

ClientHs

KEM\_pk

OKEM\_ciphertext

padding

mark

mac

32B b'\xe4"\x18o\xae|\[...]

0B b''

77B b'Z\x98B\x1dx\xe4\[...]

16B b'=\xd6\x9a\_\xd5\x[...]

16B b'm\xfe\xc8\x9f\xd[...]

e4	22	18	6f	ae	7c	1a	73	7f	b3	4c	fd	07	d0	a8	0c
9e	4c	31	04	4c	27	2b	94	c9	cf	e0	e3	e3	5f	d2	2e

5a	98	42	1d	78	e4	de	5e	76	e4	b9	ba	2d	05	3d	a1
8d	36	be	81	7c	e7	13	cf	e0	34	32	fb	6b	21	3c	c9
ab	fe	fb	7c	3c	3f	33	af	00	f8	1f	4c	e2	98	c6	cb
d1	04	2f	bb	0c	8c	1b	d8	37	6a	50	fc	a2	cd	c4	05

55	ab	0b	e5	cb	50	a8	ad	64	b8	dd	35	c9	3d	d6	9a
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

5f	d5	80	d3	d7	cf	49	04	22	2e	c6	34	cc	6d	fe	c8
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

9f	de	fd	29	7a	4a	91	41	0e	75	b8	96	6f
----	----	----	----	----	----	----	----	----	----	----	----	----