

ClientHs

KEM_pk

OKEM_ciphertext

padding

mark

mac

32B b'\x8d9\xb8\xa1V\x[...]

32B b''4\xd7\xe0\xb6\xd[...]

45B b'\xa8*\xef\xd8\x0[...]

32B b'\xde\xf7\xe4\xf5[...]

32B b'5.\xb1wl\x98\x89[...]

8d 39 b8 a1 56 7f 9d 58 26 43 1d 96 ca d7 f7 f0
f4 ba f6 5a cd 9e 41 d7 fb 03 31 74 d0 3f c7 e0

34 d7 e0 b6 db f0 46 b3 72 79 93 c3 f0 f4 ee 3b
d4 ec ae 38 c1 b1 e4 ce 77 45 92 5b 28 76 6f 27

a8 2a ef d8 0c e9 21 dc 63 28 53 4b 99 14 82 79
36 8f ce e8 f4 c0 fc 0f ff ef c3 95 64 d1 07 ff
49 a7 58 67 ab 25 99 9d a3 23 09 1c 6c de f7 e4

f5 89 c4 6f 59 ef e2 79 72 f9 4c dc 17 38 40 c9
b0 db 2a 89 c5 c8 57 38 fc e9 38 7a e7 35 2e b1

77 6c 98 89 0a 96 b5 03 5c a8 21 90 1a 70 69 75
7d f4 b4 03 38 18 2f 21 6d e9 1c b0 79