	Доказывающая сторона (P)	Доказательство утверждения	Верификатор (V)	Свойства доказательства
Унаследованное, универсальное доказательство				Теорема является ВЕРНОЙ ⟺ V принял доказательство **Полнота:** Теорема является ВЕРНОЙ ⇒ V определённо принял доказательство: $\mathcal{P}$ [V принял доказательство] ≡ 1 **Целостность:** Теорема является ЛОЖНОЙ ⇒ V не принял доказательство: $\mathcal{P}$ [V принял доказательство] ≡ 0
Пример: утверждение = теорема				**Полнота:** Утверждение является ВЕРНЫМ ⇒ $\mathcal{P}$ [V принял доказательство] > 1/2 **Целостность:** Утверждение является ЛОЖНЫМ ⇒ $\mathcal{P}$ [V принял доказательство] < 1/2 Свойства пороговых значений прохождения (см. примечания ниже) становятся статистическими (в сравнении с идеальными унаследованными).
Примечания	**Интерактивные доказательства (IP)** можно рассматривать в качестве обобщения унаследованных, статистическая природа которых заменяется активной ролью, которую играют Доказывающая сторона и Верификатор, обменивающиеся сообщениями и генерирующие случайные значения, которые затем будут использованы в доказательстве. Пороговое значение правдоподобия, равное ½ можно считать «слишком слабым». Однако, по желанию вероятность может быть повышена с помощью свойства полноты (равно как и снижена свойством целостности) путём многократного повторения доказательства IP и решением большинством голосов, принял V доказательство или нет. Такая стратегия может рассматриваться со всей математической строгостью и/или с непрофессиональной точки зрения: • аналитическое доказательство: неравенство Чебышева или граница Чернова • числовая проверка: вычисление вероятностей с помощью различных пороговых значений и количества повторений • по интуиции: разумно предположить, что вероятность большинства случаев попыток предоставления ложных доказательств будет снижаться с ростом количества повторений (таким образом, будет расти вероятность предоставления дополнительных верных доказательств) Кроме того, при наличии IP у утверждения можно доказать, что для того же самого утверждения мы можем получить IP с идеальной полнотой, то есть, P [V принял доказательство] ≡ 1, при том, что V будет отправлять сообщения, содержащие исключительно сгенерированные им случайные значения. Это так называемый **протокол Артура-Мерлина**, также известный как «**протокол открытой монеты**».			

Доказательство	Доказательство знания (PoK)
доказывает, что утверждение является верным; это происходит благодаря следующим (уже упомянутым) свойствам:	доказывает, что Доказывающей стороне известно нечто, то есть, это доказательство утверждения в форме «доказывающей стороне известно...». Утверждение того, что Доказывающей стороне что-то известно, означает, что она может предоставить некоторое **свидетельство W**, даже если оно не требуется при совершении обычных операций. Поэтому нам необходим новый специальный объект под названием экстрактор:
Идеальная полнота (следует помнить, что это свойство всегда можно сделать идеальным) **Целостность**	**Идеальная полнота** (иногда в этом контексте называется «**нетривиальностью**») существование **Экстрактора знания (KE)** (иногда называется «**валидностью**») по определению является объектом, способным (по необходимости вне ограничений, связанных с выполнением доказательства) выделить **свидетельство W**, касающееся знания, которым обладает Доказывающая сторона, только при **∀P* s.t. $\mathcal{P}$[V принял доказательство] > err**

- V также называется **Верификатором знания**
- Пусть вас не смущает термин «знание»: доказательство PoK может и не предполагать ZK, Zero Knowledge, то есть, нулевого разглашения (фактически, мы и не указывали на наличие такого разглашения): просто Доказывающая сторона отправляет свидетельство Верификатору
- При использовании ZKPoK Экстрактор знания не нарушает принципа нулевого разглашения, так же, как и Симулятор не нарушает принципа Целостности - KE получает W от P, используя возможности, недоступные при обычном выполнении доказательства: у него имеется доступ к оракулу (чёрному ящику) для P (например, он может «отмотать» всё)
- err является **ошибкой Экстрактора** знания в форме порогового значения, задаваемого определением KE, ниже которого нельзя выделить W
- Целостность не указывается среди свойств, поскольку она подразумевается наличием KE, поэтому она называется **Целостностью знания** или **Специальной правильностью**:

KE выделяет W ⇒ утверждение является ВЕРНЫМ (поскольку W является свидетельством утверждения) —если взять противоположное→ **Утверждение является ВЕРНЫМ ⇒ KE не может выделить W ⇒** $\forall P^* \mathcal{P}[\text{V принял доказательство}] \leq \text{err}$

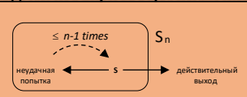
если **err = 0**, целостность является **идеальной**, а **err < 1/2** приводит к **статистической целостности** IP; если **err ≥ 1/2**, мы попадаем в довольно обычную ситуацию, в которой PoK получается через n последовательных повторений оригинального доказательства: в рамках получающегося протокола **KE Error = err^n**, что опять же даёт статистическую целостность для достаточно большого значения **n** («Пещера Али-Бабы» в рамках примера ELI5 такого типа доказательства с помощью успешного повторения базового доказательства со слишком значительной ошибкой)

Аргумент (ARG)	Аргумент знания (ARK)
Доказательство с **вычислительной целостностью**, а следовательно, в контексте вычислений требуется нестрогая целостность, при которой все участвующие стороны будут связаны, то есть, любой злоумышленник P* и добросовестная сторона P (что совсем не обязательно для доказательств, даже если это подразумевается всякий раз, когда мы говорим об их применении в реальном мире).	Доказательство знания с вычислительной целостностью, которое может быть выведено на основе вычислительного Экстрактора знания, например: **Задача DLP является сложной ⇒ вычислительный KE ⇒ вычислительная целостность** (предполагается, что логическая импликация является транзитивной, равно как и сокращение; DLP снова приводится просто как пример)

от IP к ZKP: свойство нулевого разглашения в парадигме симуляции

Доказательство с нулевым разглашением (ZKP) является доказательством IP с одним дополнительным свойством: **нулевым разглашением информации**. Грубо говоря, оно подразумевает, что верификатор V не узнает из доказательства ничего, кроме того, что утверждение является верным. Интуитивно только обмен сообщениями с доказывающей стороной P может стать источником такой информации (если она будет предоставлена), таким образом, чтобы формализовать нулевое разглашение, необходимо продемонстрировать существование объекта, называемого Симулятором S, способного исключительно на совместное с V создание транскрипта обмена сообщениями, неотличимого от оригинального: если транскрипты будут неотличимыми, то и получаемая информация тоже… но из транскрипта, создаваемого S, узнать ничего нельзя, поскольку он не обладает никакими возможностями помимо создания транскриптов, поэтому от него можно узнать то же самое (то есть, ничего), что и из IP. Предполагается, что транскрипты являются случайными переменными, которые характеризуются распределениями (благодаря способности сторон «бросать кубик»). Существует 3 разновидности неразличимости:

Идеальное нулевое разглашение (PZK)



Иногда неудача S случается (самое большее за n попыток) до получения действительного результата, распределение которого должно быть **равным** распределению транскрипта оригинального IP (таким образом может быть снижено общее отношение неудач S_n, для чего и повышалось количество *n*)

⊆

Статистическое нулевое разглашение (SZK)

- При наличии слишком отличных вероятностей в IP и S не может появиться никакого транскрипта *ts*,
- Если какие-либо вероятности транскрипта отличаются между оригинальными вероятностями IP и S, различия должны быть ничтожными:

$\Sigma_{ts} \mid \mathcal{P}[\text{IP} \to ts] - \mathcal{P}[\text{S} \to ts] \mid$ ***является «малой»***

⊆

Вычислительное нулевое разглашение (CZK)

Распределения транскриптов практически неразличимы в сравнении с любыми вычислительно ограниченными объектами.

Явное обнаружение наблюдающего «класса» объектов в доказательстве — непростая задача, поэтому часто всё сводится к решению общепринятой вычислительно сложной задачи (поскольку сложность будет присутствовать, если все объекты будут вычислительно ограничены):

Задача DLP является сложной ⇒ CZK или эквивалент: **не CZK ⇒ Задача DLP неверна**

(DLP означает задачу дискретного логарифмирования и приводится в качестве примера)

Чтобы не нарушить целостность IP (симулятор может произвести действительный транскрипт и выявить недобросовестную доказывающую сторону с её ложным утверждением), S имеет и использует некоторые возможности, недоступные при обычном выполнении IP, например, «**откат» верификатора**». Представьте, что V достиг определённой точки взаимодействия, а потом произошёл откат, и процесс возобновился с предыдущей точки. Это возможно, так как S имеет доступ к V через оракула (чёрный ящик), а это означает, что он может вызвать подпрограмму «следующего сообщения» V, когда ему это будет необходимо. (Всё это также можно рассматривать, как если бы только V является автором симуляции, использующим полный доступ к ресурсам).

Доступ посредством чёрного ящика, не затрагивающий внутренних механизмов V, как известно, не является наиболее частым способом использования V симулятором S. Но это также позволяет задействовать доказательства ZKP, являющиеся закрытыми при секвенциальной композиции (что полезно для сохранения нулевого разглашения, когда IP отправляется повторно для усиления целостности), и встраивать их во внешние протоколы. Более того, сама по себе симуляция является достаточным (⇒), но не необходимым (⇐) условием для поддержания нулевого разглашения, поэтому использование этой парадигмы уже означает отсутствие каких-либо более комплексных допусков.

в преддверии неинтерактивных доказательств с нулевым разглашением (NIZK)

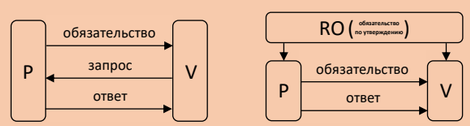
Обмен сообщениями между P и V кажется неизбежным. Учитывая, что S может произвести ложный транскрипт, мы не можем доверять исключительно предлагаемому транскрипту как соответствующему протоколу: доказательство ZKP **не передаётся третьим сторонам** (не участвующим в доказательстве), и, следовательно, для них оно является **спорным**. Тем не менее, 1 сеанс «обмена» (когда P предоставляет V доказательство для последующей проверки) представляет огромный практический интерес, поскольку не требует одновременного присутствия сторон в сети. Чтобы сделать это возможным, **стандартная/простая модель** (которую мы рассматривали до этого момента) дополняется следующими допусками:

CRS

Стимулирующим фактором в данном случае является **наличие существование общей эталонной (/случайной) строки**, которая выводится из некоторого (/равномерного) распределения вероятностей, и известна как P, так и V. Изначальная неэффективность такого подхода была частично решена недавно реализованной криптографией на основе спаривания. Однако, наличие общей строки лишь предполагается, а де-факто требует использования неопределённого протокола **доверенных настроек**, который позволил бы создать её перед предоставлением доказательства NIZK.

Эвристический подход Фиата-Шамира (FS)

Данная стратегия применима к протоколам **Сигма (Σ)**, которые являются «протоколами открытой монеты», структура которых подразумевает наличие 3 этапов: за случайным обязательством P следует случайный запрос V (эта часть обмена может повторяться множество раз), а затем следует ответ P. Хитрость состоит в замене запроса V ответом **случайного оракула (RO)**, доступного как P, так и V:



RO - это идеальная функция, выдающая случайный равномерно распределённый (но всегда один и тот же) ответ для заданных вводных. В случае с FS вводные данные включают все сообщения транскрипта вплоть до вызова RO, поскольку имитация Σ-протокола требует, чтобы вызов ДОКАЗУЕМО (что выгодно V) приходил после его обязательства, тогда случайного «броска» P было бы просто недостаточно. Целостность FS также требует включения всех открытых данных в вводные, например, утверждения, по которому предоставляется доказательство.

Цель состоит в том, чтобы вывести свойства неинтерактивных доказательств из аналогичных свойств доказательств Σ-протокола. Полнота выводится тривиально. Точно так же может быть выведена и целостность. Примечание: результатом FS всегда является Аргумент, поскольку ничем не ограниченный P* может «обойти» RO путём отправки неограниченного количества запросов. В любом случае, пороговое значение целостности в рамках Σ-протокола должно быть снижено, чтобы сбалансировать преимущество FS P* с точки зрения предварительных вычислений.

Свойство нулевого разглашения: будучи случайным, RO действует как честный верификатор методом «открытой монеты». То есть, если исходным доказательством является HVZK, его симулятор может быть использован для подделки транскрипта NIZK. При симуляции сообщения часто выстраиваются не по порядку, поэтому дополнительная возможность «**программировать**» **результаты RO** по своему усмотрению (сохраняя единообразие в целях соответствия заданному распределению) предоставляется S, чтобы отменить зависимость запроса от обязательства. Та же идея применима к «извлекаемости знания».

Случайный оракул по псевдокоду

```
output ← RO(inputs) :=
{
    if permanent_array[inputs] not exist {
        permanent_array[inputs] := new random value
    }
    output ← permanent_array[inputs]
}
```

Эвристический аспект: различные варианты реализации в качестве RO используют удобные (а значит, не идеальные) **хеш-функции**. Безопасность этого способа, как правило, признаётся. Однако, на самом деле, это предмет дальнейших исследований.

Краткое описание свойств	Полнота	Целостность	Нулевое разглашение информации	Нулевое разглашение для честного Верификатора
	связана с парой Доказывающая сторона / Верификатор, где обе стороны являются честными (то есть, следуют протоколу, предписанному доказательством). Относится к **(P, V)**	свойство честного Верификатора, не введённого в заблуждение никакой стратегией Доказывающей стороны, предоставляющей ложное утверждение. Относится к **(∀P*,V)**	Способность Доказывающей стороны не раскрывать какой-либо информации Верификатору (ещё одно преимущество «слепого» доступа S к V посредством чёрного ящика). Относится к **(P,∀V*)**	⊆ Как правило, открытая Доказывающая сторона должна быть устойчива к утечке информации при применении недобросовестным Верификатором какой-либо стратегии, и это слабая форма нулевого разглашения, которая по определению работает только в случае с честным Верификатором. Поэтому относится к **(P,V)**. Тем не менее, это свойство актуально, поскольку иногда подразумевает наличие IP для того же самого утверждения, но с более сильным свойством нулевого разглашения: • HV **SZK** → HV **SZK** для доказателств IP «Артура-Мерлина» → **SZK** для доказателств IP «Артура-Мерлина» • HV **CZK** для доказателств IP «Артура-Мерлина» → **CZK** для доказателств IP «Артура-Мерлина»

Источники и многое другое

- «Принстонский компаньон по математике», издательство Princeton University Press, Тимоти Гауэрс и др. (раздел IV.20, «Вычислительная сложность»)
- «Основы криптографии», издательство Cambridge University Press, Одед Голдрайх (том 1, главы 1 и 4; все соответствующие веб-страницы; список опечаток)
- Посты из блогов Мэтью Грина (здесь и здесь - кстати, моё первое знакомство с доказательствами ZKP), Джереми Кана (здесь, здесь и здесь) и Яника Голдгрэбе (в Medium)
- Раздел Q&A на crypto.stackexchange.com, в частности, ответы, опубликованные Иегудой Линделлом, и Жофруа Куто (некоторые были упорядочены и опубликованы на его веб-странице)
- «Учебное пособие по основам криптографии», издательство Springer, Иегуда Линделл и др. (глава 6 «Как это смоделировать»)
- Кандидатская диссертация Жофруа Куто, содержащая в вводных главах 2 и 3 вполне доступный обзор этой области знания
- «Обзор системы неинтерактивных доказательств с нулевым разглашением и способов её применения», издательство Hindawi, Хуэйсин Ву и Фенг Ванг
- 9-я Зимняя школа Университета имени Бар-Илана (BIU) по криптографии, 18-21 февраля 2019 г. (слайды и видео лекции)

Перевод шпаргалки выполнил v1docq47