

Доказательства с неразглашением

Сергей Николенко

Криптография — CS Club, осень 2009

Outline

1 Введение

- Али-Баба и сорок разбойников
- Доказательства
- Интерактивные доказательства
- Доказательства с неразглашением

2 Определения

- Интерактивные доказательства
- Доказательства с неразглашением
- Системы доказательств с неразглашением

История Али-Бабы

- Начну разговор с чудесной истории Али-Бабы и 40 разбойников, записанной J.-J. Quisquater и L. Guillou (и чуть-чуть подправленной для пущего эффекта).
- Всё началось, когда однажды на базаре у Али-Бабы украли кошелёк...

История Али-Бабы

- Али-Баба погнался за разбойником и вбежал за ним в пещеру, проход в которой разветвлялся — можно было пойти налево или направо.
- Оба пути заканчивались тупиками.
- Али-Баба выбрал один из путей, но разбойника там не оказалось. Видимо, повезло разбойнику.
- На следующий день у Али-Бабы стащили чалму...

История Али-Бабы

- ...Когда через сорок дней у Али-Бабы украли последние сандалии, он заподозрил, что что-то здесь неладно.
- Спрятавшись во тьме пещеры, он дождался следующего вбежавшего туда разбойника.
- Добежав до глухой скалы, тот произнёс «Сезам, откройся!», стены пещеры разошлись и пропустили его в другой проход.
- Прибежавший следом за разбойником купец нашёл в тупике Али-Бабу...

История Али-Бабы

- ...и разгорелся жаркий спор; услышав версию Али-Бабы, купец удивился, огорчился, но Али-Бабе не поверил.
- Али-Баба должен был доказать купцу, что в этом проходе раздвигаются стены, но не хотел, чтобы купец слышал волшебные слова.
- Что делать Али-Бабе?

История Али-Бабы

- Али-Баба с купцом решили сделать так.
 - 1 Али-Баба заходит в пещеру и скрывается в одном из проходов.
 - 2 Затем в пещеру заходит купец и кричит: «Али-Баба, выходи!», указывая при этом, слева или справа Али-Бабе нужно выйти.
 - 3 Али-Баба в точности выполняет волю купца.
- После сорока экспериментов купец поверил Али-Бабе и оставил его в покое.

История Али-Бабы

- Али-Баба стал знаменитостью, а волшебные слова передавались в его семье из поколения в поколение.
- В наши дни потомок Али-Бабы, Усама бен-Али, решил напомнить о тайне своей семьи.
- Он организовал телешоу на канале «аль-Блюзира», в котором убеждал телезрителей так же, как когда-то Али-Баба: камеры показывали оба тупика, затем бен-Али скрывался в пещере, а ведущий просил его выйти слева или справа.
- Шоу шло сорок недель, имело грандиозный успех и важное пропагандистское значение: оказалось, что Усама бен-Али владеет подлинной магией! Цены на нефть значительно выросли.

История Али-Бабы

- Телеканал ANN решил посрамить Усаму бен-Али и снять своё шоу, в котором простой американец делал бы то же самое.
- Но, конечно, Усама бен-Али никогда не стал бы сотрудничать с неверными и сообщать им свой секрет.
- Можно ли помочь телеканалу ANN?

История Али-Бабы

- Телеканал ANN смог снять своё шоу. В нём всё происходило точно так же, вот только в половине случаев простой американец не мог выйти с нужной стороны пещеры.
- Но при монтаже эту половину сцен просто вырезали, оставив только подходящие.
- Телеканалу ANN пришлось сделать не сорок дублей, а восемьдесят, но сорок недель точно такого же шоу у него в результате получилось.
- На этом история Али-Бабы заканчивается и начинается математика. :)

Что такое доказательство?

- Что такое «математическое доказательство»?

Что такое доказательство?

- Что такое «математическое доказательство»?
- Философский ответ: нечто, что убеждает других математиков и позволяет им убеждать третьих математиков.

Что такое доказательство?

- Что такое «математическое доказательство»?
- Философский ответ: нечто, что убеждает других математиков и позволяет им убеждать третьих математиков.
- Логический ответ: строка символов, порождённая по некоторым правилам, которую можно проверить на соответствие этим правилам.

Проверяемость

- Иначе говоря, важная характеристика доказательств — *проверяемость*.
- Если я хочу убедить вас, что теорема верна, я должен показать вам такое доказательство, которое вы можете проверить (здесь тоже много философских и практических issues, но в общем так и есть).
- Говоря формально, система доказательств — это эффективно вычисляемая функция, которая проверяет строки на то, являются ли они доказательствами.

Privacy

- Теперь давайте подойдём с другой стороны, с криптографической.
- Если я хочу убедить вас, что теорема верна, я должен показать вам такое доказательство, которое вы можете проверить (здесь тоже много философских и практических issues, но в общем так и есть).
- Могу ли я вас убедить, что у меня есть доказательство, не показывая его?

Наши планы

- Мы сегодня поговорим о том, как лишить доказательства их важнейшего философского свойства: как доказать вам, что теорема верна, так, чтобы вы потом не смогли убеждать в этом других.
- Это и называется *доказательства с неразглашением* (zero-knowledge proofs).
- Начнём с примеров, а потом перейдём к определениям.

Изоморфизм графов

- Вот менее романтический пример, чем история Али-Бабы, но по сути о том же. Пусть у меня есть два графа, и я хочу вам доказать, что они изоморфны.
- Формально говоря, я доказываю, что пара графов (G, H) принадлежит языку $ISO = \{(G, H) \mid G \equiv H\}$.
- Как оформить такое доказательство?

Изоморфизм графов

- Вот менее романтический пример, чем история Али-Бабы, но по сути о том же. Пусть у меня есть два графа, и я хочу вам доказать, что они изоморфны.
- Формально говоря, я доказываю, что пара графов (G, H) принадлежит языку $ISO = \{(G, H) \mid G \equiv H\}$.
- Как оформить такое доказательство?
- Очень просто: я даю вам перестановку π , для которой $\pi(G) = H$, и вы можете быстро проверить моё доказательство.

Не-изоморфизм графов

- Теперь пусть у меня есть два графа, и я хочу вам доказать, что они *не* изоморфны.
- Формально говоря, я доказываю, что пара графов (G, H) принадлежит языку $NISO = \{(G, H) \mid G \not\cong H\}$.
- Как оформить такое доказательство?

Не-изоморфизм графов

- Теперь уже сложнее: можно, например, для каждой перестановки π указать, какие вершины в ней не сходятся.
- Но всего перестановок очень много, и доказательство будет слишком большим.
- Что же делать?

Интерактивные доказательства

- Предположим, что я не просто даю вам доказательство, но могу с вами в течение нескольких раундов содержательно разговаривать.
- Как тогда мне доказать вам, что два графа не изоморфны?

Интерактивные доказательства

- Предположим, что я не просто даю вам доказательство, но могу с вами в течение нескольких раундов содержательно разговаривать.
- Как тогда мне доказать вам, что два графа не изоморфны?
 - 1 Вы случайно выбираете G или H и перестановку π .
 - 2 Посылаете мне результат применения π к выбранному графу.
 - 3 А я должен угадать, какой это был граф.
- Сработает ли такая система доказательств?

Изоморфизм графов

- Пусть у меня есть два графа, и я хочу вам доказать, что они изоморфны.
- Формально говоря, я доказываю, что пара графов (G, H) принадлежит языку $ISO = \{(G, H) \mid G \equiv H\}$.
- Мы уже знаем, как это сделать: я могу просто передать вам перестановку, а вы её проверите.
- Но тогда вы узнаете доказательство и сможете начать убеждать других, показывая им эту перестановку.

Неразглашение

- Интерактивные доказательства нам и здесь помогут. Предположим, что я знаю перестановку φ , для которой $\varphi(G) = H$, а вы нет. Рассмотрим такой протокол.
 - 1 Я случайно выбираю перестановку π и передаю вам $C = \pi(H)$.
 - 2 Вы подбрасываете монетку, выбираете G или H и спрашиваете его у меня.
 - 3 Если вы выбрали G , я передаю вам $\sigma = \pi$, если вы выбрали H , я передаю $\sigma = \pi \circ \varphi$.
 - 4 Вы проверяете, что $\sigma(\text{выбранного графа}) = C$.
- Убеждает ли вас такой протокол в том, что $G \equiv H$?

Неразглашение

- Убеждает — это хорошо. Но, более того, он не позволяет вам ничего узнать о перестановке!
- Если бы я дал вам одновременно π и $\pi \circ \varphi$, вы бы смогли найти φ .
- Но по отдельности π и $\pi \circ \varphi$ — это просто случайные перестановки.
- По одной из них вы не можете ничего узнать о перестановке φ и не можете начать убеждать других в том, что G и H изоморфны.

Outline

1 Введение

- Али-Баба и сорок разбойников
- Доказательства
- Интерактивные доказательства
- Доказательства с неразглашением

2 Определения

- Интерактивные доказательства
- Доказательства с неразглашением
- Системы доказательств с неразглашением

Обычная система доказательств

- Для обычной, логической системы доказательств крайне желательно установить два свойства:
 - 1 *корректность*: доказать можно только верные теоремы;
 - 2 *полнота*: все верные теоремы можно доказать.
- Из курса математической логики вы, наверное, знаете полные и корректные системы доказательств для логики предикатов.

Интерактивная система доказательств

- В интерактивной системе доказательств дела становятся чуть хуже: теперь враг может убедить нас в своей правоте, если он не прав, просто это должно быть маловероятно.
- Как дать определения корректности и полноты в интерактивном случае?

Интерактивная система доказательств

- Полнота: для любого $x \in L$ пружер сможет доказать это с огромной вероятностью:

$$\forall x \in L \Pr [(P, V)(x) = \text{“Да”}] \geq 1 - \epsilon(|x|).$$

- Корректность: для любого $x \notin L$ V сможет «поймать» пружер в достаточно большом числе случаев:

$$\forall x \notin L \forall P' \Pr [(P', V)(x) = \text{“Да”}] \leq \frac{1}{2}.$$

К неразглашению

- Теперь мы хотим определить неразглашение.
- Иными словами, хотим определить тот факт, что V (verifier) не получает от P (prover) *никакой информации*.
Что это значит?

К неразглашению

- Неформальное определение: V в результате разговора не получает никакой новой информации, если V может *самостоятельно*, без помощи P , сгенерировать этот разговор.
- Иными словами, V может за полиномиальное (вероятностное) время произвести на свет протокол своего разговора с P .

Примеры

- Пример: P доказывает V , что $G \equiv H$, передавая ему π :
 $\pi(G) = H$.
- Может ли V сам сгенерировать такой протокол? Конечно, нет.
- Вспомним теперь наш протокол.
 - 1 P случайно выбирает перестановку π и передаёт V граф $C = \pi(H)$.
 - 2 V подбрасывает монетку, выбирает G или H и спрашивает его у P .
 - 3 Если P выбрал G , V передаёт $\sigma = \pi$, если V выбрал H , P передаёт $\sigma = \pi \circ \varphi$.
 - 4 V проверяет, что $\sigma(\text{выбранного графа}) = C$.

Примеры

- Вот как V может сам сгенерировать протокол.
 1. Выбрать случайно π и бит b (выбирающий между G и H).
 2. Вычислить $C = \pi$ (выбранного графа).
- Здесь каждый протокол имеет ту же вероятность появления, что и при разговоре с настоящим пружером.

Определение: первая попытка

- Итак, вот первая попытка дать определение zero-knowledge.

Definition

Протокол (P, V) обладает свойством неразглашения (zero-knowledge), если существует полиномиальный вероятностный алгоритм S (симулятор), который для любого входа x порождает то же распределение на протоколах, что и настоящий разговор между P и V .

Нечестные V

- Однако тут не всё ладно. Что, если V не следует протоколу?
- Подавая какие-либо входы, не соответствующие протоколу, V может вынудить P сообщить какую-нибудь информацию, и наше определение этому никак не препятствует.
- Значит, надо учесть это в определении.

Определение: вторая попытка

- Вторая попытка.

Definition

Протокол (P, V) обладает свойством неразглашения (zero-knowledge), если для любого полиномиального вероятностного алгоритма V' существует полиномиальный вероятностный алгоритм S , который для любого входа x порождает то же распределение на протоколах, что и настоящий разговор между P и V .

- Осталось ещё прояснить, что же входит в протокол.

Пример

- Рассмотрим систему доказательств, которая пытается доказать довольно простой факт: то, что её вход x — натуральное число.
- Но делает она это довольно нетривиальным образом.
 - 1 V выбирает случайное число $x \in \mathbb{Z}_n$ и посылает x^2 .
 - 2 P выбирает случайные корень z : $z^2 = x^2$ и посылает z .

Пример

- Система, очевидно, корректна и полна.
- Обладает ли она свойством неразглашения? По идее, не должна: V при помощи P может вычислять квадратные корни (с вероятностью $\frac{1}{2}$), т.е. может разложить n на множители.
- Но протокол — это всего лишь два сообщения: (x^2, z) .
- Симулятор может просто выбирать случайный z и генерировать (z^2, z) , будет то же самое.
- Что здесь не так?

Случайные биты

- Этот пример показывает, что нужно ещё случайные биты учитывать в протоколе.
- Здесь симулятор может сгенерировать (z^2, z) , но полный протокол, со случайными битами V , будет выглядеть как $((x^2, z), x)$, а его симулированная версия — как $((x^2, x), x)$.
- Т.е. в протокол будем записывать не только переговоры P и V , но и случайные биты V (случайные биты прувера не нужны — его мы как раз удаляем, когда к симулятору переходим).
- Но и это ещё не всё.

Повторяемость и подсказки

- Во-первых, мы бы хотели, чтобы алгоритм можно было повторять.
- Иначе говоря, пружер должен иметь возможность доказать нескольким V свою «теорему», и эти несколько V , даже объединившись, не должны получать информации о доказательстве.
- Во-вторых, просто, если, скажем, V знает половину перестановки, нехорошо, если после разговора с P он узнает всю перестановку.

Подсказки

- Поэтому в определение ещё нужно добавить подсказку (advice) a : дополнительный вход, по которому надо брать квантор всеобщности.

Definition

Протокол (P, V) обладает свойством неразглашения (zero-knowledge), если для любого полиномиального вероятностного алгоритма V' существует полиномиальный вероятностный алгоритм S , который для любого входа x и любой подсказки a порождает то же распределение на протоколах, что и настоящий разговор между P и V :

$$\forall V' \exists S \forall x \in L \forall a \text{VIEW}_{P, V'(a)}(x) = S(x, a).$$

Определение

Definition


(P, V) является *системой доказательств с неразглашением* (zero-knowledge proof system) для языка L , если верны:

полнота: $\forall x \in L \Pr [(P, V)(x) = \text{“Да”}] \geq 1 - \epsilon(|x|)$;

корректность: $\forall x \notin L \forall P' \Pr [(P, V)(x) = \text{“Да”}] \leq \frac{1}{2}$;

неразглашение: $\forall V' \exists S \forall x \in L \forall a \text{VIEW}_{P, V'(a)}(x) = S(x, a)$.

Спасибо за внимание!

- Lecture notes и слайды будут появляться на моей homepage:
`http://logic.pdmi.ras.ru/~sergey/`
- Присылайте любые замечания, решения упражнений, новые численные примеры и прочее по адресам:
`sergey@logic.pdmi.ras.ru`, `snikolenko@gmail.com`
- Заходите в ЖЖ  **smartnik**.