

ClientHs

KEM\_pk

OKEM\_ciphertext

padding

mark

mac

32B b'\nd\x8e}\xe45\x7[...]

0B b''

77B b'\xba\x93\xc4\xf6[...]

16B b'R\xd7\x93\x0e\xa[...]

16B b''\xae\x97\xbe\x99[...]

0a	64	8e	7d	e4	35	7f	52	56	2e	8a	f7	e3	96	57	35
45	6b	9a	3b	87	95	13	87	d1	d6	36	d2	54	07	c1	36

ba	93	c4	f6	30	14	03	88	ed	7f	4e	03	2e	cd	51	6b
06	b9	c7	33	0f	19	32	ff	db	77	9b	dc	56	d6	c2	3c
da	15	5b	8c	5e	50	69	bd	86	35	0a	bd	83	ba	16	0c
f2	7b	94	63	e4	c3	c4	0e	56	13	65	69	28	39	a4	04
be	ea	99	9e	ae	5a	71	3d	4e	65	68	08	9b	52	d7	93

0e	a2	78	0c	b1	74	c2	5e	2e	58	fe	d8	ca	ae	97	be
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

99	e8	db	60	3e	4a	a4	93	27	78	fe	13	10
----	----	----	----	----	----	----	----	----	----	----	----	----