

ClientHs

KEM_pk

OKEM_ciphertext

padding

mark

mac

32B b'' \xb4\b4\x9dR\xfb[...]

0B b''

```
77B b'\x96B\x00\xab\x00[...]
```

16B b',l\xd6ksT\$\x15Xu[...]

16B b'u\xda*\x14cQ\x80[...]

```
b4 b4 9d 52 f6 9d eb 28 bf 52 b3 f8 6d 89 0a 32
23 e7 e0 5d 38 06 ad 27 53 9d 51 a3 fd 6d 55 af
```

96	42	00	ab	0b	06	21	cd	44	9f	65	d2	6e	e8	eb	8b
90	63	91	ae	d6	73	f5	59	2f	8b	99	a0	fd	3e	23	fd
68	42	88	dd	29	ba	1b	28	97	2c	6c	71	22	22	ad	83
9f	fa	d0	e0	27	4a	36	c4	9b	fb	95	0e	08	62	86	1a
c4	dc	1b	12	c2	ef	44	5b	61	52	93	f1	e0	2c	49	d6

6b 73 54 24 15 58 75 ad 38 ed 02 0e eb 75 da 2a

14 63 51 80 56 5d 96 ac bb b9 3c b4 d4