

ClientHs

KEM_pk

OKEM_ciphertext

padding

mark

mac

32B b'\x03\x9e\x93\xef[...]

32B b'\xf9*r\x82d\r\xb[...]

45B b'\xd2\xc5\x9d\xd7[...]

32B b'\xf7\xb6[\x9e\x0[...]

32B b''\xf6\x82\xd4\xa[...]

03	9e	93	ef	73	a7	6c	c5	7c	9d	f0	fe	ee	41	bd	28
46	80	9d	36	b4	b6	c4	95	f2	87	b6	8a	bd	18	e1	d5
f9	2a	72	82	64	0d	ba	eb	41	81	95	22	e7	39	14	30
dd	01	8e	ec	61	ff	d4	78	cc	ea	6e	27	76	69	c4	30
d2	c5	9d	d7	6c	52	32	09	ea	e5	a5	cb	82	3f	d4	4b
cb	c9	cd	a8	09	b3	d8	b2	06	65	68	c9	62	15	52	3c
e8	02	43	67	20	16	31	d4	46	01	79	0e	4a	f7	b6	5b
9e	05	69	14	29	7f	3e	41	4b	95	01	db	20	41	8a	69
7d	c5	d7	11	39	60	3b	00	c1	14	84	69	03	60	f6	82
d4	ac	84	1c	90	51	b0	55	5f	76	4d	8a	c1	4f	ff	94
85	21	d1	ee	b3	62	e3	79	07	56	0e	00	bb			