Введение в нулевое разглашение

Лекция N 5 курса "Современные задачи криптографии"

Юрий Лифшиц
yura@logic.pdmi.ras.ru

СПбГУ - SPRINT Lab

Осень'2005

План лекции

1. Интерактивные доказательства
2. Примеры интерактивных доказательств
3. Нулевое разглашение
   - Определение нулевого разглашения
   - Доказываем нулевое разглашение
4. Задачи

План лекции

Обычные доказательства

Как устроены доказательства?

- Есть список *аксиом*
- Определены *правила вывода*
- Доказательство — это последовательность утверждений, начинающаяся с аксиом. Каждое следующее утверждение получено по одному из правил из предыдущих строк

Доказательства для NP

(Формальный) язык — набор строк конечной длины из 0 и 1.

Доказательства для NP

(Формальный) язык — набор строк конечной длины из 0 и 1.

NP — класс языков. Язык L принадлежит **NP**, если существует полиномиальный алгоритм P, такой что $x \in L \Leftrightarrow \exists y : P(x, y) = 1$.

Доказательства для NP

(Формальный) язык — набор строк конечной длины из 0 и 1.

NP — класс языков. Язык L принадлежит **NP**, если существует полиномиальный алгоритм P, такой что $x \in L \Leftrightarrow \exists y : P(x, y) = 1$.

Неформально, **NP**— это те языки, принадлежность которым можно проверить перебором.

Доказательства для NP

(Формальный) язык — набор строк конечной длины из 0 и 1.

NP — класс языков. Язык L принадлежит **NP**, если существует полиномиальный алгоритм P, такой что $x \in L \Leftrightarrow \exists y : P(x, y) = 1$.

Неформально, **NP**— это те языки, принадлежность которым можно проверить перебором.

Для $x \in L$ значение такого y, что $P(x, y) = 1$, является "доказательством" принадлежности языку

Интерактивные доказательства

Инфраструктура

Два участника: **P** и **V**, строка x, язык L

P хочет убедить **V**, что $x \in L$

Они по очереди посылают сообщения друг другу

Через конечное число раундов **V** принимает или отвергает доказательство

Интерактивные доказательства

Инфраструктура

Два участника: $\mathbf{P}$ и $\mathbf{V}$, строка x, язык L

$\mathbf{P}$ хочет убедить $\mathbf{V}$, что $x \in L$

Они по очереди посылают сообщения друг другу

Через конечное число раундов $\mathbf{V}$ принимает или отвергает доказательство

Требования

Полнота $\quad \forall x \in L, \exists \mathbf{P} : [\mathbf{P}(x), \mathbf{V}(x)] = 1$

Корректность $\quad \forall x \notin L, \forall \mathbf{P}' : Pr([\mathbf{P}'(x), \mathbf{V}(x)] = 1) = \nu(|x|)$

Интерактивные доказательства

Инфраструктура

Два участника: $\mathbf{P}$ и $\mathbf{V}$, строка x, язык L

$\mathbf{P}$ хочет убедить $\mathbf{V}$, что $x \in L$

Они по очереди посылают сообщения друг другу

Через конечное число раундов $\mathbf{V}$ принимает или отвергает доказательство

Требования

Полнота $\quad \forall x \in L, \exists \mathbf{P} : [\mathbf{P}(x), \mathbf{V}(x)] = 1$

Корректность $\quad \forall x \notin L, \forall \mathbf{P}' : Pr([\mathbf{P}'(x), \mathbf{V}(x)] = 1) = \nu(|x|)$

Обычно считают, что $\mathbf{V}$ пользуется полиномиальным вероятностным алгоритмом, а $\mathbf{P}$ вычислительно не ограничен.

IP = PSPASE

Предложите схему интерактивного доказательства для языков из класса **NP**

IP = PSPASE

Предложите схему интерактивного доказательства для языков из класса **NP**

Возник вопрос, для каких языков существуют интерактивные доказательства?

Предложите схему интерактивного доказательства для языков из класса **NP**

Возник вопрос, для каких языков существуют интерактивные доказательства?

PSPACE — класс языков. Язык L принадлежит **PSPACE**, если существует алгоритм P, использующий полиномиальный объем памяти, такой что $x \in L \Leftrightarrow P(x) = 1$.

IP = PSPASE

Предложите схему интерактивного доказательства для языков из класса **NP**

Возник вопрос, для каких языков существуют интерактивные доказательства?

PSPACE — класс языков. Язык L принадлежит **PSPACE**, если существует алгоритм P, использующий полиномиальный объем памяти, такой что $x \in L \Leftrightarrow P(x) = 1$.

Теорема [Шамир, 1990]: IP = PSPACE

План лекции

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

1. P выбирает случайную перестановку π и посылает $\pi \circ G_1$

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

1. **P** выбирает случайную перестановку π и посылает $\pi \circ G_1$
2. **V** посылает случайное b

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

1. **P** выбирает случайную перестановку π и посылает $\pi \circ G_1$
2. **V** посылает случайное b
3. В зависимости от b, **P** посылает ϕ или $\pi \circ \phi$

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

1. **P** выбирает случайную перестановку π и посылает $\pi \circ G_1$
2. **V** посылает случайное b
3. В зависимости от b, **P** посылает ϕ или $\pi \circ \phi$
4. Шаги 1-3 повторяются 1000 раз

NISO доказательство

Pсобирается доказать $G_0 \not\cong G_1$.

NISO доказательство

Pсобирается доказать $G_0 \not\cong G_1$.

1. **V** выбирает случайное b и случайную перестановку π и посылает $\pi \circ G_b$

NISO доказательство

Pсобирается доказать $G_0 \not\cong G_1$.

1. **V** выбирает случайное b и случайную перестановку π и посылает $\pi \circ G_b$
2. **P** пытается угадать b

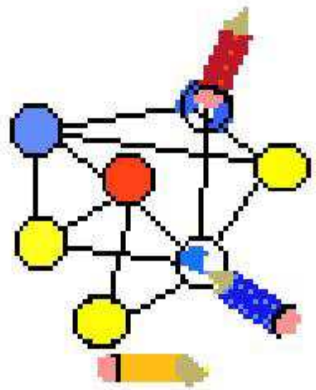
NISO доказательство

Pсобирается доказать $G_0 \not\cong G_1$.

1. **V** выбирает случайное b и случайную перестановку π и посылает $\pi \circ G_b$
2. **P** пытается угадать b
3. Шаги 1-2 повторяются 1000 раз

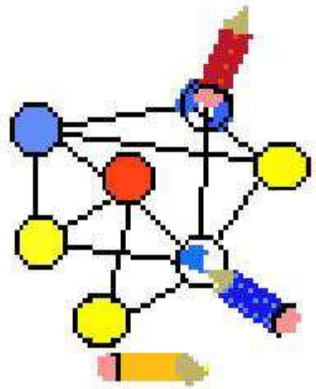
3-раскрашиваемость

P собирается доказать, что граф G правильным образом раскрашивается в три цвета.



3-раскрашиваемость

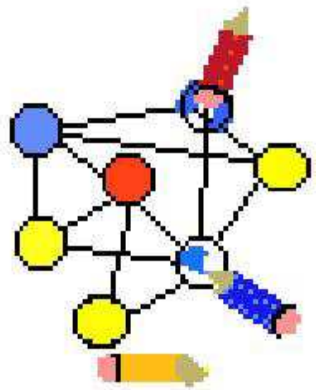
P собирается доказать, что граф G правильным образом раскрашивается в три цвета.



1. **P** случайным образом переставляет три цвета между собой

3-раскрашиваемость

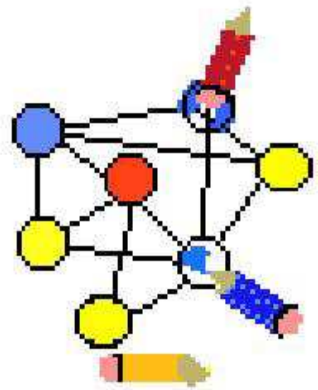
P собирается доказать, что граф G правильным образом раскрашивается в три цвета.



1. P случайным образом переставляет три цвета между собой
2. P коммитит (т.е. использует привязку к биту) цвета всех вершин

3-раскрашиваемость

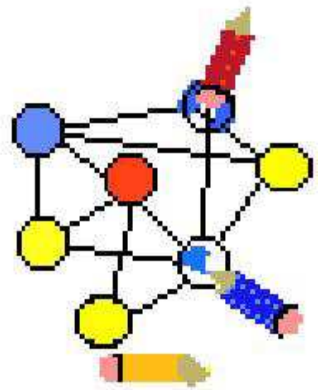
P собирается доказать, что граф G правильным образом раскрашивается в три цвета.



1. **P** случайным образом переставляет три цвета между собой
2. **P** коммитит (т.е. использует привязку к биту) цвета всех вершин
3. **V** выбирает случайную пару вершин

3-раскрашиваемость

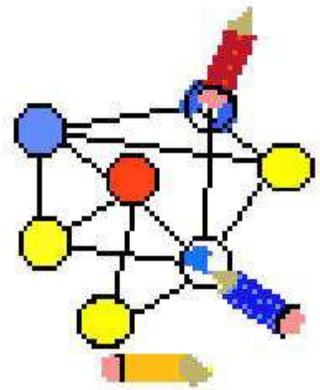
P собирается доказать, что граф G правильным образом раскрашивается в три цвета.



1. **P** случайным образом переставляет три цвета между собой
2. **P** коммитит (т.е. использует привязку к биту) цвета всех вершин
3. **V** выбирает случайную пару вершин
4. **P** открывает цвета этих вершин

3-раскрашиваемость

P собирается доказать, что граф G правильным образом раскрашивается в три цвета.



1. P случайным образом переставляет три цвета между собой
2. P коммитит (т.е. использует привязку к биту) цвета всех вершин
3. V выбирает случайную пару вершин
4. P открывает цвета этих вершин
5. Шаги 1-4 повторяются $1000n^2$ раз

План лекции

1. Интерактивные доказательства
2. Примеры интерактивных доказательств
3. **Нулевое разглашение**
   - Определение нулевого разглашения
   - Доказываем нулевое разглашение
4. Задачи

Подготовка

Пусть у **P** и **V** есть какая-то теорема ($x \in L$).

Что мы тогда будем считать знанием об x?

Подготовка

Пусть у **P** и **V** есть какая-то теорема ($x \in L$).
Что мы тогда будем считать знанием об x?

Все что можно вычислить за полиномиальное время, интереса для **V** не представляет. Он может узнать это самостоятельно.

Подготовка

Пусть у **P** и **V** есть какая-то теорема ($x \in L$).
Что мы тогда будем считать знанием об x?

Все что можно вычислить за полиномиальное время, интереса для **V** не представляет. Он может узнать это самостоятельно.

Набросок определения: интерактивное доказательство обладает **нулевым разглашением**, если все что **V** узнал об x, он мог вычислить самостоятельно.

Первая попытка

Пара алгоритмов (**P**, **V**), образующих интерактивное доказательство, обладает нулевым разглашением, если:

$$\exists S_{PPT} \forall x \in L : VIEW_{\mathbf{P},\mathbf{V}}[x] = S[x],$$

где *VIEW* — последовательность сообщений, полученных **V**

Первая попытка

Пара алгоритмов (**P**, **V**), образующих интерактивное доказательство, обладает нулевым разглашением, если:

$$\exists S_{PPT} \forall x \in L : VIEW_{\mathbf{P},\mathbf{V}}[x] = S[x],$$

где *VIEW* — последовательность сообщений, полученных **V**

То есть **V** может самостоятельно “симулировать” диалог с **P**.

Первая попытка

Пара алгоритмов (**P**, **V**), образующих интерактивное доказательство, обладает нулевым разглашением, если:

$$\exists S_{PPT} \forall x \in L : VIEW_{\mathbf{P},\mathbf{V}}[x] = S[x],$$

где *VIEW* — последовательность сообщений, полученных **V**

То есть **V** может самостоятельно "симулировать" диалог с **P**.

Является ли это условие достаточным для полного неразглашения?

Вторая попытка

Нулевое разглашение, версия 2:

$$\forall \mathbf{V'}\ \exists S_{PPT}\ \forall x \in L : VIEW_{\mathbf{P},\mathbf{V'}}[x] = S'[x]$$

Вторая попытка

Нулевое разглашение, версия 2:

$$\forall \mathbf{V'}\ \exists S_{PPT}\ \forall x \in L : VIEW_{\mathbf{P},\mathbf{V'}}[x] = S'[x]$$

Так же вводится еще более сильное свойство (симулятор с оракульным доступом):

$$\exists S_{PPT}\ \forall \mathbf{V'}\ \forall x \in L : VIEW_{\mathbf{P},\mathbf{V'}}[x] = S'^{V'}[x]$$

Применения нулевого разглашения

Многосторонние вычисления — взаимный контроль участников

Применения нулевого разглашения

Многосторонние вычисления — взаимный контроль участников

Протоколы авторизации — подслушивание бесполезно!

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

1. P выбирает случайную перестановку π и посылает $\pi \circ G_1$

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

1. **P** выбирает случайную перестановку π и посылает $\pi \circ G_1$
2. **V** посылает случайное b

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

1. **P** выбирает случайную перестановку π и посылает $\pi \circ G_1$
2. **V** посылает случайное b
3. В зависимости от b, **P** посылает ϕ или $\pi \circ \phi$

ISO доказательство

P собирается доказать $G_0 \cong G_1$. Он знает изоморфизм ϕ.

1. **P** выбирает случайную перестановку π и посылает $\pi \circ G_1$
2. **V** посылает случайное b
3. В зависимости от b, **P** посылает ϕ или $\pi \circ \phi$
4. Шаги 1-3 повторяются 1000 раз

Определяем симулятор

$\forall \mathbf{V'} \exists S_{PPT} \forall x \in L : VIEW_{\mathbf{P},\mathbf{V'}}[x] = S'[x]$

Определяем симулятор

$\forall \mathbf{V'} \exists S_{PPT} \forall x \in L : VIEW_{\mathbf{P},\mathbf{V'}}[x] = S'[x]$

Алгоритм ISO-симулятора:

1. Выбираем случайное b, случайную перестановку π

Определяем симулятор

$\forall \mathbf{V'} \exists S_{PPT} \forall x \in L : VIEW_{\mathbf{P},\mathbf{V'}}[x] = S'[x]$

Алгоритм ISO-симулятора:

1. Выбираем случайное b, случайную перестановку π
2. Скармливаем граф πG_b алгоритму $\mathbf{V'}$

Определяем симулятор

$\forall \mathbf{V'} \exists S_{PPT} \forall x \in L : VIEW_{\mathbf{P},\mathbf{V'}}[x] = S'[x]$

Алгоритм ISO-симулятора:

1. Выбираем случайное b, случайную перестановку π
2. Скармливаем граф πG_b алгоритму **V'**
3. Если **V'** просит показать изоморфизм для G_b — показываем π, если для $G_{\bar{b}}$ — сбрасываем память **V'** и пробуем еще раз

Определяем симулятор

$\forall \mathbf{V'} \exists S_{PPT} \forall x \in L : VIEW_{\mathbf{P},\mathbf{V'}}[x] = S'[x]$

Алгоритм ISO-симулятора:

1. Выбираем случайное b, случайную перестановку π
2. Скармливаем граф πG_b алгоритму **V'**
3. Если **V'** просит показать изоморфизм для G_b — показываем π, если для $G_{\bar{b}}$ — сбрасываем память **V'** и пробуем еще раз
4. Цикл по шагам 1-3 повторяем до 1000 успешных итераций

Изучаем симулятор

Какова вероятность успеха на шаге 3 (т.е. мы сможем ответить **V'**)?

Изучаем симулятор

Какова вероятность успеха на шаге 3 (т.е. мы сможем ответить **V'**)?

Этот шанс — $1/2$. Следовательно, математическое ожидание работы симулятора — полиномиально.

Изучаем симулятор

Какова вероятность успеха на шаге 3 (т.е. мы сможем ответить **V'**)?

Этот шанс — $1/2$. Следовательно, математическое ожидание работы симулятора — полиномиально.

Симулятор порождает последовательность сообщений, которая могла быть на самом деле.

Изучаем симулятор

Какова вероятность успеха на шаге 3 (т.е. мы сможем ответить **V'**)?

Этот шанс — $1/2$. Следовательно, математическое ожидание работы симулятора — полиномиально.

Симулятор порождает последовательность сообщений, которая могла быть на самом деле.

Все ли мы проверили?

Завершение доказательства

Убедимся, что симулятор с равной вероятностью выдает *случайную* последовательность сообщений между **P** и **V**':

- Фазы независимы между собой
- Мы включаем/не включаем фазы *независимо* от их содержания

Завершение доказательства

Убедимся, что симулятор с равной вероятностью выдает *случайную* последовательность сообщений между **P** и **V**':

- Фазы независимы между собой
- Мы включаем/не включаем фазы *независимо* от их содержания

Аналогия:

Студент стоит спиной к доске
Профессор выписал случайную последовательность
Студент говорит, какие символы вычеркнуть
То, что осталось — случайная последовательность!

План лекции

1. Интерактивные доказательства
2. Примеры интерактивных доказательств
3. Нулевое разглашение
   - Определение нулевого разглашения
   - Доказываем нулевое разглашение
4. **Задачи**

Задачи на дом

Докажите, что $\mathsf{IP} \subseteq \mathsf{PSPACE}$

Задачи на дом

Докажите, что IP$\subseteq$PSPACE

Пусть $N = pq$. Пусть у остатка x символ Лежандра равен 1, т.е. или $x \equiv y^2 \mod N$, или x — квадратичный невычет и по модулю p, и по модулю q. Как с нулевым разглашением доказать, что $x \equiv y^2 \mod N$?

Последний слайд

Если не запомните ничего другого:

- Интерактивное доказательство для $x \in L$ — пара алгоритмов, обладающих полнотой и корректностью

Последний слайд

Если не запомните ничего другого:

- Интерактивное доказательство для $x \in L$ — пара алгоритмов, обладающих полнотой и корректностью
- Нулевое разглашение — все, что $\mathbf{V}$ узнал о x, он мог вычислить самостоятельно

Последний слайд

Если не запомните ничего другого:

- Интерактивное доказательство для $x \in L$ — пара алгоритмов, обладающих полнотой и корректностью
- Нулевое разглашение — все, что $\mathbf{V}$ узнал о x, он мог вычислить самостоятельно
- Задачи на дом: IP$\subseteq$PSPACE, нулевое разглашение для квадратичных вычетов по составному модулю

Последний слайд

Если не запомните ничего другого:

- Интерактивное доказательство для $x \in L$ — пара алгоритмов, обладающих полнотой и корректностью
- Нулевое разглашение — все, что $\mathbf{V}$ узнал о x, он мог вычислить самостоятельно
- Задачи на дом: IP$\subseteq$PSPACE, нулевое разглашение для квадратичных вычетов по составному модулю

Последний слайд

Если не запомните ничего другого:

- Интерактивное доказательство для $x \in L$ — пара алгоритмов, обладающих полнотой и корректностью
- Нулевое разглашение — все, что $\mathbf{V}$ узнал о x, он мог вычислить самостоятельно
- Задачи на дом: IP$\subseteq$PSPACE, нулевое разглашение для квадратичных вычетов по составному модулю

Вопросы?