Internet Engineering Task Force (IETF)
Request for Comments: 9794
Category: Informational
ISSN: 2070-1721

F. Driscoll
M. Parsons
UK National Cyber Security Centre
B. Hale
Naval Postgraduate School

June 2025

Terminology for Post-Quantum Traditional Hybrid Schemes

Терминология для пост-квантовых традиционных гибридных схем

Аннотация

Одним из аспектов перехода к пост-квантовым алгоритмам в криптографических протоколах является разработка гибридных схем, включающих пост-квантовые и традиционные асимметричные алгоритмы. Этот документ определяет терминологию для таких схем. Документ предназначен для использования в качестве справочного материала и, как надеются авторы, для обеспечения согласованности и ясности в различных протоколах, стандартах и организациях.

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/rfc9794.

Оглавление

1. Введение

Математические задачи целочисленной факторизации (разложения на сомножители) и дискретного логарифмирования над конечными полями и эллиптическими кривыми лежат в основе большинства асимметричных алгоритмов, применяемых для организации ключей и цифровых подписей в Internet. Эти задачи и основанные на них алгоритмы будут уязвимы для атак с использованием алгоритма Шора (Shor) на достаточно больших квантовых компьютерах общего назначения, называемых криптографически значимыми квантовыми компьютерами (Cryptographically Relevant Quantum Computer или CRQC). Текущие прогнозы варьируются в зависимости от возможности появления таких устройств. Однако необходимо предвидеть их и готовиться к защите от такого развития событий. Данные, зашифрованные сегодня (в 2025 г.) с применением уязвимых для квантовых компьютеров алгоритмов, могут быть сохранены для расшифровки в будущем с помощью CRQC. Алгоритмы подписи в продукции, которая предположительно будет использоваться в течение многих лет и которую невозможно заменить или обновить, также подвержена риску, если CRQC будут созданы в течение срока использования такой продукции.

Текущая реакция на возможную разработку CRQC включает модификацию разработанных (или стандартизированных) протоколов использования асимметричных алгоритмов, которые предназначены для защиты как от квантовых, так и от современных классических компьютеров. Эти алгоритмы называют пост-квантовыми, а алгоритмы, основанные на целочисленной факторизации, дискретном логарифмировании над конечным полем или эллиптическими кривыми, называют традиционными криптоалгоритмами. В этом документе они также называются просто традиционными.

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

На момент публикации документа термин post-quantum обычно применялся для криптографических алгоритмов, предназначенных для защиты от злоумышленников с доступом к CRQC. Пост-квантовые алгоритмы называют также квантово-стойкими (quantum-resistant) и квантово-безопасными (quantum-safe). У каждого из терминов имеются свои достоинства, например, некоторые предпочитают использовать quantum-resistant или quantum-safe для явного указания того, что эти алгоритмы предназначены для защиты от квантовых компьютеров. Другие не согласны с этим и предпочитают использовать термин post-quantum на случай, обнаружения уязвимостей, из-за которых термины quantum-resistant и quantum-safe могут ввести в заблуждение. Кто-то предпочитает напрямую ссылаться на алгоритм Шора или иную математическую проблему, используемую для предотвращения атак. Термин пост-квантовая криптография (Post-Quantum Cryptography или PQC) широко распространён в сообществе криптографов, поэтому он будет применяться и в этом документе, равно как термин «традиционный алгоритм», который на момент публикации широко использовался, хотя некоторые предпочитают другие термины, включая классический, доквантовый, квантово-уязвимый.

Для снижения рисков может потребоваться использование протоколов с обоими типами алгоритмов в процессе перехода от традиционных алгоритмов к пост-квантовым или в качестве общего решения. Когда риск при внедрении новых алгоритмов превышает допустимый для варианта использования порог, разработчики могут объединить пост-квантовые алгоритмы с традиционными с целью добавления защиты от злоумышленников, использующих CRQC, к защитным свойствам традиционных алгоритмов. Можно также реализовать пост-квантовые алгоритмы наряду с традиционными для упрощения перехода от экосистемы, где применяются лишь традиционные алгоритмы, к экосистеме, основанной лишь на пост-квантовых. Примеры решений с обоими типами алгоритмов включают [RFC9370], [HYBRID-TLS], [COMPOSITE-KEM], [RFC9763].

Схемы, сочетающие пост-квантовые и классические алгоритмы для организации ключей и создания цифровых подписей, называют гибридными, например:

- Национальный институт стандартов и технологии США (National Institute of Standards and Technology или NIST) определяет гибридную организацию ключей как: «схему, являющуюся комбинацией двух и более компонентов, которые сами по себе являются криптографическими схемами организации ключей» [NIST_PQC_FAQ].
- Европейский институт телекоммуникационных стандартов (European Telecommunications Standards Institute или ETSI) определяет гибридный обмен ключами как: «конструкцию, объединяющую традиционный обмен ключами ... с пост-квантовым обменом ключами … в единый обмен ключами» [ETSI_TS103774].

Термин «гибридный» также применяется в криптографии для схем шифрования, сочетающих асимметричные и симметричные алгоритмы [RFC9180], поэтому его использование в пост-квантовом контексте ведёт к перегрузке и риску путаницы. Однако этот термин хорошо известен в сообществе пост-квантовой криптографии (PQC), поэтому попытка отказа от него в PQC может привести к избыточному определению того же понятия и отсутствию ясности. На момент публикации термин «гибридный» обычно применялся для схем, объединяющих пост-квантовые и традиционные алгоритмы, и в этом смысле применяется в документе, хотя имеются альтернативные предпочтения, такие как double-algorithm и multi-algorithm.

Этот документ предоставляет терминологию для описания конструкций, сочетающих пост-квантовые и традиционные алгоритмы. Конкретные решения, позволяющие применять несколько асимметричных алгоритмов в криптографических схемах, могут быть более общими, разрешая использовать исключительно традиционные или исключительно пост-квантовые алгоритмы. Там, где это уместно, обращается внимание на сочетания пост-квантовых и традиционных алгоритмов, поскольку именно им посвящено множество работ в IETF. Этот документ предназначен быть справочником по терминологии для других документов с целью обеспечения ясности и согласованности между протоколами, стандартами и организациями. Кроме того, документ призван сократить недопонимание в отношении использования термина «гибрид» и определить единый язык для различных типов пост-квантовых и традиционных гибридных конструкций.

В этом документе термин «криптографический алгоритм» определяется как в [NIST_SP_800-152] - «чётко заданная процедура расчётов, принимающая на входе переменные данные, зачастую включающие криптографические ключи, и выдающая данные на выходе». Примеры алгоритмов включают RSA, метод Диффи-Хеллмана с эллиптической кривой (Elliptic Curve Diffie-Hellman или ECDH), механизм инкапсуляции ключей на основе модульных решёток (Module-Lattice-Based Key-Encapsulation Mechanism или ML-KEM, ранее называвшийся Kyber), алгоритм цифровой подписи на основе модульных решёток (Module-Lattice-Based Digital Signature Algorithm или ML-DSA, ранее называвшийся Dilithium). Выражение «криптографическая схема» применяется для конструкций, использующих криптографический алгоритм или группу таких алгоритмов для достижения определённого криптографического результата, например, согласования ключей. Криптографическая схема может состоять из ряда функций. Например, механизм инкапсуляции ключей (Key Encapsulation Mechanism или KEM) - это криптографическая схема, состоящая из трёх функций - генерации, инкапсуляции и декапсуляции ключа. Криптографический протокол включает одну или несколько криптографических схем. Например, TLS [RFC8446] является криптографическим протоколом, включающим схемы согласования ключей, шифрования уровня записи и проверки подлинности сервера.

2. Примитивы

В этом разделе определяются термины, относящиеся к криптографическим алгоритмам и гибридным конструкциям для криптографических схем.

Traditional asymmetric cryptographic algorithm - традиционный асимметричный криптоалгоритм

Асимметричный криптографический алгоритм, основанный на разложении целых чисел на сомножители (факторизации), дискретном логарифмировании над конечным полем или эллиптической кривой, а также иных математических задачах. Связанные с этим математические задачи могут быть решены путём разложения целого числа на сомножители, нахождения дискретного логарифма над конечным полем или дискретного логарифмирования над эллиптической кривой.

Там, где невелик риск возникновения путаницы, традиционные криптографические алгоритмы могут также называться просто традиционными алгоритмами для краткости. Традиционные алгоритмы также могут называться классическими или общепринятыми (conventional).

Post-quantum asymmetric cryptographic algorithm - пост-квантовый криптоалгоритм

Асимметричный криптографический алгоритм, предназначенный для защиты от атак с применением как квантовых, так и классических компьютеров. Когда вероятность путаницы невелика, пост-квантовые криптографические алгоритмы могут называться просто пост-квантовыми алгоритмами (post-quantum algorithms). Эти алгоритмы называют также квантово-стойкими (quantum-resistant) и квантово-безопасными (quantum-safe).

Как и в любой криптографии, остаётся вероятность квантовых или классических атак на пост-квантовые алгоритмы. Поэтому нельзя считать, что алгоритмы невозможно скомпрометировать лишь потому, что они предназначены для пост-квантовой криптографии. Если будет найдена атака на пост-квантовый алгоритм, тот все равно обычно будет называться пост-квантовым, поскольку был разработан для защиты от злоумышленников с доступом к CRQC и обозначение относится к разработанным или желаемым свойствам.

Может существовать множество криптографических конструкций, не являющихся ни пост-квантовыми, ни традиционными асимметричными алгоритмами в соответствии с приведёнными выше определениями. Эти вопросы выходят за рамки данного документа.

Component asymmetric algorithm - асимметричный алгоритм-компонент

Каждый криптографический алгоритм, являющийся частью криптографической схемы.

Асимметричный алгоритм-компонент обрабатывает входные данные криптографической операции и создаёт криптографический вывод, который может использоваться сам по себе или совместно с другими для завершения криптографической операции. Если не возникает риска путаницы вместо термина component asymmetric algorithm применяется просто алгоритм-компонент (component algorithm), как это сделано в последующих определениях.

Single-algorithm scheme - схема с одним алгоритмом

Криптографическая схема с одним алгоритмом-компонентом.

Схема с одним алгоритмом может использовать традиционный или пост-квантовый алгоритм.

Multi-algorithm scheme - схема с несколькими алгоритмами

Криптографическая схема, включающая более одного алгоритма-компонента, где компоненты имеют общую криптографическую цель (назначение) как между собой, так и со схемой в целом. Например, схема подписи может включать несколько алгоритмов подписи, а схема шифрования с открытым ключом (Public Key Encryption или PKE) - несколько алгоритмов PKE. Компоненты могут быть традиционными, пост-квантовыми или их сочетанием.

Post-Quantum Traditional (PQ/T) hybrid scheme - гибридная схема (пост-квантовая и традиционная - PQ/T)

Схема с несколькими алгоритмами, в которой имеется хотя бы один пост-квантовый и хотя бы один традиционный алгоритм. Компоненты гибридной схемы PQ/T работают с одним входным сообщением, а их результаты используются совместно (последовательно или параллельно) для завершения криптографической операции. Целью разработки гибридных схем PQ/T является сохранение свойств безопасности, пока остаётся невзломанным хотя бы один из алгоритмов-компонентов.

PQ/T hybrid Key Encapsulation Mechanism (KEM) - гибридный механизм инкапсуляции ключей PQ/T

KEM с несколькими алгоритмами, из которых хотя бы один является пост-квантовым и хотя бы один - традиционным. В качестве алгоритмов-компонентов могут служить KEM или иные алгоритмы организации ключей.

PQ/T hybrid Public Key Encryption (PKE) - гибридный механизм шифрования с открытым ключом PQ/T

Схема PKE с несколькими алгоритмами-компонентами, из которых хотя бы один является пост-квантовым и хотя бы один - традиционным. В качестве компонентов могут служить PKE или иные алгоритмы организации ключей.

Стандартным свойством безопасности схемы PKE является неразличимость при атаках с выбранным обычным текстом (indistinguishability under chosen-plaintext attack или IND-CPA) [BDPR]. Безопасности IND-CPA недостаточно для защищённых коммуникаций при наличии активного атакующего, поэтому схемы PKE в общем случае не подходят для использования в Internet и требуются механизмы KEM, обеспечивающие неразличимость при атаках с выбранным шифротекстом (indistinguishability under chosen-ciphertext attack или IND-CCA) [BDPR].

PQ/T hybrid digital signature - гибридная цифровая подпись PQ/T

Схема цифровой подписи с несколькими алгоритмами-компонентами, из которых хотя бы один является пост-квантовым и хотя бы один - традиционным. Отметим, что имеется много способов создания гибридных схем подписи, примеры включают параллельные, составные (композитные) и вложенные подписи.

Гибридные PQ/T KEM, PQ/T PKE и цифровые подписи PQ/T являются примерами гибридных схем PQ/T.

Post-Quantum Traditional (PQ/T) hybrid composite scheme - гибридная композитная схема PQ/T

Схема с несколькими алгоритмами-компонентами, из которых хотя бы один является пост-квантовым и хотя бы один - традиционным, а композитная схема раскрывается как единый интерфейс такого же типа, как алгоритмы-компоненты. Гибридные композиты PQ/T могут называться просто композитами PQ/T (PQ/T composite). Примером такой схемы является единый алгоритм KEM, состоящий из PQ KEM и традиционного механизма KEM, результатом которого является механизм инкапсуляции ключей (KEM).

PQ/T hybrid combiner - гибридный сумматор PQ/T

Метод, принимающий несколько алгоритмов-компонентов и дающий в результате гибридную схему PQ/T.

PQ/PQ hybrid scheme - гибридная схема PQ/PQ

Схема с несколькими пост-квантовыми алгоритмами-компонентами. Определения типов гибридных схем PQ/T можно приспособить для определения гибридных схем PQ/PQ, которые состоят из нескольких компонентов, являющихся пост-квантовыми алгоритмами. Они разработаны для снижения рисков за счёт применения двух пост-квантовых алгоритмов, основанных на разных математических задачах. Некоторые предпочитают называть их схемами PQ/PQ с несколькими алгоритмами, оставляя термин «гибрид» для гибридных схем PQ/T.

Когда невелика вероятность путаницы с другими типами гибридной криптографии (см. определения в [RFC4949]) и компоненты схемы с несколькими алгоритмами могут быть пост-квантовыми или традиционными, можно пользоваться термином «гибридная схема» без указания PQ/T или PQ/PQ.

Component scheme - компонентная схема

Криптографическая схема, образующая гибридную схему PQ/T или гибридный протокол PQ/T.

3. Криптографические элементы

В этом разделе представлены термины, связанные с криптографическими элементами и их включением в гибридные схемы.

Cryptographic element - криптографический элемент

Любой тип данных (секретных или открытых), содержащий входную информацию для криптографического алгоритма или функции, составляющей криптоалгоритм. Типы криптографических элементов включают открытые и секретные ключи, обычные (plaintext) и шифрованные (ciphertext) данные, общие секреты, значения подписей.

Component cryptographic element - компонент криптографического элемента

Криптографический элемент алгоритма-компонента в схеме с несколькими алгоритмами. Например, в [HYBRID-TLS], общий ключ клиента (keyshare) содержит два компонента (открытые ключи) - по одному для пост-квантового и традиционного алгоритма.

Composite cryptographic element - композитный криптографический элемент

Криптографический элемент, содержащий несколько компонентов криптографических элементов одного типа для использования в схеме с несколькими алгоритмами, так что композитный элемент раскрывается как единый интерфейс того же типа, что и его компоненты. Например, композитный криптографический открытый ключ состоит из двух компонентов-открытых ключей.

PQ/T hybrid composite cryptographic element - композитный криптографический элемент PQ/T

Криптографический элемент, содержащий несколько компонентов криптографических элементов одного типа для использования в схеме с несколькими алгоритмами, так что композитный элемент раскрывается как единый интерфейс того же типа, что и его компоненты, из которых хотя бы один является пост-квантовым и хотя бы один - традиционным.

Cryptographic element combiner - криптографический элемент-сумматор

Метод, принимающий несколько криптографических элементов одного типа и объединяющий их в композитный криптографический элемент. Сумматор может быть простой конкатенацией, где два открытых ключа-компонента объединяются в композитный открытый ключ, как в [HYBRID-TLS], или чем-то более сложным, как dualPRF из [BINDEL].

4. Протоколы

В этом разделе представлены термины, связанные с совместным использованием в протоколах пост-квантовых и традиционных алгоритмов.

PQ/T hybrid protocol - гибридный протокол PQ/T

Протокол, использующий несколько алгоритмов-компонентов с одинаковой криптографической функциональностью, из которых хотя бы один алгоритм является пост-квантовым и хотя бы один - традиционным.

Например, гибридный протокол PQ/T для защиты конфиденциальности может использовать гибрид PQ/T KEM, такой как [HYBRID-TLS], или комбинировать выходные данные пост-квантового и традиционного механизмов KEM на уровне протокола для создания одного общего секрета, такого как в [RFC9370]. Гибридный протокол аутентификации PQ/T может обеспечивать проверку подлинности на основе гибридной схемы цифровых подписей PQ/T или включать сразу пост-квантовую и традиционную схемы подписи.

Протокол, который может согласовать применение любого традиционного или пост-квантового алгоритма, но не использует сразу оба типа, не является гибридным протоколом PQ/T. Протоколы, применяющие несколько алгоритмов-компонентов с разной функциональностью (например, пост-квантовый KEM и PSK[1]), также не являются гибридными протоколами PQ/T.

PQ/T hybrid protocol with composite key establishment - гибрид PQ/T с организацией композитного ключа

Гибридный протокол PQ/T, включающий гибридную композитную схему PQ/T для организации ключей так, что поля протокола и поток сообщений такие же, как в протоколе с использованием одного алгоритма. Например, гибридный протокол PQ/T с организацией композитного ключа может включать гибрид PQ/T KEM, такой как в [HYBRID-TLS].

PQ/T hybrid protocol with composite data authentication - гибрид PQ/T с композитной аутентификацией данных

Гибридный протокол PQ/T, включающий гибридную композитную схему PQ/T для аутентификации данных так, что поля протокола и поток сообщений такие же, как в протоколе с использованием одного алгоритма.

Например, гибридный протокол PQ/T с композитной аутентификацией данных путём использования гибридной композитной схемы цифровой подписи PQ/T с единым интерфейсом для подписи PQ и традиционной подписи.

PQ/T hybrid protocol with composite entity authentication - гибрид PQ/T с композитной аутентификацией субъекта

Гибридный протокол PQ/T, включающий гибридную композитную схему PQ/T для аутентификации субъекта так, что поля протокола и поток сообщений такие же, как в протоколе с использованием одного алгоритма. Например, гибридный протокол PQ/T с композитной аутентификацией субъектов путём использования гибридных композитных сертификатов PQ/T.

В гибридных протоколах PQ/T с композитной конструкцией изменения вносятся в основном в форматы криптографических элементов, а поля протокола и поток сообщений остаются практически неизменными. В реализациях большинство изменений связано с криптографическими библиотеками, а протокольные почти не меняются.

PQ/T hybrid protocol with non-composite key establishment - гибрид PQ/T с организацией некомпозитного ключа

Гибридный протокол PQ/T, включающий несколько схем с одним алгоритмом для организации ключа, в которых хотя бы один алгоритм является пост-квантовым и хотя бы один - традиционным, так, что форматы криптографических элементов остаются такими же, как при использовании в схеме с одним алгоритмом.

Например, гибридный протокол PQ/T с организацией некомпозитного ключа может включать традиционную схему обмена ключами и пост-квантовый механизм KEM. Подобная конструкция для протокола обмена ключами IKEv2 (Internet Key Exchange Protocol Version 2) описана в [RFC9370].

PQ/T hybrid protocol with non-composite authentication - гибрид с некомпозитной аутентификацией данных

Гибридный протокол PQ/T, включающий несколько схем с одним алгоритмом, в которых хотя бы один алгоритм является пост-квантовым и хотя бы один - традиционным, так, что форматы криптографических элементов остаются такими же, как при использовании в схеме с одним алгоритмом. Например, гибридный протокол PQ/T с некомпозитной аутентификацией может использовать параллельную инфраструктуру PQ/T PKI с одной традиционной и одной пост-квантовой цепочкой сертификатов.

В гибридном протоколе PQ/T с некомпозитной структурой изменения вносятся в основном в поля протокола и поток сообщений, а криптографические элементы изменяются минимально. В реализации большинство изменений вносится в библиотеки протокола, а изменения криптобиблиотек минимальны.

[1] Pre-Shared Key - заранее заданный общий ключ.

Возможно создание гибридного протокола PQ/T с композитными и некомпозитными конструкциями. Например, протокол, который предоставляет услуги конфиденциальности и проверки подлинности, может включать композитное согласование ключей и некомпозитную аутентификацию. Возможно также выполнение гибридным протоколом PQ/T некоторых криптографических операций негибридными способами, например, в [HYBRID-TLS] описан гибридный протокол PQ/T с согласованием композитных ключей и аутентификацией с одним алгоритмом.

Гибридный протокол PQ/T может не задавать некомпозитных аспектов, но может делать это для ясности, в частности при включении как композитных, так и некомпозитных аспектов.

PQ/T hybrid composite protocol - гибридный композитный протокол PQ/T
: Гибридный протокол PQ/T, использующий только составные конструкции, можно называть композитным. Примером может служить протокол, обеспечивающий лишь аутентификацию субъектов и делающий это с помощью гибридной композитной аутентификации субъектов PQ/T. Другим примером является протокол, обеспечивающий организацию ключей и аутентификацию данных с использованием композитных гибридов PQ/T для обеих служб.

PQ/T hybrid non-composite protocol - гибридный некомпозитный протокол PQ/T
: Гибридный протокол PQ/T, использующий не только составные конструкции, можно называть некомпозитным. Например, гибридный протокол PQ/T с защитой конфиденциальности и аутентификацией может применять композитное согласование ключей и некомпозитную проверку подлинности.

5. Свойства

В этом разделе описаны некоторые свойства, которые могут быть желательны для гибридной схемы или гибридного протокола PQ/T. Свойства гибридных схем PQ/T являются сферой активных исследований и разработок, например, в [BINDELHALE]. Этот раздел описывает базовый набор свойств, не претендуя на полноту.

Ни одна гибридная схема или гибридный протокол PQ/T не могут обеспечить все описанные в этом разделе свойства. Для понимания требуемых свойств разработчикам и проектировщикам нужно осознать причины применения гибрида PQ/T. Например, схема, предназначенная для обеспечения безопасности, скорей всего потребует гибридной конфиденциальности или гибридной аутентификации PQ/T, а схема для обеспечения функциональной совместимости будет требовать гибридной совместимости PQ/T.

PQ/T hybrid confidentiality - гибридная конфиденциальность PQ/T
: Обеспечение конфиденциальности с помощью гибридной схемы или гибридного протокола PQ/T, пока хотя бы один из компонентов остаётся безопасным.

PQ/T hybrid authentication - гибридная аутентификация PQ/T
: Обеспечение аутентификации с помощью гибридной схемы или гибридного протокола PQ/T, пока хотя бы один из компонентов остаётся безопасным.

Свойства безопасности гибридной схемы или протокола PQ/T зависят от безопасности алгоритмов-компонентов, выбора гибридного сумматора PQ/T и возможностей атакующего. Изменения в безопасности компонента могут влиять на свойства безопасности гибридной схемы PQ/T, обеспечивающей конфиденциальность или аутентификацию. Например, при взломе пост-квантового алгоритма в гибридной схеме PQ/T она останется защищённой от атак классических компьютеров, но станет уязвимой для атак с использованием CRQC.

Гибридные протоколы PQ/T, обеспечивающие сразу конфиденциальность и аутентификацию, не обязаны обеспечивать гибридную конфиденциальность и гибридную аутентификацию. Например, [HYBRID-TLS] обеспечивает гибридную конфиденциальность, но не обеспечивает гибридной аутентификации. Если схема [HYBRID-TLS] применяется с сертификатами X.509 на основе одного алгоритма, как указано в [RFC5280], аутентификация обеспечивается лишь на основе одного алгоритма.

PQ/T hybrid interoperability - гибридная функциональная совместимость PQ/T
: Свойство, заключающееся в том, что гибридная схема или гибридный протокол PQ/T могут успешно работать, когда обе стороны поддерживают хотя бы один из алгоритмов-компонентов. Например, гибридная цифровая подпись PQ/T может поддерживать гибридную совместимость, если подпись может быть проверена традиционным или пост-квантовым компонентом, как описано в параграфе 7.2.2 [ITU-T-X509-2019]. В этом примере от проверяющего, перешедшего на поддержку пост-квантовых алгоритмов, требуется лишь проверка подписи пост-квантового алгоритма, а не перешедший на пост-квантовые алгоритмы проверяющий будет проверять лишь традиционную подпись.

Для протокола, поддерживающего конфиденциальность и аутентификацию, гибридная совместимость PQ/T требует поддержки обеими сторонами хотя бы одного алгоритма аутентификации и одного алгоритма конфиденциальности.

Гибридная схема PQ/T не может обеспечивать одновременно гибридную совместимость PQ/T и гибридную конфиденциальность PQ/T без дополнительной функциональности на уровне протокола. Для гибридной совместимости PQ/T схема должна работать всякий раз, когда один из алгоритмов-компонентов поддерживается обеими сторонами, а для гибридной конфиденциальности PQ/T должны использоваться все компоненты. Однако оба свойства могут быть обеспечены гибридным протоколом PQ/T за счёт встраивания защиты от понижения уровня вне криптографических схем. Например, в [HYBRID-TLS] клиент использует расширение TLS для поддерживаемой группы с целью анонсирования поддержки гибридной схемы PQ/T, а сервер может выбрать эту группу, если он поддерживает схему. Для этого применяется имеющаяся в TLS защита от понижения уровня, поэтому обеспечивается гибридная конфиденциальность PQ/T и соединение может быть установлено, даже когда клиент или сервер не поддерживает гибридную схему PQ/T, поэтому гибридная совместимость PQ/T обеспечивается.

Это верно и для сочетания гибридной совместимости PQ/T с гибридной аутентификацией PQ/T. Невозможно достичь этого с использованием лишь гибридной схемы PQ/T, но можно обеспечить с помощью гибридного протокола PQ/T с защитой от понижения уровня.

PQ/T hybrid backwards compatibility - гибридная совместимость PQ/T с прежними версиями
: Свойство, благодаря которому гибридная схема или гибридный протокол PQ/T могут быть реализованы, когда обе стороны поддерживают традиционный алгоритм или оба алгоритма (традиционный и пост-квантовый).

PQ/T hybrid forwards compatibility - гибридная совместимость PQ/T с будущими версиями
: Свойство, благодаря которому гибридная схема или гибридный протокол PQ/T могут быть реализованы с использованием пост-квантового алгоритма при его поддержке обеими сторонами, а также с использованием сразу

пост-квантового и традиционного алгоритма, если обе стороны их поддерживают. Отметим, что гибридная совместимость PQ/T является свойством только протокола или только схемы.

6. Сертификаты

В этом разделе приведены термины, относящиеся к сертификатам в гибридных схемах.

PQ/T hybrid certificate - гибридный сертификат PQ/T

Цифровой сертификат, содержащий открытые ключи двух и более алгоритмов-компонентов, из которых хотя бы один является традиционным и хотя бы один - пост-квантовым. Гибридный сертификат PQ/T может применяться для реализации гибридного протокола аутентификации PQ/T, однако такой протокол не требует гибридного сертификата и может работать с отдельными сертификатами для каждого алгоритма.

Компоненты открытых ключей в гибридном сертификате PQ/T могут представляться композитным ключом или открытыми ключами отдельных компонентов.

Использование гибридного сертификата PQ/T не обязательно обеспечивает гибридную аутентификацию отправителя, она может определяться свойствами цепочки доверия. Например, сертификат конечного элемента с композитным открытым ключом, подписанный с использованием одного алгоритма, можно применять для гибридной аутентификации источника сообщения, но он не обеспечивает гибридной аутентификации отправителя.

Post-quantum certificate - пост-квантовый сертификат

Цифровой сертификат, содержащий один открытый ключ для пост-квантового алгоритма цифровой подписи.

Traditional certificate - традиционный сертификат

Цифровой сертификат, содержащий один открытый ключ для традиционного алгоритма цифровой подписи.

Сертификаты X.509 в соответствии с [RFC5280] могут быть традиционными или пост-квантовыми в зависимости от алгоритма в Subject Public Key Info. Например, сертификат с открытым ключом ML-DSA [ML-DSA] будет пост-квантовым.

Post-quantum certificate chain - пост-квантовая цепочка сертификатов

Цепочка сертификатов, где все сертификаты включают открытый ключ для пост-квантового алгоритма и подписаны с использованием пост-квантовой схемы цифровой подписи.

Traditional certificate chain - традиционная цепочка сертификатов

Цепочка сертификатов, где все сертификаты включают открытый ключ для традиционного алгоритма и подписаны с использованием традиционной схемы цифровой подписи.

PQ/T hybrid certificate chain - гибридная цепочка сертификатов PQ/T

Цепочка сертификатов, где все сертификаты являются гибридами PQ/T и каждый из них имеет две или более подписи, из которых хотя бы одна является традиционной и хотя бы одна - пост-квантовой.

Цепочка гибридных сертификатов PQ/T является одним из способов гибридной аутентификации отправителя в протоколе, но это не единственный способ. Другим вариантом является использование параллельной PQ/T PKI.

PQ/T mixed certificate chain - смешанная цепочка сертификатов PQ/T

Цепочка сертификатов, содержащая не менее двух или трёх типов сертификатов, определённых в этом документе (гибридные сертификаты PQ/T, постквантовые и традиционные сертификаты). Например, традиционный сертификат конечного элемента может быть подписан промежуточным пост-квантовым сертификатом, который, в свою очередь, подписан корневым пост-квантовым сертификатом. Это может быть желательно из-за сроков действия сертификатов, относительной сложности смены ключей или по соображениям эффективности. Свойства безопасности цепочки сертификатов, включающей традиционные и пост-квантовые алгоритмы, нужно анализировать в каждом конкретном случае.

PQ/T parallel PKI - параллельная инфраструктура PKI PQ/T

Две совместно используемые в протоколе цепочки сертификатов, одна из которых содержит пост-квантовые сертификаты, другая - традиционные. Параллельная инфраструктура PKI PQ/T может применяться для гибридной аутентификации или гибридной совместимости в зависимости от реализации протокола.

Multi-certificate authentication - аутентификация с несколькими сертификатами

Проверка подлинности в применением двух и более сертификатов конечного элемента, например, аутентификация с использованием параллельной инфраструктуры PKI PQ/T.

7. Вопросы безопасности

Этот документ определяет связанные с безопасностью термины для использования в документах, задающих гибридные протоколы и схемы PQ/T, однако сам не влияет на безопасность протоколов Internet. Вопросы безопасности каждого гибридного протокола PQ/T зависят от самого протокола и их следует обсуждать в соответствующих спецификациях. Более общие рекомендации по вопросам безопасности, срокам, преимуществам и недостаткам гибридов PQ/T также выходят за рамки этого документа.

8. Взаимодействие с IANA

Документ не требует действий IANA.

9. Литература

[BDPR] Bellare, M., Desai, A., Pointcheval, D., and P. Rogaway, "Relations Among Notions of Security for Public-Key Encryption Schemes", June 2001, <https://www.cs.ucdavis.edu/~rogaway/papers/relations.pdf>.

[BINDEL] Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., and D. Stebila, "Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange", Post-Quantum Cryptography, PQCrypto 2019, Lecture Notes in Computer Science, vol. 11505, pp. 206-226, DOI 10.1007/978-3-030-25510-7_12, July 2019, <https://doi.org/10.1007/978-3-030-25510-7_12>.

[BINDELHALE] Bindel, N. and B. Hale, "A Note on Hybrid Signature Schemes", Cryptology ePrint Archive, Paper 2023/423, 23 July 2023, <https://eprint.iacr.org/2023/423.pdf>.

[COMPOSITE-KEM] Ounsworth, M., Gray, J., Pala, M., Klaussner, J., and S. Fluhrer, "Composite ML-KEM for use in X.509 Public Key Infrastructure and CMS", Work in Progress, Internet-Draft, draft-ietf-lamps-pq-composite-kem-06, 18 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-pq-composite-kem-06>.

[ETSI_TS103774] European Telecommunications Standards Institute (ETSI), "CYBER; Quantum-safe Hybrid Key Exchanges", ETSI TS 103 744 v1.1.1, December 2020, <https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf>.

[HYBRID-TLS] Stebila, D., Fluhrer, S., and S. Gueron, "Hybrid key exchange in TLS 1.3", Work in Progress[1], Internet-Draft, draft-ietf-tls-hybrid-design-12, 14 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design-12>.

[ITU-T-X509-2019] ITU-T, "Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, October 2019, <https://www.itu.int/rec/T-REC-X.509-201910-I>.

[ML-DSA] Massimo, J., Kampanakis, P., Turner, S., and B. E. Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", Work in Progress[2], Internet-Draft, draft-ietf-lamps-dilithium-certificates-11, 22 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-11>.

[NIST_PQC_FAQ] NIST, "Post-Quantum Cryptography (PQC) FAQs", 31 January 2025, <https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs>.

[NIST_SP_800-152] Barker, E., Smid, M., and D. Branstad, "A Profile for U. S. Federal Cryptographic Key Management Systems", NIST SP 800-152, DOI 10.6028/NIST.SP.800-15, October 2015, <https://doi.org/10.6028/NIST.SP.800-152>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446[3], DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[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>.

[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>.

[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>.

Благодарности

Этот документ является результатом многочисленных плодотворных обсуждений в группе IETF PQUIP. Выражаем отдельную благодарность Mike Ounsworth, John Gray, Tim Hollebeek, Wang Guilin, Rebecca Guthrie, Stephen Farrell, Paul Hoffman, Sofía Celi за их вклад. Идеи для документа дали многие участники IETF и других организаций.

Адреса авторов

Florence Driscoll
UK National Cyber Security Centre
Email: florence.d@ncsc.gov.uk

Michael Parsons
UK National Cyber Security Centre
Email: michael.p1@ncsc.gov.uk

Britta Hale
Naval Postgraduate School
Email: britta.hale@nps.edu

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Опубликовано в RFC 9954. *Прим. перев.*
[2]Опубликовано в RFC 9881. *Прим. перев.*
[3]Заменён RFC 9846. *Прим. перев.*