Internet Engineering Task Force (IETF)
Request for Comments: 9958
Category: Informational
ISSN: 2070-1721

A. Banerjee
T. Reddy.K
D. Schoinianakis
Nokia
T. Hollebeek
DigiCert
M. Ounsworth
Entrust

June 2026

Post-Quantum Cryptography for Engineers

Пост-квантовая криптография для инженеров

Аннотация

Появление криптографически значимого квантового компьютера (cryptographically relevant quantum computer или CRQC) сделало бы устаревшими современные традиционные алгоритмы с открытым ключом, поскольку лежащие в их основе математические допущения утратили бы актуальность. Для решения проблемы протоколы и инфраструктура должны перейти на пост-квантовые алгоритмы, разработанные для противостояния как традиционным, так и квантовым атакам. В этом документе объясняется, почему инженерам нужно знать и понимать пост-квантовую криптографию (post-quantum cryptography или PQC), а также подробно описывается влияние CRQC на имеющиеся системы и рассматриваются задачи, связанные с переходом к пост-квантовым алгоритмам. В отличие от прежних обновлений криптографии, этот переход может потребовать существенной переработки протоколов из-за уникальных свойств пост-квантовых алгоритмов.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется с информационными целями.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Не все документы, одобренные IESG, претендуют на статус стандартов (см. раздел 2 в RFC 7841).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9958.

Оглавление

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Квантовые вычисления - это не просто теоретическая концепция в физике и компьютерной науке, а активная область исследований с практическими результатами. В настоящее время в разработку практических квантовых вычислительных систем вкладываются большие исследовательские усилия и огромные средства корпораций и государств. На момент публикации этого документа CRQC, способные взломать широко распространённые асимметричные алгоритмы (называемые также алгоритмами с открытым ключом), ещё не были созданы. Однако ведутся исследования и разработки в сфере квантовых вычислений с целью создания более мощных и масштабируемых квантовых компьютеров.

Один из распространённых мифов заключается в том, что квантовые компьютеры быстрее традиционных CPU и GPU во всех сферах применения. Однако это не совсем верно - как GPU превосходят традиционные CPU при решении определённых задач, так и у квантовых компьютеров есть своя ниша, где они преуспевают. К сожалению для криптографов, задачи разложения простых чисел на сомножители (факторизация) и нахождения дискретных логарифмов, лежащие в основе традиционной криптографии с отрытым ключом, попадают в ту сферу вычислений, где ожидается успех квантовых компьютеров. По мере развития квантовых технологий появляется возможность значительного влияния квантовых компьютеров на современные криптографические системы. Предсказание времени появления CRQC является сложной задачей и сохраняется неопределённость по срокам их практической доступности [CRQCThreat].

Широкие исследования привели к созданию нескольких пост-квантовых криптоалгоритмов, которые потенциально смогут обеспечить выживание криптографии в эпоху квантовых вычислений. Однако переход к пост-квантовой инфраструктуре является непростой задачей, с которой связано множество проблем, требующих разрешения. Для этого требуется сочетание усилий инженеров, упреждающей оценки и анализа доступных технологий, а также осторожного подхода к разработке и внедрению продукции.

Криптографию PQC иногда называют квантово-стойкой (quantum-proof), квантово-безопасной (quantum-safe), или квантово-резистентной (quantum-resistant). Она включает разработку криптографических алгоритмов для защиты коммуникаций и данных в мире, где квантовые компьютеры достаточно мощны, чтобы взламывать традиционные криптосистемы, такие как RSA (Rivest-Shamir-Adleman) и ECC (Elliptic Curve Cryptography). Алгоритмы PQC предназначены для защиты от атак квантовых компьютеров, использующих квантово-механические эффекты для решения математических задач, невыполнимых для традиционных компьютеров.

По мере приближения угроз со стороны CRQC инженерам, отвечающим за разработку, обслуживание и защиту криптосистем, следует готовиться к значительным изменениям, которые повлечёт за собой появление CRQC. Инженеры должны понимать, как внедрять пост-квантовые алгоритмы в приложения, оценивать компромиссы между безопасностью и производительностью, обеспечивать совместимость с имеющимися системами, где это потребуется. Это не просто замена алгоритмов и во многих случаях переход к PQC потребует заново проектировать протоколы и инфраструктуру с учётом существенных различий в использовании ресурсов и размерах ключей между традиционными алгоритмами и PQC. Из-за широты этого влияния ему посвящён весь документ, а не один раздел.

Цель этого документа состоит в предоставлении базовых рекомендаций инженерам, связанным с криптографическими библиотеками, безопасностью сетей и развитием инфраструктуры, где долгосрочное планирование защиты имеет решающее значение. Документ охватывает такие темы, как выбор подходящих алгоритмов PQC и понимание различий между механизмами инкапсуляции ключей (Key Encapsulation Mechanism или KEM) в PQC и традиционных обменах Диффи-Хеллмана (DH) и RSA, а также приводятся сведения о предполагаемых различиях размеров ключей,

шифротекстов, подписей и времени обработки в PQC и традиционных алгоритмах. Обсуждаются также угрозы со стороны CRQC для симметричной криптографии и хэш-функций.

Важно помнить, что асимметричные алгоритмы (алгоритмы с открытым ключом) применяются в основном для защищённой связи между организациями или конечными точками, которые ранее не взаимодействовали, поэтому нужно учитывать значительный объем координации между организациями, а также между экосистемами и внутри их. Такие переходы являются одними из наиболее сложных в технической области и потребуют поэтапных действий, когда обновлённые агенты будут сосуществовать и взаимодействовать с необновлёнными в невиданных ранее масштабах.

Агентство национальной безопасности США (National Security Agency или NSA) опубликовало статью о будущих требованиях к алгоритму PQC для систем национальной безопасности США [CNSA2-0], основанную на необходимости защиты от внедрения в будущем CRQC. Федеральное ведомство информационной безопасности Германии (Federal Office for Information Security или BSI) также выпустило документ по переходу на PQC и рекомендации [BSI-PQC], в значительной степени соответствующие руководству Национального института стандартов и технологий США (National Institute of Standards and Technology или NIST) и NSA, но отличающиеся в конкретных профилях алгоритма PQC.

CRQC представляют угрозу как для симметричных, так и для асимметричных криптосистем. Однако угроза для асимметричной криптографии значительно выше из-за алгоритма Шора [Shors], позволяющего взломать широко применяемые системы с открытым ключом, такие как RSA и ECC. Для симметричной криптографии и хэш-функций риск из-за алгоритма Гровера [Grovers] ниже, воздействие менее серьёзно и обычно может быть смягчено за счёт удвоения размеров ключей и дайджестов там, где имеются риски. Читателю важно понимать, что упоминание в этом документе PQC относится к асимметричной криптографии (криптографии с открытым ключом), а не к каким-либо симметричным алгоритмам на основе потоковых и блочных шифров, хэш-функциям, кодам аутентификации сообщений (Message Authentication Code или MAC) и т. п., которые менее уязвимы для квантовых компьютеров. В документе не рассматриваются случаи, когда традиционные алгоритмы могут стать уязвимыми (см. [QC-DNS] и другие документы).

Документ не охватывает такие технологии, как квантовое распространение (quantum key distribution или QKD) и квантовая генерация ключей, где применяется квантовое оборудование для защиты коммуникаций и создания ключей, соответственно. PQC основывается на традиционной математике и программах и может работать на компьютерах общего назначения.

Документ не содержит подробных математических или технических спецификаций алгоритмов PQC, а скорее предоставляет инженерам обзор текущей ситуации с угрозами и алгоритмов, разработанных для предотвращения таких угроз. Криптографические и алгоритмические рекомендации этого документа не следует считать правомочными, если они противоречат новым рекомендациям исследовательской группы Crypto Forum (CFRG).

2. Терминология

Quantum computer - квантовый компьютер
: Компьютер, выполняющий расчёты на основе явлений квантовой механики, таких как суперпозиция и спутанность.

Physical qubit - физический кубит
: Базовый физический блок квантового компьютера, подверженный шумам и ошибкам.

Logical qubit - логический кубит
: Отказоустойчивый кубит, основанный на множестве физических кубитов с использованием квантовой коррекции ошибок. Это фактический блок надёжных квантовых вычислений.

Post-Quantum Cryptography (PQC) - пост-квантовая криптография
: Криптографические алгоритмы, разработанные для защиты от квантовых и классических атак.

Cryptographically Relevant Quantum Computer (CRQC) - криптографически значимый квантовый компьютер
: Квантовый компьютер с числом логических кубитов, достаточным для взлома традиционных асимметричных криптоалгоритмов (например, RSA или ECC) за приемлемое время.

Public Key Cryptography (Asymmetric Cryptography) - криптография с открытым ключом
: Класс криптоалгоритмов, где применяются разные ключи для шифрования и расшифровки или подписания и проверки подписи. В этом документе термины Public Key Cryptography и Asymmetric Cryptography являются синонимами.

Продолжаются дискуссии об использовании терминов post-quantum, quantum ready, quantum resistant, quantum secure для описания алгоритмов, способных противостоять CRQC, и согласия пока не достигнуто. В NIST термин post-quantum применяется для алгоритмов, участвовавших в конкурсе на выбор кандидата. В этом контексте термин можно интерпретировать как «набор алгоритмов, разработанных так, чтобы сохранить их пригодность после появления квантовых компьютеров», а не как заявление об их безопасности. Термин quantum resistant или quantum secure, очевидно, указывает свойство алгоритмов, однако высказываются опасения, что указание класса алгоритмов как «квантово-стойкого» или «квантово-безопасного» может привести к путанице, если какой-либо из таких алгоритмов потом окажется менее стойким или безопасным, чем предсказывала теория. Термин quantum ready часто обозначает решение (устройство, комплекс, программный стек), достигшее зрелости в плане интеграции новых криптографических алгоритмов. Авторы отмечают значительную вариативность использования терминов, которые в данном документе являются взаимозаменяемыми при обсуждении алгоритмов.

Термины «текущий» (current), «современный» (state-of-the-art), «будущий» (ongoing) относятся к работам, исследованиям, внедрениям или разработкам на момент публикации документа.

3. Угроза криптографии со стороны CRQC

При рассмотрении рисков безопасности, связанных со способностью квантовых компьютеров атаковать традиционную криптографию, важно различать влияние на симметричные и асимметричные алгоритмы. Peter Shor и Lov Grover разработали два алгоритма, которые изменили представление о безопасности в условиях наличия CRQC.

Квантовые компьютеры по своей природе являются гибридом классических и квантовых вычислительных блоков. Например, алгоритм Шора включает комбинацию квантовых и классических расчётов. Таким образом, термин «квантовый противник» (quantum adversary) следует понимать как «противник с квантовым усилением» (quantum-enhanced adversary), что означает наличие у него доступа к квантовым и классическим методам расчётов.

Хотя ещё нет больших квантовых компьютеров, пригодных для экспериментов, теоретические свойства квантовых вычислений очень хорошо изучены. Это позволяет инженерам и исследователям рассуждать о верхних пределах квантово-усовершенствованных расчётов и разрабатывать криптоалгоритмы, устойчивые к любым мыслимым формам квантового криптоанализа.

3.1. Симметричная криптография

Для неструктурированных данных, таких как зашифрованные с симметричным ключом или криптографические хэш-значения, CRQC хотя и могут искать конкретные решения для всех возможных входных комбинаций (например, алгоритм Гровера), неизвестно ни одного квантового алгоритма для нарушения базовых свойств безопасности этих классов алгоритмов. Симметричная криптография, включающая примитивы с ключами, такие как блочные шифры (например, AES) и механизмы аутентификации сообщений (например, HMAC-SHA256), основана на секретных ключах, известных отправителю и получателю и остающихся безопасными даже в пост-квантовом мире. Симметричная криптография включает также функции хэширования (например, SHA-256), применяемые для защищённого создания дайджестов сообщений без использования общего ключевого материала. Хэшированный код аутентификации сообщения (Hashed Message Authentication Code или HMAC) - это специальная конструкция, использующая для создания кода проверки подлинности сообщения криптографическую хэш-функцию и секретный ключ, известный отправителю и получателю.

Алгоритм Гровера - это квантовый алгоритм поиска, теоретически обеспечивающий квадратичное ускорение поиска в неструктурированных базах данных по сравнению с традиционными алгоритмами поиска. Он привёл к распространённому заблуждению о необходимости удвоения размера симметричных ключей для обеспечения квантовой безопасности. Если рассматривать сопоставление хэш-значений со входными данными (известными как прообраз - pre-image) или шифротекста с соответствующими блоками открытого текста как базу данных без структуры, алгоритм Гровера теоретически требует удвоения размера ключей симметричных алгоритмов по сравнению с используемыми на момент публикации, чтобы скомпенсировать квадратичное ускорение и сохранить текущий уровень безопасности. Это связано с тем, что алгоритм Гровера сокращает число операций, требуемых для взлома 128-битовой симметричной криптографии до 2^64 квантовых операций, что может казаться достижимым. Однако квантовые операции принципиально отличаются от классических и 2^64 классических операций можно выполнять параллельно, а 2^64 должны выполняться последовательно, что делает нереальной реализацию на практически доступных квантовых компьютерах.

Алгоритм Гровера слабо распараллеливается и даже при параллельном развёртывании 2^c вычислительных блоков для подбора ключа (brute-force) время выполнения будет пропорционально 2^((128-c)/2). Проще говоря, использование 256 квантовых компьютеров сократит время перебора лишь в 16 раз, а 1024 квантовых компьютеров обеспечат 32-кратное ускорение и т. д. (см. [NIST] и [Cloudflare]). По общему мнению экспертов это сохранит безопасность AES-128 на практике и удваивать размер ключей не потребуется.

Возникает естественный вопрос о возможности разработки более совершенного алгоритма, который превзойдёт алгоритм Гровера в общем случае. Christof Zalka показал, что алгоритм Гровера обеспечивает наилучшую возможную сложность для этого типа поиска, значит существенного ускорения квантового подхода не следует ожидать [Grover-Search].

NIST в критериях оценки PQC сравнивает уровни безопасности предложенных пост-квантовых алгоритмов с традиционной и квантовой безопасностью AES-128, AES-192 и AES-256. Это показывает уверенность NIST в стабильности защитных свойств AES даже при наличии классических и квантовых атак. Таким образом, 128-битовые алгоритмы можно считать квантово-безопасными в обозримом будущем. Однако в целях соблюдения требований некоторые организации, например, Французское национальное агентство по безопасности информационных систем (French National Agency for the Security of Information Systems или ANSSI) [ANSSI] и Агентство национальной безопасности США (National Security Agency или NSA) (CNSA 2.0) [CNSA2-0], рекомендуют использовать AES-256.

3.2. Асимметричная криптография

Алгоритм Шора эффективно решает задачу разложения целых чисел на сомножители (факторизация) и связанную с ней задачу дискретного логарифма, которые являются основой большинства современных криптографических методов с открытым ключом. Это означает, что в случае создания CRQC современные алгоритмы и протоколы с открытым ключом (например, RSA, Diffie-Hellman, ECC и менее известные варианты, такие как подписи ElGamal [RFC6090] и Schnorr [RFC8235]) должны быть заменены алгоритмами и протоколами, устойчивыми к криптоанализу с использованием CRQC[1]. Исследования показывают, что при наличии CRQC можно взломать RSA-2048 за часы или даже секунды в зависимости от допущений о коррекции ошибок [RSAShor] [RSA8HRS] [RSA10SC]. Хотя пока такие машины доступны лишь в теории, это говорит о потенциальной уязвимости RSA при появлении CRQC.

Для структурированных данных, таких как открытые ключи и подписи, CRQC могут полностью решать базовые сложные задачи традиционной криптографии (см. алгоритм Шора). Поскольку увеличение размера ключевых пар не обеспечит безопасного решения (за исключением мультигигабайтных ключей RSA [PQRSA]), потребуется полная замена алгоритмов. Поэтому пост-квантовая криптография с открытым ключом должна основываться на иных принципах, нежели применяются в традиционной криптографии с открытым ключом (разложение целых чисел на сомножители, дискретный логарифм над конечным полем и дискретный алгоритм для эллиптической кривой).

3.3. Квантовые атаки по побочным каналам

Криптографические атаки по побочным каналам используют физические аспекты (такие как синхронизация, потребляемая мощность, электромагнитные излучения) для восстановления секретных ключей. Это может позволить злоумышленникам существенно расширить свои возможности с помощью квантовых методов при криптоанализе [QuantSide]. Полное рассмотрение квантовых методов для побочных каналов выходит за рамки документа, однако разработчикам криптографического оборудования следует понимать, что имеющихся сегодня методов защиты от побочных каналов может быть недостаточно при наличии у злоумышленников квантовых возможностей.

[1] Отметим, что алгоритм Шора не может работать лишь на классических компьютерах и требует CRQC.

4. Традиционные примитивы, которые могут быть заменены PQC

Любой асимметричный алгоритм, основанный на факторизации целых чисел, а также дискретных алгоритмах над конечным полем или эллиптической кривой, будет уязвим для атак с использованием алгоритма Шора на CRQC. Этот документ посвящён основным функциям асимметричной криптографии.

Согласование и доставка ключей

Схемы согласования ключей по методу Диффи-Хеллмана (Diffie-Hellman или DH) или DH с эллиптической кривой (Elliptic Curve Diffie-Hellman или ECDH), а также доставка ключей (обычно с использованием шифрования RSA) служат для организации общего криптографического ключа для защищённого взаимодействия. Эти механизмы могут быть заменены PQC, поскольку они основаны на существующей асимметричной криптографии и поэтому уязвимы для алгоритма Шора. CRQC может применять алгоритм Шора для эффективного поиска простых сомножителей длинного открытого ключа (в случае RSA), который можно использовать для раскрытия общего секрета. В случае DH компьютер CRQC потенциально способен вычислить дискретный логарифм открытого ключа DH (краткосрочного или долгосрочного), что раскроет секрет, требуемый для вывода симметричного ключа шифрования.

Цифровые подписи

Схемы цифровой подписи служат для проверки подлинности отправителя, обнаружения несанкционированного изменения данных и поддержки доверия к системе. Как и согласование ключей, подписи зависят от пары ключей (открытого и секретного), основанной на той же математике, которая применяется для согласования и доставки ключей. Поэтому взлом имеющейся асимметричной криптографии будет влиять на традиционные цифровые подписи и нужно разрабатывать для этого пост-квантовые алгоритмы.

Подписи Boneh-Boyen-Shacham (BBS)

Подписи BBS обеспечивают сохранение приватности (конфиденциальности) со свойствами, подобными доказательствам без разглашения (zero-knowledge proof), что позволяет выборочно раскрывать конкретные подписанные атрибуты без раскрытия всего набора подписанных данных. Безопасность подписей BBS основана на сложности задачи дискретного логарифма, что делает их уязвимыми для алгоритма Шора. CRQC может нарушить безопасность аутентификации BBS, но не конфиденциальность данных (параграф 6.9 в [BBS-SIG-SCHEME]).

Шифрование содержимого

Шифрование содержимого обычно подразумевает шифрование данных с использованием алгоритма с симметричным ключом, такого как AES, для обеспечения конфиденциальности. Угрозы для симметричной криптографии рассмотрены в параграфе 3.1.

5. Алгоритмы NIST PQC

На момент написания этого документа в NIST были стандартизованы 3 алгоритма PQC и предполагается стандартизация в будущем ещё большего их числа (см. [NISTFINAL]). Эти алгоритмы не обязательно будут заменой традиционным алгоритмам асимметричной криптографии, например, RSA [RSA] и ECC [RFC6090] могут применяться как в качестве KEM, так и для подписей, тогда как в настоящее время нет пост-квантовых алгоритмов, способных выполнять сразу обе функции. При обновлении протоколов важно заменить имеющиеся традиционные алгоритмы на PQC KEM или подписи PQC в зависимости от прежнего использования традиционного алгоритма. Кроме того, KEM, как указано в разделе 9, предоставляет API, отличный от примитивов создания или доставки ключей. В результате для включения новых алгоритмов могут потребоваться изменения на уровне протоколов или приложений.

5.1. Выбранные NIST кандидаты для стандартизации

5.1.1. Механизмы инкапсуляции ключей PQC KEM

ML-KEM

Инкапсуляция ключей на основе модульной решётки (Module-Lattice-Based Key-Encapsulation), FIPS 203 [ML-KEM].

HQC

Квазициклический код Хэмминга (Hamming Quasi-Cyclic) [HQC]. Алгоритм кодирования, основанный на сложности декодирования синдрома для квазициклической конкатенации кодов Reed-Muller и Reed-Solomon (RMRS) в метрике Хэмминга. Коды Рида-Мюллера (RM) - это класс блочных кодов корректировки ошибок, широко применяемый в беспроводных и космических коммуникациях, а коды Рида-Соломона широко используются для обнаружения и корректировки многобитовых ошибок. Алгоритм HQC выбран в рамках проекта NIST по пост-квантовой криптографии, но ещё не стандартизован.

5.1.2. Подписи PQC

ML-DSA

Цифровые подписи на основе модульной решётки (Module-Lattice-Based Digital Signature), FIPS 204 [ML-DSA].

SLH-DSA

Основанный на хэшировании алгоритм цифровой подписи без учёта состояний (Stateless Hash-Based Digital Signature), FIPS 205 [SLH-DSA].

FN-DSA

Алгоритм цифровой подписи с быстрым преобразованием Фурье с использованием решётки NTRU (Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm) [FN-DSA]. Отметим, что в NIST этот алгоритм называется FN-DSA, а его спецификация - FIPS 206, но на момент публикации этого документа спецификация ещё не была выпущена.

Дополнительные сведения приведены в параграфах 8.1, 8.2 и 10.2.

6. Выбранные ISO кандидаты для стандартизации

На момент написания этого документа в ISO было выбрано 3 алгоритма PQC KEM в качестве кандидатов в стандарты.

6.1. Механизмы инкапсуляции ключей PQC (KEM)

FrodoKEM

Алгоритм KEM, основанный на сложности обучения в алгебраически неструктурированных решётках [FrodoKEM].

ClassicMcEliece

Алгоритм KEM, основанный на сложности декодирования синдрома кодов Goppa - класса кодов, способных исправить некоторое число ошибок в передаваемом сообщении. Декодирование заключается в восстановлении исходного сообщения из принятого кодового слова с шумами [ClassicMcEliece].

NTRU

Алгоритм KEM, основанный на решётках усечённых полиномиальных колец степени N (N-th degree Truncated polynomial Ring Units или NTRU). Вариантом этого алгоритма является Streamlined NTRU Prime (sntrup761), применяемый в SSH [RFC9941]. См. [NTRU].

7. Сроки перехода

Сроки и мотивы перехода несколько различаются для конфиденциальности (например, шифрование) и аутентификации (например, подписи). В части конфиденциальности данных важны атаки со сбором и последующим дешифрованием данных (harvest now, decrypt later или HNDL), где злоумышленник с достаточными ресурсами может организовать сбор конфиденциальных шифрованных данных в надежде расшифровать их при появлении CRQC. Это означает, что в любой момент зашифрованные конфиденциальные данные уязвимы для атак из-за отсутствия квантово-безопасных стратегий, поскольку эти данные могут быть расшифрованы в будущем. В части аутентификации срок между подписанием и проверкой подписи зачастую очень краток (например, время согласования TLS), но в некоторых случаях (например, подписи микрокода или программ) срок действия подписи может быть большим (десятилетия), а сроки действия подписей в юридических документах и встроенных сертификатах устройств (например, смарт-карт) могут быть ещё больше. Даже для краткосрочных подписей инфраструктура часто полагается на долгосрочные корневые ключи, которые может быть сложно обновить или заменить на устройствах в полевых условиях.

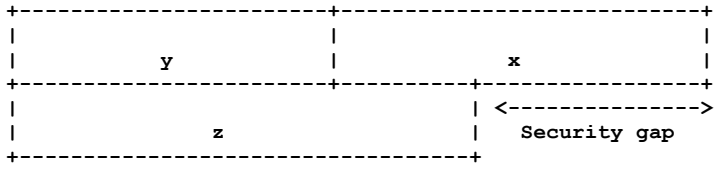

Рисунок 1. Модель Mosca.

Эти проблемы прекрасно иллюстрирует так называемая модель Моска (Mosca) рассмотренная в [Threat-Report]. На рисунке 1 «x» показывает время, в течение которого системы и данные должны оставаться безопасными, «y» - число лет на полный переход к инфраструктуре PQC, а «z» - время, в течение которого появится CRQC для взлома текущей криптографии. Модель предполагает либо перехват и сохранение зашифрованных данных до перехода через y лет, либо использование подписей в течение x лет после создания. Эти данные остаются уязвимыми в течение всех x лет своего жизненного цикла, а сумма x+y даёт оценку всего интервала времени, в течение которого данные остаются незащищёнными. По сути, модель задаёт вопрос о том, как подготовить системы ИТ в течение этих y лет (иными словами, как минимизировать y) для сокращения этапа перехода к инфраструктуре PQC и минимизации рисков раскрытия данных в будущем.

Не следует также недооценивать факторы, способные ускорить появление CRQC, например, более быстрое развитие квантовых вычислений и более совершенные версии алгоритма Шора, способные работать с меньшим числом кубитов. Инновации часто внезапны, поэтому в интересах отрасли сохранять бдительность и заранее готовиться. Кроме того, следует принимать во внимание, что кроме отслеживаемых отраслью организаций, таких как университеты и организации, публикующие свои результаты, существует множество высоко-бюджетных квантовых исследований, выполняемых частными организациями в интересах различных наций. Таким образом, фактическое развитие квантовых расчётов может на несколько лет опередить общедоступные исследования на момент публикации этого документа.

Организациям следует тщательно и честно оценивать своё время перехода y. Если учитывать лишь время между получением исправлений от поставщика технологии и их внедрением, может показаться, что y составляет лишь несколько недель. Однако это относится лишь к достаточно редким вариантам перехода и чаще переход на PQC будет включать, как минимум, замену некоторой части оборудования. Например, чувствительным к производительности приложениям потребуются CPU с аппаратным ускорением PQC. Чувствительным к безопасности приложениям потребуются PQC TPM, среды доверенного исполнения (Trusted Execution Environment или TEE), защищённые анклавы и другие криптографические сопроцессоры. Приложениям, работающим со смарт-картами потребуется замена карт и считывателей, которые могут применяться в разных вариантах - для входных дверей и турникетов, ввода PIN-кодов, ноутбуков и т. п.

Время y включает не только период внедрения, но и подготовку - интеграцию, тестирование, аудит и повторную сертификацию криптографических сред. Следует также учитывать другие факторы, влияющие на y, - время, требуемое производителям для создания поддерживающей PQC продукции, которое может включать задержки на аудит и сертификацию, время, требуемое регуляторам для принятия правил PQC, время для ознакомления аудиторов с новыми требованиями и т. п. Если учитывать в y время с момента начала внедрения функциональности PQC производителями до момента отключения последнего устройства без поддержки PQC, значение y может оказаться достаточно большим, вероятно составляющим годы даже для организаций среднего размера. Это не должно мешать принятию упреждающих мер.

Организациям, отвечающим за защиту долгосрочных конфиденциальных данных или работу критической инфраструктуры, потребуется начать переход незамедлительно, особенно при уязвимости данных к HNDL-атакам. Гибридные схемы PQ/T (Post-quantum and traditional, раздел 13) или PQ для обмена ключами сравнительно самодостаточны и обычно требуют лишь замены криптобиблиотеки (например, OpenSSL). Для цифровых подписей переход на PQ или PQ/T включает значительные изменения экосистемы, в том числе обновление сертификатов, удостоверяющих центов (CA), протоколов управления сертификатами, HSM, привязок доверия. Начав заранее внедрение гибридного обмена ключами, организация сможет получить опыт работы, а прототипирование и планирование интеграции цифровых подписей PQ/T или PQ поможет выявить воздействия на всю экосистему. Такой поэтапный подход снижает долгосрочные риски при переходе и обеспечивает готовность к более сложным обновлениям.

8. Категории PQC

Стандартизованные NIST схемы пост-квантовой криптографии можно разделить на 3 основных группы: основанные на решётках, основанные на хэшировании и основанные на коде. В рамках исследований и стандартизации изучаются также схемы на основе изогении, многомерная криптография и криптография на основе MPC-in-the-Head. Кроме того, NIST принимает дополнительные предложения по цифровым подписям для расширения набора оцениваемых вариантов [AddSig].

8.1. Криптография с открытым ключом на основе решёток

В криптографии с открытым ключом на основе решётки применяется простая конструкция из регулярного набора равномерно распределенных точек в пространстве Евклида (решётка) для создания ловушек (trapdoor). Эти задачи решаются эффективно при наличии секретных данных, но требуют сложных расчётов в ином случае. Примерами таких задач являются поиск кратчайшего и ближайшего вектора, поиск короткого целочисленного решения, обучение при наличии ошибок (включая модульное), решение задачи с округлением. Для всех таких задач имеются убедительные доказательства сведения наихудшей ситуации к средней (worst-to-average), эффективно сопоставляющего сложность худшего случая со сложностью среднего.

Открытые ключи и подписи на основе решётки длиннее классических схем, таких как RSA и ECC, но обычно менее чем на порядок для открытых ключей (6-10 раз) и на 1-2 порядка (10-100 раз) для подписей, что делает их наилучшими кандидатами для общего назначения, например, в качестве замены RSA в сертификатах PKIX. Примеры алгоритмов этого класса включают ML-KEM, FN-DSA, ML-DSA, FrodoKEM.

Примечательно, что в схемах шифрования на основе решётки требуется округление в процессе дешифровки, что создаёт ненулевую вероятность «ошибочного округления», ведущего к ошибочной расшифровке. Однако параметры кандидатов NIST для PQC тщательно подбираются так, чтобы вероятность такого отказа была криптографически пренебрежимой и намного меньше вероятности случайной ошибки при передаче или ошибки в реализации. На практике эти редкие отказы при расшифровке можно рассматривать так же, как критические ошибки при доставке - обе стороны просто заново выполняют операцию KEM, создавая новый общий ключ и шифрованный текст.

В криптоанализе оракулом (oracle) называют систему, к которой злоумышленник может обратиться с вопросом, удалось ли расшифровать данные. Наличие такого оракула поможет злоумышленнику значительно понизить уровень безопасности основанных на решётках схем, имеющих сравнительно высокую частоту отказов. Однако, как показано в [LattFail1], для большинства предложений NIST PQC число запросов к оракулу, требуемых для принудительного сбоя расшифровки, превышает практические возможности. Недавние исследования улучшили результат [LattFail1], показав, что издержки поиска дополнительных сбойных шифротекстов после нахождения 1 или 2 могут быть значительно увеличены [LattFail2]. Тем не менее, на момент публикации этого документа кандидаты NIST для PQC считались защищёнными от таких атак и проводился постоянный мониторинг по мере криптоаналитических исследований.

8.2. Криптография с открытым ключом на основе хэширования

Криптография с открытым ключом на основе хэша (Hash-based Public Key Cryptography или Hash-based PKC) существует с 1970-х годов, когда она была разработана Лэмпортом (Lamport) и Мерклом (Merkle). Метод служит для создания алгоритмов цифровой подписи и основывается на безопасности базовой криптографической хэш-функции. С 1970-х годов разработано много вариантов подписей на основе хэша (hash-based signature или HBS), включая недавние схемы XMSS [RFC8391], HSS/LMS [RFC8554], BPQS [BPQS]. В отличие от многих других методов цифровой подписи, большинство подписей HBS учитывают состояние, что означает обновление и тщательное обследование секретного ключа для создания подписи. Создание нескольких подписей с одним секретным ключом ведёт к потере безопасности и может приводить к атакам с подделкой подписи.

Подписи на основе хэша с учётом состояния и длительным сроком действия сложнее в эксплуатации, нежели иные типы подписей. Рассмотрим, например, корневой ключ со сроком действия 20 лет. Предполагается, что этот срок превышает срок жизни оборудования, где хранятся ключи, поэтому в какой-то момент потребуется перенос ключей на новое оборудование. Столь же сложными могут быть сценарии аварийного восстановления при неожиданном отказе основного узла. Это требует тщательного рассмотрения вопросов эксплуатации и соответствия требованиям, чтобы предотвратить возможность повторного использования ключа при смене оборудования или аварийном восстановлении. Одним из способов является использование HBS с учётом состояния для краткосрочных ключей, которым не требуется горизонтальное масштабирование (например, для подписи набора образов микрокода с последующим удалением ключа подписи).

Алгоритм SLH-DSA, стандартизованный NIST, использует метод HORST (Hash to Obtain Random Subset with Trees) и является единственным стандартизованным вариантом подписи на основе хэша без учёта состояния, что позволяет избежать сложностей, связанных с поддержкой состояний. SLH-DSA является усовершенствованным вариантом SPHINCS, уменьшающим размер подписей SPHINCS и делающим их более компактными.

8.3. Криптография с открытым ключом на основе кода

Это направление криптографии зародилось в 1970-80-х годах на основе фундаментальной работы Макэлиса (McEliece) и Нидеррайтера (Niederreiter), сосредоточенной на изучении криптосистем на основе кодов с корректировкой ошибок. Популярные коды с корректировкой ошибок включают коды Goppa (применяются в криптосистемах McEliece), коды синдрома кодирования и декодирования, используемые в HQC, квазициклические коды с умеренной частотой проверки ошибок чётности (quasi-cyclic moderate density parity check или QC-MDPC).

В качестве примеров можно привести все невзломанные коды, достигшие финала в четвёртом раунде NIST: Classic McEliece, HQC (выбран NIST для стандартизации), инкапсуляция ключа с обращением битов (Bit Flipping Key Encapsulation или BIKE) [BIKE].

9. KEM

Механизм инкапсуляции ключей (Key Encapsulation Mechanism или KEM) - это криптографический метод защищённого обмена симметричным ключом между двумя сторонами по незащищённому каналу. Он обычно применяется в схемах с

гибридным шифрованием, где используется сочетание асимметричного (с открытым ключом) и симметричного шифрования. Операция KEM даёт в результате симметричный ключ фиксированного размера, который может применяться с симметричным алгоритмом (обычно, блочный шифр) одним из двух способов:

- для получения ключа шифрования данных (data encryption key или DEK);
- для получения ключа шифрования ключей (key encryption key или KEK), служащего для «оборачивания» DEK.

Эти методы часто называют гибридным шифрованием с открытым ключом (Hybrid Public Key Encryption или HPKE) [RFC9180].

Термин «инкапсуляция» выбран преднамеренно, чтобы указать поведение алгоритмов KEM на уровне API, отличающееся от согласования ключей и передачи шифрованных ключей, применяемых сегодня. Схемы согласования ключей предполагают, что обе стороны применяют пару из секретного и открытого ключа при обмене, а доставка шифрованного ключа предполагает выбор симметричного ключа одной стороной и его «шифрования» или «оборачивания» для другой стороны. Схемы KEM используют показанные ниже примитивы API [PQCAPI]:

- def kemKeyGen() -> (pk, sk)
- def kemEncaps(pk) -> (ss, ct)
- def kemDecaps(ct, sk) -> ss

где pk обозначает открытый ключ, sk - секретный, ct - шифротекст, представляющий инкапсулированный ключ, а ss - общий секрет. На рисунке 2 показан пример обмена ключами на основе KEM.

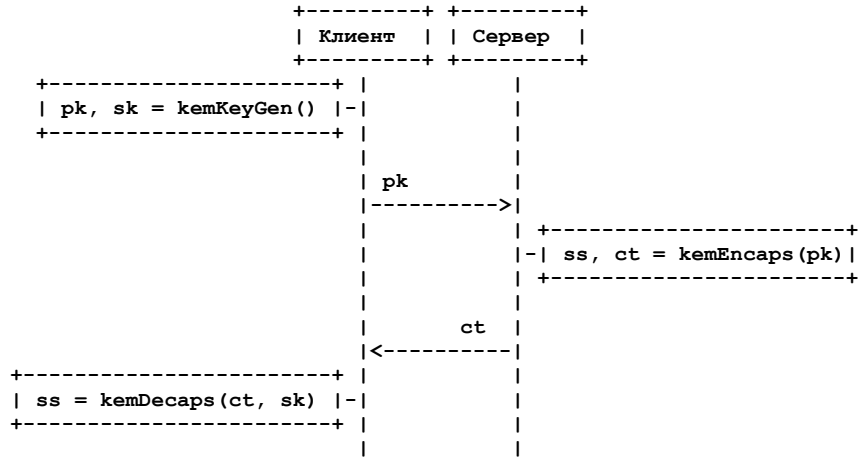

Рисунок 2. Обмен ключами на основе KEM.

9.1. Обмен ключами с аутентификацией

Аутентифицированный обмен ключами (Authenticated Key Exchange или AKE) с KEM, где обе стороны вносят открытый ключ KEM в общий сеансовый ключ, является интерактивным, как описано в параграфе 9.4 [RFC9528]. Однако односторонний метод KEM, когда один партнёр имеет ключ KEM в сертификате, а другой хочет зашифровать ключ (как в почте S/MIME или OpenPGP), можно реализовать с помощью неинтерактивного HPKE [RFC9180]. На рисунке 3 показан обмен ключами DH.

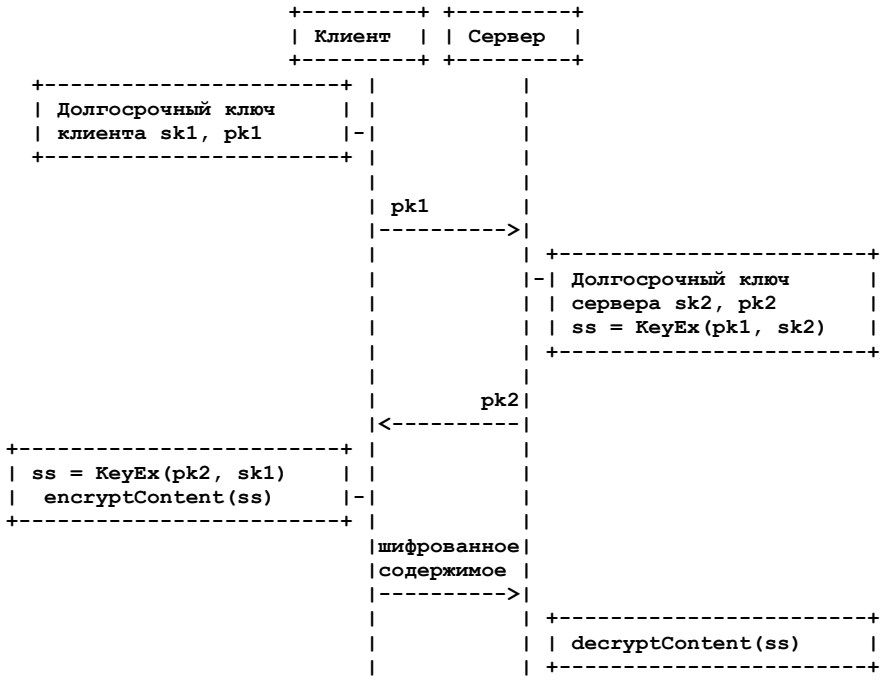

Рисунок 3. AKE на основе DH.

Важно отметить, что в примере выше общий секрет ss выводится из ключевого материала от клиента и сервера, что относит метод к числу AKE. Имеется вариант неинтерактивного обмена ключами (Non-Interactive Key Exchange или NIKE), где отправитель может рассчитать общий секрет ss и шифровать содержимое без активного взаимодействия

(обмен сообщениями через сеть) с получателем. На рисунке 3 показан обмен DH, который является AKE, поскольку обе стороны применяют долгосрочные ключи, позволяющие установить доверие (например, через сертификаты), но это не NIKE, поскольку клиент должен дождаться сетевого взаимодействия для получения открытого ключа получателя pk2, прежде чем рассчитать общий секрет ss и начать шифровать содержимое. Однако обмен DH может быть сразу AKE и NIKE, если открытый ключ получателя заранее известен отправителю (см. рисунок 4), и многие протоколы Internet полагаются на это свойство обмена ключами DH.

Рисунок 4. AKE на основе DH вместе с NIKE.

Сложность KEM заключается в недетерминированности функции Encaps(), которая включает случайность, выбранную отправителем сообщения. Поэтому для выполнения AKE клиент должен ждать, пока сервер сгенерирует требуемую случайность и выполнит Encaps() с ключом клиента, на что потребуется круговой обход через сеть (round-trip). Поэтому основанный на KEM протокол может быть AKE или NIKE, но не тем и другим сразу. Это требует заново проектировать некоторые протоколы Internet с учётом различия, добавлять круговые обходы или компромиссы в части безопасности.

Рисунок 5. AKE на основе KEM.

На рисунке выше Combiner(ss1, ss2), часто называемый объединителем KEM, - это криптографическая конструкция, принимающая два общих секрета, и возвращающая комбинированный общий секрет. Простейшим объединителем является конкатенация ss1 || ss2, но объединители могут быть разной сложности в зависимости от требуемых криптографических свойств. Например, если комбинации следует сохранять IND-CCA2 (см. параграф 9.2.1) для любых входных данных даже при злонамеренном выборе, потребуется более сложная конструкция. Ещё одним соображением при разработке объединителя являются так называемые свойства привязки (binding properties) из [KEEPINGUP], которые могут требовать включения шифротекста и открытого ключа получателя. Анализ безопасности объединителя KEM усложняется в гибридных вариантах, где два KEM представляют разные алгоритмы, например, ML-KEM и ECDH. Более подробное обсуждение объединителей KEM представлено в [KEEPINGUP], [KEM-COMBINER] и [PQ-KEM].

9.2. Безопасность KEM

Описываемые здесь свойства безопасности (IND-CCA2 и привязка) не охватывают все аспекты безопасности KEM. Они просто являются основополагающими для оценки пригодности KEM в протоколах и часто обсуждаются в работах PQC.

9.2.1. IND-CCA2

IND-CCA2 (INDistinguishability under adaptive Chosen-Ciphertext Attack[1]) - это новая концепция безопасности для схем шифрования. Это гарантирует конфиденциальность открытого текста и устойчивость к атакам с выбранным шифротекстом. Определение IND-CCA2 для методов KEM приведено в [CS01] и [BHK09]. ML-KEM [ML-KEM] и Classic McEliece обеспечивают безопасность IND-CCA2.

Понимание IND-CCA2 важно при проектировании и внедрении криптографических схем и протоколов для оценки стойкости алгоритмов, их пригодности для конкретных применений и соблюдения требований к конфиденциальности данных и безопасности. Разработчикам, переходящим на использование KEM, проверенных IETF в рамках данного протокола или потока, разбираться с IND-CCA2 не обязательно. IND-CCA2 является общепринятой концепцией безопасности для механизмов шифрования с открытым ключом, подходящей для широкого спектра приложений. При определении в спецификациях IETF новых механизмов KEM в описании свойств безопасности следует полностью указывать соответствующие криптографические свойства, включая IND-CCA2.

9.2.2. Привязка

KEM обладает также ортогональным набором свойств, которые следует учитывать при разработке протоколов - это привязка (binding) [KEEPINGUP] к шифротексту, открытому ключу, контексту или иное свойство, которое важно не менять между вызовами KEM. В общем случае считается, что KEM привязывает некое значение, если замена этого значения атакующим обязательно приведёт к выводу другого общего секрета. Например, если злоумышленник может создать два разных шифротекста, которые будут декапсулироваться в один общий секрет, создать шифротекст, который будет декапсулироваться в один общий секрет с двумя разными открытыми ключами, или целиком подменить обмены KEM между сессиями, такая конструкция не будет привязкой к шифротексту, открытому ключу или контексту, соответственно. Разработчики протоколов могут привязать сведения о состоянии протокола, такие как идентификатор транзакции или nonce, чтобы попытки использования шифротекста одной сессии в другой блокировались на уровне криптографии, поскольку сервер получит другой общий секрет и не сможет расшифровать содержимое.

Решение задачи привязки, как правило, достигается на уровне разработки протокола. Рекомендуется избегать использования выходного секрета KEM напрямую, без интеграции в соответствующий протокол. Хотя алгоритмы KEM обеспечивают секретность ключа, они по своей природе не обеспчивают подлинность источника, защиту от атак с воспроизведением и гарантию свежести. Эти защитные свойства следует обеспечивать встраиванием KEM в протокол, который проанализирован в части такой защиты. Хотя современные реализации KEM, такие как ML-KEM, обеспечивают достаточную энтропию общих секретов, из соображений привязки рекомендуется передавать общий секрет через функцию KDF, а также включать все значения, которые нужно привязать. В итоге будет получен общий секрет, который можно безопасно применять на уровне протокола.

9.3. HPKE

В современной криптографии уже давно используется термин «гибридное шифрование», где применяется асимметричный алгоритм для организации ключа и симметричный - для шифрования основного объёма содержимого. В предыдущих параграфах разъяснялись важные свойства безопасности KEM, такие как IND-CCA2 и привязка, с подчёркиванием необходимости поддержки этих свойств при разработке протоколов. Одной из широко распространённых схем реализации этого является гибридное шифрование с открытым ключом (Hybrid Public Key Encryption или HPKE) [RFC9180].

HPKE [RFC9180] работает в сочетании со схемами KEM, KDF и аутентифицированным шифрованием со связанными данными (Authenticated Encryption with Associated Data или AEAD). HPKE включает три варианта аутентификации и один из них подтверждает владение заранее распространенным ключом, а два необязательных - владение секретным ключом KEM. HPKE можно расширить для поддержки гибридных пост-квантовых KEM [PQ-HPKE]. ML-KEM не поддерживает обмен статическими эфемерными ключами, позволяющий применять HPKE на основе метода KEM DH и его необязательные режимы проверки подлинности, как описано в параграфе 1.5 [X-WING].

10. Подписи PQC

Любая схема цифровой подписи, определяющая безопасность в пост-квантовых условиях, попадает в категорию подписей PQC.

10.1. Безопасность подписей PQC

10.1.1. EUF-CMA и SUF-CMA

EUF-CMA (экзистенциальная непроницаемость при атаке на выбранное сообщение) [GMR88] - это понятие безопасности для схем цифровой подписи, гарантирующее, что злоумышленник даже при наличии доступа к оракулу подписей не сможет подделать подпись произвольного сообщения. EUF-CMA обеспечивает строгую защиту от атак с подделкой, гарантируя целостность и подлинность цифровых подписей за счёт предотвращения несанкционированных изменений и подделки. Методы ML-DSA, FN-DSA и SLH-DSA обеспечивают защиту EUF-CMA.

SUF-CMA (строгая непроницаемость при атаке на выбранное сообщение) строится на основе EUF-CMA, требуя, чтобы злоумышленник не мог создать другую действительную подпись для сообщения, которое уже подписано оракулом. Как и EUF-CMA, SUF-CMA обеспечивает надёжные гарантии для схем цифровой подписи, дополнительно повышая их безопасность. ML-DSA, FN-DSA и SLH-DSA обеспечивают защиту SUF-CMA.

Понимание защиты EUF-CMA и SUF-CMA важно для разработки и реализации криптографических схем, обеспечивающих безопасность, надёжность и отказоустойчивость цифровых подписей. Это позволяет принимать обоснованные решения, анализировать уязвимости, соблюдать стандарты и разрабатывать системы, обеспечивающие надёжную защиту от атак с подделками. Для разработчиков, переходящих на проверенные IETF схемы подписи PQC в рамках данного протокола или потока, глубокого понимания EUF-CMA и SUF-CMA может не потребоваться, поскольку проверенные IETF схемы уже соответствуют этим строгим стандартам безопасности.

[1] Неразличимость при адаптивной атаке с выбранным шифротекстом.

EUF-CMA и SUF-CMA считаются строгими показателями безопасности для алгоритмов цифровой подписи с открытым ключом, делая их подходящими для большинства приложений. Авторам спецификаций IETF следует включать все вопросы безопасности в соответствующий раздел RFC, не полагаясь на уровень знания криптографии разработчиками.

10.2. Детали FN-DSA, ML-DSA, SLH-DSA

Алгоритм цифровой подписи ML-DSA [ML-DSA] основан на сложности задач решёток над модульными решётками, т. е. проблемы модульного обучения с ошибками (Module Learning with Errors или MLWE). Алгоритм основан на предложенной Любашевским модели Фиат-Шамир с прерываниями (Fiat-Shamir with Aborts) [Lyu09], где применяется выборка с отбрасыванием для обеспечения компактности и безопасности основанных на решётках схем Fiat-Shamir (FS). В ML-DSA применяются случайные выборки с однородным распределением из небольших целых чисел для расчёта коэффициентов в векторах ошибок, что упрощает реализацию схемы по сравнению с FN-DSA [FN-DSA], где применяются числа с гауссовым распределением, что требует использования при генерации подписи арифметики с плавающей запятой.

ML-DSA предлагает как детерминированные, так и рандомизированные подписи и реализован с тремя наборами параметров, обеспечивающими разные уровни безопасности. Свойства безопасности ML-DSA рассмотрены в разделе 9 [RFC9881].

Алгоритм FN-DSA [FN-DSA] основан на схеме с решётками подписи GPV (Gentry, Peikert, Vaikuntanathan), где сначала выполняется хэширование (hash-and-sign) и требуется применение некого класса решёток и метода ловушек.

Основным принципом разработки FN-DSA является компактность, т. е. минимальная потребность в пропускной способности памяти (сумма размера подписи и открытого ключа). Это возможно благодаря компактности решёток NTRU. FN-DSA также предоставляет очень эффективные процедуры подписи и проверки. Основные возможные недостатки FN-DSA связаны с нетривиальностью алгоритмов и необходимостью поддержки операций с плавающей запятой для случайной выборки с гауссовым распределением, в то время как в других схемах с решётками применяются менее эффективные, но более простые выборки случайных чисел с однородным распределением.

При реализации FN-DSA требуется учитывать, что подписание FN-DSA сильно подвержено атакам по побочным каналам, если не применяются 64-битовые операции с плавающей запятой. Это требование зависит от платформы, как указано в отчёте NIST [NIST].

Параметры производительности ML-DSA и FN-DSA могут различаться в зависимости от реализации и аппаратной платформы. В общем случае для ML-DSA характерна сравнительно высокая скорость создания подписей, а для FN-DSA - более эффективная проверка подписей. Выбор может зависеть от потребности приложения в создании и проверке подписей (см. [LIBOQS]). Более подробные сведения о размерах и уровнях безопасности приведены в таблицах разделов 11 и 12.

В SLH-DSA [SLH-DSA] применяется концепция подписей на основе хэширования без учёта состояния, где каждая подпись уникальна и не связана с предшествующими подписями (см. параграф 8.2). Это избавляет от необходимости поддержки данных состояния в процессе подписания. Алгоритм SLH-DSA разработан для подписания до 2^64 сообщений с одной парой ключей и обеспечивает три уровня безопасности. Параметры каждого уровня выбраны так, чтобы обеспечивалась защита в 128, 192 и 256 битов. SLH-DSA обеспечивает меньшие размеры ключей, большие размеры подписей, более медленное создание и проверку подписей по сравнению с ML-DSA и FN-DSA. В SLH-DSA нет новых допущений о стойкости, помимо принятых для базовых хэш-функций. Алгоритм основан на устоявшейся криптографии, что делает его надёжным и отказоустойчивым решением для цифровых подписей в пост-квантовом мире.

Все эти алгоритмы (ML-DSA, FN-DSA, SLH-DSA) включают два режима подписи - чистый, где напрямую подписывается все содержимое сообщения, и режим предварительного хэширования, где подписывается не содержимое, а дайджест.

10.3. Детали XMSS и LMS

Расширенная схема подписи Меркла (eXtended Merkle Signature Scheme или XMSS) [RFC8391] и иерархическая схема (Hierarchical Signature Scheme или HSS) / подпись Лейтона-Микали (Leighton-Micali Signature или LMS) [RFC8554] - это схемы подписи на основе хэширования с учётом состояния, где состояние секретного ключа меняется со временем. В обеих схемах повторное использование состояния ключа ставит под угрозу гарантии криптографической защиты.

XMSS и LMS можно применять для подписания потенциально большого, но фиксированного числа сообщений, а число операций при подписании зависит от размера дерева. Оба метода обеспечивают криптографические цифровые подписи, не полагаясь на сложность математических задач, а используя свойства криптографических хэш-функций. XMSS и LMS с множеством деревьев (XMSS-MT и HSS, соответственно) используют иерархический подход на основе гипер-деревьев с деревом Меркла на каждом уровне иерархии. В [RFC8391] описаны варианты XMSS с одним и множеством деревьев, а в [RFC8554] описана система однократных подписей Лейтона-Микали (Leighton-Micali One-Time Signature или LM-OTS), а также системы N-кратных подписей LMS и HSS. Сравнение XMSS и LMS приведено в разделе 10 [RFC8554].

Число уровней дерева в XMSS и HSS с множеством деревьев обеспечивает компромисс между размером подписи и скоростью создания ключа и подписи. При увеличении числа уровней время генерации ключа и подписи снижается экспоненциально за счёт линейного роста размера подписи. HSS позволяет настраивать каждое субдерево, а XMSS-MT не делает этого, используя одну структуру для каждого субдерева.

Из-за описанных выше сложностей XMSS и LMS не подходят на замену традиционным алгоритмам подписи, таким как RSA или ECDSA. Типичными примерами приложений, для которых подходят эти методы, являются долгосрочные подписи, например для обновлений микрокода или безопасной загрузки.

10.3.1. Размеры ключей и подписей LMS

Схема LMS характеризуется наборами четырёх параметров: базовая хэш-функция (SHA2-256 или SHAKE-256), размер дайджеста (24 или 32 байта), высота дерева LMS, определяющая максимальное число подписей, создаваемых с секретным ключом, и ширина коэффициента Winternitz (параграф 4.1 в [RFC8554]). Эти параметры можно использовать

для выбора компромисса между скоростью и размером подписи. Разные комбинации позволяют создать 80 вариантов схемы.

Размеры открытого (PK) и секретного (SK) ключа зависят от длины дайджеста (M), размер подписи зависит от дайджеста, параметра Winternitz (W), высоты дерева LMS (H) и длины дайджеста. В таблице 1 приведены размеры ключа и подписи для дайджеста с M=32.

Таблица 1.

PK	SK	W	H=5	H=10	H=15	H=20	H=25
56	52	1	8684	8844	9004	9164	9324
56	52	2	4460	4620	4780	4940	5100
56	52	4	2348	2508	2668	2828	2988
56	52	8	1292	1452	1612	1772	1932

10.4. Хэширование, затем подпись

В парадигме hash-then-sign сообщение хэшируется перед созданием подписи. При предварительном хэшировании стойкость к подделкам в значительной степени зависит от стойкости применяемой хэш-функции к коллизиям. Эта парадигма позволяет увеличить производительность приложений за счёт сокращения размера подписываемого сообщения, которое нужно передавать между приложением и криптомодулем, а также делает размер подписи предсказуемым и управляемым. Хэширование обязательно даже для коротких сообщений и вносит дополнительные расчётные требования для проверяющего. Это делает производительность схем подписи с предварительным хэшированием более согласованной, но не обязательно более эффективной.

Использование хэш-функции для создания дайджеста с фиксированным размером обеспечивает совместимость подписей с широким спектром систем и протоколов, независимо от размера и формата конкретного сообщения. Этот метод значительно сокращает объем данных, передаваемых и обрабатываемых аппаратными модулями защиты (Hardware Security Module или HSM). Рассмотрим сценарий, где сетевой модуль HSM вынесен в другой ЦОД по отношению к вызывающим приложениям и смарт-картам, подключённым через USB. В таких случаях потоковая передача сообщений размером в мегабайты или гигабайты может сталкиваться с большими задержками в сети, задержками при подписании на устройстве и даже нехваткой памяти на устройстве.

Отметим, что подавляющее большинство протоколов Internet с подписью больших сообщений уже применяет то или иное хэширование на уровне протокола, поэтому данный метод предназначен в основном для фирменных крипто-протоколов и протоколов, принятых другими органами стандартизации (не IETF). Такие протоколы, как TLS 1.3 и DNSSEC используют парадигму hash-then-sign. В сообщениях TLS 1.3 [RFC8446] CertificateVerify учтённое в подписи содержимое включает вывод хеша «стенограммы» (transcript) (параграф 4.4.1 в [RFC8446]), а DNSSEC [RFC4034] использует его для аутентификации источника и обеспечения целостности данных DNS. Синтаксис криптографических сообщений (Cryptographic Message Syntax или CMS) [RFC5652] включает обязательный этап создания дайджеста сообщения перед вызовом алгоритма подписи.

ML-DSA включает внутренние операции хэширования как часть алгоритма подписи. ML-DSA принимает исходное сообщение, применяет внутреннюю хэш-функцию и использует результат хэширования для процесса создания подписи. SLH-DSA выполняет внутреннее рандомизированное сжатие сообщения с применением хэш-функции с ключом, которая может обрабатывать сообщения произвольного размера. В FN-DSA применяется функция хэширования SHAKE-256 как часть процесса для создания дайджеста подписываемого сообщения.

Таким образом, ML-DSA, FN-DSA и SLH-DSA обеспечивают защиту, усиленную по сравнению с традиционной парадигмой hash-then-sign, поскольку, благодаря встраиванию динамического ключевого материала в дайджест сообщения, конфликты значений предварительного хэширования больше не приводят к поддельным подписям. Приложения, которым нужна производительность и экономия пропускной способности, могут по-прежнему применять предварительное хэширование на уровне протокола до вызова ML-DSA, FN-DSA или SLH-DSA, но разработчикам протоколов следует понимать, что это возвращает уязвимость, из-за которой конфликты хэш-значений позволяют подделать подпись. Если для приложения это подходит, рекомендуется подписывать полное сообщение, а не дайджест.

11. Рекомендации NIST в части безопасности и производительности

Здесь представлена перепечатка информации из проекта NIST PQC [NIST] на момент публикации этого документа. В таблице 2 приведены 5 уровней безопасности, предложенных NIST для алгоритмов PQC. Ни NIST, ни IETF не дают конкретных рекомендаций по выбору уровня для использования. В общем случае протоколы будут включать алгоритмы нескольких уровней, чтобы пользователи могли выбрать уровень, соответствующий их политике и степени конфиденциальности (секретности) данных, подобно тому, как сегодня выбирается размер ключей RSA. Уровни защиты определены по расчётным издержкам, сравнимым или превышающим затраты на атаки алгоритмов AES (128, 192, 256) и SHA2/SHA3, т. е. полное восстановление ключа для AES и поиск оптимальных коллизий для SHA2/SHA3.

Таблица 2.

Уровень безопасности PQ	*Стойкость AES/SHA(2/3)*	*Алгоритм PQC*
1	AES-128 (полное восстановление ключа)	ML-KEM-512, FN-DSA-512, SLH-DSA-SHA2/SHAKE-128f/s
2	SHA-256/SHA3-256 (поиск коллизий)	ML-DSA-44
3	AES-192 (полное восстановление ключа)	ML-KEM-768, ML-DSA-65, SLH-DSA-SHA2/SHAKE-192f/s
4	SHA-384/SHA3-384 (поиск коллизий)	На этом уровне алгоритм не тестировался
5	AES-256 (полное восстановление ключа)	ML-KEM-1024, FN-DSA-1024, ML-DSA-87, SLH-DSA-SHA2/SHAKE-256f/s

Для SLH-DSA-x-yf/s значение x указывает базовую хэш-функцию (SHAKE или SHA-2), f означает быструю, а s - малую версию бита y для AES. Алгоритмы SLH-DSA подробно описаны в [RFC9814].

В таблице 3 приведено сравнение размеров подписей для разных категорий алгоритмов SLH-DSA с эквивалентным уровнем безопасности при использовании «простой» версии. Категории включают f для быстрого создания подписей и s

для малого размера подписи и быстрой проверки при более медленном создании подписи. Варианты параметров SHA-256 и SHAKE-256 дают одинаковый размер подписи поэтому указаны в таблице вместе.

Таблица 3.

Уровень безопасности PQ	***Алгоритм***	***Открытый ключ (в байтах)***	***Секретный ключ (в байтах)***	***Подпись (в байтах)***
1	SLH-DSA-{SHA2,SHAKE}-128f	32	64	17088
1	SLH-DSA-{SHA2,SHAKE}-128s	32	64	7856
3	SLH-DSA-{SHA2,SHAKE}-192f	48	96	35664
3	SLH-DSA-{SHA2,SHAKE}-192s	48	96	16224
5	SLH-DSA-{SHA2,SHAKE}-256f	64	128	49856
5	SLH-DSA-{SHA2,SHAKE}-256s	64	128	29792

В таблице 4 показано влияние производительности при разных уровнях безопасности в зависимости от размера секретных и открытых ключей, а также шифротекста или подписи.

Таблица 4.

Уровень безопасности PQ	***Алгоритм***	***Открытый ключ (в байтах)***	***Секретный ключ (в байтах)***	***Шифротекст/Подпись (в байтах)***
1	ML-KEM-512	800	1632	768
1	FN-DSA-512	897	1281	666
2	ML-DSA-44	1312	2560	2420
3	ML-KEM-768	1184	2400	1088
3	ML-DSA-65	1952	4032	3309
5	FN-DSA-1024	1793	2305	1280
5	ML-KEM-1024	1568	3168	1588
5	ML-DSA-87	2592	4896	4627

12. Сравнение PQC KEM и подписей с традиционными

В этом разделе представлены две таблицы для сравнений KEM и подписей в традиционных и пост-квантовых сценариях. В таблицах приведены размеры секретных и открытых ключей, а также шифротекста/подписей для алгоритмов PQC и их традиционных аналогов с похожими уровнями безопасности.

В таблице 5 сравниваются традиционные и PQC методы KEM по уровням безопасности, размерам ключей и шифротекста.

Таблица 5.

Уровень безопасности PQ	***Алгоритм***	***Открытый ключ (в байтах)***	***Секретный ключ (в байтах)***	***Шифротекст (в байтах)***
Традиционный	P256_HKDF_SHA-256	65	32	65
Традиционный	P521_HKDF_SHA-512	133	66	133
Традиционный	X25519_HKDF_SHA-256	32	32	32
1	ML-KEM-512	800	1632	768
3	ML-KEM-768	1184	2400	1088
5	ML-KEM-1024	1568	3168	1568

В таблице 6 сравниваются традиционные и PQC схемы подписи по уровням безопасности, размерам ключей и подписи.

Таблица 6.

Уровень безопасности PQ	***Алгоритм***	***Открытый ключ (в байтах)***	***Секретный ключ (в байтах)***	***Подпись (в байтах)***
Традиционный	RSA2048	256	256	256
Традиционный	ECDSA-P256	64	32	64
1	FN-DSA-512	897	1281	666
2	ML-DSA-44	1312	2560	2420
3	ML-DSA-65	1952	4032	3309
5	FN-DSA-1024	1793	2305	1280
5	ML-DSA-87	2592	4896	4627

Как видно из приведённых таблиц, PQC KEM и схемы подписи обычно имеют существенно более длинные ключи и подписи/шифротекст по сравнению с традиционными. Этот рост размеров может создавать проблемы для протоколов. Например, протокол обмена ключами IKEv2 (Internet Key Exchange Protocol Version 2) использует для передачи сообщений транспортный протокол UDP. Одна из проблем интеграции PQC KEM в IKEv2 заключается в невозможности фрагментации IKE при начальном обмене IKE_SA_INIT. Для решения этой проблемы в [RFC9242] предложено определить новый обмен (Intermediate Exchange), который можно фрагментировать с помощью соответствующего механизма IKE. В [RFC9370] это для обмена ключами PQC после начального обмена IKEv2 и до IKE_AUTH. Другой пример из параграфа 6.3.3 в [SP-1800-38C] показывает, что рост размеров ключей и подписей вызывает разделение сообщений протокола обмена ключами на несколько пакетов, что повышает вероятность потерь в пересчёте на пакет. В сетях с высокими потерями это может увеличить длительность обмена ключами.

13. Гибридные схемы (PQ/T)

Переход на PQC является уникальным событием в истории цифровой криптографии в том смысле, что ни традиционным, ни пост-квантовым алгоритмам нельзя полностью доверять в плане защиты данных в течение требуемого срока. Традиционные алгоритмы, такие как RSA и ECDH, будут взломаны квантовым криптоанализом, а пост-квантовые столкнутся с неопределённостью лежащей в их основе математики, проблемами соответствия требованиям, неизвестными пока уязвимостями, а также оборудованием и программами, которые не вполне готовы в плане защиты от традиционных криптоаналитических атак и ошибок реализации. В процессе перехода от традиционных алгоритмов к пост-квантовым может возникнуть потребность или необходимость использования сразу обоих типов алгоритмов. Терминология для гибридных схем PQ/T описана в [RFC9794].

13.1. Конфиденциальность PQ/T

Свойство гибридной конфиденциальности PQ/T может применяться для смягчения атак «harvest now, decrypt now» (собрать и расшифровать) и HNDL, описанных в разделе 7. Если в PQ был дефект, традиционный алгоритм (T), защищённый от современных злоумышленников, предотвратит немедленную расшифровку. Если алгоритм T будет взломан CRQC, PQ (при условии сохранения защищенности) предотвратит последующую расшифровку (т. е. HNDL). Таким образом, гибридная конструкция обеспечивает конфиденциальность, пока хотя бы один из компонентов остаётся защищённым. Ниже рассматриваются две схемы согласования ключей.

Гибридное согласование ключей с конкатенацией

Финальный общий секрет, который будет служить входными данными для функции получения ключа, является конкатенацией секретов, созданных каждой из схем согласования ключей. Например, в [TLS-HYB-KEY-EXCH] клиент использует расширение поддерживаемых TLS групп для анонсирования поддержки гибридной схемы PQ/T и сервер может выбрать группу, если он поддерживает эту схему. Клиент и сервер с поддержкой гибридной схемы устанавливают общий секрет в форме конкатенации двух общих секретов и применяют его в имеющемся расписании ключей TLS 1.3.

Каскадное гибридное согласование ключей

Финальный общий секрет рассчитывается путём множества итераций функции вывода ключей, где число итераций совпадает с количеством схем согласования ключей в гибридной схеме. Например, в [RFC9370] задано расширение IKEv2, позволяющее добавить один или несколько алгоритмов PQC к традиционному алгоритму для получения финальных ключей IKE Security Association (SA) с использованием каскадирования, описанного в параграфе 2.2.2 [RFC9370].

Были исследованы различные варианты этих гибридных схем согласования ключей. При выборе гибридной схемы следует проявлять осторожность. Выбранная схема для таких протоколов, как TLS 1.3 [TLS-HYB-KEY-EXCH] обладает отказоустойчивостью IND-CCA2, т. е. безопасность IND-CCA2 гарантируется для схемы, пока хотя бы один из применяемых в ней алгоритмов сохраняет защищенность IND-CCA2.

13.2. Аутентификация PQ/T

Свойство гибридной аутентификации PQ/T обеспечивает устойчивость к катастрофическим взломам или непредвиденным уязвимостям в алгоритмах PQC, предоставляя системам дополнительное время для стабилизации перед полным переходом к работе в среде PQ.

Это свойство гарантирует работу схемы гибридной аутентификации PQ/T, пока хотя бы из алгоритмов остаётся безопасным. Например, может применяться гибридный сертификат PQ/T [ML-DSA-X.509] для упрощения протокола гибридной аутентификации PQ/T. Однако протоколу гибридной аутентификации PQ/T не обязательно использовать гибридный сертификат PQ/T и можно воспользоваться разными сертификатами для отдельных алгоритмов [RFC9763]. При использовании раздельных сертификатов злоумышленники могут отделить один от другого или собрать воедино неожиданным способом, включая кросс-протокольные атаки. Конкретные риски в таких ситуациях сильно зависят от протокола и варианта применения, поэтому нужен полный анализ безопасности. Рекомендации по обеспечению надлежащего использования пар сертификатов приведены в параграфах 13.3.2 и 13.3.3.

Требуется тщательно оценить частоту и продолжительность обновлений системы, а также время появления широкодоступных CRQC для решения вопроса о необходимости и сроках поддержки гибридной аутентификации PQ/T.

13.3. Комбинации гибридных криптоалгоритмов - вопросы и подходы

13.3.1. Комбинации гибридных криптоалгоритмов

В гибридной схеме можно использовать более двух алгоритмов сразу с различными методами их объединения. Для целей пост-квантового перехода наиболее простой и рекомендуемой является комбинация пост-квантового и традиционного алгоритма. Рассмотрено также применение нескольких пост-квантовых алгоритмов с различной математической основой. Сочетание алгоритмов, требующее их совместного использования, обеспечивает более строгую защиту, а комбинации, не требующие совместного использования, снижают уровень безопасности, но обеспечивают другие преимущества, такие как совместимость с прежними версиями и гибкость криптографии. Применение традиционного ключа наряду с пост-квантовым зачастую оказывает минимальное влияние на пропускную способность.

13.3.2. Композитные ключи в гибридных схемах

При объединении ключей в режиме AND (И) возможно имеет смысл рассматривать их как единый ключ, а не два разных. Обычно это будет требовать меньших изменений в компонентах экосистем PKI, многие из которых не готовы работать с двумя ключами или двойными подписями. Для синтаксических анализаторов протокольного или прикладного уровня композитный алгоритм, состоящий из двух алгоритмов-компонентов, является просто новым алгоритмом и поддержка добавления новых алгоритмов, как правило, уже имеется. Трактовка множества ключей-компонентов как одного композитного ключа обеспечивает также преимущества в безопасности, такие как предотвращение кросс-протокольного неоднократного использования отдельных ключей-компонентов и гарантии отзыва или удаления всех компонентов ключа одновременно, особенно при рассмотрении композита как единого объекта на всем пути в криптомодуль.

Все, что нужно сделать, - это стандартизация форматов объединения ключей двух алгоритмов в одну структуру данных и способов объединения двух подписей или KEM в одну подпись или KEM. Решением может быть обычная конкатенация, если размеры фиксированы или легко определяются. На момент публикации этого документа ещё продолжались исследования в сфере безопасности композитных подписей и KEM на основе конкатенации в сравнении с более изощрёнными комбинациями подписей и KEM, а также протокольных контекстов, в которых достаточно этой простой комбинации.

Последний вопрос связан с конкретными парами алгоритмов, которые можно объединить. Недавняя тенденция в протоколах заключается в том, чтобы разрешать лишь небольшое число «хорошо известных» конфигураций, которые имеют смысл и часто называются в криптографии «наборами шифров» (ciphersuite), вместо допущения произвольных сочетаний вариантов конфигурации, которые могут взаимодействовать опасным способом. В настоящее время имеется

согласие в том, что такой же подход следует применять для комбинаций криптографических алгоритмов, а «заведомо хорошие» пары следует указывать явно (explicit composite) вместо разрешения выбирать произвольные комбинации из двух криптографических алгоритмов (generic composite).

Такие же соображения применимы к использованию нескольких сертификатов для доставки пары связанных ключей одного элемента (субъекта). Точный способ управления двумя сертификатами для предотвращения некоторых из упомянутых выше проблем все ещё является предметом исследований. Использование двух сертификатов упрощает инструментарий сертификации и делает его более понятным, но в конечном итоге просто переносит проблемы (требования использовать оба сертификата как пару, передавать две отдельных подписи и проверять их) на уровень управления сертификатами, где надёжное решение этих проблем может оказаться затруднительным.

Предложена по меньшей мере одна схема, позволяющая паре сертификатов существовать как единый сертификат при выдаче и управлении с динамическим расщеплением на отдельные части при необходимости [ENC-PAIR-CERTS].

13.3.3. Повторное использование ключей в гибридных схемах

Важным вопросом безопасности, особенно при использовании гибридных ключей подписи, и в меньшей степени при использовании гибридных ключей KEM, является повторное использование ключей. В традиционной криптографии могут возникать проблемы при так называемых кросс-протокольных атаках, где один ключ может использоваться несколькими протоколами, например, для подписи в согласовании TLS и подписи почтовых сообщений S/MIME. Хотя неоднократное использование ключей в рамках одного протокола (например, в нескольких сертификатах S/MIME для одного пользователя) не рекомендуется, в общем случае это не критично для безопасности. Однако повторное использование ключей становится большой проблемой безопасности в гибридных схемах.

Рассмотрим гибридный ключ {RSA, ML-DSA}, где ключ RSA присутствует также в сертификате с одним алгоритмом. В таком случае атакующий может выполнить «атаку с вырезанием данных», где он берет часть данных, подписанных с ключом {RSA, ML-DSA}, удаляет подпись ML-DSA и представляет данные, как будто они предназначались лишь для сертификата RSA. Это ведёт к набору определений безопасности, называемых «свойствами неделимости» (non-separability properties), которые относятся к стойкости системы к атакам различной сложности с понижениям/вырезанием [HYBRID-SIG-SPECT]. Поэтому разработчикам рекомендуется либо повторно использовать гибридный ключ целиком, либо генерировать новый свежий ключ для всех ключей-компонентов при каждом использовании и не брать имеющийся ключ для повторного использования в качестве компонента гибридного ключа.

13.3.4. Направления будущих исследований

Для многих аспектов гибридной криптографии исследования ещё продолжаются. Рабочая группа IETF LAMPS активно исследует свойства безопасности комбинаций и будущие стандарты будут отражать формирующийся консенсус по этим вопросам.

14. Влияние на устройства и сети с ограничениями

В алгоритмах PQC в общем случае размеры ключей, шифротекста и подписей превышают их размеры в традиционных алгоритмах с открытым ключом. Это особенно важно для устройств с ограниченными возможностями, работающих при ограниченных скоростях. В сфере IoT эти ограничения исторически приводили к значительным усилиям IETF (например, в рабочих группах LAKE и CoRE) по адаптации протоколов защиты к средам с ограниченными ресурсами.

По мере перехода на PQC эти среды столкнутся с аналогичными проблемами. Больший размер сообщений может увеличить продолжительность согласования и потребовать фрагментации. В IETF продолжается работа по исследованию возможностей внедрения PQC в устройства с ограниченными возможностями [CONSTRAIN-DEV-PCQ].

15. Вопросы безопасности

15.1. Криптоанализ

В традиционном криптоанализе используются слабые места в устройстве алгоритмов, математические уязвимости или недостатки реализаций, которыми можно воспользоваться с помощью классического (не квантового) оборудования, тогда как квантовый криптоанализ основан на возможностях CRQC для более эффективного решения конкретных математических проблем. Атаки по квантовым побочным каналам являются ещё одной формой квантового криптоанализа. В таких атаках находящееся под угрозой устройство напрямую соединено с квантовым компьютером, который передаёт спутанные (entangled) или наложенные (superimposed - суперпозиция) потоки данных для использования оборудования с недостаточной защитой от побочных каналов. Оба подхода представляют угрозу безопасности криптографических алгоритмов, включая используемые в PQC. Крайне важно разработать и внедрить новые криптографические алгоритмы, устойчивые к таким угрозам, чтобы обеспечить долгосрочную защиту в условиях развития методов криптоанализа.

Недавние атаки по побочным каналам с анализом энергопотребления на основе глубокого обучения показали, что нужна осторожность при аппаратной реализации требуемых алгоритмов PQC. Две из последних работ включают атаки на ML-KEM [KyberSide] и Saber [SaberSide]. Развивающаяся картина угроз указывает, что криптография на основе решёток действительно более уязвима к атакам по побочным каналам, как в [SideCh] и [LatticeSide]. Поэтому были предложены методы смягчения таких атак [Mitigate1], [Mitigate2], [Mitigate3].

15.2. Гибкость криптографии

Криптографическая гибкость рекомендуется как для классического, так и для квантового криптоанализа, поскольку она позволяет организации приспособиться к возникающим угрозам, внедрить более сильные алгоритмы, соблюдать стандарты и планировать долгосрочную защиту в условия развития методов криптоанализа и появления CRQC.

Имеется несколько схем PQC, которые требуется протестировать, и эксперты всего мира стремятся найти наилучшие решения. В настоящее время готовятся первые стандарты, которые подготовят внедрение PQC. Это имеет первостепенное значение и является призывом к незамедлительным действиям организаций, ведомств и предприятий

по оценке их криптографической гибкости, сложности внедрения PQC в их продукцию, процессы и системы, а также разработке планов перехода, обеспечивающих достижение целей в сфере безопасности.

Важным и зачастую упускаемым шагом в достижении криптографической гибкости является ведение криптографического реестра. Современные программные стеки включают криптографию во множестве мест, что затрудняет выявление всех экземпляров. Поэтому криптографическая гибкость и поддержка реестра имеют две основных формы. Во-первых, разработчикам приложений, ответственным за поддержку, следует активно искать в программах экземпляры жёстко закодированных криптографических алгоритмов. По возможности следует выбирать алгоритмы динамически в зависимости от конфигурации приложения. Во-вторых, администраторам, ответственным за политику, и командам проверки на соответствие следует обращать пристальное внимание на все случаи использования приложением конфигураций с криптографией. Управление такими экземплярами следует выполнять на основе письменно зафиксированной политики организации или автоматизированной системы исполнения правил политики.

Имеется множество коммерческих решений для обнаружения жёстко закодированных криптографических алгоритмов, а также поддержки плоскости управления криптографической политикой в корпоративной и производственной среде.

15.3. Фрагментация юрисдикций

Заслуживает внимания ещё одно возможное применение гибридных схем, хотя оно и не связано напрямую с PQC. Это применение гибридных решений при организации криптографических соединений между юрисдикциями. Традиционная криптография уже разделена по юрисдикциям. Следует отметить, что хотя в большинстве юрисдикций поддерживается ECDH, в США предпочтение отдано кривым NIST, а в Германии - кривым Brainpool. Китай, Россия и другие юрисдикции имеют свои национальные стандарты криптографии. Маловероятно, что ситуация с фрагментированием стандартов криптографии изменится с появлением PQC. Если гибридные схемы в режиме AND (И) будут стандартизованы по отмеченным выше причинам, можно будет предположить их использование для создания шифров, в которых одна криптографическая операция будет соответствовать криптографическим требованиям обеих сторон.

15.4. Гибридный обмен ключами и подписи в процессе перехода

Пост-квантовые алгоритмы, выбранные для стандартизации, являются сравнительно новыми и не изучены так же глубоко, как традиционные алгоритмы. Реализации PQC также будут новыми и вероятность ошибок в них будет больше, чем в проверенных практикой криптографических реализациях, на которые полагаются сегодня. Кроме того, при некоторых внедрениях может потребоваться сохранение традиционных алгоритмов по требованиям регуляторов, например, соответствие FIPS [SP-800-56C] или PCI (Payment Card Industry) [PCI]. Рекомендуется использовать гибридный обмен ключами для улучшения защиты от атак HNDL. Кроме того, гибридные подписи оставят время для реагирования в случае сообщений о разрушительной атаке на один из алгоритмов без полного отказа от традиционных криптосистем.

При гибридном обмене выполняется сразу (параллельно) классический и пост-квантовый обмен ключами. Это обеспечивает избыточность защиты на случай уязвимостей в алгоритмах PQC с постепенным ростом доверия к ним, а в решениях, совместимых с прежними версиями, обеспечит постепенное внедрение без потери совместимости с имеющимися системами. Например, в TLS 1.3 гибридный обмен ключами может сочетать широко распространённый классический алгоритм, такой как X25519, с пост-квантовым алгоритмом, таким как ML-KEM. Это позволит унаследованным клиентам продолжать использование классического обмена ключами, давая обновлённым клиентам возможность применять гибридный обмен. Гибридные решения с распределением издержек (overhead-spreading) нацелены на снижение издержек PQ. Например, подходы, подобные описанным в [PQ-MLS], снижают стоимость PQ за счёт селективного обновления PQ в процессах обмена ключами, позволяя системам обеспечить баланс между эффективностью и безопасностью. Такая стратегия обеспечивает защищённый пост-квантовый канал при сохранении управляемости для издержек, что делает её особо подходящей для сред с ограниченными возможностями.

Хотя некоторые варианты гибридного обмена ключами увеличивают издержки на вычисления и расход пропускной способности, влияние традиционных алгоритмов обмена ключами (например, размер ключей) обычно мало, что позволяет в большинстве систем сохранить управляемость ростом издержек. В средах со значительными ограничениями протоколы гибридного обмена ключами могут не подойти из-за высоких требований к ресурсам по сравнению с чисто традиционными или пост-квантовыми подходами. Однако некоторые варианты гибридного обмена ключами распределяют издержки PQC, что делает такие варианты более подходящими для сред с ограничениями. Выбор варианта гибридного обмена ключами зависит от требований конкретной системы и варианта применения.

15.5. Привязка к шифротексту для KEM и DH

Шифротекст, генерируемый KEM, может быть не связан напрямую с созданным общим секретом. Механизмы KEM позволяют использовать несколько шифротекстов для инкапсуляции одного и того же общего секрета, что обеспечивает гибкость управления ключами без строгого однозначного сопоставления шифротекста с общим секретом. Это позволяет неоднократно использовать секрет для разных получателей, сессий и операционных контекстов, что упрощает распространение ключей и сокращает вычислительные издержки. Криптографические схемы, подобные DH, связывают открытый ключ с выведенным общим секретом, что означает новый общий секрет при любом изменении открытого ключа.

16. Взаимодействие с IANA

Этот документ не требует действия IANA.

17. Дополнительная литература и ресурсы

Хорошей книгой по современной криптографии является «Serious Cryptography, 2nd Edition» Жана-Филиппа Омассона (Jean-Philippe Aumasson) [Serious-Crypt].

Открытый проект Open Quantum Safe (OQS) [OQS] предоставляет исходный код для поддержки перехода к квантово-стойкой криптографии.

Рабочая группа IETF PQUIP [PQUIP-WG] ведёт список работ по связанным с PQC протоколам в рамках IETF.

18. Литература

18.1. Нормативные документы

[ClassicMcEliece] "Classic McEliece", <https://classic.mceliece.org/>.

[FN-DSA] "FALCON: Fast Fourier lattice-based compact signatures over NTRU", <https://falcon-sign.info/>.

[FrodoKEM] "FrodoKEM", <https://frodokem.org/>.

[Grovers] Grover, L. K., "A fast quantum mechanical algorithm for database search", STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, pp. 212-219, DOI 10.1145/237814.237866, 1 July 1996, <https://dl.acm.org/doi/10.1145/237814.237866>.

[ML-DSA] NIST, "Module-Lattice-Based Digital Signature Standard", NIST FIPS 204, DOI 10.6028/NIST.FIPS.204, August 2024, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf>.

[ML-KEM] NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard", NIST FIPS 203, DOI 10.6028/nist.fips.203, August 2024, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf>.

[NTRU] "NTRU", <https://ntru.org/index.shtml>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, DOI 10.17487/RFC6090, February 2011, <https://www.rfc-editor.org/info/rfc6090>.

[RFC8235] Hao, F., Ed., "Schnorr Non-interactive Zero-Knowledge Proof", RFC 8235, DOI 10.17487/RFC8235, September 2017, <https://www.rfc-editor.org/info/rfc8235>.

[RFC8391] Huelsing, A., Butin, D., Gazdag, S., Rijneveld, J., and A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme", RFC 8391, DOI 10.17487/RFC8391, May 2018, <https://www.rfc-editor.org/info/rfc8391>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8554] McGrew, D., Curcio, M., and S. Fluhrer, "Leighton-Micali Hash-Based Signatures", RFC 8554, DOI 10.17487/RFC8554, April 2019, <https://www.rfc-editor.org/info/rfc8554>.

[RFC9180] Barnes, R., Bhargavan, K., Lipp, B., and C. Wood, "Hybrid Public Key Encryption", RFC 9180, DOI 10.17487/RFC9180, February 2022, <https://www.rfc-editor.org/info/rfc9180>.

[RFC9242] Smyslov, V., "Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9242, DOI 10.17487/RFC9242, May 2022, <https://www.rfc-editor.org/info/rfc9242>.

[RFC9370] Tjhai, CJ., Tomlinson, M., Bartlett, G., Fluhrer, S., Van Geest, D., Garcia-Morchon, O., and V. Smyslov, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9370, DOI 10.17487/RFC9370, May 2023, <https://www.rfc-editor.org/info/rfc9370>.

[RFC9881] Massimo, J., Kampanakis, P., Turner, S., and B. E. Westerbaan, "Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", RFC 9881, DOI 10.17487/RFC9881, October 2025, <https://www.rfc-editor.org/info/rfc9881>.

[RSA] Rivest, R. L., Shamir, A., and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, vol. 21, no. 2, pp. 120-126, DOI 10.1145/359340.359342, February 1978, <https://dl.acm.org/doi/pdf/10.1145/359340.359342>.

[Shors] Shor, P., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", arXiv:quant-ph/9508027v2, 25 January 1996, <https://arxiv.org/pdf/quant-ph/9508027>.

[SLH-DSA] NIST, "Stateless Hash-Based Digital Signature Standard", NIST FIPS 205, DOI 10.6028/NIST.FIPS.205, August 2024, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf>.

18.2. Дополнительная литература

[AddSig] NIST, "Post-Quantum Cryptography: Additional Digital Signature Schemes", <https://csrc.nist.gov/Projects/pqc-dig-sig/standardization>.

[ANSSI] ANSSI, "ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)", 21 December 2023, <https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf>.

[BBS-SIG-SCHEME] Looker, T., Kalos, V., Whitehead, A., and M. Lodder, "The BBS Signature Scheme", Work in Progress, Internet-Draft, draft-irtf-cfrg-bbs-signatures-10, 8 January 2026, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-bbs-signatures-10>.

[BHK09] Bellare, M., Hofheinz, D., and E. Kiltz, "Subtleties in the Definition of IND-CCA: When and How Should Challenge-Decryption be Disallowed?", Cryptology ePrint Archive, Paper 2009/418, 2009, <https://eprint.iacr.org/2009/418>.

[BIKE] "BIKE", <https://bikesuite.org/>.

[BPQS] Chalkias, K., Brown, J., Hearn, M., Lillehagen, T., Nitto, I., and T. Schroeter, "Blockchained Post-Quantum Signatures", Cryptology ePrint Archive, Paper 2018/658, <https://eprint.iacr.org/2018/658>.

[BSI-PQC] BSI, "Quantum-safe cryptography - fundamentals, current developments and recommendations", 18 May 2022, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626>.

[Cloudflare] Westerbaan, B., "NIST's pleasant post-quantum surprise", Cloudflare Blog, 8 July 2022, <https://blog.cloudflare.com/nist-post-quantum-surprise/>.

[CNSA2-0] NSA, "Announcing the Commercial National Security Algorithm Suite 2.0", September 2022, <https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF>.

[CONSTRAIN-DEV-PCQ] Reddy.K, T., Wing, D., Salter, B., and K. Kwiatkowski, "Adapting Constrained Devices for Post-Quantum Cryptography", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-hsm-constrained-05, 1 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-hsm-constrained-05>.

[CRQCThreat] Jaques, S., "Landscape of Quantum Computing", <https://sam-jaques.appspot.com/quantum_landscape_2024>.

[CS01] Cramer, R. and V. Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack", Cryptology ePrint Archive, Paper 2001/108, 2001, <https://eprint.iacr.org/2001/108>.

[ENC-PAIR-CERTS] Bonnell, C., Gray, J., Hook, D., Okubo, T., and M. Ounsworth, "A Mechanism for Encoding Differences in Paired Certificates", Work in Progress, Internet-Draft, draft-bonnell-lamps-chameleon-certs-07, 18 October 2025, <https://datatracker.ietf.org/doc/html/draft-bonnell-lamps-chameleon-certs-07>.

[GMR88] Goldwasser, S., Micali, S., and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks", SIAM Journal on Computing, vol. 17, no. 2, pp. 281-308, DOI 10.1137/0217017, April 1988, <https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Digital%20Signatures/A_Digital_Signature_Scheme_Secure_Against_Adaptive_Chosen-Message_Attack.pdf>.

[Grover-Search] Zalka, C., "Grover's quantum searching algorithm is optimal", Physical Review A, vol. 60, no. 4, pp. 2746-2751, DOI 10.1103/PhysRevA.60.2746, October 1999, <https://link.aps.org/doi/10.1103/PhysRevA.60.2746>.

[HQC] "HQC", <http://pqc-hqc.org/>.

[HYBRID-SIG-SPECT] Bindel, N., Hale, B., Connolly, D., and F. D, "Hybrid signature spectrums", Work in Progress, Internet-Draft, draft-ietf-pquip-hybrid-signature-spectrums-07, 20 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-hybrid-signature-spectrums-07>.

[KEEPINGUP] Cremers, C., Dax, A., and N. Medinger, "Keeping Up with the KEMs: Stronger Security Notions for KEMs and automated analysis of KEM-based protocols", Cryptology ePrint Archive, Paper 2023/1933, 2023, <https://eprint.iacr.org/2023/1933>.

[KEM-COMBINER] Ounsworth, M., Wussler, A., and S. Kousidis, "Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)", Work in Progress, Internet-Draft, draft-ounsworth-cfrg-kem-combiners-05, 31 January 2024, <https://datatracker.ietf.org/doc/html/draft-ounsworth-cfrg-kem-combiners-05>.

[KyberSide] Ji, Y., Wang, R., Ngo, K., Dubrova, E., and L. Backlund, "A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber", Cryptology ePrint Archive, Paper 2022/1452, 2022, <https://eprint.iacr.org/2022/1452>.

[LattFail1] D'Anvers, J., Guo, Q., Johansson, T., Nilsson, A., Vercauteren, F., and I. Verbauwhede, "Decryption Failure Attacks on IND-CCA Secure Lattice-Based Schemes", Public-Key Cryptography - PKC 2019, Lecture Notes in Computer Science, vol. 11443, pp. 565-598, DOI 10.1007/978-3-030-17259-6_19, 6 April 2019, <https://link.springer.com/chapter/10.1007/978-3-030-17259-6_19>.

[LattFail2] D'Anvers, J., Rossi, M., and F. Virdia, "(One) Failure Is Not an Option: Bootstrapping the Search for Failures in Lattice-Based Encryption Schemes", Advances in Cryptology - EUROCRYPT 2020, Lecture Notes in Computer Science, vol. 12107, pp. 3-33, DOI 10.1007/978-3-030-45727-3_1, 1 May 2020, <https://link.springer.com/chapter/10.1007/978-3-030-45727-3_1>.

[LatticeSide] Ravi, P., Roy, S. S., Chattopadhyay, A., and S. Bhasin, "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEM schemes", Cryptology ePrint Archive, Paper 2019/948, 2019, <https://eprint.iacr.org/2019/948>.

[LIBOQS] "LibOQS - Open Quantum Safe", commit 97f6b86, November 2025, <https://github.com/open-quantum-safe/liboqs>.

[Lyu09] Lyubashevsky, V., "Fiat-Shamir With Aborts: Applications to Lattice and Factoring-Based Signatures", ASIACRYPT 2009, <https://www.iacr.org/archive/asiacrypt2009/59120596/59120596.pdf>.

[Mitigate1] Hoffmann, C., Libert, B., Momin, C., Peters, T., and F. Standaert, "POLKA: Towards Leakage-Resistant Post-Quantum CCA-Secure Public Key Encryption", Cryptology ePrint Archive, Paper 2022/873, 2022, <https://eprint.iacr.org/2022/873>.

[Mitigate2] Tsai, T., Huang, S., Tseng, Y., Chuang, Y., and Y. Hung, "Leakage-Resilient Certificate-Based Authenticated Key Exchange Protocol", IEEE Open Journal of the Computer Society, vol. 3, pp. 137-148, DOI 10.1109/OJCS.2022.3198073, 2022, <https://ieeexplore.ieee.org/document/9855226>.

[Mitigate3] Azouaoui, M., Kuzovkova, Y., Schneider, T., and C. V. Vredendaal, "Post-Quantum Authenticated Encryption against Chosen-Ciphertext Side-Channel Attacks", Cryptology ePrint Archive, Paper 2022/916, 2022, <https://eprint.iacr.org/2022/916>.

[ML-DSA-X.509] Ounsworth, M., Gray, J., Pala, M., Klaußner, J., and S. Fluhrer, "Composite Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for use in X.509 Public Key Infrastructure", Work in Progress, Internet-Draft, draft-ietf-lamps-pq-composite-sigs-19, 21 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-pq-composite-sigs-19>.

[NIST] NIST, "Post-Quantum Cryptography Standardization", <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization>.

[NISTFINAL] NIST, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards", 13 August 2024, <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.

[OQS] "Open Quantum Safe Project", <https://openquantumsafe.org/>.

[PCI] PCI Security Standards Council, "Payment Card Industry Data Security Standard", PCI DSS: v4.0.1, <https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf>.

[PQ-HPKE] Barnes, R. and D. Connolly, "Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE", Work in Progress, Internet-Draft, draft-ietf-hpke-pq-04, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-pq-04>.

[PQ-KEM] Connolly, D., Barnes, R., and P. Grubbs, "Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-hybrid-kems-11, 7 May 2026, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hybrid-kems-11>.

[PQ-MLS] Tian, X., Hale, B., Mularczyk, M., and J. Alwen, "Amortized PQ MLS Combiner", Work in Progress, Internet-Draft, draft-ietf-mls-combiner-02, 22 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-mls-combiner-02>.

[PQCAPI] NIST, "PQC - API notes", <https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/example-files/api-notes.pdf>.

[PQRSA] Bernstein, D. J., Heninger, N., Lou, P., and L. Valenta, "Post-quantum RSA", 19 April 2017, <https://cr.yp.to/papers/pqrsa-20170419.pdf>.

[PQUIP-WG] IETF, "Post-Quantum Use In Protocols (pquip)", <https://datatracker.ietf.org/group/pquip/documents/>.

[QC-DNS] Hoffman, P., "Quantum Computing and the DNS", ICANN Office of the Chief Technology Officer, OCTO-031v2, 22 April 2024, <https://www.icann.org/octo-031-en.pdf>.

[QuantSide] Xu, C., Erata, F., and J. Szefer, "Exploration of Quantum Computer Power Side-Channels", arXiv:2304.03315v2, 9 May 2023, <https://arxiv.org/pdf/2304.03315>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC9528] Selander, G., Preuß Mattsson, J., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", RFC 9528, DOI 10.17487/RFC9528, March 2024, <https://www.rfc-editor.org/info/rfc9528>.

[RFC9763] Becker, A., Guthrie, R., and M. Jenkins, "Related Certificates for Use in Multiple Authentications within a Protocol", RFC 9763, DOI 10.17487/RFC9763, June 2025, <https://www.rfc-editor.org/info/rfc9763>.

[RFC9794] Driscoll, F., Parsons, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", RFC 9794, DOI 10.17487/RFC9794, June 2025, <https://www.rfc-editor.org/info/rfc9794>.

[RFC9814] Housley, R., Fluhrer, S., Kampanakis, P., and B. Westerbaan, "Use of the SLH-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)", RFC 9814, DOI 10.17487/RFC9814, July 2025, <https://www.rfc-editor.org/info/rfc9814>.

[RFC9941] Friedl, M., Mojzis, J., and S. Josefsson, "Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512", RFC 9941, DOI 10.17487/RFC9941, April 2026, <https://www.rfc-editor.org/info/rfc9941>.

[RSA10SC] QuintessenceLabs, "Breaking RSA Encryption - an Update on the State-of-the-Art", 13 June 2019, <https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art>.

[RSA8HRS] Gidney, C. and M. Ekera, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", arXiv:1905.09749v3, 13 April 2021, <https://arxiv.org/abs/1905.09749>.

[RSAShor] Beauregard, S., "Circuit for Shor's algorithm using 2n+3 qubits", arXiv:quant-ph/0205095v3, 21 February 2003, <https://arxiv.org/pdf/quant-ph/0205095.pdf>.

[SaberSide] Ngo, K., Dubrova, E., and T. Johansson, "A side-channel attack on a masked and shuffled software implementation of Saber", Journal of Cryptographic Engineering, vol. 13, pp. 443-460, DOI 10.1007/s13389-023-00315-3, 25 April 2023, <https://link.springer.com/article/10.1007/s13389-023-00315-3>.

[Serious-Crypt] Aumasson, J., "Serious Cryptography, 2nd Edition", ISBN 9781718503847, August 2024.

[SideCh] Ngo, K., Wang, R., Dubrova, E., and N. Paulsrud, "Side-Channel Attacks on Lattice-Based KEMs Are Not Prevented by Higher-Order Masking", Cryptology ePrint Archive, Paper 2022/919, 2022, <https://eprint.iacr.org/2022/919>.

[SP-1800-38C] Newhouse, W., Souppaya, M., Barke, W., Brown, C., Kampanakis, P., Goodman, J., Prat, J., Larrieu, R., Gray, J., Ounsworth, M., Viana, C., Gong, H. L. V., Kwiatkowsk, K., Hu, A., Burns, R., Paquin, C., Gilbert, J., Scinta, G., Kim, E., and V. Krumme, "Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards, Volume C: Quantum-Resistant Cryptography Technology Interoperability and Performance Report", Preliminary Draft, NIST SP 1800-38C, December 2023, <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf>.

[SP-800-56C] Barker, E., Chen, L., and R. Davis, "Recommendation for Key-Derivation Methods in Key-Establishment Schemes", NIST SP 800-56Cr2, DOI 10.6028/NIST.SP.800-56Cr2, August 2020, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf>.

[Threat-Report] Mosca, M. and M. Piani, "Quantum Threat Timeline Report 2020", Global Risk Institute, 27 January 2021, <https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/>.

[TLS-HYB-KEY-EXCH] Stebila, D., Fluhrer, S., and S. Gueron, "Hybrid key exchange in TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-hybrid-design-16, 7 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design-16>.

[X-WING] Connolly, D., Schwabe, P., and B. Westerbaan, "X-Wing: general-purpose hybrid post-quantum KEM", Work in Progress, Internet-Draft, draft-connolly-cfrg-xwing-kem-10, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-connolly-cfrg-xwing-kem-10>.

Благодарности

В этом документе используется текст из более раннего Internet-Draft, созданного Paul Hoffman. Спасибо Dan Wing, Florence D, Thom Wiggers, Sophia Grundner-Culemann, Panos Kampanakis, Ben S, Sofia Celi, Melchior Aelmans, Falko Strenzke, Deirdre Connolly, Hani Ezzadeen, Britta Hale, Scott Rose, Hilarie Orman, Thomas Fossati, Roman Danyliw, Mike Bishop, Mališa Vučinić, Éric Vyncke, Deb Cooley, Dirk Von Hugo, Daniel Van Geest за обсуждение, рецензии и комментарии.

Авторы также выражают признательность Kris Kwiatkowski за вклад в этот документ.

Адреса авторов

Aritra Banerjee
Nokia
London
United Kingdom
Email: aritra.banerjee@nokia.com

Tirumaleswar Reddy.K
Nokia
Bangalore
Karnataka
India
Email: k.tirumaleswar_reddy@nokia.com

Dimitrios Schoinianakis
Nokia
Athens
Greece
Email: dimitrios.schoinianakis@nokia-bell-labs.com

Timothy Hollebeek
DigiCert
Pittsburgh, PA
United States of America
Email: tim.hollebeek@digicert.com

Mike Ounsworth
Entrust Limited
2500 Solandt Road, Suite 100
Ottawa, Ontario K2K 3G5
Canada
Email: mike@ounsworth.ca

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru