

ClientHs

KEM\_pk

OKEM\_ciphertext

padding

mark

mac

32B b'\x16\x90v\_\xfc\$[...]

0B b''

77B b'\xf1\xc4\xfd\x8a[...]

16B b'A\xe9\xc2\xf5''\x[...]

16B b'\x05\x89R\xbb\xe[...]

16	90	76	5f	fc	24	b3	bd	e4	d5	dc	f3	3d	f2	e2	5a
87	95	82	fc	8e	45	c0	59	ab	8b	2e	ee	c9	06	f4	6b

f1	c4	fd	8a	f1	22	98	ef	a4	f4	ab	9b	83	e7	79	69
c0	fb	d1	53	a5	fa	9d	72	ea	e5	7a	50	18	be	8a	13
28	bb	84	39	90	cc	9a	31	2a	bf	a9	84	c0	19	16	78
d0	6c	cf	c8	7a	3e	2e	e5	36	b7	e4	74	54	38	01	7b
29	d2	40	93	2d	aa	c8	79	68	da	df	36	01	41	e9	c2

f5	22	01	c0	13	08	ec	a0	ac	b2	bf	2b	30	05	89	52
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

bb	ee	ce	23	2f	72	f3	0f	f9	2d	1c	97	17
----	----	----	----	----	----	----	----	----	----	----	----	----