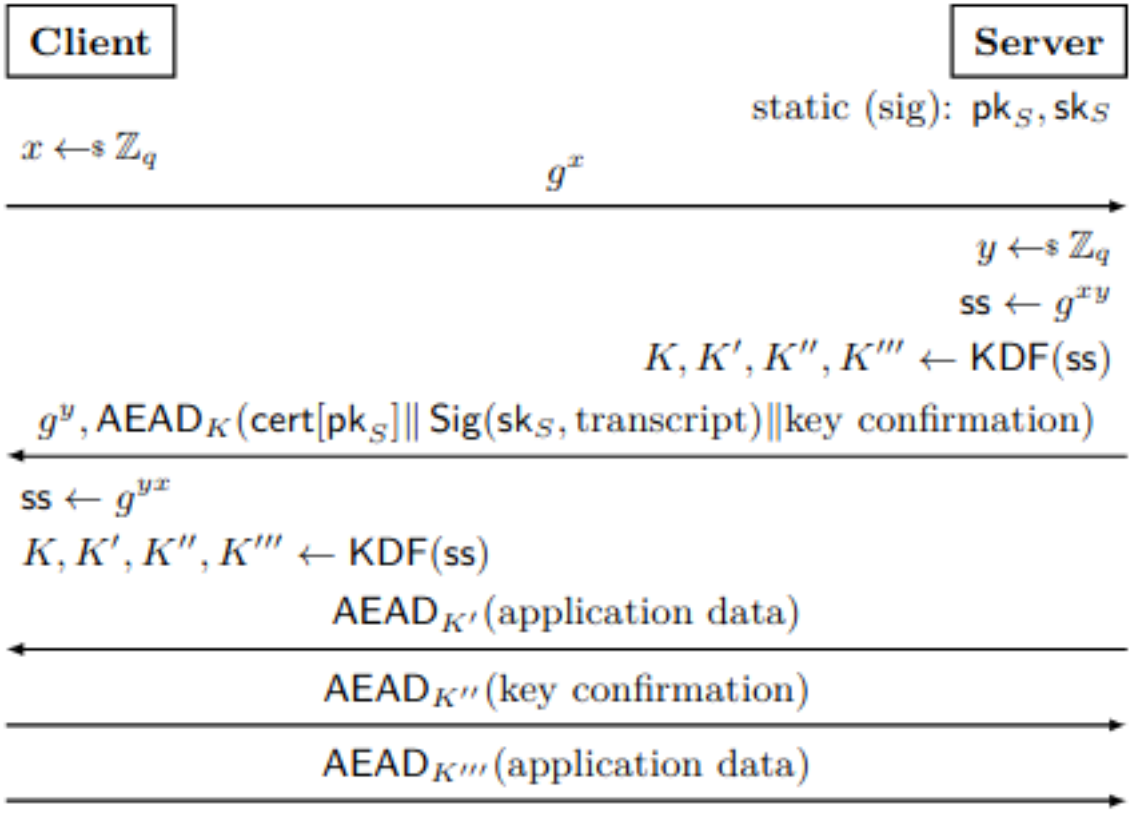
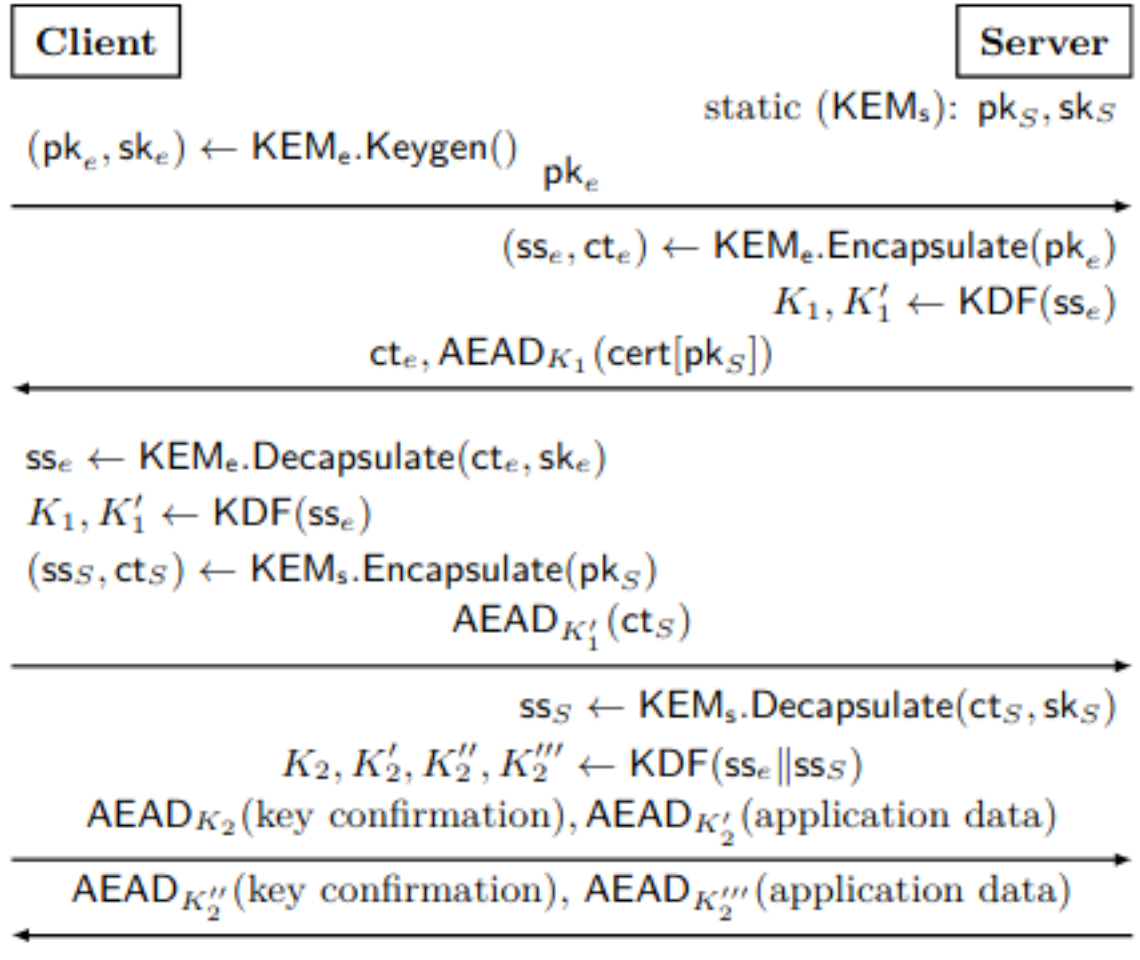

PQC Group
UTFPR

	bytes transmitted			stored	computation (≈Kcycles)		
Signatures	pubkey	sig.	sum	secret	keygen	sign	verify
Dilithium ★	1 312	2 420	3 732	2 528	1 597	4 095	1 572
Falcon ★	897	690	1 587	1 281	163 994	39 014	473
Rainbow †	161 600	66	161 666	103 648	94	907	238
KEMs	pubkey	ciph.	sum	secret	keygen	encaps	decaps
Kyber ★	800	768	1 568	1 632	440	539	490
NTRU †	699	699	1 398	953	2 867	565	538
SABER †	672	736	1 408	1 568	352	481	453

★: Scheme was selected for standardization.

†: Scheme was eliminated from the NIST standardization project.

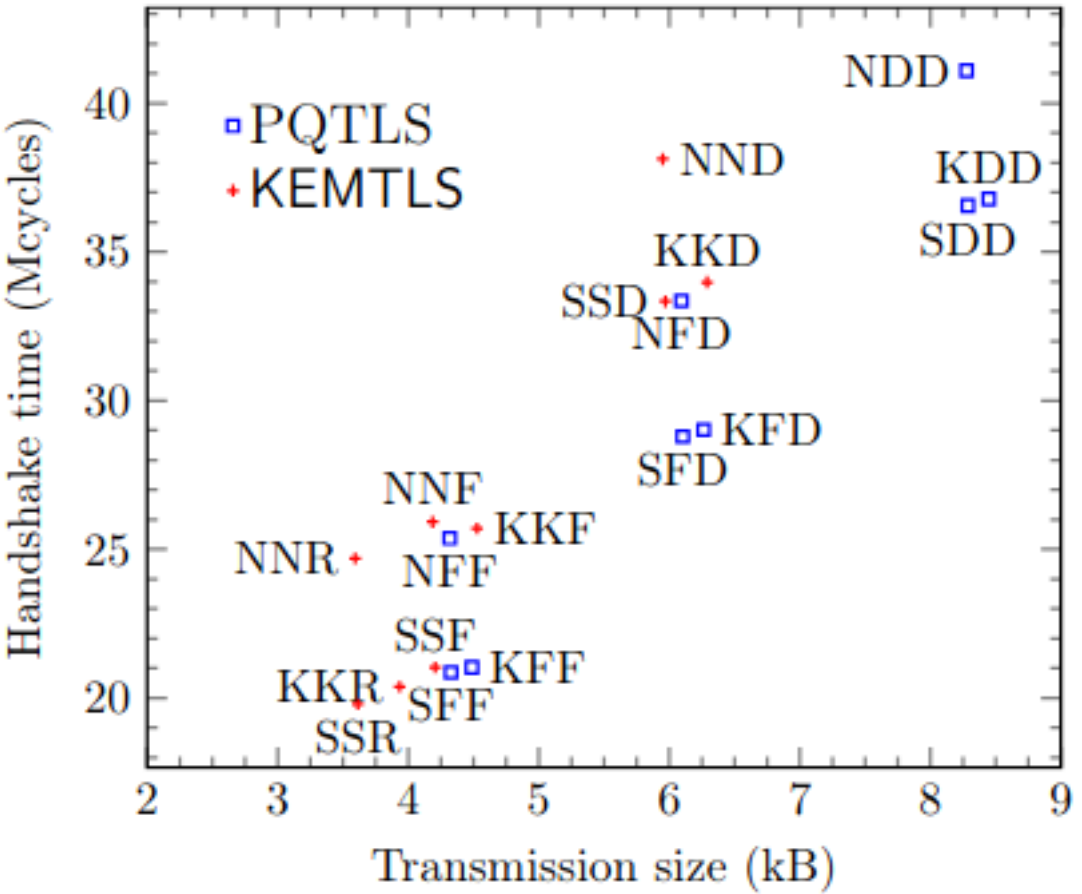

Client
Server
static (sig): $\mathsf{pk}_S, \mathsf{sk}_S$
$x \leftarrow\$ \mathbb{Z}_q$
g^x
$y \leftarrow\$ \mathbb{Z}_q$
$\mathsf{ss} \leftarrow g^{xy}$
$K, K', K'', K''' \leftarrow \mathsf{KDF}(\mathsf{ss})$
$g^y, \mathsf{AEAD}_K(\mathsf{cert}[\mathsf{pk}_S] \| \mathsf{Sig}(\mathsf{sk}_S, \text{transcript}) \| \text{key confirmation})$
$\mathsf{ss} \leftarrow g^{yx}$
$K, K', K'', K''' \leftarrow \mathsf{KDF}(\mathsf{ss})$
$\mathsf{AEAD}_{K'}(\text{application data})$
$\mathsf{AEAD}_{K''}(\text{key confirmation})$
$\mathsf{AEAD}_{K'''}(\text{application data})$


Client
Server
static ($\mathsf{KEM_s}$): $\mathsf{pk}_S, \mathsf{sk}_S$
$(\mathsf{pk}_e, \mathsf{sk}_e) \leftarrow \mathsf{KEM_e.Keygen}()$
pk_e
$(\mathsf{ss}_e, \mathsf{ct}_e) \leftarrow \mathsf{KEM_e.Encapsulate}(\mathsf{pk}_e)$
$K_1, K_1' \leftarrow \mathsf{KDF}(\mathsf{ss}_e)$
$\mathsf{ct}_e, \mathsf{AEAD}_{K_1}(\mathsf{cert}[\mathsf{pk}_S])$
$\mathsf{ss}_e \leftarrow \mathsf{KEM_e.Decapsulate}(\mathsf{ct}_e, \mathsf{sk}_e)$
$K_1, K_1' \leftarrow \mathsf{KDF}(\mathsf{ss}_e)$
$(\mathsf{ss}_S, \mathsf{ct}_S) \leftarrow \mathsf{KEM_s.Encapsulate}(\mathsf{pk}_S)$
$\mathsf{AEAD}_{K_1'}(\mathsf{ct}_S)$
$\mathsf{ss}_S \leftarrow \mathsf{KEM_s.Decapsulate}(\mathsf{ct}_S, \mathsf{sk}_S)$
$K_2, K_2', K_2'', K_2''' \leftarrow \mathsf{KDF}(\mathsf{ss}_e \| \mathsf{ss}_S)$
$\mathsf{AEAD}_{K_2}(\text{key confirmation}), \mathsf{AEAD}_{K_2'}(\text{application data})$
$\mathsf{AEAD}_{K_2''}(\text{key confirmation}), \mathsf{AEAD}_{K_2'''}(\text{application data})$

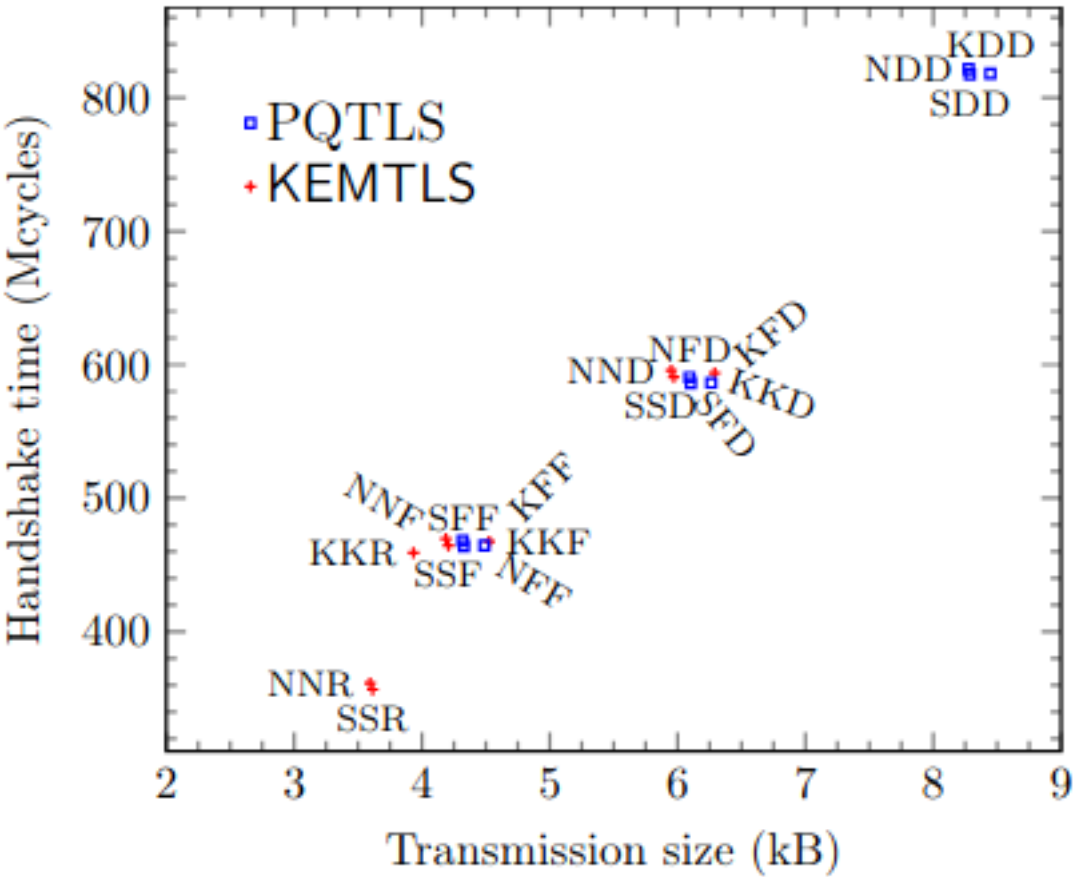
Name	Abbrev.	Bandwidth	RTT time
Broadband	BB	1 Mbit	26 ms
LTE Machine Type Communication	LTE-M	1 Mbit	120 ms
Narrowband-IoT	NB-IoT	46 kbit	3 s

	KEX	Auth.	CA	PQC code	(%)	CA size	(%)	Memory
KEMTLS	Kyber	Kyber	Dilithium	29.0 kB	(20.1%)	3.9 kB	(2.7%)	49.7 kB
	Kyber	Kyber	Falcon	25.7 kB	(18.6%)	1.7 kB	(1.2%)	52.8 kB
	Kyber	Kyber	Rainbow	29.8 kB	(9.8%)	161.8 kB	(53.4%)	167.0 kB
	NTRU	NTRU	Dilithium	203.4 kB	(63.9%)	3.9 kB	(1.2%)	49.7 kB
	NTRU	NTRU	Falcon	200.0 kB	(63.9%)	1.7 kB	(0.6%)	52.8 kB
	NTRU	NTRU	Rainbow	204.0 kB	(42.8%)	161.8 kB	(33.9%)	182.9 kB
	SABER	SABER	Dilithium	31.5 kB	(21.5%)	3.9 kB	(2.7%)	49.7 kB
	SABER	SABER	Falcon	28.2 kB	(20.0%)	1.7 kB	(1.2%)	52.8 kB
	SABER	SABER	Rainbow	32.2 kB	(10.5%)	161.8 kB	(53.0%)	167.9 kB
PQTLS	Kyber	Dilithium	Dilithium	29.0 kB	(20.1%)	4.0 kB	(2.8%)	58.0 kB
	Kyber	Falcon	Dilithium	34.4 kB	(23.0%)	4.0 kB	(2.7%)	60.7 kB
	Kyber	Falcon	Falcon	25.8 kB	(18.6%)	1.8 kB	(1.3%)	56.2 kB
	NTRU	Dilithium	Dilithium	203.4 kB	(63.8%)	4.0 kB	(1.3%)	56.6 kB
	NTRU	Falcon	Dilithium	208.7 kB	(64.4%)	4.0 kB	(1.2%)	59.3 kB
	NTRU	Falcon	Falcon	200.1 kB	(63.9%)	1.8 kB	(0.6%)	54.8 kB
	SABER	Dilithium	Dilithium	31.5 kB	(21.5%)	4.0 kB	(2.7%)	58.0 kB
	SABER	Falcon	Dilithium	36.8 kB	(24.2%)	4.0 kB	(2.6%)	60.7 kB
	SABER	Falcon	Falcon	28.2 kB	(20.0%)	1.8 kB	(1.3%)	56.2 kB

	KEX	Auth.	CA	Handshake traffic	Handshake time in Mcycles (% of crypto) BB (%)	LTE-M (%)	NB-IoT (%)
KEMTLS	Kyber	Kyber	Dilithium	6.3 kB	17.1 (30.2%)	34.0 (15.2%)	593.6 (0.9%)
	Kyber	Kyber	Falcon	4.5 kB	12.3 (27.2%)	25.7 (13.0%)	467.8 (0.7%)
	Kyber	Kyber	Rainbow	3.9 kB	11.3 (25.1%)	20.4 (13.9%)	459.0 (0.6%)
	NTRU	NTRU	Dilithium	6.0 kB	21.3 (46.0%)	38.1 (25.6%)	595.8 (1.6%)
	NTRU	NTRU	Falcon	4.2 kB	16.6 (47.8%)	25.9 (30.6%)	469.7 (1.7%)
	NTRU	NTRU	Rainbow	3.6 kB	15.7 (47.4%)	24.7 (30.1%)	361.6 (2.1%)
	SABER	SABER	Dilithium	6.0 kB	16.3 (29.4%)	33.3 (14.4%)	590.8 (0.8%)
	SABER	SABER	Falcon	4.2 kB	11.6 (25.5%)	21.0 (14.1%)	464.8 (0.6%)
	SABER	SABER	Rainbow	3.6 kB	10.7 (23.1%)	19.8 (12.5%)	356.8 (0.7%)
PQTLS	Kyber	Dilithium	Dilithium	8.4 kB	19.9 (35.9%)	36.8 (19.5%)	818.1 (0.9%)
	Kyber	Falcon	Dilithium	6.3 kB	15.5 (33.0%)	29.0 (17.6%)	586.4 (0.9%)
	Kyber	Falcon	Falcon	4.5 kB	10.9 (30.1%)	21.0 (15.6%)	464.6 (0.7%)
	NTRU	Dilithium	Dilithium	8.3 kB	24.3 (47.6%)	41.1 (28.1%)	821.3 (1.4%)
	NTRU	Falcon	Dilithium	6.1 kB	19.9 (47.8%)	33.4 (28.5%)	590.6 (1.6%)
	NTRU	Falcon	Falcon	4.3 kB	15.2 (50.3%)	25.4 (30.2%)	468.0 (1.6%)
	SABER	Dilithium	Dilithium	8.3 kB	19.7 (35.2%)	36.6 (19.0%)	817.3 (0.8%)
	SABER	Falcon	Dilithium	6.1 kB	15.3 (32.0%)	28.8 (17.0%)	586.2 (0.8%)
	SABER	Falcon	Falcon	4.3 kB	10.7 (28.5%)	20.9 (14.6%)	464.0 (0.7%)



(a) Broadband



(b) Narrowband-IoT