Examples for NIST 800–56A

Contents

1 Introduction and preliminaries **6**

1.1 Notation 6

1.2 Parameters 7

1.3 A note about hash functions 7

1.4 Key Derivation Function 8

1.5 Message Authentication Code 9

2 Parameter sets for finite field schemes **10**

2.1 Finite field $p1024$–$q160$ 10

2.2 Finite field $p2048$–$q224$ 11

2.3 Finite field $p2048$–$q256$ 12

3 Finite field key agreement schemes **13**

3.1 Parameter Sizes and Hash Functions 13

3.2 Test data for 1024–bit prime p and 160–bit prime q 14

3.2.1 dhHybrid1 14

3.2.2 MQV2 19

3.2.3 dhEphem 23

3.2.4 dhHybridOneFlow 24

3.2.5 MQV1 30

3.2.6 dhOneFlow 34

3.2.7 dhStatic 38

3.3 Test data for 2048–bit prime p and 224–bit prime q 41

3.3.1 dhHybrid1 42

3.3.2 MQV2 49

3.3.3 dhEphem 55

3.3.4 dhHybridOneFlow 57

3.3.5 MQV1 67

3.3.6 dhOneFlow 73

3.3.7 dhStatic 77

3.4 Test data for 2048–bit prime p and 256–bit prime q 82

3.4.1 dhHybrid1 82

3.4.2 MQV2 90

3.4.3 dhEphem 96

3.4.4 dhHybridOneFlow 98

3.4.5 MQV1 107

3.4.6 dhOneFlow 114

3.4.7 dhStatic 118

4 Parameter sets for elliptic curve schemes 124

4.1 Curve P–192 124

4.2 Curve P–224 125

4.3 Curve P–256 127

4.4 Curve P–384 128

4.5 Curve P–521 129

5 Elliptic curve key agreement schemes 131

5.1 Parameter sizes and hash functions 131

5.2 Test data for P–192 132

5.2.1 Full Unified Model 132

5.2.2 Full MQV 135

5.2.3 Ephemeral Unified Model 138

5.2.4 One–Pass Unified Model 139

5.2.5 One–Pass MQV 143

5.2.6 One–Pass Diffie–Hellman 146

5.2.7 Static Unified Model 148

5.3 Test data for P–224 151

5.3.1 Full Unified Model 151

5.3.2 Full MQV 154

5.3.3 Ephemeral Unified Model 158

5.3.4 One–Pass Unified Model 159

5.3.5 One–Pass MQV 163

5.3.6 One–Pass Diffie–Hellman 167

5.3.7 Static Unified Model 170

5.4 Test data for P–256 173

5.4.1 Full Unified Model 173

5.4.2 Full MQV 177

5.4.3 Ephemeral Unified Model 180

5.4.4 One–Pass Unified Model 181

5.4.5 One–Pass MQV 186

5.4.6 One–Pass Diffie–Hellman 190

5.4.7 Static Unified Model 193

5.5 Test data for P–384 196

5.5.1 Full Unified Model 196

5.5.2 Full MQV 200

5.5.3 Ephemeral Unified Model 204

5.5.4 One–Pass Unified Model 205

5.5.5 One–Pass MQV 210

5.5.6 One–Pass Diffie–Hellman 215

5.5.7 Static Unified Model 217

5.6 Test data for P–521 221

5.6.1 Full Unified Model 222

5.6.2 Full MQV 227

5.6.3 Ephemeral Unified Model 231

5.6.4 One–Pass Unified Model 233

5.6.5 One–Pass MQV 239

5.6.6 One–Pass Diffie–Hellman 244

5.6.7 Static Unified Model 247

1

Introduction and preliminaries

This document contains test data for the finite field and elliptic curve schemes described in [1, section 6]. For each of these schemes, this document provides step-by-step sample outputs that correspond precisely to steps described in [1]. The purpose is to aid in the checking of an implementation of any of these schemes.

1.1 Notation

For any prime p, we denote the finite field of order p by $GF(p)$, and we denote the multiplicative subgroup of its non-zero elements by $GF(p)^*$.

We use the symbol || to denote concatenation.

Unless otherwise noted, all numerical data is presented in hexadecimal notation.

1.2 Parameters

Each of the seven finite field schemes described in [1] can be implemented using any primes (p, q) of bit lengths chosen from one of three sets of parameter sizes: $(1024, 160)$, $(2048, 224)$, or $(2048, 256)$. Any such pair of primes must satisfy the relation $p \equiv 1 \mod q$. In addition, a generator, G, for the unique subgroup of $GF(p)^*$ of order q is needed.

Throughout this document, all examples of finite field schemes will use the three parameter sets $\{p, q, G\}$ specified in Section 2: Parameter sets for finite field key agreement schemes.

Each of the seven elliptic curve schemes described in [1] can be implemented using an elliptic curve as specified in [1, section 5.5.1.2].

Throughout this document, all examples of elliptic curve schemes will use the five parameter sets given by the curves P–192, P–224, P–256, P–384, P–521 which are specified in FIPS 186-3 [2]. For convenience, they are included in Section 4: Parameter sets for elliptic curve schemes.

1.3 A note about hash functions

Care must be taken whenever hash functions are called. The hash functions take bitstring inputs and are sensitive to leading zeroes. If a hash is called with hex and/or ASCII inputs, all ASCII strings are converted into their hex equivalents, and all hexstrings are then converted into bits. For instance, the hexstrings `2` and `02` have distinct hash values: `Hash(2)` is equivalent to `Hash(0010)`, whereas `Hash(02)` is equivalent to `Hash(00000010)`.

1.4 Key Derivation Function

Throughout this document, the key derivation function (KDF) employed is the Concatenation Key Derivation Function, which is specified in [1, section 5.8.1].

The inputs to the KDF are a shared secret byte string `Z`, and a parameter called `OtherInput`, which is comprised of an integer `keydatalen` and a bit string `OtherInfo`, which is the concatenation of five subfields (the last two are optional). The data for all but two of the schemes in this document is generated with the subfields set to the following values.

Subfield	Value	Comment
`AlgorithmID`	`12345678 9ABCDEF0`	arbitrarily chosen
`PartyUInfo`	`414C4943 45313233`	ASCII(`ALICE123`)
`PartyVInfo`	`424F4242 59343536`	ASCII(`BOBBY456`)
`SuppPubInfo`	not set	field is optional
`SuppPrivInfo`	not set	field is optional

The dhStatic and Static Unified Model schemes require that a nonce be part of `PartyUInfo`. The standard states that the format for this inclusion is to be specified by the application. In this document, it is specified as follows:

```
PartyUInfo =  414C4943 45313233 || nonceU_byte_len || nonceU
```

where `nonceU_byte_len` is a 32-bit/4-byte/4-octet big–endian value holding the length of `nonceU` in bytes, e.g., if `nonceU` is size 384-bits, then

```
nonceU_byte_len = 00000030
```

1.5 Message Authentication Code

Throughout this document, whenever a message authentication code (MAC) is required, the MAC employed shall be HMAC, which is specified in [4, section 5].

The input into the MAC function is the concatenation of five subfields.

The first subfield in the MAC data, denoted `message_string_P` in [1], is a six byte string with a value of `KC_[1 or 2]_[U or V]`, where `1` is chosen for unilateral cases, and `2` is chosen for bilateral cases, and `[U or V]` is the provider of the MAC.

The next two subfields are the ID's of the provider and the recipient. In this document `ALICE` and `BOBBY` will be used as the ID's for `U` and `V` in all schemes.

The following table provides a summary.

Subfield	Value	Comment
`ID_U`	`41 4C494345`	ASCII(`ALICE`)
`ID_V`	`42 4F424259`	ASCII(`BOBBY`)
`msg_UN_U`	`4B43 5F315F55`	ASCII(`KC_1_U`)
`msg_UN_V`	`4B43 5F315F56`	ASCII(`KC_1_V`)
`msg_BI_U`	`4B43 5F325F55`	ASCII(`KC_2_U`)
`msg_BI_V`	`4B43 5F325F56`	ASCII(`KC_2_V`)

2

Parameter sets for finite field schemes

The following three parameter sets are used to generate the finite field scheme test data in this document.

2.1 Finite field p1024–q160

```
q =       F518AA87 81A8DF27 8ABA4E7D 64B7CB9D 49462353

p =       B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6
          9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0
          13ECB4AE A9061123 24975C3C D49B83BF ACCBDD7D 90C4BD70
          98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0
          A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708
          DF1FB2BC 2E4A4371

G =       A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F
          D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213
```

```
160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1
909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A
D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24
855E6EEB 22B3B2E5
```

2.2 Finite field $p2048$–$q224$

```
q =     801C0D34 C58D93FE 99717710 1F80535A 4738CEBC BF389A99
        B36371EB

p =     AD107E1E 9123A9D0 D660FAA7 9559C51F A20D64E5 683B9FD1
        B54B1597 B61D0A75 E6FA141D F95A56DB AF9A3C40 7BA1DF15
        EB3D688A 309C180E 1DE6B85A 1274A0A6 6D3F8152 AD6AC212
        9037C9ED EFDA4DF8 D91E8FEF 55B7394B 7AD5B7D0 B6C12207
        C9F98D11 ED34DBF6 C6BA0B2C 8BBC27BE 6A00E0A0 B9C49708
        B3BF8A31 70918836 81286130 BC8985DB 1602E714 415D9330
        278273C7 DE31EFDC 7310F712 1FD5A074 15987D9A DC0A486D
        CDF93ACC 44328387 315D75E1 98C641A4 80CD86A1 B9E587E8
        BE60E69C C928B2B9 C52172E4 13042E9B 23F10B0E 16E79763
        C9B53DCF 4BA80A29 E3FB73C1 6B8E75B9 7EF363E2 FFA31F71
        CF9DE538 4E71B81C 0AC4DFFE 0C10E64F

G =     AC4032EF 4F2D9AE3 9DF30B5C 8FFDAC50 6CDEBE7B 89998CAF
        74866A08 CFE4FFE3 A6824A4E 10B9A6F0 DD921F01 A70C4AFA
        AB739D77 00C29F52 C57DB17C 620A8652 BE5E9001 A8D66AD7
        C1766910 1999024A F4D02727 5AC1348B B8A762D0 521BC98A
        E2471504 22EA1ED4 09939D54 DA7460CD B5F6C6B2 50717CBE
        F180EB34 118E98D1 19529A45 D6F83456 6E3025E3 16A330EF
        BB77A86F 0C1AB15B 051AE3D4 28C8F8AC B70A8137 150B8EEB
        10E183ED D19963DD D9E263E4 770589EF 6AA21E7F 5F2FF381
        B539CCE3 409D13CD 566AFBB4 8D6C0191 81E1BCFE 94B30269
        EDFE72FE 9B6AA4BD 7B5A0F1C 71CFFF4C 19C418E1 F6EC0179
        81BC087F 2A7065B3 84B890D3 191F2BFA
```

2.3 Finite field p2048–q256

```
q =       8CF83642 A709A097 B4479976 40129DA2 99B1A47D 1EB3750B
          A308B0FE 64F5FBD3


p =       87A8E61D B4B6663C FFBBD19C 65195999 8CEEF608 660DD0F2
          5D2CEED4 435E3B00 E00DF8F1 D61957D4 FAF7DF45 61B2AA30
          16C3D911 34096FAA 3BF4296D 830E9A7C 209E0C64 97517ABD
          5A8A9D30 6BCF67ED 91F9E672 5B4758C0 22E0B1EF 4275BF7B
          6C5BFC11 D45F9088 B941F54E B1E59BB8 BC39A0BF 12307F5C
          4FDB70C5 81B23F76 B63ACAE1 CAA6B790 2D525267 35488A0E
          F13C6D9A 51BFA4AB 3AD83477 96524D8E F6A167B5 A41825D9
          67E144E5 14056425 1CCACB83 E6B486F6 B3CA3F79 71506026
          C0B857F6 89962856 DED4010A BD0BE621 C3A3960A 54E710C3
          75F26375 D7014103 A4B54330 C198AF12 6116D227 6E11715F
          693877FA D7EF09CA DB094AE9 1E1A1597


G =       3FB32C9B 73134D0B 2E775066 60EDBD48 4CA7B18F 21EF2054
          07F4793A 1A0BA125 10DBC150 77BE463F FF4FED4A AC0BB555
          BE3A6C1B 0C6B47B1 BC3773BF 7E8C6F62 901228F8 C28CBB18
          A55AE313 41000A65 0196F931 C77A57F2 DDF463E5 E9EC144B
          777DE62A AAB8A862 8AC376D2 82D6ED38 64E67982 428EBC83
          1D14348F 6F2F9193 B5045AF2 767164E1 DFC967C1 FB3F2E55
          A4BD1BFF E83B9C80 D052B985 D182EA0A DB2A3B73 13D3FE14
          C8484B1E 052588B9 B7D2BBD2 DF016199 ECD06E15 57CD0915
          B3353BBB 64E0EC37 7FD02837 0DF92B52 C7891428 CDC67EB6
          184B523D 1DB246C3 2F630784 90F00EF8 D647D148 D4795451
          5E2327CF EF98C582 664B4C0F 6CC41659
```

3

Finite field key agreement schemes

3.1 Parameter Sizes and Hash Functions

Throughout this chapter, the following parameter sizes (in bits) and hash algorithms [3] are used.

Parameter set	Private key size	Hash algorithm	MacKey size	MacLen	Nonce size
p1024–q160	160	SHA–1	80	224	160
p2048–q224	224	SHA–224	112	224	224
p2048–q256	256	SHA–256	128	256	256

3.2 Test data for 1024–bit prime p and 160–bit prime q

In this section, we supply step–by–step test data for the seven finite field key agreement schemes described in [1, section 6] using the parameter set $p1024$–$q160$ described in Section 2.1. For each scheme, a reference to the corresponding section in [1] is provided.

3.2.1 dhHybrid1 for finite field p1024-q160

- Prerequisites:

```
xU =      3AFB7BB0 0F3550D5 A7752390 7412FA02 ED375F05

yU =      3CC7DA70 CCCF3EB4 261DEA1E B045FAB4 6AEF43EE 32C3458B
          82D49F0E 0B1B81EB F62879A4 C850414C BAAB4DA4 97561189
          7BFA3C32 DA72E945 A110A10F 747E4F18 33799BCF A245E843
          30F49B79 68F803C1 0C31DE17 B1E9B6E7 4652CEFA CFF2EDCC
          A7E9B1EA 782AB524 79EC1D45 6AA1ACBC 3DC031FE 1F4EACFE
          8F9A6BDE 1CB79CCD

xV =      2663D5BD F7E903CC 9CA76254 EE400BD2 A9A2D8EA

yV =      1535294C F6365303 0292C4CB 1EEBD8EC 94971568 B357E600
          851B667A 1733BE95 B3B370C2 6898EC8B E0CB0A1E 2E43DB98
          A72DE3AA 35BA8FE3 5E2BFA88 0F14B518 91B64B5C 09ABC858
          2CE11AAD 14CA1460 5F4232CA 8A594447 3C103106 917D92D5
          39428DBA 97D53F54 67A8EBDC C0D039F4 6B73EDC4 E04B7B04
          83A2A9B6 5BBF8827
```

- Step 1: U produces rU, tU and receives tV. U DOES NOT RECEIVE rV (shown only for the purpose of verifying this data).

```
rU =      E678306C D022FDE5 CF48A353 25A30072 8FD1FD13
```

```
tU =      8D775EE5 EB65BD84 FC35CA47 A55ED1DA 5132468A C74B0C3E
          2D3AC11A E2CDD2EB FC0F403F 91249B9E 2987F289 7A9D164C
          FC3074BA 16EEDB2F 3C9DC2A7 8AE61FEE 17204423 D33DD603
          01489E48 27B95924 5A4B51DB 21DC84A7 EF1E2102 CA232C0B
          B3FE3F8C BED76CB2 14672269 BC380EE5 F2C909C2 77EFE516
          9E0EF522 966CBD9C

rV =      84D39F54 7EEB9475 758570B3 6C338941 AE201DCB

tV =      1B506BA0 9BB10828 B6A266D3 9D2B5423 50E39177 1DCF7481
          323FDE20 3EA37B55 A19DA171 D48E2F74 1D89D56E 92D94C4A
          FB85ECA5 3D572187 0D73EC2B B5CD1698 3F9D12A7 BC2C9805
          6BDC8BBB D24E7234 D09C7133 D4843344 F2E998E0 0CFCA271
          6ABA2248 C019E963 F4B9B1E8 73833A2B 36F5D999 E438E707
          E9DF4664 7542EBA2
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     92925188088218547514077456859543576076192285416058
          62190728294348842426972716582851402453669008719033
          39030080106060667140088239088721517995235378132224
          32021365492059660721325727653097619105628186124831
          11008492304012591442143029451858621897408298376252
          59386079937372620895236729376882795319108699646298
          39570637

Z_s =     845471BA 80F64BC1 5298B45B 7748C313 AA141BED DE071950
          AF62819F F507CE1E 1370C12C 589F6593 B50D985B F93DBF6B
          036EEF7C 6E7C8BE8 50BC1F07 07E5D1A8 1F920D8F 57ED6936
          E92279D5 D2C9763C 8F78714D 09659EA7 661A4174 8B892BEC
          19C270A3 37AB85DC 99621FD0 1D8B2A55 A87EFBC4 A74C4611
          209363C0 BB15E6CD
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     591608390973519928277462907403311491915071482682 25
          449696611811339264788997750825457130742249611167 69
          291437866689670309492087308287943937647450694233 63
          292646259571026392536061897302381693326049148556 02
          671063051543248224943984553280563455506463118681 65
          369886638859788140328843792780861853118614880570 92
          54331918

Z_e =     543F71E0 80FBF42D 3D85CBB0 FCAFE52D 359D83B8 2D00E64E
          E00DA49F 01D955D3 16E17CEC 0BC7F04C C2657834 9CFF9542
          1A6BF66E 4E814440 D2A07C2C 7C27DB70 60199589 4DDCDD24
          D6354AD3 A819A658 01BFFCDD 30143143 307395A8 ED906A9C
          FD804B9B 041A65F2 8B244AE3 4B6D7018 D5DAC82B BCD2BF2B
          FF791CA8 1F2F8E0E
```

- Step 5: Shared secret.

```
Z =       543F71E0 80FBF42D 3D85CBB0 FCAFE52D 359D83B8 2D00E64E
          E00DA49F 01D955D3 16E17CEC 0BC7F04C C2657834 9CFF9542
          1A6BF66E 4E814440 D2A07C2C 7C27DB70 60199589 4DDCDD24
          D6354AD3 A819A658 01BFFCDD 30143143 307395A8 ED906A9C
          FD804B9B 041A65F2 8B244AE3 4B6D7018 D5DAC82B BCD2BF2B
          FF791CA8 1F2F8E0E 845471BA 80F64BC1 5298B45B 7748C313
          AA141BED DE071950 AF62819F F507CE1E 1370C12C 589F6593
          B50D985B F93DBF6B 036EEF7C 6E7C8BE8 50BC1F07 07E5D1A8
          1F920D8F 57ED6936 E92279D5 D2C9763C 8F78714D 09659EA7
          661A4174 8B892BEC 19C270A3 37AB85DC 99621FD0 1D8B2A55
          A87EFBC4 A74C4611 209363C0 BB15E6CD
```

- Step 6: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = CF76ACD5 EA9FD926 2E4DF274 421382F3 E17AEA6D 9FD69C5E
             1485B343 BC4FD3FA 1B0A6D4C B0FE8448
```

- If key confirmation is performed, then

```
MacKey  =     CF76 ACD5EA9F D9262E4D
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 8D775EE5 EB65BD84
            FC35CA47 A55ED1DA 5132468A C74B0C3E 2D3AC11A E2CDD2EB
            FC0F403F 91249B9E 2987F289 7A9D164C FC3074BA 16EEDB2F
            3C9DC2A7 8AE61FEE 17204423 D33DD603 01489E48 27B95924
            5A4B51DB 21DC84A7 EF1E2102 CA232C0B B3FE3F8C BED76CB2
            14672269 BC380EE5 F2C909C2 77EFE516 9E0EF522 966CBD9C
            1B506BA0 9BB10828 B6A266D3 9D2B5423 50E39177 1DCF7481
            323FDE20 3EA37B55 A19DA171 D48E2F74 1D89D56E 92D94C4A
            FB85ECA5 3D572187 0D73EC2B B5CD1698 3F9D12A7 BC2C9805
            6BDC8BBB D24E7234 D09C7133 D4843344 F2E998E0 0CFCA271
            6ABA2248 C019E963 F4B9B1E8 73833A2B 36F5D999 E438E707
            E9DF4664 7542EBA2

MacTag_U  = EECBBD70 D4D46136 6460570D 5855A03B D50B18A4
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 1B506BA0 9BB10828
            B6A266D3 9D2B5423 50E39177 1DCF7481 323FDE20 3EA37B55
            A19DA171 D48E2F74 1D89D56E 92D94C4A FB85ECA5 3D572187
            0D73EC2B B5CD1698 3F9D12A7 BC2C9805 6BDC8BBB D24E7234
            D09C7133 D4843344 F2E998E0 0CFCA271 6ABA2248 C019E963
            F4B9B1E8 73833A2B 36F5D999 E438E707 E9DF4664 7542EBA2
            8D775EE5 EB65BD84 FC35CA47 A55ED1DA 5132468A C74B0C3E
            2D3AC11A E2CDD2EB FC0F403F 91249B9E 2987F289 7A9D164C
            FC3074BA 16EEDB2F 3C9DC2A7 8AE61FEE 17204423 D33DD603
            01489E48 27B95924 5A4B51DB 21DC84A7 EF1E2102 CA232C0B
            B3FE3F8C BED76CB2 14672269 BC380EE5 F2C909C2 77EFE516
            9E0EF522 966CBD9C
```

```
MacTag_V  = BC5F8E45 EA66A682 BA257D17 B4106646 DD1742DB
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 8D775EE5 EB65BD84
            FC35CA47 A55ED1DA 5132468A C74B0C3E 2D3AC11A E2CDD2EB
            FC0F403F 91249B9E 2987F289 7A9D164C FC3074BA 16EEDB2F
            3C9DC2A7 8AE61FEE 17204423 D33DD603 01489E48 27B95924
            5A4B51DB 21DC84A7 EF1E2102 CA232C0B B3FE3F8C BED76CB2
            14672269 BC380EE5 F2C909C2 77EFE516 9E0EF522 966CBD9C
            1B506BA0 9BB10828 B6A266D3 9D2B5423 50E39177 1DCF7481
            323FDE20 3EA37B55 A19DA171 D48E2F74 1D89D56E 92D94C4A
            FB85ECA5 3D572187 0D73EC2B B5CD1698 3F9D12A7 BC2C9805
            6BDC8BBB D24E7234 D09C7133 D4843344 F2E998E0 0CFCA271
            6ABA2248 C019E963 F4B9B1E8 73833A2B 36F5D999 E438E707
            E9DF4664 7542EBA2

MacTag_U  = F06AEFAE 18A5E87A 4B9A4EAE 53F88674 5D94C226

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 1B506BA0 9BB10828
            B6A266D3 9D2B5423 50E39177 1DCF7481 323FDE20 3EA37B55
            A19DA171 D48E2F74 1D89D56E 92D94C4A FB85ECA5 3D572187
            0D73EC2B B5CD1698 3F9D12A7 BC2C9805 6BDC8BBB D24E7234
            D09C7133 D4843344 F2E998E0 0CFCA271 6ABA2248 C019E963
            F4B9B1E8 73833A2B 36F5D999 E438E707 E9DF4664 7542EBA2
            8D775EE5 EB65BD84 FC35CA47 A55ED1DA 5132468A C74B0C3E
            2D3AC11A E2CDD2EB FC0F403F 91249B9E 2987F289 7A9D164C
            FC3074BA 16EEDB2F 3C9DC2A7 8AE61FEE 17204423 D33DD603
            01489E48 27B95924 5A4B51DB 21DC84A7 EF1E2102 CA232C0B
            B3FE3F8C BED76CB2 14672269 BC380EE5 F2C909C2 77EFE516
            9E0EF522 966CBD9C

MacTag_V  = 8E72ADEE 8BF337C2 0373FBFB DA233955 F6F0E6C8
```

3.2.2 MQV2 for finite field p1024-q160

- Prerequisites:

```
xU =      4BAE4F58 49E9E1D0 138283DC 166C190D 8A1D2597

yU =      34A80DD8 DDF9CD4E BAAAA20B A8F270BB 09A64324 539AB116
          556A8DE0 FFA518E6 7B720E8A 98DF6C7F F0AE8ED1 D3E4A7FF
          5C82546E C37DC617 D8F05EB3 0921427A 698F5C6A 45035DBF
          0379DDC1 38B7513C 6F4A54C5 AFB4ECE2 F068842C 8571B353
          20649249 5FE0B36F CC92B6A6 51974A33 4CAF3273 9E136A78
          A41DDD7C BE848009

xV =      21C89A9C 104BC0F0 75EF3D74 8FA91FA0 77935DFE

yV =      9F99A0D6 BFC36193 88564725 27431817 A0FE7505 D4C7D99B
          7D4908A6 2A6782B2 716F5EFB 7FBDEDBC 2AB6E68C 8CB828FF
          6DB4DA70 392FF804 3685790E 5F551085 7B7236F2 D3647C33
          0F5FE05F BB4F368B 8D8D8477 292949B3 C6F30E39 D401DA75
          09C4F259 51FC8E00 5ABCAB18 27E3110A 61B0E12F 58BEDD8E
          A62593BD 906907E2
```

- Step 1: U produces rU, tU and receives tV. U DOES NOT RECEIVE rV (shown only for the purpose of verifying this data).

```
rU =      791C41C5 003B88D2 385569BA 5B46941B 426D6B9A

tU =      5259066A F8D19469 E96CA413 929EF8FD 66D7928E 3A1D552D
          E647F869 56D09DDE B106C750 901B17D2 9CAA9BCE 07F8D515
          A9092530 D0B5B304 5CE85D06 77C93D73 629602F1 EED26E67
          0B72E963 C55FC995 8D3A434E 0EC8C775 95BCCAA4 4286A041
          B55AFC95 A0466C12 801AAE0C 184D6050 BC466262 D6D8D944
          9C4E2887 13D567DC

rV =      D4852AED 71BC7A1B 96CAEEA4 227944D2 791407B5
```

```
tV =      AE97A25A D1AE0E5E 3928C895 A8C4C784 D47E2406 6B82ACE7
          D897BF37 8C6C69CB 4EABEA93 07C4F5E2 1EF56B10 45F3BD71
          C1BA5979 AD0842B3 2B737B06 31C544B3 C87CEE46 A3B309EF
          7F550F84 BC35713C 86BEE6BB 36235FAC 59228E2A AE20944A
          D3C26C6E 18BC6788 789E3F51 D7C6ADEC 0BE423CF 889E2737
          5E2E8D4C FC9AD4CF
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       114194839340062872348518809688071312880170485599915
          583575466012457183130481265283533367566940525073437
          371651311773954406313977518754483010308586582269977
          261818932361852792580476686594258226040867638830931
          369320903674242932549470893901713901413448403082599
          753404815929860423041029139986234681755495494872489
          685943
```

- Step 4: Shared secret converted to byte string.

```
Z =       A29E6CE5 CF0462D2 9A1B4AF1 753DD438 9F347E59 2E7013E6
          AFCE9931 8C3AA463 5FADFFA2 A3E7C7B8 905F3B9C 92D488AC
          DA583B4D EC25BC60 2C3D33D9 DAD2A230 B4A0906A 595ECE50
          508BAA48 7846766B C2D49511 A2F0F0D3 83FCD470 2D79E203
          79705C2C 98C94A94 CFC84082 0CAAA934 F4A3310D 51436C81
          84122257 745273B7
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 14E62AAA EF57793E 560C9035 E74FA9A7 87B2CF18 99E91595
             B7D2D904 5243AE35 07EF68F7 B700BFAB
```

- If key confirmation is performed, then

```
MacKey  =     14E6 2AAAEF57 793E560C
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 5259066A F8D19469
            E96CA413 929EF8FD 66D7928E 3A1D552D E647F869 56D09DDE
            B106C750 901B17D2 9CAA9BCE 07F8D515 A9092530 D0B5B304
            5CE85D06 77C93D73 629602F1 EED26E67 0B72E963 C55FC995
            8D3A434E 0EC8C775 95BCCAA4 4286A041 B55AFC95 A0466C12
            801AAE0C 184D6050 BC466262 D6D8D944 9C4E2887 13D567DC
            AE97A25A D1AE0E5E 3928C895 A8C4C784 D47E2406 6B82ACE7
            D897BF37 8C6C69CB 4EABEA93 07C4F5E2 1EF56B10 45F3BD71
            C1BA5979 AD0842B3 2B737B06 31C544B3 C87CEE46 A3B309EF
            7F550F84 BC35713C 86BEE6BB 36235FAC 59228E2A AE20944A
            D3C26C6E 18BC6788 789E3F51 D7C6ADEC 0BE423CF 889E2737
            5E2E8D4C FC9AD4CF

MacTag_U  = 0908772A 9671C57F CDB4D0AB DC6557D4 D0218AFB
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 AE97A25A D1AE0E5E
            3928C895 A8C4C784 D47E2406 6B82ACE7 D897BF37 8C6C69CB
            4EABEA93 07C4F5E2 1EF56B10 45F3BD71 C1BA5979 AD0842B3
            2B737B06 31C544B3 C87CEE46 A3B309EF 7F550F84 BC35713C
            86BEE6BB 36235FAC 59228E2A AE20944A D3C26C6E 18BC6788
            789E3F51 D7C6ADEC 0BE423CF 889E2737 5E2E8D4C FC9AD4CF
            5259066A F8D19469 E96CA413 929EF8FD 66D7928E 3A1D552D
            E647F869 56D09DDE B106C750 901B17D2 9CAA9BCE 07F8D515
            A9092530 D0B5B304 5CE85D06 77C93D73 629602F1 EED26E67
            0B72E963 C55FC995 8D3A434E 0EC8C775 95BCCAA4 4286A041
            B55AFC95 A0466C12 801AAE0C 184D6050 BC466262 D6D8D944
            9C4E2887 13D567DC
```

```
MacTag_V  = 0EA4F54A 5CC408C6 67030B69 6C665276 F512F0E1
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 5259066A F8D19469
            E96CA413 929EF8FD 66D7928E 3A1D552D E647F869 56D09DDE
            B106C750 901B17D2 9CAA9BCE 07F8D515 A9092530 D0B5B304
            5CE85D06 77C93D73 629602F1 EED26E67 0B72E963 C55FC995
            8D3A434E 0EC8C775 95BCCAA4 4286A041 B55AFC95 A0466C12
            801AAE0C 184D6050 BC466262 D6D8D944 9C4E2887 13D567DC
            AE97A25A D1AE0E5E 3928C895 A8C4C784 D47E2406 6B82ACE7
            D897BF37 8C6C69CB 4EABEA93 07C4F5E2 1EF56B10 45F3BD71
            C1BA5979 AD0842B3 2B737B06 31C544B3 C87CEE46 A3B309EF
            7F550F84 BC35713C 86BEE6BB 36235FAC 59228E2A AE20944A
            D3C26C6E 18BC6788 789E3F51 D7C6ADEC 0BE423CF 889E2737
            5E2E8D4C FC9AD4CF

MacTag_U  = AEC2850A CBCB24F7 9D51E7F4 A00DD771 A05B77E5

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 AE97A25A D1AE0E5E
            3928C895 A8C4C784 D47E2406 6B82ACE7 D897BF37 8C6C69CB
            4EABEA93 07C4F5E2 1EF56B10 45F3BD71 C1BA5979 AD0842B3
            2B737B06 31C544B3 C87CEE46 A3B309EF 7F550F84 BC35713C
            86BEE6BB 36235FAC 59228E2A AE20944A D3C26C6E 18BC6788
            789E3F51 D7C6ADEC 0BE423CF 889E2737 5E2E8D4C FC9AD4CF
            5259066A F8D19469 E96CA413 929EF8FD 66D7928E 3A1D552D
            E647F869 56D09DDE B106C750 901B17D2 9CAA9BCE 07F8D515
            A9092530 D0B5B304 5CE85D06 77C93D73 629602F1 EED26E67
            0B72E963 C55FC995 8D3A434E 0EC8C775 95BCCAA4 4286A041
            B55AFC95 A0466C12 801AAE0C 184D6050 BC466262 D6D8D944
            9C4E2887 13D567DC

MacTag_V  = E74235CE 38AF6248 5F52BC30 6C3033B3 0DA3FF3D
```

3.2.3 dhEphem for finite field p1024-q160

- Step 1: U produces rU, tU and receives tV. U DOES NOT RECEIVE rV (shown only for the purpose of verifying this data).

```
rU =      6A6764D8 837A8F5C B2D87E5B 078766D8 E1E9BED3

tU =      477EE744 F322AA81 44C02790 CD5EA571 6106420F 5D630E06
          B88A150E CFBF39CD 6566E8BC 6DC28288 32158B5F 52407D57
          441AE5C8 77B059D1 22ECFF4F 1D3CDE25 0F88F39B 6B80BA75
          134DD0B3 159CAB17 A3A11C14 467518F9 2E1657C6 9A28978E
          35292BFF 3DBA7D0A 7F6DAAA9 9D5C8711 2B58C82C 7EE6C034
          D114CA0F 4A16DEB8

rV =      4739D45C D8093C45 8EA3AD85 BBAB7700 62871BF6

tV =      09046D14 18585FA5 D32FAD23 18805CCD 19F857E5 E35CC1A3
          D7F93F7B 15D52BC7 D3B642E7 B56A07F8 1BDFF0C2 A2FE71CA
          F8F5E89C 9989A67D B6BF2332 750AD188 BE9C8372 DE48C1D0
          21473512 52FFF746 F05CBCE6 8A016614 54AE3EDB 612CC4CE
          3ABA089D 1A817F5A 210A1985 650255C0 F0E460A0 16E35BFD
          94FEC560 F9843436
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       188304618725840870222506533560341564739848864650 22
          542275583431718479865404598754768231202341099027 25
          277006571019230248414063441678565014839188034592 63
          147695107548272409268641693421663576945663334784 51
          313119342841953030676757002177533761375846968100 37
          508221469380409756784721508651254739491191353427 18
          9227329
```

- Step 4:

```
Z =       02AE79D9 8FF676CD D76FFE60 DAE97ADE 3A3B6DC7 B850F830
          B73FF712 565E029E DF98FFA6 219696D7 422E13E9 A2AE3D67
          0F40CB4B BA852729 478249F2 0BC3EF17 EC98F5E2 EE3A8306
          2264F694 6AA34B60 0BF2D235 1399BDA9 C4B8E1AF 3E353F39
          4AC1D7AE 70B5FA69 0E8E676A B5840377 1E6A37D6 3F966A7A
          3E90295A 08D6DF41
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = F8FDC02F 4987740C 1443D366 DFCFD860 824AB19A E36F2F6F
             D8F61EBB A84AA0D7 A21FFD74 1C788599
```

3.2.4 dhHybridOneFlow for finite field p1024-q160

- Prerequisites:

```
xU =      094FA39F D3843C65 5035EB7B 50E188AC 3ADE9C62

yU =      08A66B63 7260C8B3 FD45F3ED BE17D21C A7869845 65482518
          542FE047 A9DB92F9 180379AA E068E907 669D0998 993C990D
          249E74BE A890D3B6 CBAAA4AC 20F350B6 8FDE991A 606E2464
          923D9736 C31ACAA0 D9A815AA 1A6E1D17 8A782A4B 48E199DB
          7FB20145 34C7E7B5 23D86170 3E38D424 269242ED 8CD53A7E
          5A327696 9BC862F1

xV =      14F3A167 E095A989 7C980545 BA0CEA50 F53FADD3

yV =      AE55EF3A 99696BA9 7D4952AF D8BA29A8 E7394F5A 7C8CB83F
          A5D8978B EE01208F 8214DDFC D19DC37C 11D4F8E2 BAD8FB51
          68DB3B08 8496EFF8 6A174F04 069E8DDD 900A159B 342A6B43
          C89B9CDD D6BE975C 31BC9468 87DA73DE DFD4F8F4 051AB58C
          1E86F404 000D2CDB 8D32BCA5 CE0F572E 8EAF59C2 5988892D
          8839922F 08ECB5DF
```

BEGIN U's calculations

- Step 1:

```
rU =      D2F8A115 DBD8B2E7 4C5D20BA F5E5C17B E33B844B

tU =      126B756D D341EF3F 97FB0032 FC8A320D 5DCA7062 18243566
          5813F1DB C9A0B9DB 5156C6F1 CD018DE1 3868B13A 2319F7C7
          DEA6CD8A DA8D970B 7D006772 4D45E374 9F41E2F9 97B39EA6
          777A53BB 8B85C257 12C70871 52C1E68B 59BE5604 88D31982
          F7894CEF 3980BC6C C772E196 2443178C 715327E8 35485B06
          7B63865F C641560E
```

- Step 2: Decimal and hex values for static shared secret.

```
Z_s =     924234366370804901268583577893351293423293344816231
          915056973308711455580943280535084200238586453736885
          648815535047556078946791023686532083260899167790077
          876264162580798003444862573267131364576172851630222
          567191503512567964107299083652483167987797782978709
          961620605069381163375217900467446582702571545655122
          99

Z_s =     839D8717 4E8F3336 7BAEEEE3 F8A6623E F78570B8 D72202A0
          EF40D94A E8772794 5CD822E4 0FC1DD2B AC3CF907 5B46026E
          25BAEF91 00B2EF2F AB740A5A F65E413B E0C4A287 D1579C8F
          C352B49D 82B4F9F6 C8A9158F 52602E77 E7BFEDDA 9FF71B74
          E1325C8D 864F8CB2 D5C41268 D0C892AC 584F660A AC804EB6
          4A2B8B13 9DEA9C6B
```

- Step 3: Decimal and hex values for ephemeral shared secret.

```
Z_e =     832880520626218737994518384078986244088495866688345
          139042804953264961949746880705934977531022611566427
          487546292239906316090953149966895411574266965386693
          481348338511021092001414942581842340453636876933609
          558258038795986535101728354500760820572077091709533
          458991698412144948116483781373247604473276772491656
          7
```

```
Z_e =     0BDC5116 A5586877 5DAE60B1 FA1C0FEA 9D60C746 1C8F4C70
          3AB0083B 9B73A4A3 E725CA75 A0A12693 6B744F34 8194D298
          C6F692EA 11B2928D 1D407382 309ED0D0 58F3211C B50D5E42
          C009B100 70EAA1CC C55FDE24 313B5A2D 20CAA551 294E4E34
          C1267B85 E6C3C8E5 69FD2BAA B39D4E24 06A3F704 8A2F83FB
          3EB5CF40 BE804F57
```

- Step 4: Shared secret.

```
Z =       0BDC5116 A5586877 5DAE60B1 FA1C0FEA 9D60C746 1C8F4C70
          3AB0083B 9B73A4A3 E725CA75 A0A12693 6B744F34 8194D298
          C6F692EA 11B2928D 1D407382 309ED0D0 58F3211C B50D5E42
          C009B100 70EAA1CC C55FDE24 313B5A2D 20CAA551 294E4E34
          C1267B85 E6C3C8E5 69FD2BAA B39D4E24 06A3F704 8A2F83FB
          3EB5CF40 BE804F57 839D8717 4E8F3336 7BAEEEE3 F8A6623E
          F78570B8 D72202A0 EF40D94A E8772794 5CD822E4 0FC1DD2B
          AC3CF907 5B46026E 25BAEF91 00B2EF2F AB740A5A F65E413B
          E0C4A287 D1579C8F C352B49D 82B4F9F6 C8A9158F 52602E77
          E7BFEDDA 9FF71B74 E1325C8D 864F8CB2 D5C41268 D0C892AC
          584F660A AC804EB6 4A2B8B13 9DEA9C6B
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 60D7FBF4 95126B2A D4D59EDC 44A652E4 223A4BE5 FAC64948
             8BD1AA1D F27981E7 9CA267F8 45996455
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
rU =      D2F8A115 DBD8B2E7 4C5D20BA F5E5C17B E33B844B
```

```
tU =      126B756D D341EF3F 97FB0032 FC8A320D 5DCA7062 18243566
          5813F1DB C9A0B9DB 5156C6F1 CD018DE1 3868B13A 2319F7C7
          DEA6CD8A DA8D970B 7D006772 4D45E374 9F41E2F9 97B39EA6
          777A53BB 8B85C257 12C70871 52C1E68B 59BE5604 88D31982
          F7894CEF 3980BC6C C772E196 2443178C 715327E8 35485B06
          7B63865F C641560E
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     9242343663708049012685835778933512934232933448162 3
          1915056973308711455580943280535084200238586453736 8
          8564881553504755607894679102368653208326089916779 0
          0778762641625807980034448625732671313645761728516 3
          0222567191503512567964107299083652483167987797782 9
          7870996162060506938116337521790046744658270257154 5
          65512299

Z_s =     839D8717 4E8F3336 7BAEEEE3 F8A6623E F78570B8 D72202A0
          EF40D94A E8772794 5CD822E4 0FC1DD2B AC3CF907 5B46026E
          25BAEF91 00B2EF2F AB740A5A F65E413B E0C4A287 D1579C8F
          C352B49D 82B4F9F6 C8A9158F 52602E77 E7BFEDDA 9FF71B74
          E1325C8D 864F8CB2 D5C41268 D0C892AC 584F660A AC804EB6
          4A2B8B13 9DEA9C6B
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     8328805206262187379945183840789862440884958666883 4
          5139042804953264961949746880705934977531022611566 4
          2748754629223990631609095314996689541157426696538 6
          6934813483385110210920014149425818423404536368769 3
          3609558258038795986535101728354500760820572077091 7
          0953345899169841214494811648378137324760447327677 2
          4916567

Z_e =     0BDC5116 A5586877 5DAE60B1 FA1C0FEA 9D60C746 1C8F4C70
```

```
3AB0083B 9B73A4A3 E725CA75 A0A12693 6B744F34 8194D298
C6F692EA 11B2928D 1D407382 309ED0D0 58F3211C B50D5E42
C009B100 70EAA1CC C55FDE24 313B5A2D 20CAA551 294E4E34
C1267B85 E6C3C8E5 69FD2BAA B39D4E24 06A3F704 8A2F83FB
3EB5CF40 BE804F57
```

- Step 5: Shared secret.

```
Z =       0BDC5116 A5586877 5DAE60B1 FA1C0FEA 9D60C746 1C8F4C70
          3AB0083B 9B73A4A3 E725CA75 A0A12693 6B744F34 8194D298
          C6F692EA 11B2928D 1D407382 309ED0D0 58F3211C B50D5E42
          C009B100 70EAA1CC C55FDE24 313B5A2D 20CAA551 294E4E34
          C1267B85 E6C3C8E5 69FD2BAA B39D4E24 06A3F704 8A2F83FB
          3EB5CF40 BE804F57 839D8717 4E8F3336 7BAEEEE3 F8A6623E
          F78570B8 D72202A0 EF40D94A E8772794 5CD822E4 0FC1DD2B
          AC3CF907 5B46026E 25BAEF91 00B2EF2F AB740A5A F65E413B
          E0C4A287 D1579C8F C352B49D 82B4F9F6 C8A9158F 52602E77
          E7BFEDDA 9FF71B74 E1325C8D 864F8CB2 D5C41268 D0C892AC
          584F660A AC804EB6 4A2B8B13 9DEA9C6B
```

- Step 6: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 60D7FBF4 95126B2A D4D59EDC 44A652E4 223A4BE5 FAC64948
             8BD1AA1D F27981E7 9CA267F8 45996455
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     60D7 FBF49512 6B2AD4D5

nonceV =  16FBE030 F5BEB21E E4209928 096248FC D2318FB8
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 126B756D D341EF3F
            97FB0032 FC8A320D 5DCA7062 18243566 5813F1DB C9A0B9DB
            5156C6F1 CD018DE1 3868B13A 2319F7C7 DEA6CD8A DA8D970B
            7D006772 4D45E374 9F41E2F9 97B39EA6 777A53BB 8B85C257
            12C70871 52C1E68B 59BE5604 88D31982 F7894CEF 3980BC6C
            C772E196 2443178C 715327E8 35485B06 7B63865F C641560E
            16FBE030 F5BEB21E E4209928 096248FC D2318FB8

 MacTag_U  = 408B529A 1D231DFD 49DFF1F7 CD5999F5 9BA14443
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 126B756D D341EF3F
            97FB0032 FC8A320D 5DCA7062 18243566 5813F1DB C9A0B9DB
            5156C6F1 CD018DE1 3868B13A 2319F7C7 DEA6CD8A DA8D970B
            7D006772 4D45E374 9F41E2F9 97B39EA6 777A53BB 8B85C257
            12C70871 52C1E68B 59BE5604 88D31982 F7894CEF 3980BC6C
            C772E196 2443178C 715327E8 35485B06 7B63865F C641560E

 MacTag_V  = 24C43F35 FC371FCF 24394724 5363FD1D 46B8193D
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 126B756D D341EF3F
             97FB0032 FC8A320D 5DCA7062 18243566 5813F1DB C9A0B9DB
             5156C6F1 CD018DE1 3868B13A 2319F7C7 DEA6CD8A DA8D970B
             7D006772 4D45E374 9F41E2F9 97B39EA6 777A53BB 8B85C257
             12C70871 52C1E68B 59BE5604 88D31982 F7894CEF 3980BC6C
             C772E196 2443178C 715327E8 35485B06 7B63865F C641560E
             16FBE030 F5BEB21E E4209928 096248FC D2318FB8
```

```
MacTag_U  = E9F7399C 1FE6AE6C D016DDA2 6F096B4B 7AD9FE8F

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 16FBE030 F5BEB21E
            E4209928 096248FC D2318FB8 126B756D D341EF3F 97FB0032
            FC8A320D 5DCA7062 18243566 5813F1DB C9A0B9DB 5156C6F1
            CD018DE1 3868B13A 2319F7C7 DEA6CD8A DA8D970B 7D006772
            4D45E374 9F41E2F9 97B39EA6 777A53BB 8B85C257 12C70871
            52C1E68B 59BE5604 88D31982 F7894CEF 3980BC6C C772E196
            2443178C 715327E8 35485B06 7B63865F C641560E

MacTag_V  = AF5C4636 705CF0ED A3855DE9 EA20F196 282C6FE0
```

3.2.5 MQV1 for finite field p1024-q160

- Prerequisites:

```
xU =      6909DDD0 9BDA3E81 B0E04BA9 F8D2875C 0DCF37EC

yU =      5332EBD1 6525DA37 9DDC5B91 06DDC2C8 F85F35A2 5240F663
          ED517F39 102C3D3C 024DD67A 59400D19 5A72A631 E616D756
          70113601 AEB346F2 A8F7B758 02ACA00C 74D0BE4A 615ED869
          09DBBF16 3887725B 6966B9E4 A0EC986F 5659833C DED7B520
          69023063 D235857F 797C42EA 40221B10 803F5D59 548EAB6A
          C190205B 100DCA88

xV =      B3AE6EFD 1EA0924C 06B4F0EA 9F017085 3633B2AB

yV =      66365B51 BFD2A085 89F89C8F 960F7AC4 6967BC86 58DF6CA4
          65E42275 E8FD0EDC 5607F44E 05869F01 2872BDE3 9622672D
          2D81FF59 8D18D2EF C5A6C010 83E500C5 3674F1AB 6022219C
          6FA7E562 C35FC5C6 8ED23FBC F76CD9B1 1A13F9BF 8341FDB8
          294270A7 B2250DA8 5EEEC3E9 2007C913 B0B3FA7E 9E682336
          2066D88E 440B4F20
```

BEGIN U's calculations

- Step 1:

```
rU =      8DF6F73E A248FB2D 1306E460 730D0C3E 4DDA1B48

tU =      2CCD9DD2 0518A6CE 8626D45E DEAE35AE 988777BA 4AC8B8D3
          FA4AEE8D 9F09ACEA 81D16C20 331640A5 2D2C7EF2 0AB2B86A
          7AF90A52 EDAED6D9 D07677B7 06FBF346 21863617 EE1CB349
          284440B9 FEFA8DE5 AF85A9D1 B4917493 437E362F 7410797F
          B0401DE8 276C5F35 99DACFFD 00CE6C4F 177B82BB AC3E0120
          3B0024A3 753A363B
```

- Step 2: Decimal value for shared secret.

```
Z =       30301066471863050392462684369692479368802453611053
          45089560750700078591012349558968256235574756593057
          10547793969417273421989399662742145877913451980146
          69903750727178114963856928000908484187980089576834
          12508815859765603715712913508827219613279049255060
          61360605212234013402419483623823373442987647696916
          8072873
```

- Step 3: Hex value for shared secret.

```
Z =       0450A4D4 53953CCF D4F39867 161780C6 8CE329EC 24E824E2
          E5CA295D E5371C7D 80B4B826 0848586C E316DB58 00F651C0
          D4835C35 D78792B7 41B7AFB1 BADAF7F7 D167A2D3 BB3ACFB0
          D8C44AA4 FCE86832 5F97758D DD9254CF B1D1872F 9542C5BE
          3735A7CA CBE25CD3 578E2639 04B64B92 CD201F09 38FDFA43
          DB153380 EB66F0A9
```

- Step 4: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 7849B1BA C97AF822 8666735F 2CC3914C 4650B70B 51C57C86
             375BCFB1 B87C434D C9E5F63A 10414A15
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
rU =      8DF6F73E A248FB2D 1306E460 730D0C3E 4DDA1B48

tU =      2CCD9DD2 0518A6CE 8626D45E DEAE35AE 988777BA 4AC8B8D3
          FA4AEE8D 9F09ACEA 81D16C20 331640A5 2D2C7EF2 0AB2B86A
          7AF90A52 EDAED6D9 D07677B7 06FBF346 21863617 EE1CB349
          284440B9 FEFA8DE5 AF85A9D1 B4917493 437E362F 7410797F
          B0401DE8 276C5F35 99DACFFD 00CE6C4F 177B82BB AC3E0120
          3B0024A3 753A363B
```

- Step 2: N/A.

- Step 3: Decimal value for shared secret.

```
Z =       30301066471863050392462684369692479368802453611053
          45089560750700078591012349558968256235574756593057
          10547793969417273421989399662742145877913451980146
          69903750727178114963856928000908484187980089576834
          12508815859765603715712913508827219613279049255060
          61360605212234013402419483623823373442987647696916
          8072873
```

- Step 4: Hex value for shared secret.

```
Z =       0450A4D4 53953CCF D4F39867 161780C6 8CE329EC 24E824E2
          E5CA295D E5371C7D 80B4B826 0848586C E316DB58 00F651C0
          D4835C35 D78792B7 41B7AFB1 BADAF7F7 D167A2D3 BB3ACFB0
          D8C44AA4 FCE86832 5F97758D DD9254CF B1D1872F 9542C5BE
          3735A7CA CBE25CD3 578E2639 04B64B92 CD201F09 38FDFA43
          DB153380 EB66F0A9
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 7849B1BA C97AF822 8666735F 2CC3914C 4650B70B 51C57C86
             375BCFB1 B87C434D C9E5F63A 10414A15
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     7849 B1BAC97A F8228666

nonceV =  15901F58 CC49C997 A955AF26 4946F302 0567CC55
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 2CCD9DD2 0518A6CE
            8626D45E DEAE35AE 988777BA 4AC8B8D3 FA4AEE8D 9F09ACEA
            81D16C20 331640A5 2D2C7EF2 0AB2B86A 7AF90A52 EDAED6D9
            D07677B7 06FBF346 21863617 EE1CB349 284440B9 FEFA8DE5
            AF85A9D1 B4917493 437E362F 7410797F B0401DE8 276C5F35
            99DACFFD 00CE6C4F 177B82BB AC3E0120 3B0024A3 753A363B
            15901F58 CC49C997 A955AF26 4946F302 0567CC55

MacTag_U  = 95C0E106 D988E6A0 9F48B52B A8B211E9 FA70D19C
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 2CCD9DD2 0518A6CE
            8626D45E DEAE35AE 988777BA 4AC8B8D3 FA4AEE8D 9F09ACEA
            81D16C20 331640A5 2D2C7EF2 0AB2B86A 7AF90A52 EDAED6D9
            D07677B7 06FBF346 21863617 EE1CB349 284440B9 FEFA8DE5
            AF85A9D1 B4917493 437E362F 7410797F B0401DE8 276C5F35
            99DACFFD 00CE6C4F 177B82BB AC3E0120 3B0024A3 753A363B
```

```
MacTag_V  = 234F4696 4F442EDB B767994D 6F3AE3B2 B9CA9174
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 2CCD9DD2 0518A6CE
            8626D45E DEAE35AE 988777BA 4AC8B8D3 FA4AEE8D 9F09ACEA
            81D16C20 331640A5 2D2C7EF2 0AB2B86A 7AF90A52 EDAED6D9
            D07677B7 06FBF346 21863617 EE1CB349 284440B9 FEFA8DE5
            AF85A9D1 B4917493 437E362F 7410797F B0401DE8 276C5F35
            99DACFFD 00CE6C4F 177B82BB AC3E0120 3B0024A3 753A363B
            15901F58 CC49C997 A955AF26 4946F302 0567CC55

MacTag_U  = 3AF6EA6D F917A5D3 787EFB53 6EF0AEBC 1CC01042

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 15901F58 CC49C997
            A955AF26 4946F302 0567CC55 2CCD9DD2 0518A6CE 8626D45E
            DEAE35AE 988777BA 4AC8B8D3 FA4AEE8D 9F09ACEA 81D16C20
            331640A5 2D2C7EF2 0AB2B86A 7AF90A52 EDAED6D9 D07677B7
            06FBF346 21863617 EE1CB349 284440B9 FEFA8DE5 AF85A9D1
            B4917493 437E362F 7410797F B0401DE8 276C5F35 99DACFFD
            00CE6C4F 177B82BB AC3E0120 3B0024A3 753A363B

MacTag_V  = BC6BAB06 2F55A228 52E848A2 0A5CC496 8E63430D
```

3.2.6 dhOneFlow for finite field p1024-q160

- Prerequisites:

```
xV =      773E35A0 38EC0573 200ADEB8 55725EDD 3526D03D
```

```
yV =      824753E5 B95439D2 3D673084 D34C6D4B 7337706C 2CDA9A71
          30EAC18A C9774CEF 81083211 9A4A402D 40500284 5C464D4D
          766C56EC 4039D954 7CF20867 02BE2D31 6E804DEA A1DFC82F
          D794789A D67C11D1 A599CE83 9B778FC7 C269DF84 C5C8B93B
          17A9B05B 446C9FE6 2F082C80 78512968 AD0EA1B1 38F4D0F5
          267AF3DD 130D03CA
```

BEGIN U's calculations

- Step 1:

```
rU =      57E700B4 ED7EAB54 F5B86A6A D9BB390A 0288C123

tU =      9B4E7F1B 15216504 0D261882 00FF423B 696C024E CCC7BCD9
          F8CE63BF 17C53A28 77504673 7745F85C 3B1925EC 6B25F8AA
          AB72FDB4 AC4D1A88 59D92A7D 25454CC0 0413B903 0F98A822
          6EF0958F 18518343 8895B4BF 0C0CD12B 8D72FF93 B9799B55
          61CBB9F1 4C6BDD74 9DA83FA6 D2E162A6 468DF7AF 3C4DF818
          9DF63FBD EE42DC73
```

- Step 2: Decimal value for shared secret.

```
Z =       863858053820000536101604553560423556911758758428 82
          490110128866297267340650423857092211652172811702 68
          349522790613436904972294276159127397780613004903 19
          864903064393529292642685826191210428831016779852 66
          604749931617701761154981744555569556465461307162 29
          454968263493934833414109723822352189273338427187 49
          53019563
```

- Step 3: Hex value for shared secret.

```
Z =       7B0478EE 8B3B8C52 D0D4BD1D 31E2D4F6 3B0D6343 33B27D02
          570FC855 638E2BFD A746D86F 6D7969B8 02B4B5AA 06B8039F
          36A3843C 5684C3AE 91E1E647 31906578 B99E982C 7AB372D3
          610BC3DE FCFDE1C1 E993C6C0 9906E1A7 FD237648 26EB0B8B
          EFAEB84F 54C1E677 11F8DC54 BE1DC4D2 0CA1BFE9 1BD8DCC9
          8A4B8D22 3B9380AB
```

- Step 4: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 42E4B5B2 1C61F9F6 8657D5BE 0630CC73 22B5C620 F45A7AA5
             A841C0ED 7B2D469F 8F416AE2 6E0B4EB3
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
rU =      57E700B4 ED7EAB54 F5B86A6A D9BB390A 0288C123

tU =      9B4E7F1B 15216504 0D261882 00FF423B 696C024E CCC7BCD9
          F8CE63BF 17C53A28 77504673 7745F85C 3B1925EC 6B25F8AA
          AB72FDB4 AC4D1A88 59D92A7D 25454CC0 0413B903 0F98A822
          6EF0958F 18518343 8895B4BF 0C0CD12B 8D72FF93 B9799B55
          61CBB9F1 4C6BDD74 9DA83FA6 D2E162A6 468DF7AF 3C4DF818
          9DF63FBD EE42DC73
```

- Step 2: N/A.

- Step 3: Decimal value for shared secret.

```
Z =       863858053820000536101604553560423556911758758428824
          901101288662972673406504238570922116521728117026834
          952279061343690497229427615912739778061300490319864
          903064393529292642685826191210428831016779852666047
          499316177017611549817445555695564654613071622945496
          826349393483341410972382235218927333842718749530195
          63
```

- Step 4: Hex value for shared secret.

```
Z =       7B0478EE 8B3B8C52 D0D4BD1D 31E2D4F6 3B0D6343 33B27D02
          570FC855 638E2BFD A746D86F 6D7969B8 02B4B5AA 06B8039F
          36A3843C 5684C3AE 91E1E647 31906578 B99E982C 7AB372D3
          610BC3DE FCFDE1C1 E993C6C0 9906E1A7 FD237648 26EB0B8B
          EFAEB84F 54C1E677 11F8DC54 BE1DC4D2 0CA1BFE9 1BD8DCC9
          8A4B8D22 3B9380AB
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 42E4B5B2 1C61F9F6 8657D5BE 0630CC73 22B5C620 F45A7AA5
             A841C0ED 7B2D469F 8F416AE2 6E0B4EB3
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     42E4 B5B21C61 F9F68657
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 9B4E7F1B 15216504
            0D261882 00FF423B 696C024E CCC7BCD9 F8CE63BF 17C53A28
            77504673 7745F85C 3B1925EC 6B25F8AA AB72FDB4 AC4D1A88
            59D92A7D 25454CC0 0413B903 0F98A822 6EF0958F 18518343
            8895B4BF 0C0CD12B 8D72FF93 B9799B55 61CBB9F1 4C6BDD74
            9DA83FA6 D2E162A6 468DF7AF 3C4DF818 9DF63FBD EE42DC73

MacTag_V  = 7DFBA088 B114C4F1 54BC4047 4933EAFE C80C9FFB
```

3.2.7 dhStatic for finite field p1024-q160

- Prerequisites:

```
xU =      DD28462C AC7658BE 6F1806CA BC435304 A3A51D5A

yU =      08365D7F 27B6C9D1 F2F2E925 1C46A2DF E87332AD 3D4C4DC1
          13E5E180 CDC42C32 3D1772BF 2880F4B6 B246A69E 6AD8083F
          2704D4AE CAC5172D 00DB2C9D 964FDBEF 1DE2ED14 ABD687A1
          AD0FA6F8 C01A1F9F 32CEEA77 66B59347 FAF2F6B9 21C0CBA8
          25E64D6D C5361F69 F20D0853 F820E87A A729FC83 895C4010
          1B468441 5D47E654

xV =      6C6EFE04 09135D6F D406F60A 9609ABED 57404EE5

yV =      AC3EAB02 475A58D1 9FEE6492 BEA430D5 7A426731 05CA4731
          F858D16C 967FEC16 8544BD09 9BF7B3E3 FF584B78 78FEF175
          B70E01E2 CCDF0751 E056A48A 0E79E37F 7BFA8C41 3BBDEB03
          2088D5AA 860AAA2E 546A084C 194C06C2 564B4680 A28DF042
          C2483147 45C040E8 C1B4272E 6148C8D6 407FCB58 85C1A6D4
          81D3C9A5 745B08FF
```

BEGIN U's calculations

- Step 1:

```
nonceU =  7F4499AD 3FF48D5F 896D3D6D 57441882 8AD1E9D7
```

- Step 2: Decimal value for shared secret.

```
Z =       113824278728014466610682734514049357429416015312 03
          862003993337492744979863845333445336518032325929 31
          946674199773242857397965238191201173366346729438 67
          113583223520483853608874763576246115268530814767 41
          919511715398538849541195186217239239421251171144 93
          136218986191540597379229220294149868619531603249 61
          829911576
```

- Step 3: Hex value for shared secret.

```
Z =       A21755D2 EC96FFEA DABB3549 01E0DE52 0D7D0975 947B4385
          E4E6A7C1 F2E86337 7C1097B2 9FBBB515 15043A70 586D4437
          647CC60B 4EC32B1B DA78A506 8F1A819D 3EC51827 727A23D2
          E0E12D88 A59DC26B B94C795A C0F2A3B2 F37AF574 246E9D97
          38829996 BB260DD2 EFCB5EEB 6E6E7039 3D04A4CC 08D5F674
          B4C06166 7BE3FC18
```

- Step 4: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000014 7F4499AD
             3FF48D5F 896D3D6D 57441882 8AD1E9D7 424F4242 59343536

DerKeyMat  = 5B88AC5B 39DD7957 B2B5D53A 2CCB1CDA E3CB3E40 C9DCA5E0
             02FAD34B CB1574C4 D615B0DF DEF66B5E
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
nonceU =  7F4499AD 3FF48D5F 896D3D6D 57441882 8AD1E9D7
```

- Step 2: Decimal value for shared secret.

```
Z =       113824278728014466610682734514049357429416015312 03
          862003993337492744979863845333445336518032325929 31
          946674199773242857397965238191201173366346729438 67
          113583223520483853608874763576246115268530814767 41
          919511715398538849541195186217239239421251171144 93
          136218986191540597379229220294149868619531603249 61
          829911576
```

- Step 3: Hex value for shared secret.

```
Z =       A21755D2 EC96FFEA DABB3549 01E0DE52 0D7D0975 947B4385
          E4E6A7C1 F2E86337 7C1097B2 9FBBB515 15043A70 586D4437
          647CC60B 4EC32B1B DA78A506 8F1A819D 3EC51827 727A23D2
          E0E12D88 A59DC26B B94C795A C0F2A3B2 F37AF574 246E9D97
          38829996 BB260DD2 EFCB5EEB 6E6E7039 3D04A4CC 08D5F674
          B4C06166 7BE3FC18
```

- Step 4: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000014 7F4499AD
             3FF48D5F 896D3D6D 57441882 8AD1E9D7 424F4242 59343536

DerKeyMat  = 5B88AC5B 39DD7957 B2B5D53A 2CCB1CDA E3CB3E40 C9DCA5E0
             02FAD34B CB1574C4 D615B0DF DEF66B5E
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     5B88 AC5B39DD 7957B2B5

nonceV =  7DA093C4 7B8CDFF5 84DE7EAF 0D1042B1 721B98C9
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 7F4499AD 3FF48D5F
            896D3D6D 57441882 8AD1E9D7 7DA093C4 7B8CDFF5 84DE7EAF
            0D1042B1 721B98C9

MacTag_U  = FE712164 E328B17C D871F86B 666A4A33 452A4156
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U
```

```
          = 4B435F31 5F56424F 42425941 4C494345 7F4499AD 3FF48D5F
            896D3D6D 57441882 8AD1E9D7

MacTag_V  = 4C557E8C C3431FD7 F8FED556 FF2C8DBD 069745A9
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 7F4499AD 3FF48D5F
            896D3D6D 57441882 8AD1E9D7 7DA093C4 7B8CDFF5 84DE7EAF
            0D1042B1 721B98C9

MacTag_U  = E1F04D3D 40B33EC0 5CF643B9 0CB3A57C 311EFB0B

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 7DA093C4 7B8CDFF5
            84DE7EAF 0D1042B1 721B98C9 7F4499AD 3FF48D5F 896D3D6D
            57441882 8AD1E9D7

MacTag_V  = A5B7C606 9C7CEBD6 C17A3D43 CE8785DF 9EFBED0F
```

3.3 Test data for 2048–bit prime p and 224–bit prime q

In this section, we supply step–by–step test data for the seven finite field key agreement schemes described in [1, section 6] using the parameter set $p2048$–$q224$ described in Section 2.2. For each scheme, a reference to the corresponding section in [1] is provided.

3.3.1 dhHybrid1 for finite field p2048-q224

- Prerequisites:

```
xU =      361B8A2F 5C87DB85 D9CD87D9 CC97AABE 72DCE9D1 49281755
          F717D4CC

yU =      8D3CFCE5 1A57018F 59B1285E 89599F23 7F055466 B12ACDF1
          851726FE FD0CF516 A7CB0A1B 1637AC96 7A9DCC3A 2B5AF378
          BCA6607C 885722B2 89BC5599 B8DB5268 03638866 0630EBC8
          4A4B867F CDE82C24 C14C0100 67D46824 33203236 180D9287
          1818A3EC CFD796AE C5368E71 7EF9E3BC 33AD313E C60D273C
          0E24DF89 699F897B B09AA1FB 43FD34CD DD7C6868 CCB4E4A1
          6C802A7A C85F83CC AA793C03 E5310D65 74419F24 0706A00E
          C5D2AFA4 EE37D2C2 018E2D32 9D84ECCE 52CF33E4 B3D50BD6
          ED964FAF 1FF32F2B 2528BF4E 9B3B8A0D 969BCBBC CBFD88A9
          79A6DF1E 70807388 8E690D7E C23CE5F1 1E39688E AA6318EE
          995CE214 4272AF63 2860B064 EF8CD6E0

xV =      5954B770 B96ACF4A 454FE097 79AA7097 B79043B1 8CEC7CCA
          20C0CC4E

yV =      4E7B04A8 6BE05024 0D9EA891 087DE96F F77481FD 877475C2
          B69E0A42 2B0905C3 E6AB9D37 F2D5D0B3 6117FCA2 005E4F15
          558A5892 ABAEBCD8 7E7AA625 4AB40BB0 8FCFD9A5 FFD99816
          6FD365CF E1F7F265 FA846066 ABFA01B6 2DCE81C9 ED3B8E28
          31CCEE5E A30BEBCF 7D13C9B0 4D202BC3 A49D6743 339DBDF3
          5CA71061 00AB51D6 61DAE8BA 04CA4F0E 81783E59 8625A9D0
          9DAD3320 749720B9 E4EE32AA 593181F0 AC5A5571 4BB583BE
          080D7E4F 82E01564 EE8CCDFD EB006986 1E34F167 2CC2977D
          02206A37 749DF25F 54B4416B 8F92CEB8 2F6730D2 24ACE2F8
          8CBB755F B5B99742 B3F4349E BECED7F5 7E0A9BE0 AC8A6443
          87E5E055 8467F894 BAD31EC4 F652FB6B
```

- Step 1: U produces rU, tU and receives tV. U DOES NOT RECEIVE rV (shown only for the purpose of verifying this data).

```
rU =      5BDA41AF C04B07FD 026EE955 442DA60E 9B1A1ED2 01937429
          1846DE03

tU =      47995178 AB474833 B204F701 5163D73C EDCDBB99 EA5B76D0
          5750E827 79B99DED 1DC09BA2 B2249432 4BB97796 5FEEA6BC
          504F06F9 A9823BE3 3FD23270 388B1947 3822341E CBE91C21
          2A8A971C 6CD07E9C F8FEA4CB 81C90E34 176187A5 956040E0
          79A25AA8 6FD132B4 9F97C7D8 FB4B4963 135BD78C 3EDA7C7D
          B3B20170 FFA0804E 34DF99D9 DB395B5D 47A0ADCF BB411529
          FFA0A2CE 49FDFF58 2007178F 122898C3 0B55CBA2 14B03C3D
          9E811E5C 6BB29699 0DC16B89 44BFA0BC FEB194F8 092D705D
          889DB411 99F62D56 6EB2C356 6F5EFF41 ED76DEF5 209DAB34
          568DF833 11756844 5FDDD641 35FA6365 AEF79942 EBC6BB15
          3EB16E9D B4BB0E36 7A5B1C86 C3150072

rV =      590154D3 DABEE8DF B7753E99 CBD5831A FE132F14 9B07EB3E
          6616350E

tV =      76F70EAA DB78DF7C FD55091B D4F7620A EDA3BBA1 CF8D3C83
          AF54A65D C166A7EB FD24A563 1482FDBD 1309086A 87EA0EC5
          BA788A13 4B39CB45 5AC453D3 09FDAD6D 42766B0D 3CAC00F7
          F5F9D4BD 6E725821 C446938F 543CBB4D 9DDF3A7F DA48019A
          D74BDCB3 ED77F757 3AEE0910 3FFE2F85 806D1A4E 4F35456C
          D55BF262 4AB633A5 BA7A7910 3D9C82C0 D262DA05 29BED1A4
          E3A61211 D078EA2A 34FBEC8F D4B9FF60 AADFFE84 CD169890
          6E3CDC9A 35D06F0B 0D19E29A 58437BD3 CD77A2D9 B5450A35
          1EF62CBF 5ABEE183 13B4BB2D F588BB2B 6898F128 60F578BD
          9924869E 56ED5565 A686ACD6 53B7348C 97CCAB97 383A2E02
          C973DCB0 CF639284 C76CE9F2 82DCD706
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     20252066589364048951892493404684015744359324165150
          05315498731679745093891334013961749899842993917244
          03433835573138424908323284124873403406994004827913
```

```
456572847024828133230722723159713254001193957946 21
016866049181079827006416790968517207048559775944 39
171570335305599261742820889683896592704983962116 32
589560141497768558663884254933534839851403656285 65
052198465563751345221325263426935574434853349797 26
927403366943364029135022251792526267460519147494 23
258267301270434739034714203007112768505632504349 24
354495747986199545501200186481098782919302825790 21
135502134225574312623841222377046704518917830174 48
62990396277987462
```

```
Z_s =     A06D618A FF67B8A9 87163563 E4E88D8F 9CD0B301 CED78D60
          6136A046 70A35DC0 14A06E17 EAB03025 938CA27E 0010FC93
          800FD93C 37A5E7DE E45A1367 62A7D5BD C38B7094 4FB36E17
          137CEBAE 057F8019 946EDAEB 71B60D42 A8D09FE1 BB8A3418
          13A9D36A 73FDFB97 CFCFB448 CE164A92 78EC7263 5D3EF928
          F9B4BAF0 FE0ED279 193E51FB 7427B2C1 152A8C0E 4E519C2B
          A9C1A145 AFF0458C 7F99C755 4DC5F2A7 22361C42 69E6D212
          2AEA8153 92F0DCAD 0C8EB714 8B89FB42 B862C518 48C4C1EE
          ABE6ED0A E15EAA72 1EF48A58 9B3427C3 4950DDC9 7500E37A
          66BECD84 D55008DC 46E7C639 4B03C388 7C51F4A0 2B7B634C
          CBF6809E DAB0FD20 DCDAC833 25791886
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     203655326136066234832973412029041858016712020549 23
          105408094143911561851672507404759668652789552045 96
          401597868773141058405111095475814218034079118512 66
          529951877991374877835807274239266202906031985454 36
          613722420735712860714382427537947282472732315628 93
          577149073193934845817263296089985332183913896188 63
          374869030440866008329679908846387545323859634179 91
          760540270139352037986900306086687261864301661266 80
          483601403647566836448577274891699980613179093683 72
          267240612021975327066441554269304410613501940338 37
          367340068600441800254406963247585238111825680892 44
          293443572648833294303678379940293146053923187443 47
          29400470221892695
```

```
Z_e =     A1537AE0 3112D671 6ABE14C1 44BA915B 3C9E92BF 65FB7609
          7798C962 1529580D 881C0359 3FEAC70B AC74A167 A43D10ED
          B8878DE2 F14B77F2 954235A5 AB24ED01 DC10950F D8CDADDD
          74385936 3C156544 5DBFDE9F D0A51A0A 15BAA9F4 A91E3EC4
          E5D99425 7F8EF1C2 6FB8791D 82FDB494 74E39C3C D46D9901
          C77D6858 E20AC4E2 619BE78E 708C71EB CB431CFF 419FE486
          4AE33B5A 106BE7CF 362F6163 EAA5252C B54E74AB 4D1F9414
          3E05EA44 B3F3A9DC BC364B62 C08BC749 2BEB6E75 CA810283
          22657271 3D37F03B 533933D9 CEC97CD9 DD2AF106 9CA47F12
          D374416D 032469CD A251F746 863C9303 8B316904 AC1543C1
          312C4DAC 94D7E262 CA29798A 8B5C2C57
```

- Step 5: Shared secret.

```
Z =       A1537AE0 3112D671 6ABE14C1 44BA915B 3C9E92BF 65FB7609
          7798C962 1529580D 881C0359 3FEAC70B AC74A167 A43D10ED
          B8878DE2 F14B77F2 954235A5 AB24ED01 DC10950F D8CDADDD
          74385936 3C156544 5DBFDE9F D0A51A0A 15BAA9F4 A91E3EC4
          E5D99425 7F8EF1C2 6FB8791D 82FDB494 74E39C3C D46D9901
          C77D6858 E20AC4E2 619BE78E 708C71EB CB431CFF 419FE486
          4AE33B5A 106BE7CF 362F6163 EAA5252C B54E74AB 4D1F9414
          3E05EA44 B3F3A9DC BC364B62 C08BC749 2BEB6E75 CA810283
          22657271 3D37F03B 533933D9 CEC97CD9 DD2AF106 9CA47F12
          D374416D 032469CD A251F746 863C9303 8B316904 AC1543C1
          312C4DAC 94D7E262 CA29798A 8B5C2C57 A06D618A FF67B8A9
          87163563 E4E88D8F 9CD0B301 CED78D60 6136A046 70A35DC0
          14A06E17 EAB03025 938CA27E 0010FC93 800FD93C 37A5E7DE
          E45A1367 62A7D5BD C38B7094 4FB36E17 137CEBAE 057F8019
          946EDAEB 71B60D42 A8D09FE1 BB8A3418 13A9D36A 73FDFB97
          CFCFB448 CE164A92 78EC7263 5D3EF928 F9B4BAF0 FE0ED279
          193E51FB 7427B2C1 152A8C0E 4E519C2B A9C1A145 AFF0458C
          7F99C755 4DC5F2A7 22361C42 69E6D212 2AEA8153 92F0DCAD
          0C8EB714 8B89FB42 B862C518 48C4C1EE ABE6ED0A E15EAA72
          1EF48A58 9B3427C3 4950DDC9 7500E37A 66BECD84 D55008DC
          46E7C639 4B03C388 7C51F4A0 2B7B634C CBF6809E DAB0FD20
          DCDAC833 25791886
```

- Step 6: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 17F52010 17D14F6F 6D370C0F 842511A4 004FE70D 55732BD0
             8CFD2D3B B3C5A5A8 60492D19 7D4E92CF 51C6863E D1DAA58B
             57038EB4 16B911D1
```

- If key confirmation is performed, then

```
MacKey  =     17F5 201017D1 4F6F6D37 0C0F8425
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 47995178 AB474833
            B204F701 5163D73C EDCDBB99 EA5B76D0 5750E827 79B99DED
            1DC09BA2 B2249432 4BB97796 5FEEA6BC 504F06F9 A9823BE3
            3FD23270 388B1947 3822341E CBE91C21 2A8A971C 6CD07E9C
            F8FEA4CB 81C90E34 176187A5 956040E0 79A25AA8 6FD132B4
            9F97C7D8 FB4B4963 135BD78C 3EDA7C7D B3B20170 FFA0804E
            34DF99D9 DB395B5D 47A0ADCF BB411529 FFA0A2CE 49FDFF58
            2007178F 122898C3 0B55CBA2 14B03C3D 9E811E5C 6BB29699
            0DC16B89 44BFA0BC FEB194F8 092D705D 889DB411 99F62D56
            6EB2C356 6F5EFF41 ED76DEF5 209DAB34 568DF833 11756844
            5FDDD641 35FA6365 AEF79942 EBC6BB15 3EB16E9D B4BB0E36
            7A5B1C86 C3150072 76F70EAA DB78DF7C FD55091B D4F7620A
            EDA3BBA1 CF8D3C83 AF54A65D C166A7EB FD24A563 1482FDBD
            1309086A 87EA0EC5 BA788A13 4B39CB45 5AC453D3 09FDAD6D
            42766B0D 3CAC00F7 F5F9D4BD 6E725821 C446938F 543CBB4D
            9DDF3A7F DA48019A D74BDCB3 ED77F757 3AEE0910 3FFE2F85
            806D1A4E 4F35456C D55BF262 4AB633A5 BA7A7910 3D9C82C0
            D262DA05 29BED1A4 E3A61211 D078EA2A 34FBEC8F D4B9FF60
            AADFFE84 CD169890 6E3CDC9A 35D06F0B 0D19E29A 58437BD3
            CD77A2D9 B5450A35 1EF62CBF 5ABEE183 13B4BB2D F588BB2B
            6898F128 60F578BD 9924869E 56ED5565 A686ACD6 53B7348C
            97CCAB97 383A2E02 C973DCB0 CF639284 C76CE9F2 82DCD706
```

```
MacTag_U  = 73A777EB 02C9E7D6 73DD0011 2E34F079 EC1105DC 9BF92EA1
            E55BA9C1
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 76F70EAA DB78DF7C
            FD55091B D4F7620A EDA3BBA1 CF8D3C83 AF54A65D C166A7EB
            FD24A563 1482FDBD 1309086A 87EA0EC5 BA788A13 4B39CB45
            5AC453D3 09FDAD6D 42766B0D 3CAC00F7 F5F9D4BD 6E725821
            C446938F 543CBB4D 9DDF3A7F DA48019A D74BDCB3 ED77F757
            3AEE0910 3FFE2F85 806D1A4E 4F35456C D55BF262 4AB633A5
            BA7A7910 3D9C82C0 D262DA05 29BED1A4 E3A61211 D078EA2A
            34FBEC8F D4B9FF60 AADFFE84 CD169890 6E3CDC9A 35D06F0B
            0D19E29A 58437BD3 CD77A2D9 B5450A35 1EF62CBF 5ABEE183
            13B4BB2D F588BB2B 6898F128 60F578BD 9924869E 56ED5565
            A686ACD6 53B7348C 97CCAB97 383A2E02 C973DCB0 CF639284
            C76CE9F2 82DCD706 47995178 AB474833 B204F701 5163D73C
            EDCDBB99 EA5B76D0 5750E827 79B99DED 1DC09BA2 B2249432
            4BB97796 5FEEA6BC 504F06F9 A9823BE3 3FD23270 388B1947
            3822341E CBE91C21 2A8A971C 6CD07E9C F8FEA4CB 81C90E34
            176187A5 956040E0 79A25AA8 6FD132B4 9F97C7D8 FB4B4963
            135BD78C 3EDA7C7D B3B20170 FFA0804E 34DF99D9 DB395B5D
            47A0ADCF BB411529 FFA0A2CE 49FDFF58 2007178F 122898C3
            0B55CBA2 14B03C3D 9E811E5C 6BB29699 0DC16B89 44BFA0BC
            FEB194F8 092D705D 889DB411 99F62D56 6EB2C356 6F5EFF41
            ED76DEF5 209DAB34 568DF833 11756844 5FDDD641 35FA6365
            AEF79942 EBC6BB15 3EB16E9D B4BB0E36 7A5B1C86 C3150072

MacTag_V  = CF492264 724A320F 2EE6DD00 4D95C369 07224763 B23FCCDA
            BC1AF51B
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
            = 4B435F32 5F55414C 49434542 4F424259 47995178 AB474833
              B204F701 5163D73C EDCDBB99 EA5B76D0 5750E827 79B99DED
              1DC09BA2 B2249432 4BB97796 5FEEA6BC 504F06F9 A9823BE3
              3FD23270 388B1947 3822341E CBE91C21 2A8A971C 6CD07E9C
              F8FEA4CB 81C90E34 176187A5 956040E0 79A25AA8 6FD132B4
              9F97C7D8 FB4B4963 135BD78C 3EDA7C7D B3B20170 FFA0804E
              34DF99D9 DB395B5D 47A0ADCF BB411529 FFA0A2CE 49FDFF58
              2007178F 122898C3 0B55CBA2 14B03C3D 9E811E5C 6BB29699
              0DC16B89 44BFA0BC FEB194F8 092D705D 889DB411 99F62D56
              6EB2C356 6F5EFF41 ED76DEF5 209DAB34 568DF833 11756844
              5FDDD641 35FA6365 AEF79942 EBC6BB15 3EB16E9D B4BB0E36
              7A5B1C86 C3150072 76F70EAA DB78DF7C FD55091B D4F7620A
              EDA3BBA1 CF8D3C83 AF54A65D C166A7EB FD24A563 1482FDBD
              1309086A 87EA0EC5 BA788A13 4B39CB45 5AC453D3 09FDAD6D
              42766B0D 3CAC00F7 F5F9D4BD 6E725821 C446938F 543CBB4D
              9DDF3A7F DA48019A D74BDCB3 ED77F757 3AEE0910 3FFE2F85
              806D1A4E 4F35456C D55BF262 4AB633A5 BA7A7910 3D9C82C0
              D262DA05 29BED1A4 E3A61211 D078EA2A 34FBEC8F D4B9FF60
              AADFFE84 CD169890 6E3CDC9A 35D06F0B 0D19E29A 58437BD3
              CD77A2D9 B5450A35 1EF62CBF 5ABEE183 13B4BB2D F588BB2B
              6898F128 60F578BD 9924869E 56ED5565 A686ACD6 53B7348C
              97CCAB97 383A2E02 C973DCB0 CF639284 C76CE9F2 82DCD706

 MacTag_U   = F8ECD2E9 534940EA CEA46BD2 67F4AA62 53F7D3CD BB3FFC86
              12179B87

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

            = 4B435F32 5F56424F 42425941 4C494345 76F70EAA DB78DF7C
              FD55091B D4F7620A EDA3BBA1 CF8D3C83 AF54A65D C166A7EB
              FD24A563 1482FDBD 1309086A 87EA0EC5 BA788A13 4B39CB45
              5AC453D3 09FDAD6D 42766B0D 3CAC00F7 F5F9D4BD 6E725821
              C446938F 543CBB4D 9DDF3A7F DA48019A D74BDCB3 ED77F757
              3AEE0910 3FFE2F85 806D1A4E 4F35456C D55BF262 4AB633A5
              BA7A7910 3D9C82C0 D262DA05 29BED1A4 E3A61211 D078EA2A
              34FBEC8F D4B9FF60 AADFFE84 CD169890 6E3CDC9A 35D06F0B
              0D19E29A 58437BD3 CD77A2D9 B5450A35 1EF62CBF 5ABEE183
```

```
              13B4BB2D F588BB2B 6898F128 60F578BD 9924869E 56ED5565
              A686ACD6 53B7348C 97CCAB97 383A2E02 C973DCB0 CF639284
              C76CE9F2 82DCD706 47995178 AB474833 B204F701 5163D73C
              EDCDBB99 EA5B76D0 5750E827 79B99DED 1DC09BA2 B2249432
              4BB97796 5FEEA6BC 504F06F9 A9823BE3 3FD23270 388B1947
              3822341E CBE91C21 2A8A971C 6CD07E9C F8FEA4CB 81C90E34
              176187A5 956040E0 79A25AA8 6FD132B4 9F97C7D8 FB4B4963
              135BD78C 3EDA7C7D B3B20170 FFA0804E 34DF99D9 DB395B5D
              47A0ADCF BB411529 FFA0A2CE 49FDFF58 2007178F 122898C3
              0B55CBA2 14B03C3D 9E811E5C 6BB29699 0DC16B89 44BFA0BC
              FEB194F8 092D705D 889DB411 99F62D56 6EB2C356 6F5EFF41
              ED76DEF5 209DAB34 568DF833 11756844 5FDDD641 35FA6365
              AEF79942 EBC6BB15 3EB16E9D B4BB0E36 7A5B1C86 C3150072

MacTag_V  = 9146D57E CB84DF15 21DA79AF B9AD1851 4CE85DE9 D75077B6
            6920D577
```

3.3.2 MQV2 for finite field p2048-q224

- Prerequisites:

```
xU =      67679081 9B50C6C3 9C775586 1F7EBF5D 95146031 6CEACC0D
          CF3F2755

yU =      5403791A 9FD9121D E4B16472 109CEABD 2FA6941F 6993DAC8
          CF17B928 25C78DC0 5F597368 83B3AD1E AE8F4D57 97ABF3CA
          4AF3242E 6311D98F B9ED4925 9CBB709C 3F6991D5 554101CF
          10ACED55 7D9F8DC6 AF1800EB D2A64EB8 49FEE5C8 213EC872
          8F8E6C33 0D49FDB2 1BA4C74B 285416CF 7A5252A7 049B0C51
          BB26C1D0 717C91A5 A74E73A7 5AFCB778 18A92CB4 AAD1E7ED
          D2CBB305 3CA3E87D 970EBC24 B3CB2684 4F66C61C 4A4A83AC
          4EAD8EA9 7775F85C F278D704 1E8DA41D 257A131D 69E3BD0C
          55627DF4 6CD3BD24 F3C29B04 F59B1E37 13AB9E37 4CE66B6A
          3A8220AE F41F0FC9 C70FB6E7 DF2E0CED 78FA19EB 7663D2E6
          BB205B03 30E2F6A5 4EF3DD44 2C6012CC
```

```
xV =      1197EA35 7004B9D2 D0FD3952 C4BCD6EC AB867969 E4AE932B
          0B6891BE

yV =      A7383718 E8DC35E4 250A0631 4600F298 591FDCF6 7DF902BC
          850A4F7F 1D52DF78 77B89D44 E752790F 0644FF1D 855F1C3F
          0B668E6E 935E1E3B 3C494F07 59F60D59 A1580219 EBE55329
          169136CF 0E06B7E3 498FC309 6AF25103 C8D06565 418EDE00
          9CF6C59B 0878FFCF 23200233 86353FEF 47F0F486 0367DBEA
          334392FB 7A1BC5F5 FCCFEAB9 994BF89C 3368B01D 995A05F3
          1E8EE278 3CA95011 E31671ED B283111D BC0591B9 5AD26598
          0C1463C4 73F28A54 569F8588 85BD3126 42C79D51 645E1729
          B168A62D E0BC1F2F 93F739E9 29B6F739 65E761FE 1E0B5CF7
          901112FC 00C10A22 5CA07A58 A62E9128 3B3B57E1 83B8F863
          CC9944E6 6E7AB72F 1DC1DCBF D7A0FBB5
```

- Step 1: U produces rU, tU and receives tV. U DOES NOT RECEIVE rV (shown only for the purpose of verifying this data).

```
rU =      81C1B6AF D9681057 676282C5 F151D260 DE744420 E9144CA6
          1034F03F

tU =      03188D70 03F02D6F 2E2B9441 8273AF93 B2B833DE 40889A09
          75972347 1E422F73 808E9C29 9299892A 0D64504D 52026E1A
          78E24CE1 1B084829 753D91B0 AA4D8BF5 FC0ECA29 149DB9FF
          B849D9A3 36BAB99A 1C3B9A97 B9ADB1B8 D4495D13 5286E973
          E5A47A04 D3B3BCCA D7C4E21A 33E8E2AB 64EBD7B2 B43C6246
          7B41297F 01692FC5 247BFF77 C98C841C D342DC44 1DAF9F7D
          C246C1A6 290C572A 6A612DFC A2B8D46C E4C1F92D 0FCC875C
          7FE39B0D 8C98CF4B 835D493A 57DE7092 6FD86010 486AFFF7
          52568B50 4B22D66A BF4EB730 2CA575C7 6EEC47CB 24CBEB30
          F8130731 5B8E67A0 E31EDA04 B6F3301A 2BD29590 F1A0B00C
          1E9625CF DFFB3524 2BE64DAD FAE83A78

rV =      1CFC71DC 14F835CC 85685991 A5B419E4 75B6CE13 F9D401B2
          C113227A
```

```
tV =      82DB70CB D9B6EE9D AE5A94E6 5839DC0D 259C0F22 84697A9F
          B32E16B6 9228161F 52808BAA 02665E81 B3D4416D 67F6FF25
          111BE652 4A19557C 8BB686EA E8217B9D D3B4AE05 01C3C866
          26542DA3 37FE77C6 9ECD0ED6 3BAD46CE 4838E5FC 442DB362
          A1C042BD E87A5FF5 EFC316F7 861773AE 0E33E801 9D611FE0
          A4E26F21 D00ABBA9 64742C8D B6C55D90 E1A3BDAE 34B81D96
          08615192 BEC603A4 AC049A37 3CC38CDE D7CB7CD1 E1128D48
          1A3B137E DF94EFA8 C8872392 1E814921 A540126A B3897BD8
          EDB8DF2D 323BE8CA E6BC74D0 0C1A24A5 3B9102E8 7FB30034
          D145A418 68970802 9AEAAF8A 41B83C27 64F103FE D1D7E769
          F6548964 8B56FB74 93C099BB 685D31EB
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       111700796313910130466015002190130466201401445038951
          282014922876505509889092674119307116405861215854513
          555574719147991916595440835614985398038629422196542
          339588870622287500381918203683121135797175119754341
          382371677131724260628570109232273872416038987178749
          281682930511193889056003955788522968002906961865695
          788159634578246399697276767886272518505433527186121
          560717546006233179535122789344340570916147537689429
          762290119369369663527521999522333125246811136203474
          857410306192762762170050007936050400988731765742509
          324218827182469156133884527760852884465452434794665
          271352370047170622078328705195676219281608299951139
          13347
```

- Step 4: Shared secret converted to byte string.

```
Z =       08D9313B B59DBE54 40AA2606 6C93A890 3584889F DAEB74EE
          1EACEE96 62E26CB9 F98CF2B0 8F524982 D65B35FD 6AF1A77F
          9BA3D39B 52B66A32 46B33A10 FE4B97BB 7EC73CFB 22C541A5
          9957F84C C0AC009B EF88CEEA E0A23D63 58300B65 1772DECD
          482F3333 D7596E23 2E6489AC E0164311 3A9BEA07 915F1F8A
          36B0D36B 1202A43F 8A10A9E6 C0319AB1 57F1DC69 321C2520
```

```
36A32319 A42523E3 17992327 2295DBC9 6E9336C5 65569E2C
863CDB3D 56E44CDA 6ADF829F 61C5D668 012E53FD 7858C810
4A9815F1 45ABB26B 3C109A14 A255A8E4 7F02E3B5 B19E9192
89FEB810 052DC189 2E44CC2E 1D3B3F45 9C0B11B7 D8A3E0DD
C41E3E2F E3C2B779 04542392 8B9E1C03
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 68CBA8E7 CA476978 F52B7235 ECB90616 5FA9D6F5 B6CF3908
             2DC94388 4AE28F4F 140B163C E6F4F0DB 37A58F79 B3FD52A2
             4EF40B09 5B4E934B
```

- If key confirmation is performed, then

```
MacKey  =     68CB A8E7CA47 6978F52B 7235ECB9
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 03188D70 03F02D6F
            2E2B9441 8273AF93 B2B833DE 40889A09 75972347 1E422F73
            808E9C29 9299892A 0D64504D 52026E1A 78E24CE1 1B084829
            753D91B0 AA4D8BF5 FC0ECA29 149DB9FF B849D9A3 36BAB99A
            1C3B9A97 B9ADB1B8 D4495D13 5286E973 E5A47A04 D3B3BCCA
            D7C4E21A 33E8E2AB 64EBD7B2 B43C6246 7B41297F 01692FC5
            247BFF77 C98C841C D342DC44 1DAF9F7D C246C1A6 290C572A
            6A612DFC A2B8D46C E4C1F92D 0FCC875C 7FE39B0D 8C98CF4B
            835D493A 57DE7092 6FD86010 486AFFF7 52568B50 4B22D66A
            BF4EB730 2CA575C7 6EEC47CB 24CBEB30 F8130731 5B8E67A0
            E31EDA04 B6F3301A 2BD29590 F1A0B00C 1E9625CF DFFB3524
            2BE64DAD FAE83A78 82DB70CB D9B6EE9D AE5A94E6 5839DC0D
            259C0F22 84697A9F B32E16B6 9228161F 52808BAA 02665E81
            B3D4416D 67F6FF25 111BE652 4A19557C 8BB686EA E8217B9D
```

```
                D3B4AE05 01C3C866 26542DA3 37FE77C6 9ECD0ED6 3BAD46CE
                4838E5FC 442DB362 A1C042BD E87A5FF5 EFC316F7 861773AE
                0E33E801 9D611FE0 A4E26F21 D00ABBA9 64742C8D B6C55D90
                E1A3BDAE 34B81D96 08615192 BEC603A4 AC049A37 3CC38CDE
                D7CB7CD1 E1128D48 1A3B137E DF94EFA8 C8872392 1E814921
                A540126A B3897BD8 EDB8DF2D 323BE8CA E6BC74D0 0C1A24A5
                3B9102E8 7FB30034 D145A418 68970802 9AEAAF8A 41B83C27
                64F103FE D1D7E769 F6548964 8B56FB74 93C099BB 685D31EB

     MacTag_U  = 67DA6906 B6F3C78B AAFDD431 649282D0 44D20704 F2CDA42A
                 B2EB4928
```

- If UNILATERAL key confirmation provided by V to U, then

```
   MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

             = 4B435F31 5F56424F 42425941 4C494345 82DB70CB D9B6EE9D
               AE5A94E6 5839DC0D 259C0F22 84697A9F B32E16B6 9228161F
               52808BAA 02665E81 B3D4416D 67F6FF25 111BE652 4A19557C
               8BB686EA E8217B9D D3B4AE05 01C3C866 26542DA3 37FE77C6
               9ECD0ED6 3BAD46CE 4838E5FC 442DB362 A1C042BD E87A5FF5
               EFC316F7 861773AE 0E33E801 9D611FE0 A4E26F21 D00ABBA9
               64742C8D B6C55D90 E1A3BDAE 34B81D96 08615192 BEC603A4
               AC049A37 3CC38CDE D7CB7CD1 E1128D48 1A3B137E DF94EFA8
               C8872392 1E814921 A540126A B3897BD8 EDB8DF2D 323BE8CA
               E6BC74D0 0C1A24A5 3B9102E8 7FB30034 D145A418 68970802
               9AEAAF8A 41B83C27 64F103FE D1D7E769 F6548964 8B56FB74
               93C099BB 685D31EB 03188D70 03F02D6F 2E2B9441 8273AF93
               B2B833DE 40889A09 75972347 1E422F73 808E9C29 9299892A
               0D64504D 52026E1A 78E24CE1 1B084829 753D91B0 AA4D8BF5
               FC0ECA29 149DB9FF B849D9A3 36BAB99A 1C3B9A97 B9ADB1B8
               D4495D13 5286E973 E5A47A04 D3B3BCCA D7C4E21A 33E8E2AB
               64EBD7B2 B43C6246 7B41297F 01692FC5 247BFF77 C98C841C
               D342DC44 1DAF9F7D C246C1A6 290C572A 6A612DFC A2B8D46C
               E4C1F92D 0FCC875C 7FE39B0D 8C98CF4B 835D493A 57DE7092
               6FD86010 486AFFF7 52568B50 4B22D66A BF4EB730 2CA575C7
               6EEC47CB 24CBEB30 F8130731 5B8E67A0 E31EDA04 B6F3301A
               2BD29590 F1A0B00C 1E9625CF DFFB3524 2BE64DAD FAE83A78
```

```
MacTag_V  = 4D2AFD74 EE7E5335 6D2939C1 C842F87E EDEAE00B 448C3890
            633861E2
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 03188D70 03F02D6F
            2E2B9441 8273AF93 B2B833DE 40889A09 75972347 1E422F73
            808E9C29 9299892A 0D64504D 52026E1A 78E24CE1 1B084829
            753D91B0 AA4D8BF5 FC0ECA29 149DB9FF B849D9A3 36BAB99A
            1C3B9A97 B9ADB1B8 D4495D13 5286E973 E5A47A04 D3B3BCCA
            D7C4E21A 33E8E2AB 64EBD7B2 B43C6246 7B41297F 01692FC5
            247BFF77 C98C841C D342DC44 1DAF9F7D C246C1A6 290C572A
            6A612DFC A2B8D46C E4C1F92D 0FCC875C 7FE39B0D 8C98CF4B
            835D493A 57DE7092 6FD86010 486AFFF7 52568B50 4B22D66A
            BF4EB730 2CA575C7 6EEC47CB 24CBEB30 F8130731 5B8E67A0
            E31EDA04 B6F3301A 2BD29590 F1A0B00C 1E9625CF DFFB3524
            2BE64DAD FAE83A78 82DB70CB D9B6EE9D AE5A94E6 5839DC0D
            259C0F22 84697A9F B32E16B6 9228161F 52808BAA 02665E81
            B3D4416D 67F6FF25 111BE652 4A19557C 8BB686EA E8217B9D
            D3B4AE05 01C3C866 26542DA3 37FE77C6 9ECD0ED6 3BAD46CE
            4838E5FC 442DB362 A1C042BD E87A5FF5 EFC316F7 861773AE
            0E33E801 9D611FE0 A4E26F21 D00ABBA9 64742C8D B6C55D90
            E1A3BDAE 34B81D96 08615192 BEC603A4 AC049A37 3CC38CDE
            D7CB7CD1 E1128D48 1A3B137E DF94EFA8 C8872392 1E814921
            A540126A B3897BD8 EDB8DF2D 323BE8CA E6BC74D0 0C1A24A5
            3B9102E8 7FB30034 D145A418 68970802 9AEAAF8A 41B83C27
            64F103FE D1D7E769 F6548964 8B56FB74 93C099BB 685D31EB

MacTag_U  = 5E7E2F4B 1868011F 8BAA8AE2 E519F644 E9E19AC6 221FB177
            5113F906

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 82DB70CB D9B6EE9D
            AE5A94E6 5839DC0D 259C0F22 84697A9F B32E16B6 9228161F
```

```
              52808BAA 02665E81 B3D4416D 67F6FF25 111BE652 4A19557C
              8BB686EA E8217B9D D3B4AE05 01C3C866 26542DA3 37FE77C6
              9ECD0ED6 3BAD46CE 4838E5FC 442DB362 A1C042BD E87A5FF5
              EFC316F7 861773AE 0E33E801 9D611FE0 A4E26F21 D00ABBA9
              64742C8D B6C55D90 E1A3BDAE 34B81D96 08615192 BEC603A4
              AC049A37 3CC38CDE D7CB7CD1 E1128D48 1A3B137E DF94EFA8
              C8872392 1E814921 A540126A B3897BD8 EDB8DF2D 323BE8CA
              E6BC74D0 0C1A24A5 3B9102E8 7FB30034 D145A418 68970802
              9AEAAF8A 41B83C27 64F103FE D1D7E769 F6548964 8B56FB74
              93C099BB 685D31EB 03188D70 03F02D6F 2E2B9441 8273AF93
              B2B833DE 40889A09 75972347 1E422F73 808E9C29 9299892A
              0D64504D 52026E1A 78E24CE1 1B084829 753D91B0 AA4D8BF5
              FC0ECA29 149DB9FF B849D9A3 36BAB99A 1C3B9A97 B9ADB1B8
              D4495D13 5286E973 E5A47A04 D3B3BCCA D7C4E21A 33E8E2AB
              64EBD7B2 B43C6246 7B41297F 01692FC5 247BFF77 C98C841C
              D342DC44 1DAF9F7D C246C1A6 290C572A 6A612DFC A2B8D46C
              E4C1F92D 0FCC875C 7FE39B0D 8C98CF4B 835D493A 57DE7092
              6FD86010 486AFFF7 52568B50 4B22D66A BF4EB730 2CA575C7
              6EEC47CB 24CBEB30 F8130731 5B8E67A0 E31EDA04 B6F3301A
              2BD29590 F1A0B00C 1E9625CF DFFB3524 2BE64DAD FAE83A78

MacTag_V  = 15AA88A0 E0C94BE5 B197F7DE CA499A63 1CD1D9E3 D334A6FF
            EB4A6F7F
```

3.3.3 dhEphem for finite field p2048-q224

- Step 1: U produces rU, tU and receives tV. U DOES NOT RECEIVE rV (shown only for the purpose of verifying this data).

```
rU =      BCC732B2 0597BF04 893C5392 0EC2E9D0 B7BB774C F1B40640
          A2345A27

tU =      2A19E891 D3BACF8B 7C6CE3A8 538F0F89 B846A3AA 214D0D8B
          801A242F 416F6DFA 51B8D236 6F96DE6F DB985A6C 13DE3930
          23D6736E 21F0F231 B748B250 47766E47 A7A5753F 2DC3AFC1
          AE44719C 17839118 4FDC01CE 631893A8 FEC7EC16 AACEF1D2
```

```
            327DD02E 1D84B023 B20B119F 83A7BE07 417FDE59 6591BC38
            FE3655BA 040D46E4 40001C1A 68A06A44 AC252AF8 30DF5C08
            ECDC2132 D2A80E43 5EF21344 8247346E 9062E303 04907879
            7522CAD3 BC949424 2347ECB0 29A3F323 9DFCADF8 62A2539A
            35584D21 038FD2B6 21AF071C C5C827C5 90CEAD0E 98C511FA
            EA445DC1 CED852B5 40DDF6A2 E7C1CD15 C75B9279 E25092F4
            67308A60 D90AB435 5C58214E 044EF1D6

rV =        0A497196 2C7A18A1 B2A2C70D C5C50682 2863E11E 59A26128
            8D319B79

tV =        2D337F87 ADDEEDFE 123B6CB6 2AEDFCBC 9E89167F 75B75E40
            0201EBEE 9591089A 30C3C13F BC4F1B0E C051A1E6 208FBA7F
            DEC7CA1F D8BEFBF0 1A739F7A 6A0A92BE ECC776B9 F91AECDF
            3B767F11 7FCE440B D40F1B60 37E0CB03 B5E61778 C6A81EBB
            0ACFF7F7 574D7D51 ED4C1518 AB3C8114 D5D1DB68 D1D3F8B3
            FE42CFA1 32FD9CCD 931FC198 A4C3C603 6557D9E1 560F598B
            E758A537 9982DC0C 653D48AE 4AB05A68 09C8925A BB0AB5A8
            A4D46752 3F58E922 A7D7711E 0691C5EE 70948977 BAD7850A
            DA01FF2C DEE05BA5 A0ACCB30 3B619692 32FBA7F3 59A4C667
            8679A3A5 11CEBADB 361F53BE 687CA9D3 E8F9E559 1E528D2D
            57E808B4 4C639DD1 EB90CE9D 5D88659D
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =         14975688686790489248602208623009559017450506866866
            06682086719427725030308720632598417395976270607785
            04684398235439327291399561811828019671492993345726
            69735601257689833727225520207083746030517721818565
            78598988338145930373090611305984732188173675327221
            32916094592510680005853669941825602458183958193186
            36102355299995772261041988628967709538721840292220
            40398377297756461439700489066994948105228134875900
            34132575318689985898034410948907547761052464029533
            96446572749846684267954923375127482918325854993708
            28840262218516545488940781814549722943642039374394
```

```
83982131509758160248254749539758211410527916011570
86559253666034062
```

- Step 4:

```
Z =       76A15BB3 E674EC0F 00C07B8D CD6198DF EFA0379C DAF2DF26
          1BB8AC44 B89FAB46 FB09D7E5 B597C8E0 DA489710 CABA2FBF
          717601BF 1B6766BC 929B335E D7FEFAED F45D2C77 8879549D
          80C9980C 23004753 5EF1F918 5F0BBB83 D7FD2992 C2439211
          67311A32 374A4730 DC386183 5B23DA95 7D7177EB 3488CDEA
          CE2DBF55 3B7F5858 9849D9EC 44DCE6CE 27FF9E34 76ED0CEE
          ABAEC2F2 04207DA8 F3E696B4 FA01DEF5 65E05D96 F904A6C8
          5CA3D95E 77E78BBE CDDD4633 18119EA4 FDEE2DED 39C819A4
          51391B15 5E48BD70 4CDA4A88 81B37514 8BC50DE2 6C870BC1
          BEE267F5 36F253A8 1A1C7E68 0C3B6ED6 B6DFF575 932FB403
          34027291 1C09B9C1 AFF15F06 E3BD718E
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 42160183 80EC13E1 A276DC93 A7572BCE AF1D4487 3273F867
             E61E9CCC 93DAF04F 8EF77A43 1874AEE0 DFE8ACD6 690DB585
             CDB18423 FCC9C679
```

3.3.4 dhHybridOneFlow for finite field p2048-q224

- Prerequisites:

```
xU =      13F1A5D3 5735CACC 0F299663 65D0C5E4 ECE36287 5F82B5D6
          950C0367

yU =      3838CDDB AC872586 EC248DB1 561A76D3 0681B61A 18A77888
          4F12D14B 07C17BC5 023A68D9 AFFCFEB7 AF371691 103F16E6
          609B2A04 257CE2AE 460D6201 E9A97C31 CC2D660C E76C8E79
```

```
          A1EC8227 70858F28 8C4D316F 07CBEBAC 7CAF18AB 8A8EB2C8
          CD79D0F4 6AFFE5DF 33B9F86C EAB69750 902FA676 C6A9D1C0
          AEC94AE3 4E098A9A EEE1A7F2 D0E9F915 4E023C9A 863D3D1F
          CB51C3CB 43A4FCBA 389B3BC9 E789E5DB 5F5864C1 644DEA36
          246F0D1A A90BC310 56A2DDC6 C8DBF590 297EB4DC C9713C3E
          7150660F 9FF406B5 70355772 1E3BB5E9 E2157DD0 CD2D0001
          E47C9E43 167B2823 9B6AB6A5 EED7C8CD A0BEA78C BC7DEAED
          C0518CF7 3729B83B 268591CF 7DC61CAB

xV =      96E337FF 7A17E6BF 18D76A9D E185D3BA 26658BC7 0334AB4D
          55BBC0F8

yV =      3B5D6BB3 E5253584 90223639 4EBBC891 6A8DA8CF E45B109E
          211CA2E1 49F91825 9F8C1E22 831EFAB5 697E62CB 96B2CE96
          221729DD FD1A610E 9016112D 3608D053 4F2BFEE3 B692F1CE
          F8602D11 0D071925 09106B04 269E51BF 7B62D2B2 95223049
          4BB8E43C 78EEA845 43A1D391 B858A139 F7144A04 6DF47883
          A062AB0A 5BD9AB5E A686930F 79D1B5E1 824EDFFB 56977220
          357656E8 6C94F662 2EF7B14D 7D4EFE77 A8BCACB3 DBC95F94
          7EF3B071 669AD491 7EC5A00D B1CE257C C494E489 E79AC202
          63B81555 A3F9E87B D9DF6242 7A7103F0 A6F65555 7B22508F
          8296B73B E56A1076 3AC39130 AE373C26 726C06D6 52126C96
          3103736C A070FCC7 F62085B4 D51A3005
```

BEGIN U's calculations

- Step 1:

```
rU =      AB369107 264B7560 609FD6BF 731A7915 315CEABA 9EAD8B13
          9B6773AE

tU =      791E98C8 0B1EE0EE E1E32948 9CC198CB C2F76567 A3EA3CC2
          ECBBAC04 B0716027 A141A167 BEFC26B9 A13BD6BC F22B6A75
          995F2D05 67FB560B 249F46B2 7CCA8321 6482F92F B47FB0AC
          99BD3BDB 37ECE33C 2B97C855 EDED8CF3 65EEAB81 3565C100
          2F30065B DA4F853A 8BC85504 D9CC27B4 17A77B96 A42A18BF
          EF7B0DD8 C67B5201 E487E4A2 4E2865D3 6DAB5679 4A9F6314
```

```
FAA80CAD 052AA4B9 28B4D69F EFC5F92A 70DF00A3 5A0FB17B
A2E25D7A AA0EF86B 367E4267 C1D50583 83CEA31F 1902658E
95689447 94C3178F E32A3F82 4D28251F FAEE9B96 551F56B3
AD42827C 773CAC25 C5A0D450 A37A2BDF 849D19AF A2B048E0
7C7EE2E0 D5C5C0C4 6E06995A 4BBA0448
```

- Step 2: Decimal and hex values for static shared secret.

```
Z_s =     13851009560691758436977874424519822756667424924193
          77861891382948827525214244438701516415925660633767
          20582644158498919234005263980079864298148131829328
          68175717183645385490980710684598697968704456329682
          21993422486911713731400030465395116391346640632995
          68576717895788690444621216526490103761486867508107
          34981997822260279872381001476872719527014751485416
          24459761833703613726897535556559476253107423588865
          51045722643898901999414033290307577297774639430668
          52427858521321800707884983125635255124129010451495
          29674188048357316413108229769810965027450651123627
          37443965963879617810840925793105573561781745353275
          518041915860282

Z_s =     0118E2D7 191A50E2 83E74471 7F222A11 1E0C2A52 4B18A34C
          7D4C06ED 2A26E9B3 F3F90AB6 C736EB94 F934AAFE 589B6601
          81816A0D 209D724C 9C4FAF07 F917406F B5851DEB EE49CB6C
          A95559A5 4CFA8E5C 583166BF 9B8A55A8 CA83B3FB 6AB27651
          858968FF 017B76EF 6E631068 C1DD001C 47B135C5 74BED9DD
          8A29DDCF F2DDF406 322CFDFF E3FD96EF 08D1E08F CC2DFFE8
          7CF9479C 47946D23 CA22F80C E380AFBE 5477222F CAF990DD
          FA3584F0 DD240632 24A8301E 3A48ACB8 E65F6923 FE2FD18F
          61B0484C BF41079F C731A2DE 1CECFD4B A2CB0392 F8C7E36A
          E1F4636E 6CB13AFA FAF84A06 05245424 6B225154 8B3FF750
          AB350665 7809B058 E05D30A9 8F1F253A
```

- Step 3: Decimal and hex values for ephemeral shared secret.

```
Z_e =     215218918186068062995807319646545117311328994724 30
```

```
562175465427926311304088515474237684969094266507604
823354000229721261235417982142438942384591268707905
695425347506836104464962415021258096950031413407
654106582483848900912919157718003798751972059312309
865555675560055829500892366105994328907965785884515
758972121506154509636843602705020601612064475104160
664293282622346643212517017637812577248776370655714
490459383161647577049454974943707114104463189409
621086193127936499371431964545634542966103475847460
233347884526648522568495078577091905097788664020440
328737900150216615149710004001620293169719758447
05734206668708341
```

Z_e =

```
AA7C791D 3A729116 3AC8D2D5 2F60E297 B8B49691 111F8410
49F19144 80C78C72 0EE48DB2 D817421C 94B86D6C 854BA259
2D78938E DDCBAE19 B8FB4AE4 9EEDC269 97F85400 867ABE2E
82CC661D 591D7C78 87A89BDD 4D7DBD16 3F93B3E6 B558A2B3
4ADCFB6C FADF3D7E 6BD19F36 C2F70EE1 AF859942 B6AC1A62
FE00EF98 BB54BD3E B981E94A C49CC75B 2EA2658A 220652E9
A6C6D38F 7888953F F63FACA9 02AA600B 9F4D4210 7792BAEB
9D678B5D C718ABE3 FAC70EF4 73D3E324 88739921 1EDFF2A0
9A333115 6CA7338E D19F2735 3D7BE706 5A09DA7E 11267F99
5179DB59 5B5FB293 70FFA929 D56241B3 D4A1DF49 1FB9316E
832F1AED 7C09CF6B 23DD2BC9 A26499F5
```

- Step 4: Shared secret.

Z =

```
AA7C791D 3A729116 3AC8D2D5 2F60E297 B8B49691 111F8410
49F19144 80C78C72 0EE48DB2 D817421C 94B86D6C 854BA259
2D78938E DDCBAE19 B8FB4AE4 9EEDC269 97F85400 867ABE2E
82CC661D 591D7C78 87A89BDD 4D7DBD16 3F93B3E6 B558A2B3
4ADCFB6C FADF3D7E 6BD19F36 C2F70EE1 AF859942 B6AC1A62
FE00EF98 BB54BD3E B981E94A C49CC75B 2EA2658A 220652E9
A6C6D38F 7888953F F63FACA9 02AA600B 9F4D4210 7792BAEB
9D678B5D C718ABE3 FAC70EF4 73D3E324 88739921 1EDFF2A0
9A333115 6CA7338E D19F2735 3D7BE706 5A09DA7E 11267F99
5179DB59 5B5FB293 70FFA929 D56241B3 D4A1DF49 1FB9316E
832F1AED 7C09CF6B 23DD2BC9 A26499F5 0118E2D7 191A50E2
```

```
83E74471 7F222A11 1E0C2A52 4B18A34C 7D4C06ED 2A26E9B3
F3F90AB6 C736EB94 F934AAFE 589B6601 81816A0D 209D724C
9C4FAF07 F917406F B5851DEB EE49CB6C A95559A5 4CFA8E5C
583166BF 9B8A55A8 CA83B3FB 6AB27651 858968FF 017B76EF
6E631068 C1DD001C 47B135C5 74BED9DD 8A29DDCF F2DDF406
322CFDFF E3FD96EF 08D1E08F CC2DFFE8 7CF9479C 47946D23
CA22F80C E380AFBE 5477222F CAF990DD FA3584F0 DD240632
24A8301E 3A48ACB8 E65F6923 FE2FD18F 61B0484C BF41079F
C731A2DE 1CECFD4B A2CB0392 F8C7E36A E1F4636E 6CB13AFA
FAF84A06 05245424 6B225154 8B3FF750 AB350665 7809B058
E05D30A9 8F1F253A
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 7AA6541F CF654B6F 21128C21 4C8BA215 7AF623DC 87FE9EA9
             85CAF289 B6516864 2EDB9C60 7F04DAFE D2698926 89B61191
             FBD35E45 6B1DAF79
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
rU =      AB369107 264B7560 609FD6BF 731A7915 315CEABA 9EAD8B13
          9B6773AE

tU =      791E98C8 0B1EE0EE E1E32948 9CC198CB C2F76567 A3EA3CC2
          ECBBAC04 B0716027 A141A167 BEFC26B9 A13BD6BC F22B6A75
          995F2D05 67FB560B 249F46B2 7CCA8321 6482F92F B47FB0AC
          99BD3BDB 37ECE33C 2B97C855 EDED8CF3 65EEAB81 3565C100
          2F30065B DA4F853A 8BC85504 D9CC27B4 17A77B96 A42A18BF
          EF7B0DD8 C67B5201 E487E4A2 4E2865D3 6DAB5679 4A9F6314
          FAA80CAD 052AA4B9 28B4D69F EFC5F92A 70DF00A3 5A0FB17B
          A2E25D7A AA0EF86B 367E4267 C1D50583 83CEA31F 1902658E
```

```
95689447 94C3178F E32A3F82 4D28251F FAEE9B96 551F56B3
AD42827C 773CAC25 C5A0D450 A37A2BDF 849D19AF A2B048E0
7C7EE2E0 D5C5C0C4 6E06995A 4BBA0448
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     13851009560691758436977874424519822756667424924193
          77861891382948827525214244438701516415925660633767
          20582644158498919234005263980079864298148131829328
          68175717183645385490980710684598697968704456329682
          21993422486911713731400030465395116391346640632995
          68576717895788690444621216526490103761486867508107
          34981997822260279872381001476872719527014751485416
          24459761833703613726897535556559476253107423588865
          51045722643898901999414033290307577297774639430668
          52427858521321800707884983125635255124129010451495
          29674188048357316413108229769810965027450651123627
          37443965963879617810840925793105573561781745353275
          518041915860282

Z_s =     0118E2D7 191A50E2 83E74471 7F222A11 1E0C2A52 4B18A34C
          7D4C06ED 2A26E9B3 F3F90AB6 C736EB94 F934AAFE 589B6601
          81816A0D 209D724C 9C4FAF07 F917406F B5851DEB EE49CB6C
          A95559A5 4CFA8E5C 583166BF 9B8A55A8 CA83B3FB 6AB27651
          858968FF 017B76EF 6E631068 C1DD001C 47B135C5 74BED9DD
          8A29DDCF F2DDF406 322CFDFF E3FD96EF 08D1E08F CC2DFFE8
          7CF9479C 47946D23 CA22F80C E380AFBE 5477222F CAF990DD
          FA3584F0 DD240632 24A8301E 3A48ACB8 E65F6923 FE2FD18F
          61B0484C BF41079F C731A2DE 1CECFD4B A2CB0392 F8C7E36A
          E1F4636E 6CB13AFA FAF84A06 05245424 6B225154 8B3FF750
          AB350665 7809B058 E05D30A9 8F1F253A
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     21521891818606806299580731964654511731132899472430
          56217546542792631130408851547423768496909426650760
```

```
482335400022972126123541798214243894238459126870790
5695425347506836104464962415021258096950031413407
6541065824838489009129191577180037987519720593123 0
9865556755600558295008923661059943289079657858845 1
7589721215061545096368436027050206016120644751041 6
0664293282622346643212517017637812577248776370655 7
1449045938316164757704945497494370711410446318940 9
6210861931279364993714319645456345429661034758474 6
0233347884526648522568495078577091905097788664020 4
4032873790015021661514971000400162029316971975844 7
05734206668708341
```

```
Z_e =     AA7C791D 3A729116 3AC8D2D5 2F60E297 B8B49691 111F8410
          49F19144 80C78C72 0EE48DB2 D817421C 94B86D6C 854BA259
          2D78938E DDCBAE19 B8FB4AE4 9EEDC269 97F85400 867ABE2E
          82CC661D 591D7C78 87A89BDD 4D7DBD16 3F93B3E6 B558A2B3
          4ADCFB6C FADF3D7E 6BD19F36 C2F70EE1 AF859942 B6AC1A62
          FE00EF98 BB54BD3E B981E94A C49CC75B 2EA2658A 220652E9
          A6C6D38F 7888953F F63FACA9 02AA600B 9F4D4210 7792BAEB
          9D678B5D C718ABE3 FAC70EF4 73D3E324 88739921 1EDFF2A0
          9A333115 6CA7338E D19F2735 3D7BE706 5A09DA7E 11267F99
          5179DB59 5B5FB293 70FFA929 D56241B3 D4A1DF49 1FB9316E
          832F1AED 7C09CF6B 23DD2BC9 A26499F5
```

- Step 5: Shared secret.

```
Z =       AA7C791D 3A729116 3AC8D2D5 2F60E297 B8B49691 111F8410
          49F19144 80C78C72 0EE48DB2 D817421C 94B86D6C 854BA259
          2D78938E DDCBAE19 B8FB4AE4 9EEDC269 97F85400 867ABE2E
          82CC661D 591D7C78 87A89BDD 4D7DBD16 3F93B3E6 B558A2B3
          4ADCFB6C FADF3D7E 6BD19F36 C2F70EE1 AF859942 B6AC1A62
          FE00EF98 BB54BD3E B981E94A C49CC75B 2EA2658A 220652E9
          A6C6D38F 7888953F F63FACA9 02AA600B 9F4D4210 7792BAEB
          9D678B5D C718ABE3 FAC70EF4 73D3E324 88739921 1EDFF2A0
          9A333115 6CA7338E D19F2735 3D7BE706 5A09DA7E 11267F99
          5179DB59 5B5FB293 70FFA929 D56241B3 D4A1DF49 1FB9316E
          832F1AED 7C09CF6B 23DD2BC9 A26499F5 0118E2D7 191A50E2
          83E74471 7F222A11 1E0C2A52 4B18A34C 7D4C06ED 2A26E9B3
```

```
F3F90AB6 C736EB94 F934AAFE 589B6601 81816A0D 209D724C
9C4FAF07 F917406F B5851DEB EE49CB6C A95559A5 4CFA8E5C
583166BF 9B8A55A8 CA83B3FB 6AB27651 858968FF 017B76EF
6E631068 C1DD001C 47B135C5 74BED9DD 8A29DDCF F2DDF406
322CFDFF E3FD96EF 08D1E08F CC2DFFE8 7CF9479C 47946D23
CA22F80C E380AFBE 5477222F CAF990DD FA3584F0 DD240632
24A8301E 3A48ACB8 E65F6923 FE2FD18F 61B0484C BF41079F
C731A2DE 1CECFD4B A2CB0392 F8C7E36A E1F4636E 6CB13AFA
FAF84A06 05245424 6B225154 8B3FF750 AB350665 7809B058
E05D30A9 8F1F253A
```

- Step 6: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 7AA6541F CF654B6F 21128C21 4C8BA215 7AF623DC 87FE9EA9
             85CAF289 B6516864 2EDB9C60 7F04DAFE D2698926 89B61191
             FBD35E45 6B1DAF79
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     7AA6 541FCF65 4B6F2112 8C214C8B

nonceV =  335329E8 E458E4BF 5A1217D4 CAAD7EC6 FAA01804 535C1C47
          EC936D5D
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 791E98C8 0B1EE0EE
            E1E32948 9CC198CB C2F76567 A3EA3CC2 ECBBAC04 B0716027
            A141A167 BEFC26B9 A13BD6BC F22B6A75 995F2D05 67FB560B
            249F46B2 7CCA8321 6482F92F B47FB0AC 99BD3BDB 37ECE33C
```

```
              2B97C855 EDED8CF3 65EEAB81 3565C100 2F30065B DA4F853A
              8BC85504 D9CC27B4 17A77B96 A42A18BF EF7B0DD8 C67B5201
              E487E4A2 4E2865D3 6DAB5679 4A9F6314 FAA80CAD 052AA4B9
              28B4D69F EFC5F92A 70DF00A3 5A0FB17B A2E25D7A AA0EF86B
              367E4267 C1D50583 83CEA31F 1902658E 95689447 94C3178F
              E32A3F82 4D28251F FAEE9B96 551F56B3 AD42827C 773CAC25
              C5A0D450 A37A2BDF 849D19AF A2B048E0 7C7EE2E0 D5C5C0C4
              6E06995A 4BBA0448 335329E8 E458E4BF 5A1217D4 CAAD7EC6
              FAA01804 535C1C47 EC936D5D

   MacTag_U  = 6A0413EB CBE53D01 3247EE0C 9A7254FE C6D950D6 2D382E0E
               DAB926C3
```

- If UNILATERAL key confirmation provided by V to U, then

```
  MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

            = 4B435F31 5F56424F 42425941 4C494345 791E98C8 0B1EE0EE
              E1E32948 9CC198CB C2F76567 A3EA3CC2 ECBBAC04 B0716027
              A141A167 BEFC26B9 A13BD6BC F22B6A75 995F2D05 67FB560B
              249F46B2 7CCA8321 6482F92F B47FB0AC 99BD3BDB 37ECE33C
              2B97C855 EDED8CF3 65EEAB81 3565C100 2F30065B DA4F853A
              8BC85504 D9CC27B4 17A77B96 A42A18BF EF7B0DD8 C67B5201
              E487E4A2 4E2865D3 6DAB5679 4A9F6314 FAA80CAD 052AA4B9
              28B4D69F EFC5F92A 70DF00A3 5A0FB17B A2E25D7A AA0EF86B
              367E4267 C1D50583 83CEA31F 1902658E 95689447 94C3178F
              E32A3F82 4D28251F FAEE9B96 551F56B3 AD42827C 773CAC25
              C5A0D450 A37A2BDF 849D19AF A2B048E0 7C7EE2E0 D5C5C0C4
              6E06995A 4BBA0448

   MacTag_V  = 1F22DA1E 9356D5B2 96C212CC 2A3D7707 01DCDEAB 9B064261
               47A5017A
```

- If BILATERAL key confirmation, then

```
  MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
            = 4B435F32 5F55414C 49434542 4F424259 791E98C8 0B1EE0EE
              E1E32948 9CC198CB C2F76567 A3EA3CC2 ECBBAC04 B0716027
              A141A167 BEFC26B9 A13BD6BC F22B6A75 995F2D05 67FB560B
              249F46B2 7CCA8321 6482F92F B47FB0AC 99BD3BDB 37ECE33C
              2B97C855 EDED8CF3 65EEAB81 3565C100 2F30065B DA4F853A
              8BC85504 D9CC27B4 17A77B96 A42A18BF EF7B0DD8 C67B5201
              E487E4A2 4E2865D3 6DAB5679 4A9F6314 FAA80CAD 052AA4B9
              28B4D69F EFC5F92A 70DF00A3 5A0FB17B A2E25D7A AA0EF86B
              367E4267 C1D50583 83CEA31F 1902658E 95689447 94C3178F
              E32A3F82 4D28251F FAEE9B96 551F56B3 AD42827C 773CAC25
              C5A0D450 A37A2BDF 849D19AF A2B048E0 7C7EE2E0 D5C5C0C4
              6E06995A 4BBA0448 335329E8 E458E4BF 5A1217D4 CAAD7EC6
              FAA01804 535C1C47 EC936D5D

 MacTag_U   = 3E2CDFF7 7E229393 D6E2DE5B A0AC0851 AE784DED 2936778A
              E904F932

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

            = 4B435F32 5F56424F 42425941 4C494345 335329E8 E458E4BF
              5A1217D4 CAAD7EC6 FAA01804 535C1C47 EC936D5D 791E98C8
              0B1EE0EE E1E32948 9CC198CB C2F76567 A3EA3CC2 ECBBAC04
              B0716027 A141A167 BEFC26B9 A13BD6BC F22B6A75 995F2D05
              67FB560B 249F46B2 7CCA8321 6482F92F B47FB0AC 99BD3BDB
              37ECE33C 2B97C855 EDED8CF3 65EEAB81 3565C100 2F30065B
              DA4F853A 8BC85504 D9CC27B4 17A77B96 A42A18BF EF7B0DD8
              C67B5201 E487E4A2 4E2865D3 6DAB5679 4A9F6314 FAA80CAD
              052AA4B9 28B4D69F EFC5F92A 70DF00A3 5A0FB17B A2E25D7A
              AA0EF86B 367E4267 C1D50583 83CEA31F 1902658E 95689447
              94C3178F E32A3F82 4D28251F FAEE9B96 551F56B3 AD42827C
              773CAC25 C5A0D450 A37A2BDF 849D19AF A2B048E0 7C7EE2E0
              D5C5C0C4 6E06995A 4BBA0448

 MacTag_V   = 0D7C91DC 8CFEDEC8 593AA8E8 1E51A4AF 9B276529 A53A7A74
              FD4E91B1
```

3.3.5 MQV1 for finite field p2048-q224

- Prerequisites:

```
xU =      95D502E9 B30DBD21 9794E7F9 DFCBD806 DD8B1AE0 737A91CC
          DC8E85FA

yU =      0DB00B97 C62AD209 1DB317B9 EDDA1672 549D0189 2C992E69
          7B538844 B581C344 F2450940 EE2EFCF4 E0B6972C E1153D67
          22E60CCD 311435FE 8D18FB4C 6447A8E2 36626544 0BD5261F
          6CB309A7 7F37B632 771AF71E AB014C27 22C99E81 F5ED4A4E
          AD305879 1D160D0A 720E2E40 7BAC3E58 BEA90906 C52C621C
          9CA51104 0B64CB27 7A0174EC A6982D9A E62728B1 F2154076
          08C0F072 B04A4D8B 5D94B0D0 9A03F794 3CE9B525 9CE1FD1F
          5ED2194D 449C0DEB 6D21B295 4EEAC3B9 7A2356B6 8C52C06B
          8C36662B 9D381ACA F710B19B 470A7C0D 00D0974F 950AC4C5
          BAACD0E1 0659D89A 364BC96E 3CA0AAAA 2AE616A6 70AAA942
          8D9FEB01 ED5EAE07 0CCB0DEC 303A3B2A

xV =      8642112C E1F5C322 D56FA089 52DCAEB5 3D1426E3 EF45F0D5
          990224F4

yV =      941CD98A 115A39B1 312E0437 AAFBEE12 C00F6E92 FE969F32
          519A1337 73119BB7 6056F12E CB0E8DF6 7C3C07A8 1191E616
          4AA853C5 013A6AC7 B0090420 A04C99ED 15751576 9BD77C26
          893CBDA8 899BEBC7 C0DCC35F 51A06112 2D67084E D4F7CC2C
          1D9D90B8 D2A1BD5B 83E916EF F6B55D9F 6260619D C5925137
          E1992A7B 71327AF1 08203460 81DD92BD EF172301 D8FAF188
          08753BFA ED35DA37 5FA9CCCB 1E36E6FD ED0AE00A DC3BE39B
          6D0FB7A4 36F485BB E931A32A BF0A2AF1 F3BB1F64 6698ABC0
          1682A3E6 379AD890 C739A335 8BBCDA88 FD1C9046 137B75F4
          B4488F90 3190CCCE 8B785684 12AAAA8E 66AF4691 DB75BA05
          B22F8685 83F1548C 45F73B1C F4312D34
```

BEGIN U's calculations

- Step 1:

```
rU =      562ADE46 F2A0CE48 00CF996A D8AD3BE8 A30C4E21 39B25E82
          A3536ED5

tU =      5322B0D0 B59A3D19 B924200D 6B6B387C 57BE84D0 AC7C98D8
          8CB4639D 515404A5 65E71F10 77CA88C9 C45D0975 516A719F
          06C8F13A 6431FEC5 0172FD96 0EDABC96 BC86551F 3FFBAD3F
          7BBF08A9 64F3C8E3 A2F39047 141521F3 1F85AC54 FAB4A2FA
          97D05A0E 1CD21D57 9A0314E8 48BA02D7 35109B2D A01DE7E2
          21BE95FB 4F29BA7B 02186640 13948315 9746776F F2CB8327
          D435FEF3 52329A02 4E25644A 9CD29378 375F24DB 4A4070A3
          F292A0CE 56076B36 25107F01 8FBCDE60 2FAE06E9 5D4476B4
          4897AD38 13EF0E69 C45E4975 587CD5D6 8DCBA825 353C899C
          789B640B CC5DD073 3D3C1219 3FC83F61 FBC04399 8579CF4F
          3F1F3C2B 1F3B9C1B 904B0F06 B6C37F71
```

- Step 2: Decimal value for shared secret.

```
Z =       25304634843423912149493666224788107240851803301893
          20942605838916452882069146410046677834065133296442
          71102697083041354358779813362197042159813887727808
          73629892916533544842458746953244374671860146889049
          57398420686795362350866643996334263331033256888982
          99472777347970370339566889995289840805227641347345
          78496953705589212951359204495312298710516088160828
          11985839001561488867913756352435581792747465027698
          00128238625381716169678443538084137102231514364129
          68741837955127105757235435466391115929628068937729
          48984258364714901613475023864633895848559393375948
          70995232146893261311086973616643326951823799976269
          6269680986554036
```

- Step 3: Hex value for shared secret.

```
Z =       140B8DC5 06909486 52D0F83D 104BAB64 61C64C71 A30C9B83
          6358C56D A2B114AE A0F6790E 52A35B6C AF1B8B97 7F590652
          FBB5D8E4 1F40FB5E 4DE8599C 484571E7 05790330 FA8189BA
          EC67FA2F 047F2195 CF2315EA B12FE734 E1D633AC 5EA92093
```

```
EFC1E7DB 41E89C42 C008FD3E 8B506107 BCE653C3 A5F2E718
A2442396 6874BA73 11D79DD3 C72BE9F2 F11D8EFE 6D77A4DA
0921532A 272AC672 3BE0D008 9A33FAED 646A42EB 01D40EB2
1E0A53E4 39DDF53F ED0DBA10 B930CB9C AE000032 87D4B3F0
0BE3DDEF B1640485 35A665FB D9ADF83F E8E52745 F0B126E6
E30008BD D16F8285 63C837C8 8EFDB4AD 7C80FCCB B474A6DF
439E80CC CD9AA299 84F94E28 BA1BFEB4
```

- Step 4: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 04CDFFA2 A110A3E9 3CB476DD 64970360 73C8B633 B447D87E
             61A70E1A EDE2FA34 07508A32 50942876 58AB9E20 E494C7CE
             B579CF8C F996393D
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
rU =      562ADE46 F2A0CE48 00CF996A D8AD3BE8 A30C4E21 39B25E82
          A3536ED5

tU =      5322B0D0 B59A3D19 B924200D 6B6B387C 57BE84D0 AC7C98D8
          8CB4639D 515404A5 65E71F10 77CA88C9 C45D0975 516A719F
          06C8F13A 6431FEC5 0172FD96 0EDABC96 BC86551F 3FFBAD3F
          7BBF08A9 64F3C8E3 A2F39047 141521F3 1F85AC54 FAB4A2FA
          97D05A0E 1CD21D57 9A0314E8 48BA02D7 35109B2D A01DE7E2
          21BE95FB 4F29BA7B 02186640 13948315 9746776F F2CB8327
          D435FEF3 52329A02 4E25644A 9CD29378 375F24DB 4A4070A3
          F292A0CE 56076B36 25107F01 8FBCDE60 2FAE06E9 5D4476B4
          4897AD38 13EF0E69 C45E4975 587CD5D6 8DCBA825 353C899C
          789B640B CC5DD073 3D3C1219 3FC83F61 FBC04399 8579CF4F
          3F1F3C2B 1F3B9C1B 904B0F06 B6C37F71
```

- Step 2: N/A.

- Step 3: Decimal value for shared secret.

```
Z =        25304634843423912149493666224788107240851803301893
           20942605838916452882069146410046677834065133296442
           71102697083041354358779813362197042159813887727808
           73629892916533544842458746953244374671860146889049
           57398420686795362350866643996334263331033256888982
           99472777347970370339566889995289840805227641347345
           78496953705589212951359204495312298710516088160828
           11985839001561488867913756352435581792747465027698
           00128238625381716169678443538084137102231514364129
           68741837955127105757235435466391115929628068937729
           48984258364714901613475023864633895848559393375948
           70995232146893261311086973616643326951823799976269
           6269680986554036
```

- Step 4: Hex value for shared secret.

```
Z =        140B8DC5 06909486 52D0F83D 104BAB64 61C64C71 A30C9B83
           6358C56D A2B114AE A0F6790E 52A35B6C AF1B8B97 7F590652
           FBB5D8E4 1F40FB5E 4DE8599C 484571E7 05790330 FA8189BA
           EC67FA2F 047F2195 CF2315EA B12FE734 E1D633AC 5EA92093
           EFC1E7DB 41E89C42 C008FD3E 8B506107 BCE653C3 A5F2E718
           A2442396 6874BA73 11D79DD3 C72BE9F2 F11D8EFE 6D77A4DA
           0921532A 272AC672 3BE0D008 9A33FAED 646A42EB 01D40EB2
           1E0A53E4 39DDF53F ED0DBA10 B930CB9C AE000032 87D4B3F0
           0BE3DDEF B1640485 35A665FB D9ADF83F E8E52745 F0B126E6
           E30008BD D16F8285 63C837C8 8EFDB4AD 7C80FCCB B474A6DF
           439E80CC CD9AA299 84F94E28 BA1BFEB4
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 04CDFFA2 A110A3E9 3CB476DD 64970360 73C8B633 B447D87E
             61A70E1A EDE2FA34 07508A32 50942876 58AB9E20 E494C7CE
             B579CF8C F996393D
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =      4CD FFA2A110 A3E93CB4 76DD6497

nonceV =  127F8E19 0549F774 1C0E62EE BC35B82D C9E884C5 A3D94742
          6765724C
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 5322B0D0 B59A3D19
            B924200D 6B6B387C 57BE84D0 AC7C98D8 8CB4639D 515404A5
            65E71F10 77CA88C9 C45D0975 516A719F 06C8F13A 6431FEC5
            0172FD96 0EDABC96 BC86551F 3FFBAD3F 7BBF08A9 64F3C8E3
            A2F39047 141521F3 1F85AC54 FAB4A2FA 97D05A0E 1CD21D57
            9A0314E8 48BA02D7 35109B2D A01DE7E2 21BE95FB 4F29BA7B
            02186640 13948315 9746776F F2CB8327 D435FEF3 52329A02
            4E25644A 9CD29378 375F24DB 4A4070A3 F292A0CE 56076B36
            25107F01 8FBCDE60 2FAE06E9 5D4476B4 4897AD38 13EF0E69
            C45E4975 587CD5D6 8DCBA825 353C899C 789B640B CC5DD073
            3D3C1219 3FC83F61 FBC04399 8579CF4F 3F1F3C2B 1F3B9C1B
            904B0F06 B6C37F71 127F8E19 0549F774 1C0E62EE BC35B82D
            C9E884C5 A3D94742 6765724C

MacTag_U  = FE688298 FEAFE2E4 C9C5836D DAACADDC 614E0530 99003E95
             105FF9A5
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 5322B0D0 B59A3D19
            B924200D 6B6B387C 57BE84D0 AC7C98D8 8CB4639D 515404A5
            65E71F10 77CA88C9 C45D0975 516A719F 06C8F13A 6431FEC5
```

```
            0172FD96 0EDABC96 BC86551F 3FFBAD3F 7BBF08A9 64F3C8E3
            A2F39047 141521F3 1F85AC54 FAB4A2FA 97D05A0E 1CD21D57
            9A0314E8 48BA02D7 35109B2D A01DE7E2 21BE95FB 4F29BA7B
            02186640 13948315 9746776F F2CB8327 D435FEF3 52329A02
            4E25644A 9CD29378 375F24DB 4A4070A3 F292A0CE 56076B36
            25107F01 8FBCDE60 2FAE06E9 5D4476B4 4897AD38 13EF0E69
            C45E4975 587CD5D6 8DCBA825 353C899C 789B640B CC5DD073
            3D3C1219 3FC83F61 FBC04399 8579CF4F 3F1F3C2B 1F3B9C1B
            904B0F06 B6C37F71

 MacTag_V  = E5226FE4 35C6F96F C52992C1 A2426DB2 A0A2FEED 006AD789
             F33E9B05
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 5322B0D0 B59A3D19
            B924200D 6B6B387C 57BE84D0 AC7C98D8 8CB4639D 515404A5
            65E71F10 77CA88C9 C45D0975 516A719F 06C8F13A 6431FEC5
            0172FD96 0EDABC96 BC86551F 3FFBAD3F 7BBF08A9 64F3C8E3
            A2F39047 141521F3 1F85AC54 FAB4A2FA 97D05A0E 1CD21D57
            9A0314E8 48BA02D7 35109B2D A01DE7E2 21BE95FB 4F29BA7B
            02186640 13948315 9746776F F2CB8327 D435FEF3 52329A02
            4E25644A 9CD29378 375F24DB 4A4070A3 F292A0CE 56076B36
            25107F01 8FBCDE60 2FAE06E9 5D4476B4 4897AD38 13EF0E69
            C45E4975 587CD5D6 8DCBA825 353C899C 789B640B CC5DD073
            3D3C1219 3FC83F61 FBC04399 8579CF4F 3F1F3C2B 1F3B9C1B
            904B0F06 B6C37F71 127F8E19 0549F774 1C0E62EE BC35B82D
            C9E884C5 A3D94742 6765724C

 MacTag_U  = 73416D87 80E362D7 9E041EC9 93567041 E862FCEF F423C233
             FD38CA4A

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U
```

```
            = 4B435F32 5F56424F 42425941 4C494345 127F8E19 0549F774
              1C0E62EE BC35B82D C9E884C5 A3D94742 6765724C 5322B0D0
              B59A3D19 B924200D 6B6B387C 57BE84D0 AC7C98D8 8CB4639D
              515404A5 65E71F10 77CA88C9 C45D0975 516A719F 06C8F13A
              6431FEC5 0172FD96 0EDABC96 BC86551F 3FFBAD3F 7BBF08A9
              64F3C8E3 A2F39047 141521F3 1F85AC54 FAB4A2FA 97D05A0E
              1CD21D57 9A0314E8 48BA02D7 35109B2D A01DE7E2 21BE95FB
              4F29BA7B 02186640 13948315 9746776F F2CB8327 D435FEF3
              52329A02 4E25644A 9CD29378 375F24DB 4A4070A3 F292A0CE
              56076B36 25107F01 8FBCDE60 2FAE06E9 5D4476B4 4897AD38
              13EF0E69 C45E4975 587CD5D6 8DCBA825 353C899C 789B640B
              CC5DD073 3D3C1219 3FC83F61 FBC04399 8579CF4F 3F1F3C2B
              1F3B9C1B 904B0F06 B6C37F71

MacTag_V    = 39D30820 F9E2DED0 DC3C16F3 6C9F8C96 7BCADDF0 C04AD4F7
              7470F329
```

3.3.6 dhOneFlow for finite field p2048-q224

- Prerequisites:

```
xV =        A01F624D 48AD5FD2 EA6F37C2 17C7A3A0 DE8C87DE 89DEF096
            138BFD96

yV =        142670DC 713C7584 EAB89C10 2898F9F4 DC3FA94D 116FFD6C
            B682B6A7 488E04F7 2CC60078 3182B499 FD7EF4AC 127F19D4
            85CFFF0D A1FB5D13 6201DA50 99B8D081 97530CB1 7FFEF040
            27484F4F 38536945 C56C96EA 540595E8 6799A50E 966111A5
            B5A98C1A C0545DF3 AD6F2513 A2E3A43B A5F8B26C 6FBFA820
            316527ED 8DF874ED 247FAF60 A7464A8D 5204B2BF 3E35AA75
            0CE5EF82 2F44D8D3 96851B77 790A4837 9B5B1BB7 FB750A1E
            EB596E03 F74DAEF1 6D0432D0 FB846EF7 E0E97E4E A5FD941D
            A389ECED 4A376755 46B92DFF D3E5049F 480731C0 3149FCD2
            1AEFE734 289FA9E6 4F4DAB1C C29E8F17 35533AE0 B05E9079
            AC7FCD6A B89B0812 362A8ACA C4763046
```

BEGIN U's calculations

- Step 1:

```
rU =      9424284D 0FB6108F 9A2FDD3C 36182FD1 547AD8F7 7B7CE22F
          F3988DCD

tU =      2B60B150 6B3AC0EF 11D85601 E7F5890C 97609407 A0E178E5
          3543996F F83912AE 05AA3151 6AE22CAE CD23B86D 3431B580
          12A7BBB0 92C503B9 8E867E43 97EF7A9B 26C6DADC 07A74A57
          73C27162 221634E4 07CB3C58 F6294B14 380C902F 01360D2B
          737AE20B 28B02CB7 C40A1B8A 2F8F81AF 82E36DC5 03A6BFCA
          087D5025 BF1B60C1 3A8D6E01 A745A00E EB344A76 103E71FC
          A73AF143 92FA9FCC 0E8B7103 2011D40F 1932BA0E 30A431A6
          C9B236AC 0AA40C0F 0A5EF5CC 0B6B53A5 D442465A A45DA902
          8B846B43 1F4078FB 08E0CA5C D40D382A 32678E22 7B72A0F7
          07ACA352 E43C9B49 8AD87B24 BC39714B 9926DBCF F5BD02DF
          BEE14BFA 9E963341 A842BC23 017A2D6E
```

- Step 2: Decimal value for shared secret.

```
Z =       1421542413505125237299895035579863207862875697955 4
          199516205392885525712251644548067268799822366145 03
          853354048079378727644472783235975960474502496432 18
          281680241622495204692054541022159642155337192027 10
          146634965210555984385586436359688757295747530596 34
          221526779222638827969068750885323201310668033896 79
          314937219157616478849301976961105952107103986104 79
          586552684634486216967780893593116293215170581595 85
          553054559230082841241305504844825320646812108564 57
          531253336917947801547814748719184033174889542577 96
          731097349758229572722850356680092847282935599559 34
          743459821699673374782785907704533433336758103055 73
          93775495949932551
```

- Step 3: Hex value for shared secret.

```
Z =       709B9C12 178888E5 A2B5E521 25F5BECB 6B722FDF 9523DB87
          1E4DC2C4 61D31A73 959B310B 1A3AA162 63BCA84A 227A0B97
```

```
A328978E 47F1611D 8A4D2FC6 7F1BE728 0185C564 9C2A0B97
5A4EDE3F 534BFDEE BF4D0ED6 99289B57 1E3E9572 A06FD588
FBD4D7AB 39034174 09CD367C BF853030 EF38A5DA EDC6D28C
89075AC4 56187357 A8C5C8C2 03810146 46FA0587 1384FAE3
7E61AA8A EB74BA71 0DD62ECB 18F8E755 3343463B 89F347F3
7BD8E01D 5089828F 946DC6FF 9AC75A3C E8C1345A 0010E780
3F0C556E 6B5C034A 19422DEE F5EB3B19 C697EB28 323F48CC
EE31BD4E D2809140 91DEB4A4 7C4D7EF7 05C21E9D 25A4112E
060E4009 0F762871 4757F07D B5AD5807
```

- Step 4: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 6B45A37B DA1865BE 63873C02 2E8AA105 35F40188 7BCB0481
             656D1502 54404344 1A1662FF FA3C25F6 72E1B933 6EBFA469
             C26C7CF6 313EE0ED
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
rU =      9424284D 0FB6108F 9A2FDD3C 36182FD1 547AD8F7 7B7CE22F
          F3988DCD

tU =      2B60B150 6B3AC0EF 11D85601 E7F5890C 97609407 A0E178E5
          3543996F F83912AE 05AA3151 6AE22CAE CD23B86D 3431B580
          12A7BBB0 92C503B9 8E867E43 97EF7A9B 26C6DADC 07A74A57
          73C27162 221634E4 07CB3C58 F6294B14 380C902F 01360D2B
          737AE20B 28B02CB7 C40A1B8A 2F8F81AF 82E36DC5 03A6BFCA
          087D5025 BF1B60C1 3A8D6E01 A745A00E EB344A76 103E71FC
          A73AF143 92FA9FCC 0E8B7103 2011D40F 1932BA0E 30A431A6
          C9B236AC 0AA40C0F 0A5EF5CC 0B6B53A5 D442465A A45DA902
          8B846B43 1F4078FB 08E0CA5C D40D382A 32678E22 7B72A0F7
          07ACA352 E43C9B49 8AD87B24 BC39714B 9926DBCF F5BD02DF
          BEE14BFA 9E963341 A842BC23 017A2D6E
```

- Step 2: N/A.
- Step 3: Decimal value for shared secret.

```
Z =        1421542413505125237299895035579863207862875697955 4
           1995162053928855257122516445480672687998223661450 3
           8533540480793787276444727832359759604745024964321 8
           2816802416224952046920545410221596421553371920271 0
           1466349652105559843855864363596887572957475305963 4
           2215267792226388279690687508853232013106680338967 9
           3149372191576164788493019769611059521071039861047 9
           5865526846344862169677808935931162932151705815958 5
           5530545592300828412413055048448253206468121085645 7
           5312533369179478015478147487191840331748895425779 6
           7310973497582295727228503566800928472829355995593 4
           7434598216996733747827859077045334333367581030557 3
           93775495949932551
```

- Step 4: Hex value for shared secret.

```
Z =        709B9C12 178888E5 A2B5E521 25F5BECB 6B722FDF 9523DB87
           1E4DC2C4 61D31A73 959B310B 1A3AA162 63BCA84A 227A0B97
           A328978E 47F1611D 8A4D2FC6 7F1BE728 0185C564 9C2A0B97
           5A4EDE3F 534BFDEE BF4D0ED6 99289B57 1E3E9572 A06FD588
           FBD4D7AB 39034174 09CD367C BF853030 EF38A5DA EDC6D28C
           89075AC4 56187357 A8C5C8C2 03810146 46FA0587 1384FAE3
           7E61AA8A EB74BA71 0DD62ECB 18F8E755 3343463B 89F347F3
           7BD8E01D 5089828F 946DC6FF 9AC75A3C E8C1345A 0010E780
           3F0C556E 6B5C034A 19422DEE F5EB3B19 C697EB28 323F48CC
           EE31BD4E D2809140 91DEB4A4 7C4D7EF7 05C21E9D 25A4112E
           060E4009 0F762871 4757F07D B5AD5807
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 6B45A37B DA1865BE 63873C02 2E8AA105 35F40188 7BCB0481
             656D1502 54404344 1A1662FF FA3C25F6 72E1B933 6EBFA469
             C26C7CF6 313EE0ED
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     6B45 A37BDA18 65BE6387 3C022E8A
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 2B60B150 6B3AC0EF
            11D85601 E7F5890C 97609407 A0E178E5 3543996F F83912AE
            05AA3151 6AE22CAE CD23B86D 3431B580 12A7BBB0 92C503B9
            8E867E43 97EF7A9B 26C6DADC 07A74A57 73C27162 221634E4
            07CB3C58 F6294B14 380C902F 01360D2B 737AE20B 28B02CB7
            C40A1B8A 2F8F81AF 82E36DC5 03A6BFCA 087D5025 BF1B60C1
            3A8D6E01 A745A00E EB344A76 103E71FC A73AF143 92FA9FCC
            0E8B7103 2011D40F 1932BA0E 30A431A6 C9B236AC 0AA40C0F
            0A5EF5CC 0B6B53A5 D442465A A45DA902 8B846B43 1F4078FB
            08E0CA5C D40D382A 32678E22 7B72A0F7 07ACA352 E43C9B49
            8AD87B24 BC39714B 9926DBCF F5BD02DF BEE14BFA 9E963341
            A842BC23 017A2D6E

MacTag_V  = F32AC736 B93E62A7 55BC5FFB 2F759C8D 1A3CE63B E7FAA806
             84E79400
```

3.3.7 dhStatic for finite field p2048-q224

- Prerequisites:

```
xU =      37771A6C 04AC7F44 31F72CAE 83207E7F E20BC32D C3A72C20
          14499018

yU =      ABE34B79 CDE5D4F8 22284AA2 16B3EE36 1D5C80CA F36FBFB5
          62FFFC53 3F0F135E FF484B07 ED64CCEE D3BD636F 8667E68C
          B07AF6E0 83F048AF 4844CE22 0AB58FB9 235B7F21 CA16F32B
```

```
            4AE24B35 7FA4E322 A477BAD1 DC8D63B0 8CC6B796 B44C7D7A
            B45D9209 19CA56AF 0A7C8866 9CF16D23 F8305A96 AE2A167F
            D96B1884 F13D8CE3 A5A70484 EDEC6909 263F5FC0 60F56E20
            388B5BF6 A93B73C6 F16CD21A 6058CB0F DB102AFB 25404DD0
            2605DDEC 72A5D297 B882A0A7 36788298 C160FF9F 5509C9B3
            F9C2A984 3D46C15E 64736FDF 1B737ED3 D070B5FD 0FB3BC6E
            1BC5AC0E 88A536E8 9F7E8B11 B4046F8D CCFDACFF CDC0C2CD
            A366026D 71BADAAD 869BD984 7E628E7C

xV =        3AF20255 267E7209 378F9495 7B7186A0 73BA18A4 5B9A1F1B
            727E8A1C

yV =        A772D1BB 7C66AE4A 9237E671 D7B2C981 E796EFE5 C0B23FEB
            2BE90B80 1D9C896E 1ADD82A3 93B9DA8A 66227D79 51CA13A1
            11020521 A6313795 1A893B4D 02643159 74F3571D DA54FF9E
            AB9CC47B BEB20317 A227335A 5066F6CC EE89F093 B37D2417
            09EA8D86 CF48A971 513F04FC 8CBEFF73 46024BC5 E543A205
            6B201020 BD6C14D2 6342CCC5 28ABD0AD 5D103CCD 3B09E1D1
            205176AD C5A2888C 6DB04CA0 00ECFFEC 46571046 C7FFFD73
            90F8C09B FFC5E3F9 CC7B3541 C05A28B4 19B4648F 23E4C897
            2742E451 685626FB 2073A0D8 4C5664D6 642D824C 18215429
            777DF837 4E555F12 9129E474 4AA5D9A8 BA220A98 3AFBA3C5
            EC823F4B 4C86FDD5 6DC7E86D B5B9AFF6
```

BEGIN U's calculations

- Step 1:

```
nonceU =    4A23EA37 4B5C9BCA 5F42E584 4881806C F1241218 C4BDAF7F
            6E4FF6A2
```

- Step 2: Decimal value for shared secret.

```
Z =         38228407595297545827222085139884109649122359507556
            05670585412145234680996937913637525598692091569849
            27716143220729516222769995327343162376881736046827
            57933055608886535013804263158549167607560413489760
            42861150987026210098761577500034041952557372864290
```

```
184507481258312797855285564028005624915401881177 12
242895786753984324427311068123187518838854943510 4
220583874746563346410151274629996204247226585273 01
025941557981750070078300233207147312116270579626 51
001517946628048742906057529607895447589599276884 85
208586931593468578218520452135795511443242703402 21
719213759166709751278210390287330081650062703045 29
8381911174265622
```

- Step 3: Hex value for shared secret.

```
Z =        1E486120 1D438969 BD518246 DD5DBEDB B1F143AF B1511F5F
           B3465DA7 E93ECAF3 04F201BD D6CE2ABC 7765F4B1 B9F5A05B
           4C88033E 8D8CE266 B45D1D68 B6A3175E 20F1CFC5 25B7C78B
           86176057 22B1935E 985AE285 7519B5EB 9D7FC7A5 DC1312F5
           116EEADF 37616B97 A2281869 3AC9C9D0 D07E6E41 65B28CD0
           EE827C16 F681156E 18C74723 8B9177DD 9789A201 46DC0D7D
           D29737DE B32BA252 4D0A5E56 1150E0CE A5A56199 CBC573F9
           9A741385 0D24B845 635E9923 3ACF8DB8 7E3161CC C583A505
           E9D4C4DA 8D0331D4 98E8F050 9262AAFE E9E0DE14 66923C28
           BF16F12B 4470F297 226EBE66 0F13D879 6A3795D1 571C9E7A
           1F7FCA14 EF3B5656 FE6920DB 82E5BB16
```

- Step 4: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 0000001C 4A23EA37
             4B5C9BCA 5F42E584 4881806C F1241218 C4BDAF7F 6E4FF6A2
             424F4242 59343536

DerKeyMat  = 64D5FC20 F8561DD6 F8E4D358 FF1CEA9C 714C5EBD 37772D66
             2955B3D3 4EAF9874 594CAC62 FC009580 5122AFA3 60B1996D
             59FD46C8 630ED334
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
nonceU =  4A23EA37 4B5C9BCA 5F42E584 4881806C F1241218 C4BDAF7F
          6E4FF6A2
```

- Step 2: Decimal value for shared secret.

```
Z =       38228407595297545827222085139884109649122359507556
          05670585412145234680996937913637525598692091569849
          27716143220729516222769995327343162376881736046827
          57933055608886535013804263158549167607560413489760
          42861150987026210098761577500034041952557372864290
          18450748125831279785528556402800562491540188117712
          24289578675398432442731106812318751883885494351 04
          22058387474656334641015127462999620424722658527301
          02594155798175007007830023320714731211627057962651
          00151794662804874290605752960789544758959927688485
          20858693159346857821852045213579551144324270340221
          71921375916670975127821039028733008165006270304529
          8381911174265622
```

- Step 3: Hex value for shared secret.

```
Z =       1E486120 1D438969 BD518246 DD5DBEDB B1F143AF B1511F5F
          B3465DA7 E93ECAF3 04F201BD D6CE2ABC 7765F4B1 B9F5A05B
          4C88033E 8D8CE266 B45D1D68 B6A3175E 20F1CFC5 25B7C78B
          86176057 22B1935E 985AE285 7519B5EB 9D7FC7A5 DC1312F5
          116EEADF 37616B97 A2281869 3AC9C9D0 D07E6E41 65B28CD0
          EE827C16 F681156E 18C74723 8B9177DD 9789A201 46DC0D7D
          D29737DE B32BA252 4D0A5E56 1150E0CE A5A56199 CBC573F9
          9A741385 0D24B845 635E9923 3ACF8DB8 7E3161CC C583A505
          E9D4C4DA 8D0331D4 98E8F050 9262AAFE E9E0DE14 66923C28
          BF16F12B 4470F297 226EBE66 0F13D879 6A3795D1 571C9E7A
          1F7FCA14 EF3B5656 FE6920DB 82E5BB16
```

- Step 4: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 0000001C 4A23EA37
             4B5C9BCA 5F42E584 4881806C F1241218 C4BDAF7F 6E4FF6A2
             424F4242 59343536
```

```
DerKeyMat  = 64D5FC20 F8561DD6 F8E4D358 FF1CEA9C 714C5EBD 37772D66
             2955B3D3 4EAF9874 594CAC62 FC009580 5122AFA3 60B1996D
             59FD46C8 630ED334
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     64D5 FC20F856 1DD6F8E4 D358FF1C

nonceV =  3D0C33C1 61DB1311 EB467369 F5F225FA 9A275A6E E15825FB
          F31AB335
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 4A23EA37 4B5C9BCA
            5F42E584 4881806C F1241218 C4BDAF7F 6E4FF6A2 3D0C33C1
            61DB1311 EB467369 F5F225FA 9A275A6E E15825FB F31AB335

MacTag_U  = A122A341 9EE23D83 CC7BC381 82C4D4B4 0F12F829 28C7F4DF
            BA46B79C
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 4A23EA37 4B5C9BCA
            5F42E584 4881806C F1241218 C4BDAF7F 6E4FF6A2

MacTag_V  = C92D059E F716EA2F F308E761 3DCD9AC0 E770143D 68AD87EC
            4BA57EE2
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
            = 4B435F32 5F55414C 49434542 4F424259 4A23EA37 4B5C9BCA
              5F42E584 4881806C F1241218 C4BDAF7F 6E4FF6A2 3D0C33C1
              61DB1311 EB467369 F5F225FA 9A275A6E E15825FB F31AB335

 MacTag_U  = AD894167 B37D4290 4A78DCF2 6CD303BF F3FBE340 64B7B4B9
              691DF8E9

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

            = 4B435F32 5F56424F 42425941 4C494345 3D0C33C1 61DB1311
              EB467369 F5F225FA 9A275A6E E15825FB F31AB335 4A23EA37
              4B5C9BCA 5F42E584 4881806C F1241218 C4BDAF7F 6E4FF6A2

 MacTag_V  = 5B09D35B 47CA9369 2E8E2BA8 A79F89F5 1B1D3BC4 B1E69459
              9DB39D9E
```

3.4 Test data for 2048–bit prime p and 256–bit prime q

In this section, we supply step–by–step test data for the seven finite field key agreement schemes described in [1, section 6] using the parameter set $p2048$–$q256$ described in Section 2.3. For each scheme, a reference to the corresponding section in [1] is provided.

3.4.1 dhHybrid1 for finite field p2048-q256

- Prerequisites:

```
xU =      3AE68B99 B70BB90F B4EFC2A3 3C83AF0F 606762BF E9B34E4E
          EFE5C123 5F7B9FC0
```

```
yU =      425E4CDC BEF08130 CEEBC5E5 12EA6D40 A9434062 CAD43B23
          D5E23AA3 914F34BB 36F32F97 6E5465A2 9747554C F016D7D5
          F95ED81B 9A4983EC 4611D5B2 D9CFFDCB 83E853E7 1F746271
          05DC9E45 AA2DFC1A F2DEDF7F 6D18349A 53241AD1 92229984
          F6441FB4 DD70AD81 CBAE7447 67CF3474 761F16DD 91CB8768
          44814686 10728163 12B70D89 6990781B CB48CE2D E73B8099
          8A136A7B 98CCF739 00E8A9C5 B333345B 474C818C 8D1C481E
          BC2ADA0B 4AC5CE4D 7804096E E7DAB63B 5A195A09 3E2EF1A1
          8C2FF6B1 3B1DB21A B4A64FE7 68EC0544 15EC86EB 32161939
          B165807C 929528CC FE5E10B1 F402491B 01F1B286 122C645F
          C81C0503 4B66E28F 00E53D84 3A501CE2

xV =      2CE2DCDB 3B767F9E BD883178 1A74DB8F 9BCD9FA2 3E589630
          DDDD3F9A A7F1B027

yV =      73AC4BAD 1AEF0782 F019EB87 7CCEA247 F95B158A 8177CF91
          DF5469CB F013EDCE E30550A9 C668B8DE B44FC2D6 91934EDE
          1DF8F702 C19A85E6 823EEE05 D04BF274 EE62AEF1 68497B57
          A1489B78 DC84EFB7 4411533E BEC049F1 3DADC407 382EEF46
          7C4FF8FD 71006723 0B5B54C2 DB379504 8659907C 5859914C
          A743150E 09255C59 C65BFC74 EB03DF03 27594A83 DF2BA7E5
          7FDD989A 46B68990 387FC520 022625C3 74FE7657 95569B53
          F0BE89DC FBFA736D A73A97F8 471F24FC C2EEB4D7 6E0FE0A7
          AD81F1AB ADC256F8 50FDF19A 42D4488F 6FA7F34A 041DCDE9
          ACB98F27 AE74DCA9 40D7D0FF 7AEEF1E7 EBB0C97A 39E9CD1C
          F0A19929 D04582CB F8B55784 828E911A
```

- Step 1: U produces rU, tU and receives tV. U DOES NOT RECEIVE rV (shown only for the purpose of verifying this data).

```
rU =      6D12B3DB 72105EEF 40DA18C7 66D54EFC BF49D1EC D9143B81
          29FD50C3 454AC0F8

tU =      776204C1 DD00AE99 470F7152 5455E518 ABE02404 29D3D679
          96E522DC A1030D20 F824CFB2 3FC5AA31 47D9B353 05EB2303
          791965DD BC84F1A0 1182AED4 3D56BA0E 00405304 032DB61E
          5DCA9E6C 8921BAF3 B010DA93 BFB36747 96F44D29 CCA6AE4E
```

```
            F11FA51C 11F34406 60E7639B 9F9819CA D2746734 79A5CF97
            8E03F8C1 C7D6EC48 39B3D0C3 6EA5C34A 46D3C921 DB7EDCD0
            B39185D2 E89143EB 0B5A03EB AF12A8EE 0D6333C4 9259CAA2
            5FCA903C 39388750 2561A135 28503FDD 77B658ED F4278F34
            8A8B548E 489EF357 71A25DE9 B0647F4F CDC5F5E4 D73DACD6
            44C00D2F 15206A17 D10D34FC B48C0292 2180D348 9686CCAF
            9DC63837 46DFDA1C 124E433C E5B5158A

rV =        284F486A A9679306 70565602 B10A1CD9 AF2A27C4 96730BA1
            32044D00 2F6A0417

tV =        7D04B9E5 3FEF9586 CE9507B2 3B0AE337 5B09663D D3A1D03B
            230826E9 D57828E7 5B438123 09CBD78A 8DC8926C 7E66B2F1
            05DEDAF3 27936800 E54E8DEC 52F3829B 6005CED6 5BB8BEFB
            65704C21 73D14759 B35AD5B0 64B86C4B D3915A0A 956160C0
            91AA14AC D96D1DD8 66C9C015 31054F9A EA307E3F 71E109FD
            A0BD9692 B7F79D30 C8763242 490F444E 84C71956 4A8A52E3
            6650FC33 FAB25E2D A54E0A4D 6EA23179 18A5A5DF 2298BA39
            8EA2DCFC D51C5C3B E2F969F8 82A2EDA3 B4BF129A 52088943
            97537C84 A3BE67E9 8948B333 A388E3E9 14223F03 6EE75218
            0CB13DCD 57191D83 4FAE396D 6F6242A3 D292BA77 D3EE9DEE
            140FFD68 548AB5F9 F2D9D1A7 B896008E
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =       170534274287163821713462734929255587197769902100 14
            554857619257160615736159245123400710750680934774 32
            947850032921278913267172806262178582973049539702 10
            726571392124080009088059820685681462843519950362 88
            867365235579936589396615628720666076599359962291 71
            083505885578271675978091110905014144856462338749 10
            822080393486683006547385402012530257194322910854 95
            147311270270827609588569020440635118422373689066 35
            566405812006213699041938952096765507865497163081 95
            886645002878425036202409232272932543568077091974 19
            005820861936413974002375317681497755224879831344 12
```

```
0184167976412832189832645051521132652350214881649 5
5600742498285103

Z_s =     0D82485C F7D62FFC EA343388 CFEC1527 3A394B84 32EEB632
          1BE31D4F CD1615C8 1C6937C0 8D92416E DBDD2010 FA8B6E0A
          8A603DAD E010BC9C D76B14E3 E2190E3B A300E71A DDBF244C
          F8062949 76EAF07D 023BDB57 FC5D1964 C7D4206E 72061BFE
          1EE4EEBC 9200E13A 6CBA3286 9DBE8082 CDF3645B 5A727DD2
          7CA503F4 EDEB73E8 8A3A552C 7E00D4EE 72421372 36A0965C
          1EC3EBC0 B48C2B46 7EB84241 5A283F55 E220FFD1 8819256D
          A2474D28 FC3B04E0 C07E4D25 C1749341 D2229701 5CD8178C
          3918BE8C 5CDF0FBF BB9A5ACC DD82AF07 83EFE4DF 64A8D892
          828F8DE5 8C5D569B 5B084558 96C4D3C3 4FD3CE93 C434C38E
          F56CED30 561C371A F9F2D864 FDC5B62F
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     8704779961141820537257085925016212217050860552755 1
          5766663280397127769902232918334397610206338279402 5
          2905683714709206859155449401950462863806070443869 6
          7294662145805285485359955362465759102557335736574 0
          7522354801598759810359171492649307688025540418508 6
          7354569059858535984032872251313767222211405600609 6
          5395796946507662460060865835150641858494061426796 0
          2102181825031368165780034078393469686544288506475 2
          4147041349452391884198195548086680455001602805953 9
          6918235106953020143113117417656013825223427327396 4
          6148939905372183434791575771200786089678509442381 5
          1809037801201343112961409802451585098109664302712 6
          0325811175523915

Z_e =     44F48409 F31BF350 9451DB4D 304BEBD8 3C2AD650 1C1B85E6
          32BC9258 8E2D48B5 D2B84444 62AD94E8 A444941E D4975C97
          9117D75A 0A2BA810 DFA8804A 0FE9426D D7EB95F2 9CA430DA
          37EFA52C 42DA1DE2 23763BDD C95E466A A3B8D206 B8218EDF
          23973D05 F3C7C22B 224653D4 F9218545 7983262F 27BC55A0
          A7AEE543 5455D43C 0E0C6D80 67ADAF90 42B6B777 7E198D67
```

```
60830D96 B29A6AAE F574D75E 2D654355 0F7555CF 8982C821
C4EC9B82 662B0936 69FD246D 4DCCBFF3 1D984EF6 3C4F95D7
39C77E66 F69B6DB0 D9FC1A97 3F5233D1 1FE7154B 8A6BE150
467D92DA F0914434 F0CF176E 961B313F E3E23BFE 378B87BA
F273937F FAA68565 8B09781D 2697864B
```

- Step 5: Shared secret.

```
Z =       44F48409 F31BF350 9451DB4D 304BEBD8 3C2AD650 1C1B85E6
          32BC9258 8E2D48B5 D2B84444 62AD94E8 A444941E D4975C97
          9117D75A 0A2BA810 DFA8804A 0FE9426D D7EB95F2 9CA430DA
          37EFA52C 42DA1DE2 23763BDD C95E466A A3B8D206 B8218EDF
          23973D05 F3C7C22B 224653D4 F9218545 7983262F 27BC55A0
          A7AEE543 5455D43C 0E0C6D80 67ADAF90 42B6B777 7E198D67
          60830D96 B29A6AAE F574D75E 2D654355 0F7555CF 8982C821
          C4EC9B82 662B0936 69FD246D 4DCCBFF3 1D984EF6 3C4F95D7
          39C77E66 F69B6DB0 D9FC1A97 3F5233D1 1FE7154B 8A6BE150
          467D92DA F0914434 F0CF176E 961B313F E3E23BFE 378B87BA
          F273937F FAA68565 8B09781D 2697864B 0D82485C F7D62FFC
          EA343388 CFEC1527 3A394B84 32EEB632 1BE31D4F CD1615C8
          1C6937C0 8D92416E DBDD2010 FA8B6E0A 8A603DAD E010BC9C
          D76B14E3 E2190E3B A300E71A DDBF244C F8062949 76EAF07D
          023BDB57 FC5D1964 C7D4206E 72061BFE 1EE4EEBC 9200E13A
          6CBA3286 9DBE8082 CDF3645B 5A727DD2 7CA503F4 EDEB73E8
          8A3A552C 7E00D4EE 72421372 36A0965C 1EC3EBC0 B48C2B46
          7EB84241 5A283F55 E220FFD1 8819256D A2474D28 FC3B04E0
          C07E4D25 C1749341 D2229701 5CD8178C 3918BE8C 5CDF0FBF
          BB9A5ACC DD82AF07 83EFE4DF 64A8D892 828F8DE5 8C5D569B
          5B084558 96C4D3C3 4FD3CE93 C434C38E F56CED30 561C371A
          F9F2D864 FDC5B62F
```

- Step 6: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 4235AC89 C9F33E5D BB11601A 2983E376 E2153997 87D839A0
             3855FE04 533E1A67 66915E67 C25EEB04 0828E96C D3D6EF0A
             B7D17B43 1343A7F3 AAC68F0C 4A7E779B
```

- If key confirmation is performed, then

```
MacKey  = 4235AC89 C9F33E5D BB11601A 2983E376
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 776204C1 DD00AE99
            470F7152 5455E518 ABE02404 29D3D679 96E522DC A1030D20
            F824CFB2 3FC5AA31 47D9B353 05EB2303 791965DD BC84F1A0
            1182AED4 3D56BA0E 00405304 032DB61E 5DCA9E6C 8921BAF3
            B010DA93 BFB36747 96F44D29 CCA6AE4E F11FA51C 11F34406
            60E7639B 9F9819CA D2746734 79A5CF97 8E03F8C1 C7D6EC48
            39B3D0C3 6EA5C34A 46D3C921 DB7EDCD0 B39185D2 E89143EB
            0B5A03EB AF12A8EE 0D6333C4 9259CAA2 5FCA903C 39388750
            2561A135 28503FDD 77B658ED F4278F34 8A8B548E 489EF357
            71A25DE9 B0647F4F CDC5F5E4 D73DACD6 44C00D2F 15206A17
            D10D34FC B48C0292 2180D348 9686CCAF 9DC63837 46DFDA1C
            124E433C E5B5158A 7D04B9E5 3FEF9586 CE9507B2 3B0AE337
            5B09663D D3A1D03B 230826E9 D57828E7 5B438123 09CBD78A
            8DC8926C 7E66B2F1 05DEDAF3 27936800 E54E8DEC 52F3829B
            6005CED6 5BB8BEFB 65704C21 73D14759 B35AD5B0 64B86C4B
            D3915A0A 956160C0 91AA14AC D96D1DD8 66C9C015 31054F9A
            EA307E3F 71E109FD A0BD9692 B7F79D30 C8763242 490F444E
            84C71956 4A8A52E3 6650FC33 FAB25E2D A54E0A4D 6EA23179
            18A5A5DF 2298BA39 8EA2DCFC D51C5C3B E2F969F8 82A2EDA3
            B4BF129A 52088943 97537C84 A3BE67E9 8948B333 A388E3E9
            14223F03 6EE75218 0CB13DCD 57191D83 4FAE396D 6F6242A3
            D292BA77 D3EE9DEE 140FFD68 548AB5F9 F2D9D1A7 B896008E

MacTag_U  = A9D7D7F9 439C737C 97D65250 7F4CDEFE 0BA44074 03D1FE50
            6769A5B0 FBFD121A
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U
```

```
= 4B435F31 5F56424F 42425941 4C494345 7D04B9E5 3FEF9586
  CE9507B2 3B0AE337 5B09663D D3A1D03B 230826E9 D57828E7
  5B438123 09CBD78A 8DC8926C 7E66B2F1 05DEDAF3 27936800
  E54E8DEC 52F3829B 6005CED6 5BB8BEFB 65704C21 73D14759
  B35AD5B0 64B86C4B D3915A0A 956160C0 91AA14AC D96D1DD8
  66C9C015 31054F9A EA307E3F 71E109FD A0BD9692 B7F79D30
  C8763242 490F444E 84C71956 4A8A52E3 6650FC33 FAB25E2D
  A54E0A4D 6EA23179 18A5A5DF 2298BA39 8EA2DCFC D51C5C3B
  E2F969F8 82A2EDA3 B4BF129A 52088943 97537C84 A3BE67E9
  8948B333 A388E3E9 14223F03 6EE75218 0CB13DCD 57191D83
  4FAE396D 6F6242A3 D292BA77 D3EE9DEE 140FFD68 548AB5F9
  F2D9D1A7 B896008E 776204C1 DD00AE99 470F7152 5455E518
  ABE02404 29D3D679 96E522DC A1030D20 F824CFB2 3FC5AA31
  47D9B353 05EB2303 791965DD BC84F1A0 1182AED4 3D56BA0E
  00405304 032DB61E 5DCA9E6C 8921BAF3 B010DA93 BFB36747
  96F44D29 CCA6AE4E F11FA51C 11F34406 60E7639B 9F9819CA
  D2746734 79A5CF97 8E03F8C1 C7D6EC48 39B3D0C3 6EA5C34A
  46D3C921 DB7EDCD0 B39185D2 E89143EB 0B5A03EB AF12A8EE
  0D6333C4 9259CAA2 5FCA903C 39388750 2561A135 28503FDD
  77B658ED F4278F34 8A8B548E 489EF357 71A25DE9 B0647F4F
  CDC5F5E4 D73DACD6 44C00D2F 15206A17 D10D34FC B48C0292
  2180D348 9686CCAF 9DC63837 46DFDA1C 124E433C E5B5158A

MacTag_V  = 1A102044 DB2D371A 6B0F4A8F 65AC2068 95ECAFF3 B1B972F8
            FE8064A3 65C8F99A
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 776204C1 DD00AE99
            470F7152 5455E518 ABE02404 29D3D679 96E522DC A1030D20
            F824CFB2 3FC5AA31 47D9B353 05EB2303 791965DD BC84F1A0
            1182AED4 3D56BA0E 00405304 032DB61E 5DCA9E6C 8921BAF3
            B010DA93 BFB36747 96F44D29 CCA6AE4E F11FA51C 11F34406
            60E7639B 9F9819CA D2746734 79A5CF97 8E03F8C1 C7D6EC48
            39B3D0C3 6EA5C34A 46D3C921 DB7EDCD0 B39185D2 E89143EB
```

```
                0B5A03EB AF12A8EE 0D6333C4 9259CAA2 5FCA903C 39388750
                2561A135 28503FDD 77B658ED F4278F34 8A8B548E 489EF357
                71A25DE9 B0647F4F CDC5F5E4 D73DACD6 44C00D2F 15206A17
                D10D34FC B48C0292 2180D348 9686CCAF 9DC63837 46DFDA1C
                124E433C E5B5158A 7D04B9E5 3FEF9586 CE9507B2 3B0AE337
                5B09663D D3A1D03B 230826E9 D57828E7 5B438123 09CBD78A
                8DC8926C 7E66B2F1 05DEDAF3 27936800 E54E8DEC 52F3829B
                6005CED6 5BB8BEFB 65704C21 73D14759 B35AD5B0 64B86C4B
                D3915A0A 956160C0 91AA14AC D96D1DD8 66C9C015 31054F9A
                EA307E3F 71E109FD A0BD9692 B7F79D30 C8763242 490F444E
                84C71956 4A8A52E3 6650FC33 FAB25E2D A54E0A4D 6EA23179
                18A5A5DF 2298BA39 8EA2DCFC D51C5C3B E2F969F8 82A2EDA3
                B4BF129A 52088943 97537C84 A3BE67E9 8948B333 A388E3E9
                14223F03 6EE75218 0CB13DCD 57191D83 4FAE396D 6F6242A3
                D292BA77 D3EE9DEE 140FFD68 548AB5F9 F2D9D1A7 B896008E

 MacTag_U  = CDE1E574 073FE04C E099E059 94E4F5D9 8139C84A B248AD08
                85714776 09CA817A

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

           = 4B435F32 5F56424F 42425941 4C494345 7D04B9E5 3FEF9586
                CE9507B2 3B0AE337 5B09663D D3A1D03B 230826E9 D57828E7
                5B438123 09CBD78A 8DC8926C 7E66B2F1 05DEDAF3 27936800
                E54E8DEC 52F3829B 6005CED6 5BB8BEFB 65704C21 73D14759
                B35AD5B0 64B86C4B D3915A0A 956160C0 91AA14AC D96D1DD8
                66C9C015 31054F9A EA307E3F 71E109FD A0BD9692 B7F79D30
                C8763242 490F444E 84C71956 4A8A52E3 6650FC33 FAB25E2D
                A54E0A4D 6EA23179 18A5A5DF 2298BA39 8EA2DCFC D51C5C3B
                E2F969F8 82A2EDA3 B4BF129A 52088943 97537C84 A3BE67E9
                8948B333 A388E3E9 14223F03 6EE75218 0CB13DCD 57191D83
                4FAE396D 6F6242A3 D292BA77 D3EE9DEE 140FFD68 548AB5F9
                F2D9D1A7 B896008E 776204C1 DD00AE99 470F7152 5455E518
                ABE02404 29D3D679 96E522DC A1030D20 F824CFB2 3FC5AA31
                47D9B353 05EB2303 791965DD BC84F1A0 1182AED4 3D56BA0E
                00405304 032DB61E 5DCA9E6C 8921BAF3 B010DA93 BFB36747
                96F44D29 CCA6AE4E F11FA51C 11F34406 60E7639B 9F9819CA
```

```
              D2746734 79A5CF97 8E03F8C1 C7D6EC48 39B3D0C3 6EA5C34A
              46D3C921 DB7EDCD0 B39185D2 E89143EB 0B5A03EB AF12A8EE
              0D6333C4 9259CAA2 5FCA903C 39388750 2561A135 28503FDD
              77B658ED F4278F34 8A8B548E 489EF357 71A25DE9 B0647F4F
              CDC5F5E4 D73DACD6 44C00D2F 15206A17 D10D34FC B48C0292
              2180D348 9686CCAF 9DC63837 46DFDA1C 124E433C E5B5158A

MacTag_V  = 2A5994C4 439987DA F3D0F0E2 E37B9A9E 466C3451 EC85B5E5
              821E3321 4B4CC00F
```

3.4.2 MQV2 for finite field p2048-q256

- Prerequisites:

```
xU =      80B650EB 3F3A0756 61E749BE 7C014D00 682414BE B5C22B02
          CD5F415C 31DD714D

yU =      3BC0117F DBBC6876 A001AAA2 809ABAC6 1388AD25 DE6DFC5D
          51E973B7 8E5B0C83 BAA6E255 40945C98 9A58C94E F774D371
          8BF0757C B83BADD8 FF045394 09A21B4D E908A4D2 8BAF3D92
          49C69F3A 49BE59AC FA629CE3 E956FBC0 5E8C6E49 30094B16
          AA7436B0 DDC35023 CD261566 ABCBC3DE BD8D11AC 92EF2358
          9596216D 994C8EC4 024DC38A 4362BC3C 8B8C0A75 C8A8D322
          594D4768 B838E850 846CE1EB E338B493 72D5C7EB B011C943
          03E97FCE A6F749C9 300D6B16 225CF372 208BC014 67D73DE3
          1F0563DB F98C0C26 ACB16CA5 A2D7B394 C6BA26B9 7F56E49F
          B825F867 9B87F8BC 02AA2BC1 B30A8119 AB432088 C10D0810
          628052A2 8B76F0A0 69447941 EEA0F42C

xV =      7E24A4CA 22EB375F 819A112B 3D10CA88 BEDAF368 07B7BD5C
          CC64D2C3 804BE42B

yV =      2D2D675D F3A5766D 56560AB7 9D082B57 48C001D8 B7470227
          4539A4C0 81E0B18E 2ADEAC1D 43345847 D0DDA886 E4EA402B
          44022E79 3B8552F3 92B2436D 59FAEE6B CAB4037F 01B3DB04
          F0B2FCEA 83432F8D 744F05C1 BBC9D104 73D57BEC F62EA494
```

```
1F3832BB 7BAB88FE FCB3B2F1 E3E36C1A F2FD58E6 C0311924
80FFD804 3A3A4583 17C54636 FF94E0CE 1F0E85F6 57E36212
24401EA2 96CAEDFC AD615B93 AC135DA9 AC019790 6F12C4C0
E9080AF2 C4B562AF 8F174B7A 72287451 15AAB55D C0623506
102675DE 2667F8C0 86023726 C5D6C395 044D0ADA D5EC6AFD
4B61D1C3 0D07CCA0 F4A125AB 49A827BA FC51C5CC 88E8B3C6
F465607D 59D54238 B7A770B6 2D3F6035
```

- Step 1: U produces rU, tU and receives tV. U DOES NOT RECEIVE rV (shown only for the purpose of verifying this data).

```
rU =      6A549A85 356D09C3 D845D365 49167D36 6D669B18 198B52A5
          0E2F3A5C 0B9AE350

tU =      31BACD07 71AE01D1 58C4C5A5 EAB21226 A2AAB682 8589CD21
          977C7131 D3D8CAC7 8CB1F20A C4D51391 AA42EB53 B7F6C832
          D921988F 7696700D 91EF3319 4FCDC9C3 EE2B531B F9CE7329
          996769F1 0636FA99 4D975709 EAF7E30F FD7983E9 26D75E30
          44559023 6FE9CB41 2CA553F8 AD3E6FD5 B52FCD92 D65AE374
          0665A719 6EB9F6F9 2AFF8798 B0206839 ED1D0481 A52E5623
          EB6D5C6E DCC23711 C7F66C86 EDE8E41F A97765A5 491BF90B
          6CB923C7 49173B2F E4A8C6E7 932D9B77 A15F4D2D 3DF3F181
          D8A8A56B 8B7020F3 BBD1C722 826C04B8 8AEC8523 531A6FD6
          D7D6EA3C 254C75E3 67723773 75598CA7 83408A65 6ECB957A
          F28334B9 692B7807 8725CDC7 6C524E50

rV =      89AADFB3 8E4F91AD 5D7575F6 8F41785F E17A23B5 7BA779A8
          90CCDC15 D5BFD888

tV =      1F7702BA 6C10A98C 5A70D3C0 EABCFE04 081FAE95 48FB2EFE
          699999A5 9EBBEF78 044E5700 26FE5B9B CB33871D 0C2F494C
          05AA3AE9 BB148DF4 12BC608A F22A8143 221513ED 9326499F
          2154819E ED5B113F 9BBBABF2 C9251FF1 AC5ED293 CA17BC7B
          F275CF4F 57036C78 F0A410B9 E37C24CD ADBEBDA2 6F7B8E20
          521FD698 D4D1D209 67B7669D 044C2CF3 BB235BAF 5BC7E520
          2A3EA8FC E06D355F 733B59B6 45BF9F8D C5EE28A4 AACCA937
          C1EA47E1 6F52234C A09CCEAF 9D056954 E0023C73 7432230A
```

```
4BDBC3CB BA99B1A0 F20CC7FE AC6A41BA B8C2C639 F93C7BEC
F416E757 558D124D 899E20BA 2144348B 1B7E0769 770DFFDA
9B5A8FF4 D0519705 50EBE74B 32A92119
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       109924541557386561351942254420888173709487883076 14
          946746939317944312022480164350948673848392594506 21
          780674006263198807489303292383655833177592387385 74
          349822416951931799896462481430382308636098366214 58
          403092086243556121679182637777626275688904049508 30
          394446695442626099134864071400617747092518390245 89
          083202767087133730592701612824019837017104236965 23
          035771335767590044133187913510862968042737140333 42
          707836938553501789462399072222974509263653359531 43
          411804270983232444055439641548093676415221463113 42
          831066203485371654984845442596293053070922677179 28
          648141942064990832011482309309503598445788234819 47
          99211366173120187
```

- Step 4: Shared secret converted to byte string.

```
Z =       5713B6EE F9D248C6 E87885EA FD7CB70A 111AB995 9C5BDAB1
          2FF68951 3DBB0154 0222DA46 ACE4FBC8 8689BD44 844AA092
          2AF444CF 9C88E35C 8BA23131 4617A5A7 C33B4385 63A38258
          C31900C1 55D4D523 F7879A67 09D84E9E 2765DC74 459ECB26
          C3646124 477D68DE 0599E25E FC26C40B 5929D37B 8D273DE1
          4D345C8A 0DC61A28 ACA556BE 431D1B54 AAD2C2F0 81B19693
          0EDFE4D0 75746094 C90A780A 66F2AEFC 08C3E1F6 143981E4
          CDDFCE1E C104A89C C770A9C8 D26B6270 4C7C148B 481D02C1
          DCC81428 7AF7F99C 9139DAA5 13B8F043 6F656B14 65E69213
          73B08EAA 553CE81D 087EA4E7 E4421A1A 1423C47D 9818E975
          8ED18470 208ACC35 E346A143 227C16BB
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 70C0460A 7E4434DD DB81874C 9F2A5A37 B104D11B F56C2933
             4F07743D C437BA2F C6DF5D93 635357DD 1A6E780C 15A3A2CD
             5E91FE49 6D8247AB 6AE7DFC9 6923261E
```

- If key confirmation is performed, then

```
MacKey  = 70C0460A 7E4434DD DB81874C 9F2A5A37
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 31BACD07 71AE01D1
            58C4C5A5 EAB21226 A2AAB682 8589CD21 977C7131 D3D8CAC7
            8CB1F20A C4D51391 AA42EB53 B7F6C832 D921988F 7696700D
            91EF3319 4FCDC9C3 EE2B531B F9CE7329 996769F1 0636FA99
            4D975709 EAF7E30F FD7983E9 26D75E30 44559023 6FE9CB41
            2CA553F8 AD3E6FD5 B52FCD92 D65AE374 0665A719 6EB9F6F9
            2AFF8798 B0206839 ED1D0481 A52E5623 EB6D5C6E DCC23711
            C7F66C86 EDE8E41F A97765A5 491BF90B 6CB923C7 49173B2F
            E4A8C6E7 932D9B77 A15F4D2D 3DF3F181 D8A8A56B 8B7020F3
            BBD1C722 826C04B8 8AEC8523 531A6FD6 D7D6EA3C 254C75E3
            67723773 75598CA7 83408A65 6ECB957A F28334B9 692B7807
            8725CDC7 6C524E50 1F7702BA 6C10A98C 5A70D3C0 EABCFE04
            081FAE95 48FB2EFE 699999A5 9EBBEF78 044E5700 26FE5B9B
            CB33871D 0C2F494C 05AA3AE9 BB148DF4 12BC608A F22A8143
            221513ED 9326499F 2154819E ED5B113F 9BBBABF2 C9251FF1
            AC5ED293 CA17BC7B F275CF4F 57036C78 F0A410B9 E37C24CD
            ADBEBDA2 6F7B8E20 521FD698 D4D1D209 67B7669D 044C2CF3
            BB235BAF 5BC7E520 2A3EA8FC E06D355F 733B59B6 45BF9F8D
            C5EE28A4 AACCA937 C1EA47E1 6F52234C A09CCEAF 9D056954
            E0023C73 7432230A 4BDBC3CB BA99B1A0 F20CC7FE AC6A41BA
            B8C2C639 F93C7BEC F416E757 558D124D 899E20BA 2144348B
            1B7E0769 770DFFDA 9B5A8FF4 D0519705 50EBE74B 32A92119
```

```
MacTag_U  = 578008F9 D8BC5E9A BF92E4AE 99EDB577 6CB18BCA 9AE78179
            63EA453B E7F2E978
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 1F7702BA 6C10A98C
            5A70D3C0 EABCFE04 081FAE95 48FB2EFE 699999A5 9EBBEF78
            044E5700 26FE5B9B CB33871D 0C2F494C 05AA3AE9 BB148DF4
            12BC608A F22A8143 221513ED 9326499F 2154819E ED5B113F
            9BBBABF2 C9251FF1 AC5ED293 CA17BC7B F275CF4F 57036C78
            F0A410B9 E37C24CD ADBEBDA2 6F7B8E20 521FD698 D4D1D209
            67B7669D 044C2CF3 BB235BAF 5BC7E520 2A3EA8FC E06D355F
            733B59B6 45BF9F8D C5EE28A4 AACCA937 C1EA47E1 6F52234C
            A09CCEAF 9D056954 E0023C73 7432230A 4BDBC3CB BA99B1A0
            F20CC7FE AC6A41BA B8C2C639 F93C7BEC F416E757 558D124D
            899E20BA 2144348B 1B7E0769 770DFFDA 9B5A8FF4 D0519705
            50EBE74B 32A92119 31BACD07 71AE01D1 58C4C5A5 EAB21226
            A2AAB682 8589CD21 977C7131 D3D8CAC7 8CB1F20A C4D51391
            AA42EB53 B7F6C832 D921988F 7696700D 91EF3319 4FCDC9C3
            EE2B531B F9CE7329 996769F1 0636FA99 4D975709 EAF7E30F
            FD7983E9 26D75E30 44559023 6FE9CB41 2CA553F8 AD3E6FD5
            B52FCD92 D65AE374 0665A719 6EB9F6F9 2AFF8798 B0206839
            ED1D0481 A52E5623 EB6D5C6E DCC23711 C7F66C86 EDE8E41F
            A97765A5 491BF90B 6CB923C7 49173B2F E4A8C6E7 932D9B77
            A15F4D2D 3DF3F181 D8A8A56B 8B7020F3 BBD1C722 826C04B8
            8AEC8523 531A6FD6 D7D6EA3C 254C75E3 67723773 75598CA7
            83408A65 6ECB957A F28334B9 692B7807 8725CDC7 6C524E50

MacTag_V  = 08CD11C2 4EA59CC3 EB95B4E3 CEADB71D 6AEB9476 E1D7D163
            B3066927 36263974
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
            = 4B435F32 5F55414C 49434542 4F424259 31BACD07 71AE01D1
              58C4C5A5 EAB21226 A2AAB682 8589CD21 977C7131 D3D8CAC7
              8CB1F20A C4D51391 AA42EB53 B7F6C832 D921988F 7696700D
              91EF3319 4FCDC9C3 EE2B531B F9CE7329 996769F1 0636FA99
              4D975709 EAF7E30F FD7983E9 26D75E30 44559023 6FE9CB41
              2CA553F8 AD3E6FD5 B52FCD92 D65AE374 0665A719 6EB9F6F9
              2AFF8798 B0206839 ED1D0481 A52E5623 EB6D5C6E DCC23711
              C7F66C86 EDE8E41F A97765A5 491BF90B 6CB923C7 49173B2F
              E4A8C6E7 932D9B77 A15F4D2D 3DF3F181 D8A8A56B 8B7020F3
              BBD1C722 826C04B8 8AEC8523 531A6FD6 D7D6EA3C 254C75E3
              67723773 75598CA7 83408A65 6ECB957A F28334B9 692B7807
              8725CDC7 6C524E50 1F7702BA 6C10A98C 5A70D3C0 EABCFE04
              081FAE95 48FB2EFE 699999A5 9EBBEF78 044E5700 26FE5B9B
              CB33871D 0C2F494C 05AA3AE9 BB148DF4 12BC608A F22A8143
              221513ED 9326499F 2154819E ED5B113F 9BBBABF2 C9251FF1
              AC5ED293 CA17BC7B F275CF4F 57036C78 F0A410B9 E37C24CD
              ADBEBDA2 6F7B8E20 521FD698 D4D1D209 67B7669D 044C2CF3
              BB235BAF 5BC7E520 2A3EA8FC E06D355F 733B59B6 45BF9F8D
              C5EE28A4 AACCA937 C1EA47E1 6F52234C A09CCEAF 9D056954
              E0023C73 7432230A 4BDBC3CB BA99B1A0 F20CC7FE AC6A41BA
              B8C2C639 F93C7BEC F416E757 558D124D 899E20BA 2144348B
              1B7E0769 770DFFDA 9B5A8FF4 D0519705 50EBE74B 32A92119

 MacTag_U   = 4FF2D69D 454FCCA6 77D433B6 29921F3B A8D4FAC2 FE8FCC79
              80F47840 D25724BD

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

            = 4B435F32 5F56424F 42425941 4C494345 1F7702BA 6C10A98C
              5A70D3C0 EABCFE04 081FAE95 48FB2EFE 699999A5 9EBBEF78
              044E5700 26FE5B9B CB33871D 0C2F494C 05AA3AE9 BB148DF4
              12BC608A F22A8143 221513ED 9326499F 2154819E ED5B113F
              9BBBABF2 C9251FF1 AC5ED293 CA17BC7B F275CF4F 57036C78
              F0A410B9 E37C24CD ADBEBDA2 6F7B8E20 521FD698 D4D1D209
              67B7669D 044C2CF3 BB235BAF 5BC7E520 2A3EA8FC E06D355F
              733B59B6 45BF9F8D C5EE28A4 AACCA937 C1EA47E1 6F52234C
              A09CCEAF 9D056954 E0023C73 7432230A 4BDBC3CB BA99B1A0
```

```
              F20CC7FE AC6A41BA B8C2C639 F93C7BEC F416E757 558D124D
              899E20BA 2144348B 1B7E0769 770DFFDA 9B5A8FF4 D0519705
              50EBE74B 32A92119 31BACD07 71AE01D1 58C4C5A5 EAB21226
              A2AAB682 8589CD21 977C7131 D3D8CAC7 8CB1F20A C4D51391
              AA42EB53 B7F6C832 D921988F 7696700D 91EF3319 4FCDC9C3
              EE2B531B F9CE7329 996769F1 0636FA99 4D975709 EAF7E30F
              FD7983E9 26D75E30 44559023 6FE9CB41 2CA553F8 AD3E6FD5
              B52FCD92 D65AE374 0665A719 6EB9F6F9 2AFF8798 B0206839
              ED1D0481 A52E5623 EB6D5C6E DCC23711 C7F66C86 EDE8E41F
              A97765A5 491BF90B 6CB923C7 49173B2F E4A8C6E7 932D9B77
              A15F4D2D 3DF3F181 D8A8A56B 8B7020F3 BBD1C722 826C04B8
              8AEC8523 531A6FD6 D7D6EA3C 254C75E3 67723773 75598CA7
              83408A65 6ECB957A F28334B9 692B7807 8725CDC7 6C524E50

MacTag_V  = EDA710AF E416AC09 38CCE3B3 7122F789 AA3026E5 E63AA14F
            B0504F96 1F66F488
```

3.4.3 dhEphem for finite field p2048-q256

- Step 1: U produces rU, tU and receives tV. U DOES NOT RECEIVE rV (shown only for the purpose of verifying this data).

```
rU =      95796E6F 829106A4 2208D7D7 894B735C 626496C5 76D03AEE
          BE3DF641 FCF2E0E1

tU =      2E9380C8 323AF975 45BC4941 DEB0EC37 42C62FE0 ECE824A6
          ABDBE66C 59BEE024 2911BFB9 67235CEB A35AE13E 4EC752BE
          630B92DC 4BDE2847 A9C62CB8 15274542 1FB7EB60 A63C0FE9
          159FCCE7 26CE7CD8 523D7450 667EF840 E4919121 EB5F01C8
          C9B0D3D6 48A93BFB 75689E82 44AC134A F544711C E79A02DC
          C3422668 4780DDDC B4985941 06C37F5B C7985648 7AF5AB02
          2A2E5E42 F09897C1 A85A11EA 0212AF04 D9B4CEBC 937C3C1A
          3E15A8A0 342E3376 15C84E7F E3B8B9B8 7FB1E73A 15AF12A3
          0D746E06 DFC34F29 0D797CE5 1AA13AA7 85BF6658 AFF5E4B0
          93003CBE AF665B3C 2E113A3A 4E905269 341DC071 1426685F
          4EF37E86 8A8126FF 3F2279B5 7CA67E29
```

```
rV =      7D62A7E3 EF36DE61 7B13D1AF B82C780D 83A23BD4 EE670564
          5121F371 F546A53D

tV =      575F0351 BD2B1B81 7448BDF8 7A6C362C 1E289D39 03A30B98
          32C5741F A250363E 7ACBC7F7 7F3DACBC 1F131ADD 8E03367E
          FF8FBBB3 E1C57844 24809B25 AFE4D226 2A1A6FD2 FAB64105
          CA30A674 E07F7809 85208863 2FC04923 3791AD4E DD083A97
          8B883EE6 18BC5E0D D047415F 2D95E683 CF14826B 5FBE10D3
          CE41C6C1 20C78AB2 0008C698 BF7F0BCA B9D7F407 BED0F43A
          FB2970F5 7F8D1204 3963E66D DD320D59 9AD9936C 8F44137C
          08B180EC 5E985CEB E186F3D5 49677E80 607331EE 17AF3380
          A725B078 2317D7DD 43F59D7A F9568A9B B63A84D3 65F92244
          ED120988 219302F4 2924C7CA 90B89D24 F71B0AB6 97823D7D
          EB1AFF5B 0E8E4A45 D49F7F53 757E1913
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       17014086483691799988179156384159336252014329275393
          54206744899725452335140588665348467087589506642580
          56749459279726135406146753953813645792406438006074
          78115624552232273920609963621474643404371687604213
          61186490258949121810305586450024155046326100657873
          01639682944896871170712618094623782435200684871624
          51349161678002179549584100958328488783183164728487
          11068458748569427217544624298072911100126995766342
          76864677367000401743824008824179942431953835338777
          53639707402834149856651558563193835398981103773564
          50833552080021513813408975159461416341852559558246
          75850808142720983330136576557157066364574374740800
          37115205807529340
```

- Step 4:

```
Z =       86C70BF8 D0BB81BB 01078A17 219CB7D2 7203DB2A 19C877F1
          D1F19FD7 D77EF225 46A68F00 5AD52DC8 4553B78F C60330BE
          51EA7C06 72CAC151 5E4B35C0 47B9A551 B88F39DC 26DA14A0
```

```
9EF74774 D47C762D D177F9ED 5BC2F11E 52C879BD 95098504
CD9EECD8 A8F9B3EF BD1F008A C5853097 D9D1837F 2B18F77C
D7BE01AF 80A7C7B5 EA3CA54C C02D0C11 6FEE3F95 BB873993
85875D7E 86747E67 6E728938 ACBFF709 8E05BE4D CFB24052
B83AEFFB 14783F02 9ADBDE7F 53FAE920 84224090 E007CEE9
4D4BF2BA CE9FFD4B 57D2AF7C 724D0CAA 19BF0501 F6F17B4A
A10F425E 3EA76080 B4B9D6B3 CEFEA115 B2CEB878 9BB8A3B0
EA87FEBE 63B6C8F8 46EC6DB0 C26C5D7C
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 43E728EE 01356F51 07F22746 CDB11B87 92AF4120 1B337464
             33196196 FB4E4985 AFACD373 761ADFA0 CA45183D 1DA6C92B
             E3A11325 AA26FC53 028D70E8 EE97F203
```

3.4.4 dhHybridOneFlow for finite field p2048-q256

- Prerequisites:

```
xU =      50747886 14D3894F 98934CAD 9700E887 2E1FB6AD BFD54521
          6B218FB3 244188B0

yU =      5DDE1EF2 670295BA A29AB5D0 CA52380D 7C0D08C8 D7C35CA1
          48F8D568 D67B5B0C FBA261E7 590ACA11 83792006 268F5B7D
          DEBDFB7D 73D48940 DB60C800 13044C70 15B63BF3 F6922D5A
          9150A2BC 742520A0 4260C29E E75250CC E52D2794 7687C777
          5F918CCD 07C98C2D 97CF4F91 78C6BEBC 663808AA 74909264
          FC14C0CA 358D3A1C 9E9394BE 3FB885BE B50F14D4 A77B3AA1
          4623549B 8B43B864 99171F8F C74BCDA0 B9280314 27B2491B
          5B02D311 F0A6EFCD 68C5574E 7DBE00D1 8C5EF846 52182F17
          D0EB416D 36C8947D 7DAFD3FC 4EBFA9C0 25378483 05EEE467
          AAD8125B DD42356A 2F07E5E8 A5A10AB7 547BE3A1 E487986E
          47391635 BD43C762 0A560D67 F6580661
```

```
xV =      8963089D B60A16FA B2B87138 50C9E56A 47DEC386 36AFFFFF
          E7C88A67 AC0A393B

yV =      7B88BFB5 DD684755 A822EDF2 3235EC6F C61DE430 30C9F0EF
          38444B96 88337004 4AB21BD2 22811539 934F92E6 F4347084
          1CDC849E D61BD3EF E6413CCB F3E3FFEC 6B629331 2690C881
          10A2C1FB CA2DF7C1 96B5CD01 EA7975E2 C525089B D2783B11
          35DF884B 8F8D743F D52E874C DF401FBC 2846AF50 2C494090
          4DA7B47A 4CEFEC29 5B6EBD68 147944CC 97773E18 2B8848F2
          105E5193 B04A0E20 181B4F69 BBB98B7A C94D131E 2416AAB9
          A5858CCC 68BFDDC4 4CA7DC22 7EA9B618 3887658B 575C44FF
          4A536BDD 2F358EAD BB37E4AF 3C0E6151 DA73C9F7 20C6E69E
          6A6EAB0E 53ED6A86 0395647B 3255BBE8 C41FC36F 29073119
          11AFC1B9 97A7BD9A 00D0362C 645E2BB8
```

BEGIN U's calculations

- Step 1:

```
rU =      30615E1E 9F6D6B97 28963E76 CE8ECB8B 44CE61BC 76FA4C6A
          903A2E9A 70114B2B

tU =      0AB497C2 CDE8456F 56922239 140BED9E 1D09B5AB CCB84341
          63BD4CD3 559DEC35 2F3BDE1A B3C5DCD8 42B6BEB9 009679C6
          DF6D3FB5 60188FB1 255AE1AB D7CC1894 DC4413BA 139831F4
          68465C89 581A6995 B6FAC3FA E945FCC3 C8C3D555 A4E950C6
          00EBB058 313E44F6 3463552E 1DCA28A5 7D36E5F4 694DC67B
          8CCA855C AD6750D6 0F9DF426 84EB6B1A A0E7962E 42217AF5
          7A66AC2A 8A387341 2D3A9F24 01D91CC8 8CC0C935 56C7992B
          9BCB3DB3 484B5C9E 56208519 116F4BE4 E88E90D3 50B4110E
          0785445A 2A506F42 73DE95AB 035A637A 5526B711 85F7B67F
          6F95A608 7FF8836B 998EF574 A53072C2 2CD97F17 D4F08F40
          E639B674 251BA582 67F6985E 3B606295
```

- Step 2: Decimal and hex values for static shared secret.

```
Z_s =     1075162015635517471022212212817694205837684202590 7
          715550959097915120712103276052369736186797163629 61
          534805354757150256615080656708648335848301647423 95
          090773282245522825191266005282530801755119268817 92
          300958062442975576800491345223438515330670797276 26
          347781234956395130525963185714341974577650363509 63
          072325387463368016480040077005753381844652576778 42
          324334781572161513477620623748166152323536090285 47
          765303797282007079854980699864591718119736469191 61
          665737719558386900715685324071271231364937659405 68
          580538099295111174528256288675183242900707781316 80
          327131375121459123682641199988483416943463756834 62
          83559688763081453

Z_s =     552B5323 50CD2FC9 0263F1ED 74DA5C37 DCCBC3A1 7C8BA769
          AEC10114 8DACB80C BAFED968 DA74FE33 9C037DE5 9C0F8404
          910174B7 278929BD 8509D021 6CE06DCD C1FBAEF4 A47B4CB8
          AAD97448 98DA2080 92B5E591 BD17BFA0 86C1B134 5C8F8F01
          FE809A24 8A1426DD 7CA849CE E343E614 2ADA16A8 46568ADF
          98BE53CD C2BEA9F1 6B98612E 416FC9D4 E882DD0D 1480B83B
          DBC81E30 708A24EF F1C4FD98 AD4DC843 7F16739D 92E198CE
          6702C083 ED75306E 56F3837F D9EE5A0F 65FA6EA2 DCFF547B
          DDA5B4BD 187695F4 026417D0 767DE59C 355211C9 754D1ED8
          DBFAD415 449998EF 1C635F06 ED04E7B4 D3B677E8 092BFF0B
          7E3A99A0 E068B7E7 536BFB62 368002ED
```

- Step 3: Decimal and hex values for ephemeral shared secret.

```
Z_e =     483828955839666922908022504405787624938056633058 94
          906835223050511287343783791606937632902845442820 25
          927312951944402504258989771050011642058412577481 37
          582677857351895903452442546534049456016103278180 51
          800579283578546112981512471939088026312938152412 19
          409663467296374548875294278306068029331849100842 65
          985919767166658728545044095061472020836651499112 98
          055363933478203934299479585491591013347478229842 90
          177084109060427910207204192106237464897954084094 18
          828633858602331931113507109597721424625546593734 35
```

```
            2405545178139434946664818476525667690430291244621 5
            3963308290900519136315812746168752796948705889141 2
            1274743651551789

Z_e =       26539E6A 05909271 A3A8DFBF A6C5C1CB EECB9B38 83CF2DA5
            392955FD A44740A8 EBDCBFAA CF173787 8540DADF FBDC999C
            D08D32A2 CBD32350 5EECE030 B2947018 9EC79C04 3E1C26C6
            15C61E43 4A8477A0 578D2772 549B11DD 4E872764 B34385F8
            B1C36ECC 3FB2411F F43BA64D 8C5628A7 946CC6A7 918BF11E
            5BB952E1 5A1000C2 C90AACAB 62334B3F 4FEFD46E 0A3A1232
            FB286FFC 9ADF93B9 5912965F 5DE46D54 6CFE24F8 B7903FD2
            EF6B123E 544E375C 3DCBA92A CDF9C93A ABC68D87 3D3CF3C0
            41528D87 6065CC6F 4258BE06 06CB79F4 C10F2CDC C126ADE1
            462FED22 5192475F 7D91EF04 A3F39309 10215A1D 5D08D6A0
            575419C4 8B804E96 5860FC4B 701BCA2D
```

- Step 4: Shared secret.

```
Z =         26539E6A 05909271 A3A8DFBF A6C5C1CB EECB9B38 83CF2DA5
            392955FD A44740A8 EBDCBFAA CF173787 8540DADF FBDC999C
            D08D32A2 CBD32350 5EECE030 B2947018 9EC79C04 3E1C26C6
            15C61E43 4A8477A0 578D2772 549B11DD 4E872764 B34385F8
            B1C36ECC 3FB2411F F43BA64D 8C5628A7 946CC6A7 918BF11E
            5BB952E1 5A1000C2 C90AACAB 62334B3F 4FEFD46E 0A3A1232
            FB286FFC 9ADF93B9 5912965F 5DE46D54 6CFE24F8 B7903FD2
            EF6B123E 544E375C 3DCBA92A CDF9C93A ABC68D87 3D3CF3C0
            41528D87 6065CC6F 4258BE06 06CB79F4 C10F2CDC C126ADE1
            462FED22 5192475F 7D91EF04 A3F39309 10215A1D 5D08D6A0
            575419C4 8B804E96 5860FC4B 701BCA2D 552B5323 50CD2FC9
            0263F1ED 74DA5C37 DCCBC3A1 7C8BA769 AEC10114 8DACB80C
            BAFED968 DA74FE33 9C037DE5 9C0F8404 910174B7 278929BD
            8509D021 6CE06DCD C1FBAEF4 A47B4CB8 AAD97448 98DA2080
            92B5E591 BD17BFA0 86C1B134 5C8F8F01 FE809A24 8A1426DD
            7CA849CE E343E614 2ADA16A8 46568ADF 98BE53CD C2BEA9F1
            6B98612E 416FC9D4 E882DD0D 1480B83B DBC81E30 708A24EF
            F1C4FD98 AD4DC843 7F16739D 92E198CE 6702C083 ED75306E
            56F3837F D9EE5A0F 65FA6EA2 DCFF547B DDA5B4BD 187695F4
            026417D0 767DE59C 355211C9 754D1ED8 DBFAD415 449998EF
```

```
1C635F06 ED04E7B4 D3B677E8 092BFF0B 7E3A99A0 E068B7E7
536BFB62 368002ED
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 211E46BB CFF4502C F719C952 6D37738B E1173440 5ECCBC0B
             64166E3F FC228556 F3758678 BDF7823E 63C09375 04C922D0
             D00CAB82 B39223C1 A2EAB529 EAC4C24E
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
rU =      30615E1E 9F6D6B97 28963E76 CE8ECB8B 44CE61BC 76FA4C6A
          903A2E9A 70114B2B

tU =      0AB497C2 CDE8456F 56922239 140BED9E 1D09B5AB CCB84341
          63BD4CD3 559DEC35 2F3BDE1A B3C5DCD8 42B6BEB9 009679C6
          DF6D3FB5 60188FB1 255AE1AB D7CC1894 DC4413BA 139831F4
          68465C89 581A6995 B6FAC3FA E945FCC3 C8C3D555 A4E950C6
          00EBB058 313E44F6 3463552E 1DCA28A5 7D36E5F4 694DC67B
          8CCA855C AD6750D6 0F9DF426 84EB6B1A A0E7962E 42217AF5
          7A66AC2A 8A387341 2D3A9F24 01D91CC8 8CC0C935 56C7992B
          9BCB3DB3 484B5C9E 56208519 116F4BE4 E88E90D3 50B4110E
          0785445A 2A506F42 73DE95AB 035A637A 5526B711 85F7B67F
          6F95A608 7FF8836B 998EF574 A53072C2 2CD97F17 D4F08F40
          E639B674 251BA582 67F6985E 3B606295
```

- Step 2: N/A.

- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     1075162015635517471022212212817694205837684202590 7
          715550959097915120712103276052369736186797163629 61
          534805354757150256615080656708648335848301647423 95
          090773282245522825191266005282530801755119268817 92
          300958062442975576800491345223438515330670797276 26
          347781234956395130525963185714341974577650363509 63
          072325387463368016480040077005753381844652576778 42
          324334781572161513477620623748166152323536090285 47
          765303797282007079854980699864591718119736469191 61
          665737719558386900715685324071271231364937659405 68
          580538099295111174528256288675183242900707781316 80
          327131375121459123682641199988483416943463756834 62
          83559688763081453

Z_s =     552B5323 50CD2FC9 0263F1ED 74DA5C37 DCCBC3A1 7C8BA769
          AEC10114 8DACB80C BAFED968 DA74FE33 9C037DE5 9C0F8404
          910174B7 278929BD 8509D021 6CE06DCD C1FBAEF4 A47B4CB8
          AAD97448 98DA2080 92B5E591 BD17BFA0 86C1B134 5C8F8F01
          FE809A24 8A1426DD 7CA849CE E343E614 2ADA16A8 46568ADF
          98BE53CD C2BEA9F1 6B98612E 416FC9D4 E882DD0D 1480B83B
          DBC81E30 708A24EF F1C4FD98 AD4DC843 7F16739D 92E198CE
          6702C083 ED75306E 56F3837F D9EE5A0F 65FA6EA2 DCFF547B
          DDA5B4BD 187695F4 026417D0 767DE59C 355211C9 754D1ED8
          DBFAD415 449998EF 1C635F06 ED04E7B4 D3B677E8 092BFF0B
          7E3A99A0 E068B7E7 536BFB62 368002ED
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     483828955839666922908022504405787624938056633058 94
          906835223050511287343783791606937632902845442820 25
          927312951944402504258989771050011642058412577481 37
          582677857351895903452442546534049456016103278180 51
          800579283578546112981512471939088026312938152412 19
          409663467296374548875294278306068029331849100842 65
          985919767166658728545044095061472020836651499112 98
          055363933478203934299479585491591013347478229842 90
          177084109060427910207204192106237464897954084094 18
          828633858602331931113507109597721424625546593734 35
```

```
            2405545178139434946664818476525667690430291244621 5
            3963308290900519136315812746168752796948705889141 2
            1274743651551789

Z_e =       26539E6A 05909271 A3A8DFBF A6C5C1CB EECB9B38 83CF2DA5
            392955FD A44740A8 EBDCBFAA CF173787 8540DADF FBDC999C
            D08D32A2 CBD32350 5EECE030 B2947018 9EC79C04 3E1C26C6
            15C61E43 4A8477A0 578D2772 549B11DD 4E872764 B34385F8
            B1C36ECC 3FB2411F F43BA64D 8C5628A7 946CC6A7 918BF11E
            5BB952E1 5A1000C2 C90AACAB 62334B3F 4FEFD46E 0A3A1232
            FB286FFC 9ADF93B9 5912965F 5DE46D54 6CFE24F8 B7903FD2
            EF6B123E 544E375C 3DCBA92A CDF9C93A ABC68D87 3D3CF3C0
            41528D87 6065CC6F 4258BE06 06CB79F4 C10F2CDC C126ADE1
            462FED22 5192475F 7D91EF04 A3F39309 10215A1D 5D08D6A0
            575419C4 8B804E96 5860FC4B 701BCA2D
```

- Step 5: Shared secret.

```
Z =         26539E6A 05909271 A3A8DFBF A6C5C1CB EECB9B38 83CF2DA5
            392955FD A44740A8 EBDCBFAA CF173787 8540DADF FBDC999C
            D08D32A2 CBD32350 5EECE030 B2947018 9EC79C04 3E1C26C6
            15C61E43 4A8477A0 578D2772 549B11DD 4E872764 B34385F8
            B1C36ECC 3FB2411F F43BA64D 8C5628A7 946CC6A7 918BF11E
            5BB952E1 5A1000C2 C90AACAB 62334B3F 4FEFD46E 0A3A1232
            FB286FFC 9ADF93B9 5912965F 5DE46D54 6CFE24F8 B7903FD2
            EF6B123E 544E375C 3DCBA92A CDF9C93A ABC68D87 3D3CF3C0
            41528D87 6065CC6F 4258BE06 06CB79F4 C10F2CDC C126ADE1
            462FED22 5192475F 7D91EF04 A3F39309 10215A1D 5D08D6A0
            575419C4 8B804E96 5860FC4B 701BCA2D 552B5323 50CD2FC9
            0263F1ED 74DA5C37 DCCBC3A1 7C8BA769 AEC10114 8DACB80C
            BAFED968 DA74FE33 9C037DE5 9C0F8404 910174B7 278929BD
            8509D021 6CE06DCD C1FBAEF4 A47B4CB8 AAD97448 98DA2080
            92B5E591 BD17BFA0 86C1B134 5C8F8F01 FE809A24 8A1426DD
            7CA849CE E343E614 2ADA16A8 46568ADF 98BE53CD C2BEA9F1
            6B98612E 416FC9D4 E882DD0D 1480B83B DBC81E30 708A24EF
            F1C4FD98 AD4DC843 7F16739D 92E198CE 6702C083 ED75306E
            56F3837F D9EE5A0F 65FA6EA2 DCFF547B DDA5B4BD 187695F4
            026417D0 767DE59C 355211C9 754D1ED8 DBFAD415 449998EF
```

```
1C635F06 ED04E7B4 D3B677E8 092BFF0B 7E3A99A0 E068B7E7
536BFB62 368002ED
```

- Step 6: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 211E46BB CFF4502C F719C952 6D37738B E1173440 5ECCBC0B
             64166E3F FC228556 F3758678 BDF7823E 63C09375 04C922D0
             D00CAB82 B39223C1 A2EAB529 EAC4C24E
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 211E46BB CFF4502C F719C952 6D37738B

nonceV =  08A04CED 97B00731 33B4DD87 3DBAD54C A5B7848C 09A13B66
          F2408417 218B037A
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 0AB497C2 CDE8456F
            56922239 140BED9E 1D09B5AB CCB84341 63BD4CD3 559DEC35
            2F3BDE1A B3C5DCD8 42B6BEB9 009679C6 DF6D3FB5 60188FB1
            255AE1AB D7CC1894 DC4413BA 139831F4 68465C89 581A6995
            B6FAC3FA E945FCC3 C8C3D555 A4E950C6 00EBB058 313E44F6
            3463552E 1DCA28A5 7D36E5F4 694DC67B 8CCA855C AD6750D6
            0F9DF426 84EB6B1A A0E7962E 42217AF5 7A66AC2A 8A387341
            2D3A9F24 01D91CC8 8CC0C935 56C7992B 9BCB3DB3 484B5C9E
            56208519 116F4BE4 E88E90D3 50B4110E 0785445A 2A506F42
            73DE95AB 035A637A 5526B711 85F7B67F 6F95A608 7FF8836B
            998EF574 A53072C2 2CD97F17 D4F08F40 E639B674 251BA582
            67F6985E 3B606295 08A04CED 97B00731 33B4DD87 3DBAD54C
            A5B7848C 09A13B66 F2408417 218B037A
```

```
MacTag_U  = 008116B9 5807D2CD 6DC706B7 B62D2174 E6A90B22 9C29EFD1
            C0130C38 CD969DAB
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 0AB497C2 CDE8456F
            56922239 140BED9E 1D09B5AB CCB84341 63BD4CD3 559DEC35
            2F3BDE1A B3C5DCD8 42B6BEB9 009679C6 DF6D3FB5 60188FB1
            255AE1AB D7CC1894 DC4413BA 139831F4 68465C89 581A6995
            B6FAC3FA E945FCC3 C8C3D555 A4E950C6 00EBB058 313E44F6
            3463552E 1DCA28A5 7D36E5F4 694DC67B 8CCA855C AD6750D6
            0F9DF426 84EB6B1A A0E7962E 42217AF5 7A66AC2A 8A387341
            2D3A9F24 01D91CC8 8CC0C935 56C7992B 9BCB3DB3 484B5C9E
            56208519 116F4BE4 E88E90D3 50B4110E 0785445A 2A506F42
            73DE95AB 035A637A 5526B711 85F7B67F 6F95A608 7FF8836B
            998EF574 A53072C2 2CD97F17 D4F08F40 E639B674 251BA582
            67F6985E 3B606295

MacTag_V  = A2EE5EF5 A8C38A74 1A28B4EE 2AD99554 1CC52C8B 12D20ADD
            23F61D64 FFF286B2
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 0AB497C2 CDE8456F
            56922239 140BED9E 1D09B5AB CCB84341 63BD4CD3 559DEC35
            2F3BDE1A B3C5DCD8 42B6BEB9 009679C6 DF6D3FB5 60188FB1
            255AE1AB D7CC1894 DC4413BA 139831F4 68465C89 581A6995
            B6FAC3FA E945FCC3 C8C3D555 A4E950C6 00EBB058 313E44F6
            3463552E 1DCA28A5 7D36E5F4 694DC67B 8CCA855C AD6750D6
            0F9DF426 84EB6B1A A0E7962E 42217AF5 7A66AC2A 8A387341
            2D3A9F24 01D91CC8 8CC0C935 56C7992B 9BCB3DB3 484B5C9E
            56208519 116F4BE4 E88E90D3 50B4110E 0785445A 2A506F42
            73DE95AB 035A637A 5526B711 85F7B67F 6F95A608 7FF8836B
```

```
              998EF574 A53072C2 2CD97F17 D4F08F40 E639B674 251BA582
              67F6985E 3B606295 08A04CED 97B00731 33B4DD87 3DBAD54C
              A5B7848C 09A13B66 F2408417 218B037A

MacTag_U  = 45AF68B2 CB093A48 FD174892 7A58D406 AF637EC2 F0DB55F8
            FED3487A B4BF03AA

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 08A04CED 97B00731
            33B4DD87 3DBAD54C A5B7848C 09A13B66 F2408417 218B037A
            0AB497C2 CDE8456F 56922239 140BED9E 1D09B5AB CCB84341
            63BD4CD3 559DEC35 2F3BDE1A B3C5DCD8 42B6BEB9 009679C6
            DF6D3FB5 60188FB1 255AE1AB D7CC1894 DC4413BA 139831F4
            68465C89 581A6995 B6FAC3FA E945FCC3 C8C3D555 A4E950C6
            00EBB058 313E44F6 3463552E 1DCA28A5 7D36E5F4 694DC67B
            8CCA855C AD6750D6 0F9DF426 84EB6B1A A0E7962E 42217AF5
            7A66AC2A 8A387341 2D3A9F24 01D91CC8 8CC0C935 56C7992B
            9BCB3DB3 484B5C9E 56208519 116F4BE4 E88E90D3 50B4110E
            0785445A 2A506F42 73DE95AB 035A637A 5526B711 85F7B67F
            6F95A608 7FF8836B 998EF574 A53072C2 2CD97F17 D4F08F40
            E639B674 251BA582 67F6985E 3B606295

MacTag_V  = 8E35A256 0E539E6C 58745F42 674E415C 18A04AAA B9F2E11A
            10323271 C6E10CDB
```

3.4.5 MQV1 for finite field p2048-q256

- Prerequisites:

```
xU =      26DC8BED 912F1348 AAFBE989 657253AC B35A59D1 B20605BE
          B7282179 8B18F384

yU =      596A5667 612A3993 9B4A702B C43D8A26 2E870EAC 656049BD
          BBA26825 EBBA837D E7AC76CA 449A8FEC 52E4473F 9095F3F2
```

```
            B3AF4AE1 0DECF8B1 DF2CB72C 42E5165B C82F0A43 47FD2FC8
            E051BC3B 892A07A8 660AD8FC 280FB3CA 5B0DB43D 70431981
            BEA414DC ACF5B1F7 067812FB A99A30C4 C98EB4F0 EA8A61B8
            4FE98734 4150E3F4 6A9F0937 25D02440 5F79B6E7 859BB633
            6171FF06 E26C68E3 8A9F4D70 250CDDFD 906CD0C1 F63C8DCC
            35661830 99EFB28A 62259BD4 67A027C9 C9640E31 545964A9
            1C6B1A8D 8E441CB3 4139F2C8 78412613 8284646D D23FFB7B
            4336B533 AD32655F 657C320A F3669B11 B947D648 9B5E412F
            F0C2107F E7477CA8 73260504 CDB33CBD

    xV =    AE2E218E BF3C0EDC 3DBF87F9 AFDD6C0E DEB669B4 1D3F6FEA
            0E85CD10 DB2380A2

    yV =    85CDAF25 EACF7F2D 2DD51B86 1E6D9567 3B033DE6 F7159FB3
            DC69E037 188A8C24 7E8CB8D4 2639CE97 64F0081C 54036D7D
            BDAEC329 7CDDD640 7150D907 55B5D5F7 FE491C6B AE60E917
            0E1CCE19 D525017D BE845801 2BBE7F9E 30B87579 FB6AEACA
            FA6B7A7B 03F34D28 4135556C ADBEB3D6 8DF84797 B72D5681
            7D008952 08694A7E D935C796 34B9F92F B5156FF5 A8DB725F
            919D8FB0 CD07E1F9 5BC8FFD9 484F9E42 BD35335B 5614CB64
            063B74CE 3B6BFFF5 5596171C EBC52630 0ADB8E18 B0662CBD
            AC318925 AD3DBE47 A4DBAD60 A9660745 C1A73B1C 27A2CF73
            8BB56046 CE433E5A 30DC0E84 AF576E97 19F14CCB 988B9986
            A7410240 45AFFDE4 26D63F0B CC04F1F7
```

BEGIN U's calculations

- Step 1:

```
    rU =    ADAFCAAF 2D880675 8C5094B9 C65AD8C3 FD1935F0 928CA293
            EA40B0E7 F4C10089

    tU =    58EA5EA6 75A27704 2C2E842C 05061136 B6B53163 20233F49
            D5338C38 48C71852 738F6E1E 39371F50 C84A7910 2C76DA3B
            C1BFD15C 83CAA8D2 378D9C32 8C6E5CB0 8F669763 6BB13CC7
            77A38855 9237858F 05606E0A 8014194E 9487DB1F F14E9903
            E84EAB89 13EC38BC 439F2F38 5F2D1E34 DB4A538C AA6161BF
```

```
552AD467 62C4C404 75880763 D69AFA49 34DBEBD0 EB5388F4
CA3FE8FD B08948B3 1CDC1A5B 7814BD34 5C0F0EFD E4418C1A
F6197C7E 8A02B3DB 78C28F67 EAF85130 F5E04A65 5AFC1673
29E13B3E 709B6255 97DE7A65 B15EB7A4 92154007 7CD43D24
5C060D5C 14F98AFE EC9B039B E1460A59 4A46CD16 7DA70237
27259822 91932C86 947B4D53 8B4B180D
```

- Step 2: Decimal value for shared secret.

```
Z =     10333878484818308254936608013700904259680505768192
        21350517434340158955727528454412915857344975378229
        84654253411558279803568418424255513839327915434594
        21020501953468538620510203594030480496065986999459
        94896919718399541085996382571260734905529470511344
        56122627744659857762078313136760420394685082650295
        40318325454869175888659484239214851010016246270990
        80143347143104673666566467691171817303729106030380
        73220359337076669513972258297750387640005710499799
        77074880225657601366715899025052515802124883852805
        75323556267330376869273645269583212240657339651301
        97026486306621496644875621316337183186657056946537
        7285625151661757 2
```

- Step 3: Hex value for shared secret.

```
Z =     51DC2E96 72AA6621 4D32485E 17344B26 5C622A7F 2B7F2B8A
        E1B2EEA5 091C4DCC 0E3A7A7F B1610014 12BC7FB7 E923ABE0
        CE876543 C6AF4A15 7ACB4E5F 3041B2EB 9CE411F5 A8BE3AD4
        B1E45BA9 867EE3B9 C117C2F1 A813BD49 743AF2BE 3BE7093C
        1E42D1BE DE2CF8D0 85A2FF6F 1A79DAC2 F2222D5C 80B26BAE
        F1153714 A778BA0C 7A4B4CB3 352B4A0A D9B78B0E 92B78354
        640927FF A3CB433E 3A11A2D8 FB5D2179 8033530B 95C02F67
        B1734AA2 DD8DEEE4 9AEC1332 DFBF62A9 717C3F8F 1410D0EE
        A86D5CC7 2729BE13 33709895 06E9F228 75D593F3 9CB65C91
        D7987A6E EECAFC18 C10AE7D1 93E54445 E41D0959 65705737
        38A31262 40E75989 5681AD0C 86EA8364
```

- Step 4: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 979CA810 0BCF89EC 6DC9DA5F 62729DFA 068AED5D 2BB085A4
             B046D5EC 89CFE0DC CFC5D126 0B1CF955 EEDB7D9C F5254DFD
             99CF5B8C 39CABACE D2F3DD2A 53E8DEEA
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
rU =      ADAFCAAF 2D880675 8C5094B9 C65AD8C3 FD1935F0 928CA293
          EA40B0E7 F4C10089

tU =      58EA5EA6 75A27704 2C2E842C 05061136 B6B53163 20233F49
          D5338C38 48C71852 738F6E1E 39371F50 C84A7910 2C76DA3B
          C1BFD15C 83CAA8D2 378D9C32 8C6E5CB0 8F669763 6BB13CC7
          77A38855 9237858F 05606E0A 8014194E 9487DB1F F14E9903
          E84EAB89 13EC38BC 439F2F38 5F2D1E34 DB4A538C AA6161BF
          552AD467 62C4C404 75880763 D69AFA49 34DBEBD0 EB5388F4
          CA3FE8FD B08948B3 1CDC1A5B 7814BD34 5C0F0EFD E4418C1A
          F6197C7E 8A02B3DB 78C28F67 EAF85130 F5E04A65 5AFC1673
          29E13B3E 709B6255 97DE7A65 B15EB7A4 92154007 7CD43D24
          5C060D5C 14F98AFE EC9B039B E1460A59 4A46CD16 7DA70237
          27259822 91932C86 947B4D53 8B4B180D
```

- Step 2: N/A.
- Step 3: Decimal value for shared secret.

```
Z =       10333878484818308254936608013700904259680505768192
          21350517434340158955727528454412915857344975378229
          84654253411558279803568418424255513839327915434594
          21020501953468538620510203594030480496065986999459
          94896919718399541085996382571260734905529470511344
          56122627744659857762078313136760420394685082650295
          40318325454869175888659484239214851010016246270990
```

```
80143347143104673666566467691171817303729106030380
73220359337076669513972258297750387640005710499799
77074880225657601366715899025052515802124883852805
75323556267330376869273645269583212240657339651301
97026486306621496644875621316337183186657056946537
72856251516617572
```

- Step 4: Hex value for shared secret.

```
Z =       51DC2E96 72AA6621 4D32485E 17344B26 5C622A7F 2B7F2B8A
          E1B2EEA5 091C4DCC 0E3A7A7F B1610014 12BC7FB7 E923ABE0
          CE876543 C6AF4A15 7ACB4E5F 3041B2EB 9CE411F5 A8BE3AD4
          B1E45BA9 867EE3B9 C117C2F1 A813BD49 743AF2BE 3BE7093C
          1E42D1BE DE2CF8D0 85A2FF6F 1A79DAC2 F2222D5C 80B26BAE
          F1153714 A778BA0C 7A4B4CB3 352B4A0A D9B78B0E 92B78354
          640927FF A3CB433E 3A11A2D8 FB5D2179 8033530B 95C02F67
          B1734AA2 DD8DEEE4 9AEC1332 DFBF62A9 717C3F8F 1410D0EE
          A86D5CC7 2729BE13 33709895 06E9F228 75D593F3 9CB65C91
          D7987A6E EECAFC18 C10AE7D1 93E54445 E41D0959 65705737
          38A31262 40E75989 5681AD0C 86EA8364
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 979CA810 0BCF89EC 6DC9DA5F 62729DFA 068AED5D 2BB085A4
             B046D5EC 89CFE0DC CFC5D126 0B1CF955 EEDB7D9C F5254DFD
             99CF5B8C 39CABACE D2F3DD2A 53E8DEEA
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 979CA810 0BCF89EC 6DC9DA5F 62729DFA

nonceV =  19B7D0AA 84E65DDA DEC2401C B8035C91 D15F2EA7 7E39B4A4
          39FE0E6C 7B22BFC6
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 58EA5EA6 75A27704
            2C2E842C 05061136 B6B53163 20233F49 D5338C38 48C71852
            738F6E1E 39371F50 C84A7910 2C76DA3B C1BFD15C 83CAA8D2
            378D9C32 8C6E5CB0 8F669763 6BB13CC7 77A38855 9237858F
            05606E0A 8014194E 9487DB1F F14E9903 E84EAB89 13EC38BC
            439F2F38 5F2D1E34 DB4A538C AA6161BF 552AD467 62C4C404
            75880763 D69AFA49 34DBEBD0 EB5388F4 CA3FE8FD B08948B3
            1CDC1A5B 7814BD34 5C0F0EFD E4418C1A F6197C7E 8A02B3DB
            78C28F67 EAF85130 F5E04A65 5AFC1673 29E13B3E 709B6255
            97DE7A65 B15EB7A4 92154007 7CD43D24 5C060D5C 14F98AFE
            EC9B039B E1460A59 4A46CD16 7DA70237 27259822 91932C86
            947B4D53 8B4B180D 19B7D0AA 84E65DDA DEC2401C B8035C91
            D15F2EA7 7E39B4A4 39FE0E6C 7B22BFC6

 MacTag_U  = BB5A371C 1AE76B0E E752822A 51D203FD BD98832F 69321086
             79316FA8 64A1E2C4
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 58EA5EA6 75A27704
            2C2E842C 05061136 B6B53163 20233F49 D5338C38 48C71852
            738F6E1E 39371F50 C84A7910 2C76DA3B C1BFD15C 83CAA8D2
            378D9C32 8C6E5CB0 8F669763 6BB13CC7 77A38855 9237858F
            05606E0A 8014194E 9487DB1F F14E9903 E84EAB89 13EC38BC
            439F2F38 5F2D1E34 DB4A538C AA6161BF 552AD467 62C4C404
            75880763 D69AFA49 34DBEBD0 EB5388F4 CA3FE8FD B08948B3
            1CDC1A5B 7814BD34 5C0F0EFD E4418C1A F6197C7E 8A02B3DB
            78C28F67 EAF85130 F5E04A65 5AFC1673 29E13B3E 709B6255
            97DE7A65 B15EB7A4 92154007 7CD43D24 5C060D5C 14F98AFE
            EC9B039B E1460A59 4A46CD16 7DA70237 27259822 91932C86
            947B4D53 8B4B180D
```

```
MacTag_V  = EA86BE00 C8783454 FE3BB6FF B42CA0FF D6561DB8 07E7D968
            DFDFA22E 99F4098E
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 58EA5EA6 75A27704
            2C2E842C 05061136 B6B53163 20233F49 D5338C38 48C71852
            738F6E1E 39371F50 C84A7910 2C76DA3B C1BFD15C 83CAA8D2
            378D9C32 8C6E5CB0 8F669763 6BB13CC7 77A38855 9237858F
            05606E0A 8014194E 9487DB1F F14E9903 E84EAB89 13EC38BC
            439F2F38 5F2D1E34 DB4A538C AA6161BF 552AD467 62C4C404
            75880763 D69AFA49 34DBEBD0 EB5388F4 CA3FE8FD B08948B3
            1CDC1A5B 7814BD34 5C0F0EFD E4418C1A F6197C7E 8A02B3DB
            78C28F67 EAF85130 F5E04A65 5AFC1673 29E13B3E 709B6255
            97DE7A65 B15EB7A4 92154007 7CD43D24 5C060D5C 14F98AFE
            EC9B039B E1460A59 4A46CD16 7DA70237 27259822 91932C86
            947B4D53 8B4B180D 19B7D0AA 84E65DDA DEC2401C B8035C91
            D15F2EA7 7E39B4A4 39FE0E6C 7B22BFC6

MacTag_U  = BDC52F83 335115A8 F882B1F2 6909E62C 976D7C6F 2B982594
            E6F95A2B 215A54C2

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 19B7D0AA 84E65DDA
            DEC2401C B8035C91 D15F2EA7 7E39B4A4 39FE0E6C 7B22BFC6
            58EA5EA6 75A27704 2C2E842C 05061136 B6B53163 20233F49
            D5338C38 48C71852 738F6E1E 39371F50 C84A7910 2C76DA3B
            C1BFD15C 83CAA8D2 378D9C32 8C6E5CB0 8F669763 6BB13CC7
            77A38855 9237858F 05606E0A 8014194E 9487DB1F F14E9903
            E84EAB89 13EC38BC 439F2F38 5F2D1E34 DB4A538C AA6161BF
            552AD467 62C4C404 75880763 D69AFA49 34DBEBD0 EB5388F4
            CA3FE8FD B08948B3 1CDC1A5B 7814BD34 5C0F0EFD E4418C1A
            F6197C7E 8A02B3DB 78C28F67 EAF85130 F5E04A65 5AFC1673
            29E13B3E 709B6255 97DE7A65 B15EB7A4 92154007 7CD43D24
            5C060D5C 14F98AFE EC9B039B E1460A59 4A46CD16 7DA70237
            27259822 91932C86 947B4D53 8B4B180D
```

```
MacTag_V  = 6106CBC5 730CF460 F9626599 61F9C07B 454C2F1D E1F228A5
            7D15A76E 2D97CD55
```

3.4.6 dhOneFlow for finite field p2048-q256

- Prerequisites:

```
xV =      3D37042D FD8441A4 3D5A4EA9 3A4DBEEC 0D71E3B5 3719CC52
          F894C3D5 3A830B3A

yV =      15C08EFE 47F2418B 1275137F BC028A9E 62016029 DF8444F1
          4327E37E D68FAECA 11400570 B914D149 AC076F29 C6ED1E3F
          E0A96EBF 973378F6 0590858F EAF85A3C CF9265D2 37B93697
          95BB5A2F 88876EC3 82BF68DE 3A0C252A 0518BAED 9707088F
          E87CC2DC 399CA046 EAE4015C 5D4D2851 1509C43A 8D1F04C9
          6C714ABF 27B5B6C8 7C2227FF F021C7CF 82216668 49020644
          E3C6E905 A115242A D01B9428 021EB450 501C64BB 8FF095EE
          61B2FAEF 5F20F169 28FCDF46 1F65B5DE 783C2A4D 0DD5A9BA
          7602DBB6 90184267 586B1222 68167AC5 064478AE 0204B17E
          B8E59B5E 4475767C 695FAE00 78360263 E7220FE7 ECE8BB91
          3ED0AB88 197C5FCF 06513975 5097542C
```

BEGIN U's calculations

- Step 1:

```
rU =      04B7AF95 7BF80E5E 93CE6EAE 1E67165D C04E4391 A61A56C5
          A5E02E10 AB4E6939

tU =      6A99740F E11FF1E3 DFCEB45C 8C5124C2 8C1715E1 D35194EB
          2531E781 C25C13E0 97A36400 84DD83CB 889ECD7D 8FCA033E
          A1C8C265 A3981E0E 7F186E92 0CC18622 BE0F74DE 2621108B
          4074EADF 75D7D8FF DC431C27 2EF7FFBC 8D7AB16C 75EBD292
          3060930B 2E59D80C 01FAC985 9E34915E A122642E CE081F29
          D6715B25 2B16E884 BE75589C B9A2111C 3443199A 238018D9
          BF4BA49D 9ADAF3FF 60BBC5EB B4A9F7AE E2823CB0 F195148D
```

```
307F893C 954A0DE3 6E9CFA1A FF6B02F4 87DC5A99 978362FD
AF65F4CD 86BFE9CA 32CB7A5F 48DFC235 8087F7CD 858AE877
A97D7408 15F830FD C32D8CFD E09831BB 686F02A0 5F2C0F16
939D4758 8742EA8A C04C960D 1393C1CE
```

- Step 2: Decimal value for shared secret.

```
Z =     565555301327327211078313600413389565972343485934 92
        999657927518511182503194993896287840188868320677 34
        733382275785925160603721639141357927752360815734 52
        878859836120861915756648383621838085531435698666 35
        389047932741998746644464921858149685851430942969 44
        327505327512336028920506267734003056339679422921 12
        371248696471763516267021093600930631004269889070 93
        258708433244513806536781346868574157981304631857 28
        301659915621431101258601805707746956224415851685 35
        057435968289404365809393542999522611905822002329 13
        751543361668274362304327433192416641369804156813 15
        544107805732790261978347537383081820317949698513 54
        9143890239816261
```

- Step 3: Hex value for shared secret.

```
Z =     2CCCF4BF A6286776 0C662AA3 59D9822E 48F4431A 60C42451
        EB4F7568 F737A880 B36C6186 B431F8E7 91693C1A DD39A06E
        38A4C28A 455F0A31 80D5368F 401FDC6F 86FB72F6 A293EEB0
        0F9A81D1 ACF202C7 38AF497F BAD8AB4C A691C3FA 3F004BE8
        C07F6140 90858BD4 74E0B2CF 4029EF6B 3E332E1E 619827D9
        049A9A0C 232A92F0 3BAE0880 F868BB0A 38B3D9CD 42D70B14
        30645534 D251C2C5 3FAD8CD9 88CD3C6E 8D736CA0 37A7F58E
        1DE1C74A B184D37D B8CF82B9 A5355706 0C05D3D6 9B5A048A
        5D4212C4 DD67669B 6CE480C4 3293ADDB 5E576F5C A9E99BB0
        8DFB5532 807D77A1 4A9B1D5D 93D9F409 33092D1F D5D18726
        20D8D453 FD8E76CA 01DEEF38 F8F60245
```

- Step 4: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 4EE8467B 0AE068F6 C1848CCE 805A8222 A1DAF8AE 88B54777
             51A7A625 8BAA19B9 29DE8380 C694F277 9CDD3DC3 64D79845
             F75B3B18 18459649 617986C2 B6F0967E
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
rU =      04B7AF95 7BF80E5E 93CE6EAE 1E67165D C04E4391 A61A56C5
          A5E02E10 AB4E6939

tU =      6A99740F E11FF1E3 DFCEB45C 8C5124C2 8C1715E1 D35194EB
          2531E781 C25C13E0 97A36400 84DD83CB 889ECD7D 8FCA033E
          A1C8C265 A3981E0E 7F186E92 0CC18622 BE0F74DE 2621108B
          4074EADF 75D7D8FF DC431C27 2EF7FFBC 8D7AB16C 75EBD292
          3060930B 2E59D80C 01FAC985 9E34915E A122642E CE081F29
          D6715B25 2B16E884 BE75589C B9A2111C 3443199A 238018D9
          BF4BA49D 9ADAF3FF 60BBC5EB B4A9F7AE E2823CB0 F195148D
          307F893C 954A0DE3 6E9CFA1A FF6B02F4 87DC5A99 978362FD
          AF65F4CD 86BFE9CA 32CB7A5F 48DFC235 8087F7CD 858AE877
          A97D7408 15F830FD C32D8CFD E09831BB 686F02A0 5F2C0F16
          939D4758 8742EA8A C04C960D 1393C1CE
```

- Step 2: N/A.
- Step 3: Decimal value for shared secret.

```
Z =       56555530132732721107831360041338956597234348593492
          99965792751851118250319499389628784018886832067734
          73338227578592516060372163914135792775236081573452
          87885983612086191575664838362183808553143569866635
          38904793274199874664446492185814968585143094296944
          32750532751233602892050626773400305633967942292112
          37124869647176351626702109360093063100426988907093
```

```
2587084332445138065367813468685741579813046318572 8
3016599156214311012586018057077469562244158516853 5
0574359682894043658093935429995226119058220023291 3
7515433616682743623043274331924166413698041568131 5
5441078057327902619783475373830818203179496985135 4
9143890239816261
```

- Step 4: Hex value for shared secret.

```
Z =       2CCCF4BF A6286776 0C662AA3 59D9822E 48F4431A 60C42451
          EB4F7568 F737A880 B36C6186 B431F8E7 91693C1A DD39A06E
          38A4C28A 455F0A31 80D5368F 401FDC6F 86FB72F6 A293EEB0
          0F9A81D1 ACF202C7 38AF497F BAD8AB4C A691C3FA 3F004BE8
          C07F6140 90858BD4 74E0B2CF 4029EF6B 3E332E1E 619827D9
          049A9A0C 232A92F0 3BAE0880 F868BB0A 38B3D9CD 42D70B14
          30645534 D251C2C5 3FAD8CD9 88CD3C6E 8D736CA0 37A7F58E
          1DE1C74A B184D37D B8CF82B9 A5355706 0C05D3D6 9B5A048A
          5D4212C4 DD67669B 6CE480C4 3293ADDB 5E576F5C A9E99BB0
          8DFB5532 807D77A1 4A9B1D5D 93D9F409 33092D1F D5D18726
          20D8D453 FD8E76CA 01DEEF38 F8F60245
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 4EE8467B 0AE068F6 C1848CCE 805A8222 A1DAF8AE 88B54777
             51A7A625 8BAA19B9 29DE8380 C694F277 9CDD3DC3 64D79845
             F75B3B18 18459649 617986C2 B6F0967E
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 4EE8467B 0AE068F6 C1848CCE 805A8222
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 6A99740F E11FF1E3
            DFCEB45C 8C5124C2 8C1715E1 D35194EB 2531E781 C25C13E0
            97A36400 84DD83CB 889ECD7D 8FCA033E A1C8C265 A3981E0E
            7F186E92 0CC18622 BE0F74DE 2621108B 4074EADF 75D7D8FF
            DC431C27 2EF7FFBC 8D7AB16C 75EBD292 3060930B 2E59D80C
            01FAC985 9E34915E A122642E CE081F29 D6715B25 2B16E884
            BE75589C B9A2111C 3443199A 238018D9 BF4BA49D 9ADAF3FF
            60BBC5EB B4A9F7AE E2823CB0 F195148D 307F893C 954A0DE3
            6E9CFA1A FF6B02F4 87DC5A99 978362FD AF65F4CD 86BFE9CA
            32CB7A5F 48DFC235 8087F7CD 858AE877 A97D7408 15F830FD
            C32D8CFD E09831BB 686F02A0 5F2C0F16 939D4758 8742EA8A
            C04C960D 1393C1CE

MacTag_V  = 0FC1F505 73B09265 D719CAAE 42EE2151 4E412ACC 44E31180
             DED05D4B 6737F1DC
```

3.4.7 dhStatic for finite field p2048-q256

- Prerequisites:

```
xU =      484850F2 2E54702A 97F54702 46F9AF25 3BEE47ED A5B9A713
          6F43F834 E3F4AA4C

yU =      120CE9E1 C7F69749 26B5D2FC 157022D8 CDDD23B1 048E98F9
          34B39D2D EB6BABEE 454F358C 1D54FB41 72267273 9AB2541C
          9DDD53B7 8299AC32 90F5DC68 49ADF3F3 C7F99076 E53F9CE5
          49C8687A BDB4DD1E E9FF36C4 A3A2942A F516A104 4F833CAC
          466E388E 6C8BCB83 4CAB0AF8 CD5B99B9 06A720AA BA969293
          2DC77995 926D9B91 05B45809 6E8907B8 22DF0BB9 B3DEAF2E
          ABE20C17 6BDFF0B5 A0085DEA 2109294A 787A6FDC 177AFB88
          F43D6697 E8A2CC68 DFE6D8E4 7FB4F3C2 7DF7C53A 8784FEC8
          8E31D36C 54BF614F 628C36EE FC74B2D9 420DCD31 0DE19536
          9D9D3AE4 F61C026E 1239876A 2C207B47 5FD7149B 354E2D34
          308A5767 847495F1 939B8EDD 4C23BCC7
```

```
xV =      4105E2A1 14F13D63 42CD1382 095AAAF7 1CAAB3C3 0BB7BDEB
          77E138B9 BB837E9F

yV =      135C398E 5E9F767C 7C95B7E0 C6FB172A D45D805E 3BC2E6C3
          80A41CF2 46927EF8 10B21797 7A18B387 F6698677 97EB7047
          19D998AA EA4F21D1 B4E24DBC 0E242FC0 5540CB76 0FBB6A8C
          CFAF008E 0A664706 8FAA0B77 0CEF04A2 5A230393 131FCD77
          8ACD2EB6 B11B026A 8D49C11D F80BA6B7 C088CFA3 38BE53B5
          D936C679 C894C55D 9B219FC6 12079FA3 56B4888D 92E54C39
          A3582308 D596C9EF EBF76731 BE5FACC9 FC7C2F05 1624733F
          C3AF7175 7D3CB16D B49D8044 061AC2A9 A1EDE377 33FD4ED3
          1F2179A3 142FA8FE 8FCA3786 664D476D DB5B3A69 B1AE229D
          6F0F5487 3C4B862C 0497284F 1A8ED3C0 247E2737 6E2FC936
          03743B0F 37C3FFC9 3D01B05B ECCDECC4
```

BEGIN U's calculations

- Step 1:

```
nonceU =  021DDABB 1C8326DA EACC8E35 7607DECB 56DC8640 30BBEA24
          94352DEB 6791F02F
```

- Step 2: Decimal value for shared secret.

```
Z =       816911630565552416851401357637102898324558073471984
          455338046822015433696327063656769884258360052525419
          041581336609758049189218686825135110240824586353182
          943502445166871292294924725137907180177598514276821
          919651226803286047475918702100819459286793165993592
          761510096314291175525476403650596751179928280987510
          138006469405689259859341110713189763935627140864194
          637760724994690177483585831163646709654405915142698
          896724532663112866857938488164005919331279295040862
          045933424883937086910995907369274663786968314443676
          408530641319516848529302823857445807904753504947034
          206058051447055689329462396419346795790244519441072
          74367
```

- Step 3: Hex value for shared secret.

```
Z =       40B63CDD B7129BE7 AD46DF54 FC20474C 94B78D2D 9A2B13D6
          CA8C431D 16752E90 59B41E22 FD2F7678 13FB572A AAEFFE72
          A588F710 58C59EF9 1DE12450 F3CCD515 45E76401 09AD05AC
          9CAC9FC1 AB8FBCF3 13E73AED A41C8FF9 22640604 68FAA6E2
          AB9F8683 D6838F67 9C9D76EF 42CE37BC DE5D0C09 2139782D
          019659EF 938ABE10 9795BFDD B0043312 5DAF3F6B BE888251
          B3F0A154 1BB59581 3B852451 FDB2F7AB 2974C5E1 429D2CAB
          19EAD1D0 99CD3CDE 9322B6B1 72058E6D F901D97B 71875AE3
          D367BC72 501DB04D ED6E7208 7EBB7837 D6FBB222 97883F6D
          3662331B 49A49F72 7B2BF08F 3FAE3BC6 EFBE81E3 8101B09B
          9AA86090 41AA1669 0718316F 0220F07F
```

- Step 4: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000020 021DDABB
             1C8326DA EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB
             6791F02F 424F4242 59343536

DerKeyMat  = ED20415A F9BF8EC6 47B7AD98 0D73B310 12237492 1B8E797A
             BED9CAB5 508107EC 626C2E4D 3388FC15 4691D5C1 2ADEF4CC
             0F870EE6 500D84C6 9D4A5FF7 2BD9D615
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
nonceU =  021DDABB 1C8326DA EACC8E35 7607DECB 56DC8640 30BBEA24
          94352DEB 6791F02F
```

- Step 2: Decimal value for shared secret.

```
Z =       81691163056555241685140135763710289832455807347198
          45533804682201543369632706365676988425836005252541
          90415813366097580491892186868251351102408245863531
```

```
829435024451668712922949247251379071801775985142 76
821919651226803286047475918702100819459286793165 99
359276151009631429117552547640365059675117992828 09
875101380064694056892598593411107131897639356271 40
864194637760724994690177483585831163646709654405 91
514269889672453266311286685793848816400591933127 92
950408620459334248839370869109959073692746637869 68
314443676408530641319516848529302823857445807904 75
350494703420605805144705568932946239641934679579 02
4451944107274367
```

- Step 3: Hex value for shared secret.

```
Z =        40B63CDD B7129BE7 AD46DF54 FC20474C 94B78D2D 9A2B13D6
           CA8C431D 16752E90 59B41E22 FD2F7678 13FB572A AAEFFE72
           A588F710 58C59EF9 1DE12450 F3CCD515 45E76401 09AD05AC
           9CAC9FC1 AB8FBCF3 13E73AED A41C8FF9 22640604 68FAA6E2
           AB9F8683 D6838F67 9C9D76EF 42CE37BC DE5D0C09 2139782D
           019659EF 938ABE10 9795BFDD B0043312 5DAF3F6B BE888251
           B3F0A154 1BB59581 3B852451 FDB2F7AB 2974C5E1 429D2CAB
           19EAD1D0 99CD3CDE 9322B6B1 72058E6D F901D97B 71875AE3
           D367BC72 501DB04D ED6E7208 7EBB7837 D6FBB222 97883F6D
           3662331B 49A49F72 7B2BF08F 3FAE3BC6 EFBE81E3 8101B09B
           9AA86090 41AA1669 0718316F 0220F07F
```

- Step 4: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000020 021DDABB
             1C8326DA EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB
             6791F02F 424F4242 59343536

DerKeyMat  = ED20415A F9BF8EC6 47B7AD98 0D73B310 12237492 1B8E797A
             BED9CAB5 508107EC 626C2E4D 3388FC15 4691D5C1 2ADEF4CC
             0F870EE6 500D84C6 9D4A5FF7 2BD9D615
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = ED20415A F9BF8EC6 47B7AD98 0D73B310

nonceV =  10033DD1 41ED4A76 F3D0D3E5 2983222B 2AD10743 AD163E5C
          007F3EF3 B9891062
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 021DDABB 1C8326DA
            EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB 6791F02F
            10033DD1 41ED4A76 F3D0D3E5 2983222B 2AD10743 AD163E5C
            007F3EF3 B9891062

MacTag_U  = 06FAB167 88FDB5C9 F64ADF85 ACD7880C C48C4CBF 14940786
            43DC5F91 57643C1F
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 021DDABB 1C8326DA
            EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB 6791F02F

MacTag_V  = 4DD37DC7 F1BF2617 E722D0B7 5E186AE2 FFB57FB7 00595E99
            893DE1AD 09C80B01
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 021DDABB 1C8326DA
            EACC8E35 7607DECB 56DC8640 30BBEA24 94352DEB 6791F02F
            10033DD1 41ED4A76 F3D0D3E5 2983222B 2AD10743 AD163E5C
            007F3EF3 B9891062
```

```
 MacTag_U  = F90027B3 99F4799B F230FE7F 5B126C09 7546987E F6EB1D55
             E46EFC57 EFDE4298

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

           = 4B435F32 5F56424F 42425941 4C494345 10033DD1 41ED4A76
             F3D0D3E5 2983222B 2AD10743 AD163E5C 007F3EF3 B9891062
             021DDABB 1C8326DA EACC8E35 7607DECB 56DC8640 30BBEA24
             94352DEB 6791F02F

 MacTag_V  = 1864F290 44B87A7D A058E511 054386D1 6E1AED64 9C9709F7
             59CADFEE 121F79B5
```

4

Parameter sets for elliptic curve schemes

The following five parameter sets, used throughout this document in the elliptic curve schemes, are the recommended elliptic curves for federal government use from FIPS 186-3 [2].

Since each field has prime order, there is no basis choice or parameter. Since each group has prime order, the cofactor, (often denoted by h), is always equal to 1. Thus the basis and cofactor parameters are not included in what follows.

One can generate alternate parameter sets which satisfy the size requirements given in [1, section 5.5.1.2, Table 2] as specified in ANS X.9.62 [5].

4.1 Curve P–192

Field size:

```
q =       FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF
```

Curve parameter:

```
a =       FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFC
```

Curve parameter:

```
b =       64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1
```

Seed used to generate parameter b:

```
seed =    3045AE6F C8422F64 ED579528 D38120EA E12196D5
```

x-coordinate of base point G:

```
xG =      188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012
```

y-coordinate of base point G:

```
yG =      07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811
```

Order of the point G:

```
n =       FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831
```

4.2 Curve P–224

Field size:

```
q =       FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF 00000000 00000000
          00000001
```

Curve parameter:

```
a =       FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF
          FFFFFFFE
```

Curve parameter:

```
b =       B4050A85 0C04B3AB F5413256 5044B0B7 D7BFD8BA 270B3943
          2355FFB4
```

Seed used to generate parameter b:

```
seed =    BD713447 99D5C7FC DC45B59F A3B9AB8F 6A948BC5
```

x-coordinate of base point G:

```
xG =      B70E0CBD 6BB4BF7F 321390B9 4A03C1D3 56C21122 343280D6
          115C1D21
```

y-coordinate of base point G:

```
yG =      BD376388 B5F723FB 4C22DFE6 CD4375A0 5A074764 44D58199
          85007E34
```

Order of the point G:

```
n =       FFFFFFFF FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945
          5C5C2A3D
```

4.3 Curve P–256

Field size:

```
q =       FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF
          FFFFFFFF FFFFFFFF
```

Curve parameter:

```
a =       FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF
          FFFFFFFF FFFFFFFC
```

Curve parameter:

```
b =       5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6
          3BCE3C3E 27D2604B
```

Seed used to generate parameter b:

```
seed =    C49D3608 86E70493 6A6678E1 139D26B7 819F7E90
```

x-coordinate of base point G:

```
xG =      6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0
          F4A13945 D898C296
```

y-coordinate of base point G:

```
yG =      4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE
          CBB64068 37BF51F5
```

Order of the point G:

```
n =       FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84
          F3B9CAC2 FC632551
```

4.4 Curve P–384

Field size:

```
q =       FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
          FFFFFFFF FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFF
```

Curve parameter:

```
a =       FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
          FFFFFFFF FFFFFFFE FFFFFFFF 00000000 00000000 FFFFFFFC
```

Curve parameter:

```
b =       B3312FA7 E23EE7E4 988E056B E3F82D19 181D9C6E FE814112
          0314088F 5013875A C656398D 8A2ED19D 2A85C8ED D3EC2AEF
```

Seed used to generate parameter b:

```
seed =    A335926A A319A27A 1D00896A 6773A482 7ACDAC73
```

x-coordinate of base point G:

```
xG =      AA87CA22 BE8B0537 8EB1C71E F320AD74 6E1D3B62 8BA79B98
          59F741E0 82542A38 5502F25D BF55296C 3A545E38 72760AB7
```

y-coordinate of base point G:

```
yG =      3617DE4A 96262C6F 5D9E98BF 9292DC29 F8F41DBD 289A147C
          E9DA3113 B5F0B8C0 0A60B1CE 1D7E819D 7A431D7C 90EA0E5F
```

Order of the point G:

```
n =       FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
          C7634D81 F4372DDF 581A0DB2 48B0A77A ECEC196A CCC52973
```

4.5 Curve P–521

Field size:

```
q =       000001FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
          FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
          FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
```

Curve parameter:

```
a =       000001FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
          FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
          FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFC
```

Curve parameter:

```
b =       00000051 953EB961 8E1C9A1F 929A21A0 B68540EE A2DA725B
          99B315F3 B8B48991 8EF109E1 56193951 EC7E937B 1652C0BD
          3BB1BF07 3573DF88 3D2C34F1 EF451FD4 6B503F00
```

Seed used to generate parameter b:

```
seed =    D09E8800 291CB853 96CC6717 393284AA A0DA64BA
```

x-coordinate of base point G:

```
xG =      000000C6 858E06B7 0404E9CD 9E3ECB66 2395B442 9C648139
          053FB521 F828AF60 6B4D3DBA A14B5E77 EFE75928 FE1DC127
          A2FFA8DE 3348B3C1 856A429B F97E7E31 C2E5BD66
```

y-coordinate of base point G:

```
yG =      00000118 39296A78 9A3BC004 5C8A5FB4 2C7D1BD9 98F54449
          579B4468 17AFBD17 273E662C 97EE7299 5EF42640 C550B901
          3FAD0761 353C7086 A272C240 88BE9476 9FD16650
```

Order of the point G:

```
n =       000001FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
          FFFFFFFF FFFFFFFF FFFFFFFA 51868783 BF2F966B 7FCC0148
          F709A5D0 3BB5C9B8 899C47AE BB6FB71E 91386409
```

5

Elliptic curve key agreement schemes

5.1 Parameter sizes and hash functions

Throughout this chapter, the following parameter sizes (in bits) and hash algorithms [3] are used.

Parameter set	Private key size	Hash algorithm	MacKey size	MacLen	Nonce size
P–192	192	SHA-1	96	160	192
P–224	224	SHA–224	112	224	224
P–256	256	SHA–256	128	256	256
P–384	384	SHA–384	192	384	384
P–521	521	SHA–512	256	512	512

5.2 Test data for P–192

In this section, we supply step–by–step test data for the seven elliptic curve key agreement schemes described in [1, section 6] using the parameter set P–192 described in Appendix 4.1. For each scheme, a reference to the corresponding section in [1] is provided.

5.2.1 Full Unified Model for curve P–192

- Prerequisites:

```
dsU   =   6D430452 8586E674 0A967BF3 4157C80A 81062AC5 E1C0D8A6

x_QsU =   9E9D6910 B25CC142 2487B29C 775239C7 976BFB63 DBC32CFA

y_QsU =   DA5F1F56 56DBD935 3D2062B9 3EA3B2A9 E7DCB57C 21FEF14F

dsV   =   7E93F69B 83F57B90 95ABCA59 7D73B948 F2A5C542 A79B1520

x_QsV =   F95C0961 5671A879 5A580D21 B0501A9C 44D7C668 66680576

y_QsV =   E1BB79AB D7D73CF4 60EB2A9C 72D9D992 4D3A695D 2E3C3FA9
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   2FF958DD F8E907D0 027BC381 7E82C7F9 A856EE3A 867F4686

x_QeU =   B31BC3F3 BC1B4328 AE5A4557 F720410D 3DB64200 9BC70FCE

y_QeU =   401786B5 384992DB A0D860D8 73E5B7E6 32E02A8C 05CFDCE6

deV   =   9CFC8B21 4EEF74A8 2C945E5F 640EC15A A0587C0F D78804BC
```

```
x_QeV =   2CBF953A 8B111F35 9D097ABC 2A423076 9B3EAB6D E10010EE

y_QeV =   D1C3B54A 9C38EC8C 05EA7AB4 16F66A01 54E81CF1 F6F2DAFA
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     546780023949586533887733132311426155383125603417957
          7387866

Z_s =     DEFE7F85 9F0D89F8 0AEA2A3F ABFA97C2 E559E006 4E4D9B5A
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     335234936728289305417352746387413728643984445292270
          9299405

Z_e =     88B82915 B3B94941 BF42F8D0 979003F7 108E0AC3 43DCD0CD
```

- Step 5: Shared secret.

```
Z =       88B82915 B3B94941 BF42F8D0 979003F7 108E0AC3 43DCD0CD
          DEFE7F85 9F0D89F8 0AEA2A3F ABFA97C2 E559E006 4E4D9B5A
```

- Step 6: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = CD401051 B3BA8DBF 91364AD3 24D95DFD 71F1DBE1 C4E56025
             DBECE7F6 CA01E6A9 3A804F0D 2116C89B
```

- If key confirmation is performed, then

```
MacKey  = CD401051 B3BA8DBF 91364AD3
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 B31BC3F3 BC1B4328
            AE5A4557 F720410D 3DB64200 9BC70FCE 401786B5 384992DB
            A0D860D8 73E5B7E6 32E02A8C 05CFDCE6 2CBF953A 8B111F35
            9D097ABC 2A423076 9B3EAB6D E10010EE D1C3B54A 9C38EC8C
            05EA7AB4 16F66A01 54E81CF1 F6F2DAFA

 MacTag_U  = 880488DD F88D1A99 07B1C0E6 3026F43E 8DAC75DE
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 2CBF953A 8B111F35
            9D097ABC 2A423076 9B3EAB6D E10010EE D1C3B54A 9C38EC8C
            05EA7AB4 16F66A01 54E81CF1 F6F2DAFA B31BC3F3 BC1B4328
            AE5A4557 F720410D 3DB64200 9BC70FCE 401786B5 384992DB
            A0D860D8 73E5B7E6 32E02A8C 05CFDCE6

 MacTag_V  = 738F2EB8 1AC3800F B69FDC4B 2BD29C06 DDC7AE0A
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 B31BC3F3 BC1B4328
             AE5A4557 F720410D 3DB64200 9BC70FCE 401786B5 384992DB
             A0D860D8 73E5B7E6 32E02A8C 05CFDCE6 2CBF953A 8B111F35
             9D097ABC 2A423076 9B3EAB6D E10010EE D1C3B54A 9C38EC8C
             05EA7AB4 16F66A01 54E81CF1 F6F2DAFA

 MacTag_U  = B76F5EE6 2D3F65D7 27BC4E1A 46B4A4AB F193A6A0
```

```
MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 2CBF953A 8B111F35
            9D097ABC 2A423076 9B3EAB6D E10010EE D1C3B54A 9C38EC8C
            05EA7AB4 16F66A01 54E81CF1 F6F2DAFA B31BC3F3 BC1B4328
            AE5A4557 F720410D 3DB64200 9BC70FCE 401786B5 384992DB
            A0D860D8 73E5B7E6 32E02A8C 05CFDCE6

MacTag_V  = 1526FE29 A31EB3DE 4413051C 9DF36A62 4589937C
```

5.2.2 Full MQV for curve P–192

- Prerequisites:

```
dsU   =   75CAA21D 238D38E0 146EC318 040734A1 0DD11F7D 409E8FDA

x_QsU =   BC454041 4C64E777 E95449F4 643971E0 84E6A88B 6F1E557E

y_QsU =   0E9BD20B 6B1C408B 934C3F49 7E5B25AD 2E73A50F 4A74A847

dsV   =   8ED403CF 78F66AC4 84F141F6 8724F196 434FFA01 540187DA

x_QsV =   BF5F88EC DACE966D 73F36DDF B4D52E21 AA1853A3 AFEDCF81

y_QsV =   E2454F18 CE7D2D1E 0A1371CC E3C3875F 4DBD9C20 5BD8761D
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   C53443F4 2D845604 302FC7BF F71CFDCD 403514CF F42F1497

x_QeU =   13657559 76B8E4D8 42D8E959 FB2F0E71 EBAB2AE2 211BECAB

y_QeU =   B757FF94 E88FF9F5 16A42A8F 34A36E87 E9575FF8 97535ACD
```

```
deV   =   11E5649D 82879D0D 14F4212C 2125663B AAE0D710 F8CC5F98

x_QeV =   DBADE7CA 23706FA0 CC685796 390D47F0 EEA5E48B 29E64885

y_QeV =   8E56B9E9 72FD6E61 E30EDA64 59A524F7 52F5F410 FE9A46DC
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       29819955045123990967397335135590082548538870398295
          81516049
```

- Step 4: Shared secret converted to byte string.

```
Z =       799D7C59 A117747A 5AF792CF 7EA143A4 DFF2669D FAC84D11
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = ACA895E1 F1942B66 DAFBB365 D7B342EC 8D78C7CB 12968599
             FAADC726 D2864E1E A305B6D0 EA13B2BB
```

- If key confirmation is performed, then

```
MacKey  = ACA895E1 F1942B66 DAFBB365
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 13657559 76B8E4D8
            42D8E959 FB2F0E71 EBAB2AE2 211BECAB B757FF94 E88FF9F5
            16A42A8F 34A36E87 E9575FF8 97535ACD DBADE7CA 23706FA0
            CC685796 390D47F0 EEA5E48B 29E64885 8E56B9E9 72FD6E61
            E30EDA64 59A524F7 52F5F410 FE9A46DC
```

```
MacTag_U  = 832F5036 EA429341 C0A5ABFB 97D40C97 280CE91E
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 DBADE7CA 23706FA0
            CC685796 390D47F0 EEA5E48B 29E64885 8E56B9E9 72FD6E61
            E30EDA64 59A524F7 52F5F410 FE9A46DC 13657559 76B8E4D8
            42D8E959 FB2F0E71 EBAB2AE2 211BECAB B757FF94 E88FF9F5
            16A42A8F 34A36E87 E9575FF8 97535ACD

MacTag_V  = 5BEEBEBE A6240F40 882B4E38 5C8FA24E FD245297
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 13657559 76B8E4D8
            42D8E959 FB2F0E71 EBAB2AE2 211BECAB B757FF94 E88FF9F5
            16A42A8F 34A36E87 E9575FF8 97535ACD DBADE7CA 23706FA0
            CC685796 390D47F0 EEA5E48B 29E64885 8E56B9E9 72FD6E61
            E30EDA64 59A524F7 52F5F410 FE9A46DC

MacTag_U  = 93F38054 B0D5B05C D519222A 383F2B63 A997FB6F

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 DBADE7CA 23706FA0
            CC685796 390D47F0 EEA5E48B 29E64885 8E56B9E9 72FD6E61
            E30EDA64 59A524F7 52F5F410 FE9A46DC 13657559 76B8E4D8
            42D8E959 FB2F0E71 EBAB2AE2 211BECAB B757FF94 E88FF9F5
            16A42A8F 34A36E87 E9575FF8 97535ACD

MacTag_V  = E9311938 D9EFFDFA AABA6741 FDDA02D0 EE99CC80
```

5.2.3 Ephemeral Unified Model for curve P–192

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   0C5FABD9 A3A79D09 3D57A6C8 D18FFC57 7CE69FBD 00C8BA71

x_QeU =   E496011D F3832BFE 8A13A2BF 49697822 7E186D1D 23EE49E8

y_QeU =   36B18BF3 D714D777 6279BE8E 7F571D54 F1E547ED 4CE452F1

deV   =   A8DC54A1 3B6BFECD 905A34E6 89A796FF 1CEB7761 0E698B81

x_QeV =   243D7694 E3301CF4 4C03DC19 F6BB6E28 C5E29B6C 075582EA

y_QeV =   3D05DF80 B641863D 44BF3A09 1655C692 B313525F 85A5D291
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       106104521639639730501949514433129329947091515354513
          6541490
```

- Step 4:

```
Z =       2B45D435 CF6EDF4C 1891152B A11EBA09 D46AD2C0 88458F32
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = D3BD32CB AB330685 CCEFF78A 51ABCDD4 F2B01432 E7AA52BB
             066639C1 8329219C 8BC9BCAA EC50E5AC
```

5.2.4 One–Pass Unified Model for curve P–192

- Prerequisites:

```
dsU   =   0E15C6F5 55738E90 1172BD10 3296D1BE 8755FB7B D75B0CBA

x_QsU =   57803CDA FED342E6 5AA32ECE 17919092 E21FD609 6F7D7598

y_QsU =   12D5FB9F 28FE2979 72045C88 4B599039 81430F53 B030963C

dsV   =   B769B2FE D1EBCD6E 09FB21A4 170F594E BE534B86 53FD4E9F

x_QsV =   FCF80D6D 60656608 2B32CD15 263E6FF3 6E32390E E76D3CC5

y_QsV =   40F0FCE5 326F2B45 807B672E 05EB70C1 7785CF00 485C2651
```

BEGIN U's calculations

- Step 1:

```
deU   =   C22C7EA2 37CFCE3D C886055F 0BA89B42 61E3C151 82803915

x_QeU =   44EFBC07 70F3D6FB 3CCD78E5 8DDC0663 D2E97497 17C1B535

y_QeU =   ABEA77A4 68A4D919 AA61BC42 BF8A8EB7 1D4FA4A7 C9F07186
```

- Step 2: Decimal and hex values for static shared secret.

```
Z_s =     181581114404837557544042024466320945185422562883030
          58801555

Z_s =     4A0DF3F2 2D5C17B2 795A07A3 1E3455FA 56176B8B B1178C93
```

- Step 3: Decimal and hex values for ephemeral shared secret.

```
Z_e =     348149522189416573368787071392765867644153277294802
          2765060
```

```
Z_e =     8DFC8191 434F7239 D345D2F6 ECE44684 ECC7BD53 CC99A604
```

- Step 4: Shared secret.

```
Z =       8DFC8191 434F7239 D345D2F6 ECE44684 ECC7BD53 CC99A604
          4A0DF3F2 2D5C17B2 795A07A3 1E3455FA 56176B8B B1178C93
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 6B4D066A 0134B584 DBCDAF0C 08C8D98E F7F60F8D BF57E5F8
             CF68C831 20724BD7 4C0548E4 8BAD3AB3
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   C22C7EA2 37CFCE3D C886055F 0BA89B42 61E3C151 82803915

x_QeU =   44EFBC07 70F3D6FB 3CCD78E5 8DDC0663 D2E97497 17C1B535

y_QeU =   ABEA77A4 68A4D919 AA61BC42 BF8A8EB7 1D4FA4A7 C9F07186
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     181581114404837557544042024466320945185422562883030
          58801555

Z_s =     4A0DF3F2 2D5C17B2 795A07A3 1E3455FA 56176B8B B1178C93
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     34814952218941657336878707139276586764415327729480
          22765060

Z_e =     8DFC8191 434F7239 D345D2F6 ECE44684 ECC7BD53 CC99A604
```

- Step 5: Shared secret.

```
Z =       8DFC8191 434F7239 D345D2F6 ECE44684 ECC7BD53 CC99A604
          4A0DF3F2 2D5C17B2 795A07A3 1E3455FA 56176B8B B1178C93
```

- Step 6: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 6B4D066A 0134B584 DBCDAF0C 08C8D98E F7F60F8D BF57E5F8
             CF68C831 20724BD7 4C0548E4 8BAD3AB3
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 6B4D066A 0134B584 DBCDAF0C

nonceV =  039DF777 1E27AEA9 FA71686C 8C1FB557 62754277 E3A6BF94
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 44EFBC07 70F3D6FB
            3CCD78E5 8DDC0663 D2E97497 17C1B535 ABEA77A4 68A4D919
            AA61BC42 BF8A8EB7 1D4FA4A7 C9F07186 039DF777 1E27AEA9
            FA71686C 8C1FB557 62754277 E3A6BF94

MacTag_U  = E4CE2D27 248BA354 65ECE081 25853F32 2D816D35
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 44EFBC07 70F3D6FB
            3CCD78E5 8DDC0663 D2E97497 17C1B535 ABEA77A4 68A4D919
            AA61BC42 BF8A8EB7 1D4FA4A7 C9F07186

 MacTag_V  = 2EA2B130 5745B28A 0DE6B3BF 48269FB8 C22C70E3
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 44EFBC07 70F3D6FB
             3CCD78E5 8DDC0663 D2E97497 17C1B535 ABEA77A4 68A4D919
             AA61BC42 BF8A8EB7 1D4FA4A7 C9F07186 039DF777 1E27AEA9
             FA71686C 8C1FB557 62754277 E3A6BF94

 MacTag_U  = CC650736 FC3B3097 B2BB0918 7450C89A 07F2CAD3

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

           = 4B435F32 5F56424F 42425941 4C494345 039DF777 1E27AEA9
             FA71686C 8C1FB557 62754277 E3A6BF94 44EFBC07 70F3D6FB
             3CCD78E5 8DDC0663 D2E97497 17C1B535 ABEA77A4 68A4D919
             AA61BC42 BF8A8EB7 1D4FA4A7 C9F07186

 MacTag_V  = 98DD1D78 5767B74F E662DA0E A71CA575 3D7F9705
```

5.2.5 One–Pass MQV for curve P–192

- Prerequisites:

```
dsU   =   010F45D9 1856415F 38D5D2E0 A7127218 A6A03C65 94403097

x_QsU =   7C02D467 082D8C2E 0C34C530 41E8AAE2 EA18799B BC844787

y_QsU =   52D4BF48 963FDB9B D4212F21 F9D0B4F6 44550A49 A2B39D09

dsV   =   678FB36F ACB325FA 2107AFDE 71C02143 6334FD7B A974294A

x_QsV =   13CC1467 6D4B0C7C 159DE35F A49EF001 E67E9494 A56736B4

y_QsV =   650C6BB7 9F6CDEC8 34963728 71D7034A A6559965 6F1BD27D
```

  BEGIN U's calculations

- Step 1:

```
deU   =   CE0583B9 10D494EC 92DBA7C6 692A12E8 2A1A027D BFF04AAC

x_QeU =   4A58FEF3 ECC45FED 092F4636 41EBF2E4 42D16768 9BCEEE87

y_QeU =   C9A8E9CB 2BC92C73 F352262E EC183724 6012DB0A 8686A049
```

- Step 2: Decimal value for shared secret.

```
Z =       42847190837735524690641161434173129240953116684998
          71446707
```

- Step 3: Hex value for shared secret.

```
Z =       AEBE8DF5 B363B8BD 639F7975 F8B2BD1B 4CDA0F67 F62036B3
```

- Step 4: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 60668614 DAF4D034 BC8D41B0 5FB65E37 8F34FD93 7A857E99
             A8CDD5D9 2E4440F3 E9CFB776 3BB1650C
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   CE0583B9 10D494EC 92DBA7C6 692A12E8 2A1A027D BFF04AAC

x_QeU =   4A58FEF3 ECC45FED 092F4636 41EBF2E4 42D16768 9BCEEE87

y_QeU =   C9A8E9CB 2BC92C73 F352262E EC183724 6012DB0A 8686A049
```

- Step 2: N/A.
- Step 3: Decimal value for shared secret.

```
Z =       42847190837735524690641161434173129240953116684998
          71446707
```

- Step 4: Hex value for shared secret.

```
Z =       AEBE8DF5 B363B8BD 639F7975 F8B2BD1B 4CDA0F67 F62036B3
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 60668614 DAF4D034 BC8D41B0 5FB65E37 8F34FD93 7A857E99
             A8CDD5D9 2E4440F3 E9CFB776 3BB1650C
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 60668614 DAF4D034 BC8D41B0

nonceV =  2C7A5EB5 BEF34D32 E03BDEBA 1BDD7F62 F7D2BFFA 862A5596
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 4A58FEF3 ECC45FED
            092F4636 41EBF2E4 42D16768 9BCEEE87 C9A8E9CB 2BC92C73
            F352262E EC183724 6012DB0A 8686A049 2C7A5EB5 BEF34D32
            E03BDEBA 1BDD7F62 F7D2BFFA 862A5596

MacTag_U  = FD0F4E6C 11443AB9 A6283AB8 D90EB28B D4227A23
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 4A58FEF3 ECC45FED
            092F4636 41EBF2E4 42D16768 9BCEEE87 C9A8E9CB 2BC92C73
            F352262E EC183724 6012DB0A 8686A049

MacTag_V  = 28E19B12 130D697C 50DC0657 A96FB4E4 A45B09F3
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 4A58FEF3 ECC45FED
             092F4636 41EBF2E4 42D16768 9BCEEE87 C9A8E9CB 2BC92C73
             F352262E EC183724 6012DB0A 8686A049 2C7A5EB5 BEF34D32
             E03BDEBA 1BDD7F62 F7D2BFFA 862A5596

MacTag_U  = D101D73B F4A920BF 5AB75BDA FBB6D1D7 67053953

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

           = 4B435F32 5F56424F 42425941 4C494345 2C7A5EB5 BEF34D32
             E03BDEBA 1BDD7F62 F7D2BFFA 862A5596 4A58FEF3 ECC45FED
             092F4636 41EBF2E4 42D16768 9BCEEE87 C9A8E9CB 2BC92C73
             F352262E EC183724 6012DB0A 8686A049

MacTag_V  = FC543D21 353CD0B4 0AA3A368 6042118B 6A4FEF12
```

5.2.6 One–Pass Diffie–Hellman for curve P–192

- Prerequisites:

```
dsV   =   78498A4D DAC64855 CFB42CF3 2EDE25BB 73480043 B54A51A6

x_QsV =   24EAA57B AD4B1247 6E937F1E FA6E5B84 8F731BB3 EB2EF7D8

y_QsV =   5722235B AF139417 AFE6912B B5D53A5E DBE974B1 85F83E51
```

BEGIN U's calculations

- Step 1:

```
deU   =   3A698479 13822590 6EFDA188 D67D7798 9FAB055D E540A757

x_QeU =   914E6CC4 A26D1F7F D1385FBA C605B76A 3C9D2A2A 966A9E8B

y_QeU =   95EC7DAF D149DFC8 7EF98553 06015C6E F14A476C D7C1A4DE
```

- Step 2: Decimal value for shared secret.

```
Z =       134506481711365272905645351637624224055161571807091
          8349342
```

- Step 3: Hex value for shared secret.

```
Z =       36DB21C6 A5D67ADA 78CD18C2 C6A2B1C7 DDDFC372 B31C821E
```

- Step 4: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = B550514F 0C24A321 923E4C42 F6A06C46 4D62B034 1045F474
             FAEE6B7D 73A9AD38 19D53721 2B153F8A
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   3A698479 13822590 6EFDA188 D67D7798 9FAB055D E540A757

x_QeU =   914E6CC4 A26D1F7F D1385FBA C605B76A 3C9D2A2A 966A9E8B

y_QeU =   95EC7DAF D149DFC8 7EF98553 06015C6E F14A476C D7C1A4DE
```

- Step 2: N/A.
- Step 3: Decimal value for shared secret.

```
Z =       1345064817113652729056453516376242240551615718070918349342
```

- Step 4: Hex value for shared secret.

```
Z =       36DB21C6 A5D67ADA 78CD18C2 C6A2B1C7 DDDFC372 B31C821E
```

- Step 5: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = B550514F 0C24A321 923E4C42 F6A06C46 4D62B034 1045F474
             FAEE6B7D 73A9AD38 19D53721 2B153F8A
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = B550514F 0C24A321 923E4C42
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 914E6CC4 A26D1F7F
            D1385FBA C605B76A 3C9D2A2A 966A9E8B 95EC7DAF D149DFC8
            7EF98553 06015C6E F14A476C D7C1A4DE

MacTag_V  = 58F29C6C 1AA43321 F4C077E5 12BCC6E7 8AD35F6A
```

5.2.7 Static Unified Model for curve P–192

- Prerequisites:

```
dsU   =   23232AEF 6E4B145E BAD0EB2A A3320C4B 14AA4BDA 38CD678C

x_QsU =   A77DD313 B6091BEA 8C399DE0 316ABD8F 50CAC5C7 919A5A89

y_QsU =   534B2BA6 65CE315C 22F62FBE AE4D91DB F1817364 174B609F

dsV   =   9A7BD877 31618CF4 66012780 BDE864C7 9F07FDF7 37137B70

x_QsV =   21B09A8E 3D20DD76 3E34B10C C7DCECF4 2305F107 7F909F79

y_QsV =   C071147E 57AAB400 DF851E79 E2108266 EB0B66C9 29860BE6
```

BEGIN U's calculations

- Step 1:

```
nonceU =  E6EC913F 1599D1CE 3F5300B3 3A39F022 E9815034 1EAD20BD
```

- Step 2: Decimal value for shared secret.

```
Z =       23533910631393876064288232207326807697590307046205
          97460689
```

- Step 3: Hex value for shared secret.

```
Z =       5FFA8C95 259F1E6A 013550B7 5996A458 E72D2947 A3C8BED1
```

- Step 4: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000018 E6EC913F
             1599D1CE 3F5300B3 3A39F022 E9815034 1EAD20BD 424F4242
             59343536
```

```
DerKeyMat  = 5CCF4223 070B7811 B89B9438 A2297BA8 1F781F65 4525E345
             618C0A81 776FFAAF A6A9F5E2 09DCE3B3
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
nonceU =  E6EC913F 1599D1CE 3F5300B3 3A39F022 E9815034 1EAD20BD
```

- Step 2: Decimal value for shared secret.

```
Z =       23533910631393876064288232207326807697590307046205
          97460689
```

- Step 3: Hex value for shared secret.

```
Z =       5FFA8C95 259F1E6A 013550B7 5996A458 E72D2947 A3C8BED1
```

- Step 4: Additional inputs into the key derivation function and two blocks (320 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000018 E6EC913F
             1599D1CE 3F5300B3 3A39F022 E9815034 1EAD20BD 424F4242
             59343536

DerKeyMat  = 5CCF4223 070B7811 B89B9438 A2297BA8 1F781F65 4525E345
             618C0A81 776FFAAF A6A9F5E2 09DCE3B3
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 5CCF4223 070B7811 B89B9438

nonceV =  E1EE2763 49C8C9F1 2B82AB59 9BEB1C04 4EEF0AA2 4A37811B
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 E6EC913F 1599D1CE
            3F5300B3 3A39F022 E9815034 1EAD20BD E1EE2763 49C8C9F1
            2B82AB59 9BEB1C04 4EEF0AA2 4A37811B

 MacTag_U  = E720250E EEEAF7AC 211435DA 6461C189 37FBFB44
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 E6EC913F 1599D1CE
            3F5300B3 3A39F022 E9815034 1EAD20BD

 MacTag_V  = AE38FD6C B2B576C1 B04258BF 56CBDCF2 014E0697
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 E6EC913F 1599D1CE
             3F5300B3 3A39F022 E9815034 1EAD20BD E1EE2763 49C8C9F1
             2B82AB59 9BEB1C04 4EEF0AA2 4A37811B

 MacTag_U  = D02E9A86 58F1B69D 558B8C91 08F3EE41 E4EE3C3E

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

           = 4B435F32 5F56424F 42425941 4C494345 E1EE2763 49C8C9F1
             2B82AB59 9BEB1C04 4EEF0AA2 4A37811B E6EC913F 1599D1CE
             3F5300B3 3A39F022 E9815034 1EAD20BD

 MacTag_V  = 020708A5 BE53520A 5C81AB9E E3261D24 94801B27
```

5.3 Test data for P–224

In this section, we supply step–by–step test data for the seven elliptic curve key agreement schemes described in [1, section 6] using the parameter set P–224 described in Appendix 4.2. For each scheme, a reference to the corresponding section in [1] is provided.

5.3.1 Full Unified Model for curve P–224

- Prerequisites:

```
dsU   =   546474B8 AF5DED41 21293B2B D1046FD8 33C8E1F2 6DC068C2
          EFD8AF2C

x_QsU =   21BD69CA 4748B6E8 8B4CB85F 62B11E43 2344CA08 405737D3
          74A06DBD

y_QsU =   8089289E 04748185 9D2F8596 45E3EB72 96CAE37E 39AB71AD
          6388B9FB

dsV   =   6C170FF8 34A9A7C9 82C0AD12 B8A0A4A8 F9ED6156 19F0DBE9
          FE471252

x_QsV =   2181D767 F94343E8 90931CBC 21F1C4E9 4C09ACA9 70F24DE2
          07478067

y_QsV =   983F9F74 B90A7E00 BDC88D63 AAD9B588 5BE5310F E407BFC5
          28A944C8
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   99E9A638 9C2C8005 C445316E F6B541CF C74966FC 973C6C13
          1AAB9E10
```

```
x_QeU =   AAB47C8F 476AF10C AD7B06FD 3BB61F39 B4BD4153 F2B60691
          B3938BD8

y_QeU =   43991C37 7CDC21B1 92FB37A6 4D840452 38466C3C 41709A02
          00B450AB

deV   =   E7A28FCE 482B86C6 3324EF6E 654B52F1 BB4E45ED 73287B5D
          7B3EDD1E

x_QeV =   318D0AE4 1D0C812C C00FC7AB 7F9E6E19 FC62CA88 0CDACFBA
          D078B1CF

y_QeV =   BC516CBA 47F6B581 92711621 2E8275EA 5308318A 73150F44
          328A661C
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     96184294821180973743053697618395386525906238510035
          27153025847277893

Z_s =     5B551B5C 93765409 0C92FCC3 11958579 9BA8C818 1B17D9F8
          D2F23945
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     18650342325763840516104565482090219774163749062269
          452714017110288240

Z_e =     B1187885 E70E0D16 443872BE 035AF8DA 298239FA B55BD826
          1286E770
```

- Step 5: Shared secret.

```
Z =       B1187885 E70E0D16 443872BE 035AF8DA 298239FA B55BD826
          1286E770 5B551B5C 93765409 0C92FCC3 11958579 9BA8C818
          1B17D9F8 D2F23945
```

- Step 6: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = F47B437F 4B69F3F1 6DB6B2E4 8C5D75BA FA767110 CE81EEA4
             B4F2ECE4 DDC640A4 56146D87 4BAA18E7 6D45CD25 D1D8371A
             FF75DEAB B5847B08
```

- If key confirmation is performed, then

```
MacKey  =     F47B 437F4B69 F3F16DB6 B2E48C5D
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 AAB47C8F 476AF10C
            AD7B06FD 3BB61F39 B4BD4153 F2B60691 B3938BD8 43991C37
            7CDC21B1 92FB37A6 4D840452 38466C3C 41709A02 00B450AB
            318D0AE4 1D0C812C C00FC7AB 7F9E6E19 FC62CA88 0CDACFBA
            D078B1CF BC516CBA 47F6B581 92711621 2E8275EA 5308318A
            73150F44 328A661C

MacTag_U  = CBDF0E45 5042568C AE49F96B CA502CDA 46EB597E E5690B1F
             8004DCA7
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 318D0AE4 1D0C812C
            C00FC7AB 7F9E6E19 FC62CA88 0CDACFBA D078B1CF BC516CBA
            47F6B581 92711621 2E8275EA 5308318A 73150F44 328A661C
            AAB47C8F 476AF10C AD7B06FD 3BB61F39 B4BD4153 F2B60691
            B3938BD8 43991C37 7CDC21B1 92FB37A6 4D840452 38466C3C
            41709A02 00B450AB
```

```
MacTag_V  = 83DADDDB D2447816 1747F2B7 8B98D8A2 E928256A 5F8825E6
            CC6D9232
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 AAB47C8F 476AF10C
            AD7B06FD 3BB61F39 B4BD4153 F2B60691 B3938BD8 43991C37
            7CDC21B1 92FB37A6 4D840452 38466C3C 41709A02 00B450AB
            318D0AE4 1D0C812C C00FC7AB 7F9E6E19 FC62CA88 0CDACFBA
            D078B1CF BC516CBA 47F6B581 92711621 2E8275EA 5308318A
            73150F44 328A661C

MacTag_U  = B51AA873 BCC2C512 F7725847 29F57CDA A3282CE2 1096FDF5
            3F00E492

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 318D0AE4 1D0C812C
            C00FC7AB 7F9E6E19 FC62CA88 0CDACFBA D078B1CF BC516CBA
            47F6B581 92711621 2E8275EA 5308318A 73150F44 328A661C
            AAB47C8F 476AF10C AD7B06FD 3BB61F39 B4BD4153 F2B60691
            B3938BD8 43991C37 7CDC21B1 92FB37A6 4D840452 38466C3C
            41709A02 00B450AB

MacTag_V  = 3482768F B038C2FE 836BF545 81929615 6C76AED0 63434949
            DAADB9CF
```

5.3.2 Full MQV for curve P–224

- Prerequisites:

```
dsU   =   AF95D66D 74889660 8E1EE256 AE111517 043AC496 9570F8D2
          889D2B04
```

```
x_QsU =   4F855D7D 4C9B7195 CC222620 5E37F49D 06057892 A8F1BFBB
          43A2E0FF

y_QsU =   5331D491 CEDB3641 6830A402 5330F6B5 6E83BE18 E3E11DB6
          EC15C150

dsV   =   08CCA216 8DF41B3C 3AE997F9 A80F5E46 8F449B48 EA25DB1A
          8A6A6363

x_QsV =   42050DF6 59BAA66E E4002094 815282BD 981A4522 5214D5C0
          3EA70299

y_QsV =   75732ED9 F96F82F5 C3897C29 8A924964 88FDD1D2 12808622
          77925E67
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   E364F545 4CFD3B9D 698E328A 3D329180 ED0D3A1F 080BE416
          49890CDF

x_QeU =   DFB53B06 2E4A62E0 98D8408B 66E34140 358952CD FD5B1115
          C8FDC2CB

y_QeU =   B1CAF002 30B94666 96AB6783 D36CCD56 AD00202C 4C61C022
          1A034064

deV   =   FF144C1B 3E0BEDD9 BD769519 5C7F28E8 D530A517 B05CDF01
          D0C275FB

x_QeV =   85159070 64D7F5D3 0796127E 34A17C1E 1E700019 DC9589D9
          48C17C77

y_QeV =   1DD55746 F7515944 84C920C6 5BC59961 661FA5FE 03EFAEA1
          1FFD3CD4
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =        1620444093107767566634275358073411091272964924849 0
           350815535214247870
```

- Step 4: Shared secret converted to byte string.

```
Z =        99DED059 2C1EECB1 1AB0ACF1 8DADC250 8EF93B37 21A936FA
           BF8A3FBE
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 67A11495 5C728E09 0BEB707B 7C1EADFF 08033850 B56C12F1
             7FDE6EB5 AED2439C 741334CD CE2A4144 F5DB30A8 53D20621
             C20030A2 44A3E141
```

- If key confirmation is performed, then

```
MacKey  =     67A1 14955C72 8E090BEB 707B7C1E
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 DFB53B06 2E4A62E0
            98D8408B 66E34140 358952CD FD5B1115 C8FDC2CB B1CAF002
            30B94666 96AB6783 D36CCD56 AD00202C 4C61C022 1A034064
            85159070 64D7F5D3 0796127E 34A17C1E 1E700019 DC9589D9
            48C17C77 1DD55746 F7515944 84C920C6 5BC59961 661FA5FE
            03EFAEA1 1FFD3CD4

MacTag_U  = 23813E0F EFA9B8E6 77CAEFD3 412CAA41 E5474841 5DADEC29
            AEA7BC93
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 85159070 64D7F5D3
            0796127E 34A17C1E 1E700019 DC9589D9 48C17C77 1DD55746
            F7515944 84C920C6 5BC59961 661FA5FE 03EFAEA1 1FFD3CD4
            DFB53B06 2E4A62E0 98D8408B 66E34140 358952CD FD5B1115
            C8FDC2CB B1CAF002 30B94666 96AB6783 D36CCD56 AD00202C
            4C61C022 1A034064

 MacTag_V  = D3C31D9D 57B6BAFA F708F162 180006BF C95D87E9 2F9375A2
             6EDF70FA
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 DFB53B06 2E4A62E0
             98D8408B 66E34140 358952CD FD5B1115 C8FDC2CB B1CAF002
             30B94666 96AB6783 D36CCD56 AD00202C 4C61C022 1A034064
             85159070 64D7F5D3 0796127E 34A17C1E 1E700019 DC9589D9
             48C17C77 1DD55746 F7515944 84C920C6 5BC59961 661FA5FE
             03EFAEA1 1FFD3CD4

 MacTag_U  = 026BC183 DAAC2178 FC1DEA58 1E56CC71 FB05FFD9 5C786062
             050026FB

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

           = 4B435F32 5F56424F 42425941 4C494345 85159070 64D7F5D3
             0796127E 34A17C1E 1E700019 DC9589D9 48C17C77 1DD55746
             F7515944 84C920C6 5BC59961 661FA5FE 03EFAEA1 1FFD3CD4
             DFB53B06 2E4A62E0 98D8408B 66E34140 358952CD FD5B1115
             C8FDC2CB B1CAF002 30B94666 96AB6783 D36CCD56 AD00202C
             4C61C022 1A034064

 MacTag_V  = D779406F C7AF164A EE0293B9 76B29C9A 02256922 20DB6001
             C23A6F22
```

5.3.3 Ephemeral Unified Model for curve P–224

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   E29A8727 74B90BB1 B2B3481D 0AF97A17 63B5F3E9 9E351D74
          E088EC57

x_QeU =   A1381358 7945B280 4F0E6CE2 9EE82F9D BFEFEEED D825DB43
          DF4BA829

y_QeU =   2E4A7E31 2ECEC157 368ADFFC 8BB1F94F 416AD252 00D0BB03
          3D99F78A

deV   =   F19F9E23 05AAB14E C43B4E78 0A71001F 35D0D2C0 AA0AE4E4
          DF3CCCB0

x_QeV =   60DBF3D7 5953812D 5A4460E8 FA2C7F5E 9F0AD36E 26B71434
          5F696372

y_QeV =   F5E6427F 46CF17D9 2C5C014E 56771FF3 CF9369D9 49476058
          2BF67824
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       50536439188148753161280880991099858203711795317198
          12947464819080464
```

- Step 4:

```
Z =       2FFCBA54 E17A0BBC 0558A6A9 38333F74 12190661 D94ECAF4
          30547D10
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = FB2A4D3B 7E1CA13F BB6A55BE 273DD68D 3D4518EB 2D950268
             CDB2D0AF 17C8864A 879A7353 6B6DBE78 65F301BE 8A28D7CD
             5E073464 3882F04D
```

5.3.4 One–Pass Unified Model for curve P–224

- Prerequisites:

```
dsU   =   45966353 D660C94B EE247E1A 222A47F8 00EB0061 AFC72A80
          CBAF1768

x_QsU =   A8C6FFEE 9D1822BD 7EAF4508 88288C4D 7775BB54 7AAB2755
          CCF3AD75

y_QsU =   AE63C1A7 30743D5B 90E70AEA 921D59D2 A14ABECA A0F72CD9
          9E408677

dsV   =   601EC855 122BA3C3 E109B495 837867CB 82787F74 B849D176
          603FBEDD

x_QsV =   4954484D 85A51779 3CC756F5 C4F119A5 5A337229 99115971
          44742DAD

y_QsV =   44C6B49C 08647F63 BDF6F5C0 16AE26C8 71000086 3C59712C
          9FD4B38F
```

BEGIN U's calculations

- Step 1:

```
deU   =   39B4497C 3BA30558 C1EE3915 4947CB22 FA422932 449CE3BA
          8A1C23C8

x_QeU =   04553035 0A71D31F 2F5FA71F 234A105B 8BFDC7E8 CB03E67C
          B2DA3261

y_QeU =   C7285E06 A75C5B40 0BEC6CAF FF770AA6 BEA8E77D E842D1AD
          02A9D865
```

- Step 2: Decimal and hex values for static shared secret.

```
Z_s =     1773757003823366334513308354607697873401166645720 7
          083809654942982957

Z_s =     A86DA4EF 1B049CDA 80F5024F 08CD1D5F 9475DCB2 56B40A58
          FF1BE32D
```

- Step 3: Decimal and hex values for ephemeral shared secret.

```
Z_e =     1858112209173367250129219278387918391527075712907 1
          534744453398941304

Z_e =     B07034AA 69195123 2D9D865E 21ABE0A3 0E0C2FDF E2E9EC8A
          66D04E78
```

- Step 4: Shared secret.

```
Z =       B07034AA 69195123 2D9D865E 21ABE0A3 0E0C2FDF E2E9EC8A
          66D04E78 A86DA4EF 1B049CDA 80F5024F 08CD1D5F 9475DCB2
          56B40A58 FF1BE32D
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 98326061 561526C0 05F9558C 36B39760 97D8C248 AACA9D6A
             21736732 9CAA569D 0B5908BA 9ACDFAF4 49EFA6CE AF8D3650
             D74F5BCE 42950A70
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   39B4497C 3BA30558 C1EE3915 4947CB22 FA422932 449CE3BA
          8A1C23C8
```

```
x_QeU =   04553035 0A71D31F 2F5FA71F 234A105B 8BFDC7E8 CB03E67C
          B2DA3261

y_QeU =   C7285E06 A75C5B40 0BEC6CAF FF770AA6 BEA8E77D E842D1AD
          02A9D865
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     177375700382336633451330835460769787340116664572070
          83809654942982957

Z_s =     A86DA4EF 1B049CDA 80F5024F 08CD1D5F 9475DCB2 56B40A58
          FF1BE32D
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     185811220917336725012921927838791839152707571290715
          34744453398941304

Z_e =     B07034AA 69195123 2D9D865E 21ABE0A3 0E0C2FDF E2E9EC8A
          66D04E78
```

- Step 5: Shared secret.

```
Z =       B07034AA 69195123 2D9D865E 21ABE0A3 0E0C2FDF E2E9EC8A
          66D04E78 A86DA4EF 1B049CDA 80F5024F 08CD1D5F 9475DCB2
          56B40A58 FF1BE32D
```

- Step 6: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 98326061 561526C0 05F9558C 36B39760 97D8C248 AACA9D6A
             21736732 9CAA569D 0B5908BA 9ACDFAF4 49EFA6CE AF8D3650
             D74F5BCE 42950A70
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     9832 60615615 26C005F9 558C36B3

nonceV =  35F4D011 5748267D E253D105 C1B3C8E2 41617D6B 4A419BC8
          AD902513
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 04553035 0A71D31F
            2F5FA71F 234A105B 8BFDC7E8 CB03E67C B2DA3261 C7285E06
            A75C5B40 0BEC6CAF FF770AA6 BEA8E77D E842D1AD 02A9D865
            35F4D011 5748267D E253D105 C1B3C8E2 41617D6B 4A419BC8
            AD902513

 MacTag_U  = 281C0DFC 779FC1D8 66A4740C E4505642 0241495E DB92C55D
             1C5470E8
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 04553035 0A71D31F
            2F5FA71F 234A105B 8BFDC7E8 CB03E67C B2DA3261 C7285E06
            A75C5B40 0BEC6CAF FF770AA6 BEA8E77D E842D1AD 02A9D865

 MacTag_V  = 0B091615 21837B72 B5C848B5 678473A0 29456E46 A8F35534
             36DA9761
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
            = 4B435F32 5F55414C 49434542 4F424259 04553035 0A71D31F
              2F5FA71F 234A105B 8BFDC7E8 CB03E67C B2DA3261 C7285E06
              A75C5B40 0BEC6CAF FF770AA6 BEA8E77D E842D1AD 02A9D865
              35F4D011 5748267D E253D105 C1B3C8E2 41617D6B 4A419BC8
              AD902513

 MacTag_U  = 8884A9A1 FB9F21C6 1A3A4D4E 9883151A 03C446F3 B3327477
              9D37CEC6

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

            = 4B435F32 5F56424F 42425941 4C494345 35F4D011 5748267D
              E253D105 C1B3C8E2 41617D6B 4A419BC8 AD902513 04553035
              0A71D31F 2F5FA71F 234A105B 8BFDC7E8 CB03E67C B2DA3261
              C7285E06 A75C5B40 0BEC6CAF FF770AA6 BEA8E77D E842D1AD
              02A9D865

 MacTag_V  = 9CD3B33E 9D4D7A91 75291ED8 9001C001 01D59E12 9D13568E
              5A6C4950
```

5.3.5 One–Pass MQV for curve P–224

- Prerequisites:

```
dsU   =   23F00BDC 89F0D66D 96AB8915 C985BD38 F652EDFF DAB96CAA
          B2135AEB

x_QsU =   60E1E7AF 50B4C427 DDD7F681 DD2B2AA2 B400EE0E 0C45FA5C
          9DF9396E

y_QsU =   60688093 D48ECA01 103965CD 1EA75727 B1849DB0 2A679A52
          7CEF2EC0

dsV   =   712D8864 27B59B58 1EAF4430 7FD35E2B 55631F3B 202FE46C
          15E7B068
```

```
x_QsV =   C7ED6710 755214AF 513821C1 77DA95F5 86B152F3 2D502039
          454477AD

y_QsV =   38E3B318 888D7171 E911041A 3640AF89 B548D4DF 3A5D4CAA
          1D067008
```

BEGIN U's calculations

- Step 1:

```
deU   =   7569DAF0 B7EDD1E1 563FAE38 BD0EA19F 627040A6 73F9687A
          804257F9

x_QeU =   273B43E2 C1307A9F BAD8FA72 561A6CA2 F3FAB040 64A2D0A5
          57BD6D08

y_QeU =   162A5DDA 1917DC37 FEA6817E B8A5BA50 BA935A75 E2181167
          F0DE60BE
```

- Step 2: Decimal value for shared secret.

```
Z =       98439427878922119631210434122830878766436505437480
          92603170181338186
```

- Step 3: Hex value for shared secret.

```
Z =       5D794CA2 E777D815 B37BA38D 2D19C60F 44223648 C3A2DCB6
          874BD44A
```

- Step 4: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = C05482B0 0252C66C 0CACED99 D7D5B8D1 004FB70B 9F91571C
             5F899481 3CEE62DB B8E20DF6 0D44CF20 C090C897 75F8C23F
             9B12614C B85C1828
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   7569DAF0 B7EDD1E1 563FAE38 BD0EA19F 627040A6 73F9687A
          804257F9

x_QeU =   273B43E2 C1307A9F BAD8FA72 561A6CA2 F3FAB040 64A2D0A5
          57BD6D08

y_QeU =   162A5DDA 1917DC37 FEA6817E B8A5BA50 BA935A75 E2181167
          F0DE60BE
```

- Step 2: N/A.
- Step 3: Decimal value for shared secret.

```
Z =       98439427878922119631210434122830878766436505437480
          92603170181338186
```

- Step 4: Hex value for shared secret.

```
Z =       5D794CA2 E777D815 B37BA38D 2D19C60F 44223648 C3A2DCB6
          874BD44A
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = C05482B0 0252C66C 0CACED99 D7D5B8D1 004FB70B 9F91571C
             5F899481 3CEE62DB B8E20DF6 0D44CF20 C090C897 75F8C23F
             9B12614C B85C1828
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     C054 82B00252 C66C0CAC ED99D7D5

nonceV =  FFC7D160 1EC31635 5448A5EB 5955ADD6 B6D88298 E1AA0BBA
          99E83F55
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 273B43E2 C1307A9F
            BAD8FA72 561A6CA2 F3FAB040 64A2D0A5 57BD6D08 162A5DDA
            1917DC37 FEA6817E B8A5BA50 BA935A75 E2181167 F0DE60BE
            FFC7D160 1EC31635 5448A5EB 5955ADD6 B6D88298 E1AA0BBA
            99E83F55

MacTag_U  = 1EB745FF 43EE9E04 F4E04C9D 7162F48D CFADFF92 FBDAB98E
            BFCC5F0C
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 273B43E2 C1307A9F
            BAD8FA72 561A6CA2 F3FAB040 64A2D0A5 57BD6D08 162A5DDA
            1917DC37 FEA6817E B8A5BA50 BA935A75 E2181167 F0DE60BE

MacTag_V  = 7AF6E042 8E08AB43 382CFF98 163A1C50 DA30A86B 33110731
            DB456DF5
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 273B43E2 C1307A9F
            BAD8FA72 561A6CA2 F3FAB040 64A2D0A5 57BD6D08 162A5DDA
            1917DC37 FEA6817E B8A5BA50 BA935A75 E2181167 F0DE60BE
            FFC7D160 1EC31635 5448A5EB 5955ADD6 B6D88298 E1AA0BBA
            99E83F55
```

```
MacTag_U  = F1EB01B4 2DB6210A 03418A80 B87A289A 7900FEE7 2913AA10
            CE8808AB

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 FFC7D160 1EC31635
            5448A5EB 5955ADD6 B6D88298 E1AA0BBA 99E83F55 273B43E2
            C1307A9F BAD8FA72 561A6CA2 F3FAB040 64A2D0A5 57BD6D08
            162A5DDA 1917DC37 FEA6817E B8A5BA50 BA935A75 E2181167
            F0DE60BE

MacTag_V  = 9CBD6142 1BE24826 6135B46C 7CED9A15 6B354091 2AC82A14
            5F430054
```

5.3.6 One–Pass Diffie–Hellman for curve P–224

- Prerequisites:

```
dsV   =   2B2D4A60 A45A4231 B60F4CEF 94CF5B51 6B73B1A5 6107C6B2
          E7C57A63

x_QsV =   12E12DFE 79E5853B 9CE0C229 A60E4A40 E7C702DE EA84BD5E
          47E61513

y_QsV =   C002D7A1 8E1C2DBA 27090D2E F6D5B51D 4CF80767 2BE31BE1
          ADB5E259
```

BEGIN U's calculations

- Step 1:

```
deU   =   A7F2FCE8 F3852AA1 B1A4DB4D 50D91291 A6E8FEDD 1A0F2B16
          F283243E

x_QeU =   22F4FA90 3AE5335E FBC3366C 2302AD2C A41BFB20 FAE0F848
          3CD5C98B
```

```
y_QeU =   F77B5599 4CEC2456 D5D26070 A2B08ABC 696B3095 886B1D73
          0951CC60
```

- Step 2: Decimal value for shared secret.

```
Z =       62772831301412744196829569762161351707181909863877
          71800652066407309
```

- Step 3: Hex value for shared secret.

```
Z =       3B9B3AE1 DA0431C1 EE74C0ED A3B625C7 A231848C 571AEAD0
          C641438D
```

- Step 4: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 260E21CD 195652CE A3EA2DE1 D3F6463E F633A9EA 477A8257
             3629F9CF EC5EAB4A 2E63C963 A4F99550 98A3DD6E 4B62FC0D
             9CC5EC7B C144BF8D
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   A7F2FCE8 F3852AA1 B1A4DB4D 50D91291 A6E8FEDD 1A0F2B16
          F283243E

x_QeU =   22F4FA90 3AE5335E FBC3366C 2302AD2C A41BFB20 FAE0F848
          3CD5C98B

y_QeU =   F77B5599 4CEC2456 D5D26070 A2B08ABC 696B3095 886B1D73
          0951CC60
```

- Step 2: N/A.

- Step 3: Decimal value for shared secret.

```
Z =        627728313014127441968295697621613517071819098638777
           71800652066407309
```

- Step 4: Hex value for shared secret.

```
Z =        3B9B3AE1 DA0431C1 EE74C0ED A3B625C7 A231848C 571AEAD0
           C641438D
```

- Step 5: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 260E21CD 195652CE A3EA2DE1 D3F6463E F633A9EA 477A8257
             3629F9CF EC5EAB4A 2E63C963 A4F99550 98A3DD6E 4B62FC0D
             9CC5EC7B C144BF8D
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     260E 21CD1956 52CEA3EA 2DE1D3F6
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 22F4FA90 3AE5335E
            FBC3366C 2302AD2C A41BFB20 FAE0F848 3CD5C98B F77B5599
            4CEC2456 D5D26070 A2B08ABC 696B3095 886B1D73 0951CC60

MacTag_V  = F3CA4D3F 396AD5AA 2D9F0EAC 7892C4E7 5511754A C77BD652
             BAFC2974
```

5.3.7 Static Unified Model for curve P–224

- Prerequisites:

```
dsU   =   EE01155E 28618041 ADFA1F5A 2AC70DAB 102C4237 76878689
          A2D1F0F1

x_QsU =   4DD0EAD7 3B3AD292 B5508F44 E6BDA1A5 76E4E95D FD5326FE
          5EF759F3

y_QsU =   B07F8563 F6768F83 340E7E3C 84893417 0FC96B54 5EB56575
          6A5B5AF2

dsV   =   779CB8D3 31A40F5A 80F6B7AC 439D8FEB 98633BA2 25ED616A
          09A845EC

x_QsV =   8BBE6EF4 88B0832F 2FF2F588 230FF3D5 4EACC051 3E2D8B84
          3AA303F5

y_QsV =   6D091D37 D88D2CC7 E71E13B3 9C0EE669 20888E09 C365AE35
          0AB74108
```

BEGIN U's calculations

- Step 1:

```
nonceU =  98A188FD 5BA6ACB1 3A956536 66D404BD 3DE5430A 40519CD7
          BB2BFA3F
```

- Step 2: Decimal value for shared secret.

```
Z =       24921255708857780547714383557103657827979977430964
          619937859268322827
```

- Step 3: Hex value for shared secret.

```
Z =       ECA43780 81257587 91B67DDD AD10CDE0 8961153D 6D959D36
          7AD1260B
```

- Step 4: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 0000001C 98A188FD
             5BA6ACB1 3A956536 66D404BD 3DE5430A 40519CD7 BB2BFA3F
             424F4242 59343536

DerKeyMat  = E2B820E6 E5D0E2D4 5E7FFABE FBAABC01 9EF979D6 8742380C
             72071CC8 FCF543DE 98EC6509 9213BC1B CDD1D619 F98AC01A
             3AD314AB 02D0B507
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
nonceU =  98A188FD 5BA6ACB1 3A956536 66D404BD 3DE5430A 40519CD7
          BB2BFA3F
```

- Step 2: Decimal value for shared secret.

```
Z =       24921255708857780547714383557103657827979977430964
          619937859268322827
```

- Step 3: Hex value for shared secret.

```
Z =       ECA43780 81257587 91B67DDD AD10CDE0 8961153D 6D959D36
          7AD1260B
```

- Step 4: Additional inputs into the key derivation function and two blocks (448 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 0000001C 98A188FD
             5BA6ACB1 3A956536 66D404BD 3DE5430A 40519CD7 BB2BFA3F
             424F4242 59343536

DerKeyMat  = E2B820E6 E5D0E2D4 5E7FFABE FBAABC01 9EF979D6 8742380C
             72071CC8 FCF543DE 98EC6509 9213BC1B CDD1D619 F98AC01A
             3AD314AB 02D0B507
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =     E2B8 20E6E5D0 E2D45E7F FABEFBAA

nonceV =  34DE70BE FBEB3B51 8BF4C61B CB4CF34C 5D8448F8 776929B6
          E1D15012
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 98A188FD 5BA6ACB1
            3A956536 66D404BD 3DE5430A 40519CD7 BB2BFA3F 34DE70BE
            FBEB3B51 8BF4C61B CB4CF34C 5D8448F8 776929B6 E1D15012

MacTag_U  = D3E61CA2 1557D702 4569105A 4AF5A967 575F65B0 30BC1702
            6D80F1CD
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 98A188FD 5BA6ACB1
            3A956536 66D404BD 3DE5430A 40519CD7 BB2BFA3F

MacTag_V  = D5F21F98 A31617EE 81B62CF7 8B2DA4FE 07EF42B4 660EB489
            9B29AB4F
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 98A188FD 5BA6ACB1
             3A956536 66D404BD 3DE5430A 40519CD7 BB2BFA3F 34DE70BE
             FBEB3B51 8BF4C61B CB4CF34C 5D8448F8 776929B6 E1D15012
```

```
MacTag_U  = 2C8A9970 5A709EEF F51A2CE8 3984134F DF820E69 13778657
            97909DD9

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 34DE70BE FBEB3B51
            8BF4C61B CB4CF34C 5D8448F8 776929B6 E1D15012 98A188FD
            5BA6ACB1 3A956536 66D404BD 3DE5430A 40519CD7 BB2BFA3F

MacTag_V  = 2ECBC45B 87E6BAEF A8207319 3396DEB0 3A997B52 E3161134
            2C06EA7A
```

5.4 Test data for P–256

In this section, we supply step–by–step test data for the seven elliptic curve key agreement schemes described in [1, section 6] using the parameter set P–256 described in Appendix 4.3. For each scheme, a reference to the corresponding section in [1] is provided.

5.4.1 Full Unified Model for curve P–256

- Prerequisites:

```
dsU   =   524BF7FA 3DC5D9C9 5BB66904 438234B1 3DB2D8A0 73DE70F3
          0237D349 A8F23742

x_QsU =   D01F6500 3F81E696 444F5A4F 4A82AF8B BF30347B 9350C50F
          C5C76D58 D7CE63B1

y_QsU =   21A7CB58 F4689D08 C5E1EBFC 01293518 42C4F964 C0099B5E
          02D8AEA2 8128BAAD

dsV   =   999B3109 5B492C5C 440D2090 5B71E879 526439F3 942401AE
          1D6439DC 3EA8FE5C
```

```
x_QsV =   C03F4D85 7F887187 65C19039 78AE3F04 8C90A435 18FC3CF1
          FD711FE7 4A80C6F7

y_QsV =   60C98597 AC72EA9E 08EE5AAC A6870D06 F51262CE DEAD91A7
          2E93B926 CD9556D9
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   64C53286 75DCE204 DB5C16DB 7ADE80A6 5F998CD3 BC7FC863
          E5C76B90 951BEFC7

x_QeU =   2B96B926 FBFD4C20 A8757D18 70510977 41B6A0D6 976C4D8E
          3999B6C6 3A7C7E07

y_QeU =   6499F066 9CDD94E6 84E3DE32 89A20B21 3EFE43A8 009915FE
          F075CB33 DF645AAE

deV   =   F2C517EF 20B549FA 40237B50 FF6A32CC 3F113107 C3D50DF5
          204E6BCD E0362956

x_QeV =   6CDA0277 DC21E115 8D0C6B0A 27E8A2D6 624443A9 88D0D660
          8861C964 58C7932C

y_QeV =   FB3E8562 D093FD3C 80CAD34A 266A8357 EC1185F6 25209A9D
          769F15DA DE15D901
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     48233922230921383999031786285860919173752342739769
          954922017575945032173799804

Z_s =     6AA36EBA 1B6C71A7 87BA27C0 D8D94BB3 9B957C2E E5595086
          2EA82618 18C2C97C
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     99240730241083626431573184491304291250599253356939
          76120830971166370713549117

Z_e =     15F0D387 0249CC52 5F0A85F5 A2EED7A7 E73115CC 14D286C3
          E5280695 D967B93D
```

- Step 5: Shared secret.

```
Z =       15F0D387 0249CC52 5F0A85F5 A2EED7A7 E73115CC 14D286C3
          E5280695 D967B93D 6AA36EBA 1B6C71A7 87BA27C0 D8D94BB3
          9B957C2E E5595086 2EA82618 18C2C97C
```

- Step 6: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 64A32433 7E4AFEDA 85912D3D 341335CD C775BB3D 54BD31E7
             4B6E1C2E 5FF88FD0 625FA078 9E15A2D2 7B89DD05 D25B484D
             8FDC1A7A 1C0D0586 2C51FCC7 1632F8E9
```

- If key confirmation is performed, then

```
MacKey  = 64A32433 7E4AFEDA 85912D3D 341335CD
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 2B96B926 FBFD4C20
            A8757D18 70510977 41B6A0D6 976C4D8E 3999B6C6 3A7C7E07
            6499F066 9CDD94E6 84E3DE32 89A20B21 3EFE43A8 009915FE
            F075CB33 DF645AAE 6CDA0277 DC21E115 8D0C6B0A 27E8A2D6
            624443A9 88D0D660 8861C964 58C7932C FB3E8562 D093FD3C
            80CAD34A 266A8357 EC1185F6 25209A9D 769F15DA DE15D901
```

```
MacTag_U  = E4077A63 037C24E3 4D971496 BBC96DD3 F12D34D6 4EAF5EBE
            AE861C4A CA018790
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 6CDA0277 DC21E115
            8D0C6B0A 27E8A2D6 624443A9 88D0D660 8861C964 58C7932C
            FB3E8562 D093FD3C 80CAD34A 266A8357 EC1185F6 25209A9D
            769F15DA DE15D901 2B96B926 FBFD4C20 A8757D18 70510977
            41B6A0D6 976C4D8E 3999B6C6 3A7C7E07 6499F066 9CDD94E6
            84E3DE32 89A20B21 3EFE43A8 009915FE F075CB33 DF645AAE

MacTag_V  = BAE0625A 63CE0E56 67320B2F 72434F6A 686C8C0E A765C188
            9E883960 337A4394
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 2B96B926 FBFD4C20
            A8757D18 70510977 41B6A0D6 976C4D8E 3999B6C6 3A7C7E07
            6499F066 9CDD94E6 84E3DE32 89A20B21 3EFE43A8 009915FE
            F075CB33 DF645AAE 6CDA0277 DC21E115 8D0C6B0A 27E8A2D6
            624443A9 88D0D660 8861C964 58C7932C FB3E8562 D093FD3C
            80CAD34A 266A8357 EC1185F6 25209A9D 769F15DA DE15D901

MacTag_U  = AD0DA534 9811E26C D703DD47 511ED205 D5EDFDC4 756250C3
            F77D3892 2FC43BA8

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 6CDA0277 DC21E115
            8D0C6B0A 27E8A2D6 624443A9 88D0D660 8861C964 58C7932C
            FB3E8562 D093FD3C 80CAD34A 266A8357 EC1185F6 25209A9D
            769F15DA DE15D901 2B96B926 FBFD4C20 A8757D18 70510977
            41B6A0D6 976C4D8E 3999B6C6 3A7C7E07 6499F066 9CDD94E6
            84E3DE32 89A20B21 3EFE43A8 009915FE F075CB33 DF645AAE

MacTag_V  = 01EACBD4 BDCE8317 0951355B 8C12FE56 1DBA83BD 0422E301
            BFC58387 A02A058D
```

5.4.2 Full MQV for curve P–256

- Prerequisites:

```
dsU   =   BB590B02 D7DCD476 85AFC945 F3444CA3 542004D0 26762AFB
          D2847F88 C0A82914

x_QsU =   7BADEDD0 87811170 9E90C47E B2478520 F9D44088 9EA34E7E
          67BA8AAC E19654E7

y_QsU =   D9D22DCB 0560F232 B2F0FB9F 8625808B B7E704CE 3A727547
          EF9DE595 7BB5061A

dsV   =   53F535BA 75C1A3D0 3DE4B101 5046F3C5 6BC9E3B0 426B6C1F
          784F7CE6 F4A27CA2

x_QsV =   91556C37 1CE5CAF4 43CED96F 6F253988 EC320F92 6684270C
          03819A26 ACF1E62D

y_QsV =   3550FDBA D742DC1B C8A6A1B0 17A7ADCC 854C0136 FCCA2360
          87DB5523 CFE0B0D5
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   9CA7816F A4E94847 06181F88 6F9FF641 403E67C7 5CF2FBFC
          CB0051D7 0F3CB4CC

x_QeU =   66BC9854 6D7A249D EBB20A35 30EB0976 0A8B1DC5 22710B73
          8F5E15DF AAB2FC94

y_QeU =   A0EBFC3E 69DF85F8 02DCFDB3 862E43CC 214C1DD9 21D4F799
          0023399A 95BFDA46

deV   =   5A1E004F 753CFDD9 768BEE4B D6604E5F A1FAC9A2 AD61C42C
          8F5A3213 2110671A
```

```
x_QeV =   4EAB9479 78BD31F4 A14AA8E2 F5534CF1 668A6A74 5E6E2822
          F2CBB701 3305215D

y_QeV =   13D65687 F63CA434 B4BD6D5B 0AB47BA7 F992F9B2 064149CA
          ADA6CD5C 104D3B83
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       84877792093116323158375381820546558593610684367227
          89600828749812741044838123 4
```

- Step 4: Shared secret converted to byte string.

```
Z =       BBA720BC E2B3913B C239D611 E1910FA0 919F7507 29837E97
          5B05D7B4 2EC53532
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 7B2160FE 7CE57DBC 71B2A711 EE032550 FB908346 AFFCE4B7
             E9B45948 711C135D B276B759 19E7C830 E193E69B 1848F5E3
             2F604A1C 5033758D 4270B94C 0569269A
```

- If key confirmation is performed, then

```
MacKey  = 7B2160FE 7CE57DBC 71B2A711 EE032550
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
          = 4B435F31 5F55414C 49434542 4F424259 66BC9854 6D7A249D
            EBB20A35 30EB0976 0A8B1DC5 22710B73 8F5E15DF AAB2FC94
            A0EBFC3E 69DF85F8 02DCFDB3 862E43CC 214C1DD9 21D4F799
            0023399A 95BFDA46 4EAB9479 78BD31F4 A14AA8E2 F5534CF1
            668A6A74 5E6E2822 F2CBB701 3305215D 13D65687 F63CA434
            B4BD6D5B 0AB47BA7 F992F9B2 064149CA ADA6CD5C 104D3B83

MacTag_U  = AF5A995A E7304364 6842FE39 48338B4B 062366B6 DB9F7E53
            B2743BDE E6175BC5
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 4EAB9479 78BD31F4
            A14AA8E2 F5534CF1 668A6A74 5E6E2822 F2CBB701 3305215D
            13D65687 F63CA434 B4BD6D5B 0AB47BA7 F992F9B2 064149CA
            ADA6CD5C 104D3B83 66BC9854 6D7A249D EBB20A35 30EB0976
            0A8B1DC5 22710B73 8F5E15DF AAB2FC94 A0EBFC3E 69DF85F8
            02DCFDB3 862E43CC 214C1DD9 21D4F799 0023399A 95BFDA46

MacTag_V  = 3BC9059C D687F4C9 55F27847 6FFCF737 70EDFC57 BF7ED48E
            66C4EC8B 90BACB51
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 66BC9854 6D7A249D
             EBB20A35 30EB0976 0A8B1DC5 22710B73 8F5E15DF AAB2FC94
             A0EBFC3E 69DF85F8 02DCFDB3 862E43CC 214C1DD9 21D4F799
             0023399A 95BFDA46 4EAB9479 78BD31F4 A14AA8E2 F5534CF1
             668A6A74 5E6E2822 F2CBB701 3305215D 13D65687 F63CA434
             B4BD6D5B 0AB47BA7 F992F9B2 064149CA ADA6CD5C 104D3B83

MacTag_U  = CE94668D 9C26DF67 9A5CCC39 C05561CC 7F752D70 9C7C6317
            360A8DA6 4FAFAB15
```

```
MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 4EAB9479 78BD31F4
            A14AA8E2 F5534CF1 668A6A74 5E6E2822 F2CBB701 3305215D
            13D65687 F63CA434 B4BD6D5B 0AB47BA7 F992F9B2 064149CA
            ADA6CD5C 104D3B83 66BC9854 6D7A249D EBB20A35 30EB0976
            0A8B1DC5 22710B73 8F5E15DF AAB2FC94 A0EBFC3E 69DF85F8
            02DCFDB3 862E43CC 214C1DD9 21D4F799 0023399A 95BFDA46

MacTag_V  = F20D6304 18D0081E BF4A1747 BAE3B182 F32A3CCC E92C19F5
            8172AAA3 7B5E1C9C
```

5.4.3 Ephemeral Unified Model for curve P–256

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   1FBBB87A 02D939E4 251240F7 0B0AF36C 3AA04D03 85073D84
          6523DF77 86FFE2D0

x_QeU =   FF3844D5 13C5C874 95A92B9F 951BA3DF 34731221 6E8050DA
          07AC6A3A 6D803888

y_QeU =   ABA4F2B4 C3F4A7A0 4FF05D7F E3F07B16 6714D40D 9A045310
          CEC279D0 0BD1B691

deV   =   E204CAC1 DAB2FC4C AC396277 042D6312 8D5A5E33 5317C50F
          15CDB32C 613521E1

x_QeV =   47E05358 CF21FE52 1D36AA13 014A3043 5D6A8C75 B04B563C
          B3C90B22 9D5D88B5

y_QeV =   C15DA098 A84DC449 38BD2BD1 8F6827E3 56A4B178 D872EDB4
          E6805DDA 812FEADA
```

- Step 2: N/A.

- Step 3: Decimal value of shared secret.

```
Z =       25345118707014300900517037727481648141699552488381
          36773796378235095762572450 7
```

- Step 4:

```
Z =       3808D42D FAC73E09 0645CCD6 4E455F93 B93E6C0B B1F561DF
          14A3311A B5C3CE5B
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 6BC72361 2238E355 68521319 36C5BCF8 8F25B5F7 7054049E
             A39CECD1 07364E67 C2D5769A FF54E95A C7C33E59 F0846CA6
             2D7A475E 43D30721 8308B3A0 E85B9866
```

5.4.4 One–Pass Unified Model for curve P–256

- Prerequisites:

```
dsU   =   D40668B7 8033D3B2 112D54EE D877016E 03346C65 9947458F
          F639E557 6EAF5604

x_QsU =   D5157B6A 846E1508 5ED7669C A98E4DFC 4A9CCB27 FF39432E
          B3AAD656 75F4806D

y_QsU =   66E3F391 42FF822C 412DC7BD 6A2A615B A3F26CE1 5F1796AE
          A2FDC0C9 A8C5081D

dsV   =   74A7E3D3 15B8D8D7 6D1B05C7 B7F95AE7 DFED3510 BDC56F7F
          B42D73DD 0E74EC44
```

```
x_QsV =   92F09106 6BB64084 13FC2C5A CD018E4A ACF395E1 2C45F774
          5FD9AEB3 9190C61D

y_QsV =   971BA900 C5C16E2B 4C03B5AE D7571D65 9A869ECA C9146F44
          95A8F2D8 3B697712
```

BEGIN U's calculations

- Step 1:

```
deU   =   C4C80573 73AA42EB CE00C970 66FACD0B D60E8F87 71137A1B
          9FF38FCB C458EA52

x_QeU =   86107CC3 DFCE1EDF 945BA50E C71A938D 4D398C0E 2F6B888A
          A912136E D45DBB85

y_QeU =   95CB3C25 37B3E516 CEAC3714 62B55E45 9305F985 549B608A
          4234891A 3358DAED
```

- Step 2: Decimal and hex values for static shared secret.

```
Z_s =     105895600156577276621163626056373634893505554823801
          97401881811445180164677544

Z_s =     17697A83 6E779705 FF239B8E 4F8AA4C8 3C70776B CB9F08B0
          0E3C45AC 232F1FA8
```

- Step 3: Decimal and hex values for ephemeral shared secret.

```
Z_e =     289974655526522577559861491221264770055736030004376
          28948498912617494121669099

Z_e =     401BFBDF D28BAD7C BF1325E7 9AC49D36 65546A14 E9466660
          E31889C3 95F5E1EB
```

- Step 4: Shared secret.

```
Z =       401BFBDF D28BAD7C BF1325E7 9AC49D36 65546A14 E9466660
          E31889C3 95F5E1EB 17697A83 6E779705 FF239B8E 4F8AA4C8
          3C70776B CB9F08B0 0E3C45AC 232F1FA8
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 2C8E8588 6BC627AF A236A773 447C32FF 21E28B16 C3D6A6C1
             36277E92 775810D8 BD04EC34 EA157CCB B193503C F5DAF6EA
             4B4FF8C2 33933CCF 81074CEA B65DD9ED
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   C4C80573 73AA42EB CE00C970 66FACD0B D60E8F87 71137A1B
          9FF38FCB C458EA52

x_QeU =   86107CC3 DFCE1EDF 945BA50E C71A938D 4D398C0E 2F6B888A
          A912136E D45DBB85

y_QeU =   95CB3C25 37B3E516 CEAC3714 62B55E45 9305F985 549B608A
          4234891A 3358DAED
```

- Step 2: N/A.

- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     105895600156577276621163626056373634893505554823801
          97401881811445180164677544

Z_s =     17697A83 6E779705 FF239B8E 4F8AA4C8 3C70776B CB9F08B0
          0E3C45AC 232F1FA8
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     28997465552652257755986149122126477005573603000437
          62894849891261749412166909 9

Z_e =     401BFBDF D28BAD7C BF1325E7 9AC49D36 65546A14 E9466660
          E31889C3 95F5E1EB
```

- Step 5: Shared secret.

```
Z =       401BFBDF D28BAD7C BF1325E7 9AC49D36 65546A14 E9466660
          E31889C3 95F5E1EB 17697A83 6E779705 FF239B8E 4F8AA4C8
          3C70776B CB9F08B0 0E3C45AC 232F1FA8
```

- Step 6: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 2C8E8588 6BC627AF A236A773 447C32FF 21E28B16 C3D6A6C1
             36277E92 775810D8 BD04EC34 EA157CCB B193503C F5DAF6EA
             4B4FF8C2 33933CCF 81074CEA B65DD9ED
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 2C8E8588 6BC627AF A236A773 447C32FF

nonceV =  0E938906 F2694781 C3FD49CE 2ED386F7 2DB3085A B701F1E8
          66916DEB 90FC885D
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
          = 4B435F31 5F55414C 49434542 4F424259 86107CC3 DFCE1EDF
            945BA50E C71A938D 4D398C0E 2F6B888A A912136E D45DBB85
            95CB3C25 37B3E516 CEAC3714 62B55E45 9305F985 549B608A
            4234891A 3358DAED 0E938906 F2694781 C3FD49CE 2ED386F7
            2DB3085A B701F1E8 66916DEB 90FC885D

 MacTag_U  = 1BEC83E8 97816C26 2F32D73E E852D0A7 D41F286E 484257AA
             E2BD4B30 A741C907
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 86107CC3 DFCE1EDF
            945BA50E C71A938D 4D398C0E 2F6B888A A912136E D45DBB85
            95CB3C25 37B3E516 CEAC3714 62B55E45 9305F985 549B608A
            4234891A 3358DAED

 MacTag_V  = 489C78BB D03F17A8 19A11A90 42ACA064 D77687CA C1851B10
             1A946411 4DF72E24
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 86107CC3 DFCE1EDF
             945BA50E C71A938D 4D398C0E 2F6B888A A912136E D45DBB85
             95CB3C25 37B3E516 CEAC3714 62B55E45 9305F985 549B608A
             4234891A 3358DAED 0E938906 F2694781 C3FD49CE 2ED386F7
             2DB3085A B701F1E8 66916DEB 90FC885D

 MacTag_U  = 82D8E2E3 F5C168A8 2D01A830 4DE4AC1A 651462C4 51CABE2E
             02E8AB01 658C4FE9

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U
```

```
            = 4B435F32 5F56424F 42425941 4C494345 0E938906 F2694781
              C3FD49CE 2ED386F7 2DB3085A B701F1E8 66916DEB 90FC885D
              86107CC3 DFCE1EDF 945BA50E C71A938D 4D398C0E 2F6B888A
              A912136E D45DBB85 95CB3C25 37B3E516 CEAC3714 62B55E45
              9305F985 549B608A 4234891A 3358DAED

MacTag_V    = 624D50B7 A961B88B D24BFC02 F999100B DBAAD8B0 FD4C0F1A
              C434932E D5E71453
```

5.4.5 One–Pass MQV for curve P–256

- Prerequisites:

```
dsU   =   12B48F70 74D9A2DC 75FE2466 2C1717C0 C7ABF6DE 66364BE4
          86162124 77EAC9FB

x_QsU =   A1A32D25 A07A284E FE4A3385 4C0FE015 AA446303 C0B3485C
          CF334C9B 26BCF7C6

y_QsU =   6C240B15 D192B1CD 4398CC1B 5986129C 12C2839B 2C32E5F7
          90020120 B065C7F3

dsV   =   DB3724C2 FB3F6C0A 6F33C275 88698B52 8AA63C99 A54EF2BE
          DD84237A 4EBFF84E

x_QsV =   05CCA980 91AC53C0 F7DAE5CA 06F572A9 9F2B916A 5203108D
          0EB98D56 2543FFC4

y_QsV =   75F6EA6F 850AB643 6E5B3D2D 6BD78713 DC263787 0C626168
          AD9A459C D5DB5C7C
```

BEGIN U's calculations

- Step 1:

```
deU   =   461639AE 6B24D25B A25C7273 54BE10D6 628547A2 F6907691
          61D8F6BE F593AE15

x_QeU =   F8085422 F378EB8F CD053F85 9F61281D 826FD567 71389C17
          24EEDE42 B183D817

y_QeU =   3363B5DC BFE193E1 10BE8951 3CC341C7 CB05CFA5 9BF22DAC
          C7857137 31B523B9
```

- Step 2: Decimal value for shared secret.

```
Z =       86343143781511317946364804926227559253513145168877
          63026859136201872343035617 8
```

- Step 3: Hex value for shared secret.

```
Z =       BEE47CCF D7383865 7FE66298 D776A9CD 44F96119 73B7EC44
          B74D2565 E17754D2
```

- Step 4: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 0FE1324B 1B17521F 6758D99C 6BD9DA13 C4FA75A5 B97A77CB
             EEF9F06B 7170292D 34DFED63 75842677 0F895AAD 2E4E0359
             8F11EB50 D1E98B5A 47FBA81A C6AEC41E
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   461639AE 6B24D25B A25C7273 54BE10D6 628547A2 F6907691
          61D8F6BE F593AE15

x_QeU =   F8085422 F378EB8F CD053F85 9F61281D 826FD567 71389C17
          24EEDE42 B183D817
```

```
y_QeU =   3363B5DC BFE193E1 10BE8951 3CC341C7 CB05CFA5 9BF22DAC
          C7857137 31B523B9
```

- Step 2: N/A.
- Step 3: Decimal value for shared secret.

```
Z =       86343143781511317946364804926227559253513145168877
          63026859136201872343035617 8
```

- Step 4: Hex value for shared secret.

```
Z =       BEE47CCF D7383865 7FE66298 D776A9CD 44F96119 73B7EC44
          B74D2565 E17754D2
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 0FE1324B 1B17521F 6758D99C 6BD9DA13 C4FA75A5 B97A77CB
             EEF9F06B 7170292D 34DFED63 75842677 0F895AAD 2E4E0359
             8F11EB50 D1E98B5A 47FBA81A C6AEC41E
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =  FE1324B 1B17521F 6758D99C 6BD9DA13

nonceV =  95B33AB0 66D67F2E 2A5715EB 9B195608 6F43E614 51412A8E
          56D84FC3 47410DD8
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
          = 4B435F31 5F55414C 49434542 4F424259 F8085422 F378EB8F
            CD053F85 9F61281D 826FD567 71389C17 24EEDE42 B183D817
            3363B5DC BFE193E1 10BE8951 3CC341C7 CB05CFA5 9BF22DAC
            C7857137 31B523B9 95B33AB0 66D67F2E 2A5715EB 9B195608
            6F43E614 51412A8E 56D84FC3 47410DD8

MacTag_U  = E63B85C1 EB14746D FC9E2FB1 75F50901 944DE05D 84125561
            F6851144 E9B58B2A
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 F8085422 F378EB8F
            CD053F85 9F61281D 826FD567 71389C17 24EEDE42 B183D817
            3363B5DC BFE193E1 10BE8951 3CC341C7 CB05CFA5 9BF22DAC
            C7857137 31B523B9

MacTag_V  = 84E623A1 8B8D1D69 5536ED6B CC8EF1F4 3F5B6CC0 D7DF0C2C
            F118E8D5 FE76A0D1
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 F8085422 F378EB8F
             CD053F85 9F61281D 826FD567 71389C17 24EEDE42 B183D817
             3363B5DC BFE193E1 10BE8951 3CC341C7 CB05CFA5 9BF22DAC
             C7857137 31B523B9 95B33AB0 66D67F2E 2A5715EB 9B195608
             6F43E614 51412A8E 56D84FC3 47410DD8

MacTag_U  = DDF68A24 F45D9EB3 AE886F32 BC8028FC 1AD5B245 B3CBC2BA
            81199EA4 D917ACF2

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U
```

```
            = 4B435F32 5F56424F 42425941 4C494345 95B33AB0 66D67F2E
              2A5715EB 9B195608 6F43E614 51412A8E 56D84FC3 47410DD8
              F8085422 F378EB8F CD053F85 9F61281D 826FD567 71389C17
              24EEDE42 B183D817 3363B5DC BFE193E1 10BE8951 3CC341C7
              CB05CFA5 9BF22DAC C7857137 31B523B9

MacTag_V    = E5226CB5 732D7151 0993F911 C2012C77 61131D33 1DFA2812
              7A8DD947 C2951B34
```

5.4.6 One–Pass Diffie–Hellman for curve P–256

- Prerequisites:

```
dsV   =   9582DED0 7427AD3D 66C45B15 67B22D55 02C2CC64 0294BD74
          648BCD53 152FAE00

x_QsV =   9577991E C1B310F6 CC861CF6 E809C81A D3C623C8 42B9930E
          15E46F01 0348C0AC

y_QsV =   06F381CB 99D47981 B6197BA3 C2C923EC 8F29E767 372F2F30
          B9EB2105 7504FADD
```

BEGIN U's calculations

- Step 1:

```
deU   =   B48B98EB 52CF9E33 65E6B8D1 F22348B4 1CE88326 38A63A48
          0C395F5D 31384949

x_QeU =   8E2B2782 2D45D4B6 4327F0D2 D7206507 1F4D2EB1 FC986907
          2C62AEA7 0F8BAEB9

y_QeU =   DC6AC01E A0C1B0EC 964D080F 9F1BB476 7802A9BE 51C2EA66
          43CF2F39 C3918E44
```

- Step 2: Decimal value for shared secret.

```
Z =        69085148781183159548104185209935800148175827618525
           58978295603387156780605987 0
```

- Step 3: Hex value for shared secret.

```
Z =        98BCCEFB CD9EA37F 0B9E9269 E30EA03D 33909CEF E48ACEAD
           B05EF9B5 CA40D55E
```

- Step 4: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 01847BFB 2E32735B 585BF79D B377474E 16ABB153 CF46ADF2
             6CC50AC3 7669D66F 8CF28284 1F22EDDC ADA75578 B75B7B5D
             B826B23A 04A3691B 9B9C4E4E 81191902
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =    B48B98EB 52CF9E33 65E6B8D1 F22348B4 1CE88326 38A63A48
           0C395F5D 31384949

x_QeU =    8E2B2782 2D45D4B6 4327F0D2 D7206507 1F4D2EB1 FC986907
           2C62AEA7 0F8BAEB9

y_QeU =    DC6AC01E A0C1B0EC 964D080F 9F1BB476 7802A9BE 51C2EA66
           43CF2F39 C3918E44
```

- Step 2: N/A.

- Step 3: Decimal value for shared secret.

```
Z =        69085148781183159548104185209935800148175827618525
           58978295603387156780605987 0
```

- Step 4: Hex value for shared secret.

```
Z =       98BCCEFB CD9EA37F 0B9E9269 E30EA03D 33909CEF E48ACEAD
          B05EF9B5 CA40D55E
```

- Step 5: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 01847BFB 2E32735B 585BF79D B377474E 16ABB153 CF46ADF2
             6CC50AC3 7669D66F 8CF28284 1F22EDDC ADA75578 B75B7B5D
             B826B23A 04A3691B 9B9C4E4E 81191902
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =  1847BFB 2E32735B 585BF79D B377474E
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 8E2B2782 2D45D4B6
            4327F0D2 D7206507 1F4D2EB1 FC986907 2C62AEA7 0F8BAEB9
            DC6AC01E A0C1B0EC 964D080F 9F1BB476 7802A9BE 51C2EA66
            43CF2F39 C3918E44

MacTag_V  = C0236B47 383E8C95 55495B03 A7B8F24F 29CC85B2 117FF26A
             A1346F35 9EFDA630
```

5.4.7 Static Unified Model for curve P–256

- Prerequisites:

```
dsU   =   ED8A617E 913E1E54 459137BC FA0B3513 2F504E6C E277272F
          59C9C3E7 6841A60A

x_QsU =   ABF6EC81 C19C6854 E647F95E F2C5EB51 511CD623 5701B91B
          40441142 2DDE19FA

y_QsU =   91E27A7B D6A0199B 99BFF28F CDBE973E 833B02CE BA4369FB
          4A02D479 2EE13DE0

dsV   =   5E727967 55A7BF7D 13DC3026 2AC1FAB9 0A20596E 3F78BE06
          1916292A D402E42F

x_QsV =   C43BC47B 6157E7C0 0E0F46E1 9AF9973C 5DC340BF C6A38B87
          BF528967 857A516C

y_QsV =   333B1EED 682B9A6D 398F389B 888F207B E7994406 E9F4CBDA
          A9276026 4BEF61BE
```

BEGIN U's calculations

- Step 1:

```
nonceU =  0B537E0F D59BA7A8 B31F1812 1706EB60 716C9EEB D216508B
          31340927 652D7C9E
```

- Step 2: Decimal value for shared secret.

```
Z =       38559001872467576884828443280021641947551650790688
          01200523366363905521516187 8
```

- Step 3: Hex value for shared secret.

```
Z =       553F9F25 18E51222 4BC66D5E 3A1718C2 980AC3DB 31D22B27
          2E1B589D A050F216
```

- Step 4: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000020 0B537E0F
             D59BA7A8 B31F1812 1706EB60 716C9EEB D216508B 31340927
             652D7C9E 424F4242 59343536

DerKeyMat  = 5E8CD9FE 5EA2CD45 D85D2302 423AD056 DE934601 5ABCC161
             6A0F5D6C 3F3B5A5B 4F5675B0 E8255937 CC37A7CC BFAD2FBE
             BD68591D 6D7FF097 61997CCF 7C7A33D7
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
nonceU =  0B537E0F D59BA7A8 B31F1812 1706EB60 716C9EEB D216508B
          31340927 652D7C9E
```

- Step 2: Decimal value for shared secret.

```
Z =       38559001872467576884828443280021641947551650790688
          01200523366363905521516187 8
```

- Step 3: Hex value for shared secret.

```
Z =       553F9F25 18E51222 4BC66D5E 3A1718C2 980AC3DB 31D22B27
          2E1B589D A050F216
```

- Step 4: Additional inputs into the key derivation function and two blocks (512 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000020 0B537E0F
             D59BA7A8 B31F1812 1706EB60 716C9EEB D216508B 31340927
             652D7C9E 424F4242 59343536

DerKeyMat  = 5E8CD9FE 5EA2CD45 D85D2302 423AD056 DE934601 5ABCC161
             6A0F5D6C 3F3B5A5B 4F5675B0 E8255937 CC37A7CC BFAD2FBE
             BD68591D 6D7FF097 61997CCF 7C7A33D7
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 5E8CD9FE 5EA2CD45 D85D2302 423AD056

nonceV =  280B810E 92375F31 36AB1C1E E88B3C2A 56725EC6 4F37733B
          29E6C8BB DF191F8D
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 0B537E0F D59BA7A8
            B31F1812 1706EB60 716C9EEB D216508B 31340927 652D7C9E
            280B810E 92375F31 36AB1C1E E88B3C2A 56725EC6 4F37733B
            29E6C8BB DF191F8D

MacTag_U  = 638851CC 198E23F7 C2969A26 ECFC639F FD189DFA 95F2B58C
            1E87E909 D272216B
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 0B537E0F D59BA7A8
            B31F1812 1706EB60 716C9EEB D216508B 31340927 652D7C9E

MacTag_V  = 0A7617DE 2ABEBB7D 0E7E37BB 3308664A E40198DF C745EB0A
            950FD8C5 3886F5F5
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
            = 4B435F32 5F55414C 49434542 4F424259 0B537E0F D59BA7A8
              B31F1812 1706EB60 716C9EEB D216508B 31340927 652D7C9E
              280B810E 92375F31 36AB1C1E E88B3C2A 56725EC6 4F37733B
              29E6C8BB DF191F8D

 MacTag_U  = 881DD926 F00256C7 084F1E19 532B5AA4 FEC229EA A00C82E8
              7364C629 C301EFBB

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

            = 4B435F32 5F56424F 42425941 4C494345 280B810E 92375F31
              36AB1C1E E88B3C2A 56725EC6 4F37733B 29E6C8BB DF191F8D
              0B537E0F D59BA7A8 B31F1812 1706EB60 716C9EEB D216508B
              31340927 652D7C9E

 MacTag_V  = 6DABD5A1 409B8B6D 9D02ACF7 382DDC37 A1BDD422 767FCCEB
              337BA81E CE4C1FA6
```

5.5 Test data for P–384

In this section, we supply step–by–step test data for the seven elliptic curve key agreement schemes described in [1, section 6] using the parameter set P–384 described in Appendix 4.4. For each scheme, a reference to the corresponding section in [1] is provided.

5.5.1 Full Unified Model for curve P–384

- Prerequisites:

```
dsU   =   EFAC3779 DC7EBBE4 488A337C 500CDCB3 89B25D04 FBB52615
          CDEE92BE F4B6DB79 4BE1545C 8FABE76B 41995EC8 BE6D7541

x_QsU =   8B63F1F8 BAA118A3 28184E33 D65F4DDE 2A48FA83 48FA35D8
          D1CE81A9 062979FB 903E41D3 3786BF36 F77D94BF 7D253F50
```

```
y_QsU =   C5076F32 94176241 81D6EB8A 083E0E37 E725660F AC806771
          3F1563F5 F8D2DD6B F1FF237E 8E4FF7C7 C35DCE5D C2F7EA65

dsV   =   19AFCCF2 5DD618DC 1A92F538 2209B5AA E0B6C032 ABB97C8B
          980E6F5F D200E398 21464A3F D58ABAF9 509D23AA 6A2D1E09

x_QsV =   ACEAF614 75072C4F F4857B09 8067FC06 76A93E03 96E0A54C
          4EC5DDCD 2235E7A8 7B742242 B1F0C4CD 8A5F2CC8 C9B7A766

y_QsV =   CE50165A 0338EB3E 50122E4B 88CC2A3D 73ECF652 C4BFF9BB
          710DEC92 D86072F5 6ED711FF E86D59D8 182B2E01 F951A888
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   FEAD0DC3 7EE11A64 547EE10E FD6F3103 BC5B3497 B67B95E2
          3A2562E3 662D9BBC 85EC8B8F CDDC8F03 36F8A5B0 5627B4CF

x_QeU =   03978ED1 7AD4B79D E10C9095 AF866120 21A5FA7C AFBE7704
          C75D04DD 92950DF1 6FD7587F 8EFEFA8E 6C2236A1 929E1725

y_QeU =   C60F7B98 FE4D5ADC A44B3628 1932AFB1 3E49186B F23C915C
          D8FDE338 5B004459 75C09DA2 4AA4AA65 F7A290A6 611C8DC5

deV   =   163A3B11 841421DD 71DD970E 872BDE67 59A798BA A50F01F2
          768FCA6E 5F6F33C3 3410DBB9 34F315AA 85018797 979B48F7

x_QeV =   10509F5B D2128EB7 CE523345 5FB74160 E4C079B2 7034AFB7
          98706DE9 B05D3906 382FAE47 A9B72E56 EFC43023 BD8CB17B

y_QeV =   537E1578 99E05089 EE206328 9EF39D78 1E23EC74 F9A4ED21
          B724DF26 A1EAFF58 40CD6D14 3B5C8FE6 20B299BB D82F97D3
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     2750208034428323463094590738555122189081550727830 7
          6937881199042993167684082674726243171246790487620 5
          7692889167008393

Z_s =     B2AF435C BD4DE891 CB922F11 9FD35431 03373CF4 3FD649CB
          82080C3F AA734F45 9617C8B3 B065794E 058B6772 29859289
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     2756415450491706892644176255907753888941163937820 8
          7013138713211513999674070847518759852240811564430 5
          482199692484651

Z_e =     11E8A6A1 09E3F48F 9DE64C1D D892A29F 32B99E94 F5ECB331
          B0678635 9A475D84 D5F4EBF5 F11DE01C 2EE33B5E 6F50202B
```

- Step 5: Shared secret.

```
Z =       11E8A6A1 09E3F48F 9DE64C1D D892A29F 32B99E94 F5ECB331
          B0678635 9A475D84 D5F4EBF5 F11DE01C 2EE33B5E 6F50202B
          B2AF435C BD4DE891 CB922F11 9FD35431 03373CF4 3FD649CB
          82080C3F AA734F45 9617C8B3 B065794E 058B6772 29859289
```

- Step 6: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 916E92E7 3654A486 0EB5D4A7 E598A08A 4F09B9A3 650DE618
             0C1FB4B4 A5551B46 889D20A4 DABC693E EA17A3B5 77CA3083
             85FBE74A B1E7FD4F 4CDFA38E C28DC649 748BFE1B 0D3CD45A
             7B75AB7D AE2DA7F7 61F0E75F ED246708 C7CD6BB5 30A5914A
```

- If key confirmation is performed, then

```
MacKey  = 916E92E7 3654A486 0EB5D4A7 E598A08A 4F09B9A3 650DE618
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 03978ED1 7AD4B79D
            E10C9095 AF866120 21A5FA7C AFBE7704 C75D04DD 92950DF1
            6FD7587F 8EFEFA8E 6C2236A1 929E1725 C60F7B98 FE4D5ADC
            A44B3628 1932AFB1 3E49186B F23C915C D8FDE338 5B004459
            75C09DA2 4AA4AA65 F7A290A6 611C8DC5 10509F5B D2128EB7
            CE523345 5FB74160 E4C079B2 7034AFB7 98706DE9 B05D3906
            382FAE47 A9B72E56 EFC43023 BD8CB17B 537E1578 99E05089
            EE206328 9EF39D78 1E23EC74 F9A4ED21 B724DF26 A1EAFF58
            40CD6D14 3B5C8FE6 20B299BB D82F97D3

 MacTag_U  = 5BEC60B8 E56F4911 445615E2 AFE2EA7F 40FA0D67 FE6D311F
             01404D3F F610A4BF 62EBE339 512A25B8 F604F8A9 D363B426
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 10509F5B D2128EB7
            CE523345 5FB74160 E4C079B2 7034AFB7 98706DE9 B05D3906
            382FAE47 A9B72E56 EFC43023 BD8CB17B 537E1578 99E05089
            EE206328 9EF39D78 1E23EC74 F9A4ED21 B724DF26 A1EAFF58
            40CD6D14 3B5C8FE6 20B299BB D82F97D3 03978ED1 7AD4B79D
            E10C9095 AF866120 21A5FA7C AFBE7704 C75D04DD 92950DF1
            6FD7587F 8EFEFA8E 6C2236A1 929E1725 C60F7B98 FE4D5ADC
            A44B3628 1932AFB1 3E49186B F23C915C D8FDE338 5B004459
            75C09DA2 4AA4AA65 F7A290A6 611C8DC5

 MacTag_V  = 1A698B39 FBC22AD5 23D4D4DF 7AFB9A17 4D3D5CD2 7649B9DB
             031FD46A 482F7736 F3CEF309 0D57ABF5 4B0E2497 A591B390
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V
```

```
            = 4B435F32 5F55414C 49434542 4F424259 03978ED1 7AD4B79D
              E10C9095 AF866120 21A5FA7C AFBE7704 C75D04DD 92950DF1
              6FD7587F 8EFEFA8E 6C2236A1 929E1725 C60F7B98 FE4D5ADC
              A44B3628 1932AFB1 3E49186B F23C915C D8FDE338 5B004459
              75C09DA2 4AA4AA65 F7A290A6 611C8DC5 10509F5B D2128EB7
              CE523345 5FB74160 E4C079B2 7034AFB7 98706DE9 B05D3906
              382FAE47 A9B72E56 EFC43023 BD8CB17B 537E1578 99E05089
              EE206328 9EF39D78 1E23EC74 F9A4ED21 B724DF26 A1EAFF58
              40CD6D14 3B5C8FE6 20B299BB D82F97D3

 MacTag_U  = 829F6E31 7BC70DEE E9B0C687 46EA1BC2 5ADF21A3 F356AFF8
              0386A3D9 73D68044 0C2CEE44 4949CEA7 571311BA F72EBCA9

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

            = 4B435F32 5F56424F 42425941 4C494345 10509F5B D2128EB7
              CE523345 5FB74160 E4C079B2 7034AFB7 98706DE9 B05D3906
              382FAE47 A9B72E56 EFC43023 BD8CB17B 537E1578 99E05089
              EE206328 9EF39D78 1E23EC74 F9A4ED21 B724DF26 A1EAFF58
              40CD6D14 3B5C8FE6 20B299BB D82F97D3 03978ED1 7AD4B79D
              E10C9095 AF866120 21A5FA7C AFBE7704 C75D04DD 92950DF1
              6FD7587F 8EFEFA8E 6C2236A1 929E1725 C60F7B98 FE4D5ADC
              A44B3628 1932AFB1 3E49186B F23C915C D8FDE338 5B004459
              75C09DA2 4AA4AA65 F7A290A6 611C8DC5

 MacTag_V  = BC1181D9 80ED67CF C2F5BCE3 B66202E5 1B22896C 3E7D6B78
              D2DE8743 48A38C95 AA770034 07D36600 4F1FC637 1DBDE2E1
```

5.5.2 Full MQV for curve P–384

- Prerequisites:

```
dsU   =   30706635 A54DE2FC F95332C5 019022A0 76FCC94B 859AAA23
          E67910B0 B9CEEC06 4E317C97 24252207 9239C778 01F461E7

x_QsU =   189A4B31 D18AA982 EB0CC6C0 D34D0D0C 45EB0028 3E1A1616
          2DF2D03D 7743EED5 952930E3 D223265C BE16947B FE092217
```

```
y_QsU =   77B45D77 456E36AA E1B355B2 99FAE1E2 B0D2E741 603D08A6
          2ABA07EB 46FBE554 46887019 EB7AEDDF EE8A393C C3C62C05

dsV   =   0D70F5B6 74A6CDD0 A3C0ACC6 8B18CAEF 3EEB9468 633434BD
          B312E089 12F83544 413BE1DD 3ACC8E8D 1DB69FEE 77B876C4

x_QsV =   83FDCE70 2E261D41 C335EA75 3F7C29B4 75BDEA69 83E52D25
          E650EB1D 84FDCB41 4664E790 825A9C75 420677E8 1E27B23B

y_QsV =   05AA5784 36E2ADAA 9A3ABA9C F91610D5 B567DDC6 F751B22E
          A2AB748A D727F520 C48F3328 33D1B281 2AD57AE8 30D50F68
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   03C5B38C 2202A15B D6D2F420 79C2CDCC BA8C3F6D AFEA7EEC
          29569AA2 0AA31925 39309F2C 143A8B91 7AD502DF A289E89E

x_QeU =   C7F8EAF4 D340D11D 9851FB6E A6FD683E 431531DD B008B170
          2C719D6D 24648235 3C54F76A 771B7E85 48D152A2 A5BDE848

y_QeU =   54CBC4A7 2DE2A8F1 80FE542E 3C6507DD CD240FE2 57DEA078
          82ED0759 510875C3 E154DF97 45B82334 3B62C028 67166D70

deV   =   9F5B9DD1 03575D09 29B98A2D 543C5866 79A57123 3572DBEA
          EF15D091 99DED7E9 65EB3644 52322422 FA09D922 5482D654

x_QeV =   866F499A EEB8129D D85C74AC C47D2BD3 60DC9E71 8D85463D
          CC0DD3FF 35BC242E 39B119E3 9EEA75E0 26DAB3CA 7A8F8FCF

y_QeV =   00C321F1 CFF66A5A E143EF78 F0278AE9 C2126C29 147E279A
          172317DD E273B822 73D05091 BFF26151 2E8F519E CFC5D6F5
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =        416213623053970843819733747136489801775378189482 86
           811993929968462812879854126498939098029781771585 84
           816955845991381
```

- Step 4: Shared secret converted to byte string.

```
Z =        1B0ABCE4 4ED8A47A EF0783DA 3437B3FF 12D44191 23E78536
           9EAF1D93 4131B59A BAAE161C 53157BAB 2B2DAF73 9E2B5BD5
```

- Step 5: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 2A6CDB4B 4D8C6B1C 0AA26BCC 89F7F8A5 B79234E9 30B7A836
             05511EAC 91A7262E 7F390D87 8FF2CF47 8DA973BF 29C14DDB
             ADCBFC27 23715E60 4A78CCD7 055AD3F0 640FE1FB B911380A
             0686E2D4 6488429C 17829B1C 67ED5A7F 1F96CF90 C85FD37D
```

- If key confirmation is performed, then

```
MacKey  = 2A6CDB4B 4D8C6B1C 0AA26BCC 89F7F8A5 B79234E9 30B7A836
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 C7F8EAF4 D340D11D
            9851FB6E A6FD683E 431531DD B008B170 2C719D6D 24648235
            3C54F76A 771B7E85 48D152A2 A5BDE848 54CBC4A7 2DE2A8F1
            80FE542E 3C6507DD CD240FE2 57DEA078 82ED0759 510875C3
            E154DF97 45B82334 3B62C028 67166D70 866F499A EEB8129D
            D85C74AC C47D2BD3 60DC9E71 8D85463D CC0DD3FF 35BC242E
            39B119E3 9EEA75E0 26DAB3CA 7A8F8FCF 00C321F1 CFF66A5A
            E143EF78 F0278AE9 C2126C29 147E279A 172317DD E273B822
            73D05091 BFF26151 2E8F519E CFC5D6F5
```

```
MacTag_U  = 04D0B01A 42CA1FE5 D591DAA6 AC93B655 C0C86697 29FC15A6
            0D1C1C22 5A488E90 6CED3719 0ADA95D8 CF89B7AC 2F69702F
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 866F499A EEB8129D
            D85C74AC C47D2BD3 60DC9E71 8D85463D CC0DD3FF 35BC242E
            39B119E3 9EEA75E0 26DAB3CA 7A8F8FCF 00C321F1 CFF66A5A
            E143EF78 F0278AE9 C2126C29 147E279A 172317DD E273B822
            73D05091 BFF26151 2E8F519E CFC5D6F5 C7F8EAF4 D340D11D
            9851FB6E A6FD683E 431531DD B008B170 2C719D6D 24648235
            3C54F76A 771B7E85 48D152A2 A5BDE848 54CBC4A7 2DE2A8F1
            80FE542E 3C6507DD CD240FE2 57DEA078 82ED0759 510875C3
            E154DF97 45B82334 3B62C028 67166D70

MacTag_V  = 179FB4D8 987E1785 74EE3155 96596C1A E2D62AFA B76991BA
            FCAEFCB1 EE56A42A D4C5EC00 DB889BE0 67C09167 7E7602EF
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 C7F8EAF4 D340D11D
            9851FB6E A6FD683E 431531DD B008B170 2C719D6D 24648235
            3C54F76A 771B7E85 48D152A2 A5BDE848 54CBC4A7 2DE2A8F1
            80FE542E 3C6507DD CD240FE2 57DEA078 82ED0759 510875C3
            E154DF97 45B82334 3B62C028 67166D70 866F499A EEB8129D
            D85C74AC C47D2BD3 60DC9E71 8D85463D CC0DD3FF 35BC242E
            39B119E3 9EEA75E0 26DAB3CA 7A8F8FCF 00C321F1 CFF66A5A
            E143EF78 F0278AE9 C2126C29 147E279A 172317DD E273B822
            73D05091 BFF26151 2E8F519E CFC5D6F5

MacTag_U  = 35B48609 2908A6E7 F54B85C6 FD989FAE AC57224E 9D045262
            1134D682 3D7AF3CD E5AB824D C803896A 9D2F98BA EA1949E3
```

```
MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 866F499A EEB8129D
            D85C74AC C47D2BD3 60DC9E71 8D85463D CC0DD3FF 35BC242E
            39B119E3 9EEA75E0 26DAB3CA 7A8F8FCF 00C321F1 CFF66A5A
            E143EF78 F0278AE9 C2126C29 147E279A 172317DD E273B822
            73D05091 BFF26151 2E8F519E CFC5D6F5 C7F8EAF4 D340D11D
            9851FB6E A6FD683E 431531DD B008B170 2C719D6D 24648235
            3C54F76A 771B7E85 48D152A2 A5BDE848 54CBC4A7 2DE2A8F1
            80FE542E 3C6507DD CD240FE2 57DEA078 82ED0759 510875C3
            E154DF97 45B82334 3B62C028 67166D70

MacTag_V  = 77C9B955 4CB7299A 55AA9951 7EF7FA7A 97B32B1E 8443FBCD
            002E832A A1988353 682A8161 4291EF0B B79FF0FE 6AF2C69F
```

5.5.3 Ephemeral Unified Model for curve P–384

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   168BBFCE 72A19F7F B7FC01DE B946757B D088CEDF 82B902BE
          1C7566CF EAAFF862 ED424DAF 1D0380CF F0049DA4 3A301548

x_QeU =   3270FDF2 E5C31C37 C6FD007D 67A81641 F55F33B0 F6AA57DE
          382A747D 09A565D6 9EDFAFDC CD29B5DD F535FE45 0DE6DB0A

y_QeU =   DB79FFCF 5944A62E 9349FC7A D04069BB F8EC8310 979E8E81
          29D44B69 E4099ED0 9058D7DC 4F6A4A84 97FD33D6 F64B59D0

deV   =   DF7525AB E9D1204F FC30B554 7BE8D889 DF7A5E5F 834E4554
          6114B382 B952D0D7 8EC0E0FC 8071F101 9EB406EF 892307B0

x_QeV =   CF8BF93A C83FC537 E980D04F FFB4B6B1 734B9DCB DF98B77D
          7594CC99 34F5F871 A2DD96EC 4D3FBAEF 56076424 8B237BD1
```

```
y_QeV =   5B5F180C 4F9A5007 1FE3ADC7 0ED64D36 5E74DB39 4F54316B
          0BF06879 9A4967C2 302C74D2 9EAC6A41 4B8DF7DF 5D1D499A
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       82733454122552091837738968118663958805876224377340
          73017846306519016530235997409287666074578949558939
          390425169049192
```

- Step 4:

```
Z =       35C0C540 33C33F0A 5597C45D 449A187D 4FDA0E10 E2DA4932
          9595D4B5 67DF7A8E 8C188055 22C743B4 53B71F87 8AB2B668
```

- Step 5: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 84736279 E66535AB C2424EE1 4BCA637C E66CE4F0 327FB1A6
             C96F2237 69D7C0B7 62AB403C 437985F7 495DC12F 7943E083
             6A41EC63 A2C3D384 A8F84403 95C9571B 233CFF98 83DA7FC3
             5030C2F4 18762D21 2C20320F 771FFB7E E124C636 31A74663
```

5.5.4 One–Pass Unified Model for curve P–384

- Prerequisites:

```
dsU   =   D56E811F 4BAAD075 E5221013 5C03B57A 74EE4D02 A80E1DAB
          0C04AFBB A38C3DFB 9421BE0E A29DCC89 B6B867A6 681BC670

x_QsU =   62C72D9E AD43CA21 75A13EA3 EB105335 C410EB35 D8A5DCE5
          D356B657 C0A9FBF5 1F747017 662E4FC9 A872339F 885D258A
```

```
y_QsU =   E962FBF9 7BC767A8 0184B0A8 3AE877D2 4022B767 562CFC43
          9EC29475 A11A732E 1C0B4F97 1BB9C225 5FD8847F D8C516BF

dsV   =   C169EFA5 027D7E5A 6E7C7866 64BA0C2B 6F3B98B4 ED91B262
          2730CC80 7FEC2004 CE3990E7 FC142EC8 A4F02CCA 21AEE192

x_QsV =   E5705621 D6661D51 39FF7169 B70DC66E 491B7787 84C7F54B
          88F3F82D 423606CD 6BEA1BCD 2599E288 19C1F1E0 4036C01C

y_QsV =   295DE704 B31B4583 BBC20754 73AB1F54 9D577020 4FAB300F
          3D370C84 886C550F D321E764 972F2B32 B01CC7ED 6221393B
```

BEGIN U's calculations

- Step 1:

```
deU   =   3C3B32E3 59905C23 047D1A8F D6C77F06 FFD1A0E0 9C0586AC
          A29F2CBC EE9BF958 059B833B 641F5604 7FD1C03F C10CC7CD

x_QeU =   AF79A9A8 5298A04F B2376A5E D10CA925 4AB35355 515C84F5
          C8A89619 58450BBD 55E63B47 A6CEC5B2 C540116D D0D948F9

y_QeU =   6D77AB6B 43437FD8 062DD756 AC25DC20 8B7AED7F 6DFDA164
          9C836936 B5262732 24CF5009 57B31EBF 0F81CB0F 83A769B6
```

- Step 2: Decimal and hex values for static shared secret.

```
Z_s =     82816089553376546161969437870182891533602133780822
          08861135274527373652221423989296842239068883893000
          88436357324350

Z_s =     05617395 5B53D1FB ACD4890F E35AF203 64E5F872 D3ED2C30
          1DFC3D0D B9EBB397 125A33E7 99DE192D 4964A748 423BDE3E
```

- Step 3: Decimal and hex values for ephemeral shared secret.

```
Z_e =     119232238663282074973481201972920734400933037897 70
          597889946518317686921692317430574555178663562569 53
          2751344502950417

Z_e =     4D777CD6 B0247D81 CFCD836A 6D69EC0F 397FC072 E1B2C79C
          894BE26C F7C70404 5EAD0941 5A077A75 ED3752A2 4239CA11
```

- Step 4: Shared secret.

```
Z =       4D777CD6 B0247D81 CFCD836A 6D69EC0F 397FC072 E1B2C79C
          894BE26C F7C70404 5EAD0941 5A077A75 ED3752A2 4239CA11
          05617395 5B53D1FB ACD4890F E35AF203 64E5F872 D3ED2C30
          1DFC3D0D B9EBB397 125A33E7 99DE192D 4964A748 423BDE3E
```

- Step 5: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = C69511E5 BF6DF458 877F5E29 CD360558 440FD0D6 4F9336FB
             F661FCA7 29EEBF92 E4834FF3 3E3C6310 4D68DB8B 3F948FE0
             6852C27F 8E1BAFEB 9F316659 359F10A0 4AA52E71 0F2388A8
             DB562C23 D02E9DC1 1F999AD3 5D001B51 5B6FB3D6 57C57FC1
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   3C3B32E3 59905C23 047D1A8F D6C77F06 FFD1A0E0 9C0586AC
          A29F2CBC EE9BF958 059B833B 641F5604 7FD1C03F C10CC7CD

x_QeU =   AF79A9A8 5298A04F B2376A5E D10CA925 4AB35355 515C84F5
          C8A89619 58450BBD 55E63B47 A6CEC5B2 C540116D D0D948F9

y_QeU =   6D77AB6B 43437FD8 062DD756 AC25DC20 8B7AED7F 6DFDA164
          9C836936 B5262732 24CF5009 57B31EBF 0F81CB0F 83A769B6
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     82816089553376546161969437870182891533602133780822
          08861135274527373652221423989296842239068883893000
          88436357324350

Z_s =     05617395 5B53D1FB ACD4890F E35AF203 64E5F872 D3ED2C30
          1DFC3D0D B9EBB397 125A33E7 99DE192D 4964A748 423BDE3E
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     11923223866328207497348120197292073440093303789770
          59788994651831768692169231743057455517866356256953
          2751344502950417

Z_e =     4D777CD6 B0247D81 CFCD836A 6D69EC0F 397FC072 E1B2C79C
          894BE26C F7C70404 5EAD0941 5A077A75 ED3752A2 4239CA11
```

- Step 5: Shared secret.

```
Z =       4D777CD6 B0247D81 CFCD836A 6D69EC0F 397FC072 E1B2C79C
          894BE26C F7C70404 5EAD0941 5A077A75 ED3752A2 4239CA11
          05617395 5B53D1FB ACD4890F E35AF203 64E5F872 D3ED2C30
          1DFC3D0D B9EBB397 125A33E7 99DE192D 4964A748 423BDE3E
```

- Step 6: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = C69511E5 BF6DF458 877F5E29 CD360558 440FD0D6 4F9336FB
             F661FCA7 29EEBF92 E4834FF3 3E3C6310 4D68DB8B 3F948FE0
             6852C27F 8E1BAFEB 9F316659 359F10A0 4AA52E71 0F2388A8
             DB562C23 D02E9DC1 1F999AD3 5D001B51 5B6FB3D6 57C57FC1
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = C69511E5 BF6DF458 877F5E29 CD360558 440FD0D6 4F9336FB

nonceV =  AD4909DC 6B7A16FA 5783FE5A 46A73B1F 7EE8D1C4 FCF3B40C
          8D53B208 C01329F6 ED3C1C17 9948C978 F39A794F D91FAD10
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 AF79A9A8 5298A04F
            B2376A5E D10CA925 4AB35355 515C84F5 C8A89619 58450BBD
            55E63B47 A6CEC5B2 C540116D D0D948F9 6D77AB6B 43437FD8
            062DD756 AC25DC20 8B7AED7F 6DFDA164 9C836936 B5262732
            24CF5009 57B31EBF 0F81CB0F 83A769B6 AD4909DC 6B7A16FA
            5783FE5A 46A73B1F 7EE8D1C4 FCF3B40C 8D53B208 C01329F6
            ED3C1C17 9948C978 F39A794F D91FAD10

MacTag_U  = A8987DC7 0702302E 162D87B2 30007372 D5D9BF04 5E25329B
            66EF4101 7165F12A 7658D428 E7D2F180 664B023D 568BC7A8
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 AF79A9A8 5298A04F
            B2376A5E D10CA925 4AB35355 515C84F5 C8A89619 58450BBD
            55E63B47 A6CEC5B2 C540116D D0D948F9 6D77AB6B 43437FD8
            062DD756 AC25DC20 8B7AED7F 6DFDA164 9C836936 B5262732
            24CF5009 57B31EBF 0F81CB0F 83A769B6

MacTag_V  = 8019ADF0 75E2A7AD 3F804827 0D2DC224 16CD9731 35B6FAD8
            F3D527AD 5A6A1780 7EF147D2 758E9442 A246BA08 40950C72
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 AF79A9A8 5298A04F
            B2376A5E D10CA925 4AB35355 515C84F5 C8A89619 58450BBD
            55E63B47 A6CEC5B2 C540116D D0D948F9 6D77AB6B 43437FD8
            062DD756 AC25DC20 8B7AED7F 6DFDA164 9C836936 B5262732
            24CF5009 57B31EBF 0F81CB0F 83A769B6 AD4909DC 6B7A16FA
            5783FE5A 46A73B1F 7EE8D1C4 FCF3B40C 8D53B208 C01329F6
            ED3C1C17 9948C978 F39A794F D91FAD10

 MacTag_U  = 05052757 2651F1E5 EE2E8766 4912B2D2 83E3DE69 9D2737CC
            EA803110 0854B04F BF3946D9 D4C25355 6295F1A7 4AAA61D0

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 AD4909DC 6B7A16FA
            5783FE5A 46A73B1F 7EE8D1C4 FCF3B40C 8D53B208 C01329F6
            ED3C1C17 9948C978 F39A794F D91FAD10 AF79A9A8 5298A04F
            B2376A5E D10CA925 4AB35355 515C84F5 C8A89619 58450BBD
            55E63B47 A6CEC5B2 C540116D D0D948F9 6D77AB6B 43437FD8
            062DD756 AC25DC20 8B7AED7F 6DFDA164 9C836936 B5262732
            24CF5009 57B31EBF 0F81CB0F 83A769B6

 MacTag_V  = 1CD1E3A0 F1007F6D 2A72A9AC 6CD9B4EA 36EFC986 560D0729
            29748454 08AFC1D0 B6ACB5A6 69046AE0 E07F121F 6A2965B0
```

5.5.5 One–Pass MQV for curve P–384

- Prerequisites:

```
dsU   =   F9634BE9 8E324734 09212F8D F069158E 4E46F37E 566D5A92
          65B5AFB8 70F45A0E 8D220770 BB345297 2782C175 B7C291BF
```

```
x_QsU =   2781D665 B405F448 DC41D917 876AF055 2BD5CC48 D706534C
          C0C94437 49D056CC D5ECBCDB 5C6E0E12 90021C70 0D14CD62

y_QsU =   AAB98B15 38110A00 DF5FF2B5 6111A639 D9D6566A B000ED70
          2142EE31 C3969B9A 572FF646 EDDB6B8F 70F95578 8C89CE69

dsV   =   6415BDA7 10CAED41 CFB7483B B8E1FAFD F26BA932 B2A0E12C
          6C876743 CF89100B 246EB606 97E15009 87537B12 DCAB64ED

x_QsV =   200E21B2 13E79714 395ECAE0 50C1F5E3 0051692A 1435B8EA
          DD64F943 E97C2754 C0C83662 DA098DB7 DE5F63E0 B0931789

y_QsV =   621D96DC 40990EB2 0EFF3D2B 8BBD1D76 BC54847D 09217E1C
          496B40DE 1FE03471 2C418CC1 92667A71 E5D33B0E 8981F4A1
```

BEGIN U's calculations

- Step 1:

```
deU   =   BA1A6DD9 02ED9322 31EAEA1F BA9ADCE6 0DDAE244 68EDC335
          2AEEA57E BF2FE1D6 15703005 45354576 45AD6D04 C7F350BB

x_QeU =   DA2603C6 30213222 7A3AD63F 2129D061 E701D25A D792B263
          47423EDA 46DBF99E 16E79A39 9EABACCF 4C62906E CA5862CE

y_QeU =   CCFD18A2 B3CBF0A3 14B79D06 093AD754 18ED826C 11742D21
          307AE0E0 6CFAA949 9DE29D45 522648BE EE61E2B3 89F74958
```

- Step 2: Decimal value for shared secret.

```
Z =       28880861358690296921706985610911770414248577801510
          13307925669136057724085360791013592486654311412130
          415429434531537
```

- Step 3: Hex value for shared secret.

```
Z =        12C3A77A 64DB8D2A 44DD3264 B2865224 E172E33A 461BCD6D
           336AA641 62E8E297 BFD7CCF5 ADF1B741 363A92FE F7FCDED1
```

- Step 4: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 686E26E6 2B639232 2CE1CDC5 9F3BCDC8 D4B3ADA8 FDA544D4
             31C45426 97BEDB62 2F36DF04 93D34108 6DB31C7C EF655E6D
             CA1BACFA 0DF37AF7 E6CE1FF8 4AB2C222 640CA642 0321563B
             B94DAD1F A1BCD7D5 AE60182E F8424D62 2CA63B00 35A5AC54
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =    BA1A6DD9 02ED9322 31EAEA1F BA9ADCE6 0DDAE244 68EDC335
           2AEEA57E BF2FE1D6 15703005 45354576 45AD6D04 C7F350BB

x_QeU =    DA2603C6 30213222 7A3AD63F 2129D061 E701D25A D792B263
           47423EDA 46DBF99E 16E79A39 9EABACCF 4C62906E CA5862CE

y_QeU =    CCFD18A2 B3CBF0A3 14B79D06 093AD754 18ED826C 11742D21
           307AE0E0 6CFAA949 9DE29D45 522648BE EE61E2B3 89F74958
```

- Step 2: N/A.
- Step 3: Decimal value for shared secret.

```
Z =        288808613586902969217069856109117704142485778015 10
           133079256691360577240853607910135924866543114121 30
           415429434531537
```

- Step 4: Hex value for shared secret.

```
Z =       12C3A77A 64DB8D2A 44DD3264 B2865224 E172E33A 461BCD6D
          336AA641 62E8E297 BFD7CCF5 ADF1B741 363A92FE F7FCDED1
```

- Step 5: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 686E26E6 2B639232 2CE1CDC5 9F3BCDC8 D4B3ADA8 FDA544D4
             31C45426 97BEDB62 2F36DF04 93D34108 6DB31C7C EF655E6D
             CA1BACFA 0DF37AF7 E6CE1FF8 4AB2C222 640CA642 0321563B
             B94DAD1F A1BCD7D5 AE60182E F8424D62 2CA63B00 35A5AC54
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 686E26E6 2B639232 2CE1CDC5 9F3BCDC8 D4B3ADA8 FDA544D4

nonceV =  32288539 A9177FF8 54F283F1 29662282 07BB7346 6B9F6B1A
          245B2851 1A1ED418 DBAFD51C 35807843 D9984043 71536F19
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 DA2603C6 30213222
            7A3AD63F 2129D061 E701D25A D792B263 47423EDA 46DBF99E
            16E79A39 9EABACCF 4C62906E CA5862CE CCFD18A2 B3CBF0A3
            14B79D06 093AD754 18ED826C 11742D21 307AE0E0 6CFAA949
            9DE29D45 522648BE EE61E2B3 89F74958 32288539 A9177FF8
            54F283F1 29662282 07BB7346 6B9F6B1A 245B2851 1A1ED418
            DBAFD51C 35807843 D9984043 71536F19

MacTag_U  = 69A8C2C5 044C8AFB 438269A9 D8C074E0 6CF7C64B EBF6A634
             BC078F48 BC81523E 5577DF16 796C4B9A BD4085A4 43C06C6F
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 DA2603C6 30213222
            7A3AD63F 2129D061 E701D25A D792B263 47423EDA 46DBF99E
            16E79A39 9EABACCF 4C62906E CA5862CE CCFD18A2 B3CBF0A3
            14B79D06 093AD754 18ED826C 11742D21 307AE0E0 6CFAA949
            9DE29D45 522648BE EE61E2B3 89F74958

 MacTag_V  = E95FB3E4 5A33D6C2 7567A814 3B29664B AF7A4BAA 5F912C7E
             B312ACB1 CF52810C E0AD6BDE 134ECFAD 2227BD2A F78DC1CA
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

           = 4B435F32 5F55414C 49434542 4F424259 DA2603C6 30213222
             7A3AD63F 2129D061 E701D25A D792B263 47423EDA 46DBF99E
             16E79A39 9EABACCF 4C62906E CA5862CE CCFD18A2 B3CBF0A3
             14B79D06 093AD754 18ED826C 11742D21 307AE0E0 6CFAA949
             9DE29D45 522648BE EE61E2B3 89F74958 32288539 A9177FF8
             54F283F1 29662282 07BB7346 6B9F6B1A 245B2851 1A1ED418
             DBAFD51C 35807843 D9984043 71536F19

 MacTag_U  = E0527249 59C2D395 671C3FF6 BB24AD25 408CA653 F1189381
             9997D84D 1B671965 D53F70E0 11309EDB 5239DE4E 2323EBF3

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

           = 4B435F32 5F56424F 42425941 4C494345 32288539 A9177FF8
             54F283F1 29662282 07BB7346 6B9F6B1A 245B2851 1A1ED418
             DBAFD51C 35807843 D9984043 71536F19 DA2603C6 30213222
             7A3AD63F 2129D061 E701D25A D792B263 47423EDA 46DBF99E
             16E79A39 9EABACCF 4C62906E CA5862CE CCFD18A2 B3CBF0A3
             14B79D06 093AD754 18ED826C 11742D21 307AE0E0 6CFAA949
             9DE29D45 522648BE EE61E2B3 89F74958

 MacTag_V  = AEA6CD5F 2C41B420 C5076BD0 A49A636E B80D9DEC 7D542503
             951CC401 F556E74D 10F1787D 45FF9A39 68436CF0 39D8CCA8
```

5.5.6 One–Pass Diffie–Hellman for curve P–384

- Prerequisites:

```
dsV   =   A9480F48 2CA8A01E 6657F4DE 4396F942 0C99B2D6 F4F6AF0D
          7C69A68F B015FFCE 52353A93 31BC6C37 BAC1854E ED257BC3

x_QsV =   A4448AD1 58D40423 F3E44E3D E7B05C7E 22129428 7A7279B6
          87BA7B77 DCAF42B0 E13D12CE 9A30E4CD 3D2994FA DDCCE467

y_QsV =   69ED132E B45519AF D8EA06F6 BAFEB199 5165D59B 0802BAD7
          A5E1D067 2176A711 DE499540 DF30C694 75AA77EE F743EA9E
```

BEGIN U's calculations

- Step 1:

```
deU   =   04D5697E 40CD5946 70542113 F255660C ED0AFDC1 2F83C337
          F8778CDC B95C6463 52CE2139 D123752E 49BB2C1D 90CE9F83

x_QeU =   BB88D43D 1929A2BA FBD30A7B 36AE785E 2DB67603 1D0AD8D6
          EABCA7D7 38807047 664A79AA 46D4A691 592DC397 2406AC25

y_QeU =   346FE358 F62A1D67 2683ACBE C4992E75 F0A5BC31 5F99D3B4
          5031DA37 AE653138 69092D33 211616A9 AD47BF55 8EDB03C6
```

- Step 2: Decimal value for shared secret.

```
Z =       24879063262001984330558516696991886938385731947413
          98266230265185703812193756543782058517050351245136
          5649840493341748
```

- Step 3: Hex value for shared secret.

```
Z =       A1A47D39 006B976F 42FC7BB5 7649C5B3 E2D46BBE 2318A9B5
          EB74EAE2 B3FC6ECA 1A24F313 A7BC1DF6 00532152 82F4AC34
```

- Step 4: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = E8DDD1B9 34A67BD7 736C3A37 69973214 1E072E88 096BCE9B
             BFE1A8EA B25FCB25 069EFA98 D982763B FCCAA406 BE84FE0E
             0F461A3A F422DCFC C214FDB4 F266B4AC 72C9894C 09AC78CF
             65E1C0C3 4E8FB3F5 18FDD4D1 2E9DB7DA FC350E9C 937E7A8C
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   04D5697E 40CD5946 70542113 F255660C ED0AFDC1 2F83C337
          F8778CDC B95C6463 52CE2139 D123752E 49BB2C1D 90CE9F83

x_QeU =   BB88D43D 1929A2BA FBD30A7B 36AE785E 2DB67603 1D0AD8D6
          EABCA7D7 38807047 664A79AA 46D4A691 592DC397 2406AC25

y_QeU =   346FE358 F62A1D67 2683ACBE C4992E75 F0A5BC31 5F99D3B4
          5031DA37 AE653138 69092D33 211616A9 AD47BF55 8EDB03C6
```

- Step 2: N/A.

- Step 3: Decimal value for shared secret.

```
Z =       24879063262001984330558516696991886938385731947413
          98266230265185703812193756543782058517050351245136
          5649840493341748
```

- Step 4: Hex value for shared secret.

```
Z =       A1A47D39 006B976F 42FC7BB5 7649C5B3 E2D46BBE 2318A9B5
          EB74EAE2 B3FC6ECA 1A24F313 A7BC1DF6 00532152 82F4AC34
```

- Step 5: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = E8DDD1B9 34A67BD7 736C3A37 69973214 1E072E88 096BCE9B
             BFE1A8EA B25FCB25 069EFA98 D982763B FCCAA406 BE84FE0E
             0F461A3A F422DCFC C214FDB4 F266B4AC 72C9894C 09AC78CF
             65E1C0C3 4E8FB3F5 18FDD4D1 2E9DB7DA FC350E9C 937E7A8C
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = E8DDD1B9 34A67BD7 736C3A37 69973214 1E072E88 096BCE9B
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 BB88D43D 1929A2BA
            FBD30A7B 36AE785E 2DB67603 1D0AD8D6 EABCA7D7 38807047
            664A79AA 46D4A691 592DC397 2406AC25 346FE358 F62A1D67
            2683ACBE C4992E75 F0A5BC31 5F99D3B4 5031DA37 AE653138
            69092D33 211616A9 AD47BF55 8EDB03C6

MacTag_V  = 77006685 1DD19C75 476F7069 2D0C7955 9C0B2CCA BFB57CCA
             32CCE3FE F9EB916C 5F9D6E60 D18EF127 09CE4F9A 52814DD1
```

5.5.7 Static Unified Model for curve P–384

- Prerequisites:

```
dsU   =   7A212B5A 9C08DB6F E2D175C2 1DF8ECED 1F68E692 2FAF225F
          470A68F9 9511FCC4 B76CBFBB 37846EB0 4465E47F 743977E3
```

```
x_QsU =   A8544048 47685BD2 E526817A CA19D8D7 53A307EB CF483F08
          D3FCA1DE 35351FA9 84008353 4B4B4C33 16626570 8B5FFE4F

y_QsU =   28600408 802AB22C 8641FB9D A7A2C927 C1E5333F 81F4702E
          DD94613E 7CC4F887 440FEDE9 8E3BAD1F 35E4E168 879708E3

dsV   =   AAF84DF4 84A1DC0F 7BF2FF2F 56988937 3BD52ABD C89F6E6A
          06F75C62 C1421309 21A16BE7 810F7059 80409382 6225CF01

x_QsV =   759CD8C8 D749B642 93DD4639 D2F70563 837515E0 FE2C9F90
          A1E82382 2014A0F9 9E03587C 10496F4A 451B7C60 43108806

y_QsV =   6B19C69C 487792AC AE5809AE E30753A7 7BDA7C14 FF366704
          0BF40199 210490F5 7A3B281A F130B8E0 B2DE2724 142F6B39
```

BEGIN U's calculations

- Step 1:

```
nonceU =  49D6B6A3 009028DD 7E085C3A C6110DC0 013A6A4F 388BE87A
          EED4C59A FA981B3F 883D001B B1AAA9E2 F450AFA9 C307476E
```

- Step 2: Decimal value for shared secret.

```
Z =       91144040835466480517069714635425829971785278492387
          53285258855397027552588367024963139434279947420836
          172357676766384
```

- Step 3: Hex value for shared secret.

```
Z =       3B37ACA7 C4055C0D EDD3CC11 C408586F 8E1EBCBC 536E6F87
          EFCDA7A7 D8C77615 8EB77744 C171ACE4 70E73E13 EF4314B0
```

- Step 4: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000030 49D6B6A3
             009028DD 7E085C3A C6110DC0 013A6A4F 388BE87A EED4C59A
             FA981B3F 883D001B B1AAA9E2 F450AFA9 C307476E 424F4242
             59343536

DerKeyMat  = D709B906 9AE91352 8C3008AF 6135FD0C 0A96462E AA196BE1
             9A02E41A 49EB227F 437D3098 49138BA8 8ADF7154 B5728BA6
             29AE8EEF 187B823C 028CCA55 33307433 27BA112E 72AEC379
             B1C11225 962FF47B AAE53B9C C29BF9C5 C8E1B137 38AD7120
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
nonceU =  49D6B6A3 009028DD 7E085C3A C6110DC0 013A6A4F 388BE87A
          EED4C59A FA981B3F 883D001B B1AAA9E2 F450AFA9 C307476E
```

- Step 2: Decimal value for shared secret.

```
Z =       91144040835466480517069714635425829971785278492387
          53285258855397027552588367024963139434279947420836
          172357676766384
```

- Step 3: Hex value for shared secret.

```
Z =       3B37ACA7 C4055C0D EDD3CC11 C408586F 8E1EBCBC 536E6F87
          EFCDA7A7 D8C77615 8EB77744 C171ACE4 70E73E13 EF4314B0
```

- Step 4: Additional inputs into the key derivation function and two blocks (768 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000030 49D6B6A3
             009028DD 7E085C3A C6110DC0 013A6A4F 388BE87A EED4C59A
             FA981B3F 883D001B B1AAA9E2 F450AFA9 C307476E 424F4242
             59343536
```

```
DerKeyMat  = D709B906 9AE91352 8C3008AF 6135FD0C 0A96462E AA196BE1
             9A02E41A 49EB227F 437D3098 49138BA8 8ADF7154 B5728BA6
             29AE8EEF 187B823C 028CCA55 33307433 27BA112E 72AEC379
             B1C11225 962FF47B AAE53B9C C29BF9C5 C8E1B137 38AD7120
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = D709B906 9AE91352 8C3008AF 6135FD0C 0A96462E AA196BE1

nonceV =  12094DDD A3B3D14E 00415E16 CFFDE659 CE3C34E6 4131BEF5
          FBB5C12B A067258D 95632EE5 C45F7085 0F513DE3 0E04413D
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 49D6B6A3 009028DD
            7E085C3A C6110DC0 013A6A4F 388BE87A EED4C59A FA981B3F
            883D001B B1AAA9E2 F450AFA9 C307476E 12094DDD A3B3D14E
            00415E16 CFFDE659 CE3C34E6 4131BEF5 FBB5C12B A067258D
            95632EE5 C45F7085 0F513DE3 0E04413D

MacTag_U  = B4F775AE 66B0DEE8 97E15DE8 2BDD7F83 2D45614D BAA2D8F6
            DB91AECF 25A6E6B8 363D3AAD 1A581333 7C631A23 513F4866
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 49D6B6A3 009028DD
            7E085C3A C6110DC0 013A6A4F 388BE87A EED4C59A FA981B3F
            883D001B B1AAA9E2 F450AFA9 C307476E

MacTag_V  = F4C560C4 DDC2D335 D997EFB4 26C121E1 559C6855 F39653E4
            D1C36A7B 2C5C0FCD A882FDBE 81EEBF50 6C734138 DC6F5B9B
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 49D6B6A3 009028DD
            7E085C3A C6110DC0 013A6A4F 388BE87A EED4C59A FA981B3F
            883D001B B1AAA9E2 F450AFA9 C307476E 12094DDD A3B3D14E
            00415E16 CFFDE659 CE3C34E6 4131BEF5 FBB5C12B A067258D
            95632EE5 C45F7085 0F513DE3 0E04413D

 MacTag_U  = C91B4221 E238D667 15A017DA C032192B 01BA220A E643D07A
            824E0EF7 B23225FA 8F6B0163 56B7F167 7C1587CB 614DACE8

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 12094DDD A3B3D14E
            00415E16 CFFDE659 CE3C34E6 4131BEF5 FBB5C12B A067258D
            95632EE5 C45F7085 0F513DE3 0E04413D 49D6B6A3 009028DD
            7E085C3A C6110DC0 013A6A4F 388BE87A EED4C59A FA981B3F
            883D001B B1AAA9E2 F450AFA9 C307476E

 MacTag_V  = 57547641 84860825 92F44364 55492CF4 EB24227D 77A78451
            CC39CA7D DD78F55D AA1B71A0 165EE07E CB938B4B D630FC70
```

5.6 Test data for P–521

In this section, we supply step–by–step test data for the seven elliptic curve key agreement schemes described in [1, section 6] using the parameter set P–521 described in Appendix 4.5. For each scheme, a reference to the corresponding section in [1] is provided.

5.6.1 Full Unified Model for curve P–521

- Prerequisites:

```
dsU   =   000001FD 44146E7F 8F564061 643890BD 814E6275 6BE3E30C
          6144C7EC C4A1E3A6 3A1976A2 CDC2061D C1E540C3 22B5CD2A
          F53FB3BE E66AA752 46CA828E FAB25709 DC48503D

x_QsU =   000000E2 38A67386 8DB5EF1C 17180648 A63DD78D 76DFC763
          EC9AC2CC C91246AC BD03A464 096B76EA 25FAE083 7B182BF5
          8C5279F1 E4ADFD2E 9D9C88A9 CC75AF94 DD641890

y_QsU =   00000079 9A1C41C5 C6D1E088 22BB9EEE 33D46CA4 11520DD5
          48707760 4FC8C0A6 1E8EF027 C1265508 2F3515AE 720F2547
          0204B516 8E8A7709 73D2F3ED 28118C3D 0E752D6C

dsV   =   000001EB A74AC4A9 5404E9AC D5C50387 17C424BF 109512BF
          B793C943 0EB01D35 9BF6DDF8 A253774A BAD5FF6E 7359AC91
          D82F60D2 B35ECF68 8435DC1F FC4EEFC3 CFF6945E

x_QsV =   000001D9 FFCD0889 3A9C0F03 5AF8B32D 28A5973E 7A8A52CD
          475BFB96 96C83A76 99A2C853 0263D6A1 C1D4FB8A DFA29950
          48E7AC9A 29476114 44F17327 4EE7A0A2 48DFCCEA

y_QsV =   000001CC 7A1E6270 22B8538E 47E83DE4 B7B6F26A E9C02B44
          2E18B56A 594E46C9 DD11533B FDC4A5F2 2D16BA75 2B7C031D
          E3538662 AAA6D892 229D1CCE 04F6104E CAB09A71
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   000001C2 C11303BF B25D9513 64A605A2 DE0CBBC1 71D01B6D
          98C224AF 0E5EBC01 91E7FBBA 5EAFC942 D676F83E 0929D40D
          BEE86EA6 8A52BFA6 23421AC3 9416B987 D6633F47

x_QeU =   0000013D 1BD3C75A 39714992 0BF9B911 55366AAE 16C6F031
          8B2582D6 4144B797 63664B77 7A03A0DC 024616AC 2E3E2BCA
          156164BE 0D2B3405 CB5A08C1 EEF6CD84 CB95BE19
```

```
y_QeU =   000000EE 3728AD4A 2CC34A39 1F6339E2 73A30A94 D91D3165
          BBDCECB0 34BC36CF FDFB9302 417BA5BF 63675C51 18E925B7
          2BBD4879 C9827579 BEBB2A9D E3F4F9BC E82447DC

deV   =   00000054 81662A80 C30CF751 EE5600C7 59B821F8 63738CF6
          A9765FFD 77E47BC3 F6E02ECA 1A467D1C AD965913 3E0E54DD
          0D64167A 606E7589 CB229DB0 EF4ACE86 8DFEDA13

x_QeV =   000001CA 6F95A11C 9AEB0C20 037B0245 CB93671C AE6B37D1
          48A082B7 3D65B0A6 A1B957A0 CD8DB5EF FF266A03 1C6B2E61
          DCB27A26 F2BB1FA7 AD3132C9 7540ACF6 4504C185

y_QeV =   0000018E 700D34A9 16BF5A78 A57CBDCA F4161806 7FBEC8E9
          F5903A9F 3140BF20 3EF62C81 D2C79569 58A5EA4F A1BD94AA
          353D9C59 5AD036B4 FB350F04 62DD7034 75C20F0C
```

- Step 2: N/A.
- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     22957812197690408971137782402672883511501590179227
          50430693269498109544831833409768031123582141918027
          73833597827107352205217682039970986876055397845238
          4325209

Z_s =     000000AB 3A28D976 265945DD 4752E525 7E7E4156 7EFBC252
          B1201F45 0544FBA4 D089D689 F2D54CBB FC744D3F 5AD4E63A
          106B1B7B 0E8972C0 FC3EA819 F5FFE338 E7F69E59
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     11081870712183046638712496567202133795315757098946
          61690912451193888110240144525462578978083781622967
          26129774771013467690317983759367319116447333004512
          9720048
```

```
Z_e =     00000052 A70191FD DCBAB459 2BF198A6 31325A3D B41EA93A
          C3FE86A3 9AE2F49F 19BF5FDD 60A0DE62 D37C033B B34C201C
          B3BF44C1 CAE44302 9F54A86E 1FA030FE 4FEA00F0
```

- Step 5: Shared secret.

```
Z =       0052A701 91FDDCBA B4592BF1 98A63132 5A3DB41E A93AC3FE
          86A39AE2 F49F19BF 5FDD60A0 DE62D37C 033BB34C 201CB3BF
          44C1CAE4 43029F54 A86E1FA0 30FE4FEA 00F000AB 3A28D976
          265945DD 4752E525 7E7E4156 7EFBC252 B1201F45 0544FBA4
          D089D689 F2D54CBB FC744D3F 5AD4E63A 106B1B7B 0E8972C0
          FC3EA819 F5FFE338 E7F69E59
```

- Step 6: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = A05EE64A 63186A85 880BE4BD B7B7059D ACFCBBDB 529B4202
             2F4E93DC 52E4B1EC 195D9275 6499E68E 707CD0E1 F1033EEE
             74071F8B 2ABD7198 54403300 11AE448D 6389D76F F2465AE7
             35D20AF4 BA6EDB1D 6CD00693 4556D6B2 D0DAD17B 92284191
             AF7CEACA EC1304B4 61908D91 F4BCCFE0 1EDA976C D50A035E
             872E5CAB 10261E7D
```

- If key confirmation is performed, then

```
MacKey  = A05EE64A 63186A85 880BE4BD B7B7059D ACFCBBDB 529B4202
          2F4E93DC 52E4B1EC
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 013D1BD3 C75A3971
            49920BF9 B9115536 6AAE16C6 F0318B25 82D64144 B7976366
            4B777A03 A0DC0246 16AC2E3E 2BCA1561 64BE0D2B 3405CB5A
```

```
              08C1EEF6 CD84CB95 BE1900EE 3728AD4A 2CC34A39 1F6339E2
              73A30A94 D91D3165 BBDCECB0 34BC36CF FDFB9302 417BA5BF
              63675C51 18E925B7 2BBD4879 C9827579 BEBB2A9D E3F4F9BC
              E82447DC 01CA6F95 A11C9AEB 0C20037B 0245CB93 671CAE6B
              37D148A0 82B73D65 B0A6A1B9 57A0CD8D B5EFFF26 6A031C6B
              2E61DCB2 7A26F2BB 1FA7AD31 32C97540 ACF64504 C185018E
              700D34A9 16BF5A78 A57CBDCA F4161806 7FBEC8E9 F5903A9F
              3140BF20 3EF62C81 D2C79569 58A5EA4F A1BD94AA 353D9C59
              5AD036B4 FB350F04 62DD7034 75C20F0C

    MacTag_U  = E87EF864 A83E2A99 9F8C0AAC DDC01A3B 338D83E0 7B255441
                FBEDA06E 253AD771 80625575 CE5EE01D 34B6A7EB BEC7121A
                ABDB63E0 D03DE7BA 9C79DE2E 5B65B5C5
```

- If UNILATERAL key confirmation provided by V to U, then

```
   MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

             = 4B435F31 5F56424F 42425941 4C494345 01CA6F95 A11C9AEB
               0C20037B 0245CB93 671CAE6B 37D148A0 82B73D65 B0A6A1B9
               57A0CD8D B5EFFF26 6A031C6B 2E61DCB2 7A26F2BB 1FA7AD31
               32C97540 ACF64504 C185018E 700D34A9 16BF5A78 A57CBDCA
               F4161806 7FBEC8E9 F5903A9F 3140BF20 3EF62C81 D2C79569
               58A5EA4F A1BD94AA 353D9C59 5AD036B4 FB350F04 62DD7034
               75C20F0C 013D1BD3 C75A3971 49920BF9 B9115536 6AAE16C6
               F0318B25 82D64144 B7976366 4B777A03 A0DC0246 16AC2E3E
               2BCA1561 64BE0D2B 3405CB5A 08C1EEF6 CD84CB95 BE1900EE
               3728AD4A 2CC34A39 1F6339E2 73A30A94 D91D3165 BBDCECB0
               34BC36CF FDFB9302 417BA5BF 63675C51 18E925B7 2BBD4879
               C9827579 BEBB2A9D E3F4F9BC E82447DC

    MacTag_V  = 7488881D 12D0CE80 7699626C B61329F3 79A4E7A3 DBE1994B
                E2577E2F F4928419 3D26C3D8 5EA8DA7F 90A404ED 5F8044F4
                4E92486E 23E70CC1 CAB40EFD 83975404
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 013D1BD3 C75A3971
            49920BF9 B9115536 6AAE16C6 F0318B25 82D64144 B7976366
            4B777A03 A0DC0246 16AC2E3E 2BCA1561 64BE0D2B 3405CB5A
            08C1EEF6 CD84CB95 BE1900EE 3728AD4A 2CC34A39 1F6339E2
            73A30A94 D91D3165 BBDCECB0 34BC36CF FDFB9302 417BA5BF
            63675C51 18E925B7 2BBD4879 C9827579 BEBB2A9D E3F4F9BC
            E82447DC 01CA6F95 A11C9AEB 0C20037B 0245CB93 671CAE6B
            37D148A0 82B73D65 B0A6A1B9 57A0CD8D B5EFFF26 6A031C6B
            2E61DCB2 7A26F2BB 1FA7AD31 32C97540 ACF64504 C185018E
            700D34A9 16BF5A78 A57CBDCA F4161806 7FBEC8E9 F5903A9F
            3140BF20 3EF62C81 D2C79569 58A5EA4F A1BD94AA 353D9C59
            5AD036B4 FB350F04 62DD7034 75C20F0C

 MacTag_U  = BEBE3E67 AF230F50 02EEDCF4 7982FDAB B7D0C8C2 E4EFD9DE
            3F542F86 8CDA7909 A957C6C8 CD4FDC62 A734DC4D 4C7B79CD
            DA8B8D72 04CEACEB A61DB245 812439F8

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 01CA6F95 A11C9AEB
            0C20037B 0245CB93 671CAE6B 37D148A0 82B73D65 B0A6A1B9
            57A0CD8D B5EFFF26 6A031C6B 2E61DCB2 7A26F2BB 1FA7AD31
            32C97540 ACF64504 C185018E 700D34A9 16BF5A78 A57CBDCA
            F4161806 7FBEC8E9 F5903A9F 3140BF20 3EF62C81 D2C79569
            58A5EA4F A1BD94AA 353D9C59 5AD036B4 FB350F04 62DD7034
            75C20F0C 013D1BD3 C75A3971 49920BF9 B9115536 6AAE16C6
            F0318B25 82D64144 B7976366 4B777A03 A0DC0246 16AC2E3E
            2BCA1561 64BE0D2B 3405CB5A 08C1EEF6 CD84CB95 BE1900EE
            3728AD4A 2CC34A39 1F6339E2 73A30A94 D91D3165 BBDCECB0
            34BC36CF FDFB9302 417BA5BF 63675C51 18E925B7 2BBD4879
            C9827579 BEBB2A9D E3F4F9BC E82447DC

 MacTag_V  = D3C2ABEF CB488B79 0FE7D377 05DB2F36 0F5807C1 01E3D253
            E45863A9 0BE43EB8 D171985C FD923D66 06124750 B4FFFEC4
            A4648E25 E40A4D90 5EC15A9F E301DD76
```

5.6.2 Full MQV for curve P–521

- Prerequisites:

```
dsU   =   0000005A 3795FC8D 92CEA6FD 15DEA79E 796497DC 05D57C0C
          F2BC5473 FF77C726 5B9B8AB7 6C416C01 C3D53DCE 55714F3E
          54A6EA82 CF0FEFB6 919AC3F4 FE538260 C075E4D3

x_QsU =   00000093 8EB5EFCE 65AAD90C 28A53493 896B18C4 43BFE3DB
          54BAFA12 5533D938 91B58217 80412178 151C67DF C55F5714
          44104E2A 56E6B4B1 8A1BB571 D17B51FB D9005B6A

y_QsU =   F2456188 7108F85C 752EC1D9 06CFA0E4 0AF13716 923C9F40
          CB9979C2 E7B5B1E9 A2337657 856C5D9B 82892947 9387F4FC
          B2C4B2B5 9D701415 DD84A396 911AB2D8

dsV   =   000000C3 385DE841 9FE3C365 4981A48A EA7FB3F0 6BA58E46
          0B01FE67 268773BD C68F38A0 6AE0BE3E 18F29033 CE1B816C
          C5919CB2 57B55E24 042E1E67 2EA4105B 03792677

x_QsV =   00000029 D32BC75F 6052EBB9 3300718A 254F7967 367A29F5
          723B53DA DA1971B1 D946DBAE BE3E33B9 1FDC4A81 93F073D9
          AC91BBC4 30E3706C CFED78CA 36984CD6 AB9D8C79

y_QsV =   0000003F 2E13598A 80C10282 5E55D699 D41EF235 F1778584
          ADA86DC1 A5F9CEDE 4DF4931F 91FB9071 C17B1A18 FEB550C5
          01FDFB57 DDF3D5E1 52B31469 24995FB3 676FC63C
```

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   000000FB 2FA87E37 97DB5DE9 ED4686D1 54535B29 59C68F3B
          E981C31C 0E6559E5 1188FFBB 0AA3A71F FA36FE9F 7D2B20F1
          4F69E3E2 31757FBE B8FA2610 C8D0020D 68BD86FE

x_QeU =   00000037 F0D60FFA B85E97B4 07C7BDC4 C3FB1214 2D1815A3
          19E0E476 4D09AE20 2321E509 2C43D04F 12D60AAB D68CD591
          CE731FE5 1026F3B0 32CB4D43 80B75C6A A76E63E7
```

```
y_QeU =   00000189 D4A3E48F 7E506D13 933DC54C D631416A 6314AECF
          CE75AECE 7184D83F F4B71377 EC537D34 2781411A 81B1D721
          2F3120A3 497F4EBA 3C16D970 63F1C2F7 2AB425D8

deV   =   00000074 F3C48B15 8D43AD57 F04CE1D9 07E9F021 BEC6CE7C
          18FD42A5 451E2ADD A9CDBA7E 6694FB20 69757BC9 E784E0F0
          E5E542B6 6B6BF9B8 20455459 71912ABC 17C3C3D3

x_QeV =   00000143 9D71B428 A158388B 79B3E438 97BA888A 7BB134D3
          D4EDD32C F9EC4D63 BA493679 E30B6AEF 14BA7602 13163B26
          F9174830 71A944E0 FE64681A 94483FD5 53A1387C

y_QeV =   000001EB 5330A787 0B9E31DE 611B4770 99509D2E DEB4A166
          F432088F 3248814C 7AE541BB 3DDE4C40 4C65581E 8B105C64
          BF0A2C2C 553EF2BE 5034F143 9E260E70 7E0BC547
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       65435760788001190710902894386964732334050135063436
          04426874581661631542456189152522235213665802108222
          75442909651237857229165636792493718610246064301777
          1352773
```

- Step 4: Shared secret converted to byte string.

```
Z =       000001E8 0ACD9DE1 A379C5C4 4B74E0F4 06270376 AA3EC09F
          0A4DA70B E4F9F34A 2A5B8831 415D4138 A122BA6C 70E83C65
          8C5D04DE 202FA510 18A105B7 F5109CF4 2D9E82C5
```

- Step 5: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerKeyMat  = EE980D40 1652541F 1C93E866 041D968D 93797ED2 76D33D96
             76ED672A 2928252D 2F234551 FC70A4C9 89AFFBB5 0FB45CC0
             06416D77 E08B9FD4 7BE7E0AE DCE3EB66 AD8935C7 28D23E94
             EC6CA2DF 49CAD406 EB6091B1 1974B773 7E364E79 37D4E381
             55C77550 13656733 0CF93139 E743A4F5 7705487D C8744F25
             0787296F B5EFC6D6
```

- If key confirmation is performed, then

```
MacKey  = EE980D40 1652541F 1C93E866 041D968D 93797ED2 76D33D96
          76ED672A 2928252D
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 0037F0D6 0FFAB85E
            97B407C7 BDC4C3FB 12142D18 15A319E0 E4764D09 AE202321
            E5092C43 D04F12D6 0AABD68C D591CE73 1FE51026 F3B032CB
            4D4380B7 5C6AA76E 63E70189 D4A3E48F 7E506D13 933DC54C
            D631416A 6314AECF CE75AECE 7184D83F F4B71377 EC537D34
            2781411A 81B1D721 2F3120A3 497F4EBA 3C16D970 63F1C2F7
            2AB425D8 01439D71 B428A158 388B79B3 E43897BA 888A7BB1
            34D3D4ED D32CF9EC 4D63BA49 3679E30B 6AEF14BA 76021316
            3B26F917 483071A9 44E0FE64 681A9448 3FD553A1 387C01EB
            5330A787 0B9E31DE 611B4770 99509D2E DEB4A166 F432088F
            3248814C 7AE541BB 3DDE4C40 4C65581E 8B105C64 BF0A2C2C
            553EF2BE 5034F143 9E260E70 7E0BC547

MacTag_U  = 759D4340 2D5E8050 1F35E340 606D6CF1 007627BF 33EEAE10
            D77F82D9 C4302C02 3C41B015 77252EE8 32E2DF15 7B24A75A
            7BC92EF4 801F63C7 E3249D25 F844FC9A
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U
```

```
          = 4B435F31 5F56424F 42425941 4C494345 01439D71 B428A158
            388B79B3 E43897BA 888A7BB1 34D3D4ED D32CF9EC 4D63BA49
            3679E30B 6AEF14BA 76021316 3B26F917 483071A9 44E0FE64
            681A9448 3FD553A1 387C01EB 5330A787 0B9E31DE 611B4770
            99509D2E DEB4A166 F432088F 3248814C 7AE541BB 3DDE4C40
            4C65581E 8B105C64 BF0A2C2C 553EF2BE 5034F143 9E260E70
            7E0BC547 0037F0D6 0FFAB85E 97B407C7 BDC4C3FB 12142D18
            15A319E0 E4764D09 AE202321 E5092C43 D04F12D6 0AABD68C
            D591CE73 1FE51026 F3B032CB 4D4380B7 5C6AA76E 63E70189
            D4A3E48F 7E506D13 933DC54C D631416A 6314AECF CE75AECE
            7184D83F F4B71377 EC537D34 2781411A 81B1D721 2F3120A3
            497F4EBA 3C16D970 63F1C2F7 2AB425D8

MacTag_V  = 21457053 1BA97D61 DEDED7C2 CD3651FB FB650960 52AA424D
            90102764 E3FD5ED8 0A8162C0 1E0CB218 8AA5C4FF C5CBCF1D
            56B4526C F2859461 4BE7FF13 E0D9E427
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 0037F0D6 0FFAB85E
            97B407C7 BDC4C3FB 12142D18 15A319E0 E4764D09 AE202321
            E5092C43 D04F12D6 0AABD68C D591CE73 1FE51026 F3B032CB
            4D4380B7 5C6AA76E 63E70189 D4A3E48F 7E506D13 933DC54C
            D631416A 6314AECF CE75AECE 7184D83F F4B71377 EC537D34
            2781411A 81B1D721 2F3120A3 497F4EBA 3C16D970 63F1C2F7
            2AB425D8 01439D71 B428A158 388B79B3 E43897BA 888A7BB1
            34D3D4ED D32CF9EC 4D63BA49 3679E30B 6AEF14BA 76021316
            3B26F917 483071A9 44E0FE64 681A9448 3FD553A1 387C01EB
            5330A787 0B9E31DE 611B4770 99509D2E DEB4A166 F432088F
            3248814C 7AE541BB 3DDE4C40 4C65581E 8B105C64 BF0A2C2C
            553EF2BE 5034F143 9E260E70 7E0BC547

MacTag_U  = 734779ED 95DE7B6F DBCEFAE4 A707B33B 2EE58EC3 E057DE32
            81162E22 BC6E4339 6E046D95 74493F8B F510C50A 82C29EB3
            BD0FBFDC 5B5F45B5 33612F2D 4A6ED19F
```

```
MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 01439D71 B428A158
            388B79B3 E43897BA 888A7BB1 34D3D4ED D32CF9EC 4D63BA49
            3679E30B 6AEF14BA 76021316 3B26F917 483071A9 44E0FE64
            681A9448 3FD553A1 387C01EB 5330A787 0B9E31DE 611B4770
            99509D2E DEB4A166 F432088F 3248814C 7AE541BB 3DDE4C40
            4C65581E 8B105C64 BF0A2C2C 553EF2BE 5034F143 9E260E70
            7E0BC547 0037F0D6 0FFAB85E 97B407C7 BDC4C3FB 12142D18
            15A319E0 E4764D09 AE202321 E5092C43 D04F12D6 0AABD68C
            D591CE73 1FE51026 F3B032CB 4D4380B7 5C6AA76E 63E70189
            D4A3E48F 7E506D13 933DC54C D631416A 6314AECF CE75AECE
            7184D83F F4B71377 EC537D34 2781411A 81B1D721 2F3120A3
            497F4EBA 3C16D970 63F1C2F7 2AB425D8

MacTag_V  = 07F6B89A 2B768C4E 9E5BBEAC 39140E66 46419B4D D3B492E3
            1AC670B3 D000DA29 B06195B6 C33D0846 B10CAC77 6B5902BB
            F07F43FA 4273F405 2442EEF6 E5791EA8
```

5.6.3 Ephemeral Unified Model for curve P–521

- Step 1: U produces deU, QeU and receives QeV. U DOES NOT RECEIVE deV (shown only for the purpose of verifying this data).

```
deU   =   0000005D 814A4477 8554AC22 F99CCEEA 849A84E6 D9D2294C
          5CB5C65E 0883194D 1978C21E 236A2C7A AE425E1A C0F3DB00
          BC356519 74853729 99AEDA53 2BE5BD7A FD319370

x_QeU =   000001EE 0381337A F5B437AD 414E60D4 9681B81C 035AD5E4
          E44B6B69 7A02F894 0A8BA8EA 3C9B7E25 FD0A85BB 108F0F44
          994CF58C 4B3005AE 205A110A 36ED971E D51D7180

y_QeU =   0000010F C5252109 1E83E94C DB494482 3427B734 470DA66A
          06C8567F BC511BFC DC2B24D8 ECC6DA76 BA125C01 B5985439
          126E785D 1B30AF77 7987C08A 466FDC10 2723DF55
```

```
deV   =   000001F6 6BAC6B8F 8A18B144 9EEB60A8 27E68C02 8C099F5A
          45982459 916BB14A 1CF990DC 42A27D33 D74207D5 4C4C64FF
          747F97D4 52BD775F 5F515E79 B8E8C8ED B691FFFA

x_QeV =   0000014E 1C22331C 606E016E 2F8B5A99 D9820C7C E30CDBCD
          B0A06D03 3BDC2A71 213654AE D4F6311B 3AAFA713 A68743A7
          761ECDBE 15AF1BCC 6B1DA4EC 75B62193 9D2AD938

y_QeV =   000000B9 1534952C E7BDB189 253C2B66 22E97A77 D2B13C45
          6ABB952B FDB604CB C5CAD319 D53E9EE9 D785464C B18159DD
          31BEB019 C79A7148 534EF2BF 2F48357D 63A790E8
```

- Step 2: N/A.
- Step 3: Decimal value of shared secret.

```
Z =       65560585252111253009882654696256902830407009540069
          19556406780084270249631704347018296764597543578465
          76421769024791220238648525507689835024346409801803
          7381796
```

- Step 4:

```
Z =       000001E8 F9228B38 FFD25CA8 7FAE88D6 C16BC786 AE397771
          1CCBA6D5 4EE9C162 3D948F49 ACDD92E6 BC97C2B3 1D70F88A
          55A8DF3E 808DDFE4 3DA0DFCC 930FE8C9 E6C0BAA4
```

- Step 5: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 26F9D22A 96E275E7 03C0CF26 2CAC1BCB 201021B0 65FADFB3
             E38FF58C CAFBE3F0 CB3B1FDA 82549D05 A7F8559F E3C0B037
             A5C20129 AC575DDD 14E2FB87 E3DBC38A 03FCAEC8 3CCCBC9E
             C5718386 09AA6F47 B6CF292A A45F4A34 DEB1B938 6786E776
             4DC2BF39 D4DFE67D B90E65D5 03A46D01 C757D87D DEAF9547
             FB4CAD00 CB891430
```

5.6.4 One–Pass Unified Model for curve P–521

- Prerequisites:

```
dsU   =   0000013E 90DE6C9F 5BC2A794 5DD9FCC5 79AF8889 2B84FB25
          63CACFC8 A8EEE659 6F051C6D 3B291146 1E82D82F B7F595D5
          027EFF4C 8227C77D 7AE7C8F5 2D491334 34BC3328

x_QsU =   00000023 323AF012 A59DCF5D 7067CC24 266CA221 FE03B21B
          F6413748 9DCE9B75 1D24E5C2 5F6A04A9 661C45D5 EC18BC88
          42104F68 861D4C54 9646E881 D1A4AEDD D93055B2

y_QsU =   00000135 FE0990BA E5ADA743 34ED61EC B8708FFF 2E9550C0
          DE7F0DD5 07D6487A 95ABEDCF A0C07A9E 0A535AB7 2755A93A
          BC48435B 1C82DB3A 833FCED5 7D754F23 F9783AA4

dsV   =   000000E5 454D525C E930EF29 1A43B205 CEF47AF6 82A9F7C4
          11B6FDB2 8DC0799B E5B5FBAF 1E042296 63FD004D BD9B0877
          64EB290B 2A40AEB5 538A35AA 1E760051 07D9C723

x_QsV =   00000135 BB02CA76 01239D39 82CD1B89 733C4381 86E61950
          1C70C43D A7C5A5B3 138A5C3E 46EDA858 3138F4A5 6C7A4E2C
          1F871902 E4DFC682 15A04807 20D66357 D48705C8

y_QsV =   0000012F 2EF9053F DCD86191 1F04F899 7AEA24FA 4791FB76
          4B088051 1ECCA0AF 6E68150D 6526612F FFE077AE 8813DC36
          772F5D51 9F4A11AD A4941768 D0BB77D4 30FC0B2F
```

BEGIN U's calculations

- Step 1:

```
deU   =   000000DF A0A19A7A B8A42B2D EC82D267 48D2DD78 CC78A4D9
          D7F045FF 8DC94060 EB8D03E8 70CCD96D 3C379FB4 55B0D945
          6A397F35 5EA496D7 9493A8E5 15C1D992 6CC4A9C1
```

```
x_QeU =   0000002D 68FD7E34 F6BBEEE5 88B7C0A7 8A195291 DDBDFF99
          3043EAE4 CEE81098 089B4B5C 298C5217 0DC40027 C25E7379
          44F518EC 8E1028B0 76A2A5B0 9C80DE2D CB1BC87F

y_QeU =   00000116 CB1F2255 CE071B0D B4E79C2B A5A2A3EA 9DCA8D2A
          A9A13900 2226AE92 82CF26D3 EEB75305 C0273F04 67085294
          C45A104E 2420364D 6DF59DF6 2C603F51 820FF5EF
```

- Step 2: Decimal and hex values for static shared secret.

```
Z_s =     41156388382507032178210764689029869271749787862223
          76789413128933349574263584525032718560604930056790
          12799094389930623472440361604221706559901504782834
          678853

Z_s =     0000001E B2225BFF 0D4F692A 121E86D8 6A4079E0 87337C67
          1CF06B61 BAE605A2 51E1D7C5 672BFB2A 8730C59C C8B45C71
          16989744 12C6009F 57F9F52B 973C9828 EDC93C45
```

- Step 3: Decimal and hex values for ephemeral shared secret.

```
Z_e =     31530950554056153646409282847677499098458267871338
          03183321214083872964970536946999256352204631473690
          80491216528733786736714405957158987333520281817289
          1318234

Z_e =     000000EB 2B279675 47E7D8CD 21C4F393 FBE254BA 876D5AA4
          51480402 D2BB684A 7F8E7070 EE73F111 F7C4060A 6F625301
          C59887C3 0D77A3AF 2922CEDD 62DB4B8B 9DAA47DA
```

- Step 4: Shared secret.

```
Z =       00EB2B27 967547E7 D8CD21C4 F393FBE2 54BA876D 5AA45148
          0402D2BB 684A7F8E 7070EE73 F111F7C4 060A6F62 5301C598
          87C30D77 A3AF2922 CEDD62DB 4B8B9DAA 47DA001E B2225BFF
          0D4F692A 121E86D8 6A4079E0 87337C67 1CF06B61 BAE605A2
          51E1D7C5 672BFB2A 8730C59C C8B45C71 16989744 12C6009F
          57F9F52B 973C9828 EDC93C45
```

- Step 5: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 0C333976 30378889 55AF43FD 5E764804 562979E0 D48154BA
             3746923B 04B5322E 5207E51F 5E4D3087 D5151DB0 D764A308
             516E9FC4 3D999B4B 02004B23 942E59CB 8466176A 66E93C75
             0977AC60 A1915723 1A17F78A 88B3C313 3F3CC5D6 C462BFD0
             B6AEA9F5 00597E30 6BBA0F94 7E143296 473E651D 7CB8E61D
             9062BEEA EEB888AF
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   000000DF A0A19A7A B8A42B2D EC82D267 48D2DD78 CC78A4D9
          D7F045FF 8DC94060 EB8D03E8 70CCD96D 3C379FB4 55B0D945
          6A397F35 5EA496D7 9493A8E5 15C1D992 6CC4A9C1

x_QeU =   0000002D 68FD7E34 F6BBEEE5 88B7C0A7 8A195291 DDBDFF99
          3043EAE4 CEE81098 089B4B5C 298C5217 0DC40027 C25E7379
          44F518EC 8E1028B0 76A2A5B0 9C80DE2D CB1BC87F

y_QeU =   00000116 CB1F2255 CE071B0D B4E79C2B A5A2A3EA 9DCA8D2A
          A9A13900 2226AE92 82CF26D3 EEB75305 C0273F04 67085294
          C45A104E 2420364D 6DF59DF6 2C603F51 820FF5EF
```

- Step 2: N/A.

- Step 3: Decimal and hex values for static shared secret.

```
Z_s =     41156388382507032178210764689029869271749787862223
          76789413128933349574263584525032718560604930056790
          12799094389930623472440361604221706559901504782834
          678853
```

```
Z_s =     0000001E B2225BFF 0D4F692A 121E86D8 6A4079E0 87337C67
          1CF06B61 BAE605A2 51E1D7C5 672BFB2A 8730C59C C8B45C71
          16989744 12C6009F 57F9F52B 973C9828 EDC93C45
```

- Step 4: Decimal and hex values for ephemeral shared secret.

```
Z_e =     31530950554056153646409282847677499098458267871338
          03183321214083872964970536946999256352204631473690
          80491216528733786736714405957158987333520281817289
          1318234

Z_e =     000000EB 2B279675 47E7D8CD 21C4F393 FBE254BA 876D5AA4
          51480402 D2BB684A 7F8E7070 EE73F111 F7C4060A 6F625301
          C59887C3 0D77A3AF 2922CEDD 62DB4B8B 9DAA47DA
```

- Step 5: Shared secret.

```
Z =       00EB2B27 967547E7 D8CD21C4 F393FBE2 54BA876D 5AA45148
          0402D2BB 684A7F8E 7070EE73 F111F7C4 060A6F62 5301C598
          87C30D77 A3AF2922 CEDD62DB 4B8B9DAA 47DA001E B2225BFF
          0D4F692A 121E86D8 6A4079E0 87337C67 1CF06B61 BAE605A2
          51E1D7C5 672BFB2A 8730C59C C8B45C71 16989744 12C6009F
          57F9F52B 973C9828 EDC93C45
```

- Step 6: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 0C333976 30378889 55AF43FD 5E764804 562979E0 D48154BA
             3746923B 04B5322E 5207E51F 5E4D3087 D5151DB0 D764A308
             516E9FC4 3D999B4B 02004B23 942E59CB 8466176A 66E93C75
             0977AC60 A1915723 1A17F78A 88B3C313 3F3CC5D6 C462BFD0
             B6AEA9F5 00597E30 6BBA0F94 7E143296 473E651D 7CB8E61D
             9062BEEA EEB888AF
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  =  C333976 30378889 55AF43FD 5E764804 562979E0 D48154BA
           3746923B 04B5322E

nonceV =  7402249A 6068975D F4E95B5F 88543FEA BABBE5AD A7EF7179
          4852849E F4D417C6 EE91361F 7269296C 15C0073E AD92856F
          F13361DC D4C0E850 756A8A54 B54AAFEC
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 002D68FD 7E34F6BB
            EEE588B7 C0A78A19 5291DDBD FF993043 EAE4CEE8 1098089B
            4B5C298C 52170DC4 0027C25E 737944F5 18EC8E10 28B076A2
            A5B09C80 DE2DCB1B C87F0116 CB1F2255 CE071B0D B4E79C2B
            A5A2A3EA 9DCA8D2A A9A13900 2226AE92 82CF26D3 EEB75305
            C0273F04 67085294 C45A104E 2420364D 6DF59DF6 2C603F51
            820FF5EF 7402249A 6068975D F4E95B5F 88543FEA BABBE5AD
            A7EF7179 4852849E F4D417C6 EE91361F 7269296C 15C0073E
            AD92856F F13361DC D4C0E850 756A8A54 B54AAFEC

MacTag_U  = 1CFC7274 59CF0F44 C2144D13 687723ED 48A18739 B570C047
             2A91EF0A C8827569 E654773D 81800EF6 A3C70471 107198A5
             1C6568BC 425FE211 937758D9 A248AF5C
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 002D68FD 7E34F6BB
            EEE588B7 C0A78A19 5291DDBD FF993043 EAE4CEE8 1098089B
            4B5C298C 52170DC4 0027C25E 737944F5 18EC8E10 28B076A2
            A5B09C80 DE2DCB1B C87F0116 CB1F2255 CE071B0D B4E79C2B
            A5A2A3EA 9DCA8D2A A9A13900 2226AE92 82CF26D3 EEB75305
            C0273F04 67085294 C45A104E 2420364D 6DF59DF6 2C603F51
            820FF5EF
```

```
MacTag_V  = F0093D84 CD421F9B 5D332932 29EDFB10 39AFCC70 25C65E9F
            5E7227C0 030B0DB2 3C2806AC C9E3DD4F 4F8C5D24 78B32903
            6B644975 1476DD78 560B8BD0 26CE1A93
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 002D68FD 7E34F6BB
            EEE588B7 C0A78A19 5291DDBD FF993043 EAE4CEE8 1098089B
            4B5C298C 52170DC4 0027C25E 737944F5 18EC8E10 28B076A2
            A5B09C80 DE2DCB1B C87F0116 CB1F2255 CE071B0D B4E79C2B
            A5A2A3EA 9DCA8D2A A9A13900 2226AE92 82CF26D3 EEB75305
            C0273F04 67085294 C45A104E 2420364D 6DF59DF6 2C603F51
            820FF5EF 7402249A 6068975D F4E95B5F 88543FEA BABBE5AD
            A7EF7179 4852849E F4D417C6 EE91361F 7269296C 15C0073E
            AD92856F F13361DC D4C0E850 756A8A54 B54AAFEC

MacTag_U  = 16ED1020 888F1714 BD75F59F 24CB691F 4EB8969B F1D7444D
            DAE634EC 07553ABF 6702F1AB D29C22CC A90C7EC3 B47CB98B
            30D48325 58A7D454 67266206 4399BA89

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 7402249A 6068975D
            F4E95B5F 88543FEA BABBE5AD A7EF7179 4852849E F4D417C6
            EE91361F 7269296C 15C0073E AD92856F F13361DC D4C0E850
            756A8A54 B54AAFEC 002D68FD 7E34F6BB EEE588B7 C0A78A19
            5291DDBD FF993043 EAE4CEE8 1098089B 4B5C298C 52170DC4
            0027C25E 737944F5 18EC8E10 28B076A2 A5B09C80 DE2DCB1B
            C87F0116 CB1F2255 CE071B0D B4E79C2B A5A2A3EA 9DCA8D2A
            A9A13900 2226AE92 82CF26D3 EEB75305 C0273F04 67085294
            C45A104E 2420364D 6DF59DF6 2C603F51 820FF5EF

MacTag_V  = 90B955A1 AFCB61E5 D04D2152 A4AAFEED D65448E8 55CFFD89
            9BF59586 F8194F53 B99CA9AB 68F05294 A4338D07 F6F7564D
            86225888 4A051DCB AED96BC3 7A6F0F6A
```

5.6.5 One–Pass MQV for curve P–521

- Prerequisites:

```
dsU   =   000001EA C98F9F1D 038F9968 35D780A1 03A2CF31 FB428D04
          9BB2675A D33E6429 43CDDB8F 9EF9D7D6 89AAD226 37BD0FBA
          8B4878C3 AEE9FADB F13AB212 E526113B F087711A

x_QsU =   00000197 E39BE273 0669A7AD 32916266 7A788A66 213611CB
          5F3A43CA 4A66D7DC 49DA28C9 8D40FDEB 087C9FEF 76E9F98C
          1D2EB689 08AEE694 A4EEBC4C 8E45371E CDFCF08D

y_QsU =   00000148 D7CD8671 941A4FBD 1522ED8F 75681590 D5B24EDC
          C0A8954F 4E90FAD3 87359153 6244A533 43E81276 4C02F473
          10ED294E 9E4D79E4 E431B1A6 8A589295 A8054B89

dsV   =   0000018E C7B5DA79 7BD87E09 3178C467 C6077223 27ED461F
          DA87C889 F8B8507E 14E92251 021C4AAC 4E2DCEE8 7520AE7D
          0AD72EF6 83190EC5 A1659984 4A084AE5 83953FA3

x_QsV =   000001F6 81A9A38F EAEBEB28 ACD9F1AD AA601B75 DF190AD9
          B35B01E7 DF0D8C8F A044032C CCB57D2E 641F028F 8F0F6707
          B3F0E7FD EC5F1D1F 3D98658C 47ECF012 22F20484

y_QsV =   000001B9 607B3B84 11FA8439 F29F341E 7B0DBEE1 1DE37AF8
          097D11B2 5A88E388 0D90B7FD E82A5AE8 6B7B7A63 01C741A4
          7860AA2A 944FF27E C09F6578 E4473C0B 06C51BEC
```

BEGIN U's calculations

- Step 1:

```
deU   =   00000113 E453F6AF 3D6352D7 748A44FE E45B88A8 31886E1A
          B7F92DC9 0DFA80DC 076B1328 217A1953 0DA36B60 5B029528
          107758C1 17EC795C 2962AF18 706EFF2E A0FE60C1
```

```
x_QeU =   000000AF FEE2C8D6 55D568AA 98726095 FD8E4293 EF94521F
          F55588F0 8EB7F783 F5AA02C7 678FAB62 D56BBED3 175E4D01
          571FC428 ADB0516C F6722928 C1A95E8C 478A7F17

y_QeU =   000000AC 8A726860 5E60EC02 DE6057AF 5D9BA465 1EE6BE89
          5651C51F 18456A62 FE72AEDD 4C23272C FCE57ACA 163181CC
          2A848DC0 5039FD23 5082EE74 2A562A6F ADC91F1C
```

- Step 2: Decimal value for shared secret.

```
Z =       56405340331302193858802304342930712176307927518537
          14694122314451707014573580257846344338994725702747
          25654106937414123860809606907366426849229462201952
          4977223
```

- Step 3: Hex value for shared secret.

```
Z =       000001A4 B0B40B35 98563D15 903DDC9F 71893CA3 E393A507
          295E853A 86EF4026 E044FB84 8A5ADBA7 31ABB994 C69FCDA2
          27E45F86 6ECB6D5D DF3EE0C0 252BA430 347B6247
```

- Step 4: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = A3EC4BCC 4BE9ECA7 A827415E 33E99903 83E97716 960041F2
             B064D6B7 56F426BE 2AA7D3CC 1C206CDA 1840EE13 15E503B7
             DE6AC328 F8BFCF4C 21BFA7C1 69FF3B9B 3D947A8A 3E063249
             34C0BAEA A3858069 0CDBC3DA B3EB594B A56AC649 F5798147
             FB194E39 B10C6C03 6A79FBAC E34F9B1B F2EE1312 72564892
             165E0527 671F6C4E
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   00000113 E453F6AF 3D6352D7 748A44FE E45B88A8 31886E1A
          B7F92DC9 0DFA80DC 076B1328 217A1953 0DA36B60 5B029528
          107758C1 17EC795C 2962AF18 706EFF2E A0FE60C1

x_QeU =   000000AF FEE2C8D6 55D568AA 98726095 FD8E4293 EF94521F
          F55588F0 8EB7F783 F5AA02C7 678FAB62 D56BBED3 175E4D01
          571FC428 ADB0516C F6722928 C1A95E8C 478A7F17

y_QeU =   000000AC 8A726860 5E60EC02 DE6057AF 5D9BA465 1EE6BE89
          5651C51F 18456A62 FE72AEDD 4C23272C FCE57ACA 163181CC
          2A848DC0 5039FD23 5082EE74 2A562A6F ADC91F1C
```

- Step 2: N/A.
- Step 3: Decimal value for shared secret.

```
Z =       56405340331302193858802304342930712176307927518537
          14694122314451707014573580257846344338994725702747
          25654106937414123860809606907366426849229462201952
          4977223
```

- Step 4: Hex value for shared secret.

```
Z =       000001A4 B0B40B35 98563D15 903DDC9F 71893CA3 E393A507
          295E853A 86EF4026 E044FB84 8A5ADBA7 31ABB994 C69FCDA2
          27E45F86 6ECB6D5D DF3EE0C0 252BA430 347B6247
```

- Step 5: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = A3EC4BCC 4BE9ECA7 A827415E 33E99903 83E97716 960041F2
             B064D6B7 56F426BE 2AA7D3CC 1C206CDA 1840EE13 15E503B7
             DE6AC328 F8BFCF4C 21BFA7C1 69FF3B9B 3D947A8A 3E063249
             34C0BAEA A3858069 0CDBC3DA B3EB594B A56AC649 F5798147
             FB194E39 B10C6C03 6A79FBAC E34F9B1B F2EE1312 72564892
             165E0527 671F6C4E
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = A3EC4BCC 4BE9ECA7 A827415E 33E99903 83E97716 960041F2
          B064D6B7 56F426BE

nonceV =  B14FA184 9CB0A749 31F1F07A D0338409 ADEC3A55 6CE87E8A
          2D01DFA1 88630E1D F76FF8EE E87D5AB5 9A10C8BA 5AD61711
          8312A3A3 A02465D4 BFEA2E8F 1AD5AECF
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 00AFFEE2 C8D655D5
            68AA9872 6095FD8E 4293EF94 521FF555 88F08EB7 F783F5AA
            02C7678F AB62D56B BED3175E 4D01571F C428ADB0 516CF672
            2928C1A9 5E8C478A 7F1700AC 8A726860 5E60EC02 DE6057AF
            5D9BA465 1EE6BE89 5651C51F 18456A62 FE72AEDD 4C23272C
            FCE57ACA 163181CC 2A848DC0 5039FD23 5082EE74 2A562A6F
            ADC91F1C B14FA184 9CB0A749 31F1F07A D0338409 ADEC3A55
            6CE87E8A 2D01DFA1 88630E1D F76FF8EE E87D5AB5 9A10C8BA
            5AD61711 8312A3A3 A02465D4 BFEA2E8F 1AD5AECF

MacTag_U  = 9F075110 E0807517 D77E940A 97898F63 9FBBEA39 D37525CC
             7BFFF79C 0671DB1D 2855844A 92602977 DB0787B9 F1F72548
             0DB2FDAC A6B60694 E5067670 70557798
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 00AFFEE2 C8D655D5
            68AA9872 6095FD8E 4293EF94 521FF555 88F08EB7 F783F5AA
            02C7678F AB62D56B BED3175E 4D01571F C428ADB0 516CF672
            2928C1A9 5E8C478A 7F1700AC 8A726860 5E60EC02 DE6057AF
            5D9BA465 1EE6BE89 5651C51F 18456A62 FE72AEDD 4C23272C
            FCE57ACA 163181CC 2A848DC0 5039FD23 5082EE74 2A562A6F
            ADC91F1C
```

```
MacTag_V  = 3A7391D0 0F533486 B80311F9 BCF53922 3E9860BF 4AAFAF21
            619504CB FF81CD79 0FBD6AF5 DB38197B F7E9C552 1B8E5D87
            0CEB8660 B68AE19E E0F4F84E 432C52FE
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 00AFFEE2 C8D655D5
            68AA9872 6095FD8E 4293EF94 521FF555 88F08EB7 F783F5AA
            02C7678F AB62D56B BED3175E 4D01571F C428ADB0 516CF672
            2928C1A9 5E8C478A 7F1700AC 8A726860 5E60EC02 DE6057AF
            5D9BA465 1EE6BE89 5651C51F 18456A62 FE72AEDD 4C23272C
            FCE57ACA 163181CC 2A848DC0 5039FD23 5082EE74 2A562A6F
            ADC91F1C B14FA184 9CB0A749 31F1F07A D0338409 ADEC3A55
            6CE87E8A 2D01DFA1 88630E1D F76FF8EE E87D5AB5 9A10C8BA
            5AD61711 8312A3A3 A02465D4 BFEA2E8F 1AD5AECF

MacTag_U  = 0870247A 109ED222 AB4FEE4D 90CBE52D 70DB2F62 B8ED060F
            4D2EB921 6509C8B2 DC796F9D 7D254980 98AE811E D2AA8028
            3B26D64A F8551F22 7F478F4C 634D218F

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 B14FA184 9CB0A749
            31F1F07A D0338409 ADEC3A55 6CE87E8A 2D01DFA1 88630E1D
            F76FF8EE E87D5AB5 9A10C8BA 5AD61711 8312A3A3 A02465D4
            BFEA2E8F 1AD5AECF 00AFFEE2 C8D655D5 68AA9872 6095FD8E
            4293EF94 521FF555 88F08EB7 F783F5AA 02C7678F AB62D56B
            BED3175E 4D01571F C428ADB0 516CF672 2928C1A9 5E8C478A
            7F1700AC 8A726860 5E60EC02 DE6057AF 5D9BA465 1EE6BE89
            5651C51F 18456A62 FE72AEDD 4C23272C FCE57ACA 163181CC
            2A848DC0 5039FD23 5082EE74 2A562A6F ADC91F1C

MacTag_V  = 40FDAD43 1F015431 3BE65B46 C72C7893 43D78F46 C90D7A0F
            D4E52864 C61E4631 18060F8F 1C45948C 9478B8E1 14F4B497
            B26CC62A F1E1BB80 BE9328C4 A2AD318D
```

5.6.6 One–Pass Diffie–Hellman for curve P–521

- Prerequisites:

```
dsV   =   000001FF D89441FF C1519E4E E605F1C0 FB3FCFAC 4C06D6E5
          A5713EF9 E1D63586 E7167DEB D582F126 A8186013 6925E9B0
          ECAECB5D 351A307A 33E1C52D 853A7602 506DD91E

x_QsV =   00000152 B3E622DF C3B7C360 A492D208 5F4DE1DD 4A6FDB34
          A2A01481 E3805AC3 A28D052F 904FAE9A E7EB90B9 593B9065
          C3084CDD 89B794FE 52DC0FCC F3CCD651 E165D4FC

y_QsV =   0000006A 474E4B0E E9B89E78 BAB91A72 53D53549 165FE945
          27D4F7C8 6A430C20 234EA02F DABD55CA 77123743 CE155C7F
          9ACC377D 523BCAD1 5274CE12 A145A2EB 831F247D
```

BEGIN U's calculations

- Step 1:

```
deU   =   000000FE 8E6343B2 BD2CC25D BB6A5D5F B388D693 302290D3
          660DF443 4B940725 8E5A8496 EC106D76 19CEBF3D 3B5641C6
          8E3110BB C54302B1 99E26AF0 2B921E1B 0098C267

x_QeU =   000001E7 B356243D 3F8A9E0D 5B519326 9BFDF459 FDFDD035
          F94302DA 6BB6F5F1 38693874 1F7846A7 6B595D44 42BC6336
          7A37C9C7 D647FB8D 89D830B1 3061F106 BD818A90

y_QeU =   000001CC D3C71FA0 C8E224B3 CF0601EE 5DEFC290 12DCC433
          D09479D4 DCEC5673 5A4D5D2B 89BF4AA2 C1BD58B4 DBEFC048
          2F0B7179 40E6D174 9A0A90E5 93DC77ED E22626A0
```

- Step 2: Decimal value for shared secret.

```
Z =       6651532431705801097107196487294161751599959680388 9
          4264862248119424820525564877523782173217545670622 6
          5992802838001975703067019311360801326501755632968 5
          0881619
```

- Step 3: Hex value for shared secret.

```
Z =       000001F0 180D471C DA3D7631 F8269154 57F00618 7C4E0408
          D77595AD A0E84C15 40E4490B 5221CBBD E51F9C85 CEAC084F
          DB0A31DE 539C53EB 400F6C85 1C571617 86CCAC53
```

- Step 4: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 1CB0948D 7C800578 AAF11678 B186DBD6 EBE3BFAA 40A0D05F
             91217367 1DF524E3 69E387CF DFBA8B70 C3E82603 BD5057F8
             F0E8DFE6 72B375EF 8695DF1E ED081261 AF747F82 8EE2EB2A
             16329004 C0D0D4DF 73229EA9 21D93CB1 14493A88 4A1E3588
             407A979D B3303E3D 3301F5DC 44D3ABC0 DBF121E6 AEE61C38
             296DB77D 344C4BFE
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
deU   =   000000FE 8E6343B2 BD2CC25D BB6A5D5F B388D693 302290D3
          660DF443 4B940725 8E5A8496 EC106D76 19CEBF3D 3B5641C6
          8E3110BB C54302B1 99E26AF0 2B921E1B 0098C267

x_QeU =   000001E7 B356243D 3F8A9E0D 5B519326 9BFDF459 FDFDD035
          F94302DA 6BB6F5F1 38693874 1F7846A7 6B595D44 42BC6336
          7A37C9C7 D647FB8D 89D830B1 3061F106 BD818A90

y_QeU =   000001CC D3C71FA0 C8E224B3 CF0601EE 5DEFC290 12DCC433
          D09479D4 DCEC5673 5A4D5D2B 89BF4AA2 C1BD58B4 DBEFC048
          2F0B7179 40E6D174 9A0A90E5 93DC77ED E22626A0
```

- Step 2: N/A.

- Step 3: Decimal value for shared secret.

```
Z =       66515324317058010971071964872941617515999596803889
          42648622481194248205255648775237821732175456706226
          59928028380019757030670193113608013265017556329685
          0881619
```

- Step 4: Hex value for shared secret.

```
Z =       000001F0 180D471C DA3D7631 F8269154 57F00618 7C4E0408
          D77595AD A0E84C15 40E4490B 5221CBBD E51F9C85 CEAC084F
          DB0A31DE 539C53EB 400F6C85 1C571617 86CCAC53
```

- Step 5: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerKeyMat  = 1CB0948D 7C800578 AAF11678 B186DBD6 EBE3BFAA 40A0D05F
             91217367 1DF524E3 69E387CF DFBA8B70 C3E82603 BD5057F8
             F0E8DFE6 72B375EF 8695DF1E ED081261 AF747F82 8EE2EB2A
             16329004 C0D0D4DF 73229EA9 21D93CB1 14493A88 4A1E3588
             407A979D B3303E3D 3301F5DC 44D3ABC0 DBF121E6 AEE61C38
             296DB77D 344C4BFE
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = 1CB0948D 7C800578 AAF11678 B186DBD6 EBE3BFAA 40A0D05F
          91217367 1DF524E3
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U
```

```
          = 4B435F31 5F56424F 42425941 4C494345 01E7B356 243D3F8A
            9E0D5B51 93269BFD F459FDFD D035F943 02DA6BB6 F5F13869
            38741F78 46A76B59 5D4442BC 63367A37 C9C7D647 FB8D89D8
            30B13061 F106BD81 8A9001CC D3C71FA0 C8E224B3 CF0601EE
            5DEFC290 12DCC433 D09479D4 DCEC5673 5A4D5D2B 89BF4AA2
            C1BD58B4 DBEFC048 2F0B7179 40E6D174 9A0A90E5 93DC77ED
            E22626A0

MacTag_V  = A7420783 76CC3CE6 ADFCF749 0D7D3089 410DF417 F532661D
             A5E54D70 0B01F801 681E167C A01BD85C D8165CC7 13EBDBCA
             6B3C17E3 42F3B074 85D6A3EA F6DF5A3A
```

5.6.7 Static Unified Model for curve P–521

- Prerequisites:

```
dsU   =   00000166 8F7C6B25 5B17B26B A15C8A25 B6573788 AD9B52E1
          D348FBBB A83208AF 82288B4C C9452323 21579082 7F5F5653
          F4734214 4AD5DEAF F10B3B3E EE995D67 DC5658A8

x_QsU =   00000093 FA98278D 2BFF8953 BA05789B 7E965FC4 52F5B48F
          5E6A5CE9 81217BBA B92F741F 16B5DD7D F2322983 62099C79
          23B3C469 C8F930EE E413F1D9 B2E903C6 0CEC5062

y_QsU =   00000015 F228D847 4600C826 B496B572 FF18D152 2BD68A0D
          9E1C109A 92F8C4EC 29508823 92398116 64E56F04 765A297F
          F33E4285 B78C58E0 3736DDEF 4272EE97 6212F8FE

dsV   =   000001E1 F8DC6B6A D4FDABDB C0887F68 079E7DE4 E07C2E95
          2AB5BF95 C455B284 11ADC49C CB016528 07228837 5D8C1E56
          7073EC34 E2FAFD43 85B3C2FE 5F20845F F2F39487

x_QsV =   000000CC C26BF3D0 1662D7BD 1D1AA06E 4AFB9F7F 4DD1ACAB
          13DBBB75 678A1E20 2C04AA52 53C613EC 190DB7B3 FDE35430
          3C15D0A4 51E5B395 A6945593 80F93F80 A1CBEB8A
```

```
y_QsV =   00000153 97BCCBEC 0340AF1A A7094220 5DDAE592 D8B04409
          EA9EC8FE 0BD56AFD 9AF8D16D 63956C05 B758C2A3 E1208104
          F7946CBA 76A55B98 3595A443 124775AE F56CCE2C
```

BEGIN U's calculations

- Step 1:

```
nonceU =  CAA5D6D8 6906E456 EFBF2CF1 BE6B49F3 F65E521B D987200F
          9315B84F 76643522 E9BFD9A7 A57999E1 FFCE1C31 61EFAEA8
          AED8FB16 AAD5B40A AFD2732E 67CA5C0C
```

- Step 2: Decimal value for shared secret.

```
Z =       15070391515847429219607233137651394167730114063580
          84864550795357863096779876281387202550310878851800
          02598477754493581467328008630253592711393405622800
          0150685
```

- Step 3: Hex value for shared secret.

```
Z =       00000070 666DEDBA B414EA0A 2953DD65 1D66D210 EEEF5C2D
          ABE58B7D 08C45091 A9EE2786 7A465EAB 6BAAFF6C 291A385E
          3AC03E70 AF738100 E6B7DCDA 470F5025 75B4B49D
```

- Step 4: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000040 CAA5D6D8
             6906E456 EFBF2CF1 BE6B49F3 F65E521B D987200F 9315B84F
             76643522 E9BFD9A7 A57999E1 FFCE1C31 61EFAEA8 AED8FB16
             AAD5B40A AFD2732E 67CA5C0C 424F4242 59343536

DerKeyMat  = F07AADA6 4BEFFD6A B498441D 0C64464B FE28BA81 7D4707E4
             3A97DCC6 AEEBDC1F 53A56032 9C39E0FE 4F2FA2F8 1F7A7DFE
             B2216A88 296C8FCD 43F7B56C E45E4743 EC5F542C 81D8C127
             1D18C423 BA286912 B9AC385D 2545E8C0 D621F797 490FDFDE
             0D1672D7 B242DA98 9532B01A 53133390 63B0DE62 E1304E5D
             00694BFF 06C323B8
```

END U's calculations

BEGIN V's calculations

- Step 1:

```
nonceU =  CAA5D6D8 6906E456 EFBF2CF1 BE6B49F3 F65E521B D987200F
          9315B84F 76643522 E9BFD9A7 A57999E1 FFCE1C31 61EFAEA8
          AED8FB16 AAD5B40A AFD2732E 67CA5C0C
```

- Step 2: Decimal value for shared secret.

```
Z =       1507039151584742921960723313765139416773011406358 0
          8486455079535786309677987628138720255031087885180 0
          0259847775449358146732800863025359271139340562280 0
          0150685
```

- Step 3: Hex value for shared secret.

```
Z =       00000070 666DEDBA B414EA0A 2953DD65 1D66D210 EEEF5C2D
          ABE58B7D 08C45091 A9EE2786 7A465EAB 6BAAFF6C 291A385E
          3AC03E70 AF738100 E6B7DCDA 470F5025 75B4B49D
```

- Step 4: Additional inputs into the key derivation function and two blocks (1024 bits) of output (`DerKeyMat = DerivedKeyingMaterial`).

```
OtherInfo  = 12345678 9ABCDEF0 414C4943 45313233 00000040 CAA5D6D8
             6906E456 EFBF2CF1 BE6B49F3 F65E521B D987200F 9315B84F
             76643522 E9BFD9A7 A57999E1 FFCE1C31 61EFAEA8 AED8FB16
             AAD5B40A AFD2732E 67CA5C0C 424F4242 59343536

DerKeyMat  = F07AADA6 4BEFFD6A B498441D 0C64464B FE28BA81 7D4707E4
             3A97DCC6 AEEBDC1F 53A56032 9C39E0FE 4F2FA2F8 1F7A7DFE
             B2216A88 296C8FCD 43F7B56C E45E4743 EC5F542C 81D8C127
             1D18C423 BA286912 B9AC385D 2545E8C0 D621F797 490FDFDE
             0D1672D7 B242DA98 9532B01A 53133390 63B0DE62 E1304E5D
             00694BFF 06C323B8
```

END V's calculations

- If key confirmation is performed, then

```
MacKey  = F07AADA6 4BEFFD6A B498441D 0C64464B FE28BA81 7D4707E4
          3A97DCC6 AEEBDC1F

nonceV =  3D8654AF 124748C3 95AFBE27 CC8735FE 741AD594 794FA9E7
          8A9F6FE5 EED2A195 840FEA75 659BEE7E CAFDE388 6F3A1D9F
          C98CB499 3B5AD5E9 B7ED06E5 0ED5857F
```

- If UNILATERAL key confirmation provided by U to V, then

```
MacData_U = msg_UN_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F31 5F55414C 49434542 4F424259 CAA5D6D8 6906E456
            EFBF2CF1 BE6B49F3 F65E521B D987200F 9315B84F 76643522
            E9BFD9A7 A57999E1 FFCE1C31 61EFAEA8 AED8FB16 AAD5B40A
            AFD2732E 67CA5C0C 3D8654AF 124748C3 95AFBE27 CC8735FE
            741AD594 794FA9E7 8A9F6FE5 EED2A195 840FEA75 659BEE7E
            CAFDE388 6F3A1D9F C98CB499 3B5AD5E9 B7ED06E5 0ED5857F

MacTag_U  = 509D6F66 86C8A4BB 42C3847B 2631647D 624290F6 1E11725E
            E607CC5C C464A906 FCF48668 96D931CA 1DE00F85 3AE7CDDA
            8ACF5BFF 1899B11B A3ACE82F BCCF1D33
```

- If UNILATERAL key confirmation provided by V to U, then

```
MacData_V = msg_UN_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F31 5F56424F 42425941 4C494345 CAA5D6D8 6906E456
            EFBF2CF1 BE6B49F3 F65E521B D987200F 9315B84F 76643522
            E9BFD9A7 A57999E1 FFCE1C31 61EFAEA8 AED8FB16 AAD5B40A
            AFD2732E 67CA5C0C

MacTag_V  = 7613C4AD 43AB419B 9D63786F 82EDDC28 A571A923 5282E472
            C5340BBB 1F21377F ABDC5195 2B2950D9 5EE2BC1D 3377DA3C
            9066DDFB 22EA7FDB 4F1C9D04 ACB2C7DD
```

- If BILATERAL key confirmation, then

```
MacData_U = msg_BI_U || ID_U || ID_V || EphemData_U || EphemData_V

          = 4B435F32 5F55414C 49434542 4F424259 CAA5D6D8 6906E456
            EFBF2CF1 BE6B49F3 F65E521B D987200F 9315B84F 76643522
            E9BFD9A7 A57999E1 FFCE1C31 61EFAEA8 AED8FB16 AAD5B40A
            AFD2732E 67CA5C0C 3D8654AF 124748C3 95AFBE27 CC8735FE
            741AD594 794FA9E7 8A9F6FE5 EED2A195 840FEA75 659BEE7E
            CAFDE388 6F3A1D9F C98CB499 3B5AD5E9 B7ED06E5 0ED5857F

 MacTag_U  = E3FB8F42 279A125D C15ACF98 9FD63C2C 55229982 18147FCD
            40C34F05 29B45666 0D66179B 6A57507C 3F654171 A48370E8
            9FEA12F7 E535CCCE 983D6F7A 53B8875C

MacData_V = msg_BI_V || ID_V || ID_U || EphemData_V || EphemData_U

          = 4B435F32 5F56424F 42425941 4C494345 3D8654AF 124748C3
            95AFBE27 CC8735FE 741AD594 794FA9E7 8A9F6FE5 EED2A195
            840FEA75 659BEE7E CAFDE388 6F3A1D9F C98CB499 3B5AD5E9
            B7ED06E5 0ED5857F CAA5D6D8 6906E456 EFBF2CF1 BE6B49F3
            F65E521B D987200F 9315B84F 76643522 E9BFD9A7 A57999E1
            FFCE1C31 61EFAEA8 AED8FB16 AAD5B40A AFD2732E 67CA5C0C

 MacTag_V  = CFFCCAE8 2A02E330 AAD11631 2FB63A54 DD25F427 9875C29B
            29280B07 C3F98948 A870C1C9 53F1FFB6 8F0EB0BF C10ACA80
            B3E2C3B2 5EEBDCCF 37DEE52C 02B2301D
```

Bibliography

[1] NIST SP 800-56A: Recommendation for Pair–Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2006.

[2] FIPS PUB 186-3: Digital Signature Standard (DSS) (Draft), March 2006.

[3] FIPS PUB 180-2: Secure Hash Standard, August 2002.

[4] FIPS PUB 198: The Keyed-Hash Message Authentication Code (HMAC), March 2002.

[5] ANS X9.62-2 (Draft), Elliptic Curve Digital Signature Algorithm (Revised), 2005.