

ClientHs

KEM_pk

OKEM_ciphertext

padding

mark

mac

32B b'\xf4{\xd0\xb4\xb[...]

32B b'\x85\xd1\x80N\xfb[...]

45B b''\xe8\x81\xf4'\x1[...]

32B b'\xf0\x1c\x89\xa9[...]

32B b'\xb0\xd27\x94si[...]

f4 7b d0 b4 b4 70 7b 8b 66 cc e2 e7 96 99 a7 0b
35 2a 8c 7d 5a 19 ed 50 e9 f4 61 30 6c 6e c5 51

85 d1 80 4e f8 89 d0 2f 88 49 68 3b 02 c2 11 32
98 5c ef 4f 4a 6d 7e 1b 85 12 7b 69 1d 39 38 52

e8 81 f4 60 16 b7 1f 8f a1 e2 83 fc de bd c9 0c
5a 10 d8 05 bd 82 fe 5c 58 d2 cd 70 e1 f1 27 c5
02 7b 7f 44 b7 39 b6 04 74 52 68 50 67 f0 1c 89

a9 a6 d2 48 35 7f 65 12 1c be 79 af 06 a3 5b f0
e4 f7 36 ec 23 f8 49 2f da 97 bd 31 02 2e b0 d2

37 94 73 69 fe 1e 5b 3c 22 ea d7 03 a0 f3 2f 95
f9 8f 8a a9 10 f2 d3 e3 73 b5 b4 1a 7d