

ClientHs

KEM_pk

OKEM_ciphertext

padding

mark

mac

32B b'\x87\xa5\x8dc\xca[...]

32B b'\x02\xdc\xdd\xce[...]

45B b'|\xe3\xdd\xef9?\x00[...]

32B b'Z\x14\xedVi\x00[...]

32B b')\x0b\x00\x9b\x08[...]

87	a5	8d	63	cb	26	96	74	1f	0c	8c	fe	f0	aa	c9	7d
31	32	e8	35	8b	37	a4	f7	ff	24	a8	de	fc	a7	82	2a
02	dc	d4	ce	a3	fc	c7	a9	dc	b7	17	10	cd	ef	3a	3e
0b	50	cc	d4	25	3e	80	8a	e1	70	56	fb	f5	20	44	6f
7c	6c	e3	d5	f9	3f	8e	a2	d1	6e	c7	04	5e	96	5d	70
d0	ac	30	22	d8	b7	d9	1e	ad	27	96	a5	e4	71	23	13
9a	b6	d4	12	2d	cf	a1	a3	54	15	9d	bf	e0	5a	14	ed
56	69	d0	90	f4	6d	72	2f	fa	44	55	2f	aa	31	4d	80
46	dc	c2	20	4e	31	21	86	6d	a2	f7	a8	bd	29	0b	c0
9b	8f	6e	6f	a4	1b	2f	65	16	30	95	60	a6	63	87	f1
d8	77	fe	76	6a	3a	fd	4f	3a	3e	a6	62	c6			