Информационные процессы, Том 25, № 2, 2025, стр. 132–141.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Квантовое распределение ключей в мобильных сетях: современные подходы и перспективы[1]

П. Ю. Вацков*, Е. М. Маврин*, В. Г. Потапов, П. В. Че***

**Сколковский институт науки и технологий, Москва*

***Институт проблем передачи информации им. А.А. Харкевича Российской академии наук, Москва*

Поступила в редколлегию 7.07.2025 г. Принята 25.07.2025 г.

Аннотация—В условиях стремительного роста угроз информационной безопасности, обусловленных как увеличением вычислительных мощностей классических компьютеров, так и перспективами появления квантовых вычислительных систем, традиционные криптографические методы утрачивают свою долгосрочную надёжность. На этом фоне технологии квантовой криптографии, в частности квантового распределения ключей (КРК), становятся важным инструментом обеспечения физически обоснованной безопасности данных. В данной работе проводится всесторонний анализ возможностей автономного применения КРК в мобильных сетях связи 4G/5G, включая аспекты практической реализации и потенциальные ограничения. Кроме того, рассматриваются сценарии интеграции постквантовой криптографии и КРК как взаимодополняющих подходов к защите пользовательских данных, а также перспективы построения защищённой инфраструктуры на основе VPN и квантового распределения ключей. Особое внимание уделено сопоставлению международного и отечественного опыта в данной области, а также анализу применимости указанных технологий в реальных мобильных сетях.

КЛЮЧЕВЫЕ СЛОВА: квантовое распределение ключей (КРК), мобильные сети 4G/5G, квантовая криптография, защищённые каналы связи.

DOI: 10.53921/18195822_2025_25_2_132

1. ВВЕДЕНИЕ

Появление квантовых компьютеров ставит под угрозу обычные криптографические системы, применяемые в современных телекоммуникационных сетях. Квантовые алгоритмы, в частности алгоритм Шора, способны за полиномиальное время взламывать широко используемые схемы шифрования, основанные на математических задачах, которые сложно решить в одном направлении, но легко обратить при наличии дополнительной информации. Это особенно критично для сетей четвёртого и пятого поколений (4G/5G), рассчитанных на поддержку приложений повышенной важности, таких как системы управления инфраструктурой, здравоохранение и промышленная автоматизация.

Квантовое распределение ключей (КРК) является одной из наиболее перспективных технологий в области квантовой криптографии, предоставляя безусловно безопасный механизм обмена ключами шифрования, гарантированный фундаментальными законами квантовой физики. В рамках КРК любая попытка перехвата квантовых состояний фотонов неизбежно приводит к возникновению детектируемых возмущений. Это позволяет участникам связи немедленно обнаруживать попытки несанкционированного доступа. Благодаря этим уникальным свойствам КРК становится привлекательным дополнением к традиционным средствам защиты данных, особенно в эпоху сетей 5G, предъявляющих повышенные требования к безопасности.

[1] Работа выполнена при поддержке ОАО "Российские железные дороги"

В данной работе рассматриваются современные подходы к внедрению КРК в мобильных сетях 4G/5G, а также анализируются технические и инфраструктурные вызовы, возникающие в процессе его реализации. Проводится сравнительный анализ основных протоколов КРК. Также обсуждаются перспективы развития КРК и его потенциальная роль в формировании защищённой инфраструктуры будущего.

2. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И ПРЕДПОСЫЛКИ РАЗВИТИЯ КК

Криптография – это наука о защите информации, основанная на преобразовании данных (шифровании) между доверенными участниками с целью предотвращения несанкционированного доступа. В центре любого криптоалгоритма лежит криптографический ключ — секретная последовательность бит. Традиционно выделяют два основных подхода.

Первый подход – симметричное шифрование, при котором отправитель (Алиса) и получатель (Боб) используют один и тот же секретный ключ для выполнения операций шифрования и дешифрования данных (Рис. 1). Данный подход сталкивается с рядом существенных ограничений. Во-первых, безопасная передача ключа между участниками связи требует предварительного обмена по защищённому каналу, что создаёт дополнительные сложности в условиях реальных телекоммуникационных сетей. Во-вторых, компрометация ключа приводит к критическим последствиям, поскольку злоумышленник получает доступ ко всем данным, зашифрованным с его использованием. В-третьих, симметричное шифрование подвержено атакам полного перебора, что делает необходимым использование ключей достаточной длины для противодействия современным и будущим вычислительным мощностям, включая потенциал квантовых компьютеров [1]. Несмотря на указанные ограничения, симметричное шифрование обладает значительными преимуществами, делающими его широко применимым в практических задачах. К ним относятся высокая скорость выполнения операций шифрования и дешифрования, а также минимальные требования к вычислительным ресурсам. Эти характеристики особенно важны в контексте работы с большими объёмами данных и в условиях ограниченных вычислительных мощностей.

Рис. 1. Процесс симметричного шифрования

Рис. 2. Процесс асимметричного шифрования

Второй подход – асимметричное шифрование (криптография с открытым ключом), использующее пару математически связанных ключей (Рис. 2). Открытый ключ, предназначенный для шифрования данных, может быть свободно распространён среди всех участников связи, тогда как закрытый ключ, необходимый для дешифрования, хранится в секрете его владельцем. Несмотря на значительные преимущества, данный метод сталкивается с рядом существенных ограничений. Во-первых, асимметричные схемы уязвимы к атакам со стороны квантовых

компьютеров. Например, алгоритм Шора, выполненный на достаточно мощном квантовом компьютере, способен решать задачи, лежащие в основе безопасности таких систем, за полиномиальное время [2]. Это делает классические асимметричные алгоритмы, такие как алгоритм Ривеста–Шамира–Адлемана (Rivest–Shamir–Adleman, RSA), основанный на задаче факторизации больших чисел, и криптография на эллиптических кривых (Elliptic Curve Cryptography, ECC), опирающаяся на вычислительную сложность дискретного логарифма, небезопасными в условиях постквантовой эпохи [3]. Во-вторых, асимметричное шифрование характеризуется более высокой вычислительной сложностью по сравнению с симметричным, что ограничивает его применимость в сценариях с большими объёмами данных. Ключевыми преимуществами асимметричного шифрования являются отсутствие необходимости предварительного обмена секретными ключами (открытый ключ можно свободно распространять) и возможность реализации цифровых подписей, обеспечивающих аутентификацию и целостность данных.

Гибридное шифрование сочетает сильные стороны симметричных и асимметричных схем: асимметричное шифрование обеспечивает безопасную доставку случайно сгенерированного сеансового симметричного ключа, а сам симметричный ключ используется для эффективного шифрования основного объёма данных.

Появление угрозы со стороны квантовых компьютеров спровоцировало два взаимодополняющих направления развития криптографии. Первое из них – постквантовая криптография (ПКК). ПКК разрабатывает новые алгоритмы в рамках классической криптографии, устойчивые как к классическим, так к квантовым атакам. Безопасность этих схем базируется на задачах, для которых пока не найдены эффективные квантовые алгоритмы: декодирование случайных линейных кодов (Code-Based), поиск кратчайшего вектора в решётке (Lattice-Based), решение многовариантных квадратичных уравнений (Multivariate), построение хэш-цепочек (Hash-Based) и суперсингулярная изогения эллиптических кривых (Isogeny-Based) [4]. NIST уже завершает стандартизацию ряда таких алгоритмов [5]. Второе направление – квантовая криптография и КРК. В отличие от традиционных методов, КРК обеспечивает физически гарантированную секретность передачи симметричных ключей между удалёнными узлами, т.к. любое вмешательство в квантовый канал неизбежно приводит к возникновению детектируемых возмущений благодаря принципу неопределённости Гейзенберга, теореме о запрете клонирования и коллапсу волновой функции.

Ключевая проблема традиционных методов криптографии заключается в том, что независимо от стойкости самого алгоритма остаётся уязвимость на уровне доставки ключей: в симметричных схемах требуется заранее безопасно передать секретный ключ, а в асимметричных – доверять открытым ключам, что делает их уязвимыми к атакам “человек посередине”. Именно для решения этой базовой задачи – безопасного распределения симметричных ключей – и была разработана технология КРК.

3. ПРИНЦИПЫ РАБОТЫ КРК

В отличие от классической криптографии, КРК использует два канала связи (Рис. 3): квантовый канал для передачи информации, закодированной в квантовых состояниях одиночных фотонов (например, поляризация, фаза), и классический (открытый) канал для передачи служебной информации, необходимой для обработки данных, полученных по квантовому каналу, и обнаружения подслушивания.

Физическая основа безопасности КРК включает три фундаментальных принципа квантовой механики: принцип неопределенности Гейзенберга (невозможно одновременно точно измерить две взаимодополняющие характеристики квантовой системы); теорему о запрете клонирования (невозможно создать точную копию произвольного неизвестного квантового состояния);

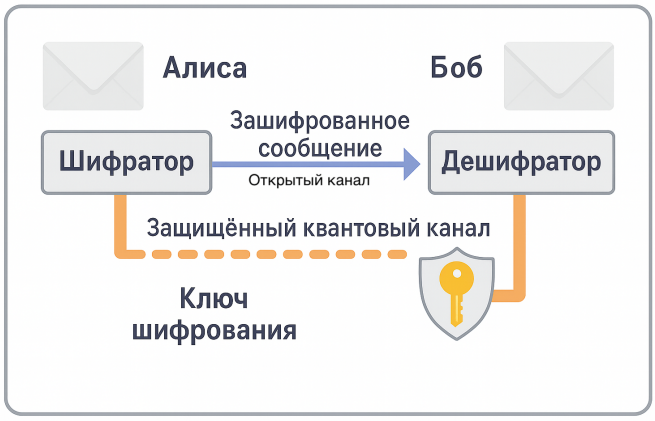

Рис. 3. Схема квантового распределения ключей

коллапс волновой функции (измерение квантовой системы приводит к необратимому коллапсу ее состояния).

Чтобы наглядно продемонстрировать, как эти законы используются для распределения ключей, обычно приводят протокол BB84 (Беннетта–Брассара, 1984) [6]. Он служит “эталоном” КРК: в нём отправитель (Алиса) случайным образом кодирует биты на фотонах, выбирая между двумя взаимодополняющими базисами, а получатель (Боб) измеряет их, тоже случайно выбирая базис. По классическому каналу они сверяют свои измерения и отбрасывают несовпавшие попытки, затем корректируют ошибки и проводят усиление секретности. В результате любая попытка подслушивания (измерения фотонов злоумышленником) приводит к росту доли ошибок и быстро обнаруживается, что и делает BB84 простым, но наглядным примером гарантированной квантовой безопасности.

Существует два подхода к реализации протоколов квантового распределения ключей. В протоколах с дискретными переменными информация кодируется в отдельно посланных фотонах — например, в их поляризации или фазе — и извлекается при помощи одноквантовых детекторов. Протоколы с непрерывными переменными используют непрерывные параметры светового поля (квадратуры амплитуды и фазы) и гомодинное детектирование, что позволяет добиться более высокой скорости генерации ключей [7, 8].

Передача квантовых сигналов возможна как по оптоволокну, так и в свободном пространстве (беспроводной канал). Оптоволоконные линии хорошо защищены от помех, но ограничены дальностью в 200–500 км без повторителей (до 1000 км в экспериментальных системах). Беспроводные квантовые каналы, организуемые с помощью компактных оптических генераторов и фотодетекторов, теоретически не имеют таких географических ограничений, однако в городских условиях им мешают атмосферные и метеоусловия.

Для “чистой” КРК требуются специализированные компоненты: квантовый передатчик (лазерный источник и модулятор), приёмник (фотонные детекторы) и сам квантовый канал (волоконный или воздушный). Главные технические вызовы здесь – ограниченная дальность и низкая скорость генерации ключей (от сотен бит в секунду до единиц мегабит), высокая стоимость оборудования, сложность интеграции с существующей сетевой инфраструктурой и точечная архитектура “точка–точка”, требующая развёртывания большого числа отдельных линков для покрытия широкой географии [9–13].

4. ВОЗМОЖНОСТИ АВТОНОМНОГО ПРИМЕНЕНИЯ ТЕХНОЛОГИИ КРК В МОБИЛЬНЫХ СЕТЯХ СВЯЗИ

В сетях 4G/5G ключевую роль играет иерархия криптографических ключей: в абонентском устройстве (UE) на USIM хранится долговременный ключ K, сеть радиодоступа (RAN) обеспечивает передачу, а в ядре (AMF, SEAF, AUSF, UDM, ARPF) происходит аутентификация и генерация рабочих ключей (например, K_{gNB}, K_{NAS}, K_{UP}) в рамках процедуры 5G-AKA. При этом классические методы защиты остаются уязвимы к квантовым атакам на шифрование SUCI (ECIES), компрометации долгосрочного ключа, атакам “человек посередине” через фальшивые базовые станции, а также к реализационным уязвимостям и несанкционированной слежке за абонентами.

Для устранения этих слабых мест технология КРК может быть внедрена автономно на трёх уровнях. Во-первых, КРК позволяет безопасно доставлять или периодически обновлять долговременный ключ K между элементами ядра (UDM/ARPF) и доверенными аппаратными модулями HSM, исключая риск перехвата через классический канал связи. Во-вторых, с её помощью можно распределять сеансовые ключи управления между узлами ядра и RAN – это повысит надёжность процедур установления защищённого канала в 5G-AKA. И, наконец, КРК даёт возможность организовать полноценное сквозное шифрование пользовательских данных: симметричные сессионные ключи генерируются по квантовому каналу между доверенными шлюзами SDE, что обеспечивает end-to-end защиту трафика без необходимости доверять оператору сети. В совокупности эти решения снимут критическую уязвимость, связанную с безопасной доставкой ключей, и выведут уровень защищённости мобильных сетей на новый физически обоснованный уровень, гарантированный фундаментальными законами квантовой физики.

4.1. Мировой опыт интеграции КРК в мобильные сети

В Китае компании QuantumCTek совместно с China Telecom и China Mobile разработали квантовую SIM-карту с встроенным чипом безопасности. Архитектура решения включает централизованную систему управления ключами, доверенные зоны и безопасную загрузку новых ключей в офисах оператора. Для установки защищённого вызова используется пара заранее записанных секретных ключей: один — для аутентификации, второй — для шифрования. Плюсы такого подхода — сквозное шифрование и абсолютная секретность ключей; минусы — необходимость личного визита абонента в офис для обновления ключей и ограничение рамками одной сети оператора. Одним из примеров реализации стала модель *Tianyi No. 1* (2022) [23], а также платформа QSS-ME [24].

Другой подход предложили SK Telecom, Samsung и ID Quantique, встроив в смартфон *Galaxy A Quantum* квантовый генератор истинно случайных чисел (QRNG). Позднее модель эволюционировала до *Galaxy Quantum 5* (2024) [25]. Чип генерирует энтропийные данные на основе квантовых флуктуаций, что повышает стойкость создаваемых на устройстве криптографических ключей без изменений в сетевой инфраструктуре. Однако этот метод не обеспечивает распределение ключей между абонентами.

В России над интеграцией квантовых технологий работают Воентелеком и Росэлектроника. Воентелеком выпускает защищённые USIM-карты с отечественными криптоалгоритмами и планирует доставку мастер-ключей в аппаратные модули HSM. Компания Росэлектроника разработала приложение «Колибри-SIP» для защищённой IP-телефонии на ОС «Аврора», которое может стать клиентским интерфейсом для получения и управления ключами КРК и ПКК.

4.2. Проблемы и перспективы автономного применения КРК для сквозного шифрования в 4G/5G

Автономное применение КРК для прямой генерации секретного ключа между удаленными оконечными устройствами сталкивается с фундаментальными проблемами. Аппаратная реализация на абонентском оборудовании затруднена из-за требований к размеру, энергопотреблению и стоимости компонентов, особенно детекторов фотонов. Обеспечение прямого квантового канала между мобильными устройствами в городских условиях без прямой видимости практически невозможно из-за атмосферных помех. Скорость генерации ключа была бы крайне низкой (единицы бит/с), а дальность – ограниченной (метры). Организация управления ключами и синхронизации между устройствами через ненадежные каналы сложна, а массовое внедрение требует решения проблем масштабируемости.

Практические гибридные подходы включают четыре основных направления. Архитектура с доверенными шлюзами оператора использует КРК между шлюзами для генерации ключей сквозного шифрования, что решает проблему интеграции на UE, но требует доверия к оператору. Модель квантовой SIM (QuantumCTek) обеспечивает сквозное шифрование через предзагруженные ключи, но требует инфраструктуры записи ключей. Спутниковое КРК перспективно для мобильных платформ спецназначения с глобальным охватом, но отличается высокой стоимостью. Интеграция QRNG в UE (Samsung/SKT) улучшает локальную безопасность, но не решает проблему распределения ключей.

5. ИНТЕГРАЦИЯ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ И КРК В МОБИЛЬНЫХ СЕТЯХ

Прямое использование симметричной криптосистемы с ключами, распределенными по квантовому каналу, в масштабных 4G/5G-сетях сталкивается с серьезными сложностями: с ростом числа абонентов количество парных ключей увеличивается комбинаторно, что требует очень надёжной и масштабируемой инфраструктуры управления ключами. Кроме того, встроенные в текущие сети механизмы шифрования глубоко интегрированы в архитектуру, поэтому их модернизация связана с высокими затратами и длительным внедрением.

В то же время анализ мирового и отечественного опыта показывает, что комбинированное применение постквантовых алгоритмов (ПКК) и КРК может решить эти проблемы. В работе [14] продемонстрировали, что использование PKI на основе алгоритмов ПКК для аутентификации участников квантового протокола позволяет каждому узлу иметь лишь один сертификат от центра сертификации. Это избавляет от необходимости предварительного обмена симметричными ключами между всеми парами участников, упрощает процедуру аутентификации и снижает нагрузку на систему управления ключами, тогда как сама передача симметричных сессионных ключей по квантовому каналу сохраняет физическую надёжность распределения.

Гибридные схемы находят применение в следующих сценариях:

- аутентификация между сегментами распределённой квантовой сети;
- защита беспроводного сегмента доступа к ключевым данным;
- противодействие атакам “человек посередине” благодаря аутентификации на базе ПКК и физической защите КРК [15, 16].

В недавних работах внимание сосредоточено на конкретных архитектурах и протоколах. В работе [17] предложили энергоэффективную мобильную платформу, где ПКК отвечает за аутентификацию и управление сертификатами, а КРК — за физически защищённое распределение симметричных ключей. А авторы [18] разработали протокол Onion Routing Relay (ORR),

который позволяет безопасно передавать ключи через промежуточные узлы с помощью ПКК, а сам обмен секретами между “крайними” узлами реализуется по квантовому каналу.

Первый практический опыт гибридных систем уже есть: в мае 2025 г. China Telecom организовала 1000-километровый защищённый голосовой звонок, объединив КРК и алгоритмы постквантового шифрования [19]. А на выставке MWC’25 Vodafone и IBM представили пилотный проект по внедрению решений Quantum Safe в инфраструктуру мобильной связи [20].

Хотя применение ПКК требует дополнительных вычислительных ресурсов для криптографических операций, гибридный подход позволяет существенно сократить число пар ключей и повысить общую надёжность. В результате совместная интеграция КРК и ПКК становится перспективным направлением для создания мобильных сетей, устойчивых к современным и будущим квантовым угрозам: физически защищённое распределение ключей сочетается здесь с надёжной аутентификацией и гибкой системой управления сертификатами.

6. ИНТЕГРАЦИЯ VPN И КВАНТОВОЙ РАСПРЕДЕЛЁННОЙ КЛЮЧЕВОЙ ИНФРАСТРУКТУРЫ В МОБИЛЬНЫХ СЕТЯХ

Организация защищённого канала связи в открытых мобильных сетях представляет собой одну из приоритетных задач современной информационной безопасности. Технология виртуальных частных сетей (VPN, Virtual Private Network) позволяет создать поверх недоверенной инфраструктуры зашифрованный туннель, внутри которого весь сетевой трафик инкапсулируется и шифруется с использованием симметричных (например, AES, ChaCha20) либо асимметричных (RSA, алгоритмы на основе эллиптических кривых) криптографических алгоритмов. Однако традиционные методы обмена ключами, включая протокол Диффи Хеллмана, RSA и их постквантовые аналоги, сталкиваются с возрастающей угрозой, обусловленной развитием квантовых вычислений.

В качестве стандартных реализаций VPN в современных сетях чаще всего применяются PPTP (Point-to-Point Tunneling Protocol), отличающийся низкими вычислительными затратами и 128-битным шифрованием, L2TP/IPsec (Layer 2 Tunneling Protocol в сочетании с Internet Protocol Security), обеспечивающий расширенную аутентификацию, контроль целостности и обмен ключами по протоколу IKE (Internet Key Exchange), а также OpenVPN, основанный на SSL/TLS и использующий библиотеку OpenSSL для гибкого выбора алгоритмов шифрования и аутентификации.

Мобильные сети четвёртого и пятого поколений (4G/LTE и 5G NR) предъявляют особые требования к надёжности VPN-соединений: потери и переуправление пакетов при переходе между базовыми станциями делают необходимым использование stateless-шифрования, когда каждый пакет содержит всю информацию для расшифровки, или stateful-режима, при котором важно сохранять состояние сеанса и ключи между последовательными пакетами. В IPsec для 4G/5G обычно используется stateless-шифрование с асимметричным обменом ключами, что повышает устойчивость к потере пакетов, но остаётся уязвимым к квантовым атакам.

КРК позволяет генерировать абсолютно секретные ключи на основе квантово-механических свойств фотонов и обнаруживать любое вмешательство злоумышленника. Интеграция КРК в протокол IKE вместо классических схем Диффи-Хеллмана обеспечивает абсолютную криптографическую стойкость: любая попытка перехвата квантовых состояний моментально нарушает их, и обе стороны получают уведомление об атаке.

Практические эксперименты демонстрируют жизнеспособность данного подхода. Так, в 2014 году была развернута защищённая линия VPN между AGH University of Science and Technology (Польша) и VSB – Technical University of Ostrava (Чехия), где для обмена ключами применялась система КРК и протокол ISAKMP (Internet Security Association and Key Management Protocol) [21]. В Китае в 2017 году канал между городами Хэфэй и Ухань исполь-

зовал КРК для постоянной генерации VPN-ключей на основе OpenVPN [22]. Коммерческие решения на базе FortiGate с интеграцией КРК-устройств Cerebris (IDQ) через открытый API продемонстрировали готовность отрасли к массовому внедрению. Аналогичным образом проект QRate совместно с Университетом Иннополис в России обеспечил защиту канала 4G между беспилотником и центром обработки данных, используя OpenVPN поверх квантового канала. Недавние исследования 2024 года подтвердили эффективность КРК в реальных условиях сетей 4G/5G для защиты VPN-соединений [23].

Таким образом, несмотря на высокую эффективность VPN в стабильных проводных сетях, классические схемы обмена ключами остаются уязвимыми перед квантовыми вычислениями. Интеграция квантового распределения ключей обеспечивает долговременную криптостойкость и надёжность передачи данных даже при потере пакетов и переключениях в сетях 4G/5G, что делает данный подход перспективным для критически важных корпоративных и государственных приложений.

7. ЗАКЛЮЧЕНИЕ

В современных условиях автономное использование КРК для прямой генерации и обмена секретными ключами между мобильными устройствами остаётся технологически невозможным. Основными препятствиями являются сложность аппаратной реализации квантовых приёмопередатчиков, необходимость в стабильном квантовом канале, ограниченная скорость генерации ключей и вопросы масштабируемости таких систем. В этой связи наиболее реалистичным путём развития выступают гибридные схемы: ключи генерируются и распространяются по стационарной квантовой инфраструктуре оператора между доверенными узлами, а для защищённой передачи на “последней миле” применяются алгоритмы ПКК. При этом доверенные зоны (например, аппаратные HSM — Hardware Security Module) и специализированные SIM/USIM-карты обеспечивают локальное хранение и периодическое обновление ключей, получаемых через КРК, а встроенные квантовые источники энтропии на мобильных устройствах повышают надёжность генерации симметричных ключей.

Дальнейшие исследования должны быть сосредоточены на уменьшении размеров и стоимости компонентов КРК, повышении скоростей квантовой генерации ключей и увеличении дальности передачи квантовых сигналов. Не менее важными являются разработка архитектур распределённых квантовых сетей с использованием доверенных узлов и квантовых повторителей, а также стандартизация гибридных решений, объединяющих КРК и ПКК, в рамках международных организаций (ETSI, ITU-T, 3GPP). Исследование альтернативных физических платформ для интеграции квантовых устройств в существующие мобильные сети позволит создать по-настоящему устойчивую к квантовым атакам инфраструктуру связи следующего поколения.

СПИСОК ЛИТЕРАТУРЫ

1. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.
2. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2), 303-332.
3. Proos, J., & Zalka, C. (2003). Shor's discrete logarithm quantum algorithm for elliptic curves. *arXiv preprint quant-ph/0301141*.
4. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188-194.
5. National Institute of Standards and Technology (NIST). *Post-Quantum Cryptography Standardization*. https://csrc.nist.gov/projects/post-quantum-cryptography

6. Bennett, Charles & Brassard, Gilles. (1984). WITHDRAWN: Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science - TCS. 560. 175-179. 10.1016/j.tcs.2011.08.039.

7. Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information*, 2(1), 1-12.

8. Zhang, Yichen & Li, Zhengyu & Chen, Ziyang & Weedbrook, Christian & Zhao, Yijia & Wang, Xiangyu & Huang, Yundi & Xu, Chunchao & Xiaoxiong, Zhang & Wang, Zhenya & Li, Mei & Zhang, Xueying & Zheng, Ziyong & Chu, Binjie & Gao, Xinyu & Meng, Nan & Cai, Weiwen & Wang, Zheng & Wang, Gan & Guo, Hong. (2019). Continuous-variable QKD over 50 km commercial fiber. Quantum Science and Technology. 4. 035006. 10.1088/2058-9565/ab19d1.

9. Liao, S. K., Cai, W. Q., Liu, W. Y., Zhang, L., Li, Y., Ren, J. G., ... & Chen, Y. A. (2017). Satellite-to-ground quantum key distribution. *Nature*, 549(7670), 43-47.

10. Wang, S., Chen, W., Yin, Z. Q., Li, H. W., He, D. Y., Li, Y. H., ... & Han, Z. F. (2014). Field test of wavelength-saving quantum key distribution network. *Optics letters*, 39(6), 1481-1484.

11. Zhang, Y., Li, Z., Chen, Z., Weedbrook, C., Zhao, Y., Wang, X., ... & Xu, B. (2019). Continuous-variable QKD over 100 km at 1.3 Gbps with a locally generated local oscillator. *Optics Express*, 27(14), 20515-20528.

12. Eriksson, T. A., Hirano, T., Puttnam, B. J., Rademacher, G., Luís, R. S., Fujiwara, M., ... & Awaji, Y. (2019). Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. *Communications Physics*, 2(1), 1-8.

13. Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, 362(6412), eaam9288.

14. Liu J.W., Kai Y.Z., Jia Y.W., Jie C., Yong H.Y., Shi B.T., Di Y., Yan L.T., Zhen L., Yu Y., Qiang Z., Jian W.P. Experimental authentication of quantum key distribution with post-quantum cryptography. *Quantum Information*, vol. 7(67), 2021, pp. 1–7.

15. Forbes Technology Council. Achieving Quantum-Level Security With Hybrid Networks Using PQC, QKD And Quantum Internet. [Online]. Available: `https://www.forbes.com/sites/forbestechcouncil/2023/02/10/achieving-quantum-level-security-with-hybrid-networks-using-pqc-qkd-and-quantum-internet`.

16. ТАСС. Антон Гугля: «На рынке постквантовой криптографии все только начинается». [Электронный ресурс]: `https://tass.ru/interviews/16279079/`.

17. Hoque S., Aydeger A., Zeydan E. 2024. Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design. In Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems (PECS '24). Association for Computing Machinery, New York, NY, USA, 9–16. https://doi.org/10.1145/3659997.3660033

18. Otero-García P., Orfila A., Canovas A., Rios R., Lujan-Mora S. Network-wide Quantum Key Distribution with Onion Routing Relay. arXiv:2505.13239, 2025.

19. China Telecom Quantum Group. Hybrid quantum-safe encryption system enables 1000km secure call. *The Quantum Insider*, May 2025.

20. Vodafone & IBM. Vodafone and IBM Partner to Implement Post-Quantum Security in Mobile Networks. *MWC 2025*, Mar. 2025.

21. Niemiec, M., Machnik, P. Authentication in virtual private networks based on quantum key distribution methods. Multimedia Tools and Applications, 75(17), 10691-10707, 2016.

22. Gao D., et al., Test analysis of practical quantum VPN gateway, EI2, 2017, pp. 1–6.

23. Sandra Helsel, *China Launches its First Quantum-Encrypted Smartphone*, Inside Quantum Technology, May 2022. `https://www.insidequantumtechnology.com/news-archive/china-launches-its-first-quantum-encrypted-smartphone/`

24. QuantumCTek, *QSS-ME: Quantum Secure Media for Mobile VOIP*, 2017. https://www.quantum-info.com/English/product/2017/1007/393.html

25. ID Quantique, *SK Telecom unveils the Samsung Galaxy Quantum 5*, 2024. https://www.idquantique.com/samsung-galaxy-quantum-5/

Quantum Key Distribution in Mobile Networks: Modern Approaches and Prospects

P. Y. Vatskov, E.M. Mavrin, V.G. Potapov, P. V. Che

In the face of growing information security threats ranging from increasing computational power to the emergence of quantum computers, traditional cryptographic methods are losing their long-term reliability. Against this backdrop, quantum cryptography technologies, particularly quantum key distribution (QKD), are emerging as promising tools for ensuring physically grounded data security. This paper presents a comprehensive analysis of the potential for autonomous implementation of QKD in 4G/5G mobile networks, focusing on practical deployment aspects and possible limitations. Additionally, the integration of post-quantum cryptography and QKD is explored as a complementary approach to securing user data, along with the prospects for building a secure infrastructure based on VPN technologies and quantum key distribution systems. Special attention is given to comparing international and domestic developments in this field and evaluating the applicability of these technologies in real-world mobile networks.

KEYWORDS: quantum key distribution (QKD), mobile networks 4G/5G, quantum cryptography, secure communication channels.