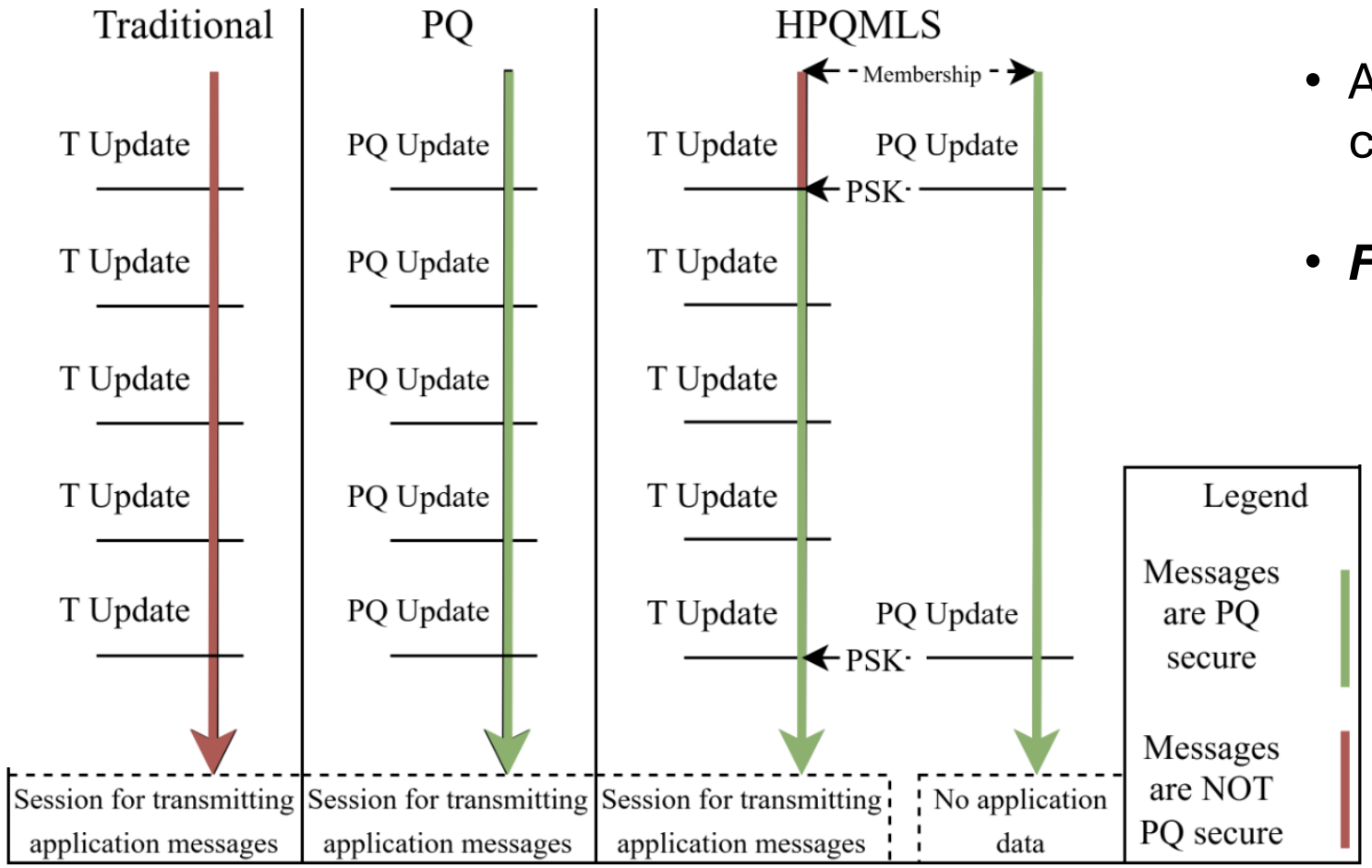
Flexible Hybrid PQ MLS Combiner

Joël Alwen Britta Hale Marta Mularczyk Xisen Tian



- Use two sessions – T and PQ and combine via exported PSKs.
- Alternative to a hybrid (e.g. PQ/T) ciphersuite approach
- ***Flexibility:*** PQ updates are tunable

  - PARTIAL update

    Traditional-only update in the traditional MLS session
  - FULL update

    PQ update in PQ group, exporter key generated and used as PSK along with a traditional update in the traditional session
  - Flexibility on PQ ratchet window

Illustration by Noah Greene

Modes

*NB: Key updates are authenticated via signatures

- PQ Confidentiality-Only mode
- PQ Confidentiality + Authenticity mode
  - PQ signatures are used to authenticate PQ updates in PQ session.

    The exporter key inherits this attestation and its inject into the

    traditional key schedule allow for PQ/T AEAD.
  - This does not include PQ non-repudiation

Average bytes / epoch for control messages (key update and associated messages) across 500 epochs

1 PQ / 100 T 1 PQ / 50 T 1 PQ / 10 T

Group Size	Traditional	Hybrid-100	Hybrid-50	Hybrid-10	PQ
2	515.80	557.74	593.28	877.60	2789.26
3	632.87	694.45	747.39	1170.91	4410.79
4	715.01	787.71	849.66	1345.26	5229.93
5	832.08	924.43	1003.78	1638.58	6851.47
10	1277.71	1434.17	1566.96	2629.28	11749.56
15	1688.41	1900.45	2078.29	3501.01	15845.26
20	2134.04	2410.23	2641.55	4492.11	20747.35
25	2544.74	2876.51	3152.88	5363.84	24843.05
30	2955.44	3342.79	3664.21	6235.57	28938.75
35	3401.07	3852.53	4227.39	7226.27	33836.84
40	3811.77	4318.81	4738.72	8098.00	37932.54
45	4222.47	4785.09	5250.05	8969.73	42028.24
50	4633.17	5251.37	5761.38	9841.46	46123.94
60	5454.57	6183.95	6784.08	11585.12	54317.33
70	6310.90	7159.97	7858.59	13447.55	63311.13
80	7132.30	8092.53	8881.25	15191.01	71502.53
90	7953.70	9025.11	9903.95	16934.67	79695.92
100	8775.10	9957.67	10926.61	18678.13	87887.32

*Improvements in both bytes on the wire and CPU cycles

Testing by Noah Greene

Timeline and Status

- Discussed at IETF 119, 120, & 121
- Adopted 26 Nov. 2024
- Various updates from feedback and…
- New draft 26 Feb.
- Asked for feedback IETF-122 (thank you to those who responded!)
- New draft 19 Jun.

No new notable feedback since…

- Time for WGLC?

Timeline and Status

- Discussed at IETF 119, 120, & 121
- Adopted 26 Nov. 2024
- Various updates from feedback and…
- New draft 26 Feb.
- Asked for feedback IETF-122 (thank you to those who responded!)
- New draft 19 Jun.

No new notable feedback since…

Request for name change away from "*combiner*" / "*hybrid*"
Proposed alternative: *Post Quantum MLS with Amortized Overhead*

- Time for WGLC?