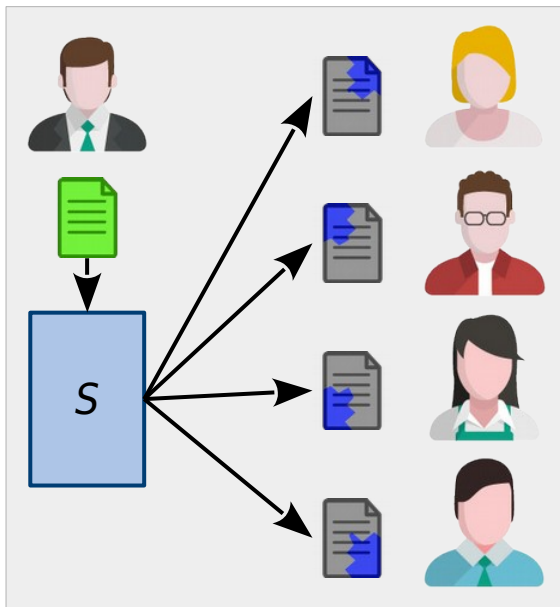
Лекция 7. Алгоритмы разделения секрета.

Дмитрий Яхонтов

“Кочерга”, 2018

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

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

S — секрет

$S_1 \dots S_n$ — доли участников

$S_1 \dots S_{n-1}$ — случайные

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

Потеря одной доли ведёт к потере всего секрета.

Решение — пороговые схемы (k из n)

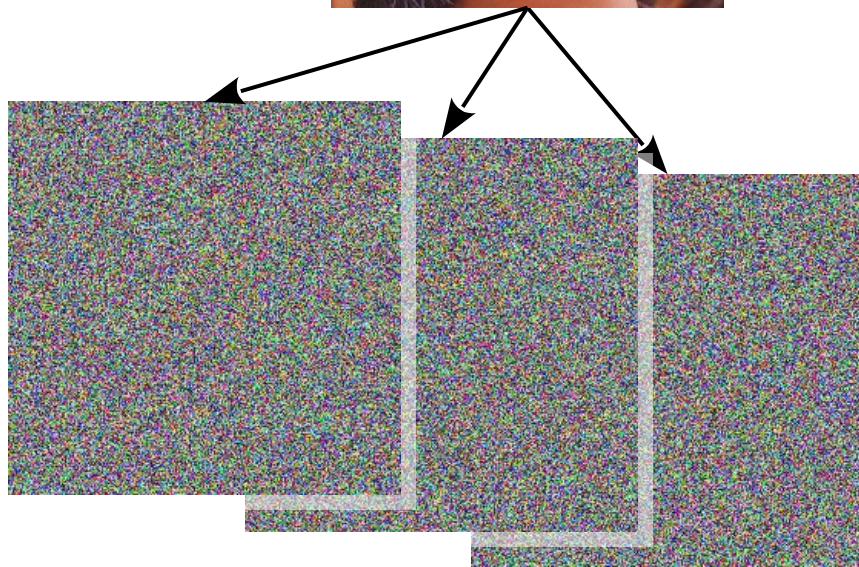


Схема Блэкли

- 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

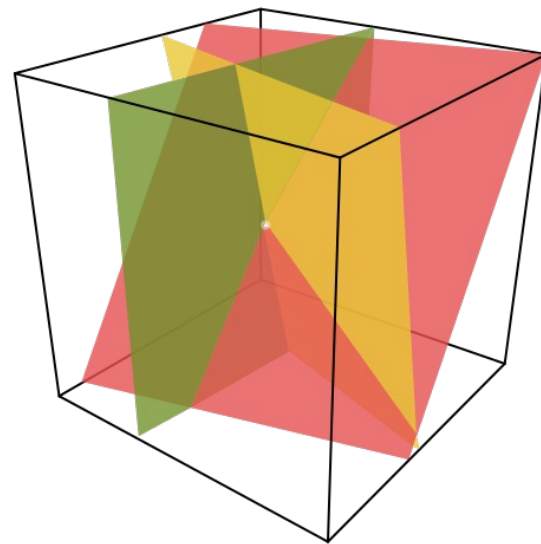
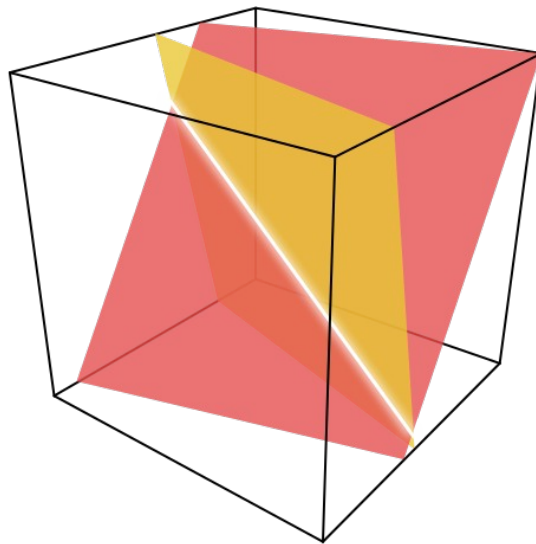
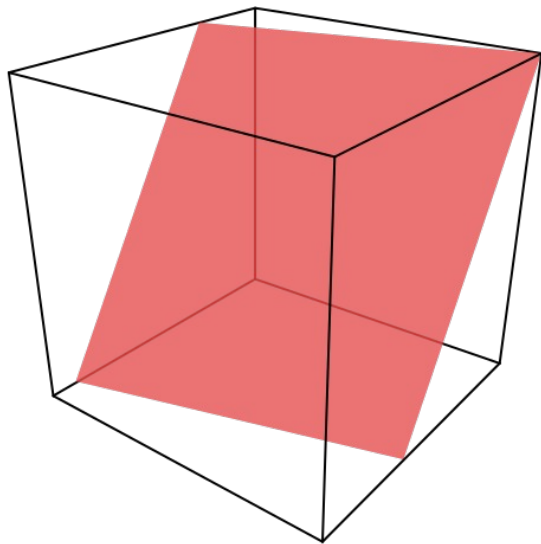


Схема Карнина–Грина–Хеллмана

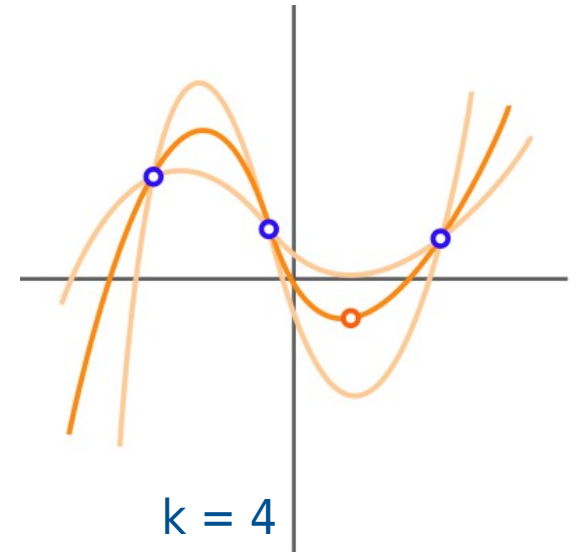
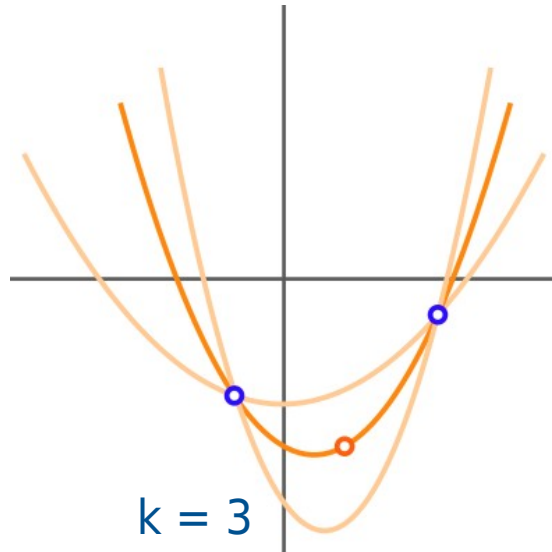
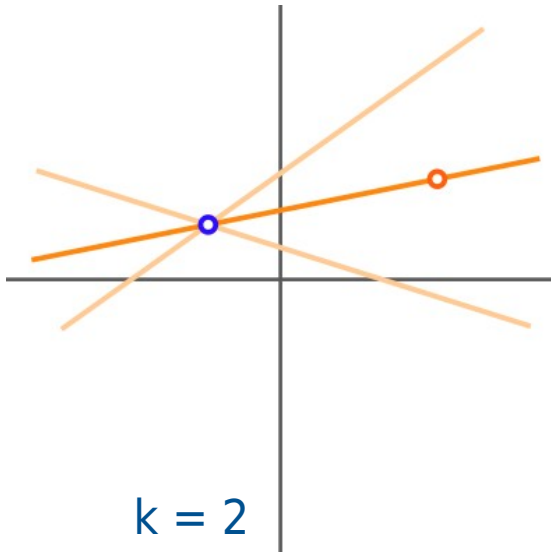
- Выбирается $n+2$ векторов $U, V_0, V_1, V_2 \dots V_n$ размерности k
- Секрет — скалярное произведение $(U \cdot V_0)$
- Доля — скалярное произведение $(U \cdot V_i)$
- Вектора $V_0, V_1, V_2 \dots V_n$ — открытые
- Для восстановления секрета необходимо решить систему из k уравнений:

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

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

Схема Шамира

- Секрет — свободный коэффициент M полинома $(k-1)$ -ой степени
$$F(x) = (a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_2x^2 + a_1x + M) \bmod p$$
- Доля — значение полинома в некоторой точке $F(x_i)$
- Для восстановления секрета необходимо интерполировать полином и восстановить его коэффициенты. Для этого необходимы k точек.



Проверяемое разделение секрета (на основе схемы Шамира)

- Секрет — свободный коэффициент M полинома

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

- Маскирующий полином

$$E(x) = (b_{k-1}x^{k-1} + b_{k-2}x^{k-2} + \dots + b_2x^2 + b_1x + R) \bmod p$$

- Открытые основания g и h

- Открытые проверочные коэффициенты

$$A_0 = g^M h^R \bmod p, A_1 = g^{a_1} h^{b_1} \bmod p, A_2 = g^{a_2} h^{b_2} \bmod p \dots$$

- Доля — значения полиномов в точке: $F(x_i)$, $E(x_i)$

- Проверка доли:

$$g^{F(x)} h^{E(x)} \bmod p = A_0 \cdot (A_1)^x \cdot (A_2)^{x^2} \cdot \dots \cdot (A_{t-2})^{x^{k-2}} \cdot (A_{t-1})^{x^{k-1}} \bmod p$$

Мошенничество

- Мэллори отдаёт вместо своей доли случайное число и срывает процесс восстановления секрета.
- Мэллори не имеет доли, но участвует в восстановлении секрета. Когда другие участники предъявили к своим долей, Мэллори восстанавливает секрет, генерирует себе долю и предъявляет её.

Решение: Раздающий подписывает каждую долю секрета. Даже зная секрет, Мэллори не может сгенерировать долю с действительной подписью.

Расширенные протоколы разделения секрета

- 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 t отрицательных долей.
- С возможностью отзыва
Протокол позволяет отозвать долю, например, в случае компрометации.

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. Мэллори участвует в восстановлении секрета и дожидается, пока будут названы k долей других участников. Даже если доли подписаны, и Мэллори не может сгенерировать свою, она уже знает секрет.

Предложите протокол, выявляющий такое мошенничество и позволяющий прервать восстановление секрета до того, как Мэллори его узнает.

Ссылки

- Обратная связь:

 android.ruberoi@gmail.com

 [@android_ruberoi](https://lesswrongru.slack.com)

- Анонсы:

 facebook.com/kocherga.club

 vk.com/kocherga_club

 vk.com/kocherga_prog

- Материалы лекций:

 github.com/notOcelot/Kocherga_crypto

- Видео:

 youtube.com/channel/UCeLSDFOndI4eKFutg3oowHg

