ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ПРОЦЕССЫ

INFORMATION SYSTEMS AND PROCESSES

Развитие территорий. 2026. № 1. С. 77—88.
Territory Development. 2026;(1):77—88.

Информационные системы и процессы

Научная статья
УДК 004.056.22.05 + 621.391.827
EDN ZCCFEM

ГИБРИДНЫЙ ПРОТОКОЛ ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ ДЛЯ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Сергей Борисович Кузнецов
Университет «Сириус», федеральная территория «Сириус», Сочи, Российская Федерация, kuznetsov.sb@talantiuspeh.ru

Аннотация. В работе представлен гибридный протокол доказательства с нулевым разглашением QZKP-Hybrid. Он создан для защиты информации от квантовых и классических атак. Протокол сочетает два подхода: устойчивую к квантовым атакам криптографию на решетках (LWE) и квантовые методы, использующие специальные квантовые состояния $|\phi_x\rangle$ и SWAP-тестирование. Протокол решает классическую задачу доказательства с нулевым разглашением (ZKP) в постквантовом контексте, находит применение в аутентификации, цифровых подписях и блокчейне. Протокол является неинтерактивным за счет применения преобразования Фиата — Шамира. Также используется запрет на клонирование квантовых состояний, что физически защищает секретную информацию от подделки. Безопасность QZKP-Hybrid доказана в модели UC-безопасности. Для этого применялась последовательность гибридных игр. Доказано, что никакой противник, даже с квантовым компьютером, не сможет взломать протокол. Реализация протокола возможна с помощью существующих технологий. Например, можно использовать оптоволоконные каналы для передачи квантовых состояний, что позволяет внедрять протокол в реальные системы. QZKP-Hybrid может применяться в постквантовых системах. Он подходит для задач, где нужно скрыть данные, но при этом подтвердить их достоверность. Протокол показал хороший баланс между безопасностью и производительностью. При размере параметра $n = 512$ он работает быстро и требует мало памяти. Это позволяет использовать его в мобильных устройствах и IoT-системах. В дальнейших исследованиях планируется изучить влияние декогеренции и шума на точность протокола, а также расширить модель на несколько участников.

Ключевые слова: доказательство с нулевым разглашением (ZKP), UC-безопасность, постквантовая криптография, квантовые протоколы, LWE, SWAP-тест, гибридная криптография

Благодарности: результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории „Сириус”» (Соглашение № 23-03 от 27.09.2024).

Для цитирования: Кузнецов С. Б. Гибридный протокол доказательства с нулевым разглашением для постквантовой криптографии // Развитие территорий. 2026. № 1. С. 77—88. EDN ZCCFEM.

Information systems and processes

Original article

A HYBRID ZERO-KNOWLEDGE PROOF PROTOCOL FOR POST-QUANTUM CRYPTOGRAPHY

Sergey B. Kuznetsov
University “Sirius”, Federal Territory “Sirius”, Sochi, Russian Federation, kuznetsov.sb@talantiuspeh.ru

Abstract. The paper presents a hybrid zero-knowledge proof protocol, QZKP-Hybrid, designed to protect information from quantum and classical attacks. The protocol combines two approaches: quantum-resistant lattice cryptography (LWE) and quantum methods using special quantum states $|\phi_x\rangle$ and SWAP testing. The protocol solves the classical zero-knowledge proof problem (ZKP) in a post-quantum context and finds application in authentication, digital signatures, and blockchain. The protocol is non-interactive due to the Fiat-Shamir transformation. A prohibition on cloning quantum states is also used, physically protecting secret information from forgery. The security of QZKP-Hybrid is proven in the UC security model using a sequence of hybrid games. It is proven that no adversary, even with a quantum computer, can break the protocol. The protocol can be implemented using existing technologies. For example, fiber-optic channels can be used to transmit quantum states, allowing the protocol to be implemented in real-world systems. QZKP-Hybrid can be used in post-quantum systems. It is suitable for tasks where data must be hidden while still being verified. The protocol has demonstrated a good balance between security and performance. With a parameter size of n = 512, it operates quickly and requires little memory. This allows it to be used in mobile devices and IoT systems. Future research plans include studying the impact of decoherence and noise on protocol accuracy and extending the model to multiple participants.

Keywords: zero-knowledge proof (ZKP), UC-security, post-quantum cryptography, quantum protocols, LWE, SWAP-test, hybrid cryptography

Acknowledgments: The results were obtained with financial support from the project “Technologies for Countering Previously Unknown Quantum Cyber Threats”, implemented under the state program of the federal territory Sirius “Scientific and Technological Development of the Federal Territory Sirius” (Agreement No. 23-03 dated September 27, 2024).

For citation: Kuznetsov S.B. A Hybrid Zero-Knowledge Proof Protocol for Post-Quantum Cryptography. Territory Development. 2026;(1):77—88. (In Russ.). https://elibrary.ru/zccfem.

Введение

Многие из существующих ZKP-протоколов построены на сложности решения математических задач факторизации больших чисел или дискретном логарифмировании. Но уже в сейчас эти задачи перестали быть надежной защитой из-за появления квантовых компьютеров. Квантовый алгоритм Шора позволяет решать их и ставит под угрозу всю систему безопасности. Поэтому в настоящее время активно развиваются постквантовые подходы LWE и Short Integer Solution (SIS).

Вопросы, возникающие при изучении гибридных алгоритмов, привлекают внимание многих исследователей. Так, в работе [1] описывается постквантовый алгоритм цифровой подписи на основе решеток, который используется как основа классической части гибридных ZKP. Приводится формальное доказательство EUF-qCMA стойкости в модели QROM.

Авторами работы [2] было введено понятие «resettable zero-knowledge». Доказывающий может быть неоднократно перезапущен противником без потери свойства нулевого знания. Это понятие необходимо при анализе устойчивости ZKP к повторным атакам.

В исследовании [3 ; 4] авторы изучают безопасность блочных шифров и хэширование в условиях квантовых атак, а также обосновывают выбор функций, используемых в гибридных протоколах.

В работе [5] определяются ограничения классических методов доказательства безопасности при переходе к квантовому случаю, а также исследуется сложность применения квантового rewinding в доказательствах ZKP.

В работе [6] представлены результаты разработки эффективных протоколов доказательства с нулевым разглашением для схем обязательств, основанных на задаче LWE над кольцами RLWE.

В исследованиях [7 ; 8] предлагается формальное определение и реализация oblivious transfer (OT) в квантовой среде с гарантией UC-безопасности. Результаты этих исследований применяются при анализе гибридных систем.

Авторы работы [9] демонстрируют возможность построения неинтерактивных доказательств с нулевым разглашением (NIZK) в условиях квантовых атак. Используются предположение о сложности LWE и случай-

ная оракульная модель. Исследование необходимо для развития постквантовых и гибридных ZKP.

Данная работа посвящена созданию гибридного протокола под названием QZKP-Hybrid. В протоколе объединены классическая криптография, основанная на задаче LWE и преобразовании Fiat-Shamir, и квантовые методы, использующие специальные квантовые состояния $|\phi_x\rangle$ и SWAP-тестирование. SWAP-тест был выбран для верификации в протоколе из-за сохранения свойства нулевого знания без раскрытия информации о секрете. Тест легко реализуется на современных квантовых устройствах. Он позволяет косвенно оценить fidelity, что важно для проверки корректности доказательства. Физическая защита от подделки обеспечивается за счет теоремы о запрете клонирования. SWAP-тест работает с одночастичными состояниями, что соответствует используемому формату квантового ключа. Все эти факты говорят в пользу выбора SWAP-теста.

Основной задачей исследования стало построение протокола, обладающего свойством UC-безопасности (Universally Composable Security).

Протокол QZKP-Hybrid решает задачу доказательства с нулевым разглашением (ZKP) в постквантовом контексте.

Формально задача заключается в следующем.

Пусть существует бинарный предикат R(x, y), который определяет отношение между секретным значением x (witness) и публичным утверждением y. Задача доказывающего P — убедить проверяющего V в том, что для данного публичного y существует такое секретное x, что R(x, y) = true, при этом не раскрывая никакой информации о самом x.

Определение предиката R(x, y)

В рамках данной модели предикат R(x, y) определяется как отношение, связывающее секретный ключ x (который далее обозначается как sk) с его публичной проекцией y (которая далее обозначается как pk), вычисленной посредством криптографической функции, устойчивой к квантовым атакам. Конкретно:

$$R(sk, pk) = \begin{cases} \text{true}, & \text{если } pk = \text{KeyGen}_{LWE}(sk, \lambda) \\ \text{false} & \text{в противном случае} \end{cases},$$

где $sk \in \{0, 1\}^{\lambda}$ — секретный ключ, сгенерированный как случайная битовая строка;

pk — открытый ключ, вычисленный из sk с использованием алгоритма, основанного на задаче LWE;

λ — параметр безопасности.

Таким образом, протокол позволяет доказать знание секретного ключа sk, соответствующего известному открытому ключу pk, без раскрытия sk. Эта фундаментальная задача лежит в основе цифровых подписей, аутентификации и многих других криптографических примитивов.

Протокол QZKP-Hybrid гарантирует выполнение трех ключевых свойств для данного предиката:

— полноты (Completeness): если P честен и знает x такое, что R(x, y) = true, то V примет доказательство с вероятностью, близкой к 1;

— корректности (Soundness): если R(x, y) = = false (т. е. P не знает валидного x), то никакой нечестный доказывающий не сможет убедить V принять доказательство, кроме как с пренебрежимо малой вероятностью;

— нулевого разглашения (Zero-Knowledge): проверяющий V не получает никакой дополнительной информации о x, кроме самого факта, что R(x, y) = true.

Статья имеет следующую структуру: в первой части описана формальная модель протокола. Рассмотрены участники, идеальный функционал и основные этапы взаимодействия. Во второй части показано, как строятся классические и квантовые ключи и создается квантовое состояние $|\phi_x\rangle$. В третьей части показано строгое доказательство UC-безопасности протокола с использованием последовательности гибридных игр, позволяющих формально оценить уровень защиты от возможных атак. В четвертой части представлена схема кодирования кубитов. В пятой части рассмотрены вопросы взаимодействия классической части протокола с квантовой. В заключении приведены основные результаты работы и указаны направления дальнейших исследований.

1. Протокол QZKP-Hybrid

Рассмотрим процесс взаимодействия участников протокола. Обозначим определенный секрет как x.

В протоколе участвуют доказывающий P (обладатель секрета x) и проверяющий V. Протокол позволяет P убедить V в знании x, удовлетворяющего предикату R(x, y), без его раскрытия. Идеальное поведение системы описывается функционалом F_{QZKP}.

В протоколе рассматривается идеальный функционал F_{QZKP}, который представляет собой эталонное поведение системы. Функционал описывает состояние, как должен выглядеть протокол доказательства с нулевым разглашением в идеальных условиях. Реали-

зация самого QZKP-Hybrid строится таким образом, чтобы максимально близко следовать этому идеальному поведению.

Для проверки соответствия реального протокола идеальному используется симулятор S.

Предполагается, что противник A представляет собой активного оппонента, обладающего квантовыми вычислительными ресурсами. В случае QZKP-Hybrid считается, что противник довольно мощный. При этом противник работает в рамках класса задач, которые можно решить за полиномиальное время на квантовом компьютере с ограниченной ошибкой.

Для защиты в протоколе используется модель случайного оракула ROM. В протоколе хэш-функции для любого входа дают случайный детерминированный результат. Это позволяет обосновать безопасность протокола при наличии квантовых атак.

В основе протокола лежат криптографические конструкции LWE, устойчивые к квантовым атакам [10]. Кроме того, используются квантовые состояния, такие как запутанные пары или специальные SWAP-состояния. Эти состояния дополнительно создают физическую защиту от подделки.

Протокол QZKP-Hybrid позволяет доказывающему P убедить проверяющего V, что он знает секретное значение x, удовлетворяющее предикату R(x, y), без раскрытия самого x. Протокол будет безопасен при любом противнике благодаря комбинированному использованию постквантовой криптографии и принципов квантовой механики [11].

Вначале происходит генерация ключей $\mathrm{KeyGen}(1^{\lambda}) \rightarrow (pk, sk)$, а также генерируется квантовое состояние $|\psi_{sk}\rangle$. Принимается параметр безопасности λ, который определяет размер ключей, сложность задач и уровень защиты от пары ключей (pk, sk). Используется постквантовый алгоритм Dilithium.

Секретный ключ sk позволяет формировать квантовое состояние $|\psi_{sk}\rangle$. Квантовое состояние будет использоваться в дальнейших этапах протокола для обеспечения квантовой верификации.

Доказывающий получает входные данные, у него есть x, y, pk и sk. Он выбирает случайное число r. С помощью r доказывающий строит коммитмент $t = g(r)$, подобный хэш, или одностороннюю функцию от случайного числа. Затем он вычисляет вызов $c = H(pk, t)$, хэшируя открытый ключ и коммитмент, чтобы получить запрос. После этого доказывающий вычисляет ответ $z = f(r, c, sk)$, который является некоторой функцией, зависящей от случайного числа, вызова и секретного ключа. Также он готовит квантовое состояние

$$|\phi_x\rangle = U_x|\psi_{sk}\rangle. \quad (1)$$

Созданные данные $(t, z, |\phi_x\rangle)$ отправляются проверяющему как доказательство знания x.

Проверка доказательства в протоколе QZKP-Hybrid также состоит из нескольких этапов. На вход подается сообщение или запрос M, доказательство $(t, z, |\phi_x\rangle)$, открытый ключ pk и публичная информация y, связанная с секретом x через правило R(x, y).

На выходе проверяющий выдает один из двух результатов accept, если доказательство корректно или reject, если обнаружены признаки подделки или ошибки.

На первом этапе проверки будет происходить восстановление вызова $c' = H(pk, t)$. Проверяющий вычисляет значение c' с помощью хэш-функции H, применяя ее к открытому ключу pk и коммитменту t. Это позволяет получить тот же вызов, который использовал доказывающий.

На втором этапе осуществляется проверка классической части доказательства. Проверяющий запускает функцию Verify (pk, t, z, c'). Эта операция проверяет, правильно ли вычислен ответ z на основе t и c'. Если результат равен false, проверка завершается отказом, и выход будет reject. Если результат равен true, продолжается квантовая проверка. Для верификации классической части доказательства используется алгоритм проверки подписи схемы Dilithium, полученной с применением преобразования Фиата — Шамира.

На третьем этапе осуществляется проверка квантовой части доказательства. Проверяющий проводит SWAP-тест между полученным квантовым состоянием $|\phi_x\rangle$, которое прислал доказывающий, и ожидаемым квантовым состоянием $U_x | \psi_{sk}\rangle$. Использование SWAP-теста позволяет косвенно проверить корректность доказательства, сравнивая его с ожидаемым состоянием. Мера между состояниями определяется из

$$F(|\phi_x\rangle, U_x | \psi_{sk}\rangle) = |\langle \phi_x | U_x | \psi_{sk}\rangle|^2, \quad (2)$$

и проверяется выполнение условия:

$$F \geq 1 - \varepsilon, \quad (3)$$

где ε — допустимая погрешность.

Если условие (3) не выполнено, то проверка завершается отказом, и выход будет

reject. Если условие выполнено, то доказательство принимается.

Доказательство считается успешным только в случае, если обе проверки прошли успешно. Классическая проверка Verify (pk, t, z, c') вернула true, и квантовая проверка показала достаточную степень схожести состояний.

Для оценки влияния параметра n, связанного с размерностью вектора в задаче LWE, на эффективность протокола приведем сравнительные характеристики при разных значениях n (таблица). Параметры, приведенные в данной работе, взяты из стандартных оценок сложности атак на задачу LWE и согласуются с рекомендациями NIST для постквантовых криптосистем. Однако они используются не чисто в классической схеме, а в гибридном протоколе доказательства с нулевым знанием, где проверка состоит из классической и квантовой.

Таблица сравнения по размеру вектора n задачи LWE
Comparison table by vector size n for the LWE problem

Параметр	Описание	n = 256	n = 512	n = 1024	QZKP-Gibrid (оценка)
Уровень безопасности, бит	С ростом n повышается сложность задачи LWE, что увеличивает стойкость к атакам	~100—128 бит	~192 бит	~256 бит	≥ 128 бит
Размер открытого ключа, бит	Прямо зависит от n, так как открытый ключ содержит матрицу A и вектор b. При $q = 2^{32}$, $n \cdot \log_2 q \cdot m$ (m — количество уравнений)	~1 КБ	~4 КБ	~16 КБ	~2—5 КБ
Размер секретного ключа, бит	Зависит от n: например, $n \cdot \log_2 q$	~256 байт	~512 байт	~1 КБ	~512 байт
Время генерации ключей	Растет полиномиально с увеличением n ($O(n^2)$ или $O(n^{2.5})$)	~1 мс	~4 мс	~15 мс	~3—5 мс
Время доказательства (Prove)	Зависит от n, если используется Fiat-Shamir и операции над решетками	~2 мс	~8 мс	~30 мс	~5—10 мс
Время проверки (Verify)	Линейно или квадратично зависит от n с учетом алгоритма верификации	~1 мс	~3 мс	~10 мс	~2—4 мс
Требования к памяти (RAM)	Выше при больших n из-за хранения больших матриц и векторов	~1 МБ	~4 МБ	~16 МБ	~5 МБ
Применимость в IoT/мобильных устройствах	При высоких n снижается из-за ограничений по памяти и мощности процессора	Да	Условно	Нет	Да (при n ≤ 512)

Анализ таблицы показывает, что QZKP-Hybrid демонстрирует хороший баланс между безопасностью, скоростью и применимостью, особенно при n ≈ 512. Он имеет низкие временные затраты и затраты памяти. Может быть адаптирован под IoT/мобильные устройства, если выбрать n = 256—512.

2. Создание ключей и доказательства

Рассмотрим создание квантового состояния $|\psi_{sk}\rangle$. Оно используется как физическое доказательство, связанное с секретным ключом sk, и не может быть скопировано из-за теоремы о запрете клонирования.

Создание состояния $|\psi_{sk}\rangle$ происходит на этапе KeyGen, где генерируется пара ключей (sk, pk) и соответствующее квантовое состояние, зависящее от sk. Это позволяет связать классический секретный ключ с квантовым объектом.

Секретный ключ sk представляет собой случайную битовую строку длины λ (например, λ = 256 бит):

$$sk = b_0 b_1 b_2 \ldots b_{\lambda-1},\ b_i \in \{0,1\}.$$

Он создается с помощью надежного генератора случайных чисел (CSPRNG), чтобы гарантировать высокую степень случайности и безопасности:

$$sk \leftarrow \{0,1\}^{\lambda}.$$

Этот ключ затем используется как основа для построения открытого ключа pk и квантового состояния $|\psi_{sk}\rangle$.

Открытый ключ pk вычисляется из sk с помощью функции, устойчивой к квантовым атакам. В данном случае используется задача LWE.

$$b = A \cdot s + e \bmod q,$$

$A \in Z_q^{n \cdot m}, s \in Z_q^n, e \in Z_q^m$ — малый шум,

где s — вектор, полученный из sk, например, через хэширование.

Тогда открытый ключ представляет пару

$$pk = (A, b).$$

Для создания квантового состояния нам необходимо преобразовать битовую строку sk в набор кубитов. Рассмотрим наиболее общий и применимый для гибридного ZKP.

Для каждого бита $b_i \in sk$ определяем соответствующий кубит:

$$|\psi_{sk}\rangle = \bigotimes_{i=0}^{\lambda-1} |b_i\rangle = |b_0\rangle \otimes |b_1\rangle \otimes \cdots \otimes |b_{\lambda-1}\rangle. \quad (4)$$

Пример: $sk = 1010 \Rightarrow |\psi_{sk}\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle$.

Это дает чистое базисное состояние, зависящее от sk.

Для повышения безопасности можно использовать запутанные пары кубитов (Bell-состояния). Например, создаются пары ЭПР (Einstein — Podolsky — Rosen) и модулируются в зависимости от sk.

Если $b_i = 1$, применяется операция Z-гейта:

$$|\Phi+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Модулированное состояние:

$$|\Phi\, b_i\rangle = \begin{cases} |\Phi+\rangle, \text{ если } b_i = 0 \\ Z \otimes I\,|\Phi+\rangle, \text{ если } b_i = 1 \end{cases}.$$

Все состояние будет иметь вид:

$$|\psi_{sk}\rangle = \otimes_{i=0}^{\lambda-1} |\Phi\, b_i\rangle.$$

На этапе доказательства к состоянию $|\psi_{sk}\rangle$ применяется унитарный оператор U_x, зависящий от доказываемого утверждения x, и получаем (1).

Например, U_x может представлять собой последовательность поворотов вокруг осей Блоха, зависящих от x:

$$U_x = R_z(\theta_x)\, R_y(\phi_x)\, R_z(\psi_x),$$

или, более формально:

$$U_x = \exp(-i\, x/2(\alpha X + \beta Y + \gamma Z)),$$

где X, Y, Z — матрицы Паули, а коэффициенты α, β, γ задают направление вращения.

На этапе проверки сравнивается полученное состояние $|\phi_x\rangle$ с ожидаемым $U_x|\psi_{sk}\rangle$ с помощью SWAP-теста. SWAP-тест измеряет степень перекрытия между двумя квантовыми состояниями и вычисляет fidelity (2), а если выполняется условие (3), то доказательство принимается.

Физическая защита от подделки квантового состояния $|\phi_x\rangle$ обеспечивается фундаментальным принципом квантовой механики — теоремой о запрете клонирования [11]. Это делает подделку $|\phi_x\rangle$ физически невозможной без знания sk.

Для примера возьмем $sk = 1010$ ($\lambda = 4$).

Кодируем каждый бит в кубит:

$$|1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle.$$

Применяем SWAP-преобразование с участием U_x, зависящего от x:

$$|\phi_x\rangle = U_x|1010\rangle.$$

Проверяющий проводит SWAP-тест:

$$F = |\langle\phi_x|U_x|1010\rangle|^2 \geq 1 - \varepsilon.$$

Если тест успешен, то доказательство принято.

Состояние $|\psi_{sk}\rangle$ создается путем применения X-вентилей к кубитам, соответствующим единичным битам секретного ключа sk. Кроме создания состояния, требуются квантовые регистры для хранения $|\psi_{sk}\rangle$, квантовые каналы для передачи $|\phi_x\rangle$ (например, одномодовые оптические линии) и меры коррекции ошибок, так как квантовые состояния чувствительны к декогеренции.

3. UC-безопасности QZKP-Hybrid

Опишем работу идеального функционала F_{QZKP}. Как уже указывалось, F_{QZKP} является моделью идеального протокола доказательства знания. Согласно этой модели, доказывающий может убедить проверяющего в том, что он знает секретное значение x, не раскрывая его.

На входе получаем запрос на доказательство от доказывающего, содержащий: сообщение M, публичные данные y, связанные с секретом x, и открытый ключ pk.

На выходе имеем результат проверки от проверяющего. Получаем accept, если доказательство принято, или reject, если есть признаки подделки или ошибки.

Функционал F_{QZKP} поддерживает следующие операции: KeyGen, Prove и Verify.

Первая операция создает пару ключей (pk, sk) и соответствующее квантовое состояние $|\psi_{sk}\rangle$, связанное с секретным ключом. Эти значения используются для подписи и верификации в рамках протокола.

На этапе доказательства функционал принимает на вход сообщение M, секретный ключ sk и возвращает классическое доказательство π и квантовое доказательство $|\phi_x\rangle$, зависящее от секретного значения x.

На последнем этапе F_{QZKP} получает сообщение M, доказательство π, квантовое состояние $|\phi_x\rangle$ и возвращает accept, если обе части доказательства корректны, или reject, если хотя бы одна из частей не прошла проверку.

Функционал F_{QZKP} гарантирует выполнение основных свойств безопасности. Если доказывающий не знает x, то вероятность того, что проверка завершится успехом, ограничена пренебрежимо малой величиной:

$$\Pr[\text{accept}] \leq \text{negl}(\lambda).$$

Если доказывающий действительно знает x, то вероятность принятия доказательства близка к единице:

$$\Pr[\text{accept}] \geq 1 - \text{negl}(\lambda).$$

Никакая внешняя система, включая квантового противника, не может с ненулевой вероятностью отличить реальное взаимодействие в рамках протокола от идеального взаимодействия с F_{QZKP}. Это свойство является ключевым для достижения UC-безопасности.

На практике это будет означать, что функционал F_{QZKP} моделирует «идеальную машину». Функционал принимает только те доказательства, которые построены на основе реального знания и полностью скрывает само значение x. Это означает, что поведение протокола в любом окружении неотличимо от идеального функционала, и даже квантовый противник не может получить дополнительную информацию или повлиять на результат доказательства.

Теорема

Протокол QZKP-Hybrid, работающий в композиции с идеальным функционалом аутентифицированного квантового канала $F_{AuthQChannel}$ и использующий EUF-qCMA — стойкую схему подписи UC, реализует идеальный функционал F_{QZKP} в квантовой среде.

Доказательство

Для доказательства построим симулятор S, который взаимодействует с идеальным функционалом F_{QZKP} и внешним окружением Z, и покажем, что его выход вычислительно неотличим от выхода реального протокола с противником A.

Симулятор S работает следующим образом:

1. Перехват и эмуляция классической части. Симулятор S перехватывает все классические сообщения от Z к A. Когда A (играя роль доказывающего P) отправляет классическое доказательство (t, z), S запускает верификацию через F_{Sig}: Verify(pk, t, z, c' = H(pk, t)). Далее симулятор S запоминает результат этой верификации.

2. Эмуляция квантового канала $F_{AuthQChannel}$. Когда A объявляет о готовности отправить квантовое состояние $|\phi_x\rangle$, S эмулирует для A поведение $F_{AuthQChannel}$. Решение S о том, что «вернуть» A (успешную доставку состояния или $\perp$), полностью зависит от его решения при взаимодействии с F_{QZKP}. Если S на шаге 1 получил false от F_{Sig}, он немедленно отправляет A сигнал $\perp$ (эмулируя сбой канала) и переходит к шагу 3. Если S на шаге 1 получил true от F_{Sig}, он откладывает эмуляцию $F_{AuthQChannel}$ до получения инструкции от F_{QZKP}.

3. Взаимодействие с F_{QZKP} и финальное решение. Симулятор S отправляет запрос в F_{QZKP}, сообщая, что получил классическое доказательство (t, z) и что квантовая часть готова к передаче (или уже передана в зависимости от модели). F_{QZKP} возвращает S решение: accept или reject. На основе этого решения S завершает эмуляцию $F_{AuthQChannel}$ для A. Если F_{QZKP} вернул accept, то S эмулирует для A успешную доставку квантового состояния. Если F_{QZKP} вернул reject, то S эмулирует для A возврат $\perp$ от $F_{AuthQChannel}$.

4. Эмуляция проверяющего. Когда Z играет роль проверяющего V и запрашивает доказательство, S запрашивает у F_{QZKP} соответствующее доказательство. Симулятор S генерирует валидную классическую подпись (t, z) через F_{Sig}. Далее S эмулирует для Z успешную передачу квантового состояния через $F_{AuthQChannel}$ (поскольку в идеальном мире F_{QZKP} гарантирует честность).

Сделаем анализ различимости. Для этого рассмотрим поведение симулятора S и реального протокола для любого противника A.

Случай 1. Классическая верификация неуспешна (Verify = false):

— Реальный мир. Протокол немедленно возвращает reject; квантовое состояние не проверяется.

— Симуляция. S немедленно эмулирует $\perp$ для A и отправляет reject в F_{QZKP}. Поведение идентично.

— Различие — 0.

Случай 2. Классическая верификация успешна (Verify = true):

— Реальный мир. Если A отправляет корректное состояние $|\phi_x\rangle$, то $F_{AuthQChannel}$ доставляет его, и протокол возвращает accept. Если A отправляет поддельное состояние, $F_{AuthQChannel}$ возвращает ⊥, и протокол возвращает reject.

— Симуляция. S отправляет запрос в F_{QZKP}. Затем F_{QZKP} возвращает accept (если A ведет себя как честный доказывающий) или reject (если A пытается обмануть). Симулятор S эмулирует $F_{AuthQChannel}$ в соответствии с решением F_{QZKP}:

F_{QZKP} = accept → S эмулирует успешную доставку.

F_{QZKP} = reject → S эмулирует ⊥.

Поведение F_{QZKP} в идеальном мире определяется тем, насколько поведение A соответствует поведению честного доказывающего. Если A отправил валидную подпись, но поддельное квантовое состояние, его поведение не соответствует честному доказывающему. Следовательно, F_{QZKP} с высокой вероятностью вернет reject, и S эмулирует ⊥, что полностью совпадает с поведением реального мира. Если A честен, F_{QZKP} вернет accept, и S эмулирует успешную доставку, что также совпадает с реальным миром.

Единственное возможное различие возникает, если F_{QZKP} примет доказательство от A, который отправил поддельное квантовое состояние. Однако, по определению F_{QZKP}, это возможно только с пренебрежимо малой вероятностью, так как F_{QZKP} требует, чтобы доказывающий знал секрет x. Поскольку A не знает x (иначе он мог бы сгенерировать корректное $|\phi_x\rangle$), то вероятность того, что F_{QZKP} примет его доказательство, пренебрежимо мала и ограничена EUF-qCMA стойкостью схемы подписи (так как A должен был подделать подпись, чтобы пройти классическую верификацию без знания sk).

Суммарное преимущество любого окружения Z в различении реального протокола (в композиции с $F_{AuthQChannel}$) и симуляции S ограничено вероятностью подделки классической подписи:

$$|\Pr[Z(\pi_{QZKP\text{-}Hybrid} \cdot F_{AuthQChannel}, A) = 1] - \Pr[Z(F_{QZKP}, S) = 1]| \le negl(\lambda).$$

Следовательно, протокол QZKP-Hybrid при наличии аутентифицированного квантового канала ($F_{AuthQChannel}$) UC реализует идеальный функционал F_{QZKP} при условии EUF-qCMA стойкости используемой схемы подписи.

Замечание

Доказательство показывает, что безопасность протокола сводится к двум хорошо изученным компонентам: постквантовой подписи и физически защищенному квантовому каналу. Это делает протокол QZKP-Hybrid жизнеспособным для практического внедрения.

4. Практическая схема кодирования кубитов

Для реализации квантовой части протокола QZKP-Hybrid предлагается использовать кодирование информации в поляризации одиночных фотонов — метод, совместимый с существующими квантовыми сетями (например, BB84). Логические состояния кодируются следующим образом: горизонтальная поляризация $|H\rangle$ соответствует $|0\rangle$, вертикальная $|V\rangle$ — $|1\rangle$.

Для обеспечения высокой чистоты однофотонных состояний фотоны генерируются с помощью SPDC-источников. Управление поляризацией осуществляется оптическими модуляторами, а детектирование реализуется с помощью высокочувствительных однофотонных детекторов (SNSPD или InGaAs APD). Передача состояний $|\phi_x\rangle$ производится по стандартным оптоволоконным каналам, что обеспечивает совместимость с телекоммуникационной инфраструктурой.

Для обеспечения надежности передачи применяются алгоритмы коррекции ошибок (например, Cascade), компенсирующие влияние декогеренции и потерь в канале. Это позволяет сохранить fidelity выше порога $1 - \varepsilon$ при проведении SWAP-теста и минимизировать количество ложных отказов.

5. Интеграция классических и квантовых компонентов

При реализации протокола QZKP-Hybrid необходимо определить, как взаимодействуют его классическая (постквантовая) и квантовая части. Их совместная работа требует согласования по нескольким направлениям.

Протокол состоит из двух частей: классического доказательства на основе LWE и квантового SWAP-тестирования. Чтобы обе проверки были корректными, важно соблюдать порядок.

Доказывающий формирует классическое доказательство (t, z) с помощью Fiat-Shamir преобразования и параллельно готовит квантовое состояние (1). Затем обе части отправляются проверяющему независимо друг от друга. Классическая часть отправляется по

обычному каналу, а квантовая передается по квантовому. Проверка проводится в два этапа, которые были описаны в первой части.

Квантовые состояния подвержены декогеренции и шуму, особенно при передаче через оптоволокно или спутниковый канал. Это может привести к снижению fidelity ниже допустимого порога даже при честном доказательстве. Для борьбы с этим будем использовать применение квантовых кодов коррекции ошибок, таких как поверхностные коды или коды Шора, фильтры и детекторы ошибок до проведения SWAP-теста [12—15]. При необходимости может потребоваться повторная передача $|\phi_x\rangle$, если уровень fidelity оказывается ниже $1 - \varepsilon$. Эти методы помогают повысить надежность квантовой части протокола и минимизировать количество ложных отказов.

Еще одной задачей является интеграция классической битовой строки sk с квантовым представлением $|\psi_{sk}\rangle$. Для этого будем каждый бит sk преобразовывать в соответствующий кубит: $0 \rightarrow |0\rangle$, $1 \rightarrow |1\rangle$. Полученные кубиты объединяются (4).

На этапе доказательства применяется унитарный оператор U_x, зависящий от утверждения x. Его будем представлять последовательностью поворотов вокруг осей Блоха (5).

Формализация связи между классическими данными и квантовыми состояниями позволяет использовать стандартные квантовые библиотеки Cirq или Qiskit [16 ; 17] для реализации U_x. Поэтому QZKP-Hybrid может быть использован в системах, поддерживающих квантовую коммуникацию. В частности, он совместим с такими протоколами, как BB84 и E91. Это открывает возможность его применения в распределенных системах, таких как блокчейн или квантовый интернет.

Несмотря на доказанную UC-безопасность и практическую реализуемость, протокол QZKP-Hybrid имеет ряд существенных ограничений, которые необходимо учитывать при его внедрении:

1. Чувствительность к декогеренции и шуму

Ограничение. Квантовые состояния $|\phi_x\rangle$, передаваемые по каналу, подвержены декогеренции, что снижает fidelity и может привести к ложному отклонению корректного доказательства.

Пути устранения. Применение протоколов коррекции ошибок (например, Cascade, Winnow) на этапе подготовки и передачи состояний. Использование квантовых повторителей или уменьшение длины канала связи. В перспективе — применение квантовых кодов коррекции ошибок (например, поверхностных кодов) для активной защиты состояний в процессе передачи.

2. Ограниченная дальность передачи квантовых состояний

Ограничение. Сегодня квантовые состояния передают по оптоволокну. Но сигнал теряется на расстоянии больше 100—200 км. Поэтому передать состояние дальше очень трудно.

Пути устранения. Можно использовать спутники. Они помогут передавать квантовые состояния между континентами. Можно создать квантовые повторители, которые будут использовать запутанные состояния. Так можно построить квантовые сети любой длины.

3. Нужен аутентифицированный квантовый канал

Ограничение. Предлагаемый протокол безопасен, только если канал сам проверяет, кто отправляет состояние. В теории это делает идеальный функционал $F_{AuthQChannel}$. На практике такого канала нет. Чтобы его заменить, нужно заранее обмениваться ключами или использовать классические ZKP. Это усложняет всю систему.

Пути устранения. Можно использовать QKD-протоколы (например, BB84). Они помогут сторонам создать общий секретный ключ. Этот ключ можно применить для аутентификации в квантовом канале. Можно разработать новые протоколы аутентификации. Они будут работать прямо во время передачи состояния $|\phi_x\rangle$. Так аутентификация станет частью самого протокола.

4. Ограниченная дальность передачи квантовых состояний

Ограничение. Современные оптоволоконные каналы с однофотонными детекторами имеют физический предел дальности (~100—200 км) из-за потерь сигнала.

Пути устранения. Использование спутниковых квантовых каналов для межконтинентальной связи. Разработка и внедрение квантовых повторителей на базе запутанных состояний для создания квантовых сетей большой протяженности.

5. Требование к аутентифицированному квантовому каналу

Ограничение. Безопасность протокола формально доказана при условии наличия идеального функционала $F_{AuthQChannel}$, который предполагает, что канал не только передает состояния, но и аутентифицирует отправителя. На практике такая аутентификация требует предварительного обмена ключами или использования классических ZKP, что усложняет систему.

Пути устранения. Интеграция с протоколами квантового распределения ключей (QKD), такими как BB84, для генерации общего секретного ключа, используемого для аутентификации квантового канала. Разработка специализированных протоколов аутентификации, встроенных в саму процедуру передачи $|\phi_x\rangle$.

6. Сложность масштабирования на большое количество участников

Ограничение. Текущая модель протокола рассчитана на взаимодействие одного доказывающего и одного проверяющего. Прямое расширение на сценарии MPC (многосторонние вычисления) или блокчейн-консенсус не определено.

Пути устранения. Разработка модифицированных версий протокола, где квантовое состояние $|\phi_x\rangle$ может быть проверено несколькими участниками параллельно или последовательно. Использование концепции «квантовых свидетелей» или распределенных квантовых регистров.

7. Зависимость от физической реализации кубитов

Ограничение. Эффективность и надежность протокола зависят от выбранной платформы (фотоны, ионы, сверхпроводящие кубиты). Например, фотоны легко передавать, но трудно хранить; сверхпроводящими кубитами легко управлять, но не передавать.

Пути устранения. Создание гибридных квантовых сетей, где для хранения используются стационарные кубиты (например, ионы), а для передачи — летающие (фотоны). Разработка универсального API для абстрагирования протокола от физического уровня.

Устранение этих ограничений является ключевым направлением для будущих исследований и будет определять практическую применимость QZKP-Hybrid в реальных инфраструктурах, таких как квантовый интернет или постквантовые блокчейны.

Заключение

Безопасность протокола доказана в рамках UC-модели. Доказательство безопасности проведено через последовательность гибридных игр. В результате показано, что преимущество любого противника пренебрежимо мало. Это означает надежность данного протокола даже при использовании в сложных системах, таких как блокчейн или распределенные сети.

В QZKP-Hybrid применяется преобразование Фиата — Шамира, чтобы сделать протокол неинтерактивным. Свойство неинтерактивности удобно для применения в сетях с ограниченной связью. Запрет на клонирование состояний в квантовых системах делает подделку доказательства невозможной без знания секретного ключа.

Протокол может применяться в системах цифровой идентификации, защищенных вычислениях, блокчейне и других областях, где важно скрыть данные, но при этом подтвердить их достоверность.

Однако есть ряд вопросов, требующих дальнейшей проработки. Нужно определить способы передачи квантовых состояний между участниками. В работе не учтено влияние декогеренции и шума на точность SWAP-тестирования. Требуется провести экспериментальные исследования на реальных квантовых устройствах.

Интерес представляет как расширение модели на случай нескольких доказывающих или проверяющих сторон, так и использование протокола в многосторонних вычислениях (MPC).

Список источников

1. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme / J. W. Bos, L. Dugas, E. Kiltz et al. URL: https://pq-crystals. Ducas org/dilithium/ (дата обращения: 09.05.2025).

2. Post-Quantum Key Exchange — A New Hope / E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe. URL: https://eprint.iacr.org/2015/1092 (дата обращения: 07.05.2025).

3. Breaking Symmetric Cryptosystems Using Quantum Period Finding / M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia // Lecture Notes in Computer Science; vol. 9815. DOI: 10.1007/978-3-662-53008-5_8

4. Canetti R. Universally Composable Security: A Tutorial / IACR Cryptology ePrint Archive. 2005. URL: https://eprint.iacr.org/2000/067 (дата обращения: 11.05.2025).

5. Resettable Zero-Knowledge / R. Canetti, O. Goldreich, S. Goldwasser, S. Micali // Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing — STOC ’00. New York, 2000. P. 235—244. URL: https://dl.acm.org/doi/10.1145/335305.335334 (дата обращения: 12.05.2025).

6. Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings / F. Benhamouda, J. Camenisch, S. Krenn, V. Lyubashevsky, G. Neven // ESORICS 2015 : conf. proc. / ed. by J. Zhou, A. Yung. Cham: Springer, 2015. P. 305—325. (Lecture Notes in Computer Science; vol. 9326). URL: https://link.springer.com/chapter/10.1007/978-3-319-24174-6_16 (дата обращения: 12.05.2025).

7. Ambainnis A., Rosmanis A., Unruh D. Quantum Attacks on Classical Proof Systems: The Hardness of Quantum Rewinding and More / IACR Cryptology ePrint Archive. Report 2020/100. 2020. URL: https://eprint.iacr.org/2014/296 (дата обращения: 11.05.2025).

8. Unruh D. Universally Composable Quantum Oblivious Transfer // ICALP 2013 : conf. proc. / ed. by F. Fomin, R. Freivalds, M. Kwiatkowska. Berlin ; Heidelberg : Springer, 2013. P. 561—572. (Lecture Notes in Computer Science. Vol. 7966). URL: https://doi.org/10.1007/978-3-642-13190-5_25

9. Bitansky N., Shmueli O. Post-Quantum Zero Knowledge in Constant Rounds // Symposium on Foundations of Computer Science (FOCS): proc. IEEE, 2020. P. 219—230. URL: https://eprint.iacr.org/2019/1279.

10. Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography // Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing — STOC ’05. New York, USA, 2005. P. 84—93. URL: https://dl.acm.org/doi/10.1145/1060590.1060603 (дата обращения: 15.06.2025).

11. Wooters W. K., Zurek W. H. A Single Quantum Cannot be Cloned // Nature. 1982. Vol. 299, no. 5886. P. 802—803. DOI: 10.1038/299802a0

12. Shor P. W. Scheme for Reducing Decoherence in Quantum Computer Memory // Physical Review A. 1995. Vol. 52, no. 4. P. R2493—R2496. DOI: 10.1103/PhysRevA.52.R2493

13. Steane A. M. Error Correcting Codes in Quantum Theory // Physical Review Letters. 1996. Vol. 77, iss. 5. P. 793—797. DOI: 10.1103/PhysRevLett.77.793

14. Gottesman D. An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation // Proceedings of Symposia in Applied Mathematics. 2010. Vol. 68. P. 13—58. URL: https://doi.org/10.48550/arXiv.0904.2557

15. Fast, Efficient Error Reconciliation for Quantum Key Distribution / W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson et al // Physical Review A. 2003. Vol. 67, no. 2. Art. 022301. URL: https://doi.org/10.1103/PhysRevA.67.052303

16. Cirq: A Python Framework for Creating Quantum Circuits / Google Quantum AI. URL: https://quantumai.google/cirq (дата обращения: 15.06.2025).

17. Qiskit: Open-Source Framework for Quantum Computing / IBM Research. URL: https://qiskit.org (дата обращения: 15.06.2025).

References

1. Bos J.W., Ducas L., Kiltz E. et al. Crystals-Dilithium: A Lattice-Based Digital Signature Scheme. Available at: https://pq-crystals. org/dilithium/ (accessed: 09.05.2025).

2. Alkim E., Ducas L., Pöppelmann T., Schwabe P. Post-Quantum Key Exchange – a New Hope. Available at: https://eprint.iacr.org/2015/1092 (accessed: 07.05.2025).

3. Kaplan M., Leurent G., Leverrier A., Naya-Plasencia M. Breaking Symmetric Cryptosystems Using Quantum Period Finding, Advances in Cryptology – CRYPTO 2016 : Annual International Cryptology Conference. Berlin ; Heidelberg : Springer, 2016, pp. 207–237 (Lecture Notes in Computer Science, vol. 9815). DOI: 10.1007/978-3-662-53008-5_8

4. Canetti R. Universally Composable Security. IACR Cryptology ePrint Archive. 2005. Available at: https://eprint.iacr.org/2000/067 (accessed: 11.05.2025).

5. Canetti R., Goldreich O., Goldwasser S., Micali S. Resettable Zero-Knowledge (extended abstract), Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21–23, 2000, New York, USA, 2000, pp. 235–244. Available at: https://dl.acm.org/doi/10.1145/335305.335334 (accessed: 12.05.2025).

6. Benhamouda F., Camenisch J., Krenn S., Lyubashevsky V., Neven G. Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings, Computer Security – ESORICS 2015 : 20th European Symposium on Research in Computer Security. Vienna, Austria, September 21–25, 2015, Proceedings, Part I. Cham: Springer, 2015, pp. 305–325. (Lecture Notes in Computer Science, vol. 9326). Available at: https://link.springer.com/chapter/10.1007/978-3-319-24174-6_16 (accessed: 12.05.2025).

7. Ambainnis A., Rosmanis A., Unruh D. Quantum Attacks on Classical Proof Systems: The Hardness of Quantum Rewinding and More, IACR Cryptology ePrint Archive. Report 2020/100. 2020. Available at: https://eprint.iacr.org/2014/296 (accessed: 11.05.2025).

8. Unruh D. Universally Composable Quantum Oblivious Transfer, ICALP 2013 : conf. proc. / ed. by F. Fomin, R. Freivalds, M. Kwiatkowska. Berlin ; Heidelberg : Springer, 2013, pp. 561–572 (Lecture Notes in Computer Science, vol. 7966). Available at: https://doi.org/10.1007/978-3-642-13190-5_25

9. Bitansky N., Shmueli O. Post-Quantum Zero Knowledge in Constant Rounds, Symposium on Foundations of Computer Science (FOCS) : proc. IEEE, 2020, pp. 219–230. Available at: https://eprint.iacr.org/2019/1279.

10. Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography, Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing – *STOC ’05*. New York, USA, 2005, pp. 84–93. Available at: https://dl.acm.org/doi/10.1145/1060590.1060603 (accessed: 15.06.2025).

11. Wooters W.K., Zurek W.H. A Single Quantum Cannot be Cloned, Nature, 1982, vol. 299, no. 5886, pp. 802–803. DOI: 10.1038/299802a0

12. Shor P.W. Scheme for Reducing Decoherence in Quantum Computer Memory, Physical Review A. 1995, vol. 52, no. 4, pp. R2493–R2496. DOI: 10.1103/PhysRevA.52.R2493

13. Steane A.M. Error Correcting Codes in Quantum Theory, Physical Review Letters, 1996, vol. 77, iss. 5, pp. 793–797. DOI: 10.1103/PhysRevLett.77.793

14. Gottesman D. An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation, Proceedings of Symposia in Applied Mathematics, 2010, vol. 68, pp. 13–58. Available at: https://doi.org/10.48550/arXiv.0904.2557

15. Buttler W.T, Lamoreaux S.K., Torgerson J.R. et al. Fast, Efficient error Reconciliation for Quantum Key Distribution, Physical Review A, 2003, vol. 67, no. 2. Art. 022301. Available at: https://doi.org/10.1103/PhysRevA.67.052303

16. Cirq: A Python Framework for Creating Quantum Circuits. Google Quantum AI. Available at: https://quantumai.google/cirq (accessed: 15.06.2025).

17. Qiskit: Open-source Framework for Quantum Computing. IBM Research. Available at: https://qiskit.org (accessed: 15.06.2025).

Информация об авторе

Кузнецов Сергей Борисович — кандидат физико-математических наук, доцент, ведущий инженер-исследователь, Научный центр информационных технологий и искусственного интеллекта, Университет «Сириус», федеральная территория «Сириус», Сочи, Российская Федерация. E-mail: kuznetsov.sb@talantiuspeh.ru

Information about the author

Sergey B. Kuznetsov — Candidate of Sciences (Physics and Mathematics), Associate Professor, Leading Research Engineer, Scientific Center for Information Technology and Artificial Intelligence, University “Sirius”, Federal Territory “Sirius”, Sochi, Russian Federation. E-mail: kuznetsov.sb@talantiuspeh.ru

Статья поступила в редакцию 23.09.2025; одобрена после рецензирования 24.12.2025; принята к публикации 14.01.2026.
The article was submitted 23.09.2025; approved after reviewing 24.12.2025; accepted for publication 14.01.2026.