ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

А.Н. Юрцев, *студент*
Волгоградский государственный университет
(Россия, г. Волгоград)

DOI:10.24412/2500-1000-2023-4-4-138-141

Аннотация. *Доказательство с нулевым разглашением – это криптографический протокол, который позволяет одной стороне (доказывающему) подтвердить истинность утверждения другой стороне (верификатору), при этом не раскрывая никакой дополнительной информации о ней (ни содержания, ни источника, из которого доказывающий узнал о правдивости).*

В данной статье показано, что на практике любое (математическое) высказывание, логическое условие – или даже код программы – можно перевести с помощью специальной техники в «circuits» – выражения, записанные в специальном синтаксисе, пригодные для доказывания с нулевым разглашением, приведены простейший и математизированный варианты иллюстрации интерактивного протокола, описаны некоторые идеи доказательств, указаны сферы возможного применения ZKP. Алгоритм позволяет аутентифицировать пользователей, опираясь на существующие в сети цепочки доверия.

Основной вывод заключается в том, что применение ZKP позволит повысить приватность пользователей в публичных сетях, пропускную способности блокчейнов, укрепить информационную безопасность за счет замены неэффективных способов аутентификации и верификации.

Ключевые слова: *доказательства с нулевым разглашением, логическое условие, математизированный вариант, бит, мультипликативность.*

В криптографии под доказательством с нулевым разглашением [1-2] (zero-knowledge proof) понимается протокол, позволяющей доказывающему (Prover) убедить другую сторону (Verifier) в истинности некоторого утверждения P, не раскрывая при этом ровно никакой дополнительной информации, кроме того, факт, что P – истинно. То есть после выполнения этого протокола верификатор будет иметь убеждённость в верности P, но не будет обладать, к примеру, возможностью убедить кого-то третьего в истинности P [3].

Например, рассмотрим утверждение «я знаю такое x, что x^3 – x + 8 = 0» Каким образом вообще можно убедить кого-то в истинности этого утверждения, кроме как предоставив этот корень на проверку? Это удивительно, но доказательства с нулевым разглашением позволяют это сделать. Человек, которого вы убеждаете, не получит вообще никакой информации об этом корне. Но этот пример не очень жизненный. А вот более реальный: пусть E – эллиптическая кривая, G – генератор, F = n*G, я хочу доказать, что знаю n, не раскрывая никакой информации об этом n. То есть, что я знаю решение задачи дискретного логарифмирования на этой кривой. С помощью ZKP это возможно. А что, если это n – мой биткоин-кошелёк, пароль от госуслуг, или ещё что-то в таком духе?

Доказать с нулевым разглашением можно «что угодно». Существуют математически строгие формулировки этого утверждения, опирающиеся на понятия np-полноты. На практике любое (математическое) высказывание, какое-то равенство, неравенство, логическое условие – или даже код программы – можно перевести с помощью специальной техники в «circuits» – выражения, записанные в специальном синтаксисе, и они будут пригодны для доказывания с нулевым разглашением.

Самым избитым иллюстрационным примером является «Пещера Али-бабы», однако, приводить мы его не станем, а рассмотрим чуть менее известный.

Пусть Алиса – дальтоник, она не различает цветов, а у Боба есть два шарика,

красный и зелёный. Он хочет убедить Алису в том, что они разных цветов. Для этого Алиса показывает Бобу один из шариков, затем уходит за гаражи и там как-то перемешивает шарики, но сама держит в уме, какой показывала Бобу. Затем выходит и предлагает Бобу определить, какой шарик она ему показывала. Боб, который действительно различает цвета, будет постоянно угадывать. Если бы шарики были одинаковые, то вероятность угадать была бы ½.

Таким образом, проведя подобный эксперимент n раз, и получив n угадываний, Алиса бы с вероятностью 1/(2^n) могла предположить, что шарики действительно разные.

Это – простейшая иллюстрация интерактивного протокола (повторяющегося несколько раз, вероятностного). Бывают и не-интерактивные, заключающиеся в однократном обмене сообщениями. Заметим, что сама Алиса не получила никакой информации (хотя здесь это и не так наглядно), но факт в том, что Алиса не может никого убедить в том, что шары действительно разные.

Рассмотрим более математизированный вариант этого протокола [4]. Доказывающему и проверяющему известна пара графов ⟨G0,G1⟩. Допустим, эти графы изоморфны и Доказывающему известен изоморфизм, то есть некоторая перестановка π, такая что G0=πG1 Алиса(доказывающий) хочет доказать Бобу(проверяющему), что графы изоморфны, не выдавая при этом ни самой перестановки, ни какой-либо информации о ней.

Для этого Алиса и Боб делают следующее:

1) Алиса генерирует случайную перестановку ϕ. Применив ее к G0, она получает граф H=ϕG0;

2) Алиса отправляет этот граф Бобу;

3) Боб выбирает случайный бит i←{0,1};

4) Боб просит Алису доказать изоморфизм Gi и H, то есть предоставить соответствие вершин этих двух графов(перестановку);

5) Если i=0, то Алиса отсылает Бобу ϕ, иначе ϕ·π

В каждом раунде Боб выбирает новый случайный бит, который неизвестен Алиса. Поэтому чтобы ответить на оба вопроса, Алисе нужно чтобы H был действительно изоморфен Gi. Это означает, что после достаточного числа раундов, Боб может быть уверен в том, что графы G0 и G1 изоморфны. С другой стороны, Алиса не раскрывает никакой информации

о перестановке π. Предположим, что у Алисы нет перестановки π. Тогда граф H, который она отсылает Бобу, будет не изоморфен хотя бы одному из пары графов ⟨G0,G1⟩. Поэтому вероятность того, что она сможет обмануть Боба в одном раунде не более 1/2. Вероятность того, что на за n раундов не более 2^ (-n). Предположим, что Боб не узнал перестановку, но хочет доказать Карлу что Алиса ее знает. Если Боб, например, заснял на видео все раунды протокола, Карл едва ли ему поверит. Кар может предположить, что Алиса и Боб в сговоре и в каждом раунде Боб заранее сообщал Алиса свой выбор случайного бита, чтобы Алиса могла передавать ему H для проверок изоморфизма. Таким образом без участия Алисы доказать изоморфизм графов, можно лишь доказав, что во всех раундах протокола выбирались действительно случайные биты.

Заметим, что во всех этих рассуждениях понимать слова «Боб не узнал ничего» следует в вычислительном смысле. То есть, конечно, Боб может просто перебрать все перестановки вершин и проверить, изоморфны ли эти графы. Но задача NP-полная, алгоритм работает очень долго для больших графов, и с практической точки зрения «знает решение» = «знает ответ на задачу, для которой не существует полиномиального алгоритма».

Некоторые основные идеи состоят в следующем:

а) Представление математических утверждений в виде некоторых утверждений вида «Я знаю многочлен, имеющий такие-то корни, и удовлетворяющий таким-то условиям». Эта техника называется «Представление в форме квадратичной арифметической программы». Дело в том, что если два многочлена одинаковой степени совпали в одной-единственной

наугад выбранной точке, то они равны с огромной вероятностью.

б) Гомоморфное шифрование. Рассмотрим одностороннюю функцию, например хэш-функцию. Она односторонняя, потому что восстановление прообраза невозможно / вычислительно сложно. А вот если бы нам удалось к односторонней функции добавить хороших свойств. Например, мультипликативность: E(xy) = E(x)E(y), можно даже привести пример такой функции – E(x) = 2^x, (mod p). Она односторонняя, потому что восстановление x по E – это решение задачи дискретного логарифмирования. Но вместе с тем, мы теперь получили возможность производить некоторые вычисления в «зашифрованном пространстве» - мы можем, отправив заранее кому-то E(x) и E(y), попросить его вычислить E(xy), и вернуть нам результат. Это позволяет производить вычисления без раскрытия информации о том, что именно вычисляется, и так же подтверждать некоторые «факты зашифрованного мира» без раскрытия прообраза этих фактов.

в) Некоторые виды zk-криптографии устойчивы к квантовому криптоанализу, что через некоторое время станет действительно важно;

г) Для части протоколов необходима «доверенная установка» – выработка (общих для всех пользователей сети) публичных параметров, исходные данные для которых должны быть сгенерированы случайным образом и затем уничтожены. Доверенная церемония Zcash была целым шоу. Цель её – убедить сообщество в том, что «токсичные отходы», позволяющие доказывать неверные утверждения и мошенничать таким образом, действительно уничтожены. В таких протоколах желающий подтвердить транзакцию с использованием публичных параметров делает это, и его доказательство с нулевым разглашением проверяемо любым участником сети. К слову, длина таких доказательств может исчисляться всего лишь сотнями байт.

Для другой части протоколов такая установка не требуется – они интерактивны. Доказательства с нулевым разглашением могут применяться в любых сферах, где требуется подтверждение владения данными без раскрытия их содержания.

Наиболее активно, конечно, ZKP применяются в финансовой сфере, особенно в криптовалютах. Транзакция может быть верифицирована участниками сети без раскрытия информации о том, от кого и кому она производится, и даже без раскрытия суммы.

Фактически все заметные криптовалюты, кроме (кажется) Биткоин, предоставляют инструменты для проведения конфиденциальных транзакций с помощью zero-knowledge, возможности писать смарт-контракты с zk. В Monero и раньше был механизм анонимности – кольцевые подписи, но теперь добавлен и более современный. Zcash вообще позиционирует себя как «самая крипто- криптовалюта в мире» – там есть возможность проводить как обычные транзакции, так и полностью скрытые. Некоторый казус в том, что на долю анонимных транзакций приходится ничтожная доля от всех транзакций в сети. Пока что люди этим не очень пользуются.

Этот протокол также можно использовать в сферах, где необходимо обеспечить безопасность данных, персональной информации – в банковской и медицинской отраслях, в государственном учёте.

Наконец, на основе ZKP можно проводить электронные выборы, результаты которых будут проверяемы любым желающим, но не будут нарушать анонимности.

Заключение. Применение ZKP позволит повысить приватность пользователей в публичных сетях, пропускную способности блокчейнов (существуют технологии, позволяющие объединить транзакции в группу и доказать «пакетом» – пропускная способность таких блокчейнов намного выше сети биткоин) и улучшение масштабируемости, укрепить информационную безопасность за счет замены неэффективных способов аутентификации и верификации. К недостаткам можно отнести некоторую требовательность к вычислительным мощностям, однако уже сегодня ZKP для смартфонов – это реальность, а сфера эта очень быстро прогрессирует.

Библиографический список

1. Горячев, А.А. Методические аспекты изложения протоколов с нулевыми знаниями: толкование термина «нулевое разглашение» в дисциплине «Криптографические протоколы» / А.А. Горячев, Р.В. Кишмар, Хо Нгок Зуй // Современное образование: содержание, технологии, качество. – 2011. – Т. 2. – С. 238-240.

2. Яковлев, А.В. Динамическая модель протокола идентификации с нулевым разглашением тайны / А.В. Яковлев, Т.С. Сычева // Актуальные проблемы деятельности подразделений УИС: Сборник материалов Всероссийской научно-практической конференции, Воронеж, 25 мая 2017 года. – Воронеж: Издательско-полиграфический центр «Научная книга», 2017. – С. 170-173.

3. Подводные камни сертификации блокчейн-решений / Андрей Елистратов, Григорий Маршалко, Владимир Светушкин // Открытые системы СУБД/2019 №1.

4. Салий, В. Н. Неприводимые расширения графов (доказательства с нулевым разглашением) / В. Н. Салий // Известия ТРТУ. – 2003. – № 4 (33). – С. 271-273.

ZERO-DISCLOSURE PROOF

A.N. Yurtsev, *Student*
Volgograd State University
(Russia, Volgograd)

Abstract. *A zero-disclosure proof is a cryptographic protocol that allows one party (the prover) to confirm the truth of the statement to the other party (the verifier), while not disclosing any additional information about it (neither the content nor the source from which the prover learned about the truthfulness).*

This article shows that in practice any (mathematical) statement, logical condition – or even program code – can be translated using a special technique into "circuits" – expressions written in a special syntax suitable for zero-disclosure proof, the simplest and mathematized versions of the interactive protocol illustration are given, some ideas of proofs are described, the areas of possible application of ZKP are indicated. The algorithm allows you to authenticate users based on the existing chains of trust in the network.

The main conclusion is that the use of ZKP will increase the privacy of users in public networks, the throughput of blockchains, strengthen information security by replacing inefficient authentication and verification methods.

Keywords: *zero-knowledge proofs, logical condition, mathematized variant, bit, multiplicativity.*