X25519Kyber768Draft00 hybrid post-quantum key agreement

Abstract

This memo defines X25519Kyber768Draft00, a hybrid post-quantum key exchange for TLS 1.3.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://bwesterb.github.io/draft-westerbaan-tls-xyber768d00/draft-tls-westerbaan-xyber768d00.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-tls-westerbaan-xyber768d00/.

Source for this draft and an issue tracker can be found at https://github.com/bwesterb/draft-westerbaan-tls-xyber768d00.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 27 March 2024.
1. Introduction

1.1. Motivation

The final draft for Kyber is expected in 2024. There are already early deployments of post-quantum key agreement, with more to come before Kyber is standardised. To promote interoperability of early implementations, this document specifies a preliminary hybrid post-quantum key agreement.

1.2. Warning: relation with X25519Kyber768Draft00 for HPKE

In [hpkexyber] a hybrid KEM with the same name is defined for use in HPKE. It differs from the hybrid KEM implicit in this document: here we use the X25519 shared secret directly, whereas in [hpkexyber], the ephemeral X25519 public key (ciphertext) is mixed in. For use in HPKE this is required to be IND-CCA2 robust. This is not required
for use in TLS 1.3, thanks to the inclusion of the keyshare in the message transcript.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 \[RFC2119\] \[RFC8174\] when, and only when, they appear in all capitals, as shown here.

3. Construction

We instantiate draft-ietf-tls-hybrid-design-06 with X25519 \[rfc7748\] and Kyber768Draft00 \[kyber\]. The latter is Kyber as submitted to round 3 of the NIST PQC process \[KyberV302\].

For the client's share, the key_exchange value contains the concatenation of the client's X25519 ephemeral share (32 bytes) and the client's Kyber768Draft00 public key (1184 bytes). The resulting key_exchange value is 1216 bytes in length.

For the server's share, the key_exchange value contains the concatenation of the server's X25519 ephemeral share (32 bytes) and the Kyber768Draft00 ciphertext (1088 bytes) returned from encapsulation for the client's public key. The resulting key_exchange value is 1120 bytes in length.

The shared secret is calculated as the concatenation of the X25519 shared secret (32 bytes) and the Kyber768Draft00 shared secret (32 bytes). The resulting shared secret value is 64 bytes in length.

4. Security Considerations

For TLS 1.3, this concatenation approach provides a secure key exchange if either component key exchange methods (X25519 or Kyber768Draft00) are secure \[hybrid\].

5. IANA Considerations

This document requests/registers a new entry to the TLS Named Group (or Supported Group) registry, according to the procedures in Section 6 of \[tlsiana\].

Value: 0x6399 (please)

Description: X25519 Kyber768Draft00

DTLS-OK: Y
6. References

6.1. Normative References


6.2. Informative References


Appendix A. Change log

RFC Editor's Note: Please remove this section prior to publication of a final version of this document.

A.1. Since draft-tls-westerbaan-xyber768d00-02

*Explain relation with HPKE hybrid

A.2. Since draft-tls-westerbaan-xyber768d00-01

*Change reference for X25519

A.3. Since draft-tls-westerbaan-xyber768d00-00

*Set working group to None.

*Bump to cfrg-schwabe-kyber-02

Authors' Addresses

Bas Westerbaan
Cloudflare

Email: bas@cloudflare.com

Douglas Stebila
University of Waterloo

Email: dstebila@uwaterloo.ca