A New Theory on PQ Migration

- Personal Viewpoints

Guilin Wang

IETF 124 @ Montreal, 1-7 Nov. 2025

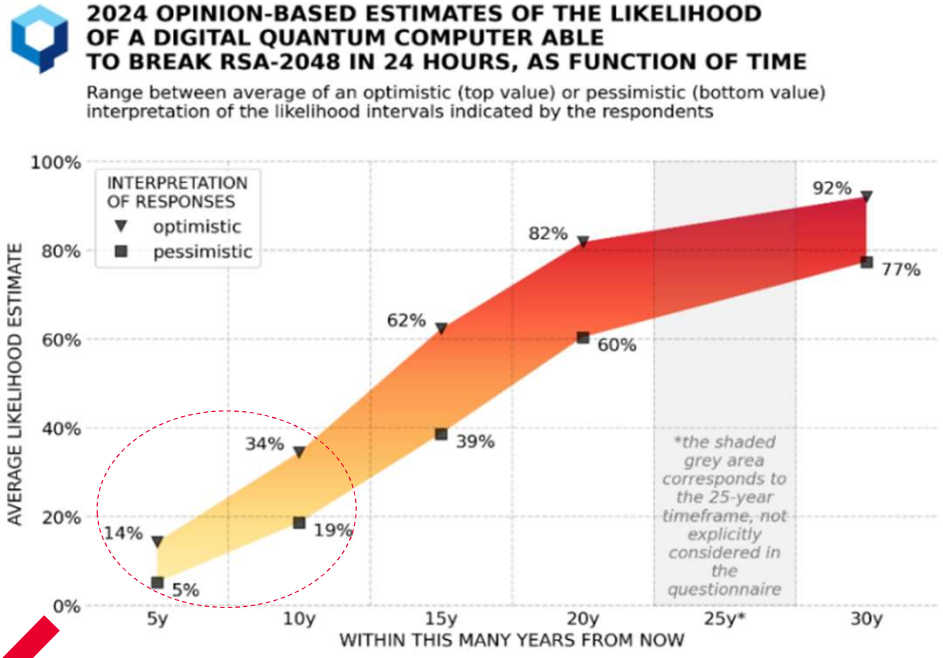
Scope of This Talk

- ❑ Hybrid Key Exchanges are already wildly accepted.
- ❑ **This talk will just cover hybrid signatures**
  - Why hybrid signatures valuable?
  - Performance and complexity?
- ❑ **Purpose of this talk**
  - Offer a new viewpoint for the value of hybrid signatures in PQ migration
  - and then invoke further thoughts on PQ migration policies
  - Not complex, understandable to everyone
- ❑ **Background of this talk**
  - Why theory? Mainly about quantitative analysis, with simple probability reasoning
  - Based on recent discussions in Pquip, Jose/Cose, and Lamps WGs on the value and complexity of hybrid signatures.

Why hybrid signatures?

Typical Questions: *"And for short term protection there is no point in dual signatures, if a CRQC is available the classic part is irrelevant. And until a CRQC is available the QR part is redundant. "*

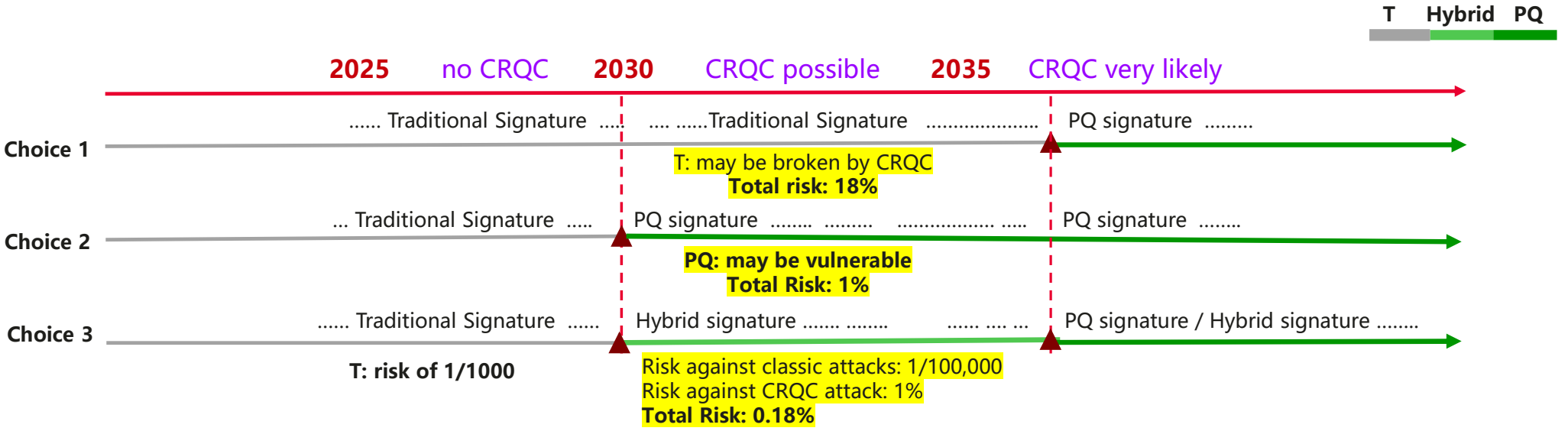
- ❑ Not a simple multiple choice question, as we do not know when CRQC will be available exactly.
- ❑ Example: Assume that most likely, a CRQC will be available after 2035 ….
- ❑ **Let us do a quantitative analysis on three possible choices!**
- ❑ **Assumptions** (arguable)**:**
  - A traditional signature has risk of 1/1000, against classic attacks, and 100%, against CRQC attacks.
  - A PQ signature has risk of 1/100, not as mature as T… before 2035, against classic and CRQC attacks.
  - A CRQC is available in the period of 2030-2035 with probability of 18%, according to opinion-based estimates by Prof. Michele Mosca, Dec. 2024
  - **Total risk = weighted risks against classic and CRQC attacks.**



Source: Quantum Threat Timeline Report 2024 by Michele Mosca and Marco Piani, Dec 2024

A CRQC is available in the period of 2030-2035 with probability of 18%: (5+14+19+34)% x 0.25=18%.

Why hybrid signatures?



❑ **From the above simple quantitative analysis, we can see**

- Choice 1 has total risk of 18%.
- Choice 2 has total risk of 1%
- Choice 3 has total risk of 0.18%.

- **So, Choice 3 even reduces total risk 5 times more than Choice 2!**

How's the complexity and performance of hybrid signatures?

Typical Questions: *"I think this will just add complexity with no value, complexity means more bugs and more ways to screw up, and must always be justified."*

- ❑ No necessarily more bugs. Actually, the hybrid is more robust, as it is safe if at least one has no bug.
- ❑ For typical combinations, sizes increasing from 3 -14.4%

Cert size in comparison to ML-DSA Certificate
(in bytes)

Algorithm	ML-DSA cert only	ML-DSA Composite cert	Difference
id-MLDSA44-ECDSA-P256-SHA256	4114	4274	160 (3.9%)
Id-MLDSA44-ECDSA-brainpoolP256r1-SHA256	4114	4274	160 (3.9%)
Id-MLDSA44-RSA2048-PSS-SHA256	4114	4668	554 (13.5%)
id-MLDSA65-ECDSA-P256-SHA512	5627	5786	159 (5.2%)
id-MLDSA65-RSA3072-PKCS15-SHA512	5627	6437	810 (14.4%)
Id-MLDSA65-RSA3072-PSS-SHA512	5627	6437	810 (14.4%)
id-MLDSA87-ECDSA-P384-SHA512	7569	7794	225 (3.0%)
id-MLDSA87-ECDSA-brainpoolP384r1-SHA512	7569	7793	224 (3.0 %)

These are all still smaller than the smallest SLH-DSA which is **8251** bytes!

Source: https://datatracker.ietf.org/meeting/119/materials/slides-119-lamps-composite-signature-v13-updates-00

- ❑ For computation, hybrid is just to compute both
  - ECDSA-p384+Dilithium3 is faster than RSA-3072.

Parameter Set	ARM Cortex-A72	
	Sign	Verify
ECDSA p384	240,4	304,7
RSA-3072	54,0	2868,3
Dilithium2	881,8	3684,1
Falcon512	76,7	6104,0
Dilithium3	550,2	2313,8
Dilithium5	462,7	1419,6
Falcon1024	35,2	3001,3

Operations/s

Parameter Set 1	Parameter Set 2	ARM Cortex-A72	
		Sign	Verify
ECDSA p256	Dilithium2	789,3	1583,9
RSA-3072	Dilithium2	51,0	1583,0
ECDSA p256	Falcon512	75,8	1921,8
RSA-3072	Falcon512	31,8	1922
ECDSA p384	Dilithium3	167,5	264,7
ECDSA p384	Dilithium5	76,2	110,8
ECDSA p384	Dalcon1024	25,4	116,0

Source: D Marchsreiter and J. Sepulved. Hybrid Post-Quantum Enhanced TLS 1.3 on Embedded Devices. In Proc. of DSD'22, IEEE

Takeaways

- Based on a quantitative analysis, this talk shows that hybrid signatures can efficiently reduce PQ migration risk.
- This is helpful, as PQ migration will involve a number of algorithms (i.e., algorithm diversity) and some uncertain periods.
- Discussions and further thoughts are welcome!

Thanks