

ClientHs

KEM_pk

OKEM_ciphertext

padding

mark

mac

32B b'\x04<\x92\x81\xb[...]

0B b''

77B b'e\t\b8\xf9R\x9d[...]

16B b'\x0f\x8bB\\U\xb2[...]

16B b'&g\xcc\xbeL%\xdd[...]

04	3c	92	81	bf	12	99	02	f7	bb	8b	ea	60	92	e9	b2
b9	4f	32	e9	4f	34	55	e9	19	92	65	4f	e6	79	1f	0f

65	09	b8	f9	52	9d	e2	e4	86	04	e4	8a	f4	e4	9a	1b
e5	0e	5d	a2	28	8e	84	fd	ff	4e	34	f5	9d	fe	72	12
b6	aa	2b	2e	ca	c5	85	07	48	6b	53	81	0b	c1	80	b5
ba	84	0a	57	81	39	e2	31	70	a8	01	17	b7	c5	b8	4b
2e	b6	7b	11	c9	a8	c3	b6	8e	e5	5c	6c	4f	0f	8b	42

5c	55	b2	8a	a1	e7	74	1f	83	e0	8b	9b	70	26	67	cc
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

be	4c	25	dd	6e	83	3c	bd	a3	50	08	a3	ea
----	----	----	----	----	----	----	----	----	----	----	----	----