

Workgroup: Internet Engineering Task Force

Published: 9 May 2023

Intended Status: Informational

Expires: 10 November 2023

Authors: S. Josefsson

**Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU
Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512**

Abstract

We document a widely deployed hybrid key exchange methods in the Secure Shell (SSH) protocol that is 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 10 November 2023.

Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

- [1. Introduction](#)

- [2. Requirements Language](#)
- [3. Key Exchange Method: snttrup761x25519-sha512](#)
- [4. Acknowledgements](#)
- [5. Security Considerations](#)
- [6. IANA Considerations](#)
- [7. References](#)
 - [7.1. Normative References](#)
 - [7.2. Informative References](#)
- [Appendix A. Test vectors](#)
- [Author's Address](#)

1. Introduction

Secure Shell (SSH) [[RFC4251](#)] is a secure remote login protocol. The key exchange protocol described in [[RFC4253](#)] supports an extensible set of methods. [[RFC5656](#)] defines how elliptic curves are integrated into this extensible SSH framework, and [[RFC8731](#)] adds curve25519-sha256 to support the pre-quantum elliptic-curve Diffie-Hellman X25519 function [[RFC7748](#)].

Streamlined NTRU Prime [[NTRUPrime](#)] [[NTRUPrimePQCS](#)] provides post-quantum small lattice-based key-encapsulation mechanisms. The variant snttrup761 instance has been implemented widely.

To hedge against attacks on either of snttrup761 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 snttrup761 and X25519 with SHA-512 [[RFC6234](#)] in SSH.

The algorithm is equivalent to the privately defined algorithm "snttrup761x25519-sha512@openssh.com", which is implemented and widely deployed in OpenSSH [[OpenSSH](#)] and TinySSH [[TinySSH](#)].

2. Requirements Language

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. Key Exchange Method: snttrup761x25519-sha512

The key-agreement is done by the X25519 Diffie-Hellman protocol as described in section 3 ([Key Exchange Methods](#)) of [[RFC8731](#)], and the key encapsulation method described in [[NTRUPrimePQCS](#)].

The key exchange procedure re-use the Elliptic Curve Diffie-Hellman (ECDH) key exchange defined in section 4 ([ECDH Key Exchange](#)) and section 7.1 ([ECDH Message Numbers](#)) of [[RFC5656](#)], and the protocol flow and the SSH_MSG_KEX_ECDH_INIT and SSH_MSG_KEX_ECDH_REPLY messages are identical, except that we use different ephemeral public values Q_C and Q_S and shared secret K as described below.

The SSH_MSG_KEX_ECDH_INIT's value Q_C that holds the client's ephemeral public key MUST be constructed by concatenating 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 [[RFC8731](#)]. The Q_C value is thus 1190 bytes.

The SSH_MSG_KEX_ECDH_REPLY's value Q_S that holds the server's ephemeral public key MUST be constructed by concatenating 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 [[RFC8731](#)]. The Q_S value is thus 1071 bytes.

Clients and servers **MUST** abort if the length of the received public keys Q_C or Q_S are not the expected lengths. An abort for these purposes is defined as a disconnect (SSH_MSG_DISCONNECT) of the session and **SHOULD** use the SSH_DISCONNECT_KEY_EXCHANGE_FAILED reason for the message [[IANA-REASON](#)]. No further validation is required beyond what is described in [[RFC7748](#)], [[RFC8731](#)] and [[NTRUPrimePQCS](#)].

The SSH_MSG_KEX_ECDH_REPLY's signature value is computed as described in [[RFC5656](#)] with a shared secret K that MUST be the SHA-512 hash computed on the concatenation of the 32-byte key output from the key encapsulation mechanism of `sntrup761` together with the 32 byte $X25519(a, X25519(b, 9)) = X25519(b, X25519(a, 9))$ output. Note that unlike `Curve25519-sha256` [[RFC8731](#)], the `X25519` output is used raw instead of bignum-encoded, and the SHA-512 output value is string-encoded.

4. Acknowledgements

The `sntrup761x25519-sha512` mechanism is identical to the `sntrup761x25519-sha512@openssh.com` mechanism designed by the OpenSSH project, inspired by the earlier `sntrup4591761x25519-sha512@tinyssh.org` mechanism designed by TinySSH.

This document was derived from [[RFC8731](#)].

5. Security Considerations

The security considerations of [[RFC4251](#)], [[RFC5656](#)], [[RFC7748](#)], and [[RFC8731](#)] are inherited.

Streamlined NTRU Prime sntrup761 is aiming for the standard goal of IND-CCA2 security, is widely implemented with good performance on a wide range of architectures, and has been studied by researchers for several years. However new cryptographic primitives should be introduced and trusted conservatively, and new research findings may be published at any time that may warrant implementation reconsiderations.

The increase in communication size and computational requirements may be a concern for restricted computational devices, which would then not be able to take advantage of the improved security properties offer by this work.

Since sntrup761x25519-sha512 is expected to offer no reduction of security compared to curve25519-sha256, we suggest that it is used and preferred whenever curve25519-sha256 is used today, when the extra communication size and computational requirements are acceptable.

6. IANA Considerations

IANA is requested to add "sntrup761x25519-sha512" to the "Key Exchange Method Names" registry for SSH [[IANA-KEX](#)] that was created in [Section 4.10](#) of [[RFC4250](#)].

7. References

7.1. 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.yt.nist/ntruprime-20201007.pdf>, October 2020.

[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>>.

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, DOI 10.17487/RFC4250, January 2006, <<https://www.rfc-editor.org/info/rfc4250>>.

[RFC4251] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, DOI 10.17487/RFC4251, January 2006, <<https://www.rfc-editor.org/info/rfc4251>>.

- [RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, January 2006, <<https://www.rfc-editor.org/info/rfc4253>>.
- [RFC5656] Stebila, D. and J. Green, "Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer", RFC 5656, DOI 10.17487/RFC5656, December 2009, <<https://www.rfc-editor.org/info/rfc5656>>.
- [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>>.
- [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>>.
- [RFC8731] Adamantiadis, A., Josefsson, S., and M. Baushke, "Secure Shell (SSH) Key Exchange Method Using Curve25519 and Curve448", RFC 8731, DOI 10.17487/RFC8731, February 2020, <<https://www.rfc-editor.org/info/rfc8731>>.

7.2. Informative References

- [IANA-KEX] IANA, "Secure Shell (SSH) Protocol Parameters: Key Exchange Method Names", <<https://www.iana.org/assignments/ssh-parameters/>>.
- [IANA-REASON] IANA, "Secure Shell (SSH) Protocol Parameters: Disconnection Messages Reason Codes and Descriptions", <<https://www.iana.org/assignments/ssh-parameters/>>.
- [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/>>.

Appendix A. Test vectors

SSH2_MSG_KEX_ECDH_INIT

client public key sntrup761:

0000: 5d b3 a9 d3 93 30 31 76 0e 8a f5 87 f7 b2 8c 4f]....01v.....0
0016: 97 a1 74 0e 6b 6f cf 1a d9 d9 99 8a 32 a5 61 e5 ..t.ko.....2.a.
0032: 9e 4d 93 67 e2 66 18 f0 0a f5 54 f4 48 65 0c 60 .M.g.f....T.He.`
0048: d1 12 92 c2 aa a9 e4 7c ea 32 a3 f5 86 cb c4 c3|.2.....
0064: d5 c2 6f 34 5e 7f d3 57 51 d3 e3 d9 cc 1c e4 49 ..o4^..WQ.....I
0080: bb ea 3e 2e 58 5e ac ba 0a b8 22 00 7c 77 a4 e0 ..>.X^....".|w..
0096: bd 16 5c 3a f7 b3 25 08 c1 81 fd 0d 9f 99 a3 be ..\:%.....
0112: ae e3 38 84 13 ff f0 b4 0f cb ab 76 1e 95 3e 1e ..8.....v..>.
0128: 7c 74 1e 58 46 f6 81 f0 f2 f2 56 5b f3 be ce c9 |t.XF.....V[....
0144: c8 99 9f 03 88 81 db 17 75 1d fb f5 b1 e2 f3 5du.....]
0160: 32 ce 19 75 49 e7 e1 17 bf 35 0d 97 7c ac 0a cf 2..uI....5..|...
0176: 6c 8a 0f fc 07 4b a7 8b c5 93 f7 47 7c b6 d5 bf l....K....G|...
0192: 02 f0 96 80 e8 dc f3 87 c9 f0 b2 91 e7 37 70 827p.
0208: 3e 47 b7 18 72 be 5a da b1 85 d3 6e 56 5d 8a a3 >G..r.Z....nV]..
0224: 62 fa 3e d0 ea 6e b9 fa 69 ec 96 86 94 81 2e 88 b.>..n..i.....
0240: 2b ba e5 af 70 1e ae ba 5f cb ea 82 e5 ba 67 0e +...p..._.....g.
0256: 4d f6 2a ec 13 a9 19 b4 08 9c b7 32 bb 40 de c3 M.*.....2.@..
0272: e9 33 e1 c4 0d 5b 72 00 06 c4 3b 7f 57 d4 85 76 .3...[r...;W..v
0288: 4c 4c 3d ab 8e 1b 00 00 ac d9 8c 05 b3 18 24 85 LL=.....\$.
0304: 77 28 74 71 0d 68 8b 02 2c 59 55 a7 4d a4 6e 37 w(tq.h.,YU.M.n7
0320: 85 6c 77 68 f5 b7 a7 52 61 af 37 b4 09 07 34 68 .lwh...Ra.7...4h
0336: b6 83 ca f2 03 25 47 f9 09 e6 da bd 82 07 7e d1%G.....~.
0352: 78 16 74 1a a5 4c 5b ac 78 d8 0f 1a 44 08 44 a7 x.t..L[.x...D.D.
0368: ef 85 00 43 19 c3 3e b4 54 e6 3f f1 ac 83 03 ce ...C...>.T.?.....
0384: 7c bd ef 3c fd eb 47 6f f7 f9 e0 1f 13 9f cb 77 |..<..Go.....w
0400: 52 40 9d 3a d7 8b ad bf cc f1 06 ec 93 32 48 be R@:.....2H.
0416: 0a 53 99 5c dd 9e 96 3b 84 21 8f b2 b4 fd b8 97 .S.\...;.!.....
0432: 8b 7a 8f 71 aa e6 af 4e 22 53 18 f0 a2 30 a0 53 .z.q...N"S...0.S
0448: 30 c9 d8 a9 d7 67 08 a5 ad 81 64 7b 3a 02 ae ff 0....g....d{:...
0464: e7 fa 41 68 d0 54 e3 42 86 da f7 f0 98 31 38 e5 ..Ah.T.B....18.
0480: 8c fa 86 5c 5c f9 82 f8 a2 09 91 91 96 72 12 e5 ...\\.....r..
0496: 8f 8b 8e 9b e8 5d bd 66 4b 6e ec a3 b3 03 c5 4e].fKn.....N
0512: 0f 7e a5 15 ef ab 01 8c 6d 02 52 77 bc 9a 02 f2 .~.....m.Rw....
0528: 2e bf 03 40 fe 5a 80 5a c0 78 1e 95 21 10 9d dd ...@.Z.Z.x...!...
0544: 37 87 00 ae 13 c5 9d 9c 81 87 37 3e 7d e0 40 bc 7.....7>}.@.
0560: 83 76 69 4f 9f c4 08 fd aa a1 7e aa 88 0e 4c 56 .vi0.....~...LV
0576: a0 47 c5 d6 94 fb 52 67 f3 36 de b2 7e bf d1 33 .G....Rg.6..~..3
0592: 41 fd 05 20 66 60 f4 91 96 5f 19 33 2d 17 ec e0 A.. f`...._3-...
0608: 3e 93 7a 66 3b b0 de f4 ad 51 90 a4 a1 94 f3 37 >.zf;....Q.....7
0624: 9a 77 11 02 67 45 6d 4d 19 80 33 58 56 2c b8 11 .w..gEmM..3XV,..
0640: 51 7b bc ec 43 fe 3d 96 ac f7 f0 8b 8d c6 2c 02 Q{..C.=.....,
0656: 2f c0 67 21 56 49 ee bf 07 17 48 f9 30 0b 18 2c /.g!VI....H.0...
0672: fa 7b 57 93 be f7 12 99 57 be 98 e7 55 84 da ed .{W.....W...U...
0688: 5c 94 71 fa 48 0f ed 97 ab e4 a5 d6 b6 26 3a e4 \.q.H.....&:..
0704: cb fe f9 ed 07 4b 42 bf e5 a1 d1 34 4d 7b 67 b9KB....4M{g.
0720: b7 06 7b d2 c7 ae 57 15 21 58 55 70 70 93 f1 87 ..{...W.!XUpp...

0736: 31 bf 85 74 fe 36 0d 08 c8 07 a2 14 fc d5 96 8b 1..t.6.....
0752: 59 62 97 30 43 75 c2 a9 4f ec f9 e9 33 a9 38 cb Yb.0Cu..0...3.8.
0768: ae ee 63 34 8c 65 54 e7 9d d4 23 a2 4f b9 00 ed ..c4.eT...#.0...
0784: b4 be 0b 1c df d4 97 c0 89 ab dd 5f 75 13 ce 37_u..7
0800: f3 d2 26 55 72 39 61 f0 d2 11 e8 e7 5f 93 5b 79 ..&Ur9a....._[y
0816: e5 6c 28 f3 0a f9 5e 99 b8 a0 e6 4a 22 88 e5 28 .l(...^....J"..(
0832: 82 0c 6f 72 1d dd 80 84 57 04 72 f4 26 56 71 f3 ..or....W.r.&Vq.
0848: 92 23 ff 9e a9 fd 05 0b 51 99 72 32 98 a5 02 87 .#.....Q.r2....
0864: fe bb 99 18 5a b3 ec ab f9 26 7b 97 79 da 5f 19Z....&{.y._.
0880: 4e e7 7d a5 2d 53 40 2a 1f 1b 62 df 3b 11 82 e6 N.}.-S@*.b.;...
0896: 90 7f 0f 56 0c 75 14 03 e7 6f aa f0 0e 0a 17 13 ...V.u...o.....
0912: 54 f5 ea d7 21 31 2c 7a c5 7f a3 ae 14 f3 05 42 T...!1,z.....B
0928: e9 c9 6c 6d d1 0a cb 19 35 7f 01 8a 8c e2 a1 09 ..lm....5.....
0944: b5 c6 e5 e8 2b 4f 1e a2 e9 ce 5b e4 76 f7 53 4f+0....[.v.S0
0960: 52 d4 75 22 4b aa 1e cd 42 0e be d7 dc 76 6f 94 R.u"K...B....vo.
0976: 0a 37 47 ca 44 bd e6 9e c1 2a 0d 57 f3 c2 47 40 .7G.D....*.W..G@
0992: 23 db a8 45 c7 9b 4a 96 13 6a 73 ad 6a a2 a8 e4 #..E..J..js.j...
1008: df 92 34 76 f9 47 8d b9 21 63 46 c2 d7 f2 64 e6 ..4v.G..!cF...d.
1024: 17 27 9f cf f3 ae cd 3a 7d ed 5e 46 7c 33 71 f6 .'.....:}.^F|3q.
1040: 71 c8 92 dc ae e6 a0 c8 05 0c e0 37 fb ea 15 ed q.....7....
1056: b0 78 a5 bf b1 48 8b 46 64 1e c8 81 00 55 82 89 .x...H.Fd....U..
1072: 25 f8 b1 8b 1c e4 96 54 f8 be 97 b1 d3 20 f3 a0 %.....T..... ..
1088: b5 c1 dd d5 27 d0 61 d9 96 2a 74 76 a8 33 10 78'.a..*tv.3.x
1104: ff b2 86 ee 4f 0b 78 73 dd 7f 7c b5 02 e9 12 350.xs..|....5
1120: d3 9e ab 81 cd 9b 61 fb 2b 33 72 ee c6 bb 8a bca.+3r.....
1136: bd 4f e5 9b c2 55 8f a0 b1 e7 1a 6a c1 e3 f1 5c .0...U.....j...\
1152: 83 8f f0 9c 5b 04[.

client public key c25519:

0000: be f9 23 79 d7 fd 4e 8a 10 55 9b dc e5 3e 62 13 ..#y..N..U...>b.
0016: eb 9b 6a 6f ca de ed 90 04 db b1 30 f6 ff ef 4f ..jo.....0...0

SSH2_MSG_KEX_ECDH_REPLY

server cipher text:

0000: 71 67 00 55 f8 ac 87 1a af 7c ef cf 1c b4 7d b9 qq.U.....|....}.
0016: 4f b6 22 5e 4d 77 81 73 4f 1d b9 82 79 ff e9 34 0."^Mw.s0...y..4
0032: 26 9f d2 2e 4e c6 a3 5f 79 9c 26 68 99 3a 0f 40 &...N..._y.&h...@
0048: 33 2a 7d dd fa 7a e7 6b 1e e7 9d 50 b7 48 0f aa 3*}..z.k...P.H..
0064: aa 97 ff e7 8c 6c ac 5d 10 df 2b e3 cc 93 ea dcl.]...+.....
0080: 18 17 b3 34 42 70 7a 27 85 58 2a ae c2 e6 b9 26 ...4Bpz'.X*....&
0096: 93 fd 23 a9 ae ac 4a 35 8b 57 c1 5c 95 cb 23 fb ..#...J5.W.\.##.
0112: e5 93 0f 7c f5 63 6b 5b a1 53 b5 55 d0 75 16 21 ...|.ck[.S.U.u.!
0128: 8a db 95 ff c8 58 ac f4 7e 46 69 0a 4c a9 c8 ccX..~Fi.L...
0144: eb e8 66 7c c4 fb fd 98 2c 0c 7f 41 8c 34 89 49 ..f|....,..A.4.I
0160: a0 25 59 eb 63 a1 e6 8f 37 bf bc b3 ce 0a da 53 .%Y.c...7.....S
0176: 54 7f c2 41 52 eb 6c 9e 6e d0 ea af 6a 82 5d 17 T..AR.l.n...j.].
0192: 6f 17 8d 06 8a 86 55 60 28 31 12 4a 0c de 6b be o.....U`(1.J..k.
0208: eb fd 38 13 6c 56 69 ad 0e 72 c8 bd b4 69 9d 32 ..8.lVi...r...i.2

0224: b4 1c 8e 6f f4 25 e1 9b c5 6f 8b 02 77 52 ae 72 ...o.%...o..wR.r
0240: eb 9b 03 c8 9f de 15 bd f6 5a e8 9d 83 81 7b 48Z....{H
0256: 7a 69 9a d0 91 41 aa 07 5a fa ad d6 e8 55 39 d9 zi...A.Z....U9.
0272: d1 0f d2 18 dc a0 9d 1c f1 e4 1c 0d f8 88 85 6bk
0288: 6d 11 24 3e 61 de 48 95 5f 2a d1 c9 ad 3f b8 41 m.\$>a.H._*...?.A
0304: 49 6d 9f 7c 3c bf 20 fe 37 7f 8c 8c 8f 72 ca f4 Im.|<. .7....r..
0320: 19 e4 cc a1 d8 08 cb 69 ec da 2b 88 e8 98 e9 1ei..+.....
0336: 29 af 86 6f 19 a8 67 56 ef b4 33 e4 2b b8 fe 61)..o..gV..3.+..a
0352: ad 36 4c 42 f8 ec 04 38 09 62 02 66 b5 54 fc 69 .6LB...8.b.f.T.i
0368: 46 29 05 27 d8 32 fd 37 4c d4 62 55 e1 ae e9 62 F).'.2.7L.bU...b
0384: 66 a0 f4 cb 4b 01 af 6b ea 09 80 00 a2 2b ff 0e f...K..k.....+..
0400: 85 2c 92 b2 5c f9 f3 eb 44 a3 9a e8 55 bb e3 2f ,,,\...D...U../
0416: 2d 20 5a 77 67 97 57 90 7f 4b b3 08 92 41 1a c0 - Zwg.W..K...A..
0432: f6 1b e9 a4 06 29 ea 31 eb 81 f0 94 96 aa 26 95).1.....&.
0448: 06 ed 4b f0 d3 9f aa 73 89 fa 6e f7 8f 4b f5 fa ..K....s..n..K..
0464: e4 5f 7c b6 08 e9 b2 18 77 99 9c ac 7b fb ec 41 ._|.....w...{..A
0480: 41 1e 29 c2 d0 a5 de bc 59 2f 14 45 6d af b1 e0 A.).....Y/.Em...
0496: 9c 77 73 0e ac 52 23 73 11 35 27 17 8c a3 ff 0e .ws..R#s.5'.....
0512: 52 5d b7 c8 06 c5 05 43 15 53 e8 fc 83 64 df 10 R]....C.S...d..
0528: 8b 9c 74 5c 0e d9 54 5e 9a 49 cf 13 e4 1d 86 35 ..t\..T^.I.....5
0544: 24 a3 27 75 d3 d6 b4 95 78 8f 0d 81 3b 80 6b 26 \$. 'u....x...;k&
0560: 25 9f 14 b1 65 73 e8 ce fa 95 6d b1 15 0c 76 3c %...es....m...v<
0576: b1 75 a9 96 78 c8 4b 91 06 a9 94 bc ec fa 44 eb .u..x.K.....D.
0592: 39 77 4d ee df ae eb 0e 90 61 eb ab 6a 17 1b 24 9wM.....a..j..\$
0608: 3c 3a 6e c4 bb 6f 72 46 3d 9a b8 8c 6a e7 45 c7 <:n..orF=...j.E.
0624: 0f 81 db 19 6e ce 65 74 ca db 73 ec 1e ce 5f d7n.et..s...._
0640: 43 6b fe ff c0 e1 61 26 aa b7 6f e0 dc 7f d1 de Ck....a&..o.....
0656: 95 f0 28 fd 24 9c 73 1c cf ef 3e fe 21 a1 e5 4e ..(.\$s...>.!..N
0672: 77 da db 12 01 7a e4 2c b5 f3 9d 30 e6 49 99 d6 w....z.,...0.I..
0688: 21 58 cc 5b 5b d5 ff ca ea df 9a fd d6 73 be cd !X.[[.....s..
0704: ae 7c 0d ea 78 e4 dd 74 f9 93 53 21 70 b7 cd 16 .|.x..t..S!p...
0720: ea c7 e9 5d 01 e0 e3 e6 53 46 7f fa a0 48 3e 5b ...]....SF...H>[
0736: af 64 46 ff 0f 0c b5 c9 92 48 e8 20 35 1d c8 ae .dF.....H. 5...
0752: d8 c4 38 31 aa 2c b5 91 6b eb 86 ac 2b fa 86 f2 ..81.,..k...+...
0768: d1 bd 7d 51 4c be f3 bf 4b d0 f0 78 0e 20 d3 30 ..}QL...K..x. .0
0784: fc f8 00 53 2a 6a 9b d9 e4 0e 08 d1 ad 52 7a ca ...S*j.....Rz.
0800: f3 8b 0e a8 fb 45 3c 66 03 66 b4 54 a5 3d 8e dfE<f.f.T.=..
0816: 4a 8f 66 f0 16 44 3b a9 f1 b3 db bb 7e d6 38 e5 J.f..D;.....~.8.
0832: 5f 62 27 bb ba 34 0a 6f 9b 78 dd ae 54 ab 54 53 _b'..4.o.x..T.TS
0848: 3a e1 d2 f1 d8 1e 8b 31 61 cd 69 8a 63 fb 7c 24 :.....1a.i.c.|\$
0864: 75 5f e6 6d 64 3d e4 12 cb 2d b3 6f 0f 5a 19 28 u_.md=...-.o.Z.(
0880: 1f d6 f6 9c ee 44 11 1a c5 84 d6 e3 a2 05 5d d4D.....].
0896: 85 db f1 8f e4 17 df bc 4c 78 98 d1 70 3b 63 d6Lx..p;c.
0912: a4 91 db f1 9e 16 23 fa e0 54 f6 64 d1 0b d0 d6#..T.d....
0928: a6 fd f1 66 72 8c 65 d8 17 af c9 33 49 c8 e9 4d ...fr.e....3I..M
0944: 1c 0a 77 2b 96 86 f2 16 55 3a e3 f6 00 bb b6 5a ..w+....U:.....Z
0960: 86 f6 fc 3f d6 f9 a4 1d fd 29 1d 5b 65 dc b3 14 ...?.....).[e...
0976: 96 10 3e c1 9a 90 23 e8 88 81 24 42 68 7a aa 25 ..>...#...\$Bhz%
0992: ba f3 50 bd b9 ae be dc b3 ff 39 81 44 89 00 9d ..P.....9.D...

```

1008: 4e 26 d6 ef df 7c e0 53 d3 ed 34 07 3d f2 1e 42 N&...|.S..4.=.B
1024: 28 af 1d 12 ce 98 c7 b0 7b 90 81 b5 ea f3 2c      (.....{.....,

server public key c25519:
0000: 18 6c 55 03 db 1c 38 e3 40 d7 09 24 77 46 14 b8 .lU...8.@..$wF..
0016: 5e e4 7f 19 98 04 9b 90 1f f6 b9 7f b0 70 9e 32 ^.....p.2

shared secret
0000: 9b 73 7d 41 d6 cf bb 12 56 c5 8c ad 0a 6a e2 c9 .s}A....V....j..
0016: bf 84 a9 0a 72 91 eb 52 e4 c1 81 c8 d2 44 7b 56 ....r..R.....D{V

client kem key:
0000: 2c 0c 5a 36 e6 77 70 b4 d8 ab 38 9a 92 96 3a cd ,.Z6.wp...8....:
0016: 10 82 38 36 40 be 2d 66 08 02 b8 17 cf eb b9 be ..86@.-f.....

concatenation of KEM key and ECDH shared key:
0000: 2c 0c 5a 36 e6 77 70 b4 d8 ab 38 9a 92 96 3a cd ,.Z6.wp...8....:
0016: 10 82 38 36 40 be 2d 66 08 02 b8 17 cf eb b9 be ..86@.-f.....
0032: 9b 73 7d 41 d6 cf bb 12 56 c5 8c ad 0a 6a e2 c9 .s}A....V....j..
0048: bf 84 a9 0a 72 91 eb 52 e4 c1 81 c8 d2 44 7b 56 ....r..R.....D{V

encoded shared secret:
0000: 00 00 00 40 42 54 58 44 6f 22 75 63 04 de d7 5a ...@BTXDo"uc...Z
0016: 1f 23 fe f9 b1 8b 36 eb e0 e6 e2 60 c3 00 12 63 .#....6....`...c
0032: b0 18 3f 42 49 07 e6 d8 22 b3 b7 6c 6c 38 37 b5 ..?BI..."..ll87.
0048: b4 1f b0 d0 76 35 c7 57 e6 5e fb ef cb 5b c3 8a ....v5.W.^...[...
0064: 1a 15 a9 6d                                     ...m

```

Figure 1

Author's Address

Simon Josefsson

Email: simon@josefsson.org

URI: <https://blog.josefsson.org/>