

ClientHs

KEM\_pk

OKEM\_ciphertext

padding

mark

mac

32B b'E\x04\xae\x92\x9[...]

32B b'\x7f3ecVG\xa35\x[...]

45B b'\xe6\xd3\xa5\xdd[...]

32B b'\xfa\xdf\x8cR\xa[...]

32B b'\x0eS \xf9\xf6\x[...]

45 f4 ae 92 91 71 7f 90 a4 3a e1 e4 b0 1e 95 97  
ef 64 df a6 69 d7 39 76 1f d8 d6 ae e1 95 6c 98

7f 33 65 63 56 47 a3 35 03 74 ea 53 24 2b f6 bf  
4e be 72 89 9a d9 8d d3 7c 9f 34 35 cc 05 a1 96

e6 d3 a5 dd a7 cd ee e0 2d 12 7b 5f 3f c9 18 f1  
9a 39 a5 a7 52 a0 3a 09 fb 9b 6d 62 47 d6 1d 6c  
f6 3a 42 54 51 a6 42 8c 6a 73 c9 fb e0 fa df 8c

52 a9 92 63 c4 ad fd 92 3d 17 7a a7 c9 b5 d3 68  
a7 20 45 a9 68 4e 67 32 1a 54 7d 22 e4 0e 53 20

f9 f6 a1 9c c0 95 62 e7 3f ba 5a ce 81 4f aa b5  
39 9c 1c 62 e2 80 df e5 28 59 d0 b6 36