TLS
Internet-Draft
Intended status: Standards Track
Expires: January 17, 2018

M. Thomson
Mozilla

July 16, 2017

Example Handshake Traces for TLS 1.3
draft-ietf-tls-tls13-vectors-02

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 17, 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): 304546ef3c866b23 cc42b5e95282e5df
16ab583ffd142c40 743dd4f306e67220

public key (32 octets): da6a859ad6d2dbb5 1124fbfe6baff63d
8f14365ec990d575 761e4a6164978d31

```
{client}  send a ClientHello handshake message

{client}  send handshake record:

   payload (512 octets):  010001fc0303af21 156b04db639e6615
      4a1fe5adfaeadf9e 413416000d57b8e1 126d4d119a8b0000
      3e130113031302c0 2bc02fcca9cca8c0 0ac009c013c023c0
      27c014009eccaa00 3300320067003900 38006b0016001300
      9c002f003c003500 3d000a0005000401 0001950000000b00
      0900000673657276 6572ff0100010000 0a00140012001d00
      1700180019010001 0101020103010400 0b00020100002300
      0000280026002400 1d0020da6a859ad6 d2dbb51124fbfe6b
```



```
      aff63d8f14365ec9 90d575761e4a6164 978d31002b000706
      7f1503030302000d 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
   ciphertext (517 octets):  1603010200010001 fc0303af21156b04
      db639e66154a1fe5 adfaeadf9e413416 000d57b8e1126d4d
      119a8b00003e1301 13031302c02bc02f cca9cca8c00ac009
      c013c023c027c014 009eccaa00330032 006700390038006b
      00160013009c002f 003c0035003d000a 0005000401000195
      0000000b00090000 06736572766572ff 01000100000a0014
      0012001d00170018 0019010001010102 01030104000b0002
      0100002300000028 00260024001d0020 da6a859ad6d2dbb5
      1124fbfe6baff63d 8f14365ec990d575 761e4a6164978d31
      002b0007067f1503 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): 909afec864953420 8dba128dead0445f
7ddb7104fcad53cf 4252e78111b042b8

public key (32 octets): 9d1bfe8053046d2d bd8e0e6221dad115
87584713c8cf4970 74d9d26d067c432f

{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):  f677c3cdac26a755 455b130efa9b1a3f
         3cafb153544ca46a ddf670df199d996e

      secret (32 octets):  0cefce00d5d29fd0 9f5de36c86fc8e72
         99b4ad11ba4211c6 7063c2cc539fc4f9

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

      PRK (32 octets):  0cefce00d5d29fd0 9f5de36c86fc8e72
         99b4ad11ba4211c6 7063c2cc539fc4f9

      hash (32 octets):  8ac51822361c5963 2de3c6b259e5808c
         e52b8278a6493de2 a976f441abbadc8c

      info (54 octets):  002012746c733133 2063206873207472
         6166666963208ac5 1822361c59632de3 c6b259e5808ce52b
         8278a6493de2a976 f441abbadc8c
```



```
      output (32 octets):  5a63db760b817b1b da96e72832333aec
         6a177deeadb5b407 501ac10c17dac0a4

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

      PRK (32 octets):  0cefce00d5d29fd0 9f5de36c86fc8e72
         99b4ad11ba4211c6 7063c2cc539fc4f9

      hash (32 octets):  8ac51822361c5963 2de3c6b259e5808c
         e52b8278a6493de2 a976f441abbadc8c

      info (54 octets):  002012746c733133 2073206873207472
         6166666963208ac5 1822361c59632de3 c6b259e5808ce52b
         8278a6493de2a976 f441abbadc8c
```

```
   output (32 octets):  3aa72a3c77b791e8 f4de243f9ccce172
      941f8392aeb05429 320f4b572ccfe744

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

   PRK (32 octets):  0cefce00d5d29fd0 9f5de36c86fc8e72
      99b4ad11ba4211c6 7063c2cc539fc4f9

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

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

   output (32 octets):  32cadf38f3089048 5c54bf4f1184eaa5
      569eeef15a43f3c7 6ab33965a47c9ff6

{server}  extract secret "master":

   salt (32 octets):  32cadf38f3089048 5c54bf4f1184eaa5
      569eeef15a43f3c7 6ab33965a47c9ff6

   ikm (32 octets):  0000000000000000 0000000000000000
      0000000000000000 0000000000000000

   secret (32 octets):  6c6d4b3e7c925460 82d7b7a32f6ce219
      3804f1bb930fed74 5c6b93c71397f424

{server}  send handshake record:

   payload (82 octets):  0200004e7f15deac 631669eaf28c6b12
      8b2091d36441e618 964dd8f0ec812e31 cda7aec1d0c11301
```



```
      002800280024001d 00209d1bfe805304 6d2dbd8e0e6221da
      d11587584713c8cf 497074d9d26d067c 432f

   ciphertext (87 octets):  1603010052020000 4e7f15deac631669
      eaf28c6b128b2091 d36441e618964dd8 f0ec812e31cda7ae
      c1d0c11301002800 280024001d00209d 1bfe8053046d2dbd
      8e0e6221dad11587 584713c8cf497074 d9d26d067c432f
```

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

   PRK (32 octets):  3aa72a3c77b791e8 f4de243f9ccce172
      941f8392aeb05429 320f4b572ccfe744

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  5727465c1d8af9bd dbbaa81aafe54bfb

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  409072c6da71d076 947e7663

{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):  3aa72a3c77b791e8 f4de243f9ccce172
      941f8392aeb05429 320f4b572ccfe744

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  ee38546c6bd4e25a a7fc5c157b096921
      977fa8de266e7284 3a1fddc6783a0d30

{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 0000840804008076 f2f558b47d45ec60
      40fd4ee50601123a 0d4a3d324428242a 743355c726007d3e
      6d85e77411de68bf 0f97e9e869a4b00e ec8130ccb5c797b8
      73294548dc615ee6 7f8e37b5025b7625 0b00394492bf676d
      2cf1dc7122620e6c cf5435424e8658b1 c64200a87126d9f8
      1fdd9657045a023f 91ea50e76d4465ab 67813911f3a76614
      000020c4d8789445 942fdc425d1c08fd c0e81ee90794595c
      82e340874c019a73 9a7b22

   ciphertext (673 octets):  170301029cd612d0 b9706b733ac1708a
      fcac1aeec92415c3 7e1c55167e267326 26ef7e4d3e266651
      d1179df924b6c2d2 76eddc07880ff0a8 23925d9d60efffc1
      3b3d5acce6c1e8e1 34aab30052cdabfc f54331057918d2fd
      e22bc67b78b5e2fb e9853fe57aad1319 7f9d22767f6fd6fa
      f82e4c198641fa7e bf6425222d08c310 67a4641ef3e29a7f
      99f704b2ea451b54 e33e1d7749b15ec4 49556d90645a1803
      f3d87dc4b5753556 e5ff1970521f75c5 db3fe7f621c2b47e
      6e5519ab4d7363a1 f7da6f35a9f3587d b3d57ee89a8f24f7
      ba9678a5466497bb 476091cec490a450 b33fdb4978a8fae4
      18f408e3c9e0992a 274eb6718106c4dc 351b8a6b7435ac8b
      2214e194e5edfeff d4a59a2056d6a45c 8f177f39b2b39dcd
      d9813c1fea04e757 6e7a1f5e218bcf8f fbb981e36006dd0b
      b6bb22a1c3d4926c 505f74f231934a57 0c12834d0582e1bf
      2ea9c2280da0b4aa 152f7dd12c81fd48 682076ecd1cd47d4
      149b6352d0975134 3c6b060a61d30ffa 4f8bd1e8a2ab61ff
      3e9f965dfcd7d1c4 7edb2eae8ff132dd fc1f7774ac77b56a
      ce0d43b8d1163638 6538ceb695da7af0 91f18236aab74859
      656e54cf53fd9960 064702b81b664518 65cd8e0d7804708c
      e842204a3dac91ad 826847ce0c3c3f0d e59392fc3b0bbec0
      5878c8f56b68eb50 f62798c86c570f1a d9254fa41b152a77
      6fb17707bfab5ea2 a834e9edd05f6239 204127cc0f5cc18b
      1dae4a070890bdf7 642704b5e9961ff2 6b931d069aeb08dd
      385f1997f804375d 238f26a9e8e8f007 47ea85747d7a7c61
```

```
      6493bd0eff96c576 87e1b409469c3c7a 0c40a9b5ca1eeafd
      f1998fbc4a671898 d8b8a37769cc0ecb 6c19f22b87d46968
      b9a4c1b660f39373 ea517cbf401fe5af 0f2cc910e5786af2
      50a392038be62b93 46b166dbb91ebe46 579f020b1e75d771
      be8ab0dcb7ccce81 48

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

   PRK (32 octets):  6c6d4b3e7c925460 82d7b7a32f6ce219
      3804f1bb930fed74 5c6b93c71397f424

   hash (32 octets):  db04b3cd015fe90a 2eb74533d351ee9c
      daf0b30a09f68391 f24bf32addd4d037

   info (54 octets):  002012746c733133 2063206170207472
      616666696320db04 b3cd015fe90a2eb7 4533d351ee9cdaf0
      b30a09f68391f24b f32addd4d037

   output (32 octets):  53b154f7205e2193 3794330173b14118
      bcd02305b39d64b8 e5271737a7402c74

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

   PRK (32 octets):  6c6d4b3e7c925460 82d7b7a32f6ce219
      3804f1bb930fed74 5c6b93c71397f424

   hash (32 octets):  db04b3cd015fe90a 2eb74533d351ee9c
      daf0b30a09f68391 f24bf32addd4d037

   info (54 octets):  002012746c733133 2073206170207472
      616666696320db04 b3cd015fe90a2eb7 4533d351ee9cdaf0
      b30a09f68391f24b f32addd4d037

   output (32 octets):  47603e72ab5a85b4 dc480897acd07e96
      d18e9db0a931bf75 1650698d6512092d

{server}  derive secret "tls13 exp master":

   PRK (32 octets):  6c6d4b3e7c925460 82d7b7a32f6ce219
      3804f1bb930fed74 5c6b93c71397f424

   hash (32 octets):  db04b3cd015fe90a 2eb74533d351ee9c
      daf0b30a09f68391 f24bf32addd4d037

   info (52 octets):  002010746c733133 20657870206d6173
      74657220db04b3cd 015fe90a2eb74533 d351ee9cdaf0b30a
```

09f68391f24bf32a ddd4d037

output (32 octets): acf49197383cc5fb 50fde04f506dfd58
68dc798219f5eedf fd4f3b7eb713b0c9

{server} derive write traffic keys for application data:

PRK (32 octets): 47603e72ab5a85b4 dc480897acd07e96
d18e9db0a931bf75 1650698d6512092d

key info (13 octets): 001009746c733133 206b657900

key output (16 octets): 698b2aa36a58ceac 77776dd2513fa7fa

iv info (12 octets): 000c08746c733133 20697600

iv output (12 octets): 7fbff5a2c0ac5bd6 7e2cd759

{server} derive read traffic keys for handshake data:

PRK (32 octets): 5a63db760b817b1b da96e72832333aec
6a177deeadb5b407 501ac10c17dac0a4

key info (13 octets): 001009746c733133 206b657900

key output (16 octets): 21103162263e8231 34d6916a82b741c2

iv info (12 octets): 000c08746c733133 20697600

iv output (12 octets): 0e1be2fa84c0bc3c b6d6afe3

{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):  f677c3cdac26a755 455b130efa9b1a3f
         3cafb153544ca46a ddf670df199d996e

      secret (32 octets):  0cefce00d5d29fd0 9f5de36c86fc8e72
         99b4ad11ba4211c6 7063c2cc539fc4f9

   {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):  3aa72a3c77b791e8 f4de243f9ccce172
         941f8392aeb05429 320f4b572ccfe744

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

```
      key output (16 octets):  5727465c1d8af9bd dbbaa81aafe54bfb

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  409072c6da71d076 947e7663

   {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):  5a63db760b817b1b da96e72832333aec
         6a177deeadb5b407 501ac10c17dac0a4

      hash (0 octets):  (empty)

      info (18 octets):  00200e746c733133 2066696e69736865 6400

      output (32 octets):  f8acf5aead23c230 5706ce75da058ecb
         f9393fd656dfb95f db225f9990d4732d

   {client}  send a Finished handshake message

   {client}  send handshake record:

      payload (36 octets):  14000020eb376f20 1f8bb90bb787263c
         1dac3472ba34a499 d547793c15f6f812 5a16d2b8
```

ciphertext (58 octets): 1703010035f879b9 6aca6de41e53173a
55015f7810bdd941 5ac444002b5d7d19 a221fee902124509
5a56aa57d42966b0 17e0fcbaa53027d5 ba2e

{client} derive write traffic keys for application data:

PRK (32 octets): 53b154f7205e2193 3794330173b14118
bcd02305b39d64b8 e5271737a7402c74

key info (13 octets): 001009746c733133 206b657900

key output (16 octets): 459caa9e3914221d 39cc67ae65f9941e

iv info (12 octets): 000c08746c733133 20697600

iv output (12 octets): 54123c2ec7106081 0086c391

{client} derive secret "tls13 res master":

PRK (32 octets): 6c6d4b3e7c925460 82d7b7a32f6ce219
3804f1bb930fed74 5c6b93c71397f424

hash (32 octets): e170b2cab483b329 c049e0d66646f247
306b56e0a03c93bb c14254b8e075924a

info (52 octets): 002010746c733133 20726573206d6173
74657220e170b2ca b483b329c049e0d6 6646f247306b56e0
a03c93bbc14254b8 e075924a

output (32 octets): 1b587a5b2c24f03f d2e2529df1d5f62a
d596b014279608a4 ed4f980662fc326e

{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} generate resumption secret "tls13 resumption":

```
      PRK (32 octets):  1b587a5b2c24f03f d2e2529df1d5f62a
         d596b014279608a4 ed4f980662fc326e

      hash (2 octets):  0000

      info (22 octets):  002010746c733133 20726573756d7074 696f6e020000

      output (32 octets):  581e8e76ee4b9f04 78d727da6d02e506
         02fe2168784575ed 7332b11fd4db81fc

   {server}  send a NewSessionTicket handshake message

   {server}  send handshake record:

      payload (189 octets):  040000b90000001e 1386bfb902000000
         a27bf25dc52d2052 79d8e53986000000 00c231b586206110
         73b1d40d9b8563f3 7900606f87d2f38d 405738e271331b9a
         c650572a63fff310 b39620685bad0483 0fb5faa414454633
         af500abb4a25c93e f991bf62fb6629a7 ffab70db6eeff17b
         2ebf1098593f9935 858b4d5764ac3469 c5ada81bc5c527a1
         10e9f571647fb1f0 bf436ea8c78718f3 82390bc7ae979b1b
         03898c946776de01 96c2c473d1f6dee8 714e310008002a00 0400000400

      ciphertext (211 octets):  17030100cea307cb 4a28329dbf6879ee
         56d1cb4e0055f889 169b3a04ee050225 69c1ad70115dc655
         7802c91832e6e5ef b69c65050f06d189 1692561d4ece8d10
         813bf7a3ea3fb430 cbb36ba1a1d71276 d405a8dd0fef782b
         402a8875245eda0b bd548b61639ba45b 9c63689104432850
         f4c7a8a76a2d13a9 746a424a65730fd1 7ab97f3488d93ab4
```



```
         ebdc0f9f8b317855 1faf72ca05f705dd 901815887a0f7f6f
         7062a3802259d9f2 7bb30b6875be1743 54d6fa59adf24a6b
         85c5415d46173c85 5aaf0dc06296099f c6daa0164ef2848c 2219ae

   {client}  send application_data record:

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

      ciphertext (72 octets):  17030100432e3b59 0791333db65b5632
```

```
      d4c9c7e066120216 08680e714177b07f 06500f28f27617d8
      a92a52ec167530f4 ee7262e40127b997 5c26499c23d8bf6e
      713c4b0c126733bf
```

{server} send application_data record:

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

   ciphertext (72 octets): 1703010043b7a6f5 f971aee65e5386b4
      18f1533c8de304b6 bb58fed0062ca441 d49ea52e219f9c0f
      10fade977cf7ce2a 0e6c9a46ca1b2b72 3b843dc8c630db6e
      64cdb1c27979b6f4
```

{client} generate resumption secret "tls13 resumption" (same as server)

{client} send alert record:

```
   payload (2 octets): 0100

   ciphertext (24 octets): 170301001367bb58 666bd833b0f3a2fc
      fbb27c1353a50493
```

{server} send alert record:

```
   payload (2 octets): 0100

   ciphertext (24 octets): 1703010013ae58fd 7ad77fcc262cdbe7
      a3088d493655a29e
```

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): 8da37c24d5e27c29 c76f3c787f43cfb3
      45e6d8bab793f6f7 50fec63df70f9502
```

```
   public key (32 octets):  4707fcfb129e989d 42c0083f74f3efdf
      1e73da08eb317ebc 2d3ce687957e060f

{client}  extract secret "early":

   salt:  (absent)

   ikm (32 octets):  581e8e76ee4b9f04 78d727da6d02e506
      02fe2168784575ed 7332b11fd4db81fc

   secret (32 octets):  40718b9ebd2b349a 900a2b3742e7a0d2
      3f227bee609e9825 4da761f9d145f7cb

{client}  send a ClientHello handshake message

{client}  calculate finished "tls13 finished":

   PRK (32 octets):  e5f760cd1bbab8da 776f4072fc9a9df9
      782857770bd141d0 eee570623ec118d9

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  16be004dc7d281b7 0a71906f294cf508
      2f546f20f6acf9b5 6b43a3da90485020

{client}  send handshake record:

   payload (512 octets):  010001fc03039aa7 6a8dbff0041077bf
      b6ba54cd905c2c88 d89fa2f9f17300dc 2b2282d1245d0000
      3e130113031302c0 2bc02fcca9cca8c0 0ac009c013c023c0
      27c014009eccaa00 3300320067003900 38006b0016001300
      9c002f003c003500 3d000a0005000401 0001950000000b00
      0900000673657276 6572ff0100010000 0a00140012001d00
      1700180019010001 0101020103010400 0b00020100002800
      260024001d002047 07fcfb129e989d42 c0083f74f3efdf1e
      73da08eb317ebc2d 3ce687957e060f00 2a0000002b000706
      7f1503030302000d 0020001e04030503 0603020308040805
      0806040105010601 0201040205020602 0202002d00020101
      0015002b00000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      2900cd00a800a27b f25dc52d205279d8 e5398600000000c2
```

```
      31b58620611073b1 d40d9b8563f37900 606f87d2f38d4057
      38e271331b9ac650 572a63fff310b396 20685bad04830fb5
      faa414454633af50 0abb4a25c93ef991 bf62fb6629a7ffab
      70db6eeff17b2ebf 1098593f9935858b 4d5764ac3469c5ad
      a81bc5c527a110e9 f571647fb1f0bf43 6ea8c78718f38239
      0bc7ae979b1b0389 8c946776de0196c2 c473d1f6dee8714e
      311386bfbf002120 3ac0405bd6b94bb8 f4759ce048668dee
      514e4ed62e9dc5f7 37000084cce510a1

   ciphertext (517 octets):  1603010200010001 fc03039aa76a8dbf
      f0041077bfb6ba54 cd905c2c88d89fa2 f9f17300dc2b2282
      d1245d00003e1301 13031302c02bc02f cca9cca8c00ac009
      c013c023c027c014 009eccaa00330032 006700390038006b
      00160013009c002f 003c0035003d000a 0005000401000195
      0000000b00090000 06736572766572ff 01000100000a0014
      0012001d00170018 0019010001010102 01030104000b0002
      0100002800260024 001d00204707fcfb 129e989d42c0083f
      74f3efdf1e73da08 eb317ebc2d3ce687 957e060f002a0000
      002b0007067f1503 030302000d002000 1e04030503060302
      0308040805080604 0105010601020104 0205020602020200
      2d00020101001500 2b00000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      00000000002900cd 00a800a27bf25dc5 2d205279d8e53986
      00000000c231b586 20611073b1d40d9b 8563f37900606f87
      d2f38d405738e271 331b9ac650572a63 fff310b39620685b
      ad04830fb5faa414 454633af500abb4a 25c93ef991bf62fb
      6629a7ffab70db6e eff17b2ebf109859 3f9935858b4d5764
      ac3469c5ada81bc5 c527a110e9f57164 7fb1f0bf436ea8c7
      8718f382390bc7ae 979b1b03898c9467 76de0196c2c473d1
      f6dee8714e311386 bfbf0021203ac040 5bd6b94bb8f4759c
      e048668dee514e4e d62e9dc5f7370000 84cce510a1

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

   PRK (32 octets):  40718b9ebd2b349a 900a2b3742e7a0d2
      3f227bee609e9825 4da761f9d145f7cb

   hash (32 octets):  4d972fbd827dbe26 746af0014f20f421
      1cb6f16cda90f26a fdeac1b81095bbc2

   info (53 octets):  002011746c733133 2063206520747261
      66666963204d972f bd827dbe26746af0 014f20f4211cb6f1
      6cda90f26afdeac1 b81095bbc2

   output (32 octets):  12567c821a3a822f 0b5e062b7d7deab4
      1a7edb836ebb8e65 47cfaf28cd3d23b0
```

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

PRK (32 octets): 12567c821a3a822f 0b5e062b7d7deab4
1a7edb836ebb8e65 47cfaf28cd3d23b0

key info (13 octets): 001009746c733133 206b657900

key output (16 octets): d260ca7678d4fd53 dce0c09e7d349141

iv info (12 octets): 000c08746c733133 20697600

iv output (12 octets): 936e9de4fb2b9ca8 acfefc24

{client} send application_data record:

payload (6 octets): 414243444546

ciphertext (28 octets): 170301001713551f 6ab760f07913c0c9
b7f44e1a9df88ad9 3025e01b

{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): 325497b8ece5b646 c0a841465c720414
1c3fac2b0fba03c2 1f798774ccd8ba8a

public key (32 octets): 40ecc2cce32711cc e41494baa7071fb8
3fccf5f18f387422 f3908bc43284e111

{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): 40718b9ebd2b349a 900a2b3742e7a0d2
3f227bee609e9825 4da761f9d145f7cb

hash (32 octets): e3b0c44298fc1c14 9afbf4c8996fb924

```
      27ae41e4649b934c a495991b7852b855

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

   output (32 octets):  3f86b90be314a149 af8854fa5c7457e5
      b814940f059a68f6 58f4f09d5e7811d5
```



```
{server}  extract secret "handshake":

   salt (32 octets):  3f86b90be314a149 af8854fa5c7457e5
      b814940f059a68f6 58f4f09d5e7811d5

   ikm (32 octets):  9c9777daeca7583c 81361536a7533e8a
      2811abe9a3a2342a d806a04bc4db3635

   secret (32 octets):  735590cdccd25055 6d463feaba32b905
      96537834f13d851c dc224338bf3148f4

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

   PRK (32 octets):  735590cdccd25055 6d463feaba32b905
      96537834f13d851c dc224338bf3148f4

   hash (32 octets):  1159439062004376 603abad6721bb808
      daea34558ebbf936 fa2c8dc05828b392

   info (54 octets):  002012746c733133 2063206873207472
      6166666963201159 439062004376603a bad6721bb808daea
      34558ebbf936fa2c 8dc05828b392

   output (32 octets):  28a089b4223c8104 845ff09b7b9e0505
      d6061bdd0ea263a7 40c2bbf5b53d8d44

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

   PRK (32 octets):  735590cdccd25055 6d463feaba32b905
      96537834f13d851c dc224338bf3148f4

   hash (32 octets):  1159439062004376 603abad6721bb808
      daea34558ebbf936 fa2c8dc05828b392
```

```
      info (54 octets):  002012746c733133 2073206873207472
         6166666963201159 439062004376603a bad6721bb808daea
         34558ebbf936fa2c 8dc05828b392

      output (32 octets):  8115875ae8e698f7 47c3cf569d893ef8
         7fd6b819c71c9daf 829efe73a33b6e59

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

      PRK (32 octets):  735590cdccd25055 6d463feaba32b905
         96537834f13d851c dc224338bf3148f4

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



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

      output (32 octets):  ef4b33b2a7895652 b7882b5d4be6abec
         f20c5c49ee18eb05 4dabbf5fe46958fd

   {server}  extract secret "master":

      salt (32 octets):  ef4b33b2a7895652 b7882b5d4be6abec
         f20c5c49ee18eb05 4dabbf5fe46958fd

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  6cfe175844d4b474 fdeb9ef04b2607f7
         ca50bc782c804aab 38502015ae8a48c4

   {server}  send handshake record:

      payload (88 octets):  020000547f158451 4164fe812b870498
         b893365b4376cd74 54d12ac987327ce1 670ef1aaaa991301
         002e002900020000 00280024001d0020 40ecc2cce32711cc
         e41494baa7071fb8 3fccf5f18f387422 f3908bc43284e111

      ciphertext (93 octets):  1603010058020000 547f1584514164fe
```

```
      812b870498b89336 5b4376cd7454d12a c987327ce1670ef1
      aaaa991301002e00 2900020000002800 24001d002040ecc2
      cce32711cce41494 baa7071fb83fccf5 f18f387422f3908b c43284e111

{server}  derive write traffic keys for handshake data:

   PRK (32 octets):  8115875ae8e698f7 47c3cf569d893ef8
      7fd6b819c71c9daf 829efe73a33b6e59

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  4c8fba78ab70af97 d3b04500f481ab11

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  5f577c7b334038c1 f02b97fd

{server}  send a EncryptedExtensions handshake message

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



```
   PRK (32 octets):  8115875ae8e698f7 47c3cf569d893ef8
      7fd6b819c71c9daf 829efe73a33b6e59

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  b0f22d31540198c4 ccac2ad418cbae8e
      0aa427339e820fef 493dfb708a1e2c6c

{server}  send a Finished handshake message

{server}  send handshake record:

   payload (74 octets):  080000220020000a 00140012001d0017
      0018001901000101 0102010301040000 0000002a00001400
      0020d5027b937d18 ab2fb0dbce52a7d6 33f0d74cb903ebf9
      44fd0cab41ebff3d 375f
```

```
      ciphertext (96 octets):  170301005b543211 a6b0602cc2e55337
         f06c9d80915cb3ad 12f78fa6817185b9 99abd80e9378e2f7
         09e51a74dba3652a ff487c27de9e2a98 1fb9a39a70073f9a
         4dcb5557fd71b847 946ea75804208dcc ebb7b0c037e9c466
         47993593815d1825

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

      PRK (32 octets):  6cfe175844d4b474 fdeb9ef04b2607f7
         ca50bc782c804aab 38502015ae8a48c4

      hash (32 octets):  49115f0895594b92 ed1913be0e9da45f
         d0f922142c4f13da 77549d789f337ac4

      info (54 octets):  002012746c733133 2063206170207472
         6166666963204911 5f0895594b92ed19 13be0e9da45fd0f9
         22142c4f13da7754 9d789f337ac4

      output (32 octets):  caac7af75d60cc5e dbf362ab55abb794
         2f7c966ce8db22c3 c5f7cc05a5b1b58c

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

      PRK (32 octets):  6cfe175844d4b474 fdeb9ef04b2607f7
         ca50bc782c804aab 38502015ae8a48c4

      hash (32 octets):  49115f0895594b92 ed1913be0e9da45f
         d0f922142c4f13da 77549d789f337ac4
```



```
      info (54 octets):  002012746c733133 2073206170207472
         6166666963204911 5f0895594b92ed19 13be0e9da45fd0f9
         22142c4f13da7754 9d789f337ac4

      output (32 octets):  c1ac084ddbd228ed feeeecb6a3a75627
         cc93d862b0af9237 3a90fd6df1040c6d

   {server}  derive secret "tls13 exp master":

      PRK (32 octets):  6cfe175844d4b474 fdeb9ef04b2607f7
         ca50bc782c804aab 38502015ae8a48c4
```

```
      hash (32 octets):  49115f0895594b92 ed1913be0e9da45f
         d0f922142c4f13da 77549d789f337ac4

      info (52 octets):  002010746c733133 20657870206d6173
         7465722049115f08 95594b92ed1913be 0e9da45fd0f92214
         2c4f13da77549d78 9f337ac4

      output (32 octets):  b060de35b5d6c782 0324c761c716efca
         bb58870ab264aae8 10a4caa122327656

   {server}  derive write traffic keys for application data:

      PRK (32 octets):  c1ac084ddbd228ed feeeecb6a3a75627
         cc93d862b0af9237 3a90fd6df1040c6d

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  2326cdc28deb238d 82e7c220c437e78b

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  8719ac805d15be7d c733a9f2

   {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):  40718b9ebd2b349a 900a2b3742e7a0d2
         3f227bee609e9825 4da761f9d145f7cb

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



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

      output (32 octets):  3f86b90be314a149 af8854fa5c7457e5
```

```
      b814940f059a68f6 58f4f09d5e7811d5

{client}  extract secret "handshake":

   salt (32 octets):  3f86b90be314a149 af8854fa5c7457e5
      b814940f059a68f6 58f4f09d5e7811d5

   ikm (32 octets):  9c9777daeca7583c 81361536a7533e8a
      2811abe9a3a2342a d806a04bc4db3635

   secret (32 octets):  735590cdccd25055 6d463feaba32b905
      96537834f13d851c dc224338bf3148f4

{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):  8115875ae8e698f7 47c3cf569d893ef8
      7fd6b819c71c9daf 829efe73a33b6e59

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  4c8fba78ab70af97 d3b04500f481ab11

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  5f577c7b334038c1 f02b97fd

{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):  1703010015f7ba63 761efb5d0f267ff7
      a7b52d308d9dfbd5 7fbb

{client}  derive write traffic keys for handshake data:

   PRK (32 octets):  28a089b4223c8104 845ff09b7b9e0505
      d6061bdd0ea263a7 40c2bbf5b53d8d44

   key info (13 octets):  001009746c733133 206b657900

   key output (16 octets):  ae0206779a397d39 abc27bf76257a20c

   iv info (12 octets):  000c08746c733133 20697600

   iv output (12 octets):  92749db888b7a638 c8896347

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

{client}  calculate finished "tls13 finished":

   PRK (32 octets):  28a089b4223c8104 845ff09b7b9e0505
      d6061bdd0ea263a7 40c2bbf5b53d8d44

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  e1e5a35bd3665879 b4aa860ac35bfb7f
      260bb3aeffc3382c a0cb136e36350629

{client}  send a Finished handshake message

{client}  send handshake record:

   payload (36 octets):  14000020f92d6397 71bceb3174f8bd06
      7886f673ba9a051e d6c8f46e42bf58db 1921c638

   ciphertext (58 octets):  1703010035dcaef2 afb9d1372ab1172f
      1a5570b78580d242 fe83be1c779caf21 c3192a14c6a45388
      5676124ae5008c2b a38695eb153f48e4 110a

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

```
      PRK (32 octets):  caac7af75d60cc5e dbf362ab55abb794
         2f7c966ce8db22c3 c5f7cc05a5b1b58c

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  a0c4168c98e0c4ad 3a0e96fdd011484d

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  7d97ef662f0667c8 f5041b4c

   {client}  derive secret "tls13 res master":

      PRK (32 octets):  6cfe175844d4b474 fdeb9ef04b2607f7
         ca50bc782c804aab 38502015ae8a48c4

      hash (32 octets):  339cbe6f1a5e94b4 199425efb7d37343
         2bc262558fd5f948 949bae9ba3d54d2e

      info (52 octets):  002010746c733133 20726573206d6173
         74657220339cbe6f 1a5e94b4199425ef b7d373432bc26255
         8fd5f948949bae9b a3d54d2e

      output (32 octets):  500175fc5b33fcf0 727df04f55f97ecb
         09cabce818b23fc1 57ea9feb3cd45a61

   {server}  derive read traffic keys for handshake data:

      PRK (32 octets):  28a089b4223c8104 845ff09b7b9e0505
         d6061bdd0ea263a7 40c2bbf5b53d8d44

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  ae0206779a397d39 abc27bf76257a20c

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  92749db888b7a638 c8896347

   {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): 1703010043ff683d 8a38b703fd3ebf8b
eac999691ca766db bdf194e607cafe0e ec111de379a8568e
716277b5cda1f932 7d1c00f074af3144 42ff59d12762932c
7c7a49bcf2c58657

{server} send application_data record:

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

ciphertext (72 octets): 1703010043aa88fd 1ad3269a01c7cf34
4970ab14cffe7743 97137cf1575c916a e01f697f81f57283
d666009af2e153cc 2c7adec41f650bba 42c14b36a75e0a7b
742227357e1fa5b4

{client} send alert record:

payload (2 octets): 0100

ciphertext (24 octets): 17030100138a3bec b5cee5fbce9f4421
1058d9b48c308476

{server} send alert record:

payload (2 octets): 0100

ciphertext (24 octets): 1703010013053a76 936d5b173ba833c9
dc9f45d4f7d8e04b

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): 674b85de6a82fa78 fc44ed35ea420c56 ab2327c447874726 743247b6a68caa24

public key (32 octets): f40d38599d529b51 72bc83b8f3246657 1d358f0d48d2b5ac e51901e0123b3b22

{client} send a ClientHello handshake message

{client} send handshake record:

payload (174 octets): 010000aa030308b5 ef1846029d644f18 b00041006116bb12 e2f0f60a209c25ac d1d4dc2daadf0000 0613011303130201 00007b0000000b00 0900000673657276 6572ff0100010000 0a00080006001d00 1700180028002600 24001d0020f40d38 599d529b5172bc83 b8f32466571d358f 0d48d2b5ace51901 e0123b3b22002b00 03027f15000d0020 001e040305030603 0203080408050806 0401050106010201 0402050206020202 002d00020101

ciphertext (179 octets): 16030100ae010000 aa030308b5ef1846 029d644f18b00041 006116bb12e2f0f6 0a209c25acd1d4dc 2daadf0000061301 130313020100007b 0000000b00090000 06736572766572ff 01000100000a0008 0006001d00170018 002800260024001d 0020f40d38599d52 9b5172bc83b8f324 66571d358f0d48d2 b5ace51901e0123b 3b22002b0003027f 15000d0020001e04 0305030603020308 0408050806040105 0106010201040205 0206020202002d00 020101

{server} send a HelloRetryRequest handshake message

{server} send handshake record:

payload (16 octets): 0600000c7f151301 0006002800020017

```
   ciphertext (21 octets):  1603010010060000 0c7f151301000600
      2800020017

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

   private key (32 octets):  3aaa3a2b63029d27 c8dd3a2ed7b1e354
      6fcc42698c293d1c 644156b94a69a643

   public key (65 octets):  04652d99b80ef319 8ea71accdc077352
      4afb7ca17af0bef4 8b4883eebcba3e1e 1f447b9246083536
      8e0ef8eb56a03d48 7ef6254ce51abd8d ab3e100a1caffc8c 9d

{client}  send a ClientHello handshake message

{client}  send handshake record:

   payload (207 octets):  010000cb030308b5 ef1846029d644f18
      b00041006116bb12 e2f0f60a209c25ac d1d4dc2daadf0000
      0613011303130201 00009c0000000b00 0900000673657276
      6572ff0100010000 0a00080006001d00 1700180028004700
```



```
      450017004104652d 99b80ef3198ea71a ccdc0773524afb7c
      a17af0bef48b4883 eebcba3e1e1f447b 92460835368e0ef8
      eb56a03d487ef625 4ce51abd8dab3e10 0a1caffc8c9d002b
      0003027f15000d00 20001e0403050306 0302030804080508
      0604010501060102 0104020502060202 02002d00020101

   ciphertext (212 octets):  16030100cf010000 cb030308b5ef1846
      029d644f18b00041 006116bb12e2f0f6 0a209c25acd1d4dc
      2daadf0000061301 130313020100009c 0000000b00090000
      06736572766572ff 01000100000a0008 0006001d00170018
      0028004700450017 004104652d99b80e f3198ea71accdc07
      73524afb7ca17af0 bef48b4883eebcba 3e1e1f447b924608
      35368e0ef8eb56a0 3d487ef6254ce51a bd8dab3e100a1caf
      fc8c9d002b000302 7f15000d0020001e 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):  fb5b23536a4ef874 f8b4a44bb3b0886d
      046790b682b9aaac 75233edad5020c7d

   public key (65 octets):  047e759436bca19e d0358962b7d0ded4
      2e744076da23ec8a 9633cf172709ee2a c7e8a06b40fbe5bf
      e41afc03a1b78920 68d610b840301e2d 2e1f40787a183f3a 2b

{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):  90975442819df737 9e40c060c3b641f3
      a315ccbf3f4e1542 f3bbe90e0089f7bc

   secret (32 octets):  5558d9a4084111c3 5092aba9f314a046
      852fc282106ad91f 8aad94dc2fcd0a6c
```

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

   PRK (32 octets):  5558d9a4084111c3 5092aba9f314a046
      852fc282106ad91f 8aad94dc2fcd0a6c

   hash (32 octets):  d615e55df3513f10 48462b9b7cc7c110
      71223806e0fff9fa 94ffc0f7432a184b

   info (54 octets):  002012746c733133 2063206873207472
      616666696320d615 e55df3513f104846 2b9b7cc7c1107122
      3806e0fff9fa94ff c0f7432a184b

   output (32 octets):  c11db498010bc4f6 6242a786c862a985
      e358018874b6ed04 61fd92e52696ee76

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

   PRK (32 octets):  5558d9a4084111c3 5092aba9f314a046
      852fc282106ad91f 8aad94dc2fcd0a6c

   hash (32 octets):  d615e55df3513f10 48462b9b7cc7c110
      71223806e0fff9fa 94ffc0f7432a184b

   info (54 octets):  002012746c733133 2073206873207472
      616666696320d615 e55df3513f104846 2b9b7cc7c1107122
      3806e0fff9fa94ff c0f7432a184b

   output (32 octets):  fd1b408bf0324ded 52e449708b1c310c
      50f0a6cd8dab23b6 e4e5e3a413ba259d

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

   PRK (32 octets):  5558d9a4084111c3 5092aba9f314a046
      852fc282106ad91f 8aad94dc2fcd0a6c
```



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

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

```
      output (32 octets):  7d54cbf473252842 3046df3f0d49d87f
         6c11ec65b9e21cbf 91163e3b92a68707

   {server}  extract secret "master":

      salt (32 octets):  7d54cbf473252842 3046df3f0d49d87f
         6c11ec65b9e21cbf 91163e3b92a68707

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  76b73d53db71bd7a a61471dde13a7364
         51802efa6881b88a 77ef23e4029e01d5

   {server}  send handshake record:

      payload (115 octets):  0200006f7f155007 6d6c334421c0ac06
         4f6e47a6409c0417 95345ee3f78ede5a 3c35c8d279a81301
         0049002800450017 0041047e759436bc a19ed0358962b7d0
         ded42e744076da23 ec8a9633cf172709 ee2ac7e8a06b40fb
         e5bfe41afc03a1b7 892068d610b84030 1e2d2e1f40787a18 3f3a2b

      ciphertext (120 octets):  1603010073020000 6f7f1550076d6c33
         4421c0ac064f6e47 a6409c041795345e e3f78ede5a3c35c8
         d279a81301004900 2800450017004104 7e759436bca19ed0
         358962b7d0ded42e 744076da23ec8a96 33cf172709ee2ac7
         e8a06b40fbe5bfe4 1afc03a1b7892068 d610b840301e2d2e
         1f40787a183f3a2b

   {server}  derive write traffic keys for handshake data:

      PRK (32 octets):  fd1b408bf0324ded 52e449708b1c310c
         50f0a6cd8dab23b6 e4e5e3a413ba259d

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  e7fc5d7c880935bc 55412aecbc2773fb

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  3a3a4d62924d7a1b d2235c95
```

```
{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):  fd1b408bf0324ded 52e449708b1c310c
      50f0a6cd8dab23b6 e4e5e3a413ba259d

   hash (0 octets):  (empty)

   info (18 octets):  00200e746c733133 2066696e69736865 6400

   output (32 octets):  e01b611aca50606e 1f247d7bce2467dd
      b01bf06041d1e849 a67cdbacc88cc47b

{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
      04008004fc5804d8 481fdfd8c6319ef6 3968daf9ec416c6c
      819e48253bdf016a bacfadfc69b0bb79 01f899429ffbe89d
      937da491491950ee 29c78ce320226366 fc0575800d3a29b6
      f383d417454ff4b4 0c12da2ac4d9a474 3ced8e420a43023e
      a1548407dd2b6b4a d0409da648ad80c8 86a6e7cca6764fab
```

```
         5b77612380a99dfa 7cf4f314000020e8 7b0043df73761a9f
         1b1a54f7c189a3c8 2f1d7647ee867ad0 db8ea5df20ab7b

      ciphertext (661 octets):  1703010290f458e3 0169c36dfd1f876f
         fe054670b609e771 9bc0b24dca1cb156 f6aa69e6d998df26
         bce69234737c12f3 05f230f03b8a9217 cd4d964ae442f1f7
         358f732e152d9b18 25620233814e8777 f7d046ba44c7c6a4
         8eb468739395642b 006fa132e735b8e0 17b51898ece31dd9
         e9ff44c75cbee059 9dab03d006336d76 505813f8ce64964d
         6064bd9c90fa5e72 a50b76baeecd9c64 b548be8032c450e6
         c2c8abb105bc394d 9bc858f3e2ce6bf8 d6314ba505f3908a
         e9990abfc30a8e64 62a6ef98a05d8c53 47dd92a866619a93
         87803ddb019b25a4 0cfbedab80f920d0 e5e294433b568434
         e796610c9e972daa 0d412a5e4e25bf81 97943fbe74604002
         a6111dbe05439010 c1bbfbe50339dfd7 99f4d72e6853fcae
         7ea453bf0ccf5bfd 338787e45fac53f0 c808861524a7237b
         b19484525eb88051 298c4d51cd8b9380 2a73c4ab9cc27084
         a69a0ee03be6b02f cd2cb5a66dde2b44 0920f408be16c408
         2e0a3dc6d8e15d37 e1f37c44c8433fcf ab9be408c54c074e
         bfa45f2af3d20559 23d2fd8a7c3c3c3d d7bf84d2826784af
         154ca2f5ca7ad8f7 c0e88cdbd7673551 4b49578726a8a26e
         33ff1133d60d8f0e 2fddb6eea294b78d abdd2974dfb1cf53
         3032d0aa71e3e603 e1d1a370c01fd1e9 0aefc1691f63c051
         c5957bea4c4a5033 63627279fec18a72 276b7cb3af42c92e
         24a605e1316f303e 80a01c4f386b5aae bcef58cc09db8b29
         7b38ba6ac277a38f 67d78960d36ea48b 6685abf0cbe9b542
         caa644931dc22656 216cdcf145228c5e eafb8a930bb97619
         e772ed92f89a80da dee692e5cd3985db 2edc81cde6306a6a
         93751e35f6054f84 96e26a2015ef0edc 502f8e96f19579aa
         3ff80c8ef8ab691e 498cf0f8d58a3c3c fcf3aed23f81e43b
         2546fdcabd7c9a80 ad1e59b8dc9a6d0f 674c177eec

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

      PRK (32 octets):  76b73d53db71bd7a a61471dde13a7364
         51802efa6881b88a 77ef23e4029e01d5

      hash (32 octets):  3f44e23dcedd02ac fb53fa70cf0721d8
         e00d9e39bfa3ce91 705d1dc55caf300d

      info (54 octets):  002012746c733133 2063206170207472
         6166666963203f44 e23dcedd02acfb53 fa70cf0721d8e00d
         9e39bfa3ce91705d 1dc55caf300d
```

```
      output (32 octets):  7bbda44aef92ee2d a1523590895f2249
         b1bed03647d8bfee 273fb3ef3b25457c

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



```
      PRK (32 octets):  76b73d53db71bd7a a61471dde13a7364
         51802efa6881b88a 77ef23e4029e01d5

      hash (32 octets):  3f44e23dcedd02ac fb53fa70cf0721d8
         e00d9e39bfa3ce91 705d1dc55caf300d

      info (54 octets):  002012746c733133 2073206170207472
         6166666963203f44 e23dcedd02acfb53 fa70cf0721d8e00d
         9e39bfa3ce91705d 1dc55caf300d

      output (32 octets):  8e7767fb35fb9d93 341b5fe1ac2691b4
         f5cafb6bbe792b53 858b44acb3b6005e

   {server}  derive secret "tls13 exp master":

      PRK (32 octets):  76b73d53db71bd7a a61471dde13a7364
         51802efa6881b88a 77ef23e4029e01d5

      hash (32 octets):  3f44e23dcedd02ac fb53fa70cf0721d8
         e00d9e39bfa3ce91 705d1dc55caf300d

      info (52 octets):  002010746c733133 20657870206d6173
         746572203f44e23d cedd02acfb53fa70 cf0721d8e00d9e39
         bfa3ce91705d1dc5 5caf300d

      output (32 octets):  ba9a598a87e25c0c 963757951c84b1fa
         6930ae37b7f10330 c79dec315bfb6f0f

   {server}  derive write traffic keys for application data:

      PRK (32 octets):  8e7767fb35fb9d93 341b5fe1ac2691b4
         f5cafb6bbe792b53 858b44acb3b6005e

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  6b3b6463ee2e9c63 167930f1cb496857
```

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

      iv output (12 octets):  870b39a26785a453 dd0683a7

   {server}  derive read traffic keys for handshake data:

      PRK (32 octets):  c11db498010bc4f6 6242a786c862a985
         e358018874b6ed04 61fd92e52696ee76

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



```
      key output (16 octets):  5fa4fe8df22a8449 86c47c46981a291a

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  d3bd79ca448e5692 571b9fe3

   {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):  90975442819df737 9e40c060c3b641f3
         a315ccbf3f4e1542 f3bbe90e0089f7bc

      secret (32 octets):  5558d9a4084111c3 5092aba9f314a046
         852fc282106ad91f 8aad94dc2fcd0a6c

   {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):  fd1b408bf0324ded 52e449708b1c310c
         50f0a6cd8dab23b6 e4e5e3a413ba259d

      key info (13 octets):  001009746c733133 206b657900

      key output (16 octets):  e7fc5d7c880935bc 55412aecbc2773fb

      iv info (12 octets):  000c08746c733133 20697600

      iv output (12 octets):  3a3a4d62924d7a1b d2235c95

   {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): c11db498010bc4f6 6242a786c862a985 e358018874b6ed04 61fd92e52696ee76

hash (0 octets): (empty)

info (18 octets): 00200e746c733133 2066696e69736865 6400

output (32 octets): 7e08634d5b4ddeed 131202f8be9528c6 541e38e44f50f0ce 9e483307b1244d69

{client} send a Finished handshake message

{client} send handshake record:

payload (36 octets): 14000020088d1825 a09b055ba971f7c1 cb072dad901d7d66 b07a12fe90a532b4 90e98d11

ciphertext (58 octets): 170301003501a1ee 3aeb36cd4afa9c7c e7184c1bd778fbc3 2ff3cb5c6c734869 062d8e3a786fd33e 6b89241f063274ac 12e559bd780c2dae 5fa1

{client} derive write traffic keys for application data:

PRK (32 octets): 7bbda44aef92ee2d a1523590895f2249 b1bed03647d8bfee 273fb3ef3b25457c

key info (13 octets): 001009746c733133 206b657900

key output (16 octets): 0655d9562ee2ccb1 33f5c62d280d0d15

iv info (12 octets): 000c08746c733133 20697600

```
      iv output (12 octets):  48964508543bc1ec d9b0e6db

   {client}  derive secret "tls13 res master":

      PRK (32 octets):  76b73d53db71bd7a a61471dde13a7364
         51802efa6881b88a 77ef23e4029e01d5

      hash (32 octets):  ddc2b704b9dd57a1 bd2a6794bc485029
         96c0d6dab1c8fbda c3b05262bc530964

      info (52 octets):  002010746c733133 20726573206d6173
         74657220ddc2b704 b9dd57a1bd2a6794 bc48502996c0d6da
         b1c8fbdac3b05262 bc530964

      output (32 octets):  130658d2f9ab0026 cee5f482b5320a27
         1c79695c97eb5401 7c60f7178382d14e

   {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):  1703010013392fc8 5183e3e957e6ed7e
         f3bb003751ff121c

   {server}  send alert record:
```



```
      payload (2 octets):  0100

      ciphertext (24 octets):  17030100130c01d2 788b80b62142f34b
         8cf68e07610a9d64
```

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-tls13-21 (work in progress), July 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