Базовые протоколы

Лекция N 1 курса
“Современные задачи криптографии”

Юрий Лифшиц
yura@logic.pdmi.ras.ru

Мат-Мех СПбГУ — SPRINT Lab

Осень’2005

“- Хорошо, дайте же сюда деньги. - На что-ж деньги? У меня вот они в руке! Как только напишете расписку, в ту же минуту их возьмете. - Да позвольте, как же мне писать расписку? Прежде нужно видеть деньги. Чичиков выпустил из рук бумажки Собакевичу, который, приблизившись к столу и накрывши их пальцами левой руки, другою написал на лоскутке бумаги, что задаток двадцать пять рублей государственными ассигнациями за проданные души получен сполна.”

Н. В. Гоголь. “Мертвые души”, глава 5.

План лекции

Разделение секрета

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

A Дверь может открыть каждый из трех

Разделение секрета

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

A Дверь может открыть каждый из трех
Решение: выдать каждому по ключу от замка

Разделение секрета

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

- **А** Дверь может открыть каждый из трех
  Решение: выдать каждому по ключу от замка
- **Б** Дверь можно открыть только при согласии всех трех

Разделение секрета

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

- **А** Дверь может открыть каждый из трех
  Решение: выдать каждому по ключу от замка
- **Б** Дверь можно открыть только при согласии всех трех
  Решение: сделать три разных замка

Разделение секрета

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

А Дверь может открыть каждый из трех
Решение: выдать каждому по ключу от замка

Б Дверь можно открыть только при согласии всех трех
Решение: сделать три разных замка

В Если речь идет о пароле?

Разделение секрета

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

- **А** Дверь может открыть каждый из трех
  Решение: выдать каждому по ключу от замка
- **Б** Дверь можно открыть только при согласии всех трех
  Решение: сделать три разных замка
- **В** Если речь идет о пароле?
  Простое решение: $p = \text{pas swo rd}$

Разделение секрета

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

А Дверь может открыть каждый из трех
Решение: выдать каждому по ключу от замка

Б Дверь можно открыть только при согласии всех трех
Решение: сделать три разных замка

В Если речь идет о пароле?
Простое решение: $p = \mathrm{pas\ swo\ rd}$
Хитрое решение: $p = ((p_1 + p_2 + p_3) \mod N)$

Разделение секрета

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

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

Электронная ставка

Алиса хочет сделать ставку у букмейкера Боба так, чтобы были выполнены свойства:

Секретность	Боб не сможет узнать, на кого поставила Алиса
Связанность	Алиса не может изменить свою ставку

Электронная ставка

Алиса хочет сделать ставку у букмейкера Боба так, чтобы были выполнены свойства:

Секретность Боб не сможет узнать, на кого поставила Алиса
Связанность Алиса не может изменить свою ставку

Простое решение: отдать ставку в запечатанном конверте:

Электронная ставка

Алиса хочет сделать ставку у букмейкера Боба так, чтобы были выполнены свойства:

Секретность Боб не сможет узнать, на кого поставила Алиса
Связанность Алиса не может изменить свою ставку

Простое решение: отдать ставку в запечатанном конверте:

Наша задача: электронная версия этого протокола

Возможно ли это?

Развод по телефону

Алиса разводится с Бобом, они делят имущество и детей. Оба претендуют на BMW. Как быть?

Развод по телефону

Алиса разводится с Бобом, они делят имущество и детей. Оба претендуют на BMW. Как быть?

Обычное решение: подбросить монетку 

Развод по телефону

Алиса разводится с Бобом, они делят имущество и детей. Оба претендуют на BMW. Как быть?

Обычное решение: подбросить монетку 

Пусть Алиса и Боб уже не могут видеть друг друга и общаются только по телефону (ICQ).

Развод по телефону

Алиса разводится с Бобом, они делят имущество и детей. Оба претендуют на BMW. Как быть?

Обычное решение: подбросить монетку 

Пусть Алиса и Боб уже не могут видеть друг друга и общаются только по телефону (ICQ).

Возможно ли электронное подбрасывание монетки?

Море протоколов

Какого типа протокол нужен для Чичикова и Собакевича?

Море протоколов

Какого типа протокол нужен для Чичикова и Собакевича?

Протоколы:

- Одновременное подписание договора
- Одновременный обмен секретами
- Цифровая подпись [на семинаре]
- Коллективное принятие решений [2ая лекция]
- Раздача карт по телефону [2ая лекция]
- Анонимность сообщений [2ая лекция, если успеем]
- Электронные выборы [3ая лекция]
- Электронные деньги [4ая лекция]

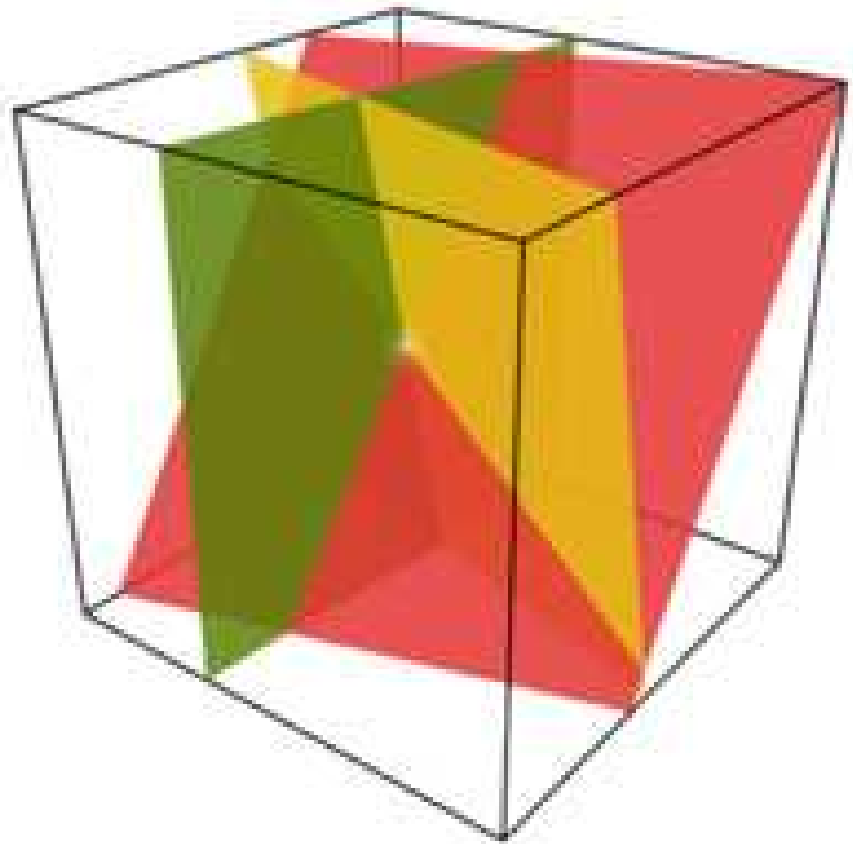
План лекции

Криптографический протокол

Основное понятие теоретической криптографии. Под протоколом понимается распределенный алгоритм с двумя или более участниками. Протокол является криптографическим, если он решает по крайней мере одну из трех задач криптографии — обеспечение *конфиденциальности*, *целостности*, *неотслеживаемости*. Определение криптографического протокола включает в себя различные компоненты: участники протокола, каналы связи между участниками, а также либо алгоритмы, используемые участниками, либо постановка той задачи, которую протокол призван решать.

Cryptography.Ru

Разделение секрета [Блэкли'79]



Разделение секрета [Блэкли'79]

Строим схему "3 из n":

Трехмерное пространство

Три плоскости общего положения определяют точку!

Разделение секрета [Блэкли'79]

Строим схему "3 из n":

Трехмерное пространство

Три плоскости общего положения определяют точку!

Подготовительные шаги:

Выберем простое p

Секрет: $x_0 \in \mathbb{Z}_p$

Случайно выбираем $y_0, z_0 \in \mathbb{Z}_p$

Получили секретную точку $Q = (x_0, y_0, z_0)$

Разделение секрета [Блэкли'79]

Строим схему "3 из n":

Трехмерное пространство

Три плоскости общего положения определяют точку!

Подготовительные шаги:

Выберем простое p

Секрет: $x_0 \in \mathbb{Z}_p$

Случайно выбираем $y_0, z_0 \in \mathbb{Z}_p$

Получили секретную точку $Q = (x_0, y_0, z_0)$

Раздача секрета:

Для каждого участника выбираем случайно $a, b \in \mathbb{Z}_p$

Вычисляем $= z_0 - a \cdot x_0 - b \cdot y_0$

Получили плоскость: $z = a \cdot x + b \cdot y + c$

Разделение секрета [Блэкли'79]

Строим схему "3 из n":

Трехмерное пространство

Три плоскости общего положения определяют точку!

Подготовительные шаги:

Выберем простое p

Секрет: $x_0 \in \mathbb{Z}_p$

Случайно выбираем $y_0, z_0 \in \mathbb{Z}_p$

Получили секретную точку $Q = (x_0, y_0, z_0)$

Раздача секрета:

Для каждого участника выбираем случайно $a, b \in \mathbb{Z}_p$

Вычисляем $= z_0 - a \cdot x_0 - b \cdot y_0$

Получили плоскость: $z = a \cdot x + b \cdot y + c$

Как построить схему "t из n"?

Схема Шамира [1979]

Постановка задачи

Нужно разделить секрет $m \in \mathbb{Z}_p$ между n участниками

Любые t из них могут восстановить m

Любые $t-1$ из них НИЧЕГО не могут узнать про m

Схема Шамира [1979]

Постановка задачи

Нужно разделить секрет $m \in \mathbb{Z}_p$ между n участниками
Любые t из них могут восстановить m
Любые $t-1$ из них НИЧЕГО не могут узнать про m

Основная идея (из матана):

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

Схема Шамира [1979]

Постановка задачи

Нужно разделить секрет $m \in \mathbb{Z}_p$ между n участниками
Любые t из них могут восстановить m
Любые $t-1$ из них НИЧЕГО не могут узнать про m

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

Схема Шамира II

Подготовительный шаг

Раздающий выбирает простое p, которое больше всех возможных секретов

Кодирование секрета

Выбираем $s_1, s_{t-1} \overset{\text{ran}}{\in} \mathbb{Z}$

Устанавливаем $s(x) \overset{def}{=} m + s_1 x + \cdots + s_{t-1} x^{t-1}$

Схема Шамира II

Подготовительный шаг

Раздающий выбирает простое p, которое больше всех возможных секретов

Кодирование секрета

Выбираем $s_1, s_{t-1} \overset{\text{ran}}{\in} \mathbb{Z}$

Устанавливаем $s(x) \overset{def}{=} m + s_1 x + \cdots + s_{t-1} x^{t-1}$

Раздача секрета

Для каждого $i = 1, 2, \ldots, n$

Посылаем участнику i пару чисел $(i, s(i))$

Восстановление секрета I

Собрались t человек

Они знают t точек на графике многочлена:

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

Восстановление секрета I

Собрались t человек

Они знают t точек на графике многочлена:

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

Выписываем систему уравнений

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{t-1} \\ 1 & x_2 & \ldots & x_2^{t-1} \\ \vdots & & \vdots & \vdots \\ 1 & x_t & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} m \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix} = \begin{pmatrix} sx_1 \\ s(x_2) \\ \vdots \\ s(x_{t-1}) \end{pmatrix}$$

Восстановление секрета I

Собрались t человек

Они знают t точек на графике многочлена:

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

Выписываем систему уравнений

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{t-1} \\ 1 & x_2 & \ldots & x_2^{t-1} \\ \vdots & & \vdots & \vdots \\ 1 & x_t & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} m \\ s_1 \\ \vdots \\ s_{t-1} \end{pmatrix} = \begin{pmatrix} sx_1 \\ s(x_2) \\ \vdots \\ s(x_{t-1}) \end{pmatrix}$$

Факт:

Если все $x_1, \ldots, x_t$ различны, определитель матрицы не ноль и система имеет единственное решение

Восстановление секрета II

Собрались t человек

Они знают t точек на графике многочлена:

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

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

Восстановление секрета II

Собрались t человек

Они знают t точек на графике многочлена:

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

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

Интерполяция Лагранжа:

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

Восстановление секрета II

Собрались t человек

Они знают t точек на графике многочлена:

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

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

Интерполяция Лагранжа:

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

Формула для ответа:

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

Разделение секрета - недостатки

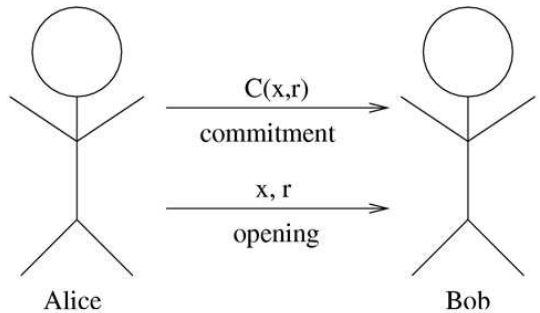
- Одноразовость
- Возможность мошенничества со стороны раздающего
- Возможность мошенничества со стороны участников

Диффи и Хеллман

“Новые направления в криптографии” [1976]:
Стойкость криптосистемы может быть основана на вычислительно-трудной задаче.

Идеология доказательства стойкости криптосистемы X:
Любой алгоритм, быстро взламывающий криптосистему X, можно переделать в алгоритм быстро решающий задачу P (про которую никто не верит, что ее можно легко решить).

Привязка к биту: постановка



Безусловная секретность	Распределения $C(0, r)$ и $C(1, r)$ совпадают
Вычислительная секретность	Распределения $C(0, r)$ и $C(1, r)$ трудноразличимы
Безусловная связанность	Бит b однозначно определен через $C(b, r)$
Вычислительная связанность	Вычислительно трудно подобрать пару r_0, r_1 т.ч. $C(0, r_0) = C(1, r_1)$

Односторонняя перестановка

Определение:
Биективная функция $F : \{0,1\}^n \longrightarrow \{0,1\}^n$ называется односторонней перестановкой, если

1) Функция F вычислима за полиномиальное время

Односторонняя перестановка

Определение:
Биективная функция $F : \{0,1\}^n \longrightarrow \{0,1\}^n$ называется односторонней перестановкой, если

1) Функция F вычислима за полиномиальное время
2) Не существует полиномиального алгоритма, который верно вычисляет F^{-1} с *хорошей вероятностью*

Односторонняя перестановка

Определение:
Биективная функция $F : \{0,1\}^n \to \{0,1\}^n$ называется односторонней перестановкой, если

1) Функция F вычислима за полиномиальное время
2) Не существует полиномиального алгоритма, который верно вычисляет F^{-1} с *хорошей вероятностью*

2') Существует предикат $h : \{0,1\}^n \to \{0,1\}$, т.ч. по $F(x)$ *трудно* вычислить $h(x)$

Привязка к биту I

Подготовительный шаг

Фиксируем одностороннюю перестановку F
и предикат h

Привязка к биту I

Подготовительный шаг

Фиксируем одностороннюю перестановку F
и предикат h

Привязка

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = (F(r), b \oplus h(r))$$

Привязка к биту I

Подготовительный шаг

Фиксируем одностороннюю перестановку F
и предикат h

Привязка

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = (F(r), b \oplus h(r))$$

Открытие секрета

Алиса посылает r

Привязка к биту I

Подготовительный шаг

Фиксируем одностороннюю перестановку F
и предикат h

Привязка

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = (F(r), b \oplus h(r))$$

Открытие секрета

Алиса посылает r

Эта схема:

Привязка к биту I

Подготовительный шаг

Фиксируем одностороннюю перестановку F
и предикат h

Привязка

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = (F(r), b \oplus h(r))$$

Открытие секрета

Алиса посылает r

Эта схема:

- Безусловная связанность

Привязка к биту I

Подготовительный шаг

Фиксируем одностороннюю перестановку F
и предикат h

Привязка

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = (F(r), b \oplus h(r))$$

Открытие секрета

Алиса посылает r

Эта схема:

- Безусловная связанность
- Вычислительная секретность

Привязка к биту II

Подготовительный шаг

Фиксируем простое p и первообразный корень g

Привязка к биту II

Подготовительный шаг

Фиксируем простое p и первообразный корень g

Привязка в два шага

Боб выбирает случайное q, посылает Алисе $y = g^q$

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = y^b g^r$$

Привязка к биту II

Подготовительный шаг

Фиксируем простое p и первообразный корень g

Привязка в два шага

Боб выбирает случайное q, посылает Алисе $y = g^q$

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = y^b g^r$$

Открытие секрета

Алиса посылает r

Привязка к биту II

Подготовительный шаг

Фиксируем простое p и первообразный корень g

Привязка в два шага

Боб выбирает случайное q, посылает Алисе $y = g^q$

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = y^b g^r$$

Открытие секрета

Алиса посылает r

Эта схема:

Привязка к биту II

Подготовительный шаг

Фиксируем простое p и первообразный корень g

Привязка в два шага

Боб выбирает случайное q, посылает Алисе $y = g^q$

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = y^b g^r$$

Открытие секрета

Алиса посылает r

Эта схема:

- Безусловная связанность

Привязка к биту II

Подготовительный шаг

Фиксируем простое p и первообразный корень g

Привязка в два шага

Боб выбирает случайное q, посылает Алисе $y = g^q$

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = y^b g^r$$

Открытие секрета

Алиса посылает r

Эта схема:

- Безусловная связанность
- Вычислительная секретность

Привязка к биту II

Подготовительный шаг

Фиксируем простое p и первообразный корень g

Привязка в два шага

Боб выбирает случайное q, посылает Алисе $y = g^q$

Алиса выбирает случайное r, посылает Бобу

$$C(b, r) = y^b g^r$$

Открытие секрета

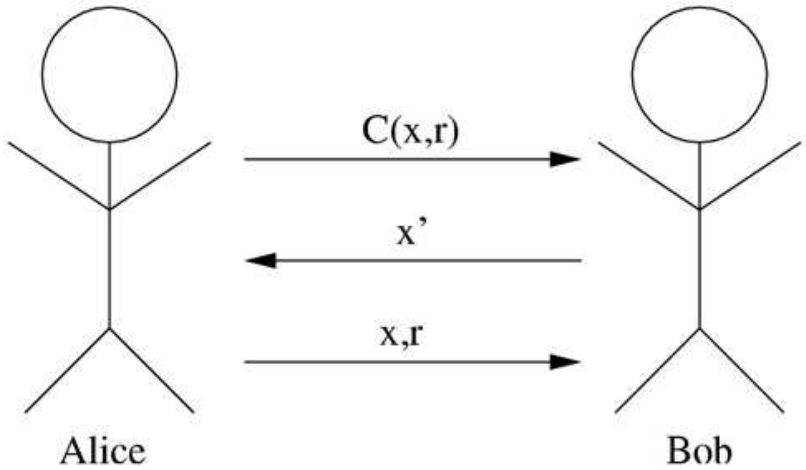
Алиса посылает r

Эта схема:

- Безусловная связанность
- Вычислительная секретность

Могут ли одновременно достигаться и безусловная связанность и безусловная секретность?

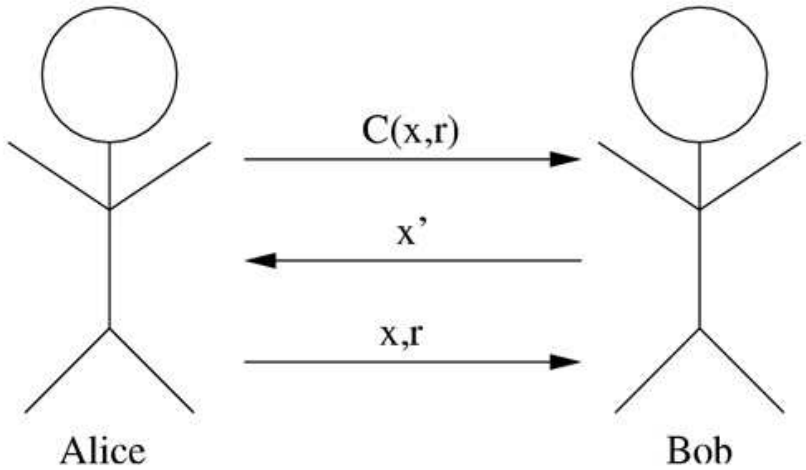
Подбрасывание монетки



Шаги:

Алиса подкидывает монетку и в связанном состоянии посылает результат x Бобу

Подбрасывание монетки

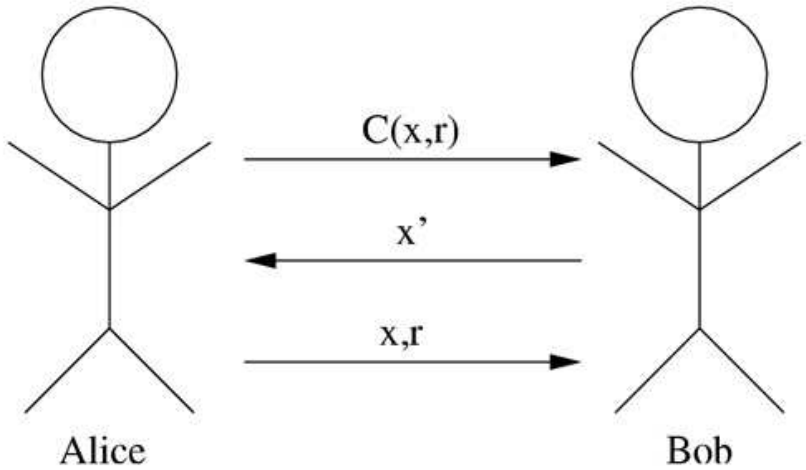


Шаги:

Алиса подкидывает монетку и в связанном состоянии посылает результат x Бобу

Боб посылает догадку x' Алисе

Подбрасывание монетки



Шаги:

Алиса подкидывает монетку и в связанном состоянии посылает результат x Бобу

Боб посылает догадку x' Алисе

Алиса открывает x

План лекции

Разделение секрета

- Визуальная криптография
- Проверяемое разделение секрета
- Пороговая криптография

Последний слайд

Если не запомните ничего другого:

- Схемы разделения секрета “t из n” могут быть основаны на интерполяции многочленов или пересечении гиперплоскостей.

Последний слайд

Если не запомните ничего другого:

- Схемы разделения секрета "t из n" могут быть основаны на интерполяции многочленов или пересечении гиперплоскостей.
- Привязка к биту может быть безусловно связанной и вычислительно секретной или наоборот

Последний слайд

Если не запомните ничего другого:

- Схемы разделения секрета "t из n" могут быть основаны на интерполяции многочленов или пересечении гиперплоскостей.
- Привязка к биту может быть безусловно связанной и вычислительно секретной или наоборот
- Подбрасывание монетки делается с помощью привязки к биту

Последний слайд

Если не запомните ничего другого:

- Схемы разделения секрета "t из n" могут быть основаны на интерполяции многочленов или пересечении гиперплоскостей.
- Привязка к биту может быть безусловно связанной и вычислительно секретной или наоборот
- Подбрасывание монетки делается с помощью привязки к биту

Последний слайд

Если не запомните ничего другого:

- Схемы разделения секрета "t из n" могут быть основаны на интерполяции многочленов или пересечении гиперплоскостей.
- Привязка к биту может быть безусловно связанной и вычислительно секретной или наоборот
- Подбрасывание монетки делается с помощью привязки к биту

Вопросы?