Псевдослучайные генераторы

Лекция N 9 курса
“Современные задачи криптографии”
СПбГУ — SPRINT Lab

Юрий Лифшиц
yura@logic.pdmi.ras.ru

Лаборатория мат. логики ПОМИ РАН

Осень’2005

План лекции

1. Понятие псевдослучаного генератора
2. Односторонние функции и генераторы
3. Криптосистема на основе генератора
4. Задача

План лекции

Основные понятия

Два распределения D_1, D_2 называются вычислительно неразличимыми, если

Основные понятия

Два распределения D_1, D_2 называются вычислительно неразличимыми, если для любого полиномиального вероятностного алгоритма A

$$|Pr_{x \leftarrow D_1}[A(x) = 1] - Pr_{x \leftarrow D_2}[A(x) = 1]| = \nu(|x|)$$

Основные понятия

Два распределения D_1, D_2 называются вычислительно неразличимыми, если для любого полиномиального вероятностного алгоритма A

$$|Pr_{x \leftarrow D_1}[A(x) = 1] - Pr_{x \leftarrow D_2}[A(x) = 1]| = \nu(|x|)$$

Функция $G : X \to Y$ называется псевдослучайным генератором, если

Основные понятия

Два распределения D_1, D_2 называются вычислительно неразличимыми, если для любого полиномиального вероятностного алгоритма A

$$|Pr_{x \leftarrow D_1}[A(x) = 1] - Pr_{x \leftarrow D_2}[A(x) = 1]| = \nu(|x|)$$

Функция $G : X \to Y$ называется псевдослучайным генератором, если $G(\mathcal{U}_X)$ и $\mathcal{U}_Y$ — вычислительно неразличимы ($\mathcal{U}_X, \mathcal{U}_Y,$ — равномерные распределения)

Основные понятия

Два распределения D_1, D_2 называются вычислительно неразличимыми, если для любого полиномиального вероятностного алгоритма A

$$|Pr_{x \leftarrow D_1}[A(x) = 1] - Pr_{x \leftarrow D_2}[A(x) = 1]| = \nu(|x|)$$

Функция $G : X \to Y$ называется псевдослучайным генератором, если $G(\mathcal{U}_X)$ и $\mathcal{U}_Y$ — вычислительно неразличимы ($\mathcal{U}_X, \mathcal{U}_Y,$ — равномерные распределения)

Итересно, только когда: $|Y| >> |X|$

Применения генераторов

- Криптография
  - Каждый генератор можно использовать как криптосистему с секретным ключом.
    Псевдослучайные генераторы - идеальная модель для блочных шифров.

Применения генераторов

- Криптография
  - Каждый генератор можно использовать как криптосистему с секретным ключом.
    Псевдослучайные генераторы - идеальная модель для блочных шифров.
- Построение алгоритмов
  - Использовать меньше случайных битов в вероятностных алгоритмах

Применения генераторов

- Криптография
  - Каждый генератор можно использовать как криптосистему с секретным ключом.
    Псевдослучайные генераторы - идеальная модель для блочных шифров.
- Построение алгоритмов
  - Использовать меньше случайных битов в вероятностных алгоритмах
- Теория сложности
  - $\mathrm{BPP} \subset \cap_{\varepsilon} DTIME(2^{n^{\varepsilon}})$

О предположениях в криптографии

Знаменитая проблема:

$\mathsf{P}=\mathsf{NP}$ или $\mathsf{P}\neq\mathsf{NP}$?

О предположениях в криптографии

Знаменитая проблема:

P=**NP** или **P**≠**NP**?

Если P=NP:

Не будет нулевого разглашения для **NP**

Не будет криптосистем с открытым ключом

Не будет передачи данных вслепую

Не будет электронных выборов

Разделение секрета выживет!

О предположениях в криптографии

Знаменитая проблема:

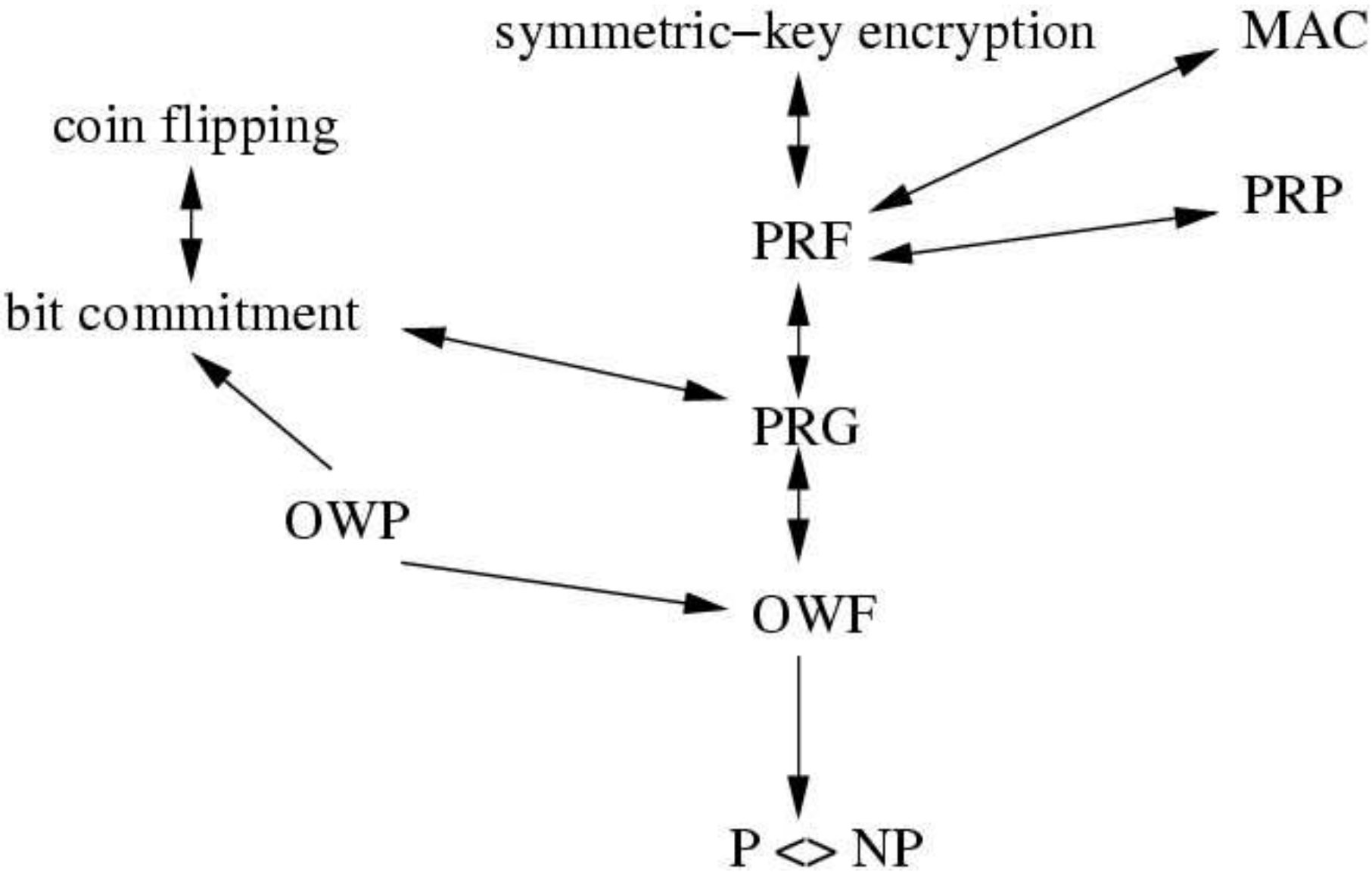
$\mathbf{P}=\mathbf{NP}$ или $\mathbf{P}\neq\mathbf{NP}$?

Если P=NP:

Не будет нулевого разглашения для **NP**
Не будет криптосистем с открытым ключом
Не будет передачи данных вслепую
Не будет электронных выборов
Разделение секрета выживет!

Следствие:

Стойкость всех конструкция основана на **предположениях**
Два базовых предположения: $\mathbf{P}\neq\mathbf{NP}$ и
существование односторонних функций


symmetric−key encryption
MAC
coin flipping
PRP
PRF
bit commitment
PRG
OWP
OWF
P <> NP

Физические генераторы

Альтернативные источники случайности:

- Помехи
- Траектория мышки
- Физические наблюдения
- Трансцендентные числа?

Физические генераторы

Альтернативные источники случайности:

- Помехи
- Траектория мышки
- Физические наблюдения
- Трансцендентные числа?

Возможные проблемы:

- Баланс между 0 и 1
- Корреляция

План лекции

1. Понятие псевдослучаного генератора
2. **Односторонние функции и генераторы**
3. Криптосистема на основе генератора
4. Задача

Односторонние функции

Напомните определение односторонней функции

Односторонние функции

Напомните определение односторонней функции

Функция $F : \{0,1\}^n \to \{0,1\}^m$ называется односторонней функцией, если

1) Функция F вычислима за полиномиальное время

Односторонние функции

Напомните определение односторонней функции

Функция $F : \{0,1\}^n \longrightarrow \{0,1\}^m$ называется односторонней функцией, если

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

Односторонние функции

Напомните определение односторонней функции

Функция $F : \{0,1\}^n \to \{0,1\}^m$ называется односторонней функцией, 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 $h(x)$

Односторонние функции

Напомните определение односторонней функции

Функция $F : \{0,1\}^n \to \{0,1\}^m$ называется односторонней функцией, 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 $h(x)$

Односторонние функции

Напомните определение односторонней функции

Функция $F : \{0,1\}^n \to \{0,1\}^m$ называется односторонней функцией, 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 $h(x)$

Функция F называется односторонней перестановкой, если $m = n$, она биективна и является односторонней функцией

Теорема

Псевдослучайный генератор $G : \{0,1\}^n \longrightarrow \{0,1\}^{n+1}$ *является односторонней функцией*

PRG $\Rightarrow$ OWF

Теорема

Псевдослучайный генератор $G : \{0,1\}^n \to \{0,1\}^{n+1}$ *является односторонней функцией*

Доказательство.

TBD $\square$

OWP $\Rightarrow$ PRG - часть 1

Теорема

Если существуют односторонние перестановки, то можно построить и псевдослучайный генератор
$G : \{0,1\}^n \to \{0,1\}^{n+1}$

OWP $\Rightarrow$ PRG - часть 1

Теорема

Если существуют односторонние перестановки, то можно построить и псевдослучайный генератор
$G : \{0,1\}^n \to \{0,1\}^{n+1}$

Доказательство.

TBD $\square$

OWP $\Rightarrow$ PRG - часть 2

Теорема

Если есть псевдослучайный генератор $G : \{0,1\}^n \to \{0,1\}^{n+1}$, *то можно построить и генератор* $G' : \{0,1\}^n \to \{0,1\}^{f(n)}$ *для любого полинома* f

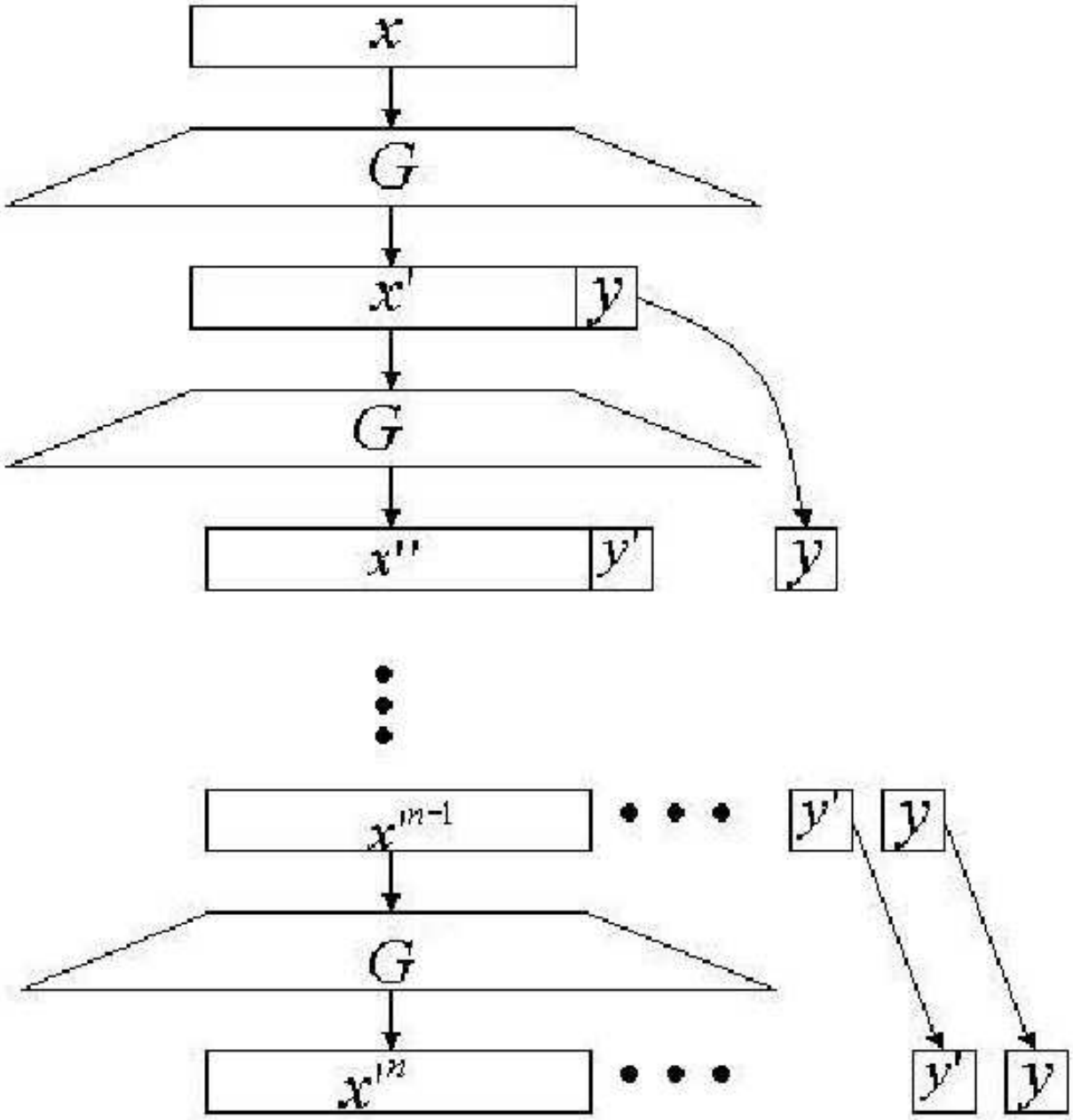
OWP $\Rightarrow$ PRG - часть 2

Теорема

Если есть псевдослучайный генератор $G : \{0,1\}^n \to \{0,1\}^{n+1}$, *то можно построить и генератор* $G' : \{0,1\}^n \to \{0,1\}^{f(n)}$ *для любого полинома* f

Доказательство.

TBD $\square$


x
G
x'
y
G
x''
y'
y
x^(n-1)
y'
y
G
x^(n)
y'
y

План лекции

1. Понятие псевдослучаного генератора
2. Односторонние функции и генераторы
3. **Криптосистема на основе генератора**
4. Задача

Описание криптосистемы

Пусть f — односторонняя перестановка с секретом. Для кодирования строки $b_1 b_2 \dots b_k$ возьмем случайное x и определим

$$E_f(b_1 b_2 \dots b_k) = f^{(k)(x)} \cdot (B(x) \oplus b_1) \cdot \dots \cdot (B(f^{(k-1)}(x)) \oplus b_k)$$

Семантическая стойкость

Алгоритм шифрования E называется семантически стойким, если для любой пары x, y распределения $E(x)$ и $E(y)$ являются вычислительно неразличимыми.

Семантическая стойкость

Алгоритм шифрования E называется семантически стойким, если для любой пары x, y распределения $E(x)$ и $E(y)$ являются вычислительно неразличимыми.

Следствие из Теоремы 3:

Криптосистема на основе псевдослучайного генератора является семантически стойкой

План лекции

1. Понятие псевдослучаного генератора
2. Односторонние функции и генераторы
3. Криптосистема на основе генератора
4. **Задача**

Задача

Пусть есть физический источник независимых битов, но вероятности 0 и 1 немного отличаются (неизвестно как). Как получить действительно случайную последовательность?

Последний слайд

Если не запомните ничего другого:

- Псевдослучайный генератор преобразует короткие строчки в длинные так, что их нельзя отличить от случайных

Последний слайд

Если не запомните ничего другого:

- Псевдослучайный генератор преобразует короткие строчки в длинные так, что их нельзя отличить от случайных
- Псевдослучайные генераторы существуют при предположении существования односторонних перестановок

Последний слайд

Если не запомните ничего другого:

- Псевдослучайный генератор преобразует короткие строчки в длинные так, что их нельзя отличить от случайных
- Псевдослучайные генераторы существуют при предположении существования односторонних перестановок
- Псевдослучайные генераторы являются моделью блочных шифров

Последний слайд

Если не запомните ничего другого:

- Псевдослучайный генератор преобразует короткие строчки в длинные так, что их нельзя отличить от случайных
- Псевдослучайные генераторы существуют при предположении существования односторонних перестановок
- Псевдослучайные генераторы являются моделью блочных шифров

Последний слайд

Если не запомните ничего другого:

- Псевдослучайный генератор преобразует короткие строчки в длинные так, что их нельзя отличить от случайных
- Псевдослучайные генераторы существуют при предположении существования односторонних перестановок
- Псевдослучайные генераторы являются моделью блочных шифров

Вопросы?