TLS
Internet-Draft
Intended status: Standards Track
Expires: January 1, 2018

M. Thomson
Mozilla

June 30, 2017

Example Handshake Traces for TLS 1.3
draft-ietf-tls-tls13-vectors-01

Abstract

Examples of TLS 1.3 handshakes are shown. Private keys and inputs are provided so that these handshakes might be reproduced. Intermediate values, including secrets, traffic keys and ivs are shown so that implementations might be checked incrementally against these values.

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 http://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 January 1, 2018.

Copyright Notice

Table of Contents

1. Introduction

TLS 1.3 [I-D.ietf-tls-tls13] defines a new key schedule and a number new cryptographic operations. This document includes sample handshakes that show all intermediate values. This allows an implementation to be verified incrementally, examining inputs and outputs of each cryptographic computation independently.

Private keys are included with the traces so that implementations can be checked by importing these values and verifying that the same outputs are produced.

2. Private Keys

Ephemeral private keys are shown as they are generated in the traces.

The server in most examples uses an RSA certificate with a private key of:

```
modulus (public):  b4bb498f8279303d 980836399b36c698 8c0c68de55e1bdb8
   26d3901a2461eafd 2de49a91d015abbc 9a95137ace6c1af1
   9eaa6af98c7ced43 120998e187a80ee0 ccb0524b1b018c3e
   0b63264d449a6d38 e22a5fda43084674 8030530ef0461c8c
   a9d9efbfae8ea6d1 d03e2bd193eff0ab 9a8002c47428a6d3
   5a8d88d79f7f1e3f

public exponent:  010001

private exponent:  04dea705d43a6ea7 209dd8072111a83c 81e322a59278b334
```

80641eaf7c0a6985 b8e31c44f6de62e1 b4c2309f6126e77b
7c41e923314bbfa3 881305dc1217f16c 819ce538e922f369
828d0e57195d8c84 88460207b2faa726 bcf708bbd7db7f67
9f893492fc2a622e 08970aac441ce4e0 c3088df25ae67923
3df8a3bda2ff9941

prime1: e435fb7cc8373775 6dacea96ab7f59a2 cc1069db7deb190e
17e33a532b273f30 a327aa0aaabc58cd 67466af9845fadc6
75fe094af92c4bd1 f2c1bc33dd2e0515

prime2: cabd3bc0e0438664 c8d4cc9f99977a94 d9bbfead8e43870a
bae3f7eb8b4e0eee 8af1d9b4719ba619 6cf2cbbaeeebf8b3
490afe9e9ffa74a8 8aa51fc645629303

exponent1: 3f57345c27fe1b68 7e6e761627b78b1b 826433dd760fa0be
a6a6acf39490aa1b 47cda4869d68f584 dd5b5029bd32093b
8258661fe715025e 5d70a45a08d3d319

exponent2: 183da01363bd2f28 85cacbdc9964bf47 64f1517636f86401
286f71893c52ccfe 40a6c23d0d086b47 c6fb10d8fd1041e0
4def7e9a40ce957c 417794e10412d139

coefficient: 839ca9a085e4286b 2c90e466997a2c68 1f21339aa3477814
e4dec11833050ed5 0dd13cc038048a43 c59b2acc416889c0
37665fe5afa60596 9f8c01dfa5ca969d

3. Simple 1-RTT Handshake

In this example, the simplest possible handshake is completed. The server is authenticated, but the client remains anonymous. After connecting, a few application data octets are exchanged. The server sends a session ticket that permits the use of 0-RTT in any resumed session.

{client} create an ephemeral x25519 key pair:

private key (32 octets): 8d471715ed09bd58 e1ea7f90f4bd1b96
b23f5f53f6d1b3c5 8d12f5c06a3921a0

public key (32 octets): 1db0a34c651f3a3f 9011b8c1bdd7714a
a3593833e2e37cea a3a4796f6ee35657

```
{client}  send a ClientHello handshake message

{client}  send handshake record:

   payload (512 octets):  010001fc0303e864 702db55462aa0e96
      ed08c0d9a1dc18d5 1cffb1d668298ac0 45a2645780f30000
      3e130113031302c0 2bc02fcca9cca8c0 0ac009c013c023c0
      27c014009eccaa00 3300320067003900 38006b0016001300
      9c002f003c003500 3d000a0005000401 0001950000000b00
      0900000673657276 6572ff0100010000 0a00140012001d00
      1700180019010001 0101020103010400 0b00020100002300
      0000280026002400 1d00201db0a34c65 1f3a3f9011b8c1bd
```



```
      d7714aa3593833e2 e37ceaa3a4796f6e e35657002b000706
      7f1403030302000d 0020001e04030503 0603020308040805
      0806040105010601 0201040205020602 0202002d00020101
      001500fc00000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000

   ciphertext (517 octets):  1603010200010001 fc0303e864702db5
      5462aa0e96ed08c0 d9a1dc18d51cffb1 d668298ac045a264
      5780f300003e1301 13031302c02bc02f cca9cca8c00ac009
      c013c023c027c014 009eccaa00330032 006700390038006b
      00160013009c002f 003c0035003d000a 0005000401000195
      0000000b00090000 06736572766572ff 01000100000a0014
      0012001d00170018 0019010001010102 01030104000b0002
      0100002300000028 00260024001d0020 1db0a34c651f3a3f
      9011b8c1bdd7714a a3593833e2e37cea a3a4796f6ee35657
      002b0007067f1403 030302000d002000 1e04030503060302
      0308040805080604 0105010601020104 0205020602020200
      2d00020101001500 fc00000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
```

```
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
```

{server} extract secret "early":

salt: (absent)

ikm (32 octets): 0000000000000000 0000000000000000
0000000000000000 0000000000000000

secret (32 octets): 33ad0a1c607ec03b 09e6cd9893680ce2
10adf300aa1f2660 e1b22e10f170f92a

{server} create an ephemeral x25519 key pair:

private key (32 octets): 8b587c8205a29c7e 7bce7475cfa595d3
78d09e79b25d7db9 07cd92259a628dc3

public key (32 octets): b80ea5ef65d8ee1b 524abb29c857142e
a9e4591fc0e38dc2 4d2361a3988be019

{server} send a ServerHello handshake message

{server} derive secret for handshake "tls13 derived":

PRK (32 octets): 33ad0a1c607ec03b 09e6cd9893680ce2
10adf300aa1f2660 e1b22e10f170f92a

hash (32 octets): e3b0c44298fc1c14 9afbf4c8996fb924
27ae41e4649b934c a495991b7852b855

info (49 octets): 00200d746c733133 2064657269766564
20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
4ca495991b7852b8 55

```
      output (32 octets):  6f2615a108c702c5 678f54fc9dbab697
         16c076189c48250c ebeac3576c3611ba

   {server}  extract secret "handshake":

      salt (32 octets):  6f2615a108c702c5 678f54fc9dbab697
         16c076189c48250c ebeac3576c3611ba

      ikm (32 octets):  5aa03a79c923fa4c 683d9cba739516c4
         c69ad15c0db40b7c 6e21e2ff71f40f06

      secret (32 octets):  e4e77cf10307c913 575026d3d193b181
         f90ee4aa69f53f17 3426d62704623e85

   {server}  derive secret "tls13 c hs traffic":

      PRK (32 octets):  e4e77cf10307c913 575026d3d193b181
         f90ee4aa69f53f17 3426d62704623e85

      hash (32 octets):  1d88ec0fc94ca5fc dbf7bd3f4be8dac8
         09f98d58af751934 771d7268c79310e3

      info (54 octets):  002012746c733133 2063206873207472
         6166666963201d88 ec0fc94ca5fcdbf7 bd3f4be8dac809f9
         8d58af751934771d 7268c79310e3
```



```
      output (32 octets):  041ae38c959b6d93 7dba0da43d2b3bc0
         a81da11279935399 5720bc155657934a

   {server}  derive secret "tls13 s hs traffic":

      PRK (32 octets):  e4e77cf10307c913 575026d3d193b181
         f90ee4aa69f53f17 3426d62704623e85

      hash (32 octets):  1d88ec0fc94ca5fc dbf7bd3f4be8dac8
         09f98d58af751934 771d7268c79310e3

      info (54 octets):  002012746c733133 2073206873207472
         6166666963201d88 ec0fc94ca5fcdbf7 bd3f4be8dac809f9
         8d58af751934771d 7268c79310e3
```

```
   output (32 octets):  b05eae2a3c213f62 9ff677f9afff5589
      368b1baf54b1bdc6 80f43b4e523f1e3b

{server}  derive secret for master "tls13 derived":

   PRK (32 octets):  e4e77cf10307c913 575026d3d193b181
      f90ee4aa69f53f17 3426d62704623e85

   hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
      27ae41e4649b934c a495991b7852b855

   info (49 octets):  00200d746c733133 2064657269766564
      20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
      4ca495991b7852b8 55

   output (32 octets):  7ed62a7bc6fb30cf 5f526ab9cb7dcc25
      cdd239c36a2985b6 938ce1619bf2647d

{server}  extract secret "master":

   salt (32 octets):  7ed62a7bc6fb30cf 5f526ab9cb7dcc25
      cdd239c36a2985b6 938ce1619bf2647d

   ikm (32 octets):  0000000000000000 0000000000000000
      0000000000000000 0000000000000000

   secret (32 octets):  e845be8dbb7556ed 9a4921f663c88cd6
      8387f72e4e2572dc 59f22c5cda035862

{server}  send handshake record:

   payload (82 octets):  0200004e7f14a6b9 ce3215b325616f22
      48f11f776a98d174 8e895118182143cc 67c46f3f11831301
```



```
      002800280024001d 0020b80ea5ef65d8 ee1b524abb29c857
      142ea9e4591fc0e3 8dc24d2361a3988b e019

   ciphertext (87 octets):  1603010052020000 4e7f14a6b9ce3215
      b325616f2248f11f 776a98d1748e8951 18182143cc67c46f
      3f11831301002800 280024001d0020b8 0ea5ef65d8ee1b52
      4abb29c857142ea9 e4591fc0e38dc24d 2361a3988be019
```

```
{server}  derive write traffic keys for handshake data:

   PRK (32 octets):  b05eae2a3c213f62 9ff677f9afff5589
      368b1baf54b1bdc6 80f43b4e523f1e3b

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  1837f9353c2e7a0d 279923526c53aead

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  876dd44a5f0cc952 08425386

{server}  send a EncryptedExtensions handshake message

{server}  send a Certificate handshake message

{server}  send a CertificateVerify handshake message

{server}  calculate finished "tls13 finished":

   PRK (32 octets):  b05eae2a3c213f62 9ff677f9afff5589
      368b1baf54b1bdc6 80f43b4e523f1e3b

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  15348eafde4ec0f8 3808818c95c7b285
      acf763920eef62ac 0e314b391632ad9e

{server}  send a Finished handshake message

{server}  send handshake record:

   payload (651 octets):  0800001e001c000a 00140012001d0017
      0018001901000101 0102010301040000 00000b0001b90000
      01b50001b0308201 ac30820115a00302 0102020102300d06
      092a864886f70d01 010b0500300e310c 300a060355040313
      03727361301e170d 3136303733303031 323335395a170d32
```



```
      3630373330303132 3335395a300e310c 300a060355040313
```

```
   0372736130819f30 0d06092a864886f7 0d01010105000381
   8d00308189028181 00b4bb498f827930 3d980836399b36c6
   988c0c68de55e1bd b826d3901a2461ea fd2de49a91d015ab
   bc9a95137ace6c1a f19eaa6af98c7ced 43120998e187a80e
   e0ccb0524b1b018c 3e0b63264d449a6d 38e22a5fda430846
   748030530ef0461c 8ca9d9efbfae8ea6 d1d03e2bd193eff0
   ab9a8002c47428a6 d35a8d88d79f7f1e 3f0203010001a31a
   301830090603551d 1304023000300b06 03551d0f04040302
   05a0300d06092a86 4886f70d01010b05 000381810085aad2
   a0e5b9276b908c65 f73a7267170618a5 4c5f8a7b337d2df7
   a594365417f2eae8 f8a58c8f8172f931 9cf36b7fd6c55b80
   f21a030151567260 96fd335e5e67f2db f102702e608ccae6
   bec1fc63a42a99be 5c3eb7107c3c54e9 b9eb2bd5203b1c3b
   84e0a8b2f759409b a3eac9d91d402dcc 0cc8f8961229ac91
   87b42b4de100000f 0000840804008052 e8915b097ea305da
   d8a511a03ea45c34 a14e04a1f13a8b45 279654262702f9d8
   b2b1897bfebae516 09b265eae67dc898 0ef9aac9514e84b3
   3b1d8dc3105e5139 5854964d9bca28e8 aab0b968808c4d99
   4c963253d13dc1ed c98945fa0c72cb74 959d9204740e968b
   9dbc9d97914fb2fb e9671300d3aeb5eb 40d3fe5ad425e014
   0000200d2c10fab6 abf8cbaa97b91816 2516fdfb4a1129c3
   98bb5fe97848d910 208036

ciphertext (673 octets):  170301029cda8377 df12c42a7c157681
   92a0a724c1a2a070 4f4901e91dd4a873 3dcee9461401f7c7
   ad2b7584fe18d87b d12d05d718c46c04 3deef39e63b7a50e
   747de04a55d8074a 14ff21803864d8ee 65482da8b307ed8f
   11df14701c81bd3b ba9f86f7e83a392f 23532abd49396450
   f3cf32d369b27eb9 2427ace4f141defe fa777cb75c5fa511
   90d2399035164350 f0d59cdba5369141 d453467634ed876c
   3e423b715d47272f f84b0e797850c89d ce8119b45af1c439
   0e5c66661f4ed0e6 ca7018d189d71e76 7addc2e28f48ccd3
   c61b236fb02160f2 38763de832b8f5b1 76d29809e6d95123
   0fb0fb0a66c0d4c4 11a0fdd1fd7b3f54 7b0abfd5f4df3b60
   a4aa4a230a69d7e0 b28c71a1bcbbc071 0474e682c1a27912
   bc4463688b2d781f 0c41e48dd169378f d5a9416ce1e89930
   a5166a4c6cf52b80 14c368a52ed0173e 56758688b99838f9
   d54e4139e5bf34ff 4a5295dd6183774a db81074abd9a8ccd
   621afc59b311cc65 0f28ce32b78fe0bc 5ea36a868bcd43ab
   f2c49223eb02318a 609820cb516afc69 89593e77002be6d8
   4b2b84159ce70e50 868fc8fd42b0d123 976f8caaf363b68d
   c390dc07ee9fa818 22840d3c3bfe2e3c 62df1e98ce6acdb6
   6f65a6b7f39599ab c21a9c6e1e3ec631 3bcf3a3add55f786
   595b394e05dbc16d 66953061ffb564d7 2f023f74b3798e16
   3454e8d206aa0e0a a737f5abe22df433 9ba24ce9500005aa
   82ea5af110a202f8 24fd9f561e57f2cd 5a54b42d672401cc
   ea1ef5a9967ecc65 b735a7b860156954 04e027e756157a3f
```

```
      88546d127c53d638 54032aafb7760205 60defc8e8f98853c
      40dd3c2772e619e4 723f2936c3b6da21 9d00caa6c13d77d9
      cfb6acfa3148fb1a 45ffcc9594f43fb2 af18f1e54ef1750f
      21bddce6449807b2 e7e8090ffda954a7 302722f2ea1333eb
      e85fcb49ae7871d2 38

{server}  derive secret "tls13 c ap traffic":

   PRK (32 octets):  e845be8dbb7556ed 9a4921f663c88cd6
      8387f72e4e2572dc 59f22c5cda035862

   hash (32 octets):  0e69e4a8fd0448d1 3862dc670e97c44f
      c157d1adc99f3639 c9bd3f9dbc2990cf

   info (54 octets):  002012746c733133 2063206170207472
      6166666963200e69 e4a8fd0448d13862 dc670e97c44fc157
      d1adc99f3639c9bd 3f9dbc2990cf

   output (32 octets):  9e0bf6b565b4c386 d3f0a7faaecffac8
      76716d97ef7e1920 9b6a82fbc2e78ab6

{server}  derive secret "tls13 s ap traffic":

   PRK (32 octets):  e845be8dbb7556ed 9a4921f663c88cd6
      8387f72e4e2572dc 59f22c5cda035862

   hash (32 octets):  0e69e4a8fd0448d1 3862dc670e97c44f
      c157d1adc99f3639 c9bd3f9dbc2990cf

   info (54 octets):  002012746c733133 2073206170207472
      6166666963200e69 e4a8fd0448d13862 dc670e97c44fc157
      d1adc99f3639c9bd 3f9dbc2990cf

   output (32 octets):  d4a9974dc6c15c4b d5e35add69b1a20c
      b78affe36ab431e8 264567a25f89d35b

{server}  derive secret "tls13 exp master":

   PRK (32 octets):  e845be8dbb7556ed 9a4921f663c88cd6
      8387f72e4e2572dc 59f22c5cda035862

   hash (32 octets):  0e69e4a8fd0448d1 3862dc670e97c44f
      c157d1adc99f3639 c9bd3f9dbc2990cf

   info (52 octets):  002010746c733133 20657870206d6173
      746572200e69e4a8 fd0448d13862dc67 0e97c44fc157d1ad
```

```
      c99f3639c9bd3f9d bc2990cf
```



```
      output (32 octets):  8169817e9b02ed1e b731b3bcfd656f73
         a674abad0541074c 9c2ce0f1dda661b2

   {server}  derive write traffic keys for application data:

      PRK (32 octets):  d4a9974dc6c15c4b d5e35add69b1a20c
         b78affe36ab431e8 264567a25f89d35b

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  474c6c4d95e3c4a7 c83d2a327573ad7a

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  57ae1cf30df22bd5 cc6c5903

   {server}  derive read traffic keys for handshake data:

      PRK (32 octets):  041ae38c959b6d93 7dba0da43d2b3bc0
         a81da11279935399 5720bc155657934a

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  cacd295502a93689 37e8a8c58962b485

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  692cb0e95a3e2c80 7ac13112

   {client}  extract secret "early":

      salt:  (absent)

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
         10adf300aa1f2660 e1b22e10f170f92a
```

```
{client}  derive secret for handshake "tls13 derived":

   PRK (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
      10adf300aa1f2660 e1b22e10f170f92a

   hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
      27ae41e4649b934c a495991b7852b855
```



```
   info (49 octets):  00200d746c733133 2064657269766564
      20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
      4ca495991b7852b8 55

   output (32 octets):  6f2615a108c702c5 678f54fc9dbab697
      16c076189c48250c ebeac3576c3611ba

{client}  extract secret "handshake":

   salt (32 octets):  6f2615a108c702c5 678f54fc9dbab697
      16c076189c48250c ebeac3576c3611ba

   ikm (32 octets):  5aa03a79c923fa4c 683d9cba739516c4
      c69ad15c0db40b7c 6e21e2ff71f40f06

   secret (32 octets):  e4e77cf10307c913 575026d3d193b181
      f90ee4aa69f53f17 3426d62704623e85

{client}  derive secret "tls13 c hs traffic" (same as server)

{client}  derive secret "tls13 s hs traffic" (same as server)

{client}  derive secret for master "tls13 derived" (same as server)

{client}  extract secret "master" (same as server)

{client}  derive read traffic keys for handshake data:

   PRK (32 octets):  b05eae2a3c213f62 9ff677f9afff5589
      368b1baf54b1bdc6 80f43b4e523f1e3b

   key info (13 octets):  001009746c733133 206b657900
```

```
   key output (16 octets):  1837f9353c2e7a0d 279923526c53aead

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  876dd44a5f0cc952 08425386

{client}  calculate finished "tls13 finished" (same as server)

{client}  derive secret "tls13 c ap traffic" (same as server)

{client}  derive secret "tls13 s ap traffic" (same as server)

{client}  derive secret "tls13 exp master" (same as server)
```



```
{client}  derive write traffic keys for handshake data (same as
   server read traffic keys)

{client}  derive read traffic keys for application data (same as
   server write traffic keys)

{client}  calculate finished "tls13 finished":

   PRK (32 octets):  041ae38c959b6d93 7dba0da43d2b3bc0
      a81da11279935399 5720bc155657934a

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  507651b6fa3d5622 34091e1cdf3c7fba
      bf2f235272831b99 dcc2accc8afb563e

{client}  send a Finished handshake message

{client}  send handshake record:

   payload (36 octets):  14000020c87d6dd1 50b92a473cbff566
      34f50b2ecba977b4 afa29a0fb654a8be 22124aae
```

```
      ciphertext (58 octets):  17030100356d8eca 3665769dee5093cd
         a2cbe4704aa214a9 4e399428cb0d584e 1878ce907f557200
         ac1fd645c5285afa cd7570117b61501c 7586

   {client}  derive write traffic keys for application data:

      PRK (32 octets):  9e0bf6b565b4c386 d3f0a7faaecffac8
         76716d97ef7e1920 9b6a82fbc2e78ab6

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  ac773626f67dfa1b 2bdae44cf89d424f

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  2726987b7549397b 1a8e0363

   {client}  derive secret "tls13 res master":

      PRK (32 octets):  e845be8dbb7556ed 9a4921f663c88cd6
         8387f72e4e2572dc 59f22c5cda035862
```



```
      hash (32 octets):  949f8ad1a8ce89e6 ff48d2dfa9da007f
         3db6820ab1c23d66 0011167a8093751b

      info (52 octets):  002010746c733133 20726573206d6173
         74657220949f8ad1 a8ce89e6ff48d2df a9da007f3db6820a
         b1c23d660011167a 8093751b

      output (32 octets):  692dcd005454d3f6 1313150d8414bc06
         f63fdaaad6e60d4d fcf0ee4350b9fc38

   {server}  calculate finished "tls13 finished" (same as client)

   {server}  derive read traffic keys for application data (same as
      client write traffic keys)

   {server}  derive secret "tls13 res master" (same as client)

   {server}  send a SessionTicket handshake message
```

```
{server}  send handshake record:

   payload (186 octets):  040000b60000001e f1655d5400a299b4
      f88531f21efd8d98 e8ad000000007142 3911a9eb9f743d9b
      e589bc89f05a0060 b46fab142a9b5055 5b729017a7235dc3
      8f9b80550570fce6 34302954540f8537 20d53a1e3eb34357
      e6161c2655fde96d 7bcbb978c074c269 2696124089322d61
      d5747dfd20d4b19d b61193d698283808 1bf8c7fde1740823
      e87e58289843230f 28a9fbe716cb5594 1a5dd7151c873aba
      36ae8cff557bb3f7 d2bfc7f126a25234 0008002a00040000 0400

   ciphertext (208 octets):  17030100cbf400c9 f93f3a2e22b8c810
      0a0ae955290eea5b 8c2288d72ebdb6b1 2a9b4fb321a82c84
      ce6a90ea3008d395 0bb54657d46cae9c e4801ee47f688bf3
      719a02378f7f2ac3 d5c54343da3f6434 3c098094788e3d18
      51e786197f4c5ab7 fb1813b4d920f115 d6a54df4aa108908
      2e5e93a02aefa91f 755fcd8ea6df0362 3fcb0b552ae026fb
      8df11d5adfddbf60 c227be282444447e 6816321cdafcdcd5
      9889b79c9092886b 021893605d9467cf 7c9b24817fe7ddbc
      66380a8cf9be9497 d886e999c571fc18 759ee03b20321a10

{client}  send application_data record:

   payload (50 octets):  0001020304050607 08090a0b0c0d0e0f
      1011121314151617 18191a1b1c1d1e1f 2021222324252627
      28292a2b2c2d2e2f 3031

   ciphertext (72 octets):  17030100434a1777 5d0e717b22921157
      5501be876d5d690b 4b28bd0211495711 bf97d20deaf2e440
```



```
      63a8e4c48ff3cf9d f3b44540bcdc53d5 1c8d4d184081b566
      15d323aa833a407a

{server}  send application_data record:

   payload (50 octets):  0001020304050607 08090a0b0c0d0e0f
      1011121314151617 18191a1b1c1d1e1f 2021222324252627
      28292a2b2c2d2e2f 3031

   ciphertext (72 octets):  1703010043ef6eb6 0c6fc258b170589e
      9a1cbefba4c52d79 15a3afb3e52da65f ef6b1dc37970a3ab
```

```
      79d5e3a513678ae5 b2bfdb2880d60f08 280f4f2ebf94c3d7
      1ce803e6a9295686

{client}  send alert record:

   payload (2 octets):  0100

   ciphertext (24 octets):  17030100134b8329 8e645242f1bf8265
      bcd6f42b795de36d

{server}  send alert record:

   payload (2 octets):  0100

   ciphertext (24 octets):  17030100133d38b5 673386ae3d722ccd
      d2996292b5a12165
```

4. Resumed 0-RTT Handshake

This handshake resumes from the handshake in Section 3. Since the server provided a session ticket that permitted 0-RTT, and the client is configured for 0-RTT, the client is able to send 0-RTT data.

```
{client}  create an ephemeral x25519 key pair:

   private key (32 octets):  ecd667eb15e77201 1a8522a5e9a90a5f
      1b4080c508baca79 68f8831d0d10811f

   public key (32 octets):  edb6949f0f6c1e2e 47001f5ea2c7d54b
      d8ec7167b52cfd1a 29dfbe5f5888cd29

{client}  extract secret "early":

   salt:  (absent)

   ikm (32 octets):  692dcd005454d3f6 1313150d8414bc06
      f63fdaaad6e60d4d fcf0ee4350b9fc38
```



```
      secret (32 octets):  bc9ef911288790a9 9e5ca2ea520d231e
      c60a28e1e958e1c6 551dbbe0bedfe63b

{client}  send a ClientHello handshake message
```

```
{client}  calculate finished "tls13 finished":

   PRK (32 octets):  7688634eb081913f 83cc5c987d302235
      c6fbc79efcd8094b 02ce1030a5f9184b

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  eb21444eb694b6ad 592708e27a9177a9
      96aa9bf9f3c786d8 e88e18a293338a48

{client}  send handshake record:

   payload (512 octets):  010001fc03032089 2088de8aa414b2bf
      0237acf603f9b20b 532df97f894fc82c aeac2e1a899f0000
      3e130113031302c0 2bc02fcca9cca8c0 0ac009c013c023c0
      27c014009eccaa00 3300320067003900 38006b0016001300
      9c002f003c003500 3d000a0005000401 0001950000000b00
      0900000673657276 6572ff0100010000 0a00140012001d00
      1700180019010001 0101020103010400 0b00020100002800
      260024001d0020ed b6949f0f6c1e2e47 001f5ea2c7d54bd8
      ec7167b52cfd1a29 dfbe5f5888cd2900 2a0000002b000706
      7f1403030302000d 0020001e04030503 0603020308040805
      0806040105010601 0201040205020602 0202002d00020101
      0015002b00000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      2900cd00a800a299 b4f88531f21efd8d 98e8ad0000000071
      423911a9eb9f743d 9be589bc89f05a00 60b46fab142a9b50
      555b729017a7235d c38f9b80550570fc e634302954540f85
      3720d53a1e3eb343 57e6161c2655fde9 6d7bcbb978c074c2
      692696124089322d 61d5747dfd20d4b1 9db61193d6982838
      081bf8c7fde17408 23e87e5828984323 0f28a9fbe716cb55
      941a5dd7151c873a ba36ae8cff557bb3 f7d2bfc7f126a252
      34f1655d5a002120 ce6d44ae651c47df 33882f31a7542f19
      cab76d4be58175d6 505f2fae5c1ec390

   ciphertext (517 octets):  1603010200010001 fc030320892088de
      8aa414b2bf0237ac f603f9b20b532df9 7f894fc82caeac2e
      1a899f00003e1301 13031302c02bc02f cca9cca8c00ac009
      c013c023c027c014 009eccaa00330032 006700390038006b
      00160013009c002f 003c0035003d000a 0005000401000195
      0000000b00090000 06736572766572ff 01000100000a0014
```

```
      0012001d00170018 0019010001010102 01030104000b0002
      0100002800260024 001d0020edb6949f 0f6c1e2e47001f5e
      a2c7d54bd8ec7167 b52cfd1a29dfbe5f 5888cd29002a0000
      002b0007067f1403 030302000d002000 1e04030503060302
      0308040805080604 0105010601020104 0205020602020200
      2d00020101001500 2b00000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      00000000002900cd 00a800a299b4f885 31f21efd8d98e8ad
      0000000071423911 a9eb9f743d9be589 bc89f05a0060b46f
      ab142a9b50555b72 9017a7235dc38f9b 80550570fce63430
      2954540f853720d5 3a1e3eb34357e616 1c2655fde96d7bcb
      b978c074c2692696 124089322d61d574 7dfd20d4b19db611
      93d6982838081bf8 c7fde1740823e87e 58289843230f28a9
      fbe716cb55941a5d d7151c873aba36ae 8cff557bb3f7d2bf
      c7f126a25234f165 5d5a002120ce6d44 ae651c47df33882f
      31a7542f19cab76d 4be58175d6505f2f ae5c1ec390
```

{client} derive secret "tls13 c e traffic":

PRK (32 octets): bc9ef911288790a9 9e5ca2ea520d231e
c60a28e1e958e1c6 551dbbe0bedfe63b

hash (32 octets): 39ce46d03e297f31 b63f1504b052e330
2f20f7a289b6b9ce 19f2f42172c9446f

info (53 octets): 002011746c733133 2063206520747261
666669632039ce46 d03e297f31b63f15 04b052e3302f20f7
a289b6b9ce19f2f4 2172c9446f

output (32 octets): 53480f2ff5f8966c 7819a2f4d861b3f7
15bbe2c21c0c6273 6a00526d8de55837

{client} derive write traffic keys for early application data:

PRK (32 octets): 53480f2ff5f8966c 7819a2f4d861b3f7
15bbe2c21c0c6273 6a00526d8de55837

key info (13 octets): 001009746c733133 206b657900

key output (16 octets): a29e150bd59e2b81 5c968627498f96c2

iv info (12 octets): 000c08746c733133 20697600

iv output (12 octets): d96cd2f516516ad1 1a70abb6

{client} send application_data record:

ciphertext (28 octets): 1703010017fb2460 727da934b3a6058f
c3a4acb6ce74f0a0 8ef7f847

{server} extract secret "early" (same as client)

{server} calculate finished "tls13 finished" (same as client)

{server} create an ephemeral x25519 key pair:

private key (32 octets): 959df6054b219c94 dd0066ffd786a9da
86871b99a55b58a7 435ce3a22a3f929d

public key (32 octets): df70bd1d47959b2a dfd4b4cc6a62ce45
a02e45106ef974c6 ccf49720920b0a4a

{server} derive secret "tls13 c e traffic" (same as client)

{server} send a ServerHello handshake message

{server} derive secret for handshake "tls13 derived":

PRK (32 octets): bc9ef911288790a9 9e5ca2ea520d231e
c60a28e1e958e1c6 551dbbe0bedfe63b

hash (32 octets): e3b0c44298fc1c14 9afbf4c8996fb924
27ae41e4649b934c a495991b7852b855

info (49 octets): 00200d746c733133 2064657269766564
20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
4ca495991b7852b8 55

output (32 octets): 1d86e68a77be72ef ffa5684961146be3
d09a83eed9e29c08 0f94cdde489b2e66

{server} extract secret "handshake":

salt (32 octets): 1d86e68a77be72ef ffa5684961146be3
d09a83eed9e29c08 0f94cdde489b2e66

ikm (32 octets): df9b4a07733c5460 fc088eb1db60f6eb

```
      6a0c67080e3c842e eaa0021cdd860e26

   secret (32 octets):  79975c2bb824f1ec 93b582e0f5bf7030
      2a2f9d81bd477d8b c52cf4d669d5392a

{server}  derive secret "tls13 c hs traffic":
```



```
   PRK (32 octets):  79975c2bb824f1ec 93b582e0f5bf7030
      2a2f9d81bd477d8b c52cf4d669d5392a

   hash (32 octets):  d4999a597a672010 646addfdf8a3583b
      ff3b1217c0c04894 c680910bbd02b86a

   info (54 octets):  002012746c733133 2063206873207472
      616666696320d499 9a597a672010646a ddfdf8a3583bff3b
      1217c0c04894c680 910bbd02b86a

   output (32 octets):  e553af85fd9769a9 d3467db9b5b29797
      7526f2f1b9cc25c1 c265093353dbceed

{server}  derive secret "tls13 s hs traffic":

   PRK (32 octets):  79975c2bb824f1ec 93b582e0f5bf7030
      2a2f9d81bd477d8b c52cf4d669d5392a

   hash (32 octets):  d4999a597a672010 646addfdf8a3583b
      ff3b1217c0c04894 c680910bbd02b86a

   info (54 octets):  002012746c733133 2073206873207472
      616666696320d499 9a597a672010646a ddfdf8a3583bff3b
      1217c0c04894c680 910bbd02b86a

   output (32 octets):  a98f17d9d9d01b97 a8a9fcfe1aa80cf2
      f0efaf4448bab35c 025d0d3658ef495d

{server}  derive secret for master "tls13 derived":

   PRK (32 octets):  79975c2bb824f1ec 93b582e0f5bf7030
      2a2f9d81bd477d8b c52cf4d669d5392a
```

```
      hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
         27ae41e4649b934c a495991b7852b855

      info (49 octets):  00200d746c733133 2064657269766564
         20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
         4ca495991b7852b8 55

      output (32 octets):  fbe525046f48f930 eac2f07f1d4c94cf
         76aa0844f5e5874e f6512dccc7e5164f

   {server}  extract secret "master":

      salt (32 octets):  fbe525046f48f930 eac2f07f1d4c94cf
         76aa0844f5e5874e f6512dccc7e5164f
```



```
      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  53850ec90133d5cd 448fa5200e7683b1
         19236c0fe93dc8b6 cad87f9ffee80f67

   {server}  send handshake record:

      payload (88 octets):  020000547f147535 eed9d16cb9437c49
         bed2329972bacd25 bb6708cef33db49b c96bd1b09cb31301
         002e002900020000 00280024001d0020 df70bd1d47959b2a
         dfd4b4cc6a62ce45 a02e45106ef974c6 ccf49720920b0a4a

      ciphertext (93 octets):  1603010058020000 547f147535eed9d1
         6cb9437c49bed232 9972bacd25bb6708 cef33db49bc96bd1
         b09cb31301002e00 2900020000002800 24001d0020df70bd
         1d47959b2adfd4b4 cc6a62ce45a02e45 106ef974c6ccf497 20920b0a4a

   {server}  derive write traffic keys for handshake data:

      PRK (32 octets):  a98f17d9d9d01b97 a8a9fcfe1aa80cf2
         f0efaf4448bab35c 025d0d3658ef495d

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  46de8022452f1a01 dae81c9c14282ab6
```

```
   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  2d1a4735b9701a76 e6ea43a4

{server}  send a EncryptedExtensions handshake message

{server}  calculate finished "tls13 finished":

   PRK (32 octets):  a98f17d9d9d01b97 a8a9fcfe1aa80cf2
      f0efaf4448bab35c 025d0d3658ef495d

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  50c8ac03c17b913f 6d3e5a1d9f884eaa
      6a01596674c96228 8b82a3becb43c8c3

{server}  send a Finished handshake message

{server}  send handshake record:
```



```
   payload (74 octets):  080000220020000a 00140012001d0017
      0018001901000101 0102010301040000 0000002a00001400
      00202f15bde7b069 12686d1dd4e09752 6119fab819f31004
      23cd33cab05d579a aeb8

   ciphertext (96 octets):  170301005b19e0b8 d03449cf5ad5a4a8
      b678b4cff2810a0d 3fb6f4573a3e95df 546560e8edb94ef6
      6ad0ad7757cf572f 60898e54020eed36 8b8024e313750873
      b7df20af09b3dd72 06da50583e126217 d3e0ad6c7bcef09f
      cc70e1f967014842

{server}  derive secret "tls13 c ap traffic":

   PRK (32 octets):  53850ec90133d5cd 448fa5200e7683b1
      19236c0fe93dc8b6 cad87f9ffee80f67

   hash (32 octets):  c6cf7192a7fd5f7c dd0a659ac9f46320
      8fc1bc089670fa8d de33a5ae2135c063
```

```
      info (54 octets):  002012746c733133 2063206170207472
         616666696320c6cf 7192a7fd5f7cdd0a 659ac9f463208fc1
         bc089670fa8dde33 a5ae2135c063

      output (32 octets):  1053e7b2069c9d9b c6cf82f8deac40ec
         927bbb9fd5ad49fe ae1ff4278e2a0031

   {server}  derive secret "tls13 s ap traffic":

      PRK (32 octets):  53850ec90133d5cd 448fa5200e7683b1
         19236c0fe93dc8b6 cad87f9ffee80f67

      hash (32 octets):  c6cf7192a7fd5f7c dd0a659ac9f46320
         8fc1bc089670fa8d de33a5ae2135c063

      info (54 octets):  002012746c733133 2073206170207472
         616666696320c6cf 7192a7fd5f7cdd0a 659ac9f463208fc1
         bc089670fa8dde33 a5ae2135c063

      output (32 octets):  117f89a3ba4efc76 5b2b940c62a31f06
         304cb3877d117131 1edeab60a6abc91f

   {server}  derive secret "tls13 exp master":

      PRK (32 octets):  53850ec90133d5cd 448fa5200e7683b1
         19236c0fe93dc8b6 cad87f9ffee80f67

      hash (32 octets):  c6cf7192a7fd5f7c dd0a659ac9f46320
         8fc1bc089670fa8d de33a5ae2135c063
```



```
      info (52 octets):  002010746c733133 20657870206d6173
         74657220c6cf7192 a7fd5f7cdd0a659a c9f463208fc1bc08
         9670fa8dde33a5ae 2135c063

      output (32 octets):  882fb13091b8f95e 5c65aa3d807e4323
         64731f93c69018ae c054ec387f27982c

   {server}  derive write traffic keys for application data:

      PRK (32 octets):  117f89a3ba4efc76 5b2b940c62a31f06
         304cb3877d117131 1edeab60a6abc91f
```

```
      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  40dd3fc22423a700 776b1cce944e7aa3

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  4b49f66dd01682ea 569164a7

   {server}  derive read traffic keys for early application data (same
      as client write traffic keys)

   {client}  derive secret for handshake "tls13 derived":

      PRK (32 octets):  bc9ef911288790a9 9e5ca2ea520d231e
         c60a28e1e958e1c6 551dbbe0bedfe63b

      hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
         27ae41e4649b934c a495991b7852b855

      info (49 octets):  00200d746c733133 2064657269766564
         20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
         4ca495991b7852b8 55

      output (32 octets):  1d86e68a77be72ef ffa5684961146be3
         d09a83eed9e29c08 0f94cdde489b2e66

   {client}  extract secret "handshake":

      salt (32 octets):  1d86e68a77be72ef ffa5684961146be3
         d09a83eed9e29c08 0f94cdde489b2e66

      ikm (32 octets):  df9b4a07733c5460 fc088eb1db60f6eb
         6a0c67080e3c842e eaa0021cdd860e26

      secret (32 octets):  79975c2bb824f1ec 93b582e0f5bf7030
         2a2f9d81bd477d8b c52cf4d669d5392a
```



```
   {client}  derive secret "tls13 c hs traffic" (same as server)

   {client}  derive secret "tls13 s hs traffic" (same as server)

   {client}  derive secret for master "tls13 derived" (same as server)
```

```
{client}  extract secret "master" (same as server)

{client}  derive read traffic keys for handshake data:

   PRK (32 octets):  a98f17d9d9d01b97 a8a9fcfe1aa80cf2
      f0efaf4448bab35c 025d0d3658ef495d

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  46de8022452f1a01 dae81c9c14282ab6

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  2d1a4735b9701a76 e6ea43a4

{client}  calculate finished "tls13 finished" (same as server)

{client}  derive secret "tls13 c ap traffic" (same as server)

{client}  derive secret "tls13 s ap traffic" (same as server)

{client}  derive secret "tls13 exp master" (same as server)

{client}  send a EndOfEarlyData handshake message

{client}  send handshake record:

   payload (4 octets):  05000000

   ciphertext (26 octets):  17030100155d2a07 204498a910fd60e4
      6eb384049ec93d62 b12c

{client}  derive write traffic keys for handshake data:

   PRK (32 octets):  e553af85fd9769a9 d3467db9b5b29797
      7526f2f1b9cc25c1 c265093353dbceed

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  867143c4068df3a5 ae6b12a486b9b847

   iv info (12 octets):  000c08746c733133 20697600
```

```
   iv output (12 octets):  5e04c80f859988e7 c102c719

{client}  derive read traffic keys for application data (same as
   server write traffic keys)

{client}  calculate finished "tls13 finished":

   PRK (32 octets):  e553af85fd9769a9 d3467db9b5b29797
      7526f2f1b9cc25c1 c265093353dbceed

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  17c916392da3bfd7 1448ad824b4ec15e
      062a7da6925fd07e 9e3ed647a38555ed

{client}  send a Finished handshake message

{client}  send handshake record:

   payload (36 octets):  1400002064283341 14b550e38e4b03ef
      e0fba441c3e73804 76bae41722a0ab8e be0f8b67

   ciphertext (58 octets):  17030100351f82bd 499964e8f8b70cb4
      85cc0dd0efe07561 887202f33db44327 3d667fe7d1a48cb2
      7502638cf4fc2b99 bc7efa1f1e33d210 186d

{client}  derive write traffic keys for application data:

   PRK (32 octets):  1053e7b2069c9d9b c6cf82f8deac40ec
      927bbb9fd5ad49fe ae1ff4278e2a0031

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  38c79b0728fa3451 774f093adac1dd04

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  a3d605be250cfd5d 209615ee

{client}  derive secret "tls13 res master":

   PRK (32 octets):  53850ec90133d5cd 448fa5200e7683b1
      19236c0fe93dc8b6 cad87f9ffee80f67

   hash (32 octets):  2233547d4b607f2b 5f516e0f29f467d9
      88e805512434d38a 87154d47488b72b4
```

```
      info (52 octets):  002010746c733133 20726573206d6173
         746572202233547d 4b607f2b5f516e0f 29f467d988e80551
         2434d38a87154d47 488b72b4

      output (32 octets):  91eeb3e2bb46fcf6 810ec7bff5c1d905
         22d1cc1b196e3ef4 a72f6f6bd86f5aae

   {server}  derive read traffic keys for handshake data:

      PRK (32 octets):  e553af85fd9769a9 d3467db9b5b29797
         7526f2f1b9cc25c1 c265093353dbceed

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  867143c4068df3a5 ae6b12a486b9b847

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  5e04c80f859988e7 c102c719

   {server}  calculate finished "tls13 finished" (same as client)

   {server}  derive read traffic keys for application data (same as
      client write traffic keys)

   {server}  derive secret "tls13 res master" (same as client)

   {client}  send application_data record:

      payload (50 octets):  0001020304050607 08090a0b0c0d0e0f
         1011121314151617 18191a1b1c1d1e1f 2021222324252627
         28292a2b2c2d2e2f 3031

      ciphertext (72 octets):  1703010043108855 d836d933a3b33e5e
         3bcccfe9ebbb75ad 3d4ee46f02063528 384adfec59cede3b
         13d5dd68442833ef 1c13014af62d56e3 c9661c0eb0ef4fdc
         e7808b45f077ca2b

   {server}  send application_data record:

      payload (50 octets):  0001020304050607 08090a0b0c0d0e0f
         1011121314151617 18191a1b1c1d1e1f 2021222324252627
```

```
      28292a2b2c2d2e2f 3031

   ciphertext (72 octets):  1703010043c23be9 5ad85b168bd2e206
      cd17b2b598f67cdf 558992521a6ed4ec eeff45ec22a93675
      1bd733fc63e3a98d 092dcd93ec848c08 afdfda839f524e2e
      69b474197cae81cb
```



```
{client}  send alert record:

   payload (2 octets):  0100

   ciphertext (24 octets):  1703010013c4f33d 08ac5ad28a35c0b3
      2559bf45718f9bc7

{server}  send alert record:

   payload (2 octets):  0100

   ciphertext (24 octets):  17030100139f73be 8cc18eb517547f85
      26b1219f757cdc2d
```

5. HelloRetryRequest

In this example, the client initiates a handshake with an X25519 [RFC7748] share. The server however prefers P-256 [FIPS186] and sends a HelloRetryRequest that requires the client to generate a key share on the P-256 curve.

```
{client}  create an ephemeral x25519 key pair:

   private key (32 octets):  68f119d51cf43e70 b7bc4080d5911317
      b22482211908f4a0 7cd3ee6148f05a65

   public key (32 octets):  fff63faea1e4f9b0 8ae2fc158749f72a
      b274015b21903399 434279416a1c3866

{client}  send a ClientHello handshake message

{client}  send handshake record:

   payload (174 octets):  010000aa03032b47 3d43b9e45db4ff9f
      9ae53f63f495bc90 a308136caa6570cd 6a3d682e23fc0000
```

```
      0613011303130201 00007b0000000b00 0900000673657276
      6572ff0100010000 0a00080006001d00 1700180028002600
      24001d0020fff63f aea1e4f9b08ae2fc 158749f72ab27401
      5b21903399434279 416a1c3866002b00 03027f14000d0020
      001e040305030603 0203080408050806 0401050106010201
      0402050206020202 002d00020101

   ciphertext (179 octets):  16030100ae010000 aa03032b473d43b9
      e45db4ff9f9ae53f 63f495bc90a30813 6caa6570cd6a3d68
      2e23fc0000061301 130313020100007b 0000000b00090000
      06736572766572ff 01000100000a0008 0006001d00170018
      002800260024001d 0020fff63faea1e4 f9b08ae2fc158749
      f72ab274015b2190 3399434279416a1c 3866002b0003027f
```



```
      14000d0020001e04 0305030603020308 0408050806040105
      0106010201040205 0206020202002d00 020101

   {server}  send a HelloRetryRequest handshake message

   {server}  send handshake record:

      payload (16 octets):  0600000c7f141301 0006002800020017

      ciphertext (21 octets):  1603010010060000 0c7f141301000600
         2800020017

   {client}  create an ephemeral P-256 key pair:

      private key (32 octets):  686029ea60fdbf90 952a205f36867184
         21d39ccb83e1332e 6449da8f62a455f7

      public key (65 octets):  0439a9c0e3dea88c 76323ea8a30a779f
         caa782d88935df99 ca2f94f386227247 066af9a46ebc7f88
         6f1d8e81a08779f2 6c5420c69609a68a 6762b91329670b5d e1

   {client}  send a ClientHello handshake message

   {client}  send handshake record:

      payload (207 octets):  010000cb03032b47 3d43b9e45db4ff9f
         9ae53f63f495bc90 a308136caa6570cd 6a3d682e23fc0000
         0613011303130201 00009c0000000b00 0900000673657276
```

```
      6572ff0100010000 0a00080006001d00 1700180028004700
      450017004104 39a9c0e3dea88c76323ea8a30a779fcaa782
      d88935df99ca2f94 f386227247066af9a46ebc7f886f1d8e
      81a08779f26c5420 c69609a68a6762b9 1329670b5de1002b
      0003027f14000d00 20001e0403050306 0302030804080508
      0604010501060102 0104020502060202 02002d00020101

   ciphertext (212 octets):  16030100cf010000 cb03032b473d43b9
      e45db4ff9f9ae53f 63f495bc90a30813 6caa6570cd6a3d68
      2e23fc0000061301 130313020100009c 0000000b00090000
      06736572766572ff 01000100000a0008 0006001d00170018
      0028004700450017 00410439a9c0e3de a88c76323ea8a30a
      779fcaa782d88935 df99ca2f94f38622 7247066af9a46ebc
      7f886f1d8e81a087 79f26c5420c69609 a68a6762b9132967
      0b5de1002b000302 7f14000d0020001e 0403050306030203
      0804080508060401 0501060102010402 050206020202002d 00020101

{server}  extract secret "early":

   salt:  (absent)
```



```
   ikm (32 octets):  0000000000000000 0000000000000000
      0000000000000000 0000000000000000

   secret (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
      10adf300aa1f2660 e1b22e10f170f92a

{server}  create an ephemeral P-256 key pair:

   private key (32 octets):  cf5cb678b37d617e 4e3b978d52758db3
      5bee4147c5a4c48d f62ec7f3e26b7b0d

   public key (65 octets):  0438bafba512d58e 57a62ceaee1c0c3e
      5678082cacf126d3 dac009720572d79f 341f7098b24fb7f1
      b8ee222d6433f310 e8862c8b9f2c9337 fe6eb1a54665d465 3b

{server}  send a ServerHello handshake message

{server}  derive secret for handshake "tls13 derived":

   PRK (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
      10adf300aa1f2660 e1b22e10f170f92a
```

```
      hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
         27ae41e4649b934c a495991b7852b855

      info (49 octets):  00200d746c733133 2064657269766564
         20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
         4ca495991b7852b8 55

      output (32 octets):  6f2615a108c702c5 678f54fc9dbab697
         16c076189c48250c ebeac3576c3611ba

   {server}  extract secret "handshake":

      salt (32 octets):  6f2615a108c702c5 678f54fc9dbab697
         16c076189c48250c ebeac3576c3611ba

      ikm (32 octets):  df4cde9bf625ee9b e21cc6bd4a51f662
         00c857b0b104cb68 7731c3851eefbc9a

      secret (32 octets):  61ebb724b8eaa8d4 83de05c018a83947
         b5c2a866847154ce 2b2e33fce8e538cf

   {server}  derive secret "tls13 c hs traffic":

      PRK (32 octets):  61ebb724b8eaa8d4 83de05c018a83947
         b5c2a866847154ce 2b2e33fce8e538cf
```



```
      hash (32 octets):  dad1f7541198d854 97203f23e9856b9a
         97937e6a2d22f3c0 1e22be12bee0ee56

      info (54 octets):  002012746c733133 2063206873207472
         616666696320dad1 f7541198d8549720 3f23e9856b9a9793
         7e6a2d22f3c01e22 be12bee0ee56

      output (32 octets):  f52e0805a26cd615 ec012fd6b1950258
         a9aae77b336a8cac a443df877e99ec61

   {server}  derive secret "tls13 s hs traffic":

      PRK (32 octets):  61ebb724b8eaa8d4 83de05c018a83947
         b5c2a866847154ce 2b2e33fce8e538cf
```

```
      hash (32 octets):  dad1f7541198d854 97203f23e9856b9a
         97937e6a2d22f3c0 1e22be12bee0ee56

      info (54 octets):  002012746c733133 2073206873207472
         616666696320dad1 f7541198d8549720 3f23e9856b9a9793
         7e6a2d22f3c01e22 be12bee0ee56

      output (32 octets):  ed0ea7ec428dd7bb 3f89df21b4679286
         fb19f61c5fe0ef81 35c0f54d687bc50c

   {server}  derive secret for master "tls13 derived":

      PRK (32 octets):  61ebb724b8eaa8d4 83de05c018a83947
         b5c2a866847154ce 2b2e33fce8e538cf

      hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
         27ae41e4649b934c a495991b7852b855

      info (49 octets):  00200d746c733133 2064657269766564
         20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
         4ca495991b7852b8 55

      output (32 octets):  3f0c9f13e5dd95f7 27c7bf2c82b4f75f
         91e26cf5e1f89ae5 36becd5b48f08357

   {server}  extract secret "master":

      salt (32 octets):  3f0c9f13e5dd95f7 27c7bf2c82b4f75f
         91e26cf5e1f89ae5 36becd5b48f08357

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000
```



```
      secret (32 octets):  23bdfa8bb085b65a 8095c55a79f20ab0
         7646d7bac8c67803 2aa5985df2a1b7c1

   {server}  send handshake record:

      payload (115 octets):  0200006f7f1439d0 5400265319e5a369
         3e2a5479b46a5e8c 10a12daa5d01cdc0 cb21730536d51301
```

```
      0049002800450017 00410438bafba512 d58e57a62ceaee1c
      0c3e5678082cacf1 26d3dac009720572 d79f341f7098b24f
      b7f1b8ee222d6433 f310e8862c8b9f2c 9337fe6eb1a54665 d4653b

   ciphertext (120 octets):  1603010073020000 6f7f1439d0540026
      5319e5a3693e2a54 79b46a5e8c10a12d aa5d01cdc0cb2173
      0536d51301004900 2800450017004104 38bafba512d58e57
      a62ceaee1c0c3e56 78082cacf126d3da c009720572d79f34
      1f7098b24fb7f1b8 ee222d6433f310e8 862c8b9f2c9337fe
      6eb1a54665d4653b

{server}  derive write traffic keys for handshake data:

   PRK (32 octets):  ed0ea7ec428dd7bb 3f89df21b4679286
      fb19f61c5fe0ef81 35c0f54d687bc50c

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  ea3b74f7e0223840 dc5fbc1d3864b73b

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  97621bb779bba789 402021f6

{server}  send a EncryptedExtensions handshake message

{server}  send a Certificate handshake message

{server}  send a CertificateVerify handshake message

{server}  calculate finished "tls13 finished":

   PRK (32 octets):  ed0ea7ec428dd7bb 3f89df21b4679286
      fb19f61c5fe0ef81 35c0f54d687bc50c

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  03c5ee66699c919c db206db4053b9314
      f56449f899baead8 c0d82b63fefaa19b
```

```
{server}  send a Finished handshake message

{server}  send handshake record:

   payload (639 octets):  080000120010000a 0008000600170018
      001d000000000b00 01b9000001b50001 b0308201ac308201
      15a0030201020201 02300d06092a8648 86f70d01010b0500
      300e310c300a0603 5504031303727361 301e170d31363037
      3330303132333539 5a170d3236303733 303031323335395a
      300e310c300a0603 5504031303727361 30819f300d06092a
      864886f70d010101 050003818d003081 8902818100b4bb49
      8f8279303d980836 399b36c6988c0c68 de55e1bdb826d390
      1a2461eafd2de49a 91d015abbc9a9513 7ace6c1af19eaa6a
      f98c7ced43120998 e187a80ee0ccb052 4b1b018c3e0b6326
      4d449a6d38e22a5f da43084674803053 0ef0461c8ca9d9ef
      bfae8ea6d1d03e2b d193eff0ab9a8002 c47428a6d35a8d88
      d79f7f1e3f020301 0001a31a30183009 0603551d13040230
      00300b0603551d0f 0404030205a0300d 06092a864886f70d
      01010b0500038181 0085aad2a0e5b927 6b908c65f73a7267
      170618a54c5f8a7b 337d2df7a5943654 17f2eae8f8a58c8f
      8172f9319cf36b7f d6c55b80f21a0301 5156726096fd335e
      5e67f2dbf102702e 608ccae6bec1fc63 a42a99be5c3eb710
      7c3c54e9b9eb2bd5 203b1c3b84e0a8b2 f759409ba3eac9d9
      1d402dcc0cc8f896 1229ac9187b42b4d e100000f00008408
      0400806f43289ae7 efa4a473bedf613e 4e92e9554fb2871a
      df28b8612b27998c be8e8690f4c81b8a cb3fb981396962e0
      7a506b790cb6cb07 1caeb49acc217f39 058d7375cf9d2174
      a8fa29ba60dc35ef 7a43827278489428 2c75d4750400532e
      069fafa01577b431 bbf764f4be901643 07a30b59081c286b
      18ba58649637d676 d5cee614000020bc 521faec41d6c9d2d
      e9f0de7887121fb7 e7a6000a82caa148 565ab19e0aef8f

   ciphertext (661 octets):  1703010290b02e90 0efe58c26b437b75
      4cb31ff7e592e595 405b265fa8c3f2bd 6b9a168fbaf70940
      91d27872271925ac b0e8d878f17a60ea c39a6b233bcbb2f4
      9f6774b77c11827e e77798976db2b76b c236a8cae6751c0b
      498402f364d0118c d21483365d82a82e df95f3bcf5a2a0ed
      3941ef0be0619fbc 2a4489c241f2fc75 3381cf064813ca4e
      dec9bd213c29f4cd 5c3d7b52bc34ef9d 6d3db2e3ce370414
      d9e87c18e7190448 8dd0d7cd359fcb2d ee00aba5283c2dd4
      31afa8e17bf25643 00fbc24f11ae9fb6 6c4cec5f38b03e10
      fbb510b4f3a716e8 4e395128b526aa00 24425fec5e0d9072
      b42fdabfa93686bb 0036963bf3d6d122 fb205fb024c41422
      7e2f054787af00aa b17b78ad2d5c31c1 5812c0420b0ea344
      2f3f5197533e9325 082f44434e502d4e fb73c5987fd3ee55
      228c92bd600e1f81 22a447caba8f2fd2 fbf49d43f99a441d
      2695809c89dc1c89 9c7975b8a78ec2a9 8399922e58d538f8
      009bc07b50573da6 1bbe41ef1f251ee9 dcca0e2d9e8c20fb
```

```
      c3659b8eef131094 cc9effc3697ac767 248616db9576ccb1
      b937775cd97aeb81 f015dcc4bc53143f 0337e90ad800f7cc
      6c09b23352acbf06 59c1d0ac6a145342 9d288a83f2c16ecd
      419abf7bcfeb05df b70292296847cd7d d91d305ec162436b
      6e645028a3d9c068 1cd118093c9a9978 08585fc3ddecab33
      fff96c099b607516 4db17fb609747daf c511dcfe212c49e3
      399c74fe7d36b962 5206204cf411e42c 6b5da8c5cc7d522d
      c8a7747f4cd08e50 a180ed43d8ac0a4c cbc93207e1bd667f
      e2f784eeeb5be6cc 22ffd75c2d134a02 7618bf3f270c4809
      58c2016507f7f825 dc7a116f7f06670b 8c926c47a919b4ec
      f8eab3c0451be841 e90a55e9ce7fee05 919525b0042e4943
      4c70e792e055a6a6 50d69a4c9697bde8 0d8d004b41

{server}  derive secret "tls13 c ap traffic":

   PRK (32 octets):  23bdfa8bb085b65a 8095c55a79f20ab0
      7646d7bac8c67803 2aa5985df2a1b7c1

   hash (32 octets):  d35385d7ef5cda3f e72850e6b878c915
      e603150fe9dd009a 83ebf3e8b73525dc

   info (54 octets):  002012746c733133 2063206170207472
      616666696320d353 85d7ef5cda3fe728 50e6b878c915e603
      150fe9dd009a83eb f3e8b73525dc

   output (32 octets):  3e97f6ece946f6cf a25aac0c4294f752
      adf68ce3769ba8f1 a72140e960e00b75

{server}  derive secret "tls13 s ap traffic":

   PRK (32 octets):  23bdfa8bb085b65a 8095c55a79f20ab0
      7646d7bac8c67803 2aa5985df2a1b7c1

   hash (32 octets):  d35385d7ef5cda3f e72850e6b878c915
      e603150fe9dd009a 83ebf3e8b73525dc

   info (54 octets):  002012746c733133 2073206170207472
      616666696320d353 85d7ef5cda3fe728 50e6b878c915e603
      150fe9dd009a83eb f3e8b73525dc

   output (32 octets):  9bf644ffdb8feb85 11240075595cb94f
      411a5682e3cb4a82 f0b1f7daf0322a92
```

{server} derive secret "tls13 exp master":

PRK (32 octets): 23bdfa8bb085b65a 8095c55a79f20ab0
7646d7bac8c67803 2aa5985df2a1b7c1

hash (32 octets): d35385d7ef5cda3f e72850e6b878c915
e603150fe9dd009a 83ebf3e8b73525dc

info (52 octets): 002010746c733133 20657870206d6173
74657220d35385d7 ef5cda3fe72850e6 b878c915e603150f
e9dd009a83ebf3e8 b73525dc

output (32 octets): c8dd1dcfbb99ea14 e3ad390c6a4cd3e0
c4f20c2221aa33e2 68eb807de344a179

{server} derive write traffic keys for application data:

PRK (32 octets): 9bf644ffdb8feb85 11240075595cb94f
411a5682e3cb4a82 f0b1f7daf0322a92

key info (13 octets): 001009746c733133 206b657900

key output (16 octets): d46da4e755ba9e74 7a46246bda64c866

iv info (12 octets): 000c08746c733133 20697600

iv output (12 octets): 73deb5c4dfcc38ff 19bb9943

{server} derive read traffic keys for handshake data:

PRK (32 octets): f52e0805a26cd615 ec012fd6b1950258
a9aae77b336a8cac a443df877e99ec61

key info (13 octets): 001009746c733133 206b657900

key output (16 octets): f34edc87549aca05 6bf5d3ebbfb58934

iv info (12 octets): 000c08746c733133 20697600

iv output (12 octets): 018f4bc56b7fa73b 50a1b497

```
{client}  extract secret "early":

   salt:  (absent)

   ikm (32 octets):  0000000000000000 0000000000000000
      0000000000000000 0000000000000000

   secret (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
      10adf300aa1f2660 e1b22e10f170f92a

{client}  derive secret for handshake "tls13 derived":
```



```
   PRK (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
      10adf300aa1f2660 e1b22e10f170f92a

   hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
      27ae41e4649b934c a495991b7852b855

   info (49 octets):  00200d746c733133 2064657269766564
      20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
      4ca495991b7852b8 55

   output (32 octets):  6f2615a108c702c5 678f54fc9dbab697
      16c076189c48250c ebeac3576c3611ba

{client}  extract secret "handshake":

   salt (32 octets):  6f2615a108c702c5 678f54fc9dbab697
      16c076189c48250c ebeac3576c3611ba

   ikm (32 octets):  df4cde9bf625ee9b e21cc6bd4a51f662
      00c857b0b104cb68 7731c3851eefbc9a

   secret (32 octets):  61ebb724b8eaa8d4 83de05c018a83947
      b5c2a866847154ce 2b2e33fce8e538cf

{client}  derive secret "tls13 c hs traffic" (same as server)

{client}  derive secret "tls13 s hs traffic" (same as server)

{client}  derive secret for master "tls13 derived" (same as server)
```

{client} extract secret "master" (same as server)

{client} derive read traffic keys for handshake data:

PRK (32 octets): ed0ea7ec428dd7bb 3f89df21b4679286
fb19f61c5fe0ef81 35c0f54d687bc50c

key info (13 octets): 001009746c733133 206b657900

key output (16 octets): ea3b74f7e0223840 dc5fbc1d3864b73b

iv info (12 octets): 000c08746c733133 20697600

iv output (12 octets): 97621bb779bba789 402021f6

{client} calculate finished "tls13 finished" (same as server)

{client} derive secret "tls13 c ap traffic" (same as server)

{client} derive secret "tls13 s ap traffic" (same as server)

{client} derive secret "tls13 exp master" (same as server)

{client} derive write traffic keys for handshake data (same as server read traffic keys)

{client} derive read traffic keys for application data (same as server write traffic keys)

{client} calculate finished "tls13 finished":

PRK (32 octets): f52e0805a26cd615 ec012fd6b1950258
a9aae77b336a8cac a443df877e99ec61

hash (0 octets): (empty)

info (18 octets): 00200e746c733133 2066696e69736865 6400

output (32 octets): c6ceb1fb180f7d97 62734c4b88430995
2c56d60e95490950 2884f84f4a6be5f0

```
{client}  send a Finished handshake message

{client}  send handshake record:

   payload (36 octets):  14000020735ebda7 9ccdab14ab392f67
      c0866555678946a1 b1b13f3d1a240d3f 1403efb9

   ciphertext (58 octets):  17030100357d5aa6 afb0db48fa79159d
      8074fb1eb26ac08d 6be5c0674197dbd6 efab491f8e99036c
      c16fe5a80f6207a6 c110c8975d753c84 1fa9

{client}  derive write traffic keys for application data:

   PRK (32 octets):  3e97f6ece946f6cf a25aac0c4294f752
      adf68ce3769ba8f1 a72140e960e00b75

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  a2a1d780fe8dcc66 a2c9524da5adcb36

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  774928e1cb918bb5 fabbdec1

{client}  derive secret "tls13 res master":
```



```
   PRK (32 octets):  23bdfa8bb085b65a 8095c55a79f20ab0
      7646d7bac8c67803 2aa5985df2a1b7c1

   hash (32 octets):  24852c1da1686926 86e24b558b6aaa12
      698570f0e85c3925 23ad59b8b89e2aae

   info (52 octets):  002010746c733133 20726573206d6173
      7465722024852c1d a168692686e24b55 8b6aaa12698570f0
      e85c392523ad59b8 b89e2aae

   output (32 octets):  a4fccac589ec1324 762aa9ace2eb916b
      3124acfa5297f8ac b5a025f99375d171

{server}  calculate finished "tls13 finished" (same as client)
```

{server} derive read traffic keys for application data (same as client write traffic keys)

{server} derive secret "tls13 res master" (same as client)

{client} send alert record:

payload (2 octets): 0100

ciphertext (24 octets): 1703010013b48a63 7c14b155f5bc2804 04056c6a4b0a34e2

{server} send alert record:

payload (2 octets): 0100

ciphertext (24 octets): 1703010013523066 0fa8cae6196c4565 ac8207fcaf163e8f

6. Security Considerations

It probably isn't a good idea to use the private key here. If it weren't for the fact that it is too small to provide any meaningful security, it is now very well known.

7. References

7.1. Normative References

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-20 (work in progress), April 2017.

7.2. Informative References

[FIPS186] National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)", NIST PUB 186-4 , July 2013.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January

2016, <http://www.rfc-editor.org/info/rfc7748>.

Appendix A. Acknowledgements

None of this would have been possible without Franziskus Kiefer, Eric Rescorla and Tim Taubert, who did a lot of the work in NSS.

Author's Address

Martin Thomson
Mozilla

Email: martin.thomson@gmail.com