Workgroup: Internet Engineering Task Force
Published: 11 May 2023
Intended Status: Informational
Expires: 12 November 2023
Authors: S. Josefsson

Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761+x25519+sha512

Abstract

We document a widely deployed hybrid key exchange method based on Streamlined NTRU Prime sntrup761 and X25519 with SHA-512.

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 12 November 2023.

Table of Contents

1. Introduction

Streamlined NTRU Prime [NTRUPrime] [NTRUPrimePQCS] provides post-quantum small lattice-based key-encapsulation mechanisms. The variant sntrup761 instance has been implemented widely.

The pre-quantum elliptic-curve Diffie-Hellman X25519 function [RFC7748] has been widely implemented.

To hedge against attacks on either of sntrup761 or X25519 a hybrid construction may be used, with the intention that the hybrid would be secure if either of the involved algorithms are flawed.

This document describes how to implement key exchange based on a hybrid between Streamlined NTRU Prime sntrup761 and X25519 with SHA-512 [RFC6234].

This hybrid construction was introduced for the Secure Shell protocol as sntrup761x25519-sha512, and we offer this document for other protocols that desire to use an established hybrid key exchange method.

2. Key Exchange Method: sntrup761+x25519+sha512

The key-agreement is done by the X25519 Diffie-Hellman protocol as described in section 6.1 (Curve25519) of [RFC7748], and the key encapsulation method described in [NTRUPrimePQCS].

Alice sends a concatenation of the 1158 byte public key output from the key generator of sntrup761 with the 32 byte K_A = X25519(a, 9) as described in [NTRUPrimePQCS] and [RFC7748]. The output value is thus 1190 bytes.

Bob sends a concatenation of the 1039 byte ciphertext output from the key encapsulation mechanism of sntrup761 with the 32 byte K_B = X25519(b, 9) as described in [NTRUPrimePQCS] and [RFC7748]. The output value is thus 1071 bytes.

Alice derive the 32 byte shared K1 based on the X25519 values as described in [RFC7748] and performs the sntrup761 key decapsulation operation as described in [NTRUPrimePQCS] to yield the 32 byte shared secret K2. Alice derives the final hybrid shared secret key K using

SHA-512 [RFC6234] as SHA512(K1||K2) where || denote concatenation. The output is 64 bytes.

Bob derive the 32 byte shared K1 based on the X25519 values as described in [RFC7748] and takes the 32 byte shared secret key K2 from the earlier key encapsulation method of sntrup761. Bob derives the final hybrid shared secret secret key K using SHA-512 [RFC6234] as SHA512(K1||K2) where || denote concatenation. The output is 64 bytes.

Alice and Bob has now established a shared key.

3. Acknowledgements

This work is a simple generalization of the sntrup761x25519-sha512 mechanism due to [OpenSSH] and TinySSH [TinySSH] documented in draft-josefsson-ntruprime-ssh-00.

4. Security Considerations

The security considerations of [RFC7748], [NTRUPrimePQCS] and [RFC6234] are inherited.

While the construct should remain secure if either X25519 or sntrup761 is found to be insecure, the security of the combined hybrid construction depends on the security of the SHA-512 algorithm.

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. Normative References

[NTRUPrimePQCS] Bernstein, D.J., Brumley, B. B., Chen,, M., Chuengsatiansup, C., Lange, T., Marotzke, A., Peng, B., Tuveri, N., Vredendaal, C. V., and B. Yang, "NTRU Prime: round 3", WWW https://ntruprime.cr.yp.to/nist/ntruprime-20201007.pdf, October 2020.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

6.2. Informative References

[NTRUPrime] Bernstein, D.J., Chuengsatiansup, C., Lange, T., and C. van Vredendaal, "NTRU Prime: reducing attack surface at low cost", WWW https://ntruprime.cr.yp.to/ntruprime-20170816.pdf, August 2017.

[OpenSSH] OpenSSH group of OpenBSD, "The OpenSSH Project", <https://www.openssh.com/>.

[TinySSH] TinySSH, "TinySSH - minimalistic SSH server which implements only a subset of SSHv2 features", <https://www.tinyssh.org/>.

Author's Address

Simon Josefsson

Email: simon@josefsson.org
URI: https://blog.josefsson.org/