Internet Engineering Task Force (IETF)
Request for Comments: 9954
Category: Informational
ISSN: 2070-1721

D. Stebila
University of Waterloo
S. Fluhrer
Cisco Systems
S. Gueron
U. Haifa & Meta

July 2026

Hybrid Key Exchange in TLS 1.3

Гибридный обмен ключами в TLS 1.3

Аннотация

Гибридным обменом ключами называется применение одновременно нескольких алгоритмов обмена ключами с объединением их результатов для обеспечения безопасности даже в тех случаях, когда будут найдены способы взломать шифры всех алгоритмов, кроме одного. Это обусловлено переходом к пост-квантовой криптографии. Документ описывает схему гибридного обмена ключами в протоколе защиты транспортного уровня (Transport Layer Security или TLS) версии 1.3.

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/rfc9954.

Оглавление

1. Введение

В этом документе описана схема гибридного обмена ключами в TLS 1.3, основанная на простой конкатенации, - каждую комбинацию при гибридном обмене следует рассматривать как единый метод обмена ключами, которые нужно согласовать и передать с использованием имеющихся механизмов TLS 1.3. Документ не предлагает конкретных пост-квантовых механизмов. Область действия документа рассмотрена в параграфе 1.3.

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

1.1. Терминология

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

Для целей этого документа полезно разделить криптографические алгоритмы на два класса.

- Традиционные алгоритмы - это широко распространённые в настоящее время алгоритмы, которые в будущем могут быть сочтены устаревшими. В контексте TLS 1.3 примеры традиционных алгоритмов включают Elliptic Curve Diffie-Hellman (ECDH) с использованием secp256r1, x25519 и метод Диффи-Хеллмана над конечным полем.
- Алгоритмы нового поколения (next-generation или next-gen) - это алгоритмы, ещё не получившие широкого распространения, но со временем способные стать таковыми. Ещё одной особенностью этих алгоритмов является то, что криптографическое сообщество может быть менее уверено в их безопасности по причине относительной новизны и недостаточной изученности. В число алгоритмов нового поколения входят пост-квантовые алгоритмы.

В этом контексте гибридный обмен ключами означает использование двух (и более) алгоритмов обмена ключами на основе разных криптографических допущений, например, одного традиционного алгоритма и одного алгоритма нового поколения, чтобы итоговый сеансовый ключ оставался защищённым, пока хотя бы один из применённых в обмене ключами алгоритмов остаётся невзломанным. Когда один из алгоритмов является традиционным, а другой - пост-квантовым, это называется Post-Quantum Traditional Hybrid Scheme [PQUIP-TERM], хотя документ не ограничивается только такой схемой. Термин «алгоритмы-компоненты» в документе обозначает алгоритмы, объединяемые в гибридном обмене ключами.

Некоторые исследователи предпочитают использовать термин «композитный» (composite) для применения нескольких алгоритмов, чтобы отличить его от гибридного шифрования открытого ключа (hybrid public key encryption), где комбинируются механизмы инкапсуляции ключа и данных для шифрования открытого ключа.

Предполагается, что алгоритмы-компоненты гибридного обмена ключами должны исполняться (т. е. согласовываться и передаваться) в рамках согласования TLS 1.3 (handshake). Отмен ключевым материалом по отдельному каналу (out-of-band) в документе не рассматривается.

Основной целью документа является подготовка к пост-квантовым алгоритмам. Однако возможно, что криптография с открытым ключом на основе дополнительных математических конструкций станет желательной для снижения рисков, не связанных с квантовыми компьютерами, например, в случае прорыва в криптоанализе. Поэтому в документе используется более общий термин «алгоритмы нового поколения», а не только пост-квантовые алгоритмы.

Отметим, что в TLS 1.3 термин «группа» относится в алгоритмам обмена ключами (например, расширение supported_groups), поскольку в TLS 1.3 все алгоритмы обмена ключами основаны на методе Диффи-Хеллмана (Diffie-Hellman или DH). В результате этого в некоторых частях документа упоминаются структуры данных или сообщения, содержащие термин «группа», хотя применяется алгоритм обмена ключами, не связанный ни с DH, ни с группой.

1.2. Мотивы использования гибридного обмена ключами

Гибридный обмен ключами позволяет пользователям, стремящимся к пост-квантовой безопасности, использовать её потенциал (возможно, с помощью малоизученного алгоритма), сохраняя при этом безопасность, обеспечиваемую традиционными алгоритмами. Возможно, им даже придётся сохранить традиционные алгоритмы, например, из-за требований FIPS[1] Национального института стандартов и технологии США (US National Institute of Standards and Technology или NIST).

В идеальном случае не следует пользоваться гибридным обменом ключами - нужно быть уверенным в одном алгоритме и параметрах, которые пройдут проверку временем. Однако с учётом развития квантовых компьютеров и успехов криптоанализа это может оказаться не так.

Многие (хотя и не все) рассматриваемые в настоящее время пост-квантовые алгоритмы, являются сравнительно новыми и не были изучены столь же глубоко, как RSA или метод Диффи-Хеллмана над конечным полем или эллиптической кривой. В результате разработчики в сфере безопасности не имеют достаточной уверенности в базовой безопасности алгоритмов или уровне безопасности при конкретных наборах параметров. Кроме того, вполне возможно, что после задания алгоритмов нового поколения в течение некоторого времени консервативные пользователи не будут полностью доверять некоторым из них.

Некоторые пользователи могут захотеть ускорить внедрение пост-квантовой криптографии из-за угроз ретроактивной расшифровки (retroactive decryption или harvest-now-decrypt-later[2]). Если криптографические допущения станут ложными в результате развития квантовых компьютеров или какого-либо прорыва в криптоанализе, конфиденциальность прошлых данных может быть нарушена любым злоумышленником, который пассивно записывал согласования и шифрованные коммуникации. Гибридный обмен ключами может обеспечить защиту от ретроактивной расшифровки без полного отказа от традиционных криптосистем.

Таким образом, для некоторых пользователей гибридный обмен ключами является подходящим шагом в подготовке к переходу на алгоритмы нового поколения. Пользователям следует учитывать уровень доверия к каждому компоненту гибрида для оценки соответствия гибридной схемы желаемым требованиям.

1.3. Область действия

Этот документ посвящен гибридному обмену эфемерными ключами в TLS 1.3 [TLS13] и намеренно не рассматривает указанные ниже вопросы.

---

[1] Federal Information Processing Standards - Федеральные стандарты обработки информации (США). *Прим. перев.*

[2] Собрать сейчас, расшифровать потом.

- Выбор алгоритмов нового поколения для использования в TLS 1.3, а также идентификаторы и механизмы кодирования для алгоритмов нового поколения.
- Аутентификация с использованием алгоритмов нового поколения. Хотя квантовые компьютеры смогут ретроактивно расшифровать прежние сессии, ретроактивный взлом аутентификации таких сессий невозможен.

1.4. Цели

Основной целью гибридного механизма обмена ключами является создание общего секрета, остающегося безопасным, пока не взломан хотя бы один из компонентов механизма обмена ключами. В дополнение к основной криптографической цели в контексте TLS 1.3 имеются дополнительные цели, указанные ниже.

- Совместимость с прежними версиями. Клиентам и серверам с поддержкой гибридного подхода, т. е. соответствующим любому из стандартов гибридного обмена ключами для TLS, следует оставаться совместимыми с конечными точками и промежуточными устройствами, не поддерживающими гибридные схемы. Возможны три варианта:
  1. клиент и сервер поддерживают гибриды и им следует создавать гибридный общий секрет;
  2. клиент поддерживает гибриды, сервер - нет и им следует создавать негибридный общий секрет (в предположении, что клиент понизит свой уровень);
  3. сервер поддерживает гибриды, клиент - нет и им следует создавать негибридный общий секрет (в предположении, что сервер понизит свой уровень).

  В идеале совместимость с прежней версией следует обеспечивать без дополнительных круговых обходов (round trip) и передачи дублирующей информации (см. ниже).
- Высокая производительность. Использование гибридного обмена ключами не должно приводить к чрезмерным вычислительным издержкам. В общем случае это будет зависеть от параметров производительности конкретных криптографических алгоритмов и этот вопрос выходит за рамки документа. Предварительные оценки производительности представлены в [PST].
- Малые задержки. Использование гибридного обмена ключами не должно приводить к существенной задержке организации соединения. Влияющие на задержку факторы включают:
  - вычислительную производительность применяемых алгоритмов (см. выше);
  - размер передаваемых сообщений, который для открытых ключей и шифротекста пост-квантовых алгоритмов может включать от сотен байтов до 100 Кбайт и больше, поэтому влияние может быть существенным; предварительные результаты лабораторных исследований приведены в [PST], а предварительные результаты для более реалистичных сетей - в [LANGLEY];
  - дополнительные круговые обходы в протоколе (см. ниже).
- Отсутствие дополнительных круговых обходов. Попыткам гибридного согласования ключей не следует приводить к дополнительным круговым обходам ни в одном из трёх указанных выше вариантов.
- Минимальное дублирование информации. Попыткам гибридного согласования ключей не следует приводить к передаче нескольких открытых ключей одного типа.

Допустимое снижение производительности и увеличение задержки в результате применения гибридного обмена ключами будут зависеть от контекста и варианта использования вовлечённых систем и сетей.

2. Механизмы инкапсуляции ключей

В этом документе организация ключей моделируется как механизмы инкапсуляции ключей (key encapsulation mechanism или KEM), включающие три алгоритма.

KeyGen() -> (pk, sk)
: Вероятностный алгоритм генерации открытого (pk) и секретного (sk) ключа.

Encaps(pk) -> (ct, ss)
: Вероятностный алгоритм инкапсуляции, принимающий открытый ключ pk и выдающий шифротекст ct и общий секрет ss.

Decaps(sk, ct) -> ss
: Алгоритм декапсуляции, принимающий секретный ключ sk и шифротекст ct, а на выходе дающий общий секрет ss или (в некоторых случаях) различимое значение ошибки.

Основным свойством безопасности для KEM является неразличимость при адаптивных атаках с выбранным шифротекстом (IND-CCA2), что означает невозможность отличить значения общих секретов от случайных строк даже при способности декапсулировать произвольный шифротекст. IND-CCA2 соответствует защите от активных атак, а пара из открытого и секретного ключа может считаться долгосрочной или применяться неоднократно. Распространенным способом обеспечения безопасности при неоднократном применении ключа является преобразование Фудзисаки-Окамото (Fujisaki-Okamoto или FO) [FO] или его вариант [HHK].

Более слабым вариантом является неразличимость при атаках с выбранными открытми данными (IND-CPA), когда значениям общего секрета следует быть неотличимыми от случайных строк при наличии копии открытого ключа. IND-CPA примерно соответствует защите от пассивных атак и иногда соответствует обмену одноразовыми ключами.

Определения безопасности для IND-CCA2 и IND-CPA представлены в [KATZ] и [HHK].

Обмен ключами в TLS 1.3 обсуждается в терминах метода DH в группе. Обмен ключами DH можно представить как KEM с (1) алгоритмом KeyGen, соответствующим выбору показателя степени x как секретного ключа и расчёту открытого ключа g^x, (2) инкапсуляцией, соответствующей выбору показателя степени y и расчёту шифротекста g^y и общего секрета g^(xy), и (3) декапсуляцией, соответствующей расчёту общего секрета g^(xy). Более подробные сведения о механизмах инкапсуляции ключей на основе DH представлены в [HPKE]. Обмен ключами DH в качестве

KEM, формально не соответствует требованиям IND-CCA2, но остаётся безопасным для обмена эфемерными ключами в TLS 1.3 (см., например, [DOWLING]).

TLS 1.3 не требует, чтобы эфемерные ключи применялись лишь в одной сессии обмена ключами и некоторые реализации могут неоднократно использовать ключи за счёт ограничения секретности в будущем (forward secrecy). В результате любой механизм KEM, применяемый в соответствии с этим документом, **должен** быть явно устроен так, чтобы обеспечивать безопасность в случаях повторного использования открытого ключа. Методы DH над конечным полем и эллиптической кривой, применяемые в TLS 1.3, соответствуют этому критерию. Для базовых KEM это означает соответствие IND-CCA2 или применение преобразования, подобного [FO] [HHK]. Хотя рекомендуется избегать повтороного использования открытых ключей KEM, реализации с повторным использованием открытых ключей KEM **должны** гарантировать, что число повторных применений соответствует ограничениям, заданным спецификацией KEM или последующим анализом безопасности. Реализациям **недопустимо** повторно использовать случайные значения при создании шифротекста KEM.

3. Схема гибридного обмена ключами

3.1. Согласование

Каждая конкретная пара алгоритмов в гибридном обмене ключами представляется NamedGroup и передаётся в расширении supported_groups. В значении идентификатора не предполагается и не требуется какой-либо внутренней структуры, это просто неразбираемый (opaque) идентификатор.

Каждому значению, представляющему гибридный обмен ключами, соответствует упорядоченный набор из двух (или более) алгоритмов. Отметим, что на это не повлияют будущие документы, стандартизирующие исключительно пост-квантовые методы обмена ключами, которым должны будут назначаться свои идентификаторы.

3.2. Передача открытых ключей и шифротекста

В этом документе используется сравнительно простой метод конкатенации. Сообщения от двух или нескольких алгоритмов объединяются путём конкатенации и передаются как одно значение, чтобы избежать необходимости изменения имеющихся структур данных. Значения объединяются напрямую без дополнительного кодирования или размеров полей, а представление и размер элементов **должны** задаваться выбором алгоритмов.

В TLS 1.3 (см. параграф 4.3.8[1] в [TLS13]) открытый ключ или шифротекст KEM представляется как KeyShareEntry

```
struct {
    NamedGroup group;
    opaque key_exchange<1..2^16-1>;
} KeyShareEntry;
```

Эта структура передаётся в полях extension_data расширений KeyShareClientHello и KeyShareServerHello

```
struct {
    KeyShareEntry client_shares<0..2^16-1>;
} KeyShareClientHello;

struct {
    KeyShareEntry server_share;
} KeyShareServerHello;
```

Значения (share) клиента указываются в порядке снижения предпочтений клиента, а сервер выбирает один алгоритм и передаёт соответствующий секрет.

В гибридном обмене ключами поле key_exchange структуры KeyShareEntry содержит конкатенацию полей key_exchange каждого из алгоритмов гибрида. Порядок значений (share) в конкатенации **должен** совпадать с порядком алгоритмов в определении NamedGroup.

Клиентское значение key_exchange содержит конкатенацию вывода pk соответствующих алгоритмов KEM KeyGen, если алгоритм соответствует KEM, или эфемерных ключей (EC)DH, если алгоритм соответствует группе (EC)DH. Серверное значение key_exchange содержит конкатенацию вывода ct алгоритмов KEM Encaps, соответствующих KEM, или эфемерных ключей (EC)DH, алгоритмов, соответствующих группе (EC)DH.

Параграф 4.3.81 в [TLS13] требует: «Значения key_exchange для каждой записи KeyShareEntry **должны** генерироваться независимо». В контексте этого документа один алгоритм может присутствовать в нескольких именованных группах. Таким образом, документ смягчает приведённое выше требование, разрешая использовать значение key_exchange для одного алгоритма в нескольких записях KeyShareEntry одного сообщения ClientHello. Однако значения key_exchange для разных алгоритмов **должны** создаваться независимо. Если NamedGroup указывает гибридный обмен ключами MyECDHMyPQKEM, значения KeyShareEntry.key_exchange **должны** создаваться одним из двух способов, указанных ниже.

```
MyECDHMyPQKEM.KeyGen() = (MyECDH.KeyGen(), MyPQKEM.KeyGen())
KeyShareClientHello {
    KeyShareEntry {
        NamedGroup: 'MyECDH',
        key_exchange: MyECDH.KeyGen()
    },
    KeyShareEntry {
        NamedGroup: 'MyPQKEM',
        key_exchange: MyPQKEM.KeyGen()
    },
    KeyShareEntry {
        NamedGroup: 'MyECDHMyPQKEM',
        key_exchange: MyECDHMyPQKEM.KeyGen()
    },
}
```

[1] В оригинале ошибочно указан параграф 4.2.8, см. https://errata.rfc-editor.org/eid9136/. *Прим. перев.*

Повторное использование значений key_exchange одного алгоритма внутри одного сообщения ClientHello имеет вид

```
myecdh_key_share = MyECDH.KeyGen()
mypqkem_key_share = MyPQKEM.KeyGen()
myecdh_mypqkem_key_share = (myecdh_key_share, mypqkem_key_share)

KeyShareClientHello {
    KeyShareEntry {
        NamedGroup: 'MyECDH',
        key_exchange: myecdh_key_share
    },
    KeyShareEntry {
        NamedGroup: 'MyPQKEM',
        key_exchange: mypqkem_key_share
    },
    KeyShareEntry {
        NamedGroup: 'MyECDHMyPQKEM',
        key_exchange: myecdh_mypqkem_key_share
    },
}
```

3.3. Расчёт общего секрета

Для общих секретов в документе также используется простой метод конкатенации - два общих секрета объединяются и служат единым общим секретом в имеющемся планировании ключей TLS 1.3 без добавления какой-либо структуры (размеры полей) как для традиционных групп, так и для пост-квантовых KEM. Выходной размер общего секрета фиксирован для конкретной эллиптической кривой или набора параметров. Иными словами, если NamedGroup - это MyECDHMyPQKEM, общий секрет рассчитывается как

```
concatenated_shared_secret = MyECDH.shared_secret || MyPQKEM.shared_secret
```

и помещается в расписание ключей TLS 1.3 вместо общего секрета (EC)DHE, как показано на рисунке 1.

```
                                          0
                                          |
                                          v
                                PSK ->  HKDF-Extract = Early Secret
                                          |
                                          +-----> Derive-Secret(...)
                                          +-----> Derive-Secret(...)
                                          +-----> Derive-Secret(...)
                                          |
                                          v
                                     Derive-Secret(., "derived", "")
                                          |
                                          v
                   concatenated_shared_secret -> HKDF-Extract = Handshake Secret
                   ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^           |
                                          +-----> Derive-Secret(...)
                                          +-----> Derive-Secret(...)
                                          |
                                          v
                                     Derive-Secret(., "derived", "")
                                          |
                                          v
                                   0 -> HKDF-Extract = Main Secret
                                          |
                                          +-----> Derive-Secret(...)
                                          +-----> Derive-Secret(...)
                                          +-----> Derive-Secret(...)
                                          +-----> Derive-Secret(...)
```

Рисунок 1. Расписание ключей при гибридном обмене.

В части соответствия FIPS документы NIST [NIST-SP-800-56C] и [NIST-SP-800-135] содержат рекомендации по методам выведения ключей в протоколах обмена ключами. Некоторые гибридные комбинации могут сочетать общий секрет из одобренного NIST алгоритма (например, ECDH с кривой nistp256/secp256r1) с обшим секретом из неутверждённого алгоритма (например, пост-квантового). В [NIST-SP-800-56C] простая конкатенация указана как утверждённый метод создания гибридных общих секретов, в которых один из компонентов получен одобренным методом.

4. Обсуждение

Больший размер открытых ключей и шифротекста

Поле key_exchange структуры KeyShareEntry в параграфе 3.2 ограничивает размеры открытых ключей и шифротекста значением 2^16-1 байт. В некоторых пост-квантовых KEM размер ключа или шифротекста больше, например, наименьший набор параметров Classic McEliece имеет открытый ключ размером 261120 байтов [Classic-McEliece]. Однако все наборы параметров для механизма инкапсуляции ключей на основе модульной решётки (Module-Lattice-Based Key Encapsulation Mechanism или ML-KEM) [NIST-FIPS-203] имеют открытые ключи и шифротекст в рамках ограничений TLS (хотя в результате сообщение ClientHello может превышать размер пакета).

Дублирование ключей

Конкатенация открытых ключей в поле key_exchange структуры KeyShareEntry, описанной в параграфе 3.2, может приводить к дублированию общих значений (key share). Например, если клиент хочет предложить поддержку двух комбинаций, скажем, SecP256r1MLKEM768 и X25519MLKEM768 [ECDHE-MLKEM], он будет передавать два открытых ключа ML-KEM-768, поскольку KeyShareEntry для каждой комбинации содержит копию ключа ML-KEM-768. Это может создавать проблемы для пост-квантовых алгоритмов с большими открытыми ключами. Если же клиент предложит, например, SecP256r1MLKEM768 и secp256r1 (для совместимости с прежними версиями), дублированных данных будет относительно немного (ключи secp256r1 сравнительно малы).

5. Взаимодействие с IANA

Агентство IANA включило ссылку на этот документ в реестр TLS Supported Groups [IANA-TLS].

Для гибридных комбинаций, заданных этим документом, IANA будет выделять идентификаторы из диапазона, отличного от диапазона для групп над конечными полями. В столбце Recommended **следует** указывать значение N (нет), а в столбце DTLS-OK **следует** указывать Y (да).

6. Вопросы безопасности

Общие секреты при гибридном обмене ключами следует рассчитывать так, чтобы обеспечить свойство гибрида - полученный секрет должен оставаться безопасным, пока хотя бы один из алгоритмов-компонентов сохраняется невзломанным. Исследованию этого вопроса посвящены работы [GIACON] и [BINDEL]. При допущении фиксированного размера общих секретов после выбора комбинации алгоритмов, конструкция из параграфа 3.3 соответствует сумматору с двумя PRF[1] [BINDEL], для которого показано сохранение безопасности при условии использования хэш-функции dual-PRF.

Как отмечено в разделе 2, KEM, применяемые в соответствии с этим документом, **должны** быть явно спроектированы для обеспечения безопасности в случаях повторного использования открытого ключа, например, путём обеспечения защиты от IND-CCA2 или применения преобразования, подобного Fujisaki-Okamoto. ML-KEM обеспечивает такие свойства безопасности. Однако некоторые другие пост-квантовые KEM, разработанные для обеспечения защиты от IND-CPA (т. е. без мер противодействия, подобных преобразованию FO), совсем небезопасны при неоднократном использовании открытого ключа. Например, некоторые KEM на основе решёток, защищённые от IND-CPA, уязвимы для атак, позволяющих получить секретный ключ всего по нескольким тысячам выборок [FLUHRER].

Открытым ключам, шифротексту и общему секрету следует иметь постоянный размер. В этом документе предполагается, что после выбора алгоритма размер каждого открытого ключа, шифротекста и общего секрета фиксирован. Это справедливо для ML-KEM.

Отметим, что секреты переменного размера в общем случае опасны. В частности, при использовании ключевого материала переменного размера и его обработке с использованием хэш-функций может возникать побочный временной канал. Чем длиннее секрет, тем больше блоков может потребоваться обрабатывать внутри хэш-функции. В некоторых неблагоприятных обстоятельствах это приводило к атакам по времени, например, Lucky Thirteen [LUCKY13] и Raccoon [RACCOON].

Кроме того, в [AVIRAM] указан риск использования секретов переменного размера в случае нестойкости к коллизиям применяемой при выводе ключей хэш-функции.

Если конкатенация применяется для значений, не имеющих фиксированного размера, требуется использовать префикс размера или иное однозначное кодирование для гарантии инъективности композиции и механизм, отличный от заданного в этом документе.

Поэтому данная спецификация **должна** применяться только с общими секретами фиксированного размера (после того, как был зафиксирован выбор алгоритма в согласовании NamedGroup, описанном в параграфе 3.1).

7. Литература

7.1. Нормативные документы

[FO] Fujisaki, E. and T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes", Journal of Cryptology, vol. 26, no. 1, pp. 80-101, DOI 10.1007/s00145-011-9114-1, December 2011, <https://doi.org/10.1007/s00145-011-9114-1>.

[HHK] Hofheinz, D., Hövelmanns, K., and E. Kiltz, "A Modular Analysis of the Fujisaki-Okamoto Transformation", Theory of Cryptography (TCC 2017), Lecture Notes in Computer Science, vol. 10677, pp. 341-371, DOI 10.1007/978-3-319-70500-2_12, 2017, <https://doi.org/10.1007/978-3-319-70500-2_12>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[TLS13] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 9846, DOI 10.17487/RFC9846, July 2026, <https://www.rfc-editor.org/info/rfc9846>.

7.2. Дополнительная литература

[AVIRAM] Nimrod Aviram, Benjamin Dowling, Ilan Komargodski, Kenny Paterson, Eyal Ronen, and Eylon Yogev, "[TLS] Combining Secrets in Hybrid Key Exchange in TLS 1.3", 1 September 2021, <https://mailarchive.ietf.org/arch/msg/tls/F4SVeL2xbGPaPB2GW_GkBbD_a5M/>.

[BCNS15] Bos, J., Costello, C., Naehrig, M., and D. Stebila, "Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem", 2015 IEEE Symposium on Security and Privacy, pp. 553-570, DOI 10.1109/sp.2015.40, May 2015, <https://doi.org/10.1109/sp.2015.40>.

[BERNSTEIN] Bernstein, D. J., Ed., Buchmann, J., Ed., and E. Dahmen, Ed., "Post-Quantum Cryptography", Springer Berlin, DOI 10.1007/978-3-540-88702-7, 2009, <https://doi.org/10.1007/978-3-540-88702-7>.

[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, 2019, <https://doi.org/10.1007/978-3-030-25510-7_12>.

[1] Pseudorandom function - псевдо-случайная функция. *Прим. перев.*

[CAMPAGNA] Campagna, M. and E. Crockett, "Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)", Work in Progress, Internet-Draft, draft-campagna-tls-bike-sike-hybrid-07, 2 September 2021, <https://datatracker.ietf.org/doc/html/draft-campagna-tls-bike-sike-hybrid-07>.

[CECPQ1] Braithwaite, M., "Experimenting with Post-Quantum Cryptography", Google Security Blog, 7 July 2016, <https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html>.

[CECPQ2] Langley, A., "CECPQ2", 12 December 2018, <https://www.imperialviolet.org/2018/12/12/cecpq2.html>.

[Classic-McEliece] Josefsson, S., "Classic McEliece", Work in Progress, Internet-Draft, draft-josefsson-mceliece-05, 23 June 2026, <https://datatracker.ietf.org/doc/html/draft-josefsson-mceliece-05>.

[DODIS] Dodis, Y. and J. Katz, "Chosen-Ciphertext Security of Multiple Encryption", Theory of Cryptography (TCC 2005), Lecture Notes in Computer Science, vol. 3378, pp. 188-209, DOI 10.1007/978-3-540-30576-7_11, 2005, <https://doi.org/10.1007/978-3-540-30576-7_11>.

[DOWLING] Dowling, B., Fischlin, M., Günther, F., and D. Stebila, "A Cryptographic Analysis of the TLS 1.3 Handshake Protocol", Journal of Cryptology, vol. 34, article 37, DOI 10.1007/s00145-021-09384-1, July 2021, <https://doi.org/10.1007/s00145-021-09384-1>.

[ECDHE-MLKEM] Kwiatkowski, K., Kampanakis, P., Westerbaan, B., and D. Stebila, "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3", Work in Progress[1], Internet-Draft, draft-ietf-tls-ecdhe-mlkem-05, 26 May 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-ecdhe-mlkem-05>.

[ETSI] Campagna, M., Ed., et al., "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges", ETSI White Paper No. 8, June 2015, <https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf>.

[EVEN] Even, S. and O. Goldreich, "On the Power of Cascade Ciphers", Advances in Cryptology, pp. 43-50, DOI 10.1007/978-1-4684-4730-9_4, 1984, <https://doi.org/10.1007/978-1-4684-4730-9_4>.

[EXTERN-PSK] Housley, R., "TLS 1.3 Extension for Certificate-Based Authentication with an External Pre-Shared Key", RFC 8773, DOI 10.17487/RFC8773, March 2020, <https://www.rfc-editor.org/info/rfc8773>.

[FLUHRER] Fluhrer, S., "Cryptanalysis of ring-LWE based key exchange with key share reuse", Cryptology ePrint Archive, Paper 2016/085, 2016, <https://eprint.iacr.org/2016/085>.

[FRODO] Bos, J., Costello, C., Ducas, L., Mironov, I., Naehrig, M., Nikolaenko, V., Raghunathan, A., and D. Stebila, "Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1006-1018, DOI 10.1145/2976749.2978425, October 2016, <https://doi.org/10.1145/2976749.2978425>.

[GIACON] Giacon, F., Heuer, F., and B. Poettering, "KEM Combiners", Public-Key Cryptography (PKC 2018), Lecture Notes in Computer Science, vol. 10769, pp. 190-218, DOI 10.1007/978-3-319-76578-5_7, 2018, <https://doi.org/10.1007/978-3-319-76578-5_7>.

[HARNIK] Harnik, D., Kilian, J., Naor, M., Reingold, O., and A. Rosen, "On Robust Combiners for Oblivious Transfer and Other Primitives", Advances in Cryptology (EUROCRYPT 2005), Lecture Notes in Computer Science, vol. 3494, pp. 96-113, DOI 10.1007/11426639_6, 2005, <https://doi.org/10.1007/11426639_6>.

[HPKE] 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>.

[IANA-TLS] IANA, "TLS Supported Groups", <https://www.iana.org/assignments/tls-parameters>.

[IKE-PSK] Fluhrer, S., Kampanakis, P., McGrew, D., and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, DOI 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/info/rfc8784>.

[KATZ] Katz, J. and Y. Lindell, "Introduction to Modern Cryptography", Third Edition, CRC Press, 2021.

[KIEFER] Kiefer, F. and K. Kwiatkowski, "Hybrid ECDHE-SIDH Key Exchange for TLS", Work in Progress, Internet-Draft, draft-kiefer-tls-ecdhe-sidh-00, 5 November 2018, <https://datatracker.ietf.org/doc/html/draft-kiefer-tls-ecdhe-sidh-00>.

[LANGLEY] Langley, A., "Post-quantum confidentiality for TLS", 11 April 2018, <https://www.imperialviolet.org/2018/04/11/pqconftls.html>.

[LUCKY13] Al Fardan, N. and K. Paterson, "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols", 2013 IEEE Symposium on Security and Privacy, pp. 526-540, DOI 10.1109/sp.2013.42, May 2013, <https://doi.org/10.1109/sp.2013.42>.

[NIELSEN] Nielsen, M. A. and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, 2000.

[NIST] NIST, "Post-Quantum Cryptography", <https://www.nist.gov/pqcrypto>.

[NIST-FIPS-203] 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>.

[NIST-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://doi.org/10.6028/nist.sp.800-56cr2>.

[NIST-SP-800-135] Dang, Q., "Recommendation for Existing Application-Specific Key Derivation Functions", NIST SP 800-135r1, DOI 10.6028/nist.sp.800-135r1, December 2011, <https://doi.org/10.6028/nist.sp.800-135r1>.

[1] Опубликовано в RFC 10024. *Прим. перев.*

[OQS-102] "OQS-OpenSSL-1-0-2_stable", commit 537b2f9, 31 January 2020, <https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_0_2-stable>.

[OQS-111] "OQS-OpenSSL-1-1-1_stable", commit 5f49b7a, 8 January 2025, <https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_1_1-stable>.

[OQS-PROV] "OQS Provider for OpenSSL 3", commit 573fb25, 8 January 2026, <https://github.com/open-quantum-safe/oqs-provider/>.

[PQUIP-TERM] 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>.

[PST] Paquin, C., Stebila, D., and G. Tamvada, "Benchmarking Post-quantum Cryptography in TLS", Post-Quantum Cryptography (PQCrypto 2020), Lecture Notes in Computer Science, vol. 12100, pp. 72-91, DOI 10.1007/978-3-030-44223-1_5, 2020, <https://doi.org/10.1007/978-3-030-44223-1_5>.

[RACCOON] Merget, R., Brinkmann, M., Aviram, N., Somorovsky, J., Mittmann, J., and J. Schwenk, "Raccoon Attack: Finding and Exploiting Most-Significant-Bit-Oracles in TLS-DH(E)", September 2020, <https://raccoon-attack.com/>.

[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>.

[S2N] Hopkins, A. and M. Campagna, "Post-quantum TLS now supported in AWS KMS", AWS Security Blog, 4 November 2019, <https://aws.amazon.com/blogs/security/post-quantum-tls-now-supported-in-aws-kms/>.

[SCHANCK] Schanck, J. M. and D. Stebila, "A Transport Layer Security (TLS) Extension For Establishing An Additional Shared Secret", Work in Progress, Internet-Draft, draft-schanck-tls-additional-keyshare-00, 17 April 2017, <https://datatracker.ietf.org/doc/html/draft-schanck-tls-additional-keyshare-00>.

[WHYTE12] Schanck, J. M., Whyte, W., and Z. Zhang, "Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.2", Work in Progress, Internet-Draft, draft-whyte-qsh-tls12-02, 22 July 2016, <https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls12-02>.

[WHYTE13] Whyte, W., Zhang, Z., Fluhrer, S., and O. Garcia-Morchon, "Quantum-Safe Hybrid (QSH) Key Exchange for Transport Layer Security (TLS) version 1.3", Work in Progress, Internet-Draft, draft-whyte-qsh-tls13-06, 3 October 2017, <https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls13-06>.

[XMSS] 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>.

[ZHANG] Zhang, R., Hanaoka, G., Shikata, J., and H. Imai, "On the Security of Multiple Encryption or CCA-security+CCA-security=CCA-security?", Public Key Cryptography (PKC 2004), Lecture Notes in Computer Science, vol. 2947, pp. 360-374, DOI 10.1007/978-3-540-24632-9_26, 2004, <https://doi.org/10.1007/978-3-540-24632-9_26>.

Приложение A. Смежные работы

Квантовые вычисления и пост-квантовая криптография в целом выходят за рамки документа. Общее введение в квантовые вычисления можно найти в стандартных учебниках, например, [NIELSEN]. Обзор пост-квантовой криптографии по состоянию на 2009 г. содержится в [BERNSTEIN], где много полезных сведений, хотя и не отражены последние достижения. Текущее состояние проекта стандартизации пост-квантовой криптографии NIST (Post-Quantum Cryptography Standardization Project) приведено в [NIST]. Дополнительные сведения о перспективах перехода от традиционной криптографии к пост-квантовой приведены в [ETSI] и других документах.

Иммется несколько документов Internet-Draft, описывающих механизмы встраивания пост-квантового и гибридного обмена ключами в TLS:

- TLS 1.2: [WHYTE12], [CAMPAGNA];
- TLS 1.3: [KIEFER], [SCHANCK], [WHYTE13].

Было разработано несколько прототипов реализаций пост-квантового и гибридного обмена ключами в TLS:

- TLS 1.2: [BCNS15], [CECPQ1], [FRODO], [OQS-102], [S2N];
- TLS 1.3: [CECPQ2], [OQS-111], [OQS-PROV], [PST].

В этих экспериментальных реализациях использовался специализированный подход и не предпринималось попыток реализовать какой-либо из документов Internet-Draft, указанных выше.

В недавнем документе рабочей группы TLS [EXTERN-PSK] рассмотрены вопросы комбинирования разнотипного ключевого материвала в TLS, не относящиеся к пост-квантовой криптографии.

В [RFC9370] со статусом предложенного стандарта (Proposed Standard) рассмотрен обмен с несколькими ключами в протоколе IKEv2 (Internet Key Exchange Protocol Version 2), а другая работа IETF включает применение заранее распространённых пост-квантовых ключей в IKEv2 [IKE-PSK]. Расширенная схема подписи Меркла (eXtended Merkle Signature Scheme или XMSS) была опубликована в информационном RFC исследовательской группы Internet (Internet Research Task Force или IRTF) [XMSS].

В научной литературе Ивен (Even) и Голдрайх (Goldreich) [EVEN] инициировали изучение комбинации нескольких симметричных схем шифрования, в работах [ZHANG], [DODIS] и [HARNIK] исследовано сочетание нескольких схем шифрования с открытым ключом, а в работе [HARNIK] введён термин «надежный сумматор» (robust combiner) для обозначения компилятора, создающего из отдельных схем гибридную схему с сохранением свойств безопасности. В статьях [GIACON] и [BINDEL] исследовались комбинации нескольких механизмов инкапсуляции ключей.

Благодарности

Изложенные в документе идеи возникли в ходе обсуждений с многочисленными коллегами, включая Christopher Wood, Matt Campagna, Eric Crockett, Deirdre Connolly, авторов гибридных документов и реализаций, упомянутых в документе, и членов рабочей группы TLS. Непосредственным толчком к созданию документа послужили дискуссии с участниками семинара по пост-квантовым программам в Маунтин-Вью, штат Калифорния, в январе 2019 г. Daniel J. Bernstein и Tanja Lange высказали соображения о рисках неоднократного использования эфемерных открытых ключей. Matt Campagna и команда Amazon Web Services внесли дополнительные предложения. Nimrod Aviram предложил ограничиться секретами фиксированного размера.

Адреса авторов

Douglas Stebila
University of Waterloo
Email: dstebila@uwaterloo.ca

Scott Fluhrer
Cisco Systems
Email: sfluhrer@cisco.com

Shay Gueron
University of Haifa and Meta
Email: shay.gueron@gmail.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru