

ClientHs

KEM_pk

OKEM_ciphertext

padding

mark

mac

32B b'q\xdc\rWS\x77q~\ [...]

32B b'\xe51\xc66C\xb4\ [...]

45B b'\xd4\x17T\x94\xa [...]

32B b':\xbe+t\x9,\x80 [...]

32B b'\xa0*'\x15\x01\x [...]

71	dc	0d	57	53	f7	71	7e	b3	ce	f9	1e	8c	28	39	58
b9	d5	77	de	8d	91	9c	61	72	e0	8e	a2	f1	2e	c2	5e

e5	31	c6	36	43	b4	b6	76	25	5a	d3	6e	e1	46	52	59
c0	df	50	84	b3	e2	22	9f	5c	42	e5	e2	a0	5f	08	06

d4	17	54	94	a9	dd	ae	cf	12	97	e4	10	ee	1b	6a	b8
1d	c0	93	94	75	33	58	ff	77	45	b6	1a	16	00	74	d1
58	10	c9	60	44	34	94	4d	7a	4d	12	52	e4	3a	be	2b

74	f9	2c	80	a1	04	a8	73	18	90	4b	87	df	a5	5c	eb
9a	58	44	ba	61	5e	ab	c5	cf	21	4d	e2	41	a0	2a	60

15	01	ce	f0	69	cf	03	a5	f1	df	5d	23	94	7f	ad	93
7d	d0	97	d2	fb	8e	53	ec	df	dd	01	cd	22			