Network Working Group
Internet-Draft
Intended status: Experimental
Expires: May 10, 2019

F. Kiefer
Mozilla
K. Kwiatkowski
Cloudflare

November 06, 2018

Hybrid ECDHE-SIDH Key Exchange for TLS
draft-kiefer-tls-ecdhe-sidh-00

Abstract

This draft specifies a TLS key exchange that combines the post-quantum key exchange, Supersingular elliptic curve isogenie diffie-hellman (SIDH), with elliptic curve Diffie-Hellman (ECDHE) key exchange.

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 May 10, 2019.

1. Introduction

Supersingular elliptic curve isogenie diffie-hellman (SIDH) has been proposed [SIDH] as a diffie-hellman like key-exchange protocol secure against quantum computers. Because there's not enough confidence in the security of SIDH yet it should only be used in combination with a classical key-exchange scheme.

This document defines a way to combine [eSIDH] with the ECDHE key exchanges defined in [RFC7748] for the TLS 1.3 [RFC8446] key-exchange.

"x25519" is combined with "sidh503" and "x448" is combined with "sidh751".

1.1. Performance Considerations

Both handshake partners have to compute the SIDH values in addition to the ECDHE values, which requires additional time for computation. The handshake messages also get larger because the SIDH values are added (see Section 4 for details).

1.2. Notation

x25519 and x448 denote the ECDHE algorithms defined over the respective curve from [RFC7748]. sidh503 and sidh751 denote the SIDH algorithms defined using a prime of bit-length "503" and "751" respectively.

1.3. Terminology

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.

2. Hybrid SIDH-ECDHE Key Exchange

A hybrid key exchange takes the output of two separate key exchanges and mixes the results in a secure way.

The ECDHE and SIDH shared secrets are calculated independently. The shared secret for ECDHE-SIDH is then the concatenation of the ECDHE and the SIDH shared secrets. For x25519sidh503 for example this is

secret = x25519_secret || sidh_secret

The HKDF-Extract step used by TLS is relied on to combine entropy from both secrets.

2.1. ECDHE shared secret calculation

The ECDHE shared secret calculation is performed as described in Section 7.4.2 of [RFC8446].

2.2. SIDH Key Exchange

This document uses primes p503 and p751 defined in [eSIDH] and [SIKE] for sidh503 and sidh751. See [SIKE] for details on how to compute key-exchange messages and the shared secret. Optimised versions of the algorithms mentioned here might be used.

2.2.1. Field Element Representation

Each element ("c=a+b*i") of the underlying quadratic field GF(p^2) is encoded as an array of bytes in little-endian order, i.e., the least significant octet appears first, where each element "a,b" from GF(p) is encoded using "itoos" from [SIKE] Section 1.2.6. In particular, an element of GF(p) is converted to

e_(n-1) * 256^(n-1) + ... + e_1 * 256 + e_0

with "n" 63 for p503 and 94 for p751. The octet representation of each element is then the concatenation of "e_i" in little endian, i.e. "e_0||...||e_(n-1)", and the octet representation of element "c" is the concatenation of "a" and "b", "a||b".

See "fp2toos" [SIKE] Section 1.2.6 to 1.2.8 for details.

2.2.2. Key-exchange message generation

After choosing a private key each party computes its public key (P, Q, R) using "isogen_l" from [SIKE] Section 1.3.5 and converts each element into octets (cf. Section 2.2.1).

See "pktoos" from [SIKE] Section 1.2.9 for details on converting the public key to octets.

2.2.3. Shared secret calculation

The SIDH shared secret is calculated as described in Section 1.3.6 of [SIKE] using "isoex_l".

Calculating SIDH shared secret requires each side to use isogenies of different degree. This document assumes parameterizations as

described in [SIKE], which is based on 4- and 3-power degree isogenies. In order to calculate the shared secret, the client always generates an ephemeral key pair based on 4-power degree isogenies. Accordingly, the server always generates an ephemeral key pair based on 3-power degree isogenies.

The shared secret is a j-invariant and therefore an element of GF(p^2). It is converted to octets as described in Section 2.2.1.

See "fp2toos" [SIKE] Section 1.2.6 to 1.2.8 for details. All values are encoded without length prefixes or separators.

3. Negotiated Groups

This document extends the enum of NamedGroups to use in the "supported_groups" extension from TLS 1.3 [RFC8446] Section 4.2.7. The new codepoint for the "Supported Groups Registry" is:

```
enum {
    ...,
    x25519sidh503(0x0105), x448sidh751(0x0106),
} NamedGroup;
```

4. ECDHE-SIDH key exchange parameters

This document defines ECDHE-SIDH parameters to use in the "key_share" extension from TLS 1.3 (see Section 4.2.8 of [RFC8446]).

ECDHE parameters for both clients and servers are encoded in the "key_exchange" field of a KeyShareEntry as described in Section 4.2.8 of [RFC8446] and [RFC7748]. SIDH parameters are appended to this value.

In particular, the contents are the serialised value of the following struct:

```
   struct {
       opaque X[coordinate_length];
       opaque P[sidh_coordinate_length];
       opaque Q[sidh_coordinate_length];
       opaque R[sidh_coordinate_length];
   } UncompressedPointRepresentation;
```

X is the public point from x25519 or x448 as described in [RFC7748].

P, Q, and R are the binary representations of three field elements over GF(p503^2) and GF(p751^2) respectively from the public SIDH key

values as described in Section 2.2.2. All values in the struct are encoded without length prefixes or separators.

Implementers MUST perform the checks to verify the SIDH public key as specified in Section 9 of [eSIDH].

5. Security Considerations

Security of SIDH is based on the isogeny walk problem, assuming elliptic curves between isogenies are supersingular (see [SIKE] chapter 4.1). Algorithms solving this problem as well as usage of isogenies as drop-in replacement for Diffie-Hellman are relatively young area of research. Therefore the security behind the ECDHE-SIDH handshake does not rely on the security of SIDH exclusively.

Idea behind ECDHE-SIDH hybrid scheme is to combine an existing key-agreement algorithm with what's believed to be a quantum-resistant one. When large quantum computers are available they will be able to break both x25519 and x448. In this case the ECDHE-SIDH scheme is still safe assuming SIDH is secure. On the other hand, if SIDH is found to be flawed, the hybrid scheme is still secure against classical attacks assuming security of x25519/x448. Security estimates for classical and quantum computers are provided in table below based on [SIKE] and [RFC7748]. [RNSL] Chapter 1 provides introduction to quantum resource estimates.

Scheme	Classical	Quantum	NIST PQ category
x25519sidh503	128-bit	64-qubit	1
x448sidh751	224-bit	96-qubit	3

As described in [ISOSEC] it is possible to perform active attacks on static-static or non-interactive variants of the SIDH scheme. The countermeasure for this attack was described in [KLM15]. Research proposes so-called "indirect key validation", using Fujisaki-Okamoto type transform. However, using this transform is impractical and thus SIDH can be considered secure only if used for ephemeral keys. A more detailed discussion can be found in [URBJAO].

Security against side-channel attacks is described in [SIKE]. Implementers are encouraged to use a constant-time implementation.

The security of the described key exchange relies on the security, in particular the collision resistance, of the used key-derivation function. TLS 1.3 uses HKDF [RFC5869] as its key-derivation

function. It is therefore important that the hash function used in HKDF is collision-resistant.

6. Test vectors

This section gives a test vectors for "x25519sidh503".

6.1. 1-RTT Handshake

Client SIDH-ECDHE public key:

```
Public Key (X25519||SIDH) [Len: 410 (32+378)]
    2b 5b 10 41 56 2f c7 04 d8 56 ce 41 9c e3 7d e6
    ae 0e 32 a9 98 5e a5 95 47 5a 9d a2 98 59 67 16
    6f ed 78 ba b1 01 e7 f4 c4 f4 9a d6 4f ac 8d ee
    ee 46 57 10 f7 12 40 41 7a 45 53 c2 35 b5 f7 a0
    42 9e c3 38 d3 7c 47 11 78 f7 8d d3 c9 18 9c 79
    7c dc d3 7f e4 93 ac 63 c4 77 5e 36 43 d5 2a 43
    ee a9 37 b6 88 41 86 98 c9 dc d6 b7 20 66 ab 3d
    d1 e4 f7 90 80 8d 8e fb 0b bf 79 bb b6 e2 13 c0
    38 4e 86 20 13 49 81 be 31 f9 2c 73 a3 2a e9 3c
    e1 7e b5 1b 75 2d 3f 26 79 7c c2 e5 e5 16 57 1d
    6f b4 06 4b 5d b1 9b bd d2 cf 4b f1 2b cd f9 b2
    5f 2c 9d 1b d1 78 55 4c b7 ec fa 7a 3a 64 dd db
    6b 43 0f 67 e9 61 1d 57 fe 63 c8 d4 b3 0f 7a 2f
    60 1b 0f 6a 3a e6 80 0c 14 b7 05 ae 06 bb 5c 46
    71 1b 0e d7 a0 e7 bb 5d 87 37 c4 56 d8 c4 b2 e1
    01 a6 39 70 14 13 50 22 4f cf d9 20 77 51 f7 c4
    37 27 c0 57 5c f2 be 36 3b f7 38 1f 95 5f 54 fc
    f4 ce 96 24 fa 04 d8 62 03 aa 9b 24 28 56 47 e9
    c3 04 24 5e ee b5 3e 16 25 c9 b3 0d 70 6e e7 a1
    a8 76 bf 8c 53 78 7f d0 a3 13 26 fd 3a b5 f6 11
    05 60 af 4a ad 7e 45 0c 41 de 52 e5 29 4d a1 42
    c3 7b 88 7b 6a ed 66 03 04 25 12 78 31 36 94 58
    86 e6 00 59 13 99 0c c1 5d 1c d0 f7 aa c3 73 a9
    dd 25 ac cd 4d 04 2a dd 77 f0 b0 96 6e 3a 0b 76
    df 59 92 de 38 fe e5 10 5d 8b 6d e5 b9 1e 1e 8c
    8b 9c a5 9c 52 2f 26 d6 73 0d
```

Client SIDH-ECDHE private key:

```
SIDH Private Key [Len: 32]
    37 83 09 b4 a8 c4 b8 6a 83 84 36 8a 18 55 d8 48
    69 f2 31 60 2e f0 a6 70 d3 24 fe 92 e5 25 82 01

X25519 Private Key [Len: 32]
    a0 31 67 54 87 02 0f cb ef 07 40 af d3 ec 90 19
    88 02 fa d5 83 46 46 c9 8e 0e 49 c0 e1 3e 86 1a
```

Client Hello:

CH [Len: 522]

```
01 00 02 06 03 03 bf d0 ca 2e 81 e2 6e c4 d8 01
6b 2e 86 f3 2e d9 d0 f9 83 93 85 03 50 3f 67 05
71 cf 82 1d 5c e4 00 00 02 13 01 01 00 01 db 00
00 00 0b 00 09 00 00 06 73 65 72 76 65 72 ff 01
00 01 00 00 0a 00 04 00 02 01 05 00 33 01 a0 01
9e 01 05 01 9a 2b 5b 10 41 56 2f c7 04 d8 56 ce
41 9c e3 7d e6 ae 0e 32 a9 98 5e a5 95 47 5a 9d
a2 98 59 67 16 6f ed 78 ba b1 01 e7 f4 c4 f4 9a
d6 4f ac 8d ee ee 46 57 10 f7 12 40 41 7a 45 53
c2 35 b5 f7 a0 42 9e c3 38 d3 7c 47 11 78 f7 8d
d3 c9 18 9c 79 7c dc d3 7f e4 93 ac 63 c4 77 5e
36 43 d5 2a 43 ee a9 37 b6 88 41 86 98 c9 dc d6
b7 20 66 ab 3d d1 e4 f7 90 80 8d 8e fb 0b bf 79
bb b6 e2 13 c0 38 4e 86 20 13 49 81 be 31 f9 2c
73 a3 2a e9 3c e1 7e b5 1b 75 2d 3f 26 79 7c c2
e5 e5 16 57 1d 6f b4 06 4b 5d b1 9b bd d2 cf 4b
f1 2b cd f9 b2 5f 2c 9d 1b d1 78 55 4c b7 ec fa
7a 3a 64 dd db 6b 43 0f 67 e9 61 1d 57 fe 63 c8
d4 b3 0f 7a 2f 60 1b 0f 6a 3a e6 80 0c 14 b7 05
ae 06 bb 5c 46 71 1b 0e d7 a0 e7 bb 5d 87 37 c4
56 d8 c4 b2 e1 01 a6 39 70 14 13 50 22 4f cf d9
20 77 51 f7 c4 37 27 c0 57 5c f2 be 36 3b f7 38
1f 95 5f 54 fc f4 ce 96 24 fa 04 d8 62 03 aa 9b
24 28 56 47 e9 c3 04 24 5e ee b5 3e 16 25 c9 b3
0d 70 6e e7 a1 a8 76 bf 8c 53 78 7f d0 a3 13 26
fd 3a b5 f6 11 05 60 af 4a ad 7e 45 0c 41 de 52
e5 29 4d a1 42 c3 7b 88 7b 6a ed 66 03 04 25 12
78 31 36 94 58 86 e6 00 59 13 99 0c c1 5d 1c d0
f7 aa c3 73 a9 dd 25 ac cd 4d 04 2a dd 77 f0 b0
96 6e 3a 0b 76 df 59 92 de 38 fe e5 10 5d 8b 6d
e5 b9 1e 1e 8c 8b 9c a5 9c 52 2f 26 d6 73 0d 00
2b 00 03 02 7f 1c 00 0d 00 04 00 02 04 01 00 2d
00 02 01 01 00 1c 00 02 40 01
```

Server selected KE = (EC)DHE. Group = 261.

Server SIDH-ECDHE public key:

```
Public Key (X25519||SIDH) [Len: 410 (32+378)]
    f8 c6 8f 4e 57 6b fb ec b3 de 23 d9 db 89 fc 1b
    f4 6f 01 a5 c0 91 61 fd c4 e7 bc 58 b4 eb 5f 76
    44 c4 c7 7b a3 09 1a 60 c7 15 8f 1e d6 83 f2 1c
    f8 36 13 a4 b3 c5 bc 4e 73 41 96 36 34 9a 9e 5a
    bc fc 9d fa 2b c3 2c 85 17 44 9b 21 8f bf ba f7
    7b 6c 19 c3 07 19 45 34 1e 88 cd 86 41 f8 32 38
    41 3d 75 20 e1 c9 4a 94 03 e4 2f 4b 38 2d 93 39
    b7 71 e9 84 80 b9 aa ca 97 39 5a c6 68 a7 b2 6f
    b0 3e 10 f0 02 e3 e3 62 78 23 b4 f7 f1 a8 ce cd
    71 a8 3a 23 81 63 ba 70 92 ea c6 9b 2c 35 93 6d
    b5 58 61 6d 2c 06 a5 4d 0d 27 35 20 0b 77 d0 0d
    65 f0 24 11 71 0b 71 45 2b 73 9c 42 fd d4 09 ba
    8a ed d2 9e 78 9c 2f 43 91 5d e7 3a 19 0b f8 2b
    71 6d 47 ae 86 e4 7a 9e e1 a0 de b5 08 bd a4 30
    bb c1 3e ad db 75 79 36 a0 0a ea 70 a0 9c 64 f7
    ba 92 a4 02 05 4d d4 9b ba a8 b3 9e 92 cd 28 13
    0e 84 81 90 84 cd ae 09 b2 0b 12 23 1c b4 3a 18
    cb 66 a1 8a 81 63 d4 e7 06 1c 16 04 29 20 2b cf
    da a3 90 55 15 4a 15 ab 30 95 f1 20 b0 84 f5 7e
    0f 92 f6 7f 4d 8c 22 2a a8 80 41 7b ee fa 85 f8
    e2 4d 45 38 28 eb e2 fd a5 c6 1e 37 98 9f a2 ed
    13 b9 dd f5 21 bc 78 10 2f 99 21 dc 30 55 57 58
    c6 59 89 13 f9 76 aa e1 ec 0d 82 27 74 a1 86 b5
    d1 74 12 49 5f ac a0 25 d2 91 5a 26 11 5e 0e f8
    d2 7f 00 7f 8e 8b 7d 89 93 ba 69 4c 5f c7 7c df
    d0 45 f4 17 3c 0c 03 df bf 1e

Server SIDH-ECDHE private key:

SIDH Private Key [Len: 32]
    ca a5 1b 8d cc 2e df b0 b9 f5 ed 9d b0 1c f4 7c
    b6 61 07 4d 5f e3 9d 6a 24 48 71 48 f3 11 4d 0a

X25519 Private Key [Len: 32]
    a1 27 74 2c 0e ea 56 25 41 68 f4 7c d0 94 30 03
    5e 7e cb 3d e0 4f 84 36 41 e8 b4 39 1e 45 99 91

Handshake secrets "tls13 s hs traffic":
```

PRK [Len: 32]
35 7b 46 ed 6d f0 40 77 ae 2a a0 f4 47 cc df c1
78 54 74 48 d4 ff 69 05 f9 d5 2f 9a 00 1c e8 86

Hash [Len: 32]
52 a5 04 4f 78 da 41 12 b8 ac 35 f3 37 54 0c 51
18 ba c9 be c7 de 06 21 b2 f8 22 b6 e1 fa b5 96

Info [Len: 54]
00 20 12 74 6c 73 31 33 20 73 20 68 73 20 74 72
61 66 66 69 63 20 52 a5 04 4f 78 da 41 12 b8 ac
35 f3 37 54 0c 51 18 ba c9 be c7 de 06 21 b2 f8
22 b6 e1 fa b5 96

Derived key [Len: 32]
e4 31 ba e7 1e 38 f1 d6 81 17 83 56 d3 8d 0e 35
cf 42 6a 05 a2 2b 03 df d6 bb 4f 72 94 d2 9f c3

Handshake secrets "tls13 c hs traffic":

Info [Len: 54]
00 20 12 74 6c 73 31 33 20 63 20 68 73 20 74 72
61 66 66 69 63 20 52 a5 04 4f 78 da 41 12 b8 ac
35 f3 37 54 0c 51 18 ba c9 be c7 de 06 21 b2 f8
22 b6 e1 fa b5 96

Derived key [Len: 32]
d2 99 cb cb 70 91 05 b6 3f 62 a5 e7 a2 5c 9c 07
2b 98 d9 0c d0 92 1c f2 0f c3 6a fa b3 57 4d 2a

Server Handshake:

SH [Len: 468]
02 00 01 d0 03 03 8b 94 f0 f0 25 bd 87 30 3f 1c
7c 86 e0 bc 25 e3 7f d7 ca 77 88 c5 a3 3c 69 34
c8 ec a9 64 15 85 00 13 01 00 01 a8 00 33 01 9e
01 05 01 9a f8 c6 8f 4e 57 6b fb ec b3 de 23 d9
db 89 fc 1b f4 6f 01 a5 c0 91 61 fd c4 e7 bc 58
b4 eb 5f 76 44 c4 c7 7b a3 09 1a 60 c7 15 8f 1e
d6 83 f2 1c f8 36 13 a4 b3 c5 bc 4e 73 41 96 36
34 9a 9e 5a bc fc 9d fa 2b c3 2c 85 17 44 9b 21
8f bf ba f7 7b 6c 19 c3 07 19 45 34 1e 88 cd 86
41 f8 32 38 41 3d 75 20 e1 c9 4a 94 03 e4 2f 4b
38 2d 93 39 b7 71 e9 84 80 b9 aa ca 97 39 5a c6
68 a7 b2 6f b0 3e 10 f0 02 e3 e3 62 78 23 b4 f7
f1 a8 ce cd 71 a8 3a 23 81 63 ba 70 92 ea c6 9b
2c 35 93 6d b5 58 61 6d 2c 06 a5 4d 0d 27 35 20
0b 77 d0 0d 65 f0 24 11 71 0b 71 45 2b 73 9c 42

```
      fd d4 09 ba 8a ed d2 9e 78 9c 2f 43 91 5d e7 3a
      19 0b f8 2b 71 6d 47 ae 86 e4 7a 9e e1 a0 de b5
      08 bd a4 30 bb c1 3e ad db 75 79 36 a0 0a ea 70
      a0 9c 64 f7 ba 92 a4 02 05 4d d4 9b ba a8 b3 9e
      92 cd 28 13 0e 84 81 90 84 cd ae 09 b2 0b 12 23
      1c b4 3a 18 cb 66 a1 8a 81 63 d4 e7 06 1c 16 04
      29 20 2b cf da a3 90 55 15 4a 15 ab 30 95 f1 20
      b0 84 f5 7e 0f 92 f6 7f 4d 8c 22 2a a8 80 41 7b
      ee fa 85 f8 e2 4d 45 38 28 eb e2 fd a5 c6 1e 37
      98 9f a2 ed 13 b9 dd f5 21 bc 78 10 2f 99 21 dc
      30 55 57 58 c6 59 89 13 f9 76 aa e1 ec 0d 82 27
      74 a1 86 b5 d1 74 12 49 5f ac a0 25 d2 91 5a 26
      11 5e 0e f8 d2 7f 00 7f 8e 8b 7d 89 93 ba 69 4c
      5f c7 7c df d0 45 f4 17 3c 0c 03 df bf 1e 00 2b
      00 02 7f 1c

   SH [Len: 651]
      08 00 00 14 00 12 00 0a 00 04 00 02 01 05 00 1c
      00 02 40 01 00 00 00 00 0b 00 01 c3 00 00 01 bf
      00 01 ba 30 82 01 b6 30 82 01 1f a0 03 02 01 02
      02 01 05 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b
      05 00 30 13 31 11 30 0f 06 03 55 04 03 0c 08 72
      73 61 5f 73 69 67 6e 30 1e 17 0d 31 38 30 36 31
      30 31 30 32 34 31 32 5a 17 0d 32 38 30 36 31 30
      31 30 32 34 31 32 5a 30 13 31 11 30 0f 06 03 55
      04 03 0c 08 72 73 61 5f 73 69 67 6e 30 81 9f 30
      0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 81
      8d 00 30 81 89 02 81 81 00 c6 96 5e 96 71 5a ea
      40 c2 c0 60 c7 c7 4e 98 b3 40 0c 02 a3 1c 9c 8e
      e7 c6 57 6b 48 8c 23 04 d4 e8 54 09 37 c2 b8 b1
      ac b4 49 b7 76 ef 59 f8 3f 7c 4e e3 6a fa 32 04
      53 74 85 2d 0d 8e 91 ad 2d 65 52 ec f2 54 1c 82
      f1 b5 46 c8 5e ec e1 4e 6a f1 a1 c8 9f 9c 2b e1
      79 3b 85 58 80 19 d5 f2 87 cb c0 13 5f 56 56 d3
      75 78 bb 71 ef fa df e4 98 76 31 47 72 9b 5d 6a
      fe d7 c9 58 e6 d2 c6 2c 5f 02 03 01 00 01 a3 1a
      30 18 30 09 06 03 55 1d 13 04 02 30 00 30 0b 06
      03 55 1d 0f 04 04 03 02 07 80 30 0d 06 09 2a 86
      48 86 f7 0d 01 01 0b 05 00 03 81 81 00 07 58 be
      81 c3 60 a0 cb 94 bc 79 81 0c b5 c6 ec 84 c6 c0
      f8 d9 63 50 0a 7e b2 9d 80 95 5d b2 ba c9 31 72
      73 d5 78 97 d1 5f e3 d9 f8 54 25 e0 1a 0e 7f 2b
      ec 20 27 b6 ba ff 9c 38 42 23 ed 10 c4 51 54 f2
      a3 45 54 df 59 be 83 d4 b8 00 7f 13 a3 27 40 ca
      af 66 72 f5 f7 cf 1e 4d 6c 94 e4 02 46 cf f7 9d
      13 7e 72 6b 77 20 15 9c c9 f7 c2 f1 5f 00 91 d3
      da c6 2e 71 f0 51 82 db 13 b2 ee c7 0c 00 00 0f
      00 00 84 04 01 00 80 7e c8 cb 1d d8 2e 83 d4 7e
```

```
    69 8a db 8d 39 79 13 49 9f 03 21 7a 2f 5f ef df
    2e 07 58 a8 0f 4b 61 85 10 25 01 3c cc 14 ef ac
    35 17 c8 ed 27 17 0f 6e e5 78 7e 19 b5 0a 99 2d
    bd 68 f4 47 0e 0a 11 cb 57 12 d5 73 cd 20 05 a4
    b5 04 6c 13 6c 1b 9a f9 15 aa cc ca c2 22 83 fe
    37 5f c3 f2 24 09 e3 d5 df 26 9f ab 84 e9 92 68
    38 73 09 b1 58 55 43 79 02 59 0c 13 cc 68 4f 53
    62 4b 72 d7 3b 17 86 14 00 00 20 d1 6e ba a6 9a
    12 01 ec 46 fb e4 2c 8b 0e dd b5 73 a9 d7 e1 da
    ba c5 c3 0d 53 5d 90 24 fd 53 60
```

Client finished handshake:

```
Client finished [Len: 36]
    14 00 00 20 8e 34 2d 9d 69 fb 95 76 65 05 03 4d
    cf 27 21 59 7c 45 f7 0e 3f 1e d9 29 18 4b 29 87
    6a a5 c1 4d
```

Shared secret (server & client):

```
Shared secret (X25519||SIDH) [Len: 158 (32+126)]
    f0 93 ac 03 ca 0b 5c 05 e6 c3 d3 7f ae 71 10 57
    a6 a6 3e c7 7c 12 8d 21 8b 39 fc a5 8a 19 69 02
    31 c8 0b 85 96 07 d4 f2 9b 5d ca a1 2d 69 78 2a
    4f d8 1e c5 ea 87 ff 24 a2 7e b3 96 db 63 d5 66
    cd f8 13 d3 34 70 e8 03 10 34 44 68 2d 6b 11 1a
    a9 a0 58 cd 54 ed ce 8b 27 bc 3d ef 23 4b 2e f7
    0b 28 de 95 d9 de 45 4a 73 48 d1 ad 51 21 f6 fe
    fa ae 22 64 b5 2c db f7 99 7e 5b 3c 09 06 d9 eb
    e1 a3 a7 8f 34 74 a2 77 a0 85 ca 11 d4 1b 44 53
    ed eb 8c 67 b4 f2 62 6e 54 4c 97 a9 1a 27
```

7. IANA Considerations

TODO: register the codepoints

8. References

8.1. Normative References

[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>.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <https://www.rfc-editor.org/info/rfc5869>.

[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>.

[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/info/rfc8446>.

[SIDH] Jao, D. and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenie", PQCrypto-2011 , 2011, <https://eprint.iacr.org/2011/506.pdf>.

[SIKE] Azarderakhsh, R., Campagna, M., Costello, C., De Feo, L., Hess, B., Jalali, A., Jao, D., Koziel, B., LaMacchia, B., Longa, P., Naehrig, M., Renes, J., Soukharev, V., and D. Urbanik, "Supersingular Isogeny Key Encapsulation", Submission to the NIST Post-Quantum Standardization project , 2017, <http://sike.org/files/SIDH-spec.pdf>.

8.2. Informative References

[eSIDH] Costello, C., Longa, P., and M. Naehrig, "Efficient algorithms for supersingular isogeny Diffie-Hellman", IACR-CRYPTO-2016 , 2016, <https://eprint.iacr.org/2016/413.pdf>.

[ISOSEC] Galbraith, S., Petit, C., Shani, B., and Y. Bo Ti, "On the security of supersingular isogeny cryptosystems", IACR-CRYPTO-2016 , 2016, <https://eprint.iacr.org/2016/859.pdf>.

[KLM15] Kirkwood, D., Lackey, B., McVey, J., Motley, M., Solinas, J., and D. Tuller, "Failure is not an Option: Standardization Issues for Post-Quantum Key Agreement", Workshop on Cybersecurity in a Post Quantum World, 2015 , 2015.

[RNSL] Roetteler, M., Naehrig, M., Svore, K., and K. Lauter, "Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms", arXiv , 2017, <https://arxiv.org/pdf/1706.06752.pdf>.

[URBJAO] Urbanik, D. and D. Jao, "SoK: The Problem Landscape of SIDH", IACR-CRYPTO-2018 , 2018, <https://eprint.iacr.org/2018/336.pdf>.

Acknowledgements

- Martin Thomson
  Mozilla
  mt@mozilla.com

Authors' Addresses

Franziskus Kiefer
Mozilla

Email: franziskuskiefer@gmail.com

Krzysztof Kwiatkowski
Cloudflare

Email: kris@cloudflare.com