Workgroup: None
Internet-Draft:
draft-kwiatkowski-tls-ecdhe-kyber-01
Published: 18 May 2023
Intended Status: Informational
Expires: 19 November 2023
Authors: K. Kwiatkowski P. Kampanakis
PQShield, LTD AWS

Post-quantum hybrid ECDHE-Kyber Key Agreement for TLSv1.3

Abstract

This draft defines a hybrid key agreement for TLS 1.3 that combines a post-quantum KEM with elliptic curve Diffie-Hellman (ECDHE).

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://post-quantum-cryptography.github.io/draft-kwiatkowski-tls-ecdhe-kyber/. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-kwiatkowski-tls-ecdhe-kyber/.

Source for this draft and an issue tracker can be found at https://github.com/https://github.com/post-quantum-cryptography/draft-kwiatkowski-tls-ecdhe-kyber.

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 19 November 2023.

Copyright Notice

Table of Contents

1. Introduction

1.1. Motivation

Kyber is a key encapsulation method (KEM) designed to be resistant to cryptanalytic attacks with quantum computers. Standardization of Kyber KEM is expected to be finalized in 2024.

Experimentation and early deployments are crucial part of the migration to post-quantum cryptography. To promote interoperability of those deployments this document provides specification of preliminary hybrid post-quantum key agreement to be used in TLS 1.3 protocol.

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. Negotiated Groups

This document defines an additional supported group which can be used for hybrid post-quantum key agreements. The hybrid key

agreement for TLS 1.3 is detailed in the [hybrid] draft. We compose the hybrid scheme with the Kyber KEM as defined in [kyber] draft, and the ECDHE scheme parametrized with elliptic curves defined in ANSI X9.62 [ECDSA] and NIST SP 800-186 [DSS].

The new group allows deriving TLS session keys by using FIPS-approved schemes. NIST's special publication 800-56Cr2 [SP56C] approves the usage of HKDF [HKDF] with two distinct shared secrets as long as the first one is computed by a FIPS-approved key-establishment scheme. Both ECDHE and a curve secp256r1 (NIST P-256) are FIPS-approved by NIST SP 800-56Ar3 [SP56A] and NIST SP 800-186 [DSS] correspondingly.

3.1. Construction

The name of the new supported hybrid post-quantum group is SecP256r1Kyber768Draft00.

When this group is negotiated, the client's share is a fixed-size concatenation of the ECDHE share and Kyber's public key. The ECDHE share is the serialized value of the uncompressed ECDH point representation as defined in Section 4.2.8.2 of [RFC8446]. The Kyber's ephemeral share is the public key of the KeyGen step (see [kyber]) represented as an octet string. The size of client share is 1248 bytes.

The server's share is a fixed-size concatenation of ECDHE share and Kyber's ciphertext returned from encapsulation (see [kyber]). The server ECDHE share is the serialized value of the uncompressed ECDH point representation UncompressedPointRepresentation as defined in Section 4.2.8.2 of [RFC8446]. The server share is the Kyber's ciphertext returned from the Encapsulate step (see [kyber]) represented as an octet string. The size of server's share is 1152 bytes.

Finally, the shared secret is a concatenation of the ECDHE and the Kyber shared secrets. The ECDHE shared secret is the x-coordinate of the ECDH shared secret elliptic curve point represented as an octet string as defined in Section 7.4.2 of [RFC8446]. The Kyber shared secret is the value returned from either encapsulation (on the server side) or decapsulation (on the client side) represented as an octet string. The size of a shared secret is 64 bytes.

4. Security Considerations

The same security considerations as those described in [hybrid] apply to the approach used by this document. Implementers are encouraged to use implementations resistant to side-channel attacks, especially those that can be applied by remote attackers.

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]. These identifiers are to be used with the point-in-time specified versions of Kyber in the third round of NIST's Post-quantum Project which is specified in [kyber]. The identifiers used with the final, ratified by NIST, version of Kyber will be specified later with in a different draft. [EDNOTE: The identifiers for the final, ratified version of Kyber should preferrably by different that the commonly used OQS codepoints]

Value: 0x639A

Description: SecP256r1Kyber768Draft00

DTLS-OK: Y

Recommended: N

Reference: This document

Comment: Combining secp256r1 ECDH with pre-standards version of Kyber768

6. References

6.1. Normative References

[kyber] Schwabe, P. and B. Westerbaan, "Kyber Post-Quantum KEM", Work in Progress, Internet-Draft, draft-cfrg-schwabe-kyber-02, 31 March 2023, <https://datatracker.ietf.org/doc/html/draft-cfrg-schwabe-kyber-02>.

[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/rfc/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/rfc/rfc8174>.

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

6.2. Informative References

[DSS]

Moody, D., "Recommendations for Discrete Logarithm-based Cryptography:: Elliptic Curve Domain Parameters", National Institute of Standards and Technology report, DOI 10.6028/nist.sp.800-186, 2022, <https://doi.org/10.6028/nist.sp.800-186>.

[ECDSA] American National Standards Institute, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI ANS X9.62-2005, November 2005.

[HKDF] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC Editor report, DOI 10.17487/rfc5869, May 2010, <https://doi.org/10.17487/rfc5869>.

[hybrid] Stebila, D., Fluhrer, S., and S. Gueron, "Hybrid key exchange in TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-hybrid-design-06, 27 February 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design-06>.

[SP56A] Barker, E., Chen, L., Roginsky, A., Vassilev, A., and R. Davis, "Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography", National Institute of Standards and Technology report, DOI 10.6028/nist.sp.800-56ar3, April 2018, <https://doi.org/10.6028/nist.sp.800-56ar3>.

[SP56C] Barker, E., Chen, L., and R. Davis, "Recommendation for Key-Derivation Methods in Key-Establishment Schemes", National Institute of Standards and Technology report, DOI 10.6028/nist.sp.800-56cr2, August 2020, <https://doi.org/10.6028/nist.sp.800-56cr2>.

[tlsiana] Salowey, J. A. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8447bis-04, 27 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8447bis-04>.

Authors' Addresses

Kris Kwiatkowski
PQShield, LTD

Email: kris@amongbytes.com

Panos Kampanakis
AWS

Email: kpanos@amazon.com