ВикипедиЯ

Доказательство с нулевым разглашением

Материал из Википедии — свободной энциклопедии

Доказа́тельство с нулевы́м разглаше́нием (информа́ции) в криптографии (англ. *Zero-knowledge proof*) — интерактивный криптографический протокол, позволяющий одной из взаимодействующих сторон («The verifier» — проверяющей) убедиться в достоверности какого-либо утверждения (обычно математического), не имея при этом никакой другой информации от второй стороны («The prover» — доказывающей). Причём последнее условие является необходимым, так как обычно доказать, что сторона обладает определёнными сведениями в большинстве случаев тривиально, если она имеет право просто раскрыть информацию. Вся сложность состоит в том, чтобы доказать, что у одной из сторон есть информация, не раскрывая её содержания. Протокол должен учитывать, что *доказывающий* сможет убедить *проверяющего* только в случае, если утверждение действительно доказано. В противном случае сделать это будет невозможно, или крайне маловероятно из-за вычислительной сложности.

Под интерактивностью протокола подразумевается непосредственный обмен информацией сторонами[1][2].

Таким образом, рассматриваемый протокол требует наличия интерактивных исходных данных (interactive input) от *проверяющего*, как правило, в виде задачи или проблемы. Цель легального *доказывающего* (имеющего доказательство) в этом протоколе — убедить *проверяющего* в том, что у него есть решение, не выдав при этом даже части «секретного» доказательства («нулевое разглашение»). Цель *проверяющего* же — это удостовериться в том, что доказывающая сторона «не лжёт»[2][3].

Также были разработаны протоколы доказательства с нулевым разглашением[4][5], для которых не требовалось наличия интерактивных исходных данных, при этом доказательство которых, как правило, опирается на предположение об идеальной криптографической хеш-функции, то есть предполагается, что выход однонаправленной хеш-функции невозможно предсказать, если неизвестен её вход[6].

Доказательство с нулевым разглашением используется в нескольких блокчейнах, кроме того, находит применение для проверки наличия сведений без передачи самих сведений[7][8].

Содержание

Определение

Доказательство с нулевым разглашением — интерактивный вероятностный протокол, который позволяет доказать, что доказываемое утверждение верно, и Доказывающий знает *это* доказательство, в то же время не предоставляя никакой информации о самом доказательстве данного утверждения[9]. Данный криптографический протокол должен обладать тремя свойствами:

1. **Полнота**: если утверждение действительно верно, то Доказывающий убедит в этом Проверяющего с любой наперед заданной точностью.
2. **Корректность**: если утверждение неверно, то любой, даже «нечестный», Доказывающий не сможет убедить Проверяющего за исключением пренебрежимо малой вероятности.
3. **Нулевое разглашение**: если утверждение верно, то любой, даже «нечестный», Проверяющий не узнает ничего кроме самого факта, что утверждение верно[10].

Доказательства с нулевым разглашением не являются доказательствами в математическом смысле этого термина, потому что есть некоторая небольшая вероятность, что обманом доказывающая сторона сможет убедить Проверяющего в ложном утверждении (ошибка *корректности*). Иными словами, доказательства с нулевым разглашением — это вероятностные доказательства, а не детерминированные. Тем не менее, есть методы, позволяющие уменьшить ошибку *корректности* до пренебрежимо малых значений[11][12].

Различные виды нулевого разглашения

Выполнение протокола *доказательства с нулевым разглашением* приводит к выводу результата *Принять/Отклонить* и также порождает стенограмму доказательства. Различные варианты нулевого разглашения могут быть определены путём формализации самого понятия и сравнения распространения информации различных моделей с протоколом следующими способами[13][14]:

- *Идеальный протокол нулевого разглашения* — если случайные величины в стенограмме доказательства рассматриваемой модели являются равномерно распределенными и не зависят от общих входных данных[15]. Хорошей иллюстрацией будет пример Пегги и Виктора в пещере.
- *Статистически нулевое разглашение*[16] означает, что распределение не обязательно такое же, но они по крайней мере статистически близки, при этом статистическая разница есть незначительная функция[17].
- *С вычислительно нулевым разглашением* называют такую модель, если не существует на данный момент такого эффективного алгоритма, который смог бы отличить распределение величин от распространения информации в идеальном протоколе[18].

История развития


Шафи Гольдвассер

В 1986 году в работе Сильвио Микали, Одеда Голдрейха и Ави Вигдерсона было описано применение доказательств с нулевым разглашением для создания криптографических протоколов, которые должны обеспечивать *«честное поведение»* сторон, сохраняя при этом конфиденциальность[19].

Доказательство с нулевым разглашением было придумано и разработано следующими учёными: Шафи Гольдвассер, Сильвио Микали и Чарльзом Реккофом, и опубликовано ими в статье «Знание и сложность интерактивной системы с доказательством»[20] в 1989 году. Эта работа представила иерархию интерактивных систем с доказательством, основываясь на объёме информации о доказательстве, который необходимо передать от Доказывающего до Проверяющего. Ими также было предложено первое доказательство конкретно поставленного доказательства с нулевым разглашением — квадратичного вычета по некоторому модулю m[21]. Впоследствии, дополнив свою работу, они были удостоены первой премии Гёделя в 1993 году[22].

Ави Вигдерсон

В дальнейшем криптосистема Гольдвассер — Микали, основанная на рассматриваемом интерактивном протоколе, являющаяся криптографической системой с открытым ключом, разработанная Шафи Гольдвассер и Сильвио Микали в 1982 году, является первой схемой вероятностного шифрования с открытым ключом, доказуемо стойкая при стандартных криптографических предположениях. Предложенная система была высоко оценена жюри: Гольдовассер и Микали стали лауреатами Премии Тьюринга за 2012 год[23], за создание криптосистемы с вероятностным шифрованием, отмеченная в номинации как новаторская работа, оказавшая существенное влияние на современную криптографию. Однако, криптосистема является неэффективной, так как порождаемый ею шифротекст может быть в сотни раз длиннее, чем шифруемое сообщение.

Для доказательства свойств стойкости криптосистемы Голдвассер и Микали ввели понятие семантической стойкости[24][25].

В 2021 году Ласло Ловас и Ави Вигдерсон были удостоены Абелевской премии, за их работы в области теоретической информатики, внёсшие важнейший вклад в развитие теории сложности вычислений, теории графов, методы распределенных вычислений и концепцию доказательств с нулевым разглашением[26].

Общая структура доказательств с нулевым разглашением

Каждый раунд, или аккредитация доказательства, состоит из трёх этапов. Схематично их можно изобразить следующим образом:

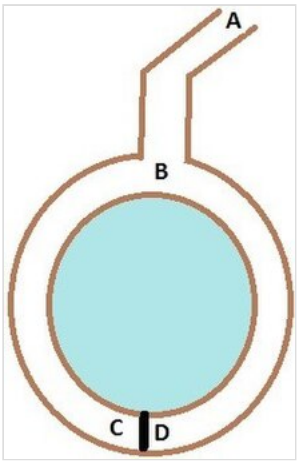
- $A \Rightarrow B$: доказательство (witness)
- $A \Leftarrow B$: вызов (challenge)
- $A \Rightarrow B$: ответ (response)

Сначала *A* выбирает из заранее определённого непустого множества некоторый элемент, который становится её секретом — закрытым ключом. По этому элементу вычисляется, а затем публикуется открытый ключ. Знание секрета определяет множество вопросов, на которые *A* всегда сможет дать правильные ответы. Затем *A* выбирает случайный элемент из множества, по определённым правилам (в зависимости от конкретного алгоритма) вычисляет доказательство и затем отсылает его *B*. После этого *B* выбирает из всего множества вопросов один и просит *A* ответить на него (вызов). В зависимости от вопроса, *A* посылает *B* ответ[27]. Полученной информации *B* достаточно, чтобы проверить действительно ли *A* владеет секретом. Раунды можно повторять сколько угодно раз, пока вероятность того, что *A* «угадывает» ответы, не станет достаточно низкой. Такой подход называется также «разрезать и выбрать» («cut-and-choose»), впервые использованный в криптографии Михаэлем Рабином[28][29].

Примеры

Пещера нулевого разглашения

Впервые данный пример был написан в хорошо известной работе по доказательству с нулевым разглашением «Как объяснить протокол доказательства с нулевым разглашением вашим детям» Жан-Жаком Кискатером[30].



Пещера нулевого разглашения

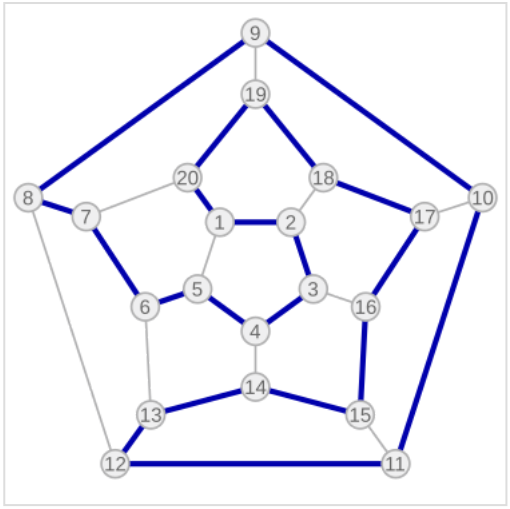
В данном случае Пегги выступает в качестве Доказывающего утверждение, и Виктор — в качестве Проверяющего (в англоязычной литературе обычно используются наименование сторон *Пегги* и *Виктор* (от «Prover» и «Verifier» соответственно). Пегги знает магическое слово («ключ»), ввод которого позволяет открыть ей дверь между C и D. Виктор хочет узнать, действительно ли Пегги знает пароль, при этом Пегги не хочет выдавать сам пароль. Пещера имеет круглую форму, как представлено на рисунке. Для того чтобы решить проблему, они поступают следующим способом. Пока Виктор находится в точке A, Пегги идёт к двери, и после того, как она исчезает из виду, Виктор идёт к разветвлению, то есть в точку B, и кричит оттуда: «Пегги нужно выйти *справа*» или «Пегги нужно выйти *слева*». Получаем каждый раз вероятность того, что Пегги не знает пароль, равна 50 %. Если же повторить процесс k раз, то вероятность будет $\frac{1}{2^k}$. При 20 же повторениях эта вероятность будет порядка 10^{-6}, что является достаточным для справедливости предположения о том, что Пегги знает ключ[30].

Если Виктор запишет все происходящее на камеру, то полученная видеозапись не будет являться доказательством для какой-либо другой стороны. Ведь они могли заранее сговориться, откуда будет выходить Пегги. Соответственно, она сможет найти выход, не зная при этом самого ключа. Существует ещё один способ: Виктор просто вырезает все неудачные попытки Пегги. Эти описанные выше действия доказывают, что пример с пещерой удовлетворяет свойствам: полноты, корректности и нулевому разглашению[31].

Гамильтонов цикл для больших графов

Этот пример был придуман Мануэлем Блюмом и описан в его работе в 1986 году[32]. Назовём проверяющую сторону Виктор, а доказывающую сторону Пегги. Допустим, Пегги известен гамильтонов цикл в большом графе *G*. Виктору известен граф *G*, но он не знает гамильтонова цикла в нём. Пегги хочет доказать Виктору, что она знает гамильтонов цикл, не выдавая при этом ни самого

цикла, ни какой-либо информации о нём (возможно Виктор хочет купить информацию об этом гамильтоновом цикле у Пегги, но перед этим желает удостовериться, что Пегги действительно знает его).



Граф додекаэдра с выделенным циклом Гамильтона.

Для этого Виктор и Пегги совместно выполняют несколько раундов протокола:

- Вначале Пегги создаёт граф H, изоморфный G. Преобразование гамильтонова цикла между изоморфными графами — тривиальная задача, поэтому если Пегги известен гамильтонов цикл в G, то она также знает гамильтонов цикл в порождаемом графе H.
- Пегги передаёт граф H Виктору.
- Виктор выбирает случайный бит $b \in \{0, 1\}$.
  - Если $b = 0$, то Виктор просит Пегги доказать изоморфизм G и H, то есть предоставить взаимнооднозначное соответствие вершин этих двух графов. Виктор может проверить, действительно ли G и H изоморфны.
  - Если $b = 1$, то Виктор просит Пегги указать гамильтонов цикл в H. Для задачи изоморфизма графов на данный момент не доказана ни её принадлежность классу $\boldsymbol{P}$, ни её $\boldsymbol{NP}$-полнота, поэтому будем здесь считать, что невозможно из гамильтонова цикла в H вычислить гамильтонов цикл в изоморфном G[32].

В каждом раунде Виктор выбирает новый случайный бит, который неизвестен Пегги, поэтому, чтобы Пегги могла ответить на оба вопроса, нужно чтобы H был в самом деле изоморфен G, и Пегги должна знать гамильтонов цикл в H (а значит также и в G). Поэтому после достаточного числа раундов, Виктор может быть уверен в том, что у Пегги действительно есть знание о гамильтоновом цикле в G. С другой стороны, Пегги не раскрывает никакой информации о гамильтоновом цикле в G. Более того, Виктору сложно будет доказать кому-либо ещё, что он сам или Пегги знают гамильтонов цикл в G[32].

Предположим, что Пегги неизвестен гамильтонов цикл в G, но она хочет обмануть Виктора. Тогда Пегги необходим неизоморфный G граф G', в котором она всё-таки знает гамильтонов цикл. В каждом раунде она может передавать Виктору либо H' — изоморфный G', либо H — изоморфный G. Если Виктор попросит доказать изоморфизм графов, и ему был передан H, то обман не вскроется. Аналогично, если он просит показать гамильтонов цикл, и ему был передан H'. В таком случае вероятность того, что Пегги всё-таки обманет Виктора после k раундов, равна $\frac{1}{2^k}$, что может быть меньше любой заранее заданной величины при достаточном числе раундов[32].

Предположим, что Виктор не узнал гамильтонов цикл, но хочет доказать Бобу, что Пегги его знает. Если Виктор, например, заснял на видео все раунды протокола, Боб едва ли ему поверит. Боб может предположить, что Виктор и Пегги в сговоре, и в каждом раунде Виктор заранее сообщал Пегги свой выбор случайного бита, чтобы Пегги могла передавать ему H для проверок изоморфизма и H' для проверок гамильтонова цикла. Таким образом без участия Пегги доказать, что она знает гамильтонов цикл, можно лишь доказав, что во всех раундах протокола выбирались действительно случайные биты[33].

Применение на практике

Теорема, гласящая, что для любой NP-полной задачи существует доказательство с нулевым разглашением, при этом, если использовать односторонние функции, можно создать корректные криптографические протоколы, была доказана Одедом Голдрейхом, Сильвио Микали и Ави

Вигдерсоном[19][34]. То есть, можно доказать любому скептику, что обладаешь доказательством некоей математической теоремы, не раскрывая самого доказательства. Это тоже показывает, как может быть использован данный протокол в практических целях[13].

Следующим методом, где может быть использовано доказательство с нулевым разглашением, является определением идентичности, при этом закрытый ключ у Пегги является так называемым «показателем идентичности», и, используя рассматриваемый протокол, можно доказать свою идентичность. То есть, можно доказать свою личность без использования различных физических устройств и данных (символов), таких как паспорта, различных снимков человека (сетчатки глаза, пальцев рук, лица и т. д.), а принципиально другим образом[35]. Однако, он имеет ряд недостатков, которые могут быть применены для обхода защиты. Описанный выше метод был впервые предложен Амосом Фиатом, Ади Шамиром и Уриэлем Фейге в 1987 году[36].

Также доказательства с нулевым разглашением могут быть использованы в протоколах конфиденциального вычисления, которые позволяют нескольким участникам убедиться в том, что другая сторона следует протоколу честно[19].

Доказательства с нулевым разглашением применяются в блокчейнах криптовалют Zcash, Byzantium (форк Ethereum), Zerocoin и других. Созданы реализации протоколов доказательства с нулевым разглашением, в частности, Software Development Kit QED-IT. Голландский банк ING создал свой вариант протокола, ZKRP (*Zero-Knowledge Range Proof*), и применил его для доказательства наличия у клиента достаточного размера заработной платы без раскрытия её истинного размера[7][8].

Наибольшее распространение получили протоколы zk-SNARKs, именно протоколы такого класса используются в ZCash, Zcoin и в протоколе Metropolis блокчейна Ethereum[37][8].

Аббревиатура zk-SNARK расшифровывается как (англ.) zero-knowledge succinct non-interactive argument of knowledge — краткий неинтерактивный аргумент знания с нулевым разглашением[37][8]. Алгоритм zk-SNARK состоит из генератора ключей, доказывающего и верификатора, обязательно поддерживает нулевое знание, имеет краткость (вычисляется за короткое время), является неинтерактивным (верификатор получает только одно сообщение от доказывающего)[8].

Злоупотребления

Предложено несколько способов злоупотребления доказательством с нулевым разглашением, которые используют те или иные слабые стороны протокола:

Проблема гроссмейстера

В данном примере некоторая сторона может доказать владение секретом, не обладая им на самом деле или, другими словами, может имитировать то лицо, которому на самом деле принадлежит секрет[38]. В настоящее время предложен способ решения проблемы Томасом Бетом и Иво Десмедтом[39].

Обман с несколькими личностями

Если сторона сможет создать несколько секретов, то соответственно она также сможет создать «несколько личностей». Пусть одна из них никогда не будет использоваться. Такая возможность обеспечивает разовую анонимность, что позволяет, например, уйти от ответственности: сторона идентифицирует себя никогда не используемой личностью и совершает преступление. После этого

данная «личность» никогда больше не используется. Выследить или сопоставить с кем-либо правонарушителя практически невозможно. Такое злоупотребление предотвращается, если изначально исключить возможность создания второго секрета[40].

Обман, выполненный мафией

Ещё один пример, когда одна сторона выдает себя за другую. Пусть имеется 4 участника: *A*, *B*, *C*, *D*. Причём *B* и *C* сотрудничают между собой («принадлежат одной мафии»). *A* доказывает свою личность *B*, а *C* хочет выдать себя за *A* перед *D*. *B* владеет рестораном, принадлежащим мафии, *C* — также представитель мафии, *D* — ювелир. *A* и *D* не знают о предстоящем мошенничестве. В момент, когда *A* готов заплатить за обед и идентифицировать себя перед *B*, *B* извещает *C* о начале мошенничества. Это возможно благодаря наличию радиоканала между ними. В это время *C* выбирает бриллиант, который хочет купить, и *D* начинает идентифицировать личность *C*, который выдает себя за *A*. *C* передаёт протокольный вопрос к *B*, а тот в свою очередь, задаёт его *A*. Ответ передаётся в обратном порядке. Таким образом *A* заплатит не только за обед, но и за дорогой бриллиант. Как видно из вышеописанного, существуют определённые требования для подобного мошенничества. Когда *A* начинает доказывать свою личность перед *B*, а *C* — перед *D*, действия *B* и *C* должны быть синхронизированы. Данное злоупотребление тоже разрешимо. Например, если в магазине ювелира будет клетка Фарадея, то «мафиози» не смогут обмениваться сообщениями[41].

Возможные атаки

Атака на основе подобранного шифротекста

Данная атака осуществима при использовании неинтерактивного метода взаимодействия в протоколе нулевого разглашения.

При использовании такого протокола возникает несколько проблем. Во-первых, нужно решить, как нужно осуществлять взаимодействие, и при этом должны быть сохранены фундаментальные особенности самого протокола: полнота, корректность и «нулевое разглашение». Помимо того, что можно достаточно просто доказать нулевое знание другой стороне, если можно прослушивать канал, то есть столкнуться с проблемой гроссмейстера.

Так вот сама атака заключается в следующем: злоумышленник, используя сложность доказательства обладанием знания, включает «атакующий» шифротекст, подсовывая его в кучу других шифротекстов, которые должны быть расшифрованы. Данная атака называется «playback» атака[42].

Возможное решение основано на работе Мони Наора и Моти Юнга, которая заключается в следующем: Доказывающий и Проверяющий шифруют сообщения публичным ключом, это приводит к тому, что описанная выше атака перестает работать[43].

Атака на мультипротокольную систему нулевого знания

Тида и Ямамото предложили такую реализацию протокола нулевого знания, которая значительно повышает скорость доказательств обладанием нулевым знанием при одновременном доказательстве сразу нескольких утверждений и, как следствие, производительность всей системы в целом[44]. Ключевой особенностью является ограничение на количество итераций для доказательства. Как было показано в работе К. Пэна[45], данный алгоритм оказался полностью неустойчивым к следующей атаке. Используя несколько правильно подобранных итераций, злоумышленник может пройти верификацию и нарушить главные положения о протоколе. Причём было показано, что данная атака всегда осуществима на такую систему.

Атака с помощью квантового компьютера

В 2005 году Джоном Ватрусом было показано , что не все системы с нулевым знанием являются устойчивыми к атакам с помощью квантового компьютера. Однако было доказано, что можно всегда построить такую систему, которая будет устойчива против квантовых атак, в предположении, что существуют квантовые системы с «сокрытием обязательств»[46].

См. также

- Ослепление (криптография)
- Криптосистема с открытым ключом
- Криптографическая хеш-функция
- Атака на основе подобранного шифротекста
- Схема Шнорра
- Протокол Фиата — Шамира
- Протокол Фейга — Фиата — Шамира
- Протокол Гиллу — Кискатра

Примечания

1. Goldreich, 2013.
2. Шнайер, 2002, pp. 87—92.
3. Goldwasser, Micali, Rackoff, 1989, pp. 186—189.
4. Santis, Micali, Persiano, 1988.
5. Blum, Feldman, Micali, 1988.
6. Шнайер, 2002, pp. 90—91.
7. ForkLog, 2019.
8. Губанова, 2018.
9. Blum, 1988, p. 1444.
10. Menezes et al, 1996, pp. 406—408.
11. Шнайер, 2002, pp. 86—89.
12. Goldwasser, Micali, Rackoff, 1989, pp. 188—189.
13. Шнайер, 2002, pp. 91—92.
14. Mao, 2005, pp. 683—696.
15. Mao, 2005, pp. 684—688.
16. Sahai, Vadhan, 2003.
17. Mao, 2005, p. 696.
18. Mao, 2005, pp. 692—696.
19. Goldreich, Micali, Wigderson, 1986.
20. Goldwasser, Micali, Rackoff, 1989.
21. Goldwasser, Micali, Rackoff, 1989, pp. 198—205.
22. Goldwasser, Micali and Rackoff Receive Gödel Prize in 1993 (https://web.archive.org/web/20151208062326/http://www.sigact.org/Prizes/Godel/1993.html). ACM Sigact (1993). Архивировано из оригинала (http://www.sigact.org/Prizes/Godel/1993.html) 8 декабря 2015 года.
23. Goldwasser, Micali Receive ACM Turing Award for Advances in Cryptography (https://web.archive.org/web/20130316052703/http://www.acm.org/press-room/news-releases/2013/turing-award-12). ACM. Дата обращения: 13 марта 2013. Архивировано из оригинала (http://www.acm.org/press-room/news-releases/2013/turing-award-12) 16 марта 2013 года.
24. Goldwasser, Micali, 1982.
25. Mao, 2005, pp. 524—528.

26. Абелевская премия — 2021 • Андрей Райгородский • Новости науки на «Элементах» • Математика, Наука и общество (https://elementy.ru/novosti_nauki/433790/Abelevskaya_premiya_2021). Дата обращения: 17 мая 2021. Архивировано (https://web.archive.org/web/20210603111510/https://elementy.ru/novosti_nauki/433790/Abelevskaya_premiya_2021) 3 июня 2021 года.
27. Mao, 2005, pp. 678—682.
28. *M.O.Rabin.* Digital signatures (https://smartech.gatech.edu/bitstream/handle/1853/40598/g-36-619_142482.pdf?sequence=1) . — Foundations of Secure Computation. — New York: Academic Press, 1978. — С. 155—168. — ISBN 0122103505. — [Архивировано (https://web.archive.org/web/20151121065359/https://smartech.gatech.edu/bitstream/handle/1853/40598/g-36-619_142482.pdf?sequence=1) 21 ноября 2015 года.]
29. Шнайер, 2002, pp. 87—89.
30. Quisquater et al, 1990.
31. Шнайер, 2002, pp. 87—88.
32. Blum, 1988.
33. Шнайер, 2002, pp. 89—90.
34. Goldreich, Micali, Wigderson, 1987.
35. Шнайер, 2002, p. 92.
36. Fiat, Shamir, 1987.
37. Chain Media, 2017.
38. Шнайер, 2002, pp. 92—93.
39. Beth, Desmedt, 1991.
40. Шнайер, 2002, pp. 93—94.
41. Шнайер, 2002, p. 93.
42. Rackoff, Simon, 1992.
43. Naor, Yung, 1990.
44. Chida, Yamamoto, 2008.
45. Peng, 2012.
46. Watrous, 2006.

Литература

книги и монографии

- *Мао В.* Современная криптография: Теория и практика / пер. Д. А. Клюшина — М.: Вильямс, 2005. — 768 с. — ISBN 978-5-8459-0847-6
- *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
- *Menezes A. J., van Oorschot P., Vanstone S. A.* Chapter 10 (http://cacr.uwaterloo.ca/hac/about/chap10.pdf) // Handbook of Applied Cryptography (https://cacr.uwaterloo.ca/hac/) (англ.) — Boca Raton: CRC Press, 1996. — P. 405—417. — 816 p. — (Discrete Mathematics and Its Applications) — ISBN 978-0-8493-8523-0
- *Саломаа А.* Криптография с открытым ключом — М.: Мир, 1995. — 318 с. — ISBN 978-5-03-001991-8
- *Goldreich O.* A Short Tutorial of Zero-Knowledge (http://www.wisdom.weizmann.ac.il/~oded/zk-tut02.html) (англ.) // *Secure Multi-Party Computation* — Amsterdam, Berlin, Tokyo, Washington, D.C.: IOS Press, 2013. — P. 28—60. — 285 p. — ISBN 978-1-61499-168-7

статьи

- *Goldwasser S., Micali S.* Probabilistic encryption & how to play mental poker keeping secret all partial information (https://www.cs.purdue.edu/homes/ninghui/readings/Qual2/Goldwasser-Micali82.pdf) (англ.) // *STOC'82*: *Proceedings of the fourteenth annual ACM symposium on Theory of computing* — New York

City: ACM, 1982. — P. 365—377. — ISBN 978-0-89791-070-5 — doi:10.1145/800070.802212 (https://dx.doi.org/10.1145/800070.802212)

- *Blum M.* How to Prove a Theorem So No One Else Can Claim It (http://www.mathunion.org/ICM/ICM1986.2/Main/icm1986.2.1444.1451.ocr.pdf) (англ.) // *ICM'86*: *International Congress of Mathematicians. Berkeley, California, USA, August 3-11, 1986, Proceedings* / A. Gleason — Providence: AMS, 1988. — P. 1444—1451. — 1850 p. — ISBN 978-0-8218-0110-9
- *Goldreich O., Micali S., Wigderson A.* Proofs that Yield Nothing but Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems (англ.) // *FOCS'86*: *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986. Proceedings* — IEEE Computer Society, 1986. — P. 174—187. — ISBN 978-0-8186-0740-0
- *Goldreich O., Micali S., Wigderson A.* How to Prove All NP Statements in Zero-Knowledge and a Methodology of Cryptographic Protocol Design (http://link.springer.com/content/pdf/10.1007%2F3-540-47721-7_11.pdf) (англ.): Extended Abstract // *Advances in Cryptology — CRYPTO '86*: *6th Annual International Cryptology Conference, Santa Barbara, California, USA, 1986, Proceedings* / A. M. Odlyzko — Berlin, Heidelberg, New York City, London: Springer Berlin Heidelberg, 1987. — P. 171—185. — 490 p. — (Lecture Notes in Computer Science; Vol. 263) — ISBN 978-3-540-18047-0 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/3-540-47721-7_11 (https://dx.doi.org/10.1007/3-540-47721-7_11)
- *Fiat A., Shamir A.* How to Prove Yourself: Practical Solutions to Identification and Signature Problems (https://www.cs.rit.edu/~jjk8346/FiatShamir.pdf) (англ.) // *Advances in Cryptology — CRYPTO '86*: *6th Annual International Cryptology Conference, Santa Barbara, California, USA, 1986, Proceedings* / A. M. Odlyzko — Berlin, Heidelberg, New York City, London: Springer Berlin Heidelberg, 1987. — P. 186—194. — 490 p. — (Lecture Notes in Computer Science; Vol. 263) — ISBN 978-3-540-18047-0 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/3-540-47721-7_12 (https://dx.doi.org/10.1007/3-540-47721-7_12)
- *Desmedt Y. G., Goutier C., Bengio S.* Special Uses and Abuses of the Fiat-Shamir Passport Protocol (extended abstract) (http://bengio.abracadoudou.com/cv/publications/pdf/desmedt_1988_crypto.pdf) (англ.) // *Advances in Cryptology — CRYPTO '87*: *A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proceedings* / C. Pomerance — Berlin: Springer Berlin Heidelberg, 1987. — P. 21—39. — (Lecture Notes in Computer Science; Vol. 293) — ISBN 978-3-540-18796-7 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/3-540-48184-2_3 (https://dx.doi.org/10.1007/3-540-48184-2_3)
- *Santis A. D., Micali S., Persiano G.* Non-Interactive Zero-Knowledge Proof Systems (http://link.springer.com/content/pdf/10.1007%2F3-540-48184-2_5.pdf) (англ.) // *Advances in Cryptology — CRYPTO '87*: *A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proceedings* / C. Pomerance — Berlin: Springer Berlin Heidelberg, 1988. — P. 52—72. — (Lecture Notes in Computer Science; Vol. 293) — ISBN 978-3-540-18796-7 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/3-540-48184-2_5 (https://dx.doi.org/10.1007/3-540-48184-2_5)
- *Blum M., Feldman P., Micali S.* Non-interactive zero-knowledge and its applications (англ.) // *STOC'88*: *Proceedings of the twentieth annual ACM symposium on Theory of computing* — New York City: ACM, 1988. — P. 103—112. — ISBN 978-0-89791-264-8 — doi:10.1145/62212.62222 (https://dx.doi.org/10.1145/62212.62222)
- *Goldwasser S., Micali S., Rackoff C.* The knowledge complexity of interactive proof systems (http://crypto.cs.mcgill.ca/~crepeau/COMP647/2007/TOPIC02/GMR89.pdf) (англ.) // *SIAM Journal on Computing* / M. Sudan — SIAM, 1989. — Vol. 18, Iss. 1. — P. 186—208. — ISSN 0097-5397 (https://www.worldcat.org/issn/0097-5397); 1095-7111 (https://www.worldcat.org/issn/1095-7111) — doi:10.1137/0218012 (https://dx.doi.org/10.1137/0218012)
- *Quisquater J., Quisquater M., Quisquater M., Quisquater M., Guillou L. C., Guillou M. A., Guillou G., Guillou A., Guillou G., Guillou S.* How to Explain Zero-Knowledge Protocols to Your Children (http://link.springer.com/content/pdf/10.1007%2F0-387-34805-0_60.pdf) (англ.) // *Advances in Cryptology — CRYPTO '89*: *9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings* / G. Brassard — Berlin, Heidelberg, New York City, London: Springer New York, 1990. — P. 628—631. — (Lecture Notes in Computer Science; Vol. 435) — ISBN 978-0-387-97317-3 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/0-387-34805-0_60 (https://dx.doi.org/10.1007/0-387-34805-0_60)

- *Naor M., Yung M.* Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks (http://www.wisdom.weizmann.ac.il/~naor/PAPERS/cca.pdf) (англ.) // *STOC'90*: *Proceedings of the twenty-second annual ACM symposium on Theory of computing* — New York City: ACM, 1990. — P. 427—437. — ISBN 978-0-89791-361-4 — doi:10.1145/100216.100273 (https://dx.doi.org/10.1145/100216.100273)
- *Beth T., Desmedt Y. G.* Identification Tokens — or: Solving The Chess Grandmaster Problem (http://link.springer.com/content/pdf/10.1007%2F3-540-38424-3_12.pdf) (англ.) // *Advances in Cryptology — CRYPTO '90*: *10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings* / A. J. Menezes, S. A. Vanstone — Berlin, Heidelberg, New York City, London: Springer Berlin Heidelberg, 1991. — P. 169—176. — (Lecture Notes in Computer Science; Vol. 537) — ISBN 978-3-540-54508-8 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/3-540-38424-3_12 (https://dx.doi.org/10.1007/3-540-38424-3_12)
- *Rackoff C., Simon D. R.* Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack (http://link.springer.com/content/pdf/10.1007%2F3-540-46766-1_35.pdf) (англ.) // *Advances in Cryptology — CRYPTO'91*: *11th Annual International Cryptology Conference, Santa Barbara, California, USA, 1991, Proceedings* / J. Feigenbaum — Berlin, Heidelberg, New York City, London: Springer Science+Business Media, 1992. — P. 433—444. — 484 p. — (Lecture Notes in Computer Science; Vol. 576) — ISBN 978-3-540-55188-1 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/3-540-46766-1_35 (https://dx.doi.org/10.1007/3-540-46766-1_35)
- *Bleichenbacher D.* Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1 (http://link.springer.com/content/pdf/10.1007%2FBFb0055716.pdf) (англ.) // *Advances in Cryptology — CRYPTO '98*: *18th Annual International Cryptology Conference Santa Barbara, California, USA August 23–27, 1998 Proceedings* / H. Krawczyk — Berlin, Heidelberg, New York City, London: Springer Berlin Heidelberg, 1998. — P. 1—12. — 524 p. — (Lecture Notes in Computer Science; Vol. 1462) — ISBN 978-3-540-64892-5 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743); 1611-3349 (https://www.worldcat.org/issn/1611-3349) — doi:10.1007/BFB0055716 (https://dx.doi.org/10.1007/BFB0055716)
- *Sahai A., Vadhan S.* A complete problem for statistical zero knowledge (http://web.cs.ucla.edu/~sahai/work/web/2003%20Publications/J.ACM2003.pdf) (англ.) // *Journal of the ACM* / D. J. Rosenkrantz — New York City: Association for Computing Machinery, 2003. — Vol. 50, Iss. 2. — P. 196—249. — ISSN 0004-5411 (https://www.worldcat.org/issn/0004-5411); 1557-735X (https://www.worldcat.org/issn/1557-735X) — doi:10.1145/636865.636868 (https://dx.doi.org/10.1145/636865.636868)
- *Watrous J.* Zero-Knowledge against Quantum Attacks (https://cs.uwaterloo.ca/~watrous/Papers/ZeroKnowledgeAgainstQuantum.pdf) (англ.) // *STOC'06*: *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing* — ACM, 2005. — Vol. 39, Iss. 1. — P. 25–58. — ISBN 978-1-59593-134-4 — doi:10.1137/060670997 (https://dx.doi.org/10.1137/060670997) — arXiv:quant-ph/0511020 (https://arxiv.org/abs/quant-ph/0511020)
- *Chida K., Yamamoto G.* Batch Processing for Proofs of Partial Knowledge and Its Applications (англ.) // *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences* — 2008. — Vol. E91-A, Iss. 1. — P. 150—159. — ISSN 0916-8508 (https://www.worldcat.org/issn/0916-8508); 1745-1337 (https://www.worldcat.org/issn/1745-1337); 0913-5707 (https://www.worldcat.org/issn/0913-5707); 1881-0195 (https://www.worldcat.org/issn/1881-0195) — doi:10.1093/IETFEC/E91-A.1.150 (https://dx.doi.org/10.1093/IETFEC/E91-A.1.150)
- *Peng K.* Attack against a batch zero-knowledge proof system (англ.) // *IET Information Security* — IET, 2012. — Vol. 6, Iss. 1. — P. 1—5. — ISSN 1751-8709 (https://www.worldcat.org/issn/1751-8709); 1751-8717 (https://www.worldcat.org/issn/1751-8717) — doi:10.1049/IET-IFS.2011.0290 (https://dx.doi.org/10.1049/IET-IFS.2011.0290)

Ссылки

- *Губанова, Л.* Что такое ZKP? Полное руководство по доказательству с нулевым разглашением (https://101blockchains.com/ru/доказательство-с-нулевым-разглашени/) : [арх. (https://web.archive.org/web/20210121165449/https://101blockchains.com/ru/%D0%B4%D0%BE%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE-%D1%81-%D0%BD%D1%83%D0%BB%D0%B5%D0%B2%D1%8B%D0%BC-%D1%80%D0%B0%D0%B7%D0%B3%D0%BB%D0%B0%D1%88%D0%B5%D0%BD%D0%B8/) 21 января 2021] // 101 Blockchains. — 2018. — 21 декабря.

- Что такое Zero Knowledge Proof? (http://chainmedia.ru/newcomers/zero-knowledge-proof/) // Chain Media. — 2017. — 21 ноября.
- Что такое доказательство с нулевым разглашением (zero-knowledge proof)? (https://forklog.com/chto-takoe-dokazatelstvo-s-nulevym-razglasheniem-zero-knowledge-proof/) : [арх. (https://web.archive.org/web/20200721225315/https://forklog.com/chto-takoe-dokazatelstvo-s-nulevym-razglasheniem-zero-knowledge-proof/) 21 июля 2020] // ForkLog. — 2019. — 21 мая.