Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH

Eric Crockett[1], Christian Paquin[2], and Douglas Stebila[3]

[1] *AWS* ericcro@amazon.com
[2] *Microsoft Research* cpaquin@microsoft.com
[3] *University of Waterloo, Waterloo, Ontario, Canada* dstebila@uwaterloo.ca

July 11, 2019

Abstract

Once algorithms for quantum-resistant key exchange and digital signature schemes are selected by standards bodies, adoption of post-quantum cryptography will depend on progress in integrating those algorithms into standards for communication protocols and other parts of the IT infrastructure. In this paper, we explore how two major Internet security protocols, the Transport Layer Security (TLS) and Secure Shell (SSH) protocols, can be adapted to use post-quantum cryptography.

First, we examine various design considerations for integrating post-quantum and hybrid key exchange and authentication into communications protocols generally, and in TLS and SSH specifically. These include issues such as how to negotiate the use of multiple algorithms for hybrid cryptography, how to combine multiple keys, and more. Subsequently, we report on several implementations of post-quantum and hybrid key exchange in TLS 1.2, TLS 1.3, and SSHv2. We also report on work to add hybrid authentication in TLS 1.3 and SSHv2. These integrations are in Amazon s2n and forks of OpenSSL and OpenSSH; the latter two rely on the liboqs library from the Open Quantum Safe project.

1 Introduction

Post-quantum (PQ) cryptographic algorithms have security based on mathematical problems that are widely believed to be difficult for a quantum adversary. The interest in deploying these algorithms is growing due to the desire to hedge against the future possibility of a large-scale quantum computer. NIST is currently in the process of selecting post-quantum algorithms for key exchange and authentication for standardization. Although this is an important step, the adoption of post-quantum cryptography will also depend on the successful transition of communication protocols and applications to use these new algorithms.

Some cryptographic algorithm transitions have happened relatively quickly: for example, AES was released as a FIPS standard in November 2001 [32]; an RFC for its use in TLS was published in June 2002 [13], and included in a December 2002 release of OpenSSL [48]).

However, there are many examples of cryptographic algorithms transitions that took a long time. For example, while elliptic curve cryptography (ECC) was invented in the 1980s, the first FIPS standard using ECC was in 2000 [33], the RFC for its use in TLS appeared in 2006 [31], but it was not enabled for forward secrecy by default by Google until late 2011 [29]. As another example, SHA-2 was published as a FIPS standard in 2002 [34], and theoretical weaknesses in SHA-1 were

known in 2005 [51]. Web browsers did not however stop accepting SHA-1-based certificates until January 2017 [53], only a month before the first collisions in SHA-1 were demonstrated [45, 46].

This highlights the importance of beginning to plan for the transition to post-quantum cryptography early. There are several steps in such a transition. First, each network protocol must be evaluated for any constraints that make it challenging to add new algorithms with potentially new characteristics, such as lack of ability to replace or negotiate cryptographic algorithms, or limitations on sizes of keys or packets. Next, specific choices must be made in how to integrate the new algorithm into the protocol: engineering choices, such as how parameters and keys are represented in network packets, and cryptographic choices, such as how keying material is used. Furthermore, these designs must be done in a way that preserves backward compatibility with endpoints (and middle boxes) that have not yet been upgraded, while achieving desirable protocol functionality for upgraded endpoints.

Finally, the transition to post-quantum cryptography includes a twist not seen in previous cryptographic transitions: the use of two (or more) algorithms simultaneously, in what is being called "hybrid" mode. There have been suggestions that some parties may decide to use both traditional (e.g., elliptic curve Diffie–Hellman) and post-quantum algorithms together for a variety of reasons, such as maintaining compliance with industry or government regulations that have not yet been updated while still obtaining post-quantum security, or for early adopters who want to have the potential of post-quantum security but not rely solely on a newer and relatively untested algorithm.

Contributions. In this paper, we report on case studies exploring how two major Internet security protocols, Transport Layer Security (TLS) and Secure Shell (SSH), can be adapted to use post-quantum cryptography, both for confidentiality (via post-quantum key exchange) and authentication (for post-quantum digital signatures). Each of our case studies include an evaluation of design options in the context of the protocol, selection of one or two instantiations of those design options and an implementation thereof, accompanied by observations and lessons learned from the implementation.

Our specific case studies are as follows:

- TLS 1.2: post-quantum and hybrid key exchange, in OpenSSL 1.0.2 and Amazon s2n
- TLS 1.3: post-quantum and hybrid key exchange, and post-quantum and hybrid authentication, in OpenSSL 1.1.1
- SSH 2: post-quantum and hybrid key exchange, and post-quantum and hybrid authentication, in OpenSSH 7.9

The OpenSSL and OpenSSH implementations rely on the liboqs library from the Open Quantum Safe project, which is a C library that provides implementations of post-quantum KEMs and signatures schemes in a common interface based on implementations from NIST submission packages. As of this writing, liboqs's master branch provides 22 KEMs from 5 families (BIKE, Frodo, Kyber, NewHope, and SIKE) and 9 signature schemes from 2 families (Picnic and qTesla).

The s2n implementation relies on implementations directly from NIST submission packages.

Tables 1 and 2 list the KEM and signature schemes tested in the case studies we examine, and whether each scheme's use was successful in the system.

Related work. There have been a variety of documents outlining high-level perspectives on the general transition to post-quantum cryptography, including a whitepaper by the European Telecommunications Standards Institute [11] and technical report by Hoffman [24]. There have been several Internet-Drafts submitted to the IETF describing mechanisms for adding post-quantum or

Table 1: Test results for key exchange using post-quantum and hybrid key encapsulation mechanisms in TLS and SSH implementations
Fill in table

	s2n (TLS 1.2)	**OpenSSL 1.0.2** (TLS 1.2)	**OpenSSL 1.1.1** (TLS 1.3)	**OpenSSH**
BIKE1-L1 (round 1)	✓ ✓	✓✓	✓✓	✓✓
BIKE1-L3 (round 1)	✓ ✓	✓✓	✓✓	✓✓
BIKE1-L5 (round 1)	✓ ✓	✓✓	✓✓	✓✓
BIKE2-L1 (round 1)	✓ ✓	✓✓	✓✓	✓✓
BIKE2-L3 (round 1)	✓ ✓	✓✓	✓✓	✓✓
BIKE2-L5 (round 1)	✓ ✓	✓✓	✓✓	✓✓
BIKE3-L1 (round 1)	✓ ✓	✓✓	✓✓	✓✓
BIKE3-L3 (round 1)	✓ ✓	✓✓	✓✓	✓✓
BIKE3-L5 (round 1)	✓ ✓	✓✓	✓✓	✓✓
FrodoKEM-640-AES	– –	✓✓	✓✓	✓✓
FrodoKEM-640-SHAKE	– –	✓✓	✓✓	✓✓
FrodoKEM-976-AES	– –	✓✓	✓✓	✓✓
FrodoKEM-976-SHAKE	– –	✓✓	✓✓	✓✓
FrodoKEM-1344-AES	– –	✓✓	✓✓	✓✓
FrodoKEM-1344-SHAKE	– –	✗ ✗		
Kyber512	– –	✓✓	✓✓	✓✓
Kyber768	– –	✓✓	✓✓	✓✓
Kyber1024	– –	✓✓	✓✓	✓✓
NewHope-512-CCA	– –	✓✓	✓✓	✓✓
NewHope-1024-CCA	– –	✓✓	✓✓	✓✓
NTRU-HPS-2048-509	– –	✓✓	✓✓	✓✓
NTRU-HPS-2048-677	– –	✓✓	✓✓	✓✓
NTRU-HPS-4096-821	– –	✓✓	✓✓	✓✓
NTRU-HRSS-701	– –	✓✓	✓✓	✓✓
LightSaber-KEM	– –	✓✓	✓✓	✓✓
Saber-KEM	– –	✓✓	✓✓	✓✓
FireSaber-KEM	– –	✓✓	✓✓	✓✓
SIKEp503 (round 1)	✓ ✓	✓✓	✓✓	✓✓
SIKEp751 (round 1)	✓ ✓	✓✓	✓✓	✓✓
SIKEp964 (round 1)	✓ ✓	✓✓	✓✓	✓✓
SIKEp434 (round 2)	– –	✓✓	✓✓	✓✓
SIKEp503 (round 2)	– –	✓✓	✓✓	✓✓
SIKEp610 (round 2)	– –	✓✓	✓✓	✓✓
SIKEp751 (round 2)	– –	✓✓	✓✓	✓✓

Legend: In each cell, the first symbol is for post-quantum-only key exchange, the second symbol is for post-quantum + ECDH nistp256 key exchange. ✓ denotes success, ✗ denotes failure, – denotes the combination was not tested.

hybrid key exchange in TLS 1.2 [12, 42] and TLS 1.3 [27, 41, 44, 52]; this paper is based in part on some of the ideas in [12, 44]. There have also been Internet-Drafts submitted on post-quantum security for the Internet Key Exchange version 2 (IKEv2) protocol [19, 49].

Various groups have also done experimental demonstrations of post-quantum or hybrid key exchange in TLS 1.2 [8, 9, 10, 37, 43] and TLS 1.3 [28, 38]. This paper includes results based on [37, 38, 43].

Table 2: Test results for authentication using post-quantum and hybrid signatures in TLS and SSH implementations

	OpenSSL 1.1.1 (TLS 1.3)	**OpenSSH**
Dilithium-2	✓✓	✓✓
Dilithium-3	✓✓	✓✓
Dilithium-4	✓✓	✓✓
MQDSS-31-48	✓✓	✓✓
MQDSS-31-64	✓✓	✓✓
Picnic-L1-FS	✓✓	✓✓
Picnic-L1-UR	✓✓	✓✓
Picnic-L3-FS	✗✗	✓✓
Picnic-L3-UR	✗✗	✓✓
Picnic-L5-FS	✗✗	✓✓
Picnic-L5-UR	✗✗	✓✓
Picnic2-L1-FS	✓✓	✓✓
Picnic2-L3-FS	✓✓	✓✓
Picnic2-L5-FS	✓✓	✓✓
qTesla-I	✓✓	✓✓
qTesla-III-size	✓✓	✓✓
qTesla-III-speed	✓✓	✓✓

Legend: In each cell, the first symbol is for post-quantum-only authentication, the second symbol is for post-quantum + ECDSA authentication. ✓ denotes success, ✗ denotes failure, – denotes the combination was not tested.

2 Hybrid modes

TLS and SSH are designed with algorithm agility in mind, so they permit parties to support multiple cryptographic algorithms within each category of functionality (key exchange, public key authentication, symmetric cipher, hash function, etc.); such a combination is called a "ciphersuite" in the context of TLS, and we will use that terminology to apply broadly.

Both TLS and SSH include a mechanism for negotiating which ciphersuite to use, either all-at-once or in an à la carte manner. In principle, negotiation allows for parties which support different subsets of algorithms to select a mutually agreeable ciphersuite, provided they have at least one overlapping supported algorithm in each category. In practice, negotiation works fairly well: while there have been problems with incompatibilities between implementations, these have tended to arise elsewhere in the protocol, not directly in the cryptographic algorithms supported.

However, TLS and SSH are designed to actually negotiate and subsequently use only a single algorithm in each category of the ciphersuite: while they can select from multiple key exchange mechanisms, they have to pick only one to use. To support hybrid modes of key exchange or authentication, the protocol must be modified to indicate how to negotiate a combination of algorithms to use in hybrid mode, and how to combine them cryptographically.

In this section we explore high-level goals and design considerations for hybrid modes of key exchange and authentication. In subsequent sections, we discuss options specific to particular versions of TLS and SSH.

2.1 Goals for hybrid modes

The primary goal of a hybrid mode is to ensure that the desired security property holds as long as one of the component schemes remains unbroken. For key exchange, this means that the session key should remain secure (and thus application data confidential) as long as one of the component key exchange mechanisms is unbroken. For authentication, this means that the protocol should provide authentication as long as one of the digital signatures schemes is unbroken at the time of session establishment.

In addition to the primary cryptographic goals, there may be several additional goals for hybrid modes in real-world network protocols. These include:

Backwards compatibility. Clients and servers who are "hybrid-aware", i.e., compliant with whatever hybrid mode is added to TLS or SSH, should remain compatible with endpoints and middle-boxes that are not hybrid-aware.

The three scenarios to consider are:

1. Hybrid-aware client, hybrid-aware server: These parties should negotiate and use hybrid modes.
2. Hybrid-aware client, non-hybrid-aware server: These parties should negotiate a traditional (non-PQ) ciphersuite (assuming the hybrid-aware client is willing to downgrade to traditional-only).
3. Non-hybrid-aware client, hybrid-aware server: These parties should establish a traditional (non-PQ) ciphersuite (assuming the hybrid-aware server is willing to downgrade to traditional-only).

Ideally backwards compatibility should be achieved without extra round trips and without sending duplicate information; see below.

High performance. Use of hybrid modes should not be prohibitively expensive in terms of computational performance. In general this will depend on the performance characteristics of the specific cryptographic algorithms used, and the hybridization should not substantially affect performance. Preliminary results about such performance include [8, 9, 10].

Low latency. Use of hybrid modes should not substantially increase the latency experienced to establish a connection. Factors affecting this may include the following:

- The computational performance characteristics of the specific algorithms used. See above.
- The size of messages to be transmitted. Public key / ciphertext / signature sizes for post-quantum algorithms range from hundreds of bytes to over one hundred kilobytes, so this impact can be substantial. See [8, 9] for preliminary results in a laboratory setting, and [30] for preliminary results on more realistic networks.
- Additional round trips added to the protocol. See below.

No extra round trips. Attempting to negotiate hybrid modes should not lead to extra round trips in any of the three hybrid-aware/non-hybrid-aware scenarios listed above.

No duplicate information. Attempting to negotiate hybrid modes should not mean having to send multiple cryptographic values for the same algorithm.

2.2 Design considerations for hybrid modes

In general, we identify four distinct axes along which one can make choices when adding support for hybrid modes. These are:

1. How to negotiate the use of hybridization in general, and component algorithms and parameters specifically?
2. How many component algorithms can be combined?
3. How should cryptographic data from multiple algorithms (public keys / ciphertexts / signatures) be conveyed?
4. How should cryptographic data from multiple algorithms (e.g., shared secrets) be combined?

Some of the answers to these questions are specific to details of a particular network protocol, while others are independent of protocol specifics.

2.2.1 Negotiation

Many network protocols, including TLS and SSH, negotiate which algorithms to use with the following basic approach: one party sends an ordered list of supported algorithms, and the other party responds either with a single selection from that list, or with their own ordered list of supported algorithms (and then the protocol specifies how to mutually select a single element from two ordered lists). If no mutually supported algorithm can be found, an error is raised or communicated.

For hybrid modes, the goal is to negotiate two or more algorithms and use both of them. The main choice to make when negotiating algorithms for hybrid modes is whether each algorithm in the hybrid mode should be negotiated separately or as a single combined algorithm. A second choice is whether separately or jointly negotiate parameterizations of a cryptographic algorithm. For example, in key exchange, a ciphersuite could either specify that the key exchange will be "ECDH", with parameters specified separately, or the ciphersuite could include both the algorithm and parameters, e.g., "ECDH+nistp256".

If each algorithm is to be negotiated separately, then the protocol's message formats and logic will need to be modified to allow negotiation of multiple component algorithms. The designer of the negotiation mechanism must also choose whether to separately negotiate component algorithms of different types – for example, "select one of the following traditional algorithms, select one of the following post-quantum algorithms" – or not formally (at least within the protocol syntax) distinguish between algorithm types – for example, "select two of the following algorithms" where it is up to the implementation to pick one traditional and one post-quantum. Care must be taken to ensure that individually negotiated algorithms having matching security levels. There is also the potential that additional message formats for conveying a second list to negotiate may affect backwards compatibility with old implementations.

In contrast, negotiating an overall combination of algorithms can be more easily accomplished by defining new identifiers that simply represent a pair of algorithms. This requires no new protocol logic or message format modifications during negotiation (although later cryptographic computations must still be updated to use both algorithms). However, drawbacks of this approach could be that a quadratic number of algorithm identifiers must be defined, one for each combination, and that some protocols may end up sending duplicate values (see TLS 1.3 key exchange below).

2.2.2 Number of component algorithms

The key decision to make here is whether the number of algorithms that can be combined in a single hybrid mode is fixed or variable, and if fixed, how many. There appears to be no consensus on this

matter: some Internet-Drafts for hybrid key exchange in TLS have fixed to two algorithms [12, 27, 41], others have a variable number of two or more [42, 52].

2.2.3 How to convey cryptographic data

If hybrid modes are to be used, then the parties must convey cryptographic data (public keys, ciphertexts, signatures) for multiple cryptosystems within the protocol. Many protocols, including TLS and SSH, are designed with some extensibility, but not in arbitrary locations: in TLS, for example, the `ClientHello` and `ServerHello` messages explicitly support extensions, but other messages do not.

To convey cryptographic data from multiple algorithms, one could either try to extend the messages in which the cryptographic data is sent to provide additional locations for cryptographic values, or one could concatenate the data from multiple algorithms into a single value and place that in the existing message structure. In general the latter is simpler (since it requires no changes to the protocol format or logic), and potentially has fewer backwards compatibility concerns, but it can lead to duplication; see the example of key exchange in TLS 1.3 in section 3.2.

2.2.4 How to combine cryptographic data

Decisions must also be made about how to cryptographically combine two or more algorithms in a way that provides the intended hybrid security property: the combination is secure as long as one of the component algorithms remains secure. For example: when combining session keys from two key exchange algorithms, should we XOR them? concatenate them? concatenate then feed into a key derivation function? Here protocol designers should make decisions informed by the literature, which we review briefly.

In terms of confidentiality properties, Even and Goldreich [18] initiated the study of combining multiple symmetric encryption schemes; [14, 23, 55] examined combining multiple public key encryption schemes, and Harnik et al. [23] coined the term "robust combiner" to refer to a compiler that constructs a hybrid scheme from individual schemes while preserving security properties. More recently, Giacon et al. [20] and Bindel et al. [6] examined combining multiple key encapsulation mechanisms.

For digital signatures, Bindel et al. [7] consider combiners for digital signature schemes.

3 Key exchange case studies

In this section we report on design considerations, instantiations, and learnings from adding post-quantum and hybrid key exchange to the TLS and SSH protocols.

3.1 Key exchange in TLS 1.2

This section describes two approaches to implementing hybrid key exchange in TLS 1.2. Although it is not clear that post-quantum TLS 1.2 will be broadly adopted in light of TLS 1.3, there are several reasons why it is interesting to implement hybrid key exchange in TLS 1.2. First, both the general interest in hybrid and the implementation efforts described below predate the standardization of TLS 1.3. Second, TLS 1.2 allows the community to evaluate hybrid key exchange on its own merits, without being complicated by orthogonal issues related to TLS 1.3 (such as infrastructure problems, implementation bugs, etc). Examining TLS 1.2 allows us to isolate problems due to the intricacies of post-quantum cryptography from issues of using a relatively new network protocol. Finally,

even though TLS 1.3 has been standardized, TLS 1.2 still accounts for 86% of encrypted internet traffic [47].[1] Although the adoption rate for TLS 1.3 is increasing, we expect that TLS 1.2 will be in use far into the future.

3.1.1 Design considerations

Besides the implementations described below [37, 43], there have been several experimental implementations of post-quantum and/or hybrid key exchange in TLS 1.2 [8, 9, 10] and proposed Internet-Drafts [12, 42].

Negotiation. For hybrid key exchange, the first choice to make, as noted in section 2.2, is whether to negotiate component algorithms individually or together. The second choice is whether to negotiate parameterizations separately or jointly. [42] negotiates the two hybrid algorithms separately: a new `TLS_QSH` ciphersuite is defined, then the particular classical and post-quantum algorithms are individually negotiated; the post-quantum algorithm parameterizations are negotiated jointly, i.e., a single algorithm identifier `ntru_eess439`. In contrast, [12, 43] defines new hybrid ciphersuites with pairs of algorithms (e.g., `ECDH_BIKE`, `ECDH_SIKE`), with parameters for the post-quantum algorithm negotiated separately. Finally, the implementations [8, 9, 10] take a third approach, in which they choose to negotiate the post-quantum algorithms and parameterizations together, by defining new ciphersuites with selected proposed combinations (e.g., `ecdh+frodo-640`, `ecdh+newhope1024`, etc.); the specific elliptic curve is negotiated using the existing curve negotiation mechanism.

Combining shared secrets. All Internet-Drafts and implementations we have seen so far concatenate the two raw shared secrets (the ECDH shared secret and the PQ shared secret) and use that as the TLS "pre-master secret", which is then input into the TLS key derivation function to compute a master secret from which session keys are derived. Other approaches could include XORing the shared secrets to derive the pre-master secret, or putting them through a KDF to derive the pre-master secret. One issue to consider carefully is checking that such a combination is supported by a security argument. [6, 20] gives a positive result for concatenation when the public keys / ciphertexts are included in the key derivation function, but the basic TLS 1.2 key schedule does not do this.

3.1.2 An example instantiation: OpenSSL

The Open Quantum Safe project implemented post-quantum and hybrid key exchange in TLS 1.2 in a fork of OpenSSL 1.0.2 [37] using KEMs from liboqs.

That implementation added both PQ-only and hybrid key exchange.[2] The rest of this subsection explains how hybrid key exchange is implemented in TLS 1.2, since PQ-only is implemented just by adding another algorithm. Only ECDH is supported as the traditional algorithm in the hybrid key exchange.

[1] At 7% of encrypted traffic, TLS 1.3 just edged out TLS 1.0 (6.8% of encrypted traffic), a protocol obsoleted by TLS 1.1 in 2006.

[2] One note about this implementation is that it relies on liboqs's "default" algorithm mechanism rather than naming each PQ algorithm specifically. liboqs provides an interface to use each of its supported algorithm at runtime, as well as a generic function for a "default" algorithm, where the mapping of the default algorithm has to be changed at compile-time. To simplify this preliminary prototype implementation of PQ algorithms in TLS 1.2, there are just two ciphersuites: one using liboqs' default algorithm, and one using liboqs' default algorithm in hybrid with ECDH. This means that the TLS implementation will end up using whichever algorithm was configured at compile-time, but cannot switch between them at runtime. This is of course not suitable for a production implementation, but as a basic prototype still allows a developer or researcher who controls both a client and server to test how TLS performs with a specific post-quantum algorithm by recompiling.

The implementation negotiates the combination of algorithms (and parameterizations) together, primarily due to the simplicity of the implementation when doing so. Note that which curve to use for ECDH is negotiated using a separate mechanism in TLS 1.2 (the `NamedCurve` extension). The number of component algorithms in a hybrid mode is fixed to two.

The hybrid implementation conveys cryptographic data (public keys / ciphertexts) of the two KEMs within the existing `ServerKeyExchange` and `ClientKeyExchange` messages, respectively, by concatenating the public keys / ciphertexts of the two algorithms to send, and then parsing them when receiving.

To compute the combined shared secret, the implementation uses the concatenation method as described above, in particular that the premaster secret is the concatenation of the shared secrets from the two algorithms. The premaster secret is used directly in the existing TLS 1.2 KDF, without including any public keys or ciphertexts in the KDF input.

3.1.3 An example instantiation: s2n

This subsection describes an alternate approach to hybrid key exchange in TLS 1.2, implemented by AWS Cryptography in version 0.9.0 of Amazon's TLS implementation, s2n [43]. The changes to the TLS handshake are formally specified in an IETF draft [12]. The draft and implementation in s2n only define hybrid ciphersuites with exactly one classical key exchange component and exactly one post-quantum key exchange component; in particular they do not implement PQ-only ciphersuites.

s2n modifies the TLS handshake so that the two key exchanges are performed simultaneously and independently. We defined new ciphersuites where the key exchange mechanism is a hybrid between ECDHE and a post-quantum KEM. For example, `TLS_ECDHE_SIKE_ECDSA_WITH_AES_256_GCM_SHA384` is a hybrid ciphersuite with ECDHE for the classical component and SIKE for the PQ component of the key exchange. The ciphersuite specifies a PQ key exchange *algorithm*, but leaves the *parameters* to an (optional) ClientHello extension. It uses a single extension to specify parameters for all PQ schemes, rather than using a different extension for each scheme, simplifying the process of extending the draft to add support for more PQ KEMs.

After the server accepts a proposed hybrid ciphersuite and selects parameters, it generates a classical ECDHE key pair and a PQ KEM key pair. Both public keys are sent in the ServerKeyExchange message by adding a new field for the KEM key. The client runs the KEM encapsulation algorithm and sends a KEM ciphertext in a new field of an augmented Client KeyExchange message. Finally, the server runs the KEM decapsulation algorithm to obtain the KEM secret.

This process produces an ECDHE secret Z and a post-quantum secret K. The TLS premaster secret is the concatenation $Z||K$ of these values. The master secret is derived from the premaster secret using the standard TLS 1.2 KDF, except that we also extend the TLS PRF seed by concatenating the ClientKeyExchange message as suggested in [5, Section 3.2]. This ensures that the hybrid key exchange is provably secure.

As described in section 3.1.2, the OQS fork of OpenSSL 1.0.2 implements hybrid key exchange in TLS 1.2 using a different method, but the OQS team has plans to update the that implementation to align with the specification [12] to achieve interoperability with s2n.

3.1.4 Lessons learned

Ease of implementation. The design choices for the OpenSSL instantiation led to a speedy implementation with relatively few changes in the OpenSSL codebase and no changes to the TLS 1.2 protocol structure. The s2n instantiation required a bit more work to add a ClientHello extension and to extend the ClientKeyExchange and ServerKeyExchange messages.

Combinatorial explosion. Both instantiations had to add new ciphersuite identifiers corresponding to our new ciphersuites. Because TLS 1.2 negotiates almost everything all at once in a combined ciphersuites, there is a "combinatorial explosion" of identifiers: a single ciphersuite contains the key exchange method (RSA versus finite-field Diffie–Hellman versus ECDH), the authentication method (RSA versus ECDSA), the symmetric cipher (AES-128-CBC, AES-128-GCM, AES-256-CBC, AES-256-GCM, Triple-DES-CBC, Camellia, IDEA, and more) and the hash function (SHA-2, SHA-1).

Adding post-quantum and hybrid algorithms to the ciphersuite would further explode the list. As noted in footnote 2, the OpenSSL instantiation actually used an indirect method with a single post-quantum algorithm identifier, and fixed the PQ algorithm at compile-time, which is sufficient for limited prototyping but not suitable for production use. The s2n instantiation limited the explosion by only supporting two PQ KEMs (BIKE and SIKE), and also by negotiating PQ parameters in a ClientHello extension rather than as part of the ciphersuite.

Which solution should be used in the long run depends on how many algorithms are selected for standardization by NIST.[3] If a large number of PQ algorithms are standardized, then it may be preferable to follow the approach taken for ECDH and [12] in TLS 1.2 and use a separate extension to negotiate the PQ parameters, despite the requirement to add a new extension and more negotiation logic. However if a small number of PQ algorithms are standardized, then it maybe preferable to put those algorithms directly into the ciphersuite and accept the accompanying combinatorial explosion.[4]

Message sizes. We did not encounter any difficulties with buffers or protocol limits with large messages. Both instantiations could be extended to support all round 2 candidates of the NIST standardization process.

No duplication. Because the key exchange algorithm is negotiated before any cryptographic data is sent in TLS 1.2, no unnecessary or duplicate data is sent, even in the OpenSSL instantiation where concatenation is used.

Use in applications. The OQS team has used its fork of OpenSSL in a range of scenarios with effectively no changes. The OpenSSL command-line test programs `s_client` and `s_server` can be used to demonstrate OpenSSL's TLS functionality directly, and work without modifications.

There are a large number of applications built upon OpenSSL. OQS has successfully used the Apache web server [2] and the Links command-line web browser [50] with PQ and hybrid ciphersuites from our OpenSSL 1.0.2 fork, simply by recompiling the applications against their version of OpenSSL and specifying the desired ciphersuite in a run-time configuration option. A team from Microsoft Research [16] also successfully built a post-quantum version of the OpenVPN virtual private networking tool [39] based on this fork.

Extensibililty. The initial design of [12] (version 00) used unique extensions to specify the parameters of each PQ algorithm. Since the draft only defined two PQ schemes, this only required two new extensions. However, this design decision made it difficult for others to extend the draft with new algorithms. Thus in the current version of the draft, clients specify the parameters they support for all PQ algorithms in a single ClientHello extension.

[3] In fact it may be that there is little appetite to add post-quantum algorithms to TLS 1.2 and focus solely on TLS 1.3, but let us presuppose desire to use PQ and hybrid in TLS 1.2 for the purposes of this discussion.

[4] This explosion can be somewhat limited by not creating ciphersuites for every possible combination: e.g. one could choose to skip ECDH+PQ+RC4+SHA1, and focus solely on adding PQ to ciphersuites with strong symmetric ciphers.

3.2 Key exchange in TLS 1.3

TLS 1.3 provides many efficiency and security benefits over its predecessor. Although the final specification approved by the IETF does not support quantum-safe cryptography, improved modularity in TLS 1.3's design makes it more amenable to supporting quantum-safe cryptography. The OQS team implemented post-quantum and hybrid key exchange in TLS 1.3 in a fork of OpenSSL 1.1.1 [38] using KEMs from liboqs.

3.2.1 Design considerations

An Internet-Draft by Stebila and Gueron [44], upon which part of this document is based, details various design choices for TLS 1.3 along the different axes identified in section 2.2. We describe some of those here.

Negotiation. TLS 1.3's overall design for negotiation is different from TLS 1.2 in that it does away with the idea of monolithic ciphersuites that negotiate all cryptographic choices at once; instead TLS 1.3 negotiates each component (symmetric cipher, digital signature scheme, key exchange method) separately. Ephemeral key exchange in TLS 1.3 as standardized is based entirely on elliptic curve Diffie–Hellman. A `supported_groups` extension is used to negotiate which named elliptic curve to use. Negotiating hybrid key exchange algorithms in TLS 1.3 could take several approaches.

For negotiating each hybrid component algorithm individually, [41] proposed adding a second extension with a second list of key exchange methods. [44, §3.1.2] proposed two other options for individual algorithm negotiation which use delimiters within the existing `supported_groups` extension.[5] All of these approaches require some change in negotiation logic.

For negotiating hybrid algorithms as a combination, one could define new entries for the `supported_groups` list for each desired combination, as in section 3.1.2 and in [27]; the identifiers for these new entries have no internal structure, and those require no new processing logic. By contrast, [52] and [44, §3.1.3.3] describes more complicated representations of combinations of algorithms with an internal structure that requires additional processing logic for negotiation.

Conveying cryptographic data. Of course one could just concatenate public keys / ciphertexts in the `key_share` extension in the `ClientHello` and `ServerHello` message, as in [27, 52]. This is simple, but has one drawback, which is that it can result in duplication or additional round trips. For example, suppose a client wants to negotiate ECDH with old servers, and ECDH+PQ with hybrid-aware servers. If the client sends just an ECDH+PQ concatenated public key, an old server will not know how to parse the ECDH portion from the concatenated public key, without triggering an extra round trip with the `HelloRetryRequest` message. The client must send one key share containing just an ECDH public key, and another keyshare containing an ECDH public key concatenated with a post-quantum key, thus sending two ECDH public keys. Admittedly ECDH public keys happen to be small compared to most PQ public keys, but wasted bytes should still be avoided where possible.

However, TLS 1.3 actually allows for the `ClientHello key_share` extension to contain multiple public keys from different algorithms, so additional public keys could be included here. (However the `ServerHello key_share` extension only allows a single public key, so an alternative would have to be identified for the server's response.)

Alternatively, [41] adds extensions to the `ClientHello` and `ServerHello` messages for sending additional key shares.

[5] Technically these are not elliptic curve groups, but the "groups" terminology is from the TLS 1.3 specification.

Combining shared secrets. The basic approaches of concatenating, XORing, or KDFing together the shared secrets from each algorithm as described for TLS 1.2 in section 3.1.2 can also be applied in TLS 1.3. The TLS 1.3 key schedule is more complex than the TLS 1.2 schedule, but conveniently hashes the transcript into the key derivation, so results on safely combining KEM keys from [6, 20] more readily apply. The more complex key schedule provides additional options for combining shared secrets in hybrid key exchange: for example [41] suggests adding a new step to the key schedule for each additional key exchange algorithm in the hybrid mode.

Size limits. The maximum size of a `key_exchange` value in a `key_share` extension in the `ClientHello` is $2^{16} - 1$ bytes, which is smaller than the public key size of some round 2 submissions (e.g., Classic McEliece parameter set "8192128f").

3.2.2 An example instantiation

The OQS team implemented both PQ-only and hybrid key exchange in OpenSSL 1.1.1.[6]

For negotiation, the basic approach is to define "groups" for the `supported_groups` extension for each new PQ or hybrid scheme (pretending to be elliptic curves for the purposes of negotiation). PQ-only algorithms are negotiated by a new algorithm identifier directly. Hybrid algorithms are negotiated by the combined method, where each combination is a new `NamedGroup` entry with no internal structure to the identifier. As noted above, this means no new negotiation logic is required. The number of algorithms combined in a hybrid mode to fixed to two at a time.

The implementation uses the concatenation approach to convey public keys. This work was started before the TLS 1.3 standard was completed, and before OpenSSL had complete support for the updated protocol. In particular, at the time OpenSSL only supported one `key_share` extension, ruling out some more complicated integrations noted above. This implementation therefore chose an approach that was easy to prototype, and would give a quick indication on how post-quantum algorithms perform in TLS 1.3. While this can result in duplication, we expect that typical usage will see clients advertise ECDH, and one or more examples of ECDH plus a hybrid algorithm, so the only duplication is the approximately 32-byte ECDH public key.

For computing the shared secret, the implementation concatenates the individual shared secrets and used them in place of the original ECDH shared secret in the TLS 1.3 key schedule.

3.2.3 Lessons learned

Ease of implementation. The OpenSSL library as currently written is not architected in a way that made modifications as general as would be desired. Note that OpenSSL is broadly structured in two components: libcrypto, which implements cryptographic primitives, and libssl, which implements SSL and TLS by relying on libcrypto for its cryptography. Since a Diffie–Hellman-like key exchange method is expected, the TLS layer calls into the crypto layer using a DH "generate key" and "generate message" API. One the other hand, NIST submissions are KEMs, and the liboqs library we use supports a 3-step KEM style API. Moreover, the lower-level crypto API doesn't have the context of the TLS-level caller, so the crypto implementation can't know if it is being called from the client or the server side of the TLS layer. Because of these limitations, the implementation couldn't integrate KEM key exchange schemes cleanly at the crypto layer of the OpenSSL library; it must instead do so at the TLS layer itself, forwarding calls to OQS as needed. Perhaps future

[6] Unlike OQS's TLS 1.2 implementation in OpenSSL 1.0.2, this implementation doesn't rely on liboqs' default identifier; each PQ algorithm gets its own full-fledged identifier in OpenSSL 1.1.1.

versions of OpenSSL will provide a KEM API from libcrypto as the KEM formalism becomes more widespread.

(Lack of) combinatorial explosion. The à la carte negotiation approach of TLS 1.3 made parts of the implementation even easier compared to the TLS 1.2 implementation, since it avoided the combinatorial explosion that came from using a single identifier for the full ciphersuite.

Unclear failures. There were some problems when integrating KEMs into TLS 1.3. In particular, not all of the KEMs present in liboqs would run successfully in the OpenSSL 1.1.1 fork. Round 1 KEMs present in liboqs for which there were failures when used in TLS 1.3 include: PQ-only and hybrid methods using bigquake1, bigquake2, bigquake3, ledakem_C5_N03, ledakem_C5_N04, lima_sp_2062_cca, titanium_cca_std, titanium_cca_hi, titanium_cca_med, titanium_cca_super, and the hybrid of nistp256 + saber_light_saber hybrid. See table 1 for a complete summary. The implementors weren't able to fully investigate the individual failures, so it is unclear whether these were due to protocol problems, quirks in OpenSSL, flaws in liboqs, or bugs in the algorithms' implementation. A preliminary conclusion however is that a PQ scheme might not work out of the box in TLS (or SSH), so it is therefore desirable to test all remaining round 2 schemes to 1) understand their real-life limitations, and 2) understand how these security protocols must evolve to accommodate PQ schemes with bigger artifact requirements.

Use in applications. The OpenSSL command-line test programs `s_client` and `s_server` can be used to demonstrate OpenSSL's TLS 1.3 functionality directly, and work without modifications.

Because OpenSSL 1.1.1 has public API changes compared to the long-lived OpenSSL 0.9 and 1.0 series, major applications are only gradually coming be updated to build against OpenSSL 1.1.1.

3.3 Key exchange in SSHv2

At the highest level, SSH version 2 has a similar architecture to TLS, with an initial negotiation, followed by establishment of an authenticated session key via key exchange and digital signatures, which then is used in symmetric authenticated encryption.

3.3.1 Design considerations

Negotiation. SSHv2 is designed for algorithm agility; one notable difference is that algorithm identifiers in SSHv2 are strings, rather than numbers or binary codes, and the list of supported algorithms is just a comma-separated list of algorithm strings. PQ algorithms can be added directly as new strings. Hybrid combinations can be added as new strings naming both algorithms.

Conveying cryptographic data. In SSHv2, each key exchange method gets to define its own message format for its messages, so it is possible for hybrid key exchange methods to provide distinct fields for each component value.

Combining shared secrets. The output of key exchange in SSHv2 is a shared secret K and an "exchange hash" H; symmetric keys are then derived by hashing K and H with various labels. The computation of the exchange hash H is specified by the key exchange mechanism, but in all cases includes a subset of the transcript including identification strings, negotiation messages, and ephemeral public keys, as well as the shared secret K. The basic approaches of concatenating, XORing, or KDFing together the shared secrets from each algorithm as described for TLS 1.2 in section 3.1.1 can all be employed.

Message sizes. Message lengths in SSHv2 are represented by 4-byte length fields, theoretically accommodating 2^{32}-byte messages, large enough for all round 2 submissions. However, RFC 4253

[54, §6.1] only requires that implementations be able to process packets containing payloads of size 32,768 bytes, and "SHOULD" be able to process larger packets. OpenSSH has a `MAX_PACKET_SIZE` of 2^{18} =262,144 bytes, which, while larger than the minimum value required by the RFC, is smaller than the public keys needed for two Round 2 candidates. In particular, all versions of NTS-KEM [1] and both parameter sets for McEliece [4] have public keys larger than 2^{18} bytes. Therefore, adding these schemes to OpenSSH would not be as straightforward as adding other PQ algorithms.

3.3.2 An example instantiation

A pre-Internet-Draft document by Hansen et al. [22] (not submitted to the IETF) describes the basic approach to how PQ and hybrid key exchange was implemented in the Open Quantum Safe project's fork of OpenSSH [36] (although that document only describes the BIKE and SIKE KEMs, [36] includes additional KEMs from liboqs).

Negotiation is as above; hybrid algorithms have new strings naming both algorithms such as `ecdh-nistp384-bike1-L1-sha384@openquantumsafe.org`. Public keys and ciphertexts are conveyed in specific fields added to the relevant key exchange message. Shared secrets are combined using concatenation.

3.3.3 Lessons learned

There were no unusual circumstances in implementing PQ and hybrid key exchange in SSHv2, including no concerns about message sizes with the schemes we implemented so far. Though this implementation does not include NTS and Classic McEliece, we reiterate that they have public keys that are too large for OpenSSH to handle; further modifications to OpenSSH would be required to support these schemes. À la carte negotiation of individual cryptographic components avoids combinatorial explosion like in TLS 1.2; however there does not appear to be a way to extend the `SSH_MSG_KEXINIT` negotiation message to provide a separate list for individually negotiating the component algorithms of a hybrid mode.

4 Authentication case studies

We now turn to case studies of adding post-quantum and hybrid authentication to the TLS and SSH protocols. Authentication has an additional complication compared to key exchange: there is a long-term credential that must be stored and distributed. In TLS, X.509 certificates are used for long-term credentials; in SSHv2, the usual format is a raw public key (there are some proposals for use of X.509 or other certificates, but raw public keys remain dominant).

4.1 Authentication in TLS 1.3

Although there have been several Internet-Drafts and experimental implementations of PQ and/or hybrid key exchange in TLS as noted in section 3.1, none of those works considered PQ or hybrid authentication. This is likely to due to the general consensus that confidentiality against quantum adversaries is a more urgent need than authenticity, since quantum adversaries could retroactively attack confidentiality of any passively recorded communication sessions, but could not retroactively impersonate parties establishing a (completed) communication session. Nonetheless, advent of a quantum computer would mean that we would eventually need to migrate to post-quantum authentication, meriting some preliminary investigation.

While there will certainly a need for implementations to support both old (non-PQ) and new (PQ) algorithms for authentication and to be backwards compatible with implementations that have not yet been upgraded during a transition period, there may perhaps be a slightly weaker need for hybrid authentication than hybrid key exchange, since post-quantum authentication may not be activated until later in the PQ transition when algorithms have had more time to be studied compared to the need for quantum-resistant confidentiality well in advance of a quantum computer. Still we consider some of the issues with hybrid authentication below.

4.1.1 Design considerations

Negotiation. TLS 1.3 has two extensions to negotiate signature algorithms: the `signature_algorithms_cert` extension is used to negotiate which algorithms are supported for signatures in certificates, and the `signature_algorithms` extension for which algorithms are supported in the protocol itself. Both of these extensions are a list of algorithm identifiers. Effectively the same considerations apply for each of these as for the `supported_groups` extension for negotiating the key exchange method as described in section 3.2.1: to negotiate hybrid components individually, additional lists could be added for each type, or delimiters could be used within the existing lists; to negotiate as a combination, new identifiers for each combination could be defined without internal structure, or with internal structure.

Conveying public keys. In TLS 1.3, public keys for authentication are usually conveyed via X.509 certificates. To convey public keys for multiple algorithms in a hybrid mode, one has to decide whether to extend the TLS protocol to convey multiple certificates, or try to convey multiple keys within the same certificate.

With regards to conveying multiple certificates within the TLS protocol, the `Certificate` message in TLS 1.3 does have a certificate list which permits multiple certificates, which could theoretically be used for this purpose. Historically, this list was used to convey a single certificate chain from the end-entity certificate through requisite intermediate CAs, and was required to be ordered. The TLS 1.3 specification says "implementations SHOULD be prepared to handle potentially extraneous certificates and arbitrary orderings from any TLS version, with the exception of the end-entity certificate which MUST be first." [40, §4.4.2] This suggests it may be possible to use multiple end-entity certificates with different algorithms in the list, though a survey of implementations would need to be made to check compatibility.

The alternative would be to have a single X.509 certificate contain multiple public keys. Again there are choices here: should the multiple algorithms be treated individually (finding different locations within the certificates to store the different keys) or combined (by concatenating them into an opaque data structure)? Similarly, how should a hybrid signature by the certificate authority be treated? Part of the answer to this question depends on whether the same certificate can be targetted to solely new hybrid-aware parties, or must be backwards-compatible with old non-hybrid-aware parties. Bindel et al. [7] and Kampanakis et al. [25] explore various ways for X.509 certificates to convey multiple keys and signatures in backwards-compatible ways.

Conveying signatures. Parties in TLS 1.3 sign the handshake transcript and convey that signature in the `CertificateVerify` message. For hybrid authentication, there would need to be a way to convey two signatures.

Unfortunately, the `CertificateVerify` message does not have any built-in way of being extended, so it could only be extended or duplicated with a change in the protocol's logic or state machine based on the result of negotiation. The simpler approach is to concatenate the two signatures into

a single message; at this point in the protocol, the parties have already agreed to use a hybrid algorithm, so there is no backwards compatibility risk nor any fear of duplicating values.

With hybrid signatures, it should be noted that there is a question of what to sign: do both algorithms sign the message, or does one algorithm sign the output (signature) from the other algorithm? This is discussed in Bindel et al. [7], but the basic answer is that both algorithms should sign the same message (or at least the hash of that message).

Size limits. The maximum size of an X.509 certificate (or raw public key) in TLS 1.3 is $2^{24} - 1$ bytes, which is large enough for all round 2 submissions. Signature size in TLS 1.3 is limited to $2^{16} - 1$ bytes, which is too small for some round 2 signature schemes, for example Picnic-{L3,L5}-{FS,UR}.

4.1.2 An example instantiation

The OQS team's implementation in OpenSSL 1.1.1 added both PQ-only and hybrid authentication, including generation of X.509 certificates with those keys and signatures.

It takes the concatenation approach to defining hybrid combinations: new algorithm identifiers are defined for each desired combination (with no internal structure to the identifier); public keys are concatenated; both signatures are on the same data, and are concatenated. This approach allowed for a simpler integration that could be traced through deeper into OpenSSL's libcrypto layer (specifically its "envelope" (EVP) API) and enabling all functionality (basic signatures, certificate management, and TLS authentication) to be supported for hybrid algorithms.

Specifically for hybrid signatures, a traditional and a PQ signature are generated on the same data, and the resulting signatures are concatenated; the traditional and PQ keys are also concatenated when serialized. The signed data is first hashed using the SHA-2 hash function matching the security level of the PQ scheme (SHA-256 for NIST level 1, SHA-384 for NIST levels 2 or 3, SHA-512 for NIST levels 4 or 5) before being signed by the traditional algorithm (which can't support arbitrarily long messages), but is passed directly to the PQ signature API (which handles arbitrarily long messages, typically via hash-and-sign). The hybrid scheme is identified as a new combo scheme with a unique identifier. Currently, the supported traditional algorithms in hybrid mode are ECDSA with nistp256 and RSA-3072 with NIST level 1 PQ schemes, and ECDSA with nistp384 with NIST level 3 PQ schemes.

4.1.3 Lessons learned

Ease of implementation. As noted above, supporting post-quantum authentication requires support in more places through the codebase since certificates come into play. For hybrid, the concatenation approach of making combined algorithms allowed for a simpler implementation, since the hybrid signatures would be treated monolithically within the existing APIs, rather than needing to adapt every API to handle two certificates, two public keys, two signatures, etc.

As noted above, TLS 1.3 has limits on the size of a signature which are constraining for some round 2 PQ signature schemes; refer to table 2. This is also the case for TLS 1.2. Earlier versions of the OQS fork of OpenSSL 1.0.2 included post-quantum authentication in TLS 1.2, and the Picnic team reports that they successfully patched our fork of OpenSSL 1.0.2 to allow a larger signature size ($2^{24} - 1$ rather than $2^{16} - 1$ by increasing a 2-byte length field to a 3-byte length field), and were subsequently able to use larger signatures successfully. This suggests that the TLS 1.3 specification could be altered to allow larger signatures, although some flag must then be used to communicate that larger length fields are being used. Recall, however, from section 3.3.1 that particular instantiations of SSH may limit packet sizes below what is required by some PQ schemes.

4.2 Authentication in SSHv2

4.2.1 Design considerations

Negotiation. Similarly to negotiation of key exchange in SSHv2, authentication is negotiated using a list of comma-separated strings, to which we can add PQ algorithms and hybrid combinations as new strings.

Conveying public keys. SSHv2 primarily uses raw public keys for authentication. Each authentication method can define its own format for the "public key blob" value, so it is possible for hybrid authentication methods to provide distinct fields for each component value.

Conveying signatures. The signature value is also algorithm-defined, so can easily accommodate concatenated signatures.

Message sizes. Message lengths in SSHv2 are represented by 4-byte length fields, theoretically accommodating 2^{32}-byte messages, large enough for all round 2 submissions. RFC 4253 [54, §6.1] requires that implementations be able to process packets containing payloads of size 32,768 bytes, and "SHOULD" be able to process larger packets. Note that Picnic-{L3,L5}-{FS,UR} has signatures greater than 2^{16} bytes but less than 2^{18} bytes. This means that while some Picnic parameters pose a challenge for use with TLS 1.3, they should work fine with OpenSSH.

4.2.2 An example instantiation

The OQS team's implementation in OpenSSH v7.9 added both PQ-only and hybrid authentication.

For hybrid modes, the basic approach is concatenation.

For negotiation, new key types have been defined for the hybrid cases, identified by concatenating algorithm names; the implementation supports RSA-3072 or ECDSA with nistp256 (for NIST level 1 schemes) or nistp384 (for NIST levels 2 or 3) as the traditional algorithm.

Public keys are serialized sequentially: the traditional key is serialized first, followed by the PQ one. The SSH key encoding contains all the length and serialization information, so the OpenSSH serialization for each type is called sequentially. These concatenated public keys are used both on the wire and in local keystores.

The traditional and PQ signature are generated on the same data, and the resulting signatures are concatenated. The OpenSSH signature code is called sequentially: the traditional handling is performed first (including hashing the signed data with the appropriate SHA-2 functions (SHA-256 for NIST level 1, SHA-384 for NIST levels 2 or 3)), followed by the PQ one (in which case the data is signed/verified directly).

4.2.3 Lessons learned

As with key exchange in SSHv2, there were no unusual circumstances, and the implementation using concatenation was relatively straightforward, especially due to the lack of X.509 certificates. See table 2 for a complete list of algorithms tested.

One general observation on SSH that applies both in key exchange and in authentication is that SSH may be less sensitive to the larger communication sizes and slower cryptographic computations of some PQ schemes due the 1-on-1 usage scenario of SSH with infrequently established connections, compared to a TLS-enabled web server handling many concurrent connections from various clients.

5 Future work

The case studies we explored provide a preliminary investigation into approaches for implementing post-quantum and hybrid key exchange and authentication in TLS 1.2, TLS 1.3, and SSH, but they are certainly not exhaustive.

Standards bodies employing hybrid cryptography will have to make choices for the various design considerations discussed in this document, and may make different choices depending on their scenarios.

The implementations revealed some challenges in TLS and SSH with respect to limits on message sizes for key exchange and signatures that may affect some round 2 submissions. While preliminary tests seem to indicate it may be possible to modify some fields in TLS accommodate larger values, this may affect compatibility.

The OQS team intends to extend the OpenSSL and OpenSSH implementations described in this report to include all round 2 KEMs and signature schemes. The first step is to get all round 2 KEMs and signature schemes into liboqs, which we are working towards with the help of the PQClean project [26]. Once into liboqs, the algorithms will be enabled in the OpenSSL and OpenSSH forks. The goals of adding all round 2 candidate schemes is to provide results on the following:

- Message size feasibility: Which schemes have public keys / ciphertexts / signatures too large to work with the TLS specification and/or OpenSSL? Does artificially increasing length fields alleviate the problem?
- Network performance in lab conditions: Following the methodology of [8, 9, 21], how does latency and throughput behave on isolated networks in the lab?
- Network performance in more realistic conditions: Attempt to develop a simulation reflects network conditions described by [30] to assess latency and throughput in more realistic network conditions.

There are many other network protocols and applications also of interest for the post-quantum transition.

Acknowledgments

This ideas in this document are based on discussions with many people, including Matthew Campagna, Shay Gueron, and Torben Hansen (Amazon Web Services); Christopher Wood; Michele Mosca and John Schanck (University of Waterloo); and others. Goutam Tamvada assisted with some of the data collection.

Contributors to the implementations described in this document are listed on the relevant GitHub sites [35, 36, 37, 38], and include: Nicholas Allen, Maxime Anvari, Mira Belenkiy, Ben Davies, Nir Drucker, Javad Doliskani, Vlad Gheorghiu, Shay Gueron, Torben Hansen, Andrew Hopkins, Kevin Kane, Karl Knopf, Tancrède Lepoint, Shravan Mishra, Christian Paquin, Alex Parent, Peter Schwabe, Douglas Stebila, John Underhill, and Sebastian Verschoor.

The Open Quantum Safe project has received funding from Amazon Web Services and the Tutte Institute for Mathematics and Computing, and in-kind contributions of developer time from Amazon Web Services, Cisco Systems, evolutionQ, and Microsoft Research. D.S. is supported in part by Natural Sciences and Engineering Research Council (NSERC) of Canada Discovery grant RGPIN-2016-05146 and a NSERC Discovery Accelerator Supplement.

References

[1] Martin Albrecht et al. *NTS-KEM*. 2019. URL: https://nts-kem.io/.

[2] Apache Software Foundation. *Apache HTTP Server Project (httpd)*. URL: https://httpd.apache.org.

[3] Nicolas Aragon et al. *BIKE: Bit Flipping Key Encapsulation*. Mar. 2019. URL: https://bikesuite.org/.

[4] Daniel J. Bernstein et al. *Classic McEliece: conservative code-based cryptography*. 2019. URL: https://classic.mceliece.org/.

[5] Nina Bindel et al. *Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange*. Cryptology ePrint Archive, Report 2018/903. https://eprint.iacr.org/2018/903. 2018.

[6] Nina Bindel et al. "Hybrid key encapsulation mechanisms and authenticated key exchange". In: *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2017*. Ed. by Jintai Ding and Rainer Steinwandt. LNCS. Springer, May 2019.

[7] Nina Bindel et al. "Transitioning to a Quantum-Resistant Public Key Infrastructure". In: *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017*. Ed. by Tanja Lange and Tsuyoshi Takagi. Springer, Heidelberg, 2017, pp. 384–405. DOI: 10.1007/978-3-319-59879-6_22.

[8] Joppe W. Bos et al. "Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE". In: *ACM CCS 2016*. Ed. by Edgar R. Weippl et al. ACM Press, Oct. 2016, pp. 1006–1018. DOI: 10.1145/2976749.2978425.

[9] Joppe W. Bos et al. "Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem". In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2015, pp. 553–570. DOI: 10.1109/SP.2015.40.

[10] Matt Braithwaite. *Experimenting with Post-Quantum Cryptography*. July 2016. URL: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.

[11] Matthew Campagna, editor. *Quantum safe cryptography and security: An introduction, benefits, enablers and challengers*. Tech. rep. 8. June 2015. URL: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

[12] Matt Campagna and Eric Crockett. *Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)*. Internet-Draft draft-campagna-tls-bike-sike-hybrid-01. IETF Secretariat, May 2019. URL: http://www.ietf.org/internet-drafts/draft-campagna-tls-bike-sike-hybrid-01.txt.

[13] Pete Chown. *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*. RFC 3268. July 2002. DOI: 10.17487/RFC3268. URL: https://rfc-editor.org/rfc/rfc3268.txt.

[14] Yevgeniy Dodis and Jonathan Katz. "Chosen-Ciphertext Security of Multiple Encryption". In: *TCC 2005*. Ed. by Joe Kilian. Vol. 3378. LNCS. Springer, Heidelberg, Feb. 2005, pp. 188–209. DOI: 10.1007/978-3-540-30576-7_11.

[15] Nir Drucker and Shay Gueron. "A toolbox for software optimization of QC-MDPC code-based cryptosystems". In: *Journal of Cryptographic Engineering* (Jan. 2019). ISSN: 2190-8516. DOI: 10.1007/s13389-018-00200-4. URL: https://doi.org/10.1007/s13389-018-00200-4.

[16] Karen Easterbrook et al. *Post-quantum Cryptography VPN*. May 2018. URL: https://www.microsoft.com/en-us/research/project/post-quantum-crypto-vpn/.

[17] Guillaume Endignoux. *Round 2 Official Comment: BIKE*. Mar. 2019. URL: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/official-comments/BIKE-round2-official-comment.pdf.

[18] Shimon Even and Oded Goldreich. "On the Power of Cascade Ciphers". In: *CRYPTO'83*. Ed. by David Chaum. Plenum Press, New York, USA, 1983, pp. 43–50.

[19] Scott Fluhrer et al. *Postquantum Preshared Keys for IKEv2*. Internet-Draft draft-ietf-ipsecme-qr-ikev2-08. Work in Progress. Internet Engineering Task Force, Mar. 2019. 18 pp. URL: https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-qr-ikev2-08.

[20] Federico Giacon, Felix Heuer, and Bertram Poettering. "KEM Combiners". In: *PKC 2018, Part I*. Ed. by Michel Abdalla and Ricardo Dahab. Vol. 10769. LNCS. Springer, Heidelberg, Mar. 2018, pp. 190–218. DOI: 10.1007/978-3-319-76578-5_7.

[21] Vipul Gupta et al. "Speeding up Secure Web Transactions Using Elliptic Curve Cryptography". In: *NDSS 2004*. The Internet Society, Feb. 2004.

[22] Torben Hansen, Matthew Campagna, and Eric Crockett. *PRE-DRAFT: Hybrid Key Exchange Integration in the Secure Shell Transport Layer*. June 2018. URL: https://github.com/open-quantum-safe/openssh-portable/blob/OQS-master/ietf_pre_draft_sike_bike_hybrid_kex.txt.

[23] Danny Harnik et al. "On Robust Combiners for Oblivious Transfer and Other Primitives". In: *EUROCRYPT 2005*. Ed. by Ronald Cramer. Vol. 3494. LNCS. Springer, Heidelberg, May 2005, pp. 96–113. DOI: 10.1007/11426639_6.

[24] Paul E. Hoffman. *The Transition from Classical to Post-Quantum Cryptography*. Internet-Draft draft-hoffman-c2pq-05. Work in Progress. Internet Engineering Task Force, May 2019. 17 pp. URL: https://datatracker.ietf.org/doc/html/draft-hoffman-c2pq-05.

[25] Panos Kampanakis et al. *The Viability of Post-quantum X.509 Certificates*. Cryptology ePrint Archive, Report 2018/063. https://eprint.iacr.org/2018/063. 2018.

[26] Matthias J. Kannwischer et al. *The PQClean project*. May 2019. URL: https://github.com/PQClean/PQClean.

[27] Franziskus Kiefer and Krzysztof Kwiatkowski. *Hybrid ECDHE-SIDH Key Exchange for TLS*. Internet-Draft draft-kiefer-tls-ecdhe-sidh-00. Work in Progress. Internet Engineering Task Force, Nov. 2018. 13 pp. URL: https://datatracker.ietf.org/doc/html/draft-kiefer-tls-ecdhe-sidh-00.

[28] Adam Langley. *CECPQ2*. Dec. 2018. URL: https://www.imperialviolet.org/2018/12/12/cecpq2.html.

[29] Adam Langley. *Forward secrecy for Google HTTPS*. Dec. 2011. URL: https://www.imperialviolet.org/2011/11/22/forwardsecret.html.

[30] Adam Langley. *Post-quantum confidentiality for TLS*. Apr. 2018. URL: https://www.imperialviolet.org/2018/04/11/pqconftls.html.

[31] Bodo Moeller et al. *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*. RFC 4492. May 2006. DOI: 10.17487/RFC4492. URL: https://rfc-editor.org/rfc/rfc4492.txt.

[32] National Institute of Standards and Technology. *Specification for the Advanced Encryption Standard (AES)*. Federal Information Professing Standards (FIPS) 197. Nov. 2001. URL: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf.

[33] National Institute of Standards and Technology. *Specification for the Digital Signature Standard (DSS)*. Federal Information Professing Standards (FIPS) 186-2. Jan. 2000. URL: https://csrc.nist.gov/CSRC/media/Publications/fips/186/2/archive/2001-10-05/documents/fips186-2-change1.pdf.

[34] National Institute of Standards and Technology. *Specification for the Secure Hash Standard*. Federal Information Professing Standards (FIPS) 180-2. Aug. 2002. URL: https://csrc.nist.gov/CSRC/media/Publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf.

[35] Open Quantum Safe Project. *liboqs*. Nov. 2018. URL: https://github.com/open-quantum-safe/liboqs.

[36] Open Quantum Safe Project. *OQS-OpenSSH*. Nov. 2018. URL: https://github.com/open-quantum-safe/openssh-portable.

[37] Open Quantum Safe Project. *OQS-OpenSSL_1_0_2-stable*. Nov. 2018. URL: https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_0_2-stable.

[38] Open Quantum Safe Project. *OQS-OpenSSL_1_1_1-stable*. Nov. 2018. URL: https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_1_1-stable.

[39] OpenVPN. *OpenVPN*. URL: https://openvpn.net.

[40] Eric Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. Aug. 2018. DOI: 10.17487/RFC8446. URL: https://rfc-editor.org/rfc/rfc8446.txt.

[41] John M. Schanck and Douglas Stebila. *A Transport Layer Security (TLS) Extension For Establishing An Additional Shared Secret*. Internet-Draft draft-schanck-tls-additional-keyshare-00. Work in Progress. Internet Engineering Task Force, Apr. 2017. 10 pp. URL: https://datatracker.ietf.org/doc/html/draft-schanck-tls-additional-keyshare-00.

[42] John M. Schanck, William Whyte, and Zhenfei Zhang. *Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.2*. Internet-Draft draft-whyte-qsh-tls12-02. Work in Progress. Internet Engineering Task Force, July 2016. 19 pp. URL: https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls12-02.

[43] Amazon Web Services. *s2n*. https://github.com/awslabs/s2n. 2014.

[44] Douglas Steblia and Shay Gueron. *Design issues for hybrid key exchange in TLS 1.3*. Internet-Draft draft-stebila-tls-hybrid-design-00. Work in Progress. Internet Engineering Task Force, Mar. 2019. 22 pp. URL: https://datatracker.ietf.org/doc/html/draft-stebila-tls-hybrid-design-00.

[45] Marc Stevens et al. "The First Collision for Full SHA-1". In: *CRYPTO 2017, Part I*. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10401. LNCS. Springer, Heidelberg, Aug. 2017, pp. 570–596. DOI: 10.1007/978-3-319-63688-7_19.

[46] Marc Stevens et al. *The first collision for full SHA-1*. Cryptology ePrint Archive, Report 2017/190. http://eprint.iacr.org/2017/190. 2017.

[47] Nick Sullivan. *Haskell numeric prelude*. Twitter. Sept. 2018. URL: https://twitter.com/grittygrease/status/1039656938768756736.

[48] The OpenSSL project. *Changelog*. May 2019. URL: https://www.openssl.org/news/changelog.html.

[49] C. Tjhai et al. *Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2)*. Internet-Draft draft-tjhai-ipsecme-hybrid-qske-ikev2-03. Work in Progress. Internet Engineering Task Force, Jan. 2019. 19 pp. URL: https://datatracker.ietf.org/doc/html/draft-tjhai-ipsecme-hybrid-qske-ikev2-03.

[50] Twibright Labs. *Links 2.17*. Sept. 2018. URL: http://links.twibright.com.

[51] Xiaoyun Wang, Andrew Yao, and Frances Yao. *New Collision Search for SHA-1*. Crypto 2005 Rump Session. Aug. 2005. URL: https://www.iacr.org/conferences/crypto2005/r/2.pdf.

[52] William Whyte et al. *Quantum-Safe Hybrid (QSH) Key Exchange for Transport Layer Security (TLS) version 1.3*. Internet-Draft draft-whyte-qsh-tls13-06. Work in Progress. Internet Engineering Task Force, Oct. 2017. 19 pp. URL: https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls13-06.

[53] Wikipedia contributors. *SHA-1 — Wikipedia, The Free Encyclopedia*. [Online; accessed 29-May-2019]. 2019. URL: https://en.wikipedia.org/w/index.php?title=SHA-1&oldid=899014033.

[54] T. Ylonen and C. Lonvick. *The Secure Shell (SSH) Transport Layer Protocol*. RFC 4253. Jan. 2006. URL: https://tools.ietf.org/html/rfc4253.

[55] Rui Zhang et al. "On the Security of Multiple Encryption or CCA-security+CCA-security=CCA-security?" In: *PKC 2004*. Ed. by Feng Bao, Robert Deng, and Jianying Zhou. Vol. 2947. LNCS. Springer, Heidelberg, Mar. 2004, pp. 360–374. DOI: 10.1007/978-3-540-24632-9_26.