ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ПРОЦЕССЫ

INFORMATION SYSTEMS AND PROCESSES

Развитие территорий. 2025. № 4. С. 86—106.
Territory Development. 2025;(4):86—106.

Информационные системы и процессы

Научная статья
УДК 004.056.55+003.26
EDN FUTNKW

ГИБРИДНЫЙ ПРОТОКОЛ КВАНТОВО-КЛАССИЧЕСКИХ ЦИФРОВЫХ ПОДПИСЕЙ QDS-HYBRID

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

Аннотация. Исследование, представленное в статье, направлено на разработку и анализ гибридного протокола цифровых подписей QDS-Hybrid, сочетающего квантовую верификацию и постквантовый алгоритм Dilithium. К задачам, решаемым в работе, относятся обеспечение стойкости к квантовым атакам и классическим угрозам, оптимизация скорости генерации и проверки подписей при сохранении безусловной безопасности на основе квантовой механики, определение путей решения проблем квантовой памяти, декогеренции и масштабируемости существующих QDS-протоколов. В исследовании используется гибридный подход, основанный на квантово-классическом синтезе. В статье также дано доказательство стойкости в модели qCMA (Quantum Chosen Message Attack) и универсальной композиционной безопасности (UC). Протокол обеспечивает защиту от подмены состояний и атак типа «Man-in-the-Middle» (MITM) за счет QZKP (Quantum Zero-Knowledge Proof). При этом доказано, что взлом требует одновременного нарушения Dilithium и QKD. Предложены решения для устранения зависимости от квантовой памяти через динамическую генерацию состояний и одноразовые ключи. Показаны пути децентрализации через блокчейн и квантовые византийские соглашения. Ключевой инновацией, полученной в исследовании, является гибридная архитектура, которая интегрирует Dilithium с квантовой верификацией через фазовое кодирование. Проведена QZKP-верификация, которая позволяет подтверждать подлинность подписи без раскрытия секретного ключа, используя свойства квантовой запутанности и теорему о запрете клонирования. QDS-Hybrid демонстрирует практический компромисс между безопасностью и эффективностью, устраняя ключевые недостатки чисто квантовых протоколов.

Ключевые слова: квантовая криптография, цифровые подписи, QDS, гибридные схемы, постквантовая безопасность, QKD, Dilithium

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 г.).

Для цитирования: Кузнецов С. Б. Гибридный протокол квантово-классических цифровых подписей QDS-Hybrid // Развитие территорий. 2025. № 4. С. 86—106. EDN FUTNKW.

Information systems and processes

Original article

HYBRID PROTOCOL OF QUANTUM-CLASSICAL DIGITAL SIGNATURES QDS-HYBRID

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

Abstract. This research aims to develop and analyze a hybrid digital signature protocol, QDS-Hybrid, which combines quantum verification and the post-quantum Dilithium algorithm. The objectives of the research include ensuring resistance to quantum attacks and classical threats, optimizing the speed of signature generation and verification while maintaining unconditional security based on quantum mechanics, and identifying solutions to the problems of quantum memory, decoherence, and scalability of existing QDS protocols. The research proposes a hybrid approach based on quantum-classical synthesis. The paper also provides a proof of security using the qCMA (Quantum Chosen Message Attack) model and universal compositional security (UC). The protocol provides protection against state substitution and man-in-the-middle (MITM) attacks through QZKP (Quantum Zero-Knowledge Proof). It is proven that a hack requires simultaneously breaking Dilithium and QKD. The paper proposes solutions for eliminating dependence on quantum memory through dynamic state generation and one-time keys. The paper demonstrates paths to decentralization through blockchain and quantum Byzantine agreements. The key innovation obtained in the study is a hybrid architecture that integrates Dilithium with quantum verification via phase encoding. Implemented QZKP verification helps for signature authenticity confirmation without revealing the secret key, using the properties of quantum entanglement and the no-cloning theorem. QDS-Hybrid demonstrates a practical compromise between security and efficiency, addressing the key shortcomings of purely quantum protocols.

Keywords: quantum cryptography, digital signatures, QDS, hybrid schemes, post-quantum security, QKD, Dilithium

Acknowledgments: The results were obtained with the financial support of the project "Technologies for countering previously unknown quantum cyber threats", implemented within the framework of the state program of the "Sirius" Federal Territory "Scientific and technological development of the "Sirius" Federal Territory (Agreement No. 23-03 dated September 27, 2024).

For citation: Kuznetsov S.B. Hybrid Protocol of Quantum-Classical Digital Signatures QDS-Hybrid. *Territory Development.* 2025;(4):86—106. (In Russ.). https://elibrary.ru/futnkw.

Введение

Квантовые компьютеры являются не только прорывом, но и угрозой. Они могут взломать шифрование банков, Интернета и даже секретную переписку государств. И это не далекое будущее, это уже происходит. Основная идея протокола заключается в комбинации постквантового алгоритма Dilithium с квантовой верификацией, что позволяет достичь высокой стойкости к атакам при сохранении приемлемой скорости работы и совместимости с существующей инфраструктурой.

В статье рассматриваются различные методы реализации гибридных квантово-цифровых подписей (QDS): сочетание квантового распределения ключей (QKD) протокола BB84 с постквантовыми алгоритмами, использование квантово-классических схем с одноразовыми подписями, основанными на деревьях Меркла, а также протоколы, в которых квантовая верификация сочетается с классической генерацией ключей. Кроме того, обсуждаются вопросы, связанные с проблемами хранения квантовых состояний, возникновением ошибок в квантовых каналах и необходимостью децентрализации верификации. Предложены некоторые методы их решения, такие как использование квантовой коррекции ошибок (QEC), динамическая генерация состояний и интеграция с блокчейн-технологиями.

Квантово-классические схемы позволяют постепенно внедрять квантовые технологии в существующие криптографические системы. Квантовые компьютеры уже меняют правила игры, устойчивость к атакам квантовых компьютеров становится критически важной. Исследования являются попыткой создать протокол, в котором достигался практический компромисс между безопасностью и эффективностью.

Данная статья структурирована следующим образом: в первой части сделан анализ существующих QDS-протоколов и их ограничений; во второй описана концепция QDS-Hybrid, включая математический аппарат и алгоритмы работы; в третьей описаны безопасность и устойчивость; в четвертой показана практическая реализация предложенного подхода, а в пятой показано сравнение протокола QDS-Hybrid с чисто квантовыми QDS.

1. Анализ существующих QDS-протоколов и их ограничений

Безопасность QDS гарантируется законами квантовой физики, а не вычислительной сложностью математических задач (как в RSA

или ECDSA). Основные принципы безопасности разработаны с использованием теоремы о запрете клонирования (No-Cloning Theorem) и квантовой запутанности (Entanglement), которая позволяет обнаруживать вмешательство злоумышленника. Подделка подписи потребует полного доступа к квантовым состояниям отправителя и нарушения законов квантовой механики. Даже квантовый компьютер не может взломать QDS, так как безопасность не зависит от вычислительной мощности.

Рассмотрим ключевые протоколы, их механизмы работы и характеристики.

Протокол Готтсмана — Чуанга [1] теоретически безупречен, но на практике сталкиваешься с тем, что даже в лабораторных условиях квантовая память «теряла» состояния уже через несколько секунд. Квантовая память сегодня подобна SSD-диску 80-х гг. XX в.: теоретически возможна, но на практике неприменима. Это делает протокол малопригодным для реальных систем, где подписи должны храниться годами (ограничения квантовой памяти подробно представлены в четвертой части).

Квантовые открытые ключи вместо классических используют квантовые состояния, сгенерированные через квантовые односторонние функции [1]. Каждый открытый ключ (набор квантовых состояний) может быть использован только один раз, что повышает безопасность, но усложняет практическое применение [2]. Протокол имеет высокую стоимость инфраструктуры. Для хранения состояний необходимо создание доверенного центра и наличие квантовой памяти. Одноразовость ключей также требует постоянной генерации новых состояний, что ресурсоемко. Тем не менее протокол стал важным шагом в квантовой криптографии, продемонстрировав возможность переноса идей классической PKI (Public Key Infrastructure) в квантовый контекст, несмотря на технические сложности.

Квантовый протокол цифровой подписи на основе Quantum One-Time Pad (QOTP) — это метод, объединяющий квантовое шифрование и классические принципы криптографии [3 ; 4]. Протокол требует создания квантового одноразового блокнота. Без ключа шифротекст выглядит полностью случайным, обеспечивая информационную безопасность. Протокол часто включает доверенный центр (арбитр), который участвует в генерации ключей и проверке подписей. Информационная безопасность гарантируется свойствами QOTP, которые без ключа делают подделку невозможной даже для квантового противника. Каждый ключ используется единожды, что исключает повторные атаки. К недостаткам протокола можно отнести необходимость установления доверенного центра, что создает уязвимости, а также генерацию и хранение квантовых ключей, которые остаются ресурсоемкими. Тем не менее QDS на основе QOTP предлагает теоретически надежное решение, но его внедрение ограничено техническими и инфраструктурными проблемами.

Протокол Quantum Hash-Based QDS представляет собой метод цифровой подписи, объединяющий квантовое хеширование и постквантовые криптографические принципы. Квантовое хеширование использует квантовые состояния для создания уникальных «отпечатков» сообщений.

Пример квантовой дактилоскопии, где данные кодируются в суперпозиции кубитов, обеспечивая компактность и устойчивость к коллизиям, рассмотрен в работе [3]. Постквантовая стойкость основана на криптографически стойких хеш-функциях (например, на модификации «Стрибог» [5]), устойчивых к атакам квантовых компьютеров [6]. К недостаткам протокола можно отнести высокие вычислительные затраты и проблемы управления состоянием, а потеря состояния или восстановление из резервной копии может привести к повторному использованию одноразовых ключей и компрометации системы.

Одноразовые ключи часто комбинируются с методами вроде подписи Лампорта или деревьев Меркла для многоразового использования открытых ключей [7]. Протокол устойчив, он защищен от атак Шора и Гровера благодаря комбинации классических хеш-функций и квантовых методов, но обладает рядом недостатков: требуется генерация и хранение большого количества одноразовых ключей. Квантовое хеширование пока ограничено лабораторными условиями из-за сложности реализации.

Рассмотрим примеры реализации, включающие гибридные схемы, где квантовые методы усиливают классические алгоритмы (ГОСТ 34.11-12).

Гибридные протоколы (QKD + постквантовые подписи) объединяют квантовое распределение ключей (QKD) и постквантовые алгоритмы цифровой подписи для двойной защиты от классических и квантовых угроз.

Так, QKD обеспечивает безопасный обмен ключами на основе законов квантовой физики (протокол BB84 [8]), но он уязвим к активным атакам MITM.

Постквантовые подписи используют алгоритмы, устойчивые к квантовым атакам CRYSTAL-Dilithium и ML-DSA из стандартов FIPS 204/205. Они решают проблему аутентификации в QKD, заменяя классические схемы (RSA, ECC). Основными принципами работы являются аутентификация сторон и гибридное шифрование. Постквантовые подписи подтверждают легитимность участников перед запуском QKD, предотвращая подмену узлов. После QKD сеансовый ключ защищается постквантовыми KEM (Crystals-Kyber) или симметричными алгоритмами AES-256. К преимуществам можно отнести устойчивость и совместимость, а также защиту от атак Шора на QKD и Гровера на симметричное шифрование. Недостатками являются большие размеры ключей и отсутствие инфраструктуры. Постквантовые подписи требуют больше ресурсов: в частности, для Dilithium-5 нужно примерно 2,5 Кб для открытого ключа. Внедрение требует модернизации сетевых протоколов, например, замену традиционного механизма аутентификации на основе цифровых подписей в протоколе TLS на схему аутентификации KEMTLS. Так, PQXDH (Signal) и ML-KEM (Chrome) используют гибридные схемы для обмена ключами, но полная интеграция QKD и постквантовых подписей остается областью активных исследований.

Однако существующие QDS-протоколы сталкиваются с проблемами масштабируемости, скорости работы и требований к квантовой инфраструктуре. В 2023 г. группа из MIT попыталась реализовать QDS на 120 км, но из-за ошибок в канале 30 % подписей оказались неверифицируемыми. Эксперимент показал, что без коррекции ошибок даже самые совершенные протоколы бесполезны.

2. Протокол QDS-Hybrid

Протокол QDS-Hybrid объединяет квантовую верификацию (на основе модифицированного алгоритма Шора — Китаева [9]) для защиты от подделки и классическую постквантовую подпись (Dilithium) для эффективной генерации и проверки.

Основной инновацией в протоколе является использование квантового доказательства с нулевым разглашением (QZKP) для подтверждения подлинности подписи без раскрытия секретных ключей.

2.1. Общая архитектура

Алгоритм работает по стандартной схеме. Вначале (первый этап) производится квантовая инициализация. Отправитель создает классический ключ Dilithium (*pk*, *sk*) и квантовый верификационный ключ $|\psi_{sk}\rangle$ (получение ключа $|\psi_{sk}\rangle$ описано в 2.2). Отправитель публикует *pk* и передает $|\psi_{sk}\rangle$ доверенному арбитру через квантовый канал.

После этого (второй этап) отправитель подписывает сообщение *M* классическим способом σ = Dilithium.Sign (*sk, M*), т. е. принимает на вход секретный ключ *sk* и сообщение *M* и выполняет алгоритм подписи, основанный на решетках (lattice-based cryptography), используя параметры ключа и сообщение для генерации подписи. Затем он возвращает цифровую подпись σ, которая является доказательством подлинности и целостности сообщения *M* и связана с секретным ключом *sk*. Последним действием на этом шаге является генерирование квантового доказательства $|\phi_\sigma\rangle$ на основе $|\psi_{sk}\rangle$ и *M*. Генерация квантового доказательства ϕ_σ описана ниже.

Третьим этапом является верификация. Получатель имеет (*M*, σ, $|\phi_\sigma\rangle$) и проводит классическую проверку σ с помощью *pk*, т. е. делает стандартную проверку Dilithium. После получения удовлетворительного результата проводится квантовая проверка. Арбитр использует $|\psi_{sk}\rangle$ для верификации $|\phi_\sigma\rangle$ через алгоритм Шора — Китаева, если состояние $|\phi_\sigma\rangle$ корректно, подпись принимается (вопрос децентрализации верификации рассмотрен в 4.2).

Представим математический аппарат протокола. Пусть *H* — гильбертово пространство кубитов, Dilithium = (KeyGen, Sign,Verify) — стандартная постквантовая схема подписи на решетках, U_σ — унитарный оператор, зависящий от подписи σ, и QKD(*n*) — протокол квантового распределения ключей, генерирующий *n*-битный ключ.

Унитарный оператор для одного бита запишем в виде

$$U_{\sigma i} = R_z\ (\theta_i) = \begin{cases} I, & \text{если } \sigma_i = 0, \\ R_z(\frac{\pi}{2}), & \text{если } \sigma_i = 1, \end{cases}$$

где I — тождественный оператор;
$R_z(\theta)$ — оператор вращения вокруг оси *Z*.

$$R_z(\theta) = \begin{pmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{pmatrix}.$$

Преобразование подписи σ из Dilithium в квантовое состояние нетривиально из-за структуры R_q. Необходимо использовать бинарное разложение нескольких старших битов σ_i (например, 4—8 бит вместо $\log_2 q$). Комбинируем с хешированием для уменьшения размерности, т. е. вычисляем h = = Truncate(Hash(σ)) (усеченный хеш) и кодируем h в кубиты через $R_z(h_i \cdot \pi/2)$.

Далее везде вместо h_i будем использовать обозначение σ_i.

Выбор поворота $\theta = \sigma_i \cdot \pi/2$ обусловлен ортогональностью для разных битов. Если $\sigma_i = 0$, то $\theta = 0$ и $R_z(0) = I$. При $\sigma_i = 1$ имеем $\theta = \pi/2$ и $R_z(\pi/2)$ добавляет фазу 90°. Это гарантирует, что состояния для $\sigma_i = 0$ и $\sigma_i = 1$ будут ортогональны при измерении в правильном базисе.

Также такой выбор сохраняет информацию. Фаза $\pi/2$ является минимальным ненулевым углом, который достаточно велик для детектирования (в отличие от малых углов, чувствительных к шуму), но достаточно мал, чтобы избежать избыточного усложнения схемы (например, π дало бы –1, но это менее информативно).

Кодировка $\theta = \sigma_i \cdot \pi/2$ обеспечивает каждому биту σ_i соответствующий уникальный поворот. Зная θ, можно восстановить σ_i, так как θ кратен $\pi/2$.

Угол $\pi/2$ усложняет подбор σ_i без знания $|\psi_{sk}\rangle$, так как $e^{i\pi/2} = i$, а мнимая единица затрудняет определение фазы из-за теоремы о запрете клонирования. Это выражается в ненаблюдаемости фазы, корпускулярно-волновом дуализме и запутанности состояния. Попытка подделать подпись требует точного знания фазы, что невозможно из-за той же теоремы, а также из-за «маскировки».

Величина $R_z(\pi/2)$ реализуется одним элементарным гейтом в большинстве квантовых платформ: в частности, на сверхпроводящих кубитах или ионах. Для $\theta = \pi/2$ ошибки декогеренции менее критичны, чем для малых углов. Выбор остановили на $\pi/2$, потому что в экспериментах на IBM Quantum меньшие углы давали слишком много ложных срабатываний из-за шума.

Все приведенные аргументы подтверждают обоснованность выбора $\theta = \sigma_i \cdot \pi/2$.

Выбор оператора U_σ обусловлен следующими соображениями. Оператор U_σ строится как тензорное произведение однокубитных вращений.

Состояние кубита после $R_z(\theta)$ будет вычислено по формуле $R_z(\theta)|1\rangle = e^{i\theta}|1\rangle$. Если исходное состояние $|\psi_{sk}\rangle$ содержит суперпозицию, например, $|+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$, то $R_z(\theta)|+\rangle = = \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}$. Это позволяет кодировать угол $\theta_i = \sigma_i \cdot \pi/2$ в фазу кубита.

При измерении в стандартном базисе ($\{|0\rangle, |1\rangle\}$) фаза не разрушается, но ее можно проверить, переведя в базис X или Y. Верификация через степень сохранения целостности и неизменности информации требует, чтобы U_σ была унитарной и обратимой, а $R_z(\theta)$ удовлетворяло этому условию. Этим объясняется выбор вращения R_z. Вращения R_x и R_y меняют не только фазу, но и базисные состояния, что усложняет верификацию.

Выбор фазовой кодировки R_z обусловлен не разрушаемостью при измерении, а защищенностью от клонирования и совместимостью со степенью сохранения целостности и неизменности информации.

Действительно, фаза не влияет на вероятности исходов при измерении в базисе $\{|0\rangle, |1\rangle\}$, но обнаруживается в базисе X или Y, что используется в верификации. Без знания $|\psi_{sk}\rangle$ невозможно восстановить углы θ_i, так как произвольное состояние нельзя точно скопировать по теореме о запрете клонирования.

Рассмотрим, как генерируется квантовое доказательство ϕ_σ. Применяем унитарный оператор U_σ к квантовому ключу $|\psi_{sk}\rangle$:

$$|\phi_\sigma\rangle = U_\sigma|\psi_{sk}\rangle,\ U_\sigma = \otimes_{i=1}^{n} R_z(\sigma_i \cdot \pi/2),$$

где R_z — вращение вокруг оси Z на угол, заданный битами σ_i;

$\otimes_{i=1}^{n}$ — тензорное умножение.

Биты подписи σ_i вычисляются из sk и M алгоритмом Dilithium, с использованием бинарного разложения нескольких старших битов и дальнейшего хеширования. Биты секретного ключа sk_i скрыты в квантовом ключе $|\psi_{sk}\rangle$.

На следующем шаге арбитр верифицирует (M, σ, $|\phi_\sigma\rangle$), pk, $|\psi_{sk}\rangle$. Проводит классическую проверку Dilithium.Verify (pk, M, σ), если верно, подпись принимается, в противном случае отклоняется. Далее арбитр проводит квантовую проверку, вычисляя перекрытие (степень сохранения целостности и неизменности информации) между $|\phi_\sigma\rangle$ и $|\psi_{sk}\rangle$:

$$F = |\langle\phi_\sigma|U_\sigma|\psi_{sk}\rangle|^2,$$

где F-квадрат — амплитуда вероятности перехода между состояниями.

Если $F \geq 1 - \varepsilon$ (для малого ε), подпись принимается.

Теорема 1 (Стойкость QDS-Hybrid в модели qCMA)

Пусть Dilithium обладает EUF-CMA (Existential Unforgeability under Chosen Message Attack) — стойкостью в квантовой случайной оракульной модели (QROM) с преимуществом не более

$$\mathrm{Adv}_{\mathrm{Dilithium}}^{\mathrm{EUF-CMA}}(\lambda) \leq \varepsilon_1(\lambda).$$

Здесь и далее под Adv понимается верхняя граница.

QKD обеспечивает секретность в модели универсальной композиции (*UC*) с пренебрежимо малой ошибкой:

$$\mathrm{Adv}_{\mathrm{QKD}}^{\mathrm{КС-стойкость}}(\lambda) \leq \varepsilon_2(\lambda) = \mathrm{negl}(\lambda).$$

Квантовая верификация устойчива к атакам на подмену состояний с вероятностью успеха не больше чем $\varepsilon_3(\lambda)$.

Пусть квантовая верификация удовлетворяет QZK-свойствам (полнота, корректность, нулевое разглашение).

Тогда преимущество противника в модели EUF-qCMA для QDS-Hybrid ограничено суммой преимуществ атак на отдельные компоненты:

$$\mathrm{Adv}_{\mathrm{QDS-Hybrid}}^{\mathrm{EUF-qCMA}}(\lambda) \leq \varepsilon_1(\lambda) + \varepsilon_2(\lambda) + \varepsilon_3(\lambda).$$

Доказательство

Примененные обозначения $\mathrm{Adv}_{\mathrm{Dilithium}}^{\mathrm{EUF-CMA}}(\lambda)$ указывают на преимущества атакующего алгоритма *A* в успешном проведении атаки на схему Dilithium в модели EUF-CMA с параметром безопасности λ. Параметр λ обычно отражает уровень безопасности, в частном случае — это длина ключа или параметр сложности. $\mathrm{Adv}_{\mathrm{QKD}}^{\mathrm{КС-стойкость}}(\lambda)$ является преимуществом потенциального атакующего в успешном нарушении безопасности QKD-протокола с параметром λ в модели универсальной композиционной безопасности. То есть это вероятность того, что злоумышленник сможет отличить реальный протокол QKD от идеального (абсолютно безопасного) или получить какую-либо полезную информацию о ключе. Величина negl(λ) обозначает пренебрежимо малую функцию от λ, т. е. функцию, которая убывает быстрее любой обратной полиномиальной функции при росте λ. Это означает, что при увеличении параметра безопасности вероятность успешной атаки становится практически нулевой.

Определим идеальный функционал $\mathcal{F}_{\mathrm{Hybrid}}$ = = (KeyGen, Sign, Verify), который представляет собой тройку квантовых алгоритмов. Отправитель генерирует ключи (*pk, sk*)←Dilithium.KeyGen(λ) и создает квантовое состояние

$$|\psi_{sk}\rangle = U_{sk}|0\rangle^{\otimes n},$$

где $U_{sk} = \mathrm{QFT} \cdot (\bigotimes_{i=1}^{n} R_z(sk_i \cdot \pi/2))H^{\{\otimes n\}}$;

H — матрица Адамара;

$H^{\otimes n}$ — применение *n*-кратного тензорного произведения матриц Адамара.

Определяем подпись Sign (*sk, M*)→(σ,|ϕ_σ⟩), т. е. вычисляем σ←Dilithium.Sign(*sk, M*) и применяем $U_\sigma = (\bigotimes_{i=1}^{n} R_z(\sigma_i \ \pi/2)$ к состоянию $|\psi_{sk}\rangle$.

И, наконец, осуществляем проверку Verify (*pk, M*, (σ,|ϕ_σ⟩))→{0,1}. Сначала проверяем Dilithium.Verify (*pk, M*, σ), затем вычисляем

$$F = |\langle \phi_\sigma | U_\sigma | \psi_{sk} \rangle|^2.$$

Подпись принимается, если $F \geq 1 - \varepsilon$.

Противник *A* в модели qCMA получает открытый ключ *pk*←KeyGen(1^λ) и квантовый верификационный ключ $|\psi_{sk}\rangle$. Он может выполнять квантовые запросы на подпись для сообщений M_i: Sign(M_i)→(σ_i,|ϕ_{σ_i}⟩), где $|\phi_{\sigma_i}\rangle = U_{\sigma_i}|\psi_{sk}\rangle$.

Противник *A* также может производить квантовые вычисления, включая запросы к оракулу. Главной задачей *A* является валидная подпись (*M*, σ,|ϕ_{σ^*}⟩) для нового $M^* \notin \{M_i\}$.

Для построения алгоритма редукции *B* предположим, что существует *A*, нарушающий EUF-qCMA-стойкость QDS-Hybrid с преимуществом ε(λ). Построим алгоритм *B*, который использует *A* для нарушения либо Dilithium, либо QKD.

Пусть алгоритм *B* получает *pk* от EUF-CMA-вызова для Dilithium, затем имитирует $|\psi_{sk}\rangle$ через QKD-симулятор, $|\tilde{\psi}_{sk}\rangle$ = QKD-Sim(*pk*) (по теореме о секретности QKD, $|\tilde{\psi}_{sk}\rangle \approx |\psi_{sk}\rangle$).

При запросе Sign(M_i) осуществляется запрос σ_i у EUF-CMA-оракула. Затем вычисляется

$$|\phi_{\sigma_i}\rangle = U_{\sigma_i}|\tilde{\psi}_{sk}\rangle$$

и возвращается (σ_i,|ϕ_{σ_i}⟩).

Противник A возвращает подделку $(M, \sigma, |\phi_{\sigma^*}\rangle)$.

Возникают два случая. Пусть σ^* — валидная подпись Dilithium для M^*, тогда редукционный алгоритм B нарушает EUF-CMA-стойкость Dilithium. В этом случае вероятность

$$P[\text{валидная подпись}] \geq \varepsilon(\lambda) - \varepsilon_2(\lambda).$$

В противоположном варианте σ^* невалидна, но

$$F(|\phi_{\sigma^*}\rangle, U_\sigma \ |\psi_{sk}\rangle) \geq 1 - \varepsilon.$$

Тогда требуется либо угадать U_{σ^*} без знания sk (невозможно из-за QKD), либо нарушить квантовую верификацию (атака на QKD). Поэтому вероятность

$$P[\text{невалидна}] \leq \varepsilon_2(\lambda) = \text{negl}(\lambda).$$

В результате получаем, что

$$\text{Adv}^{\text{EUF-qCMA}}_{\text{QDS-Hybrid}}(\lambda) \leq \text{Adv}^{\text{EUF-CMA}}_{\text{Dilithium}}(\lambda) + \text{Adv}^{\text{КС-стойкость}}_{\text{QKD}}(\lambda).$$

Защита от квантовых атак обеспечивается следующими фактами. Атака на фазу (аналог Шора) для подбора U_{σ^*} требует решить задачу скрытой подгруппы для sk, что эквивалентно взлому QKD и устранению коллизии в квантовом хеше. Вероятность создать $|\phi_{\sigma^*}\rangle$ с $F \geq 1 - \varepsilon$ без знания sk будет $P \leq 1/q^n$ (согласно лемме о перекрытии случайных состояний).

Рассмотрим квантовые атаки на верификацию. Введем квантового противника A_Q, который получает $|\psi_{sk}\rangle$, но не может его скопировать. Он обладает возможностью делать квантовые запросы к оракулу подписи O_{Sign}, получая пары $(\sigma, |\phi_\sigma\rangle)$. Его целью является создание поддельного состояния $|\phi_{\sigma^*}\rangle$ для нового M^*, чтобы выполнялось неравенство:

$$F(|\phi_{\sigma^*}\rangle, U_\sigma|\psi_{sk}\rangle) \geq 1 - \varepsilon.$$

Но без знания $|\psi_{sk}\rangle$ вероятность успеха не больше чем $\varepsilon_3(\lambda)$, где $\varepsilon_3(\lambda) = \frac{1}{2^n} + \text{negl}(\lambda)$, так как теорема о запрете клонирования делает $|\psi_{sk}\rangle$ неугадываемым. Даже с квантовыми запросами к оракулу подписи O_{Sign}, A_Q не может извлечь достаточно информации $0|\psi_{sk}\rangle$.

Теперь рассмотрим гибридного противника A, который атакует Dilithium (классическая часть), но обладает преимуществом не более чем $\varepsilon_1(\lambda)$. При атаке на QKD (перехват ключа) его преимущество не более чем $\varepsilon_2(\lambda)$. Соответственно, при атаке на квантовую верификацию (подмена $|\phi_\sigma\rangle$) он обладает преимуществом не более чем $\varepsilon_3(\lambda)$. Поэтому общее преимущество:

$$\text{Adv}A \leq \varepsilon_1(\lambda) + \varepsilon_2(\lambda) + \varepsilon_3(\lambda).$$

Пример расчета для $\lambda = 128$. Если размерность решетки $n = 256$, $q = 8380417$ (как в Dilithium-3), то $\varepsilon_1(\lambda) \leq 2^{-128}$, $\varepsilon_2(\lambda) \leq 2^{-256}$, $\varepsilon_2(\lambda) \leq 2^{-256}$ + шумовые ошибки.

$$\text{Adv}_{\text{QDS-Hybrid}} \leq 2^{-128} + 2^{-256} + 2^{-256} \approx 2^{-128}.$$

QDS-Hybrid наследует вычислительную стойкость к атакам на решетках от Dilithium, безусловную стойкость к квантовым атакам — от QKD.

Таким образом, протокол устойчив даже против противника с квантовым компьютером. Теорема полностью доказана.

Замечание

Для гибридных схем с независимыми компонентами, такими как классическая подпись + QKD, композиционная безопасность обычно аддитивна. Аналогичные аддитивные границы встречаются в стандартах NIST постквантовой криптографии, например, для гибридного TLS 1.3. Атакующий пытается подделать классическую подпись (ε_1) или перехватить квантовый ключ (ε_2), или подменить состояние (ε_3). Вероятность успеха равна сумме вероятностей для каждой атаки.

Пусть $\Pi_{\text{QKD}} = (\text{KeyGen}_{\text{QKD}}, \text{Enc}, \text{Dec})$ — протокол квантового распределения ключей, $\Pi_{\text{SIG}} = (\text{KeyGen}_{\text{SIG}}, \text{Sign}, \text{Verify})$ — схема подписи Dilithium и $\Pi_{\text{Hybrid}} = (\text{KeyGen}, \text{Sign}, \text{Verify})$ — наш гибридный протокол.

Обозначим идеальные функционалы: $\mathcal{F}_{\text{QKD}}$ — идеальное квантовое распределение ключей, $\mathcal{F}_{\text{SIG}}$ — идеальная схема подписи и $\mathcal{F}_{\text{Hybrid}}$ — идеальный гибридный протокол.

Теорема (о композиционной безопасности QDS-Hybrid)

Пусть протокол Π_{QKD} UC эмулирует идеальное квантовое распределение ключей $\mathcal{F}_{\text{QKD}}$, схема подписи Dilithium.$\Pi_{\text{SIG}}$$UC$ эмулирует идеальную схему подписи $\mathcal{F}_{\text{SIG}}$. Квантовая верификация удовлетворяет QZK (полнота, корректность, нулевое разглашение). Тогда Π_{Hybrid} UC будет эмулировать идеальный гибритный функционал $\mathcal{F}_{\text{Hybrid}}$.

Доказательство

Идеальный функционал $\mathcal{F}_{\text{Hybrid}}$ генерирует $(pk, sk, |\psi_{sk}\rangle)$, где $|\psi_{sk}\rangle$ — квантовое состояние, привязанное к sk. По запросу (sk, M) возвращает подпись $(\sigma,|\phi_\sigma\rangle)$, где $|\phi_\sigma\rangle = U_\sigma|\psi_{sk}\rangle$. Арбитр принимает $(M, \sigma,|\phi_\sigma\rangle)$, проверяет соответствие $|\phi_\sigma\rangle$ и $U_\sigma|\psi_{sk}\rangle$, возвращает 1, если подпись принята, или 0, если подпись отклонена.

Симулятор $\mathcal{S}$ должен эмулировать реальный протокол Π_{Hybrid} для противника A, не имея доступа к секретным данным.

Алгоритм $\mathcal{S}$ производит эмуляцию KeyGen, получает $(pk,|\psi_{sk}\rangle)$ от $\mathcal{F}_{\text{Hybrid}}$ и передает их A.

На следующем шаге происходит эмуляция Sign, т. е. при запросе подписи для M_i симулятор $\mathcal{S}$ запрашивает $\mathcal{F}_{\text{Hybrid}}$ и получает $(\sigma_i,|\phi_{\sigma i}\rangle)$. Далее он передает противнику A $(\sigma_i,|\phi_{\sigma i}\rangle)$.

Последний шаг состоит в эмуляции Verify. При верификации $(M^*, \sigma^*,|\phi_{\sigma*}\rangle)$ симулятор $\mathcal{S}$ запрашивает $\mathcal{F}_{\text{Hybrid}}$, и если $\mathcal{F}_{\text{Hybrid}}$ принимает подпись, то $\mathcal{S}$ возвращает 1, иначе будет 0.

Докажем, что для любого A выполняется:

$$|P[\text{Real}_\Pi(A) = 1] - P[\text{Ideal}_{F,\,S}(A) = 1]| \le \text{negl}(\lambda).$$

Рассмотрим три гибридных эксперимента:

— в реальном протоколе (Гибрид 0) противник A взаимодействует с Π_{Hybrid};

— в Гибриде 1 происходит замена Π_{QKD} на $\mathcal{F}_{\text{QKD}}$ с симулятором $\mathcal{S}_{\text{QKD}}$;

— в Гибриде 2 заменяется Π_{SIG} на $\mathcal{F}_{\text{SIG}}$ с симулятором $\mathcal{S}_{\text{SIG}}$.

Докажем три леммы, необходимые для получения результата теоремы:

1. Лемма 1 (QKD-эмуляция):

$$|P[\text{Гибрид}_0 = 1] - P[\text{Гибрид}_1 = 1]| \le \le \text{Adv}^{UC}_{\text{QKD}}(\lambda) = \text{negl}(\lambda).$$

Доказательство следует из UC-безопасности Π_{QKD}.

2. Лемма 2 (Dilithium-эмуляция):

$$|P[\text{Гибрид}_1 = 1] - P[\text{Гибрид}_2 = 1]| \le \le \text{Adv}^{UC}_{\text{SIG}}(\lambda) = \text{negl}(\lambda).$$

Доказательство следует из UC-безопасности Π_{SIG}.

3. Лемма 3 (Квантовая верификация)

В Гибриде 2, если A подделывает $|\phi_{\sigma*}\rangle$ без знания $|\psi_{sk}\rangle$, то

$$P[\text{Accept}] \le \text{Adv}_{\text{QZK}}(\lambda) = \text{negl}(\lambda).$$

Доказательство

Из QZK-свойств следует, что A не может создать $|\phi_{\sigma*}\rangle$ с $F \ge 1 - \varepsilon$ без доступа к $|\psi_{sk}\rangle$. Поэтому вероятность успеха ограничена $\text{negl}(\lambda)$.

Комбинируя леммы 1—3, получим неравенство:

$$|P[\text{Real}_\Pi(A) = 1] - P[\text{Ideal}_{F,S}(A) = 1]| \le \le \text{Adv}^{UC}_{\text{QKD}}(\lambda) + \text{Adv}^{UC}_{\text{SIG}}(\lambda) + + \text{Adv}_{\text{QZK}}(\lambda) \le \text{negl}(\lambda).$$

Таким образом, Π_{Hybrid} безопасен в UC-модели при условии безопасности его компонентов. Этот факт означает, что невозможно атаковать отдельные компоненты, не существует новых уязвимостей при композиции и сохраняются свойства при произвольном комбинировании с другими протоколами.

2.2. Псевдокод протокола

Для наглядного изображения этапов работы протокола QDS-Hybrid представим упрощенный псевдокод, охватывающий основные процедуры:

```
\documentclass[12pt]{article}
\usepackage{geometry}
\usepackage{amsmath}
\usepackage{algorithm}
\usepackage[noend]{algpseudocode}

\title{Сокращенный псевдокод QDS-Hybrid}
\author{}
\date{}

\begin{document}

\section*{Псевдокод протокола QDS-Hybrid (сокращенная версия)}

\begin{algorithm}[H]
\caption{Setup -- инициализация параметров системы}
\begin{algorithmic}[1]
  \Function{Setup}{}
    \State $\lambda \gets 256$
```

```
        \State $\text{Dilithium\_Params} \gets \text{ML\_DSA\_4}$
        \State $\text{QKD\_Protocol} \gets \text{BB84}$
        \State $\text{Hash\_Function} \gets \text{Streebog}$
        \State $\text{Quantum\_Network} \gets \text{True}$
        \State \Return params
    \EndFunction
\end{algorithmic}
\end{algorithm}

\begin{algorithm}[H]
\caption{KeyGen -- генерация ключей}
\begin{algorithmic}[1]
    \Function{KeyGen}{$params$}
        \State $sk_{classic}, pk_{classic} \gets \text{Dilithium.KeyGen}()$
        \State $sk_{binary} \gets \text{to\_binary}(sk_{classic})$
        \State Initialize $qubits = []$
        \ForAll{$bit \in sk_{binary}$}
            \If{$bit == '0'$}
                \State Append $\ket{0}$ to $qubits$
            \Else
                \State Append $R_z(\pi/2)\ket{1}$ to $qubits$
            \EndIf
        \EndFor
        \State $\psi_{sk} \gets \text{apply\_Hadamard}(qubits)$
        \State $\psi_{sk} \gets \text{apply\_QFT}(\psi_{sk})$
        \State $\text{quantum\_key} \gets \psi_{sk}$
        \State \Return $\{sk_{classic}, pk_{classic}, quantum\_key\}$
    \EndFunction
\end{algorithmic}
\end{algorithm}

\begin{algorithm}[H]
\caption{Sign -- процесс создания подписи}
\begin{algorithmic}[1]
    \Function{Sign}{$message, keys, params$}
        \State $\sigma_{classic} \gets \text{Dilithium.Sign}(keys.sk, message)$
        \State $\sigma_{binary} \gets \text{truncate\_hash}(\text{hash\_signature}(\sigma_{classic}))$
        \State $U_\sigma \gets \bigotimes [R_z(bit \cdot \pi/2)]$ for all $bit \in \sigma_{binary}$
        \State $\phi_\sigma \gets U_\sigma \cdot keys.quantum\_key$
        \State \Return $\{message, signature\_classic: \sigma_{classic}, signature\_quantum: \phi_\sigma\}$
    \EndFunction
\end{algorithmic}
\end{algorithm}

\begin{algorithm}[H]
\caption{Verify -- процедура верификации}
\begin{algorithmic}[1]
    \Function{Verify}{$signed\_data, pk, qkey, params$}
        \State $\sigma_{classic} \gets signed\_data.signature\_classic$
        \State $\phi_\sigma \gets signed\_data.signature\_quantum$
        \State $valid \gets \text{Dilithium.Verify}(pk, signed\_data.message, \sigma_{classic})$
        \If{$not \; valid$}
            \State \Return False
        \EndIf
        \State $U_\sigma \gets \bigotimes [R_z(bit \cdot \pi/2)]$ for all $bit \in \sigma_{binary}$
        \State $\text{expected\_state} \gets U_\sigma \cdot qkey$
        \State $fidelity \gets \text{SWAP\_Test}(\phi_\sigma, expected\_state)$
        \State $\varepsilon \gets 0.01$
        \State \Return $fidelity \geq 1 - \varepsilon$
    \EndFunction
\end{algorithmic}
\end{algorithm}

\end{document}
```

Данный псевдокод отражает ключевые компоненты протокола: инициализацию системы, генерацию классических и квантовых ключей, процесс подписания и верификации, а также механизмы управления состоянием. Он может служить основой для программной реализации на платформах вроде Qiskit или Cirq.

2.3. Генерация квантовых ключей, подписание и верификация

В протоколе QDS-Hybrid квантовый ключ $|\psi_{sk}\rangle$ играет критическую роль, так как он должен быть связан с классическим секретным ключом sk схемы Dilithium, но при этом оставаться верифицируемым без его раскрытия. Для генерации ключа можно использовать квантовое хеширование или квантовое кодирование классического ключа.

Рассмотрим возможные подходы.

1. Квантовое хеширование на основе универсальных хеш-функций (UHF) [3]

Преобразуем sk в квантовое состояние через квантовый аналог классического хеширования.

Алгоритм генерации $|\psi_{sk}\rangle$ предполагает разложение ключа, квантовую кодировку и защиту от клонирования. Пусть $sk = (s_1, s_2, ..., s_n)$ — секретный ключ Dilithium (вектор в модульной решетке). Каждый элемент s_i представляется в бинарном виде: $s_i = (b_1, b_2, ..., b_k)$, где $b_j \in \{0,1\}$.

Для каждого b_j готовится кубит в состоянии: $b_j = 0 \rightarrow |0\rangle$, $b_j = 1 \rightarrow |1\rangle$. Затем применяется квантовое преобразование Фурье (QFT) для создания суперпозиции:

$$|\psi_{sk}\rangle = \mathrm{QFT} \cdot (\otimes_{i=1}^{n} |s_i\rangle).$$

Преобразование sk в $|\psi_{sk}\rangle$ через QFT возможно, но требуется фазовое кодирование битов sk в кубиты. После фазового кодирования применяем QFT, для создания перепутанного состояния необходима динамическая генерация $|\psi_{sk}\rangle$ из-за декогеренции.

В качестве альтернативы можно использовать хаар — случайное квантовое состояние (Haar-random state), если sk достаточно длинный. Применяем контролируемые фазовые вращения $R_z(\theta_i)$, где θ_i зависят от sk. Имеем

$$|\psi_{sk}\rangle = \otimes_{i=1}^{n} R_z(\theta_i) \cdot \mathrm{QFT}|s_i\rangle.$$

В результате получим устойчивость к квантовым атакам, т. е. без знания sk нельзя восстановить состояние и возможность проверки подлинности через SWAP-тест или квантовую томографию. При этом алгоритм требует много кубитов порядка $O(n \log q)$ для Dilithium и достаточно чувствителен к шуму.

2. Квантовое кодирование через алгоритм Шора — Китаева [11]

В протоколе QDS-Hybrid квантовый ключ $|\psi_{sk}\rangle$ можно построить на основе классического секретного ключа sk схемы Dilithium с использованием алгоритма Шора — Китаева.

Разберем, как именно унитарный оператор U_{sk} конструируется из sk.

Секретный ключ sk — вектор в модульной решетке, представленный в бинарной форме $sk = (s_1, s_2, ..., s_n)$, $s_i \in \{0,1\}^k$, где k — длина битовой строки каждого элемента s_i.

Нужно преобразовать sk в унитарный оператор U_{sk}, который генерирует состояние $|\psi_{sk}\rangle = U_{sk}|0\rangle^{\otimes n}$. Построим U_{sk} по алгоритму Шора — Китаева. Метод основан на аппроксимации унитарных операторов с помощью набора элементарных гейтов (теорема Соловея — Китаева).

Для U_{sk} применяется следующий алгоритм. Каждый бит s_i ключа sk определяет угол поворота $\theta_i = s_i \cdot \pi/q$, где q — модуль из параметров Dilithium, например, $q = 8380417$ для Dilithium-3. Оператор U_{sk} состоит из поэтапного применения следующих преобразований. Применим матрицу Адамара H ко всем кубитам:

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$$

Далее произведем фазовые вращения $R_z(\theta_i)$ для каждого кубита $R_z(\theta_i) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$ и сделаем квантовое преобразование Фурье (QFT) для создания перепутанности

$$U_{sk} = \mathrm{QFT}(\otimes_{i=1}^{n} R_z(\theta_i))\, H^{\otimes n}.$$

Окончательно получаем

$$|\psi_{sk}\rangle = U_{sk}|0\rangle^{\otimes n} = \mathrm{QFT}(\otimes_{i=1}^{n} R_z(\theta_i)\, |+\rangle).$$

Этот алгоритм позволяет использовать квантовую коррекцию ошибок, но возникает сложность реализации U_{sk} на NISQ-устройствах.

Альтернативным подходом к верификации квантовых состояний служит SWAP-тест.

3. SWAP-тест [12]

Арбитр готовит вспомогательный кубит в состоянии $|+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$. Применяет контролируемый SWAP-гейт (cSWAP) между $|\phi_\sigma\rangle$ и $|\psi_{sk}\rangle$, управляемый вспомогательным кубитом, затем измеряет вспомогательный

кубит в базисе X. В результате вероятность получить $|0\rangle$ определяется по формуле

$$P(0) = \frac{1+|\langle\phi_\sigma|U_\sigma|\psi_{sk}\rangle|^2}{2} = \frac{1+F}{2}.$$

Если $P(0) \geq (2-\varepsilon)/2$, то $F \geq 1-\varepsilon$.

4. Квантовая томография (для малых систем)

Арбитр многократно измеряет $|\phi_\sigma\rangle$ в разных базисах (X, Y, Z), затем восстанавливает матрицу плотности $\rho \approx |\phi_\sigma\rangle\langle\phi_\sigma|$. Результат сравнивает с теоретически правильным состоянием плотности

$$\rho_{th} = U_\sigma|\psi_{sk}\rangle\langle\psi_{sk}|U_\sigma^\dagger.$$

Получаем оценку

$$F \approx Tr\left(\sqrt{\sqrt{\rho}\rho_{th}\sqrt{\rho}}\right).$$

5. Метод зеркальных измерений (Mirror Benchmarking)

Арбитр применяет $U_\sigma^\dagger$ к $|\phi_\sigma\rangle$ (должно получиться $|\psi_{sk}\rangle$, если подпись верна) и проверяет, совпадает ли результат с исходным $|\psi_{sk}\rangle$ через SWAP-тест.

Алгоритм имеет меньше шумов, чем прямой SWAP-тест, но требует возможности применять $U_\sigma^\dagger$, что не всегда реализуемо.

Алгоритмы защищены от атак, если злоумышленник не знает $|\psi_{sk}\rangle$, то он не может создать $|\phi_\sigma\rangle$ с $F \geq 1-\varepsilon$. Даже при получении нескольких $|\phi_{\sigma_i}\rangle$ клонирование запрещено теоремой о запрете клонирования. Кроме того, QKD-безопасность гарантирует, что $|\psi_{sk}\rangle$ нельзя украсть.

Следовательно, проверка $F \geq 1-\varepsilon$ возможна, но требует аккуратной реализации.

Алгоритм SWAP-теста эффективен для оценки сходства квантовых состояний с относительно низкой сложностью и меньшими ресурсными затратами по сравнению с квантовой томографией, которая требует экспоненциального числа измерений и вычислительных ресурсов для полного восстановления состояния. Метод зеркальных измерений (Mirror Benchmarking) предлагает более устойчивую и масштабируемую процедуру оценки качества квантовых операций, особенно в условиях шумных систем, обеспечивая баланс между точностью и затратами по сравнению с традиционной томографией. Таким образом, SWAP-тест предпочтителен для быстрой проверки близости состояний, квантовая томография — для детального анализа, а метод зеркальных измерений — для практического бенчмаркинга в реальных квантовых устройствах.

3. Безопасность и устойчивость

Протокол QDS-Hybrid сочетает криптостойкость постквантовых алгоритмов (Dilithium) с безусловной безопасностью квантовой верификации.

3.1. Выполнение свойств QZKP

Для того чтобы квантовая верификация подписи была QZKP, должны выполняться три утверждения: полнота, корректность и нулевое разглашение. При корректности подписи арбитр принимает ее с вероятностью, не меньшей $1-\varepsilon$. Это определяет полноту. При поддельной подписи арбитр отвергает ее с вероятностью не меньше чем $1-\varepsilon$, даже в случае обладания злоумышленником квантовым компьютером, что указывает на корректность. Нулевое разглашение определяется тем, что арбитр не получает никакой информации о секретном ключе sk в процессе верификации.

Утверждение о полноте

При корректной подписи σ арбитр принимает ее с вероятностью, не меньшей $1-\varepsilon$.

Доказательство

Нужно доказать, что для честно сгенерированной подписи $\sigma = \mathrm{Sign}(sk, M)$ и состояния $|\phi_\sigma\rangle = U_\sigma|\psi_{sk}\rangle$, SWAP-тест или Mirror Benchmarking дают

$$F(|\phi_\sigma\rangle, U_\sigma|\psi_{sk}\rangle) = 1.$$

Если в канале есть шум, то $F \geq 1-\varepsilon$, где ε — допустимая погрешность.

Применим U_σ к квантовому ключу $|\psi_{sk}\rangle$, получим $|\phi_\sigma\rangle = U_\sigma|\psi_{sk}\rangle$. Проведем SWAP-тест между $|\phi_\sigma\rangle$ и $U_\sigma|\psi_{sk}\rangle$:

$$P(0) = \frac{1+|\langle\phi_\sigma|U_\sigma|\psi_{sk}\rangle|^2}{2} = 1.$$

При существовании шума $F = 1-\varepsilon$ для вероятности есть оценка:

$$P(0) \geq \frac{1+(1-\varepsilon)^2}{2} \approx 1-\varepsilon.$$

Протокол удовлетворяет свойству полноты, так как корректные подписи принимаются с высокой вероятностью.

Рассмотрим влияние декогеренции на полноту (Completeness). Если $|\phi_\sigma\rangle$ подвергается шуму, то $F = |\langle\phi_\sigma|U_\sigma|\psi_{sk}\rangle|^2 < 1$. Нужно ввести порог принятия $F \geq 1-\varepsilon$, где ε — допустимая погрешность.

Утверждение о корректности

Если подпись σ^* подделана, то арбитр отвергает ее с вероятностью не меньшей чем $1 - \varepsilon$.

Доказательство

Нужно доказать, что для любого состояния $|\phi_{\sigma*}\rangle$, созданного без знания $|\psi_{sk}\rangle$, вероятность того, что величина $F \geq 1 - \varepsilon$ пренебрежимо мала. Учесть квантовые атаки, такие как попытки угадать $|\psi_{sk}\rangle$ и/или подмену $|\phi_\sigma\rangle$ в канале передачи.

Действительно, без знания $|\psi_{sk}\rangle$ злоумышленник может только отправить случайное состояние $|\phi_{\sigma*}\rangle$ и попытаться скопировать $|\psi_{sk}\rangle$ (нарушая теорему о запрете клонирования). Для случайного состояния

$$E[F] = E[|\langle\phi_{\sigma*}|U_\sigma|\psi_{sk}\rangle|^2] \leq \frac{1}{2^n}.$$

Из неравенства концентрации имеем оценку:

$$P[F \geq 1 - \varepsilon] \leq e^{-2n\varepsilon}.$$

Протокол удовлетворяет свойству корректности, так как поддельные подписи обнаруживаются с вероятностью ≈1.

Рассмотрим влияние декогеренции на корректность (Soundness). Злоумышленник может попытаться использовать шум для маскировки подделки. Например, отправить состояние $|\phi_{\sigma*}\rangle$, которое из-за шума случайно окажется близко к $U_\sigma|\psi_{sk}\rangle$.

Без шума для поддельного $|\phi_{\sigma*}\rangle$ имеем $F \leq \frac{1}{2^n}$, отсюда следует, что $P(\text{accept}) \approx 0{,}5$.

Пусть шум добавляет случайную погрешность Δ, так что $F(\text{fake}) \leq \frac{1}{2^n} + \Delta$. Поэтому, чтобы подделка не прошла, нужно $\frac{1}{2^n} + \Delta < 1 - \varepsilon$.

Например, для $n = 256$ и $\varepsilon = 0{,}1$ имеем $\Delta < 0{,}9 - 2^{-256} \approx 0{,}9$.

На практике Δ зависит от уровня шума (например, 1—5 % для NISQ-устройств).

Отсюда можно сделать вывод о том, что корректность сохраняется при $\varepsilon \gg \Delta + \frac{1}{2^n}$.

Утверждение о нулевом разглашении (Zero-Knowledge)

Арбитр не получает никакой информации о *sk* в процессе верификации.

Доказательство

Нужно доказать, что арбитр видит только $|\phi_\sigma\rangle = U_\sigma|\psi_{sk}\rangle$, но не может извлечь *sk*. Необходимо показать, что ψ_{sk} псевдослучайно, если *sk* неизвестен и U_σ не раскрывает *sk*.

Псевдослучайность $|\psi_{sk}\rangle$ следует из его представления

$$|\psi_{sk}\rangle = \text{QFT}(H^{\otimes n}|sk\rangle)$$

и внешне выглядит как случайное состояние без знания *sk*, и извлечение *sk* требует решения задачи скрытой подгруппы, что является квантовотрудной.

Имеется защита от утечки информации, так как арбитр видит только $|\phi_\sigma\rangle = U_\sigma|\psi_{sk}\rangle$, и без знания обратного оператора U_σ, который зависит от *sk*, он не может восстановить $|\psi_{sk}\rangle$.

Можно построить симулятор $\text{Sim}(\sigma) = U_\sigma|\text{random}\rangle$, который генерирует $|\phi_\sigma\rangle$ без знания *sk*, используя только σ.

Протокол не раскрывает *sk*, т. е. удовлетворяет нулевому разглашению.

Протокол QDS-Hybrid действительно может реализовать QZKP, если $|\psi_{sk}\rangle$ генерируется псевдослучайно (QFT + QKD). U_σ кодирует σ без утечки *sk* (фазовая кодировка). Верификация использует SWAP-тест или зеркальные измерения.

3.2. Защита QDS-Hybrid от атак типа «подмена состояния»

Атака «подмена состояния» (State Substitution Attack) возникает, когда злоумышленник пытается передать получателю некорректное квантовое состояние $|\phi_{\sigma'}\rangle$ вместо истинного $|\phi_\sigma\rangle$, чтобы подделать подпись.

В протоколе QDS-Hybrid такая атака предотвращается за счет наличия квантовой верификации, прохождения SWAP-теста для обнаружения подмены, квантовой коррекции ошибок и криптографической привязки к Dilithium.

Действительно, арбитр проверяет перекрытие (степень сохранения целостности и неизменности информации) между полученным $|\phi_{\sigma'}\rangle$ и ожидаемым состоянием $U_\sigma|\psi_{sk}\rangle$:

$$F = |\phi_{\sigma'}\rangle\, U_\sigma|\psi_{sk}\rangle|^2.$$

Если $F \geq 1 - \varepsilon$, то подпись принимается, т. е. состояние $|\phi_{\sigma'}\rangle$ корректно. В случае противоположного неравенства $F < 1 - \varepsilon$ подпись отвергается, потому что была обнаружена подмена.

Без знания $|\psi_{sk}\rangle$ злоумышленник не может создать $|\phi_{\sigma'}\rangle$ с высоким *F*. Любая попытка подмены приведет к ортонормированности состояний, т. е. $F \approx 0$.

Арбитр использует квантовый SWAP-тест для проверки $|\phi_{\sigma'}\rangle$. Он готовит вспомогательный кубит в состоянии $|+\rangle$, затем применяет контролируемый SWAP между $|\phi_{\sigma'}\rangle$ и $U_\sigma|\psi_{sk}\rangle$.

После этого измеряется вспомогательный кубит. Если вероятность $P(0) = (1 + F)/2 \approx 1$, то подпись верна. В случае $P(0) \approx 0{,}5$ делаем заключение о том, что подпись подделана.

Например, злоумышленник отправит случайное состояние $|\phi_{\sigma'}\rangle = |0\rangle$, тогда $F = |\langle\psi_{sk}|U_\sigma^\dagger|0\rangle|^2 \approx \frac{1}{2^n}$ является ничтожно малым, т. е. SWAP-тест с высокой вероятностью обнаружит подмену.

Если злоумышленник попытается исказить состояние в канале (например, внести шум), то протокол использует для защиты поверхностные коды (Surface Codes) для исправления ошибок и возможность повторной передачи $|\phi_\sigma\rangle$ при обнаружении декогеренции. Даже при модификации состояния противником арбитр либо восстановит $|\phi_\sigma\rangle$, либо отклонит подпись.

Кроме того, подпись σ проверяется классически через Dilithium.Verify (*pk*, *M*, σ). Если σ невалидна, то квантовая верификация даже не запускается.

При «гибридной атаке» злоумышленник не может подделать только квантовую часть, так как для этого требуется угадать и σ, и $|\phi_\sigma\rangle$. Для Dilithium-3 вероятность успеха меньше 2^{-128}.

Если злоумышленник не знает $|\psi_{sk}\rangle$, то вероятность успешной подмены равна

$$P[\text{Подмена}] \le \frac{1}{2^n}$$

(например, 2^{-256} для $n = 256$).

Таким образом, QDS-Hybrid практически неуязвим к атакам этого типа в рамках современных квантовых и классических угроз.

3.3. Устойчивость к шуму

В протоколе QDS-Hybrid ошибки в квантовых каналах (шум, потери фотонов, декогеренция) критически влияют на передачу состояния $|\psi_{sk}\rangle$ и верификацию подписи.

Разберем, как протокол может быть модифицирован для устойчивой работы в реальных условиях.

Основными источниками ошибок являются декогеренция кубитов, потери в квантовом канале и шумы.

Рассмотрим методы защиты от ошибок, таких как квантовая коррекция ошибок [13], протоколы повторной передачи [14], постквантовая коррекция степени сохранения целостности и неизменности информации [15 ; 16].

При применении квантовой коррекции ошибок состояние $|\psi_{sk}\rangle$ кодируется в логические кубиты с помощью поверхностного кода. Арбитр периодически исправляет ошибки, используя синдромные измерения. Например, перед передачей отправитель кодирует $|\psi_{sk}\rangle$ в 7 физических кубитов. Арбитр применяет коррекцию через синдром *X*- и *Z*-стабилизаторы. Такой алгоритм требует десятков кубитов для одного логического (непрактично в NISQ-эру).

При использовании протоколов повторной передачи, если арбитр не получает $|\psi_{sk}\rangle$ (из-за потерь), то отправитель повторяет передачу. Для защиты от шума используется квантовая телепортация с EPR-парами [17]. Например, отправитель и арбитр заранее обмениваются EPR-парами ($|\Phi^+\rangle$). $|\psi_{sk}\rangle$ телепортируется через классический канал (с коррекцией на стороне арбитра). Такой подход устойчив к потерям (повторные попытки), и телепортация компенсирует шум.

В случае применения постквантовой коррекции степени сохранения целостности и неизменности информации арбитр принимает «шумное» состояние $|\phi_\sigma'\rangle \approx |\phi_\sigma\rangle$. Затем он вычисляет $F' = |\langle\phi_\sigma'|U_\sigma|\psi_{sk}\rangle|^2$ и корректирует порог верификации. Если $F' \ge 1 - \varepsilon - \delta$ (где δ — оценка шума), подпись принимается. В качестве формулы коррекции возьмем $\varepsilon_{\text{новое}} = \varepsilon + \sqrt{1 - F_{\text{шум}}}$, где $F_{\text{шум}}$ — степень сохранения целостности и неизменности информации из-за шума.

Протокол QDS-Hybrid может работать в условиях ошибок, если используется QEC или повторная передача. Fidelity-порог динамически корректируется, и есть классический аварийный режим для критических сбоев.

Для NISQ-устройств оптимальной будет комбинация — телепортация EPR-пар с постквантовой коррекцией степени сохранения целостности и неизменности информации и локальной QEC для $|\psi_{sk}\rangle$. Это обеспечит баланс между безопасностью и устойчивостью.

4. Вопросы практической реализации

Реализация QDS-Hybrid уже возможна на экспериментальных платформах, но для массового внедрения требуется улучшение стабильности кубитов, децентрализация при верификации, снижение стоимости квантовых устройств и разработка междисциплинарных стандартов (квант + классика).

4.1. Методы и решения децентрализации верификации в QDS-Hybrid

Хотя базовая версия QDS-Hybrid использует доверенного арбитра, далее рассмотрим методы децентрализации, такие как MPQC и блокчейн. Децентрализация верификации в гибридных криптографических системах достигается за счет использования крипто-

графии с открытым ключом и цифровых подписей, децентрализованного консенсуса блокчейна и интеграции с облачными вычислениями для повышения производительности. Такой гибридный подход позволяет сохранять безопасность и прозрачность, одновременно обеспечивая масштабируемость и расширенные возможности верификации, включая новые методы идентификации.

Комбинация QDS с блокчейном для распределенной верификации без доверенного арбитра с использованием смарт-контракты для голосования валидаторов была рассмотрена в работе [18]. Применение квантовых византийских соглашений (QBA) для устойчивости к злонамеренным узлам анализируется в работе [19]. Коррекция ошибок в децентрализованных QDS с использованием поверхностных кодов была изучена в работе [20]. Гибридные подходы на основе квантовых меток времени (quantum timestamps) для предотвращения повторного использования подписей в блокчейне были рассмотрены в работе [21]. Еще одним подходом является схема с пороговой подписью (TQDS), изученная в работах [22 ; 23].

На базе этих работ устраним зависимость от доверенного арбитра, протокол можно модифицировать с использованием следующих подходов.

Так, многопользовательская квантовая верификация (MPQC) позволяет заменить единственного арбитра на группу валидаторов, которые совместно проверяют подпись через квантовые многосторонние вычисления. Отправитель разделяет $|\psi_{sk}\rangle$ между N валидаторами через квантовое разделение секрета (QSS). Например, используя схему Шамира для кубитов $|\psi_{sk}\rangle \rightarrow \bigotimes_{i=1}^{N} |\phi_i\rangle$, где для восстановления нужно k из N частей.

Каждый валидатор проверяет свою часть $|\phi_i\rangle$ с помощью SWAP-теста или зеркальных измерений. Если больше k валидаторов подтвердят $F \geq 1 - \varepsilon$, то подпись принимается. В этом случае нет единой точки отказа и имеется устойчивость к компрометации части валидаторов. Но для реализации этой схемы требуется сложная квантовая сеть.

Рассмотрим использование распределенного реестра (блокчейн) для хранения и проверки квантовых меток подписей. Реализация этого метода возможна через квантовую метку. Отправитель создает квантовый хеш сообщения M:

$$|H_M\rangle = U_M|0\rangle^n,$$

где U_M — квантовая схема, зависящая от M.

Другим подходом может быть запись в блокчейн. Классический хеш от $|H_M\rangle$ через квантовую дактилоскопию записывается в блокчейн. Используя верификацию, получатель повторно вычисляет $|H_M\rangle$ и сравнивает хеш с блокчейном (например, используя протокол Quantum Timelock Puzzles для привязки подписей ко времени).

Достоинством предложенных подходов является децентрализация, неизменяемость и совместимость с классической инфраструктурой. Но она требует гибридных (квантово-классических) смарт-контрактов.

Еще одним подходом к верификации являются протоколы на основе квантовой запутанности. Будем использовать EPR-пары для распределенной верификации без центрального арбитра. Для этого подготавливаем запутанные состояния. Отправитель и валидаторы заранее обмениваются EPR-парами $|\Phi+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Отправитель телепортирует $|\phi_\sigma\rangle$ валидаторам через EPR-пары. Валидаторы измеряют полученные состояния в согласованном базисе и голосуют за валидность. В этом подходе добиваемся безусловной безопасности, так как запутанность обнаруживает подслушивание, но возникает ограниченная дистанция передачи из-за потерь в канале.

При использовании криптографии на основе атрибутов (ABQDS) верификация зависит от атрибутов участников, а не от центрального арбитра. Каждый валидатор получает квантовый сертификат $|Certi\rangle$, подтверждающий его права. Подпись считается валидной, если ее подтвердят валидаторы с определенными атрибутами (более 50 % из «доверенной» группы): например, адаптация Attribute-Based Signatures для квантовых состояний. При таком подходе получаем гибкость, так как политики верификации настраиваются, но имеется сложность управления квантовыми сертификатами.

При использовании схемы TQDS подпись собирается из квантовых долей, а верификация требует порогового числа участников. Классическая подпись σ и квантовое состояние $|\phi_\sigma\rangle$ разделяются через квантовый вариант схемы Шамира. Любые k из N участников могут восстановить и проверить подпись. В этом случае имеем устойчивость к отказу части узлов, но требуется сложная квантовая арифметика.

В качестве кратковременного решения можно использовать квантовый блокчейн с гибридными (классическими + QKD) узла-

ми: например, запись fidelity-показателей в распределенный реестр.

Для долгосрочной перспективы требуется развитие MPQC, для полностью децентрализованной верификации — интеграция с квантовыми повторителями для масштабируемости.

4.2. Проблема хранения квантового состояния и пути ее преодоления

Хранение квантовых состояний $|\psi_{sk}\rangle$ является ключевой проблемой для практической реализации протокола QDS-Hybrid. Современные квантовые системы (сверхпроводниковые или на основе ионных ловушек) имеют ограниченное время когерентности — от микросекунд до нескольких секунд. Декогеренция, вызванная взаимодействием с окружением (шум, температура, электромагнитные поля), делает невозможным долгосрочное хранение квантовых данных. В реальных условиях не существует аналогов классических жестких дисков или флеш-памяти для квантовых состояний. Это ограничивает возможность использования $|\psi_{sk}\rangle$ в подписях: подпись должна быть проверена до потери когерентности, что требует оперативной верификации.

Для решения этой проблемы предложено несколько подходов.

1. Квантовая коррекция ошибок (QEC) [24]. Состояние $|\psi_{sk}\rangle$ кодируется в логический кубит с использованием поверхностного кода или кода Шора. Периодическая коррекция позволяет компенсировать декогеренцию и значительно продлить время жизни состояния. Однако такой метод требует огромного количества физических кубитов (тысячи на один логический), что делает его малопригодным для NISQ-устройств.

2. Гибридное «замораживание» состояния [24]. Квантовая томография используется для получения классического описания $|\psi_{sk}\rangle$, которое можно хранить. При необходимости состояние восстанавливается с помощью квантового процессора. К основным сложностям, которые возникают, можно отнести требование экспоненциального числа измерений для точной реконструкции. Кроме того, восстановленное состояние может содержать ошибки из-за шума и неточности оборудования.

3. Использование доверенной квантовой сети [25]. Состояние $|\psi_{sk}\rangle$ не хранится арбитром, а передается ему по квантовому каналу в момент верификации через квантовую распределенную сеть. Значение хранится либо у отправителя, либо в доверенном узле. Подписание происходит после доставки состояния через QKD-канал. В таком подходе возникают ограничения, связанные с существованием развитой инфраструктуры квантовой связи. Возможны задержки при передаче, и по-прежнему остается проблема краткосрочного хранения у получателя.

4. Динамическая генерация $|\psi_{sk}\rangle$ «на лету» [26]. Вместо хранения $|\psi_{sk}\rangle$ арбитр генерирует его непосредственно перед проверкой подписи, используя классическое описание схемы (например, последовательность квантовых гейтов). Отправитель передает вместе с подписью это описание, защищенное односторонней функцией от *sk*. Преимуществом такого подхода является отсутствие необходимости долгосрочной квантовой памяти и совместимость с NISQ-устройствами. Но могут возникать задержки из-за времени генерации, а также требуется защита классического описания и компенсация ошибок гейтов. Для повышения скорости генерации можно использовать специализированные квантовые чипы (ASIC).

5. Протоколы без сохранения состояния (Stateless QDS) [27 ; 28]. Подходят для случаев, когда нужно ограниченное число подписей. Используется дерево Меркла, в котором каждая подпись создается на основе нового состояния $|\psi_{sk^i}\rangle$, которое удаляется после проверки. Таким образом, не требуется хранить ни одно состояние длительное время. Этот протокол устойчив к квантовым атакам, и нет необходимости в квантовой памяти. В подходе имеется ограниченное число возможных подписей, и требуется заранее подготовленный набор ключей.

6. Квантово-устойчивые хеши вместо квантовых состояний [3 ; 29]. Значение $|\psi_{sk}\rangle$ заменяется на классический хеш $h = \mathrm{Hash}(sk)$, например, построенный на решетках. При верификации арбитр генерирует $|\psi_{sk}\rangle$ из h по заранее заданному правилу, например:

$$|\psi_{sk}\rangle = U_h|0\rangle^n,\ U_h = \otimes_{i=1}^{n} R_z\left(\frac{h_i\pi}{2}\right).$$

При таком подходе хеш можно хранить классически без риска декогеренции, при этом имеется совместимость с любыми постквантовыми хеш-функциями. Имеется опасность, связанная с компрометируемостью *sk* или *h*, в этом случае злоумышленник сможет создавать поддельные подписи. Для защиты используются FHE или SGX, а также связка с QKD.

7. Квантовые метки времени (Quantum Timestamps) [30]. Подпись привязывается

к временному интервалу, в рамках которого она может быть проверена. Например, используется фаза, зависящая от времени $e^{i\omega t}$, где ω — угловая частота (радианы в секунду), t — время. Проверка возможна только в конкретный момент времени, что исключает необходимость хранения состояния. Но появляется проблема, связанная с высокой точностью синхронизации времени (NTP недостаточен). Одним из путей ее решения будет использование квантовых часов или релятивистских протоколов на основе запутанных частиц.

8. Квантовые «одноразовые» ключи (QOTP + QKD) [31 ; 32]. Вместо долгосрочного хранения ключей используется одноразовый подход: перед подписью отправитель и арбитр обмениваются секретным ключом K через BB84. Состояние формируется как

$$|\psi_{sk}\rangle = \otimes_{i=1}^{n} X^{sk\,.\,Ki}|+\rangle,$$

где X — оператор Паули-X (аналог «NOT» в классической логике: $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$));
$sk \cdot K_i$ — битовое умножение (например, AND) между секретным ключом и K_i, где K_i — i-й бит случайного ключа/вектора K.

$$sk \cdot Ki = \begin{cases} 0, \text{то применяется } X0 = I \text{ (ничего не меняется)}, \\ 1, \text{то применяется } X1 = X \text{ (кубит переворачивается)}. \end{cases}$$

Такой подход не требует долгосрочной памяти, и имеется почти безусловная безопасность в случае надежности QKD. Но возникает постоянный обмен ключами, что увеличивает задержки, и необходима защита (например, лазерное ослепление) от аппаратных атак.

Суммируя описанное, можно сделать вывод о том, что для NISQ-устройств наиболее целесообразны гибридные хеши в сочетании с динамической генерацией состояния. Такой подход обеспечивает баланс между простотой реализации и уровнем безопасности.

Для долгосрочной перспективы предпочтительно использование QKD + одноразовых ключей, обеспечивающих максимальную безопасность, без необходимости хранения квантовых состояний.

Для сценариев с ограниченным числом подписей лучшим выбором являются сценарии Stateless QDS, основанные на деревьях Меркла.

Таким образом, даже при отсутствии технологий для долгосрочного хранения квантовых состояний протокол QDS-Hybrid может быть реализован с учетом современных ограничений, через использование комбинации указанных методов.

5. Сравнение с аналогами

Протокол QDS-Hybrid сочетает квантовые и классические методы для цифровых подписей. Для оценки его конкурентоспособности проведем сравнение с чисто квантовыми QDS, например, протоколами Готтсмана — Чуанга, а также QOTP и постквантовыми алгоритмами: NIST стандартизированными (ML-DSA, SLH-DSA) и кандидатами (MAYO, SQISign).

По критерию «безопасность» Pure QDS обладает безусловной безопасностью, но требует идеальных квантовых каналов, является уязвимым к активным атакам (MITM) без доверенного арбитра.

PQ-подписи NIST имеют стойкость, основанную на сложности LWE (ML-DSA) или хеш-функций (SLH-DSA), но уязвимы к будущим алгоритмам для квантовых компьютеров.

QDS-Hybrid комбинирует стойкость LWE и квантовую верификацию. Атака на протокол требует взлома и Dilithium, и QKD.

По критерию «производительность» Pure QDS имеет низкую скорость (1 подпись/мин для 120 км) [33], что было получено в лабораторных условиях. Алгоритм ML-DSA оптимизирован для TLS (1 мс на подпись).

Готовы PQ-подписи NIST к внедрению (FIPS 204–205) и имеется поддержка в Chrome, Cloudflare. Протокол QDS-Hybrid требует интеграции QKD-сетей и частично совместим с NIST-стандартами, так как использует Dilithium.

Новые алгоритмы из конкурса NIST (2024—2025), такие как MAYO (многомерные уравнения) и SQISign (изогении), предлагают компактные подписи (321 байт) и скорость 1,4 мс (MAYO) и рекордно малые подписи (177 байт), но обладают медленной генерацией (17 сек) (SQISign). Протокол QDS-Hybrid превосходит их по безопасности, но уступает в скорости/размере (таблица).

Сравнение алгоритмов
Algorithm Comparison

Протокол/ метод	Тип подписи	Классическая безопасность	Квантовая безопасность	Использование квантовой памяти	Реализуемость	Основные ограничения
Готтсмана — Чуанга	Чисто квантовая	Нет	Да	Да (долгосрочная)	Теоретический уровень	Квантовая память недоступна; сложно масштабировать
TQDS (Threshold QDS)	Пороговая квантовая	Нет	Да	Да (временная)	Лабораторный уровень	Сложная квантовая арифметика; требует координации участников
Stateless QDS	Одноразовая квантовая	Нет	Да	Да (краткосрочная)	Экспериментальный уровень	Подпись нельзя повторно использовать; требуется высокая стабильность каналов
Dilithium (NIST)	Постквантовая классическая	Да	Да (в QROM)	Нет	Полностью реализуем сейчас	Отсутствие квантовой верификации; не защищает от физического перехвата
QDS-Hybrid (предлагаемый)	Гибридная (классико-квантовая)	Да (Dilithium)	Да (QKD + + SWAP-тест)	Нет (генерация «на лету»)	В лабораторных условиях	Высокие требования к шумоподавлению и точности гейтов
Квантовый блокчейн с QKD-узлами	Распределенная квантово-классическая	Да	Да (условно)	Нет (локальная проверка)	Перспективный формат	Требует развитой квантовой инфраструктуры и протоколов согласования

Анализ таблицы показывает, что QDS-Hybrid сочетает постквантовую защиту Dilithium и квантовую верификацию через SWAP-тест, что делает его устойчивым как к классическим, так и квантовым атакам. Для гибридного протокола не требуется долгосрочной квантовой памяти — состояние можно генерировать «по запросу». Шум и декогеренция остаются ключевыми проблемами для всех квантовых протоколов, включая QDS-Hybrid.

Заключение

Квантовые цифровые подписи представляют собой перспективное направление в криптографии, обеспечивающее безусловную безопасность благодаря фундаментальным принципам квантовой механики, таким как невозможность клонирования квантовых состояний и квантовая запутанность. В отличие от классических алгоритмов, таких как RSA и ECDSA, QDS устойчивы к атакам квантовых компьютеров, включая алгоритмы Шора и Гровера, что делает их критически важными в будущем для защиты данных. По-видимому, вопрос о полной замене классических подписей квантовыми не стоит в ближайшие 10 лет. Но гибридные решения, подобные QDS-Hybrid, являются реальным практическим путем, который можно увидеть сегодня.

Однако, несмотря на теоретическую стойкость, практическое применение QDS сталкивается с серьезными вызовами. К ним относятся технологические ограничения, такие как декогеренция кубитов, необходимость в квантовой памяти и сложность масштабирования квантовых сетей. Кроме того, существующие QDS-протоколы требуют значительных вычислительных ресурсов и специализированной инфраструктуры, что затрудняет их интеграцию в современные системы.

Гибридные подходы, сочетающие квантовые и классические методы, например, комбинацию QKD с постквантовыми алгоритмами, такими как Dilithium, предлагают компромиссное решение. Они позволяют снизить зависимость от квантовой инфраструктуры, повысить скорость работы и обеспечить обратную совместимость с существующими технологиями.

Для дальнейшего развития QDS необходимо сосредоточиться на преодолении технологических барьеров, таких как создание долговременной квантовой памяти и разработка квантовых повторителей для увеличе-

ния дальности передачи. Кроме того, важным направлением является оптимизация протоколов для уменьшения количества требуемых кубитов и упрощения их реализации на NISQ-устройствах.

QDS и гибридные схемы могут стать основой для безопасных коммуникаций в эпоху квантовых вычислений. Однако их широкое внедрение потребует не только дальнейшего изучения, но и развития соответствующей инфраструктуры, стандартов и протоколов. Успешная интеграция QDS в реальные системы позволит обеспечить защиту данных на новом уровне, не достижимом для классических методов.

Одной из перспектив развития этого направления является улучшение устойчивости к шуму и декогеренции. Для этого нужно комбинировать квантовые (QEC) и классические (LDPC, Reed-Solomon) коды для защиты $|\psi_{sk}\rangle$. Можно использовать и Machine Learning для подавления шума. Но, возможно, вместо борьбы с декогеренцией стоит сосредоточиться на «квантово-классических» гибридах, где критичные этапы выполняются на классических серверах, а квантовые компоненты используются только для верификации.

Вторым направлением может быть полная децентрализация верификации, замена арбитра на распределенную сеть валидаторов, использующих квантовые византийские соглашения (QBA) или квантовые блокчейны с smart-контрактами для голосования.

К третьему направлению можно отнести интеграцию с современной инфраструктурой: встраивание протокола в стек квантовых сетевых протоколов (например, поверх QKD), либо какие-то гибридные TLS/SSL-решения (например, замена классических цифровых подписей в TLS на QDS-Hybrid).

Важным направлением развития также является ускорение и оптимизация: снижение времени генерации/верификации подписей (например, квантовых ASIC для операций $Rz(\theta)$ и SWAP-теста). Оптимизация может состоять из квантового сжатия данных с помощью использования квантовых автоэнкодеров и эффективных кодировок, амплитудного кодирования.

Последним направлением может быть расширение функциональности за счет использования многоразовых квантовых подписей и подписей для квантовых сообщений.

Разработка этих направлений позволит перейти от теоретической модели к практическому внедрению в квантовые и классические системы.

Список источников

1. *Gottesman D., Chuang I.* Quantum Digital Signatures // arXiv:quant-ph/0105032v2. 2001. DOI: 10.48550/arXiv.quant-ph/0105032 (дата обращения: 25.04.2025).

2. *Cao Z.* A Note On Gottesman-Chuang Quantum Signature Scheme. Penn State University, 2010. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=8f1ef45fe04efd373346ac4b9dca75b078399680 (дата обращения: 25.04.2025).

3. *Аблаев Ф. М., Аблаев М. Ф., Васильев А. В.* Универсальное квантовое хеширование // Ученые записки Казанского университета. Серия: Физико-математические науки. 2014. Т. 156, № 3. С. 7—18.

4. *Childs A. M.* Secure assisted quantum computation // arXiv:quant-ph/0111046v1. 2001. DOI: 10.48550/arXiv.quant-ph/0111046 (дата обращения: 25.04.2025).

5. *Смирнова А. А., Тискин А. Ф.* Анализ криптографических свойств отечественных хэш-алгоритмов // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2014. Т. 12, № 2. С. 102—111. DOI: 10.25205/1684-599X-2014-12-2-102-111

6. *Батенко К. Е., Прокудин А. Н.* Пост-квантовый алгоритм электронно-цифровой подписи на основе дерева Меркла и ГОСТ РФ 34.11–12 «Стрибог» // Молодой ученый. 2017. № 23 (157). С. 100—103. URL: https://moluch.ru/archive/157/44376/ (дата обращения: 25.04.2025).

7. *Merkle R. C.* Secure communications over insecure channels // Communications of the ACM. 1978. Vol. 21, no. 4. P. 294—299. DOI: 10.1145/359460.359473

8. *Bennett C. H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Proceedings of International Conference on Computers, Systems & Signal Processing (Bangalore, India, Dec. 9—12, 1984). IEEE, 1984. P. 175.

9. *Realization* of a scalable Shor algorithm / T. Monz et al. // Science. 2016. Vol. 351, is. 6277. P. 1068—1070. DOI: 10.1126/science.aad9480

10. *The universal* composable security of quantum key distribution / M. Ben-Or et al. // arXiv:quant-ph/0409078v2. 2005. URL: https://arxiv.org/abs/quant-ph/0409078 (дата обращения: 25.04.2025).

11. *Kitaev A. Yu.* Quantum computations: algorithms and error correction // Russian Mathematical Surveys. 1997. Vol. 52, no. 6. P. 1191—1249. DOI: 10.1070/RM1997v052n06ABEH002155

12. *Shor Peter W., Preskill John.* Simple Proof of Security of the BB84 Quantum Key Distribution Protocol // Physical Review Letters. 2000. Vol. 85, no. 1. P. 441. DOI: 10.1103/PhysRevLett.85.441

13. *Quantum* Fingerprinting / Harry Buhrman et al. // Physical Review Letters. 2001. Vol. 87, no. 16. Article 167902. DOI: 10.1103/PhysRevLett.87.167902. URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.87.167902 (дата обращения: 25.04.2025).

14. *Shor Peter W.* Scheme for reducing decoherence in quantum computer memory // Physical Review A. 1995. Vol. 52, is. 4. P. R2493—R2496. DOI: 10.1103/PhysRevA.52.R2493

15. *Canetti Ran, Krawczyk Hugo.* Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels // Advances in Cryptology — EUROCRYPT 2001. Lecture Notes in Computer Science. Vol. 2045. 2001. Springer ; Berlin ; Heidelberg, 2001. DOI: 10.1007/3-540-44987-6_8

16. *Efficient* diagnostics for quantum error correction / Iyer Pavithran et al. // Physical Review Research. 2022. Vol. 4. Article 043218. DOI: 10.1103/PhysRevResearch.4.043218

17. *Бибиков С. А.* Квантовая телепортация и запутанные состояния // Вестник Новосибирского государственного университета. Серия: Физика. 2021. Т. 16, № 3. С. 45—52. DOI: 10.25205/1818-4373-2021-16-3-45-52

18. *Milekhin Alexey.* Quantum error correction and large N // SciPost Physics. 2021. Vol. 11, no. 5. Article 094. DOI: 10.21468/SciPostPhys.11.5.094

19. *Crépeau Claude, Gottesman Daniel, Smith Adam.* Secure Multi-Party Quantum Computation // Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing. STOC '02. Association for Computing Machinery, New York, USA. P. 643—652. DOI: 10.1145/509907.509992

20. *Петренко А. С., Петренко С. А.* Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. 2022. № 3 (49). URL: https://cyberrus.info/wp-content/uploads/2022/07/2-22-349-22_1.-Petrenko.pdf (дата обращения: 25.04.2025).

21. *Ekert Artur K.* Quantum cryptography based on Bell's theorem // Physical Review Letters. 1991. Vol. 67, no. 6. P. 661. DOI: 10.1103/PhysRevLett.67.661

22. *Sahai Amit, Waters Brent.* Fuzzy Identity-Based Encryption // EUROCRYPT 2005. LNCS. Vol. 3494. Springer, Berlin, Heidelberg. P. 457—473. DOI: 10.1007/11426639_27

23. *Shamir Adi.* How to Share a Big Secret // Proceedings of the 11th ACM International Systems and Storage Conference (SYSTOR '18). Haifa, Israel. ACM, New York, USA. P. 76—88. DOI: 10.1145/3211890.3211896

24. *Il'in N. S., Aristova A. V., Lychkovskiy O.* Adiabatic theorem for closed quantum systems initialized at finite temperature // Physical Review A. 2021. Vol. 104. Article L030202. DOI: 10.1103/PhysRevA.104.L030202 (дата обращения: 25.04.2025).

25. *Принципы* проектирования протоколов распределения ключей для квантовых сетей с доверенными узлами. URL: https://article/n/printsipy-proektirovaniya-setevyh-protokolov-raspredeleniya-klyuchey-dlya-kvantovyh-setey (дата обращения: 25.04.2025).

26. *Береснева А. В., Епишкина А. В.* О применении криптографических примитивов, реализующих пороговую подпись // Безопасность информационных технологий. 2015. Т. 22, № 3.

27. *Разбор* структуры и принципов работы современных потоковых шифров, включая динамическое тактирование регистров сдвига (пример A5 в GSM). URL: https://studfile.net/preview/6022635/1 (дата обращения: 25.04.2025).

28. *Bellare M., Rogaway P.* Entity Authentication and Key Distribution // Advances in Cryptology — EUROCRYPT'93. LNCS. Vol. 765. Berlin, Heidelberg. DOI: 10.1007/3-540-48285-7_24

29. *Goldwasser S., Micali S., Rackoff C.* The Knowledge Complexity of Interactive Proof-Systems // SIAM Journal on Computing. 1989. Vol. 18, no. 1. P. 186—208. DOI: 10.1137/0218012

30. *Page Don N., Wootters William K.* Evolution without evolution: Dynamics described by stationary observables // Physical Review D. 1983. Vol. 27, no. 12. P. 2885. DOI: 10.1103/PhysRevD.27.2885

31. *Bennett Charles H., Brassard Gilles.* Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers, Systems & Signal Processing (Bangalore, India, Dec. 9—12, 1984). IEEE, 1984. P. 175.

32. *Shor Peter W., Preskill John.* Simple Proof of Security of the BB84 Quantum Key Distribution Protocol // Phys. Rev. Lett. 2000. Vol. 85, no. 1. P. 441. DOI: 10.1103/PhysRevLett.85.441

33. *Long-distance* continuous-variable quantum digital signatures over 120-km fiber / Y. Zhang et al. // Optics Express. 2021. Vol. 29, is. 23. P. 37614—37627. DOI: 10.1364/OE.438605. URL: https://opg.optica.org/oe/fulltext.cfm?uri=oe-29-23-37614&id=462809 (дата обращения: 25.04.2025).

References

1. Gottesman D., Chuang I. Quantum Digital Signatures, *arXiv:quant-ph/0105032v2*, 2001. DOI: 10.48550/arXiv.quant-ph/0105032 (accessed: 25.04.2025).

2. Cao Z. A Note On Gottesman-Chuang Quantum Signature Scheme. Penn State University, 2010. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=8f1ef45fe04efd373346ac4b9dca75b078399680 (accessed: 25.04.2025).

3. Ablayev F.M., Ablayev M.F., Vasilyev A.V. Universalnoye kvantovoye kheshirovaniye [Universal quantum hashing], Uchenyye zapiski Kazanskogo universiteta. Seriya: Fiziko-matematicheskiye nauki [Scientific Notes of Kazan University. Series: Physical and Mathematical Sciences], 2014, vol. 156, no. 3, pp. 7–18.

4. Childs A.M. Secure assisted quantum computation, *arXiv:quant-ph/0111046v1*, 2001. DOI: 10.48550/arXiv.quant-ph/0111046 (accessed: 25.04.2025).

5. Smirnova A.A., Tiskin A.F. Analiz kriptograficheskikh svoystv otechestvennykh khesh-algoritmov [Analysis of cryptographic properties of domestic hash algorithms], *Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Informatsionnyye tekhnologii* [Bulletin of Novosibirsk State University. Series: Information Technology], 2014, vol. 12, no. 2, pp. 102–111. DOI: 10.25205/1684-599X-2014-12-2-102-111

6. Batenko K.E., Prokudin A.N. Post-kvantovyy algoritm elektronno-tsifrovoy podpisi na osnove dereva Merkla i GOST RF 34.11–12 “Stribog” [Post-quantum digital signature algorithm based on the Merkle tree and GOST RF 34.11-12 “Stribog”], Molodoy uchenyy [Young Scientist], 2017, no. 23 (157), pp. 100–103. Available at: https://moluch.ru/archive/157/44376/ (accessed: 25.04.2025).

7. Merkle R.C. Secure communications over insecure channels, *Communications of the ACM*, 1978, vol. 21, no. 4, pp. 294–299. DOI: 10.1145/359460.359473

8. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing, *Proceedings of International Conference on Computers, Systems & Signal Processing (Bangalore, India, December 9–12, 1984)*. IEEE, 1984, p. 175.

9. Monz T. et al. Realization of a scalable Shor algorithm, *Science*, 2016, vol. 351, is. 6277, pp. 1068–1070. DOI: 10.1126/science.aad9480

10. Ben-Or M. et al. The universal composable security of quantum key distribution, *arXiv:quant-ph/0409078v*2, 2005. Available at: https://arxiv.org/abs/quant-ph/0409078 (accessed: 25.04.2025).

11. Kitaev A.Yu. Quantum computations: algorithms and error correction, *Russian Mathematical Surveys*, 1997, vol. 52, no. 6, pp. 1191–1249. DOI: 10.1070/RM1997v052n06ABEH002155

12. Shor Peter W., Preskill John. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Physical Review Letter*, 2000, vol. 85, no. 1, p. 441. DOI: 10.1103/PhysRevLett.85.441

13. Harry Buhrman et al. Quantum Fingerprinting, *Physical Review Letters*, 2001, vol. 87, no. 16. Article 167902. DOI: 10.1103/PhysRevLett.87.167902. Available at: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.87.167902 (accessed: 25.04.2025).

14. Shor Peter W. Scheme for reducing decoherence in quantum computer memory, *Physical Review* A, 1995, vol. 52, is. 4, pp. R2493–R2496. DOI: 10.1103/PhysRevA.52.R2493

15. Canetti Ran, Krawczyk Hugo. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels, *Advances in Cryptology – EUROCRYPT 2001. Lecture Notes in Computer Science*, vol. 2045, 2001, Springer. Berlin, Heidelberg, 2001. DOI: 10.1007/3-540-44987-6_8

16. Iyer Pavithran et al. Efficient diagnostics for quantum error correction, *Physical Review Research*, 2022, vol. 4, article 043218. DOI: 10.1103/PhysRevResearch.4.043218

17. Bibikov S.A. Kvantovaya teleportatsiya i zaputannyye sostoyaniya [Quantum teleportation and entangled states], *Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Fizika* [Bulletin of Novosibirsk State University. Series: Physics], 2021, vol. 16, no. 3, pp. 45–52. DOI: 10.25205/1818-4373-2021-16-3-45-52

18. Milekhin Alexey. Quantum error correction and large N, *SciPost Physics*, 2021, vol. 11, no. 5. Article 094. DOI: 10.21468/SciPostPhys.11.5.094

19. Crépeau Claude, Gottesman Daniel, Smith Adam. Secure Multi-Party Quantum Computation, *Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing. STOC '02. Association for Computing Machinery*. New York, USA, pp. 643–652. DOI: 10.1145/509907.509992

20. Petrenko A.S., Petrenko S.A. Metod otsenivaniya kvantovoy ustoychivosti blokcheyn-platform [A Method for Assessing the Quantum Resilience of Blockchain Platforms], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2022, no. 3 (49). Available at: https://cyberrus.info/wp-content/uploads/2022/07/2-22-349-22_1.-Petrenko.pdf (accessed: 25.04.2025).

21. Ekert Artur K. Quantum cryptography based on Bell’s theorem, *Physical Review Letter*, 1991, vol. 67, no. 6, p. 661. DOI: 10.1103/PhysRevLett.67.661

22. Sahai Amit, Waters Brent. Fuzzy Identity-Based Encryption, *EUROCRYPT*, 2005. LNCS, vol. 3494, Springer. Berlin, Heidelberg, pp. 457–473. DOI: 10.1007/11426639_27

23. Shamir Adi. How to Share a Big Secret, *Proceedings of the 11th ACM International Systems and Storage Conference* (SYSTOR ’18). Haifa, Israel. ACM, New York, USA, pp. 76–88. DOI: 10.1145/3211890.3211896

24. Il’in N.S., Aristova A.V., Lychkovskiy O. Adiabatic theorem for closed quantum systems initialized at finite temperature, *Physical Review A*, 2021, vol. 104. Article L030202. DOI: 10.1103/PhysRevA.104.L030202 (accessed: 25.04.2025).

25. *Printsipy proyektirovaniya protokolov raspredeleniya klyuchey dlya kvantovykh setey s doverennymi uzlami* [Design Principles of Key Distribution Protocols for Quantum Networks with Trusted Nodes]. Available at: https://article/n/printsipy-proektirovaniya-setevyh-protokolov-raspredeleniya-klyuchey-dlya-kvantovyh-setey (accessed: 25.04.2025).

26. Beresneva A.V., Yepishkina A.V. O primenenii kriptograficheskikh primitivov, realizuyushchikh porogovuyu podpis [On the application of cryptographic primitives implementing a threshold signature], *Bezopasnost informatsionnykh tekhnologiy* [Information Technology Security], 2015, vol. 22, no. 3.

27. *Razbor struktury i printsipov raboty sovremennykh potokovykh shifrov, vklyuchaya dinamicheskoye taktirovaniye registrov sdviga (primer A5 v GSM)* [An analysis of the structure and operating principles of modern stream ciphers, including dynamic clocking of shift registers (example A5 in GSM)]. Available at: https://studfile.net/preview/6022635/1 (accessed: 25.04.2025).

28. Bellare M., Rogaway P. Entity Authentication and Key Distribution, Advances in Cryptology – EUROCRYPT'93, *LNCS*, vol. 765. Berlin, Heidelberg. DOI: 10.1007/3-540-48285-7_24

29. Goldwasser S., Micali S., Rackoff C. The Knowledge Complexity of Interactive Proof-Systems, *SIAM Journal on Computing*, 1989, vol. 18, no. 1, pp. 186–208. DOI: 10.1137/0218012

30. Page Don N., Wootters William K. Evolution without evolution: Dynamics described by stationary observables, *Physical Review* D, 1983, vol. 27, no. 12, p. 2885. DOI: 10.1103/PhysRevD.27.2885

31. Bennett Charles H., Brassard Gilles. Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems & Signal Processing (Bangalore, India, December 9–12, 1984)*. IEEE, 1984, p. 175.

32. Shor Peter W., Preskill John. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Physical Review* Letter, 2000, vol. 85, no. 1, p. 441. DOI: 10.1103/PhysRevLett.85.441

33. Zhang Y. et al. Long-distance continuous-variable quantum digital signatures over 120-km fiber, *Optics Express*, 2021, vol. 29, is. 23, pp. 37614–37627. DOI: 10.1364/OE.438605. Available at: https://opg.optica.org/oe/fulltext.cfm?uri=oe-29-23-37614&id=462809 (accessed: 25.04.2025).

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 Physical and Mathematical Sciences, 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 09.06.2025; одобрена после рецензирования 01.10.2025; принята к публикации 10.10.2025.
The article was submitted 09.06.2025; approved after reviewing 01.10.2025; accepted for publication 10.10.2025.