

ClientHs

KEM_pk

OKEM_ciphertext

padding

mark

mac

32B b'\x86\xc6\x1e\xfc[...]

32B b'(\xc0<\xc3}\xba_[...]

45B b'\x95\x87\xee\x05[...]

32B b'}[L\xbd\xcc\x81\ [...]

32B b'\xcf\xdb\xe3\x03[...]

86	c6	1e	fc	40	00	37	83	80	ae	49	77	ef	2c	eb	fb
28	fc	75	a0	76	e4	66	50	c1	e9	f5	dd	09	c7	0e	ac
28	c0	3c	c3	7d	ba	5f	59	5e	26	b6	32	08	18	20	97
82	ec	3b	7b	45	ef	1f	78	db	2e	76	7b	ca	00	ae	c6
95	87	ee	05	d3	78	0a	db	00	66	d9	7b	ec	74	00	ea
52	22	2f	32	ab	18	9c	4f	81	93	90	72	7a	dc	7f	8d
10	93	4f	13	30	bd	c6	66	3c	0f	a0	13	9a	7d	5b	4c
bd	cc	81	0a	cd	6f	a1	67	69	2c	d0	dd	18	8d	d8	c5
ba	d8	75	87	53	1e	8a	ef	e4	12	24	19	86	cf	db	e3
03	3c	73	3e	b9	52	c9	a1	fd	a2	a6	b5	0a	51	eb	34
7c	1c	59	f9	68	03	05	de	0a	1f	f5	60	c0			