CLOUDFLARE

Post quantum off the cuff

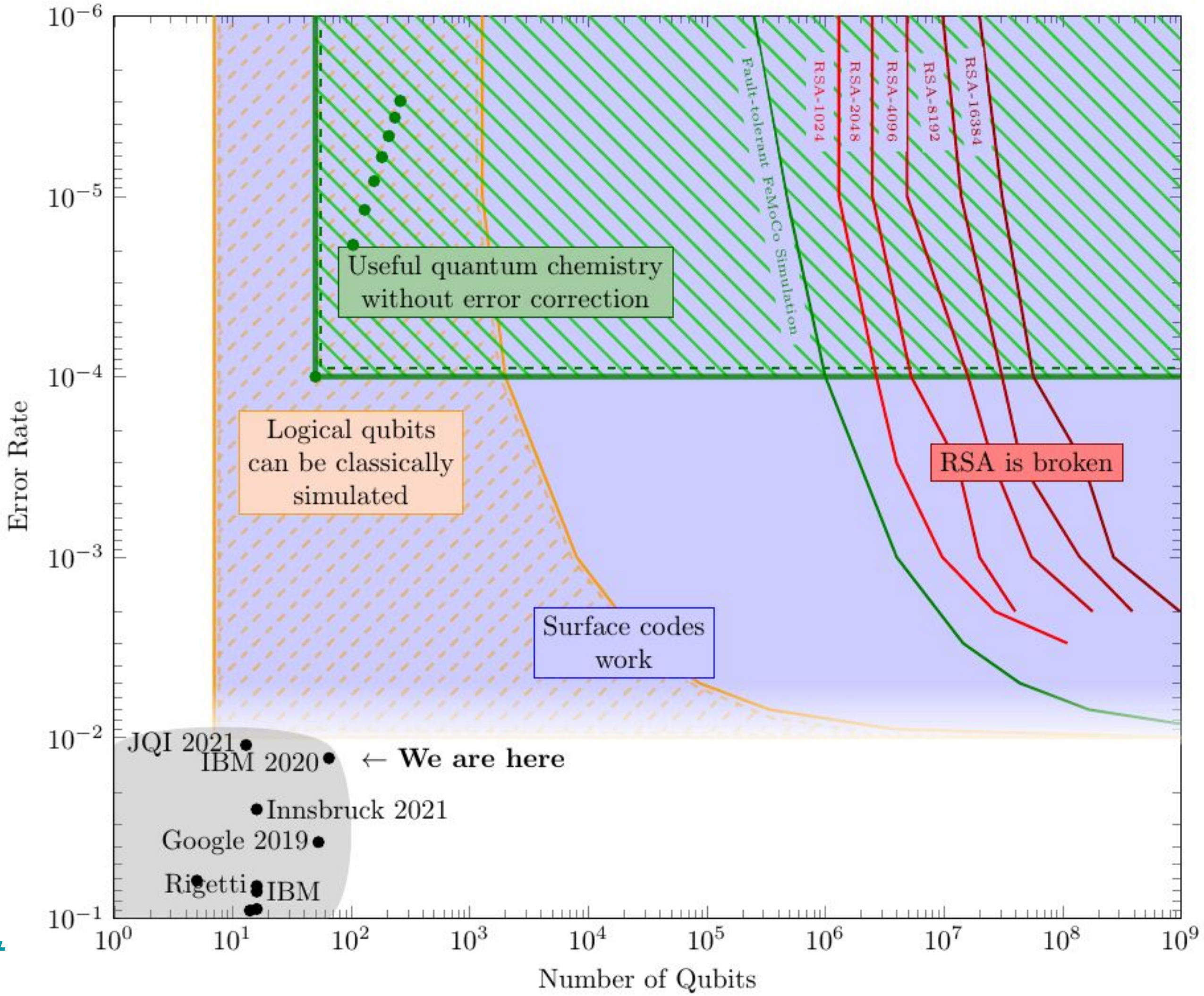
(In only about 5 minutes, I promise)

Bas Westerbaan
Research Engineer

Don’t just count qubits!

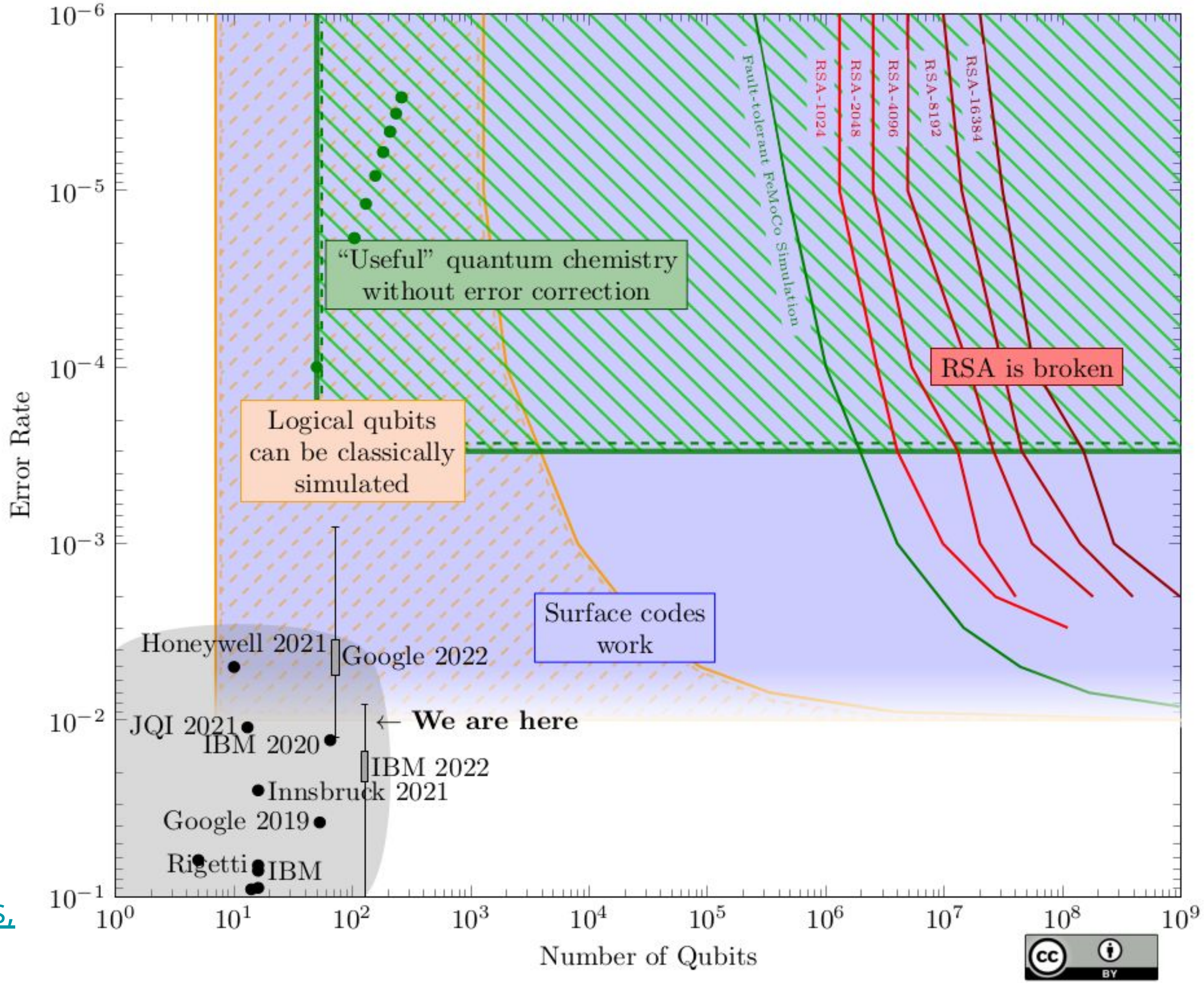
It’s about noise: Quantum computers are analog!

2021



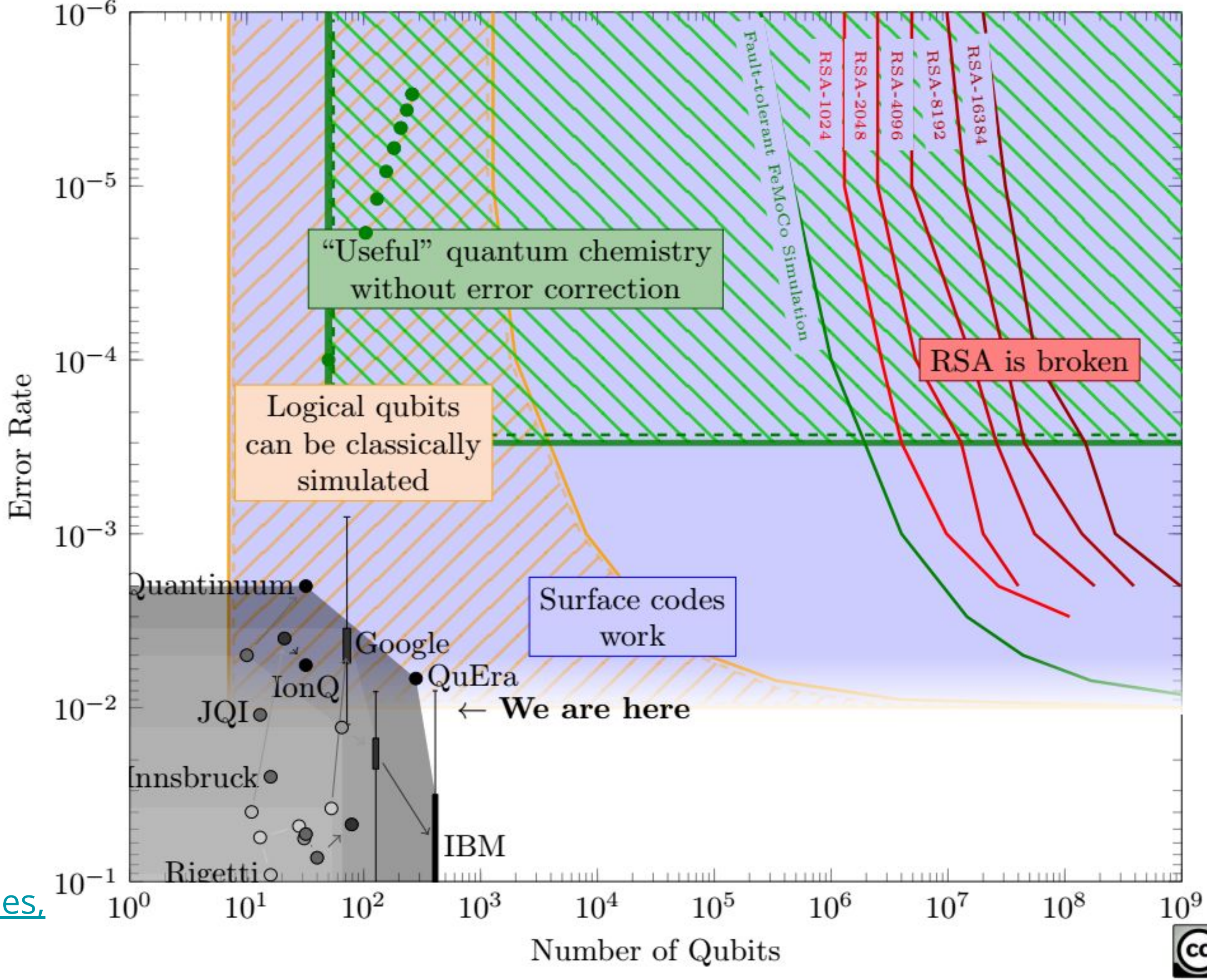
Credit: S. Jacques, U. of Waterloo.

2022

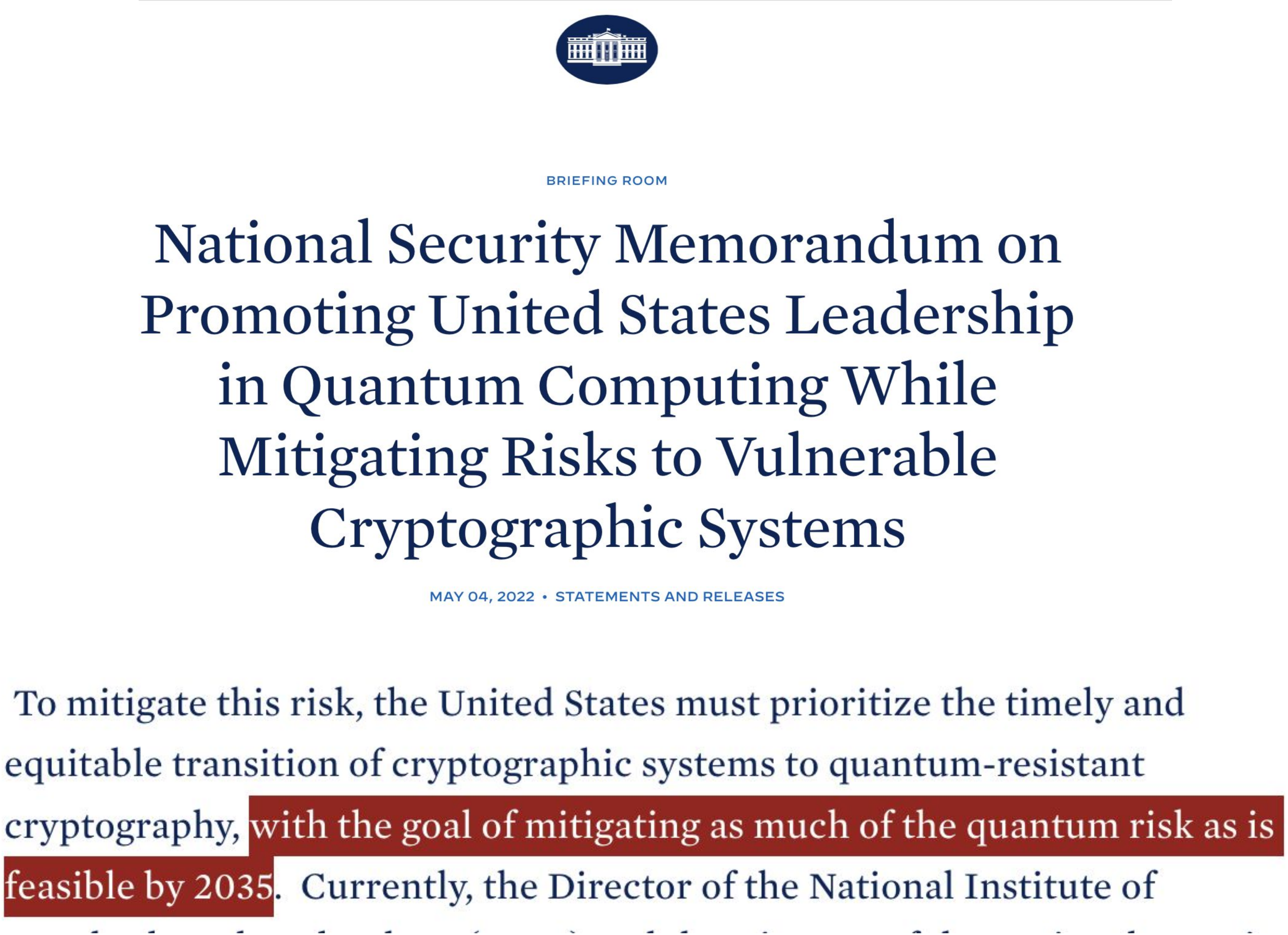


Credit: S. Jacques, U. of Waterloo.

2023



Credit: S. Jacques, U. of Waterloo.



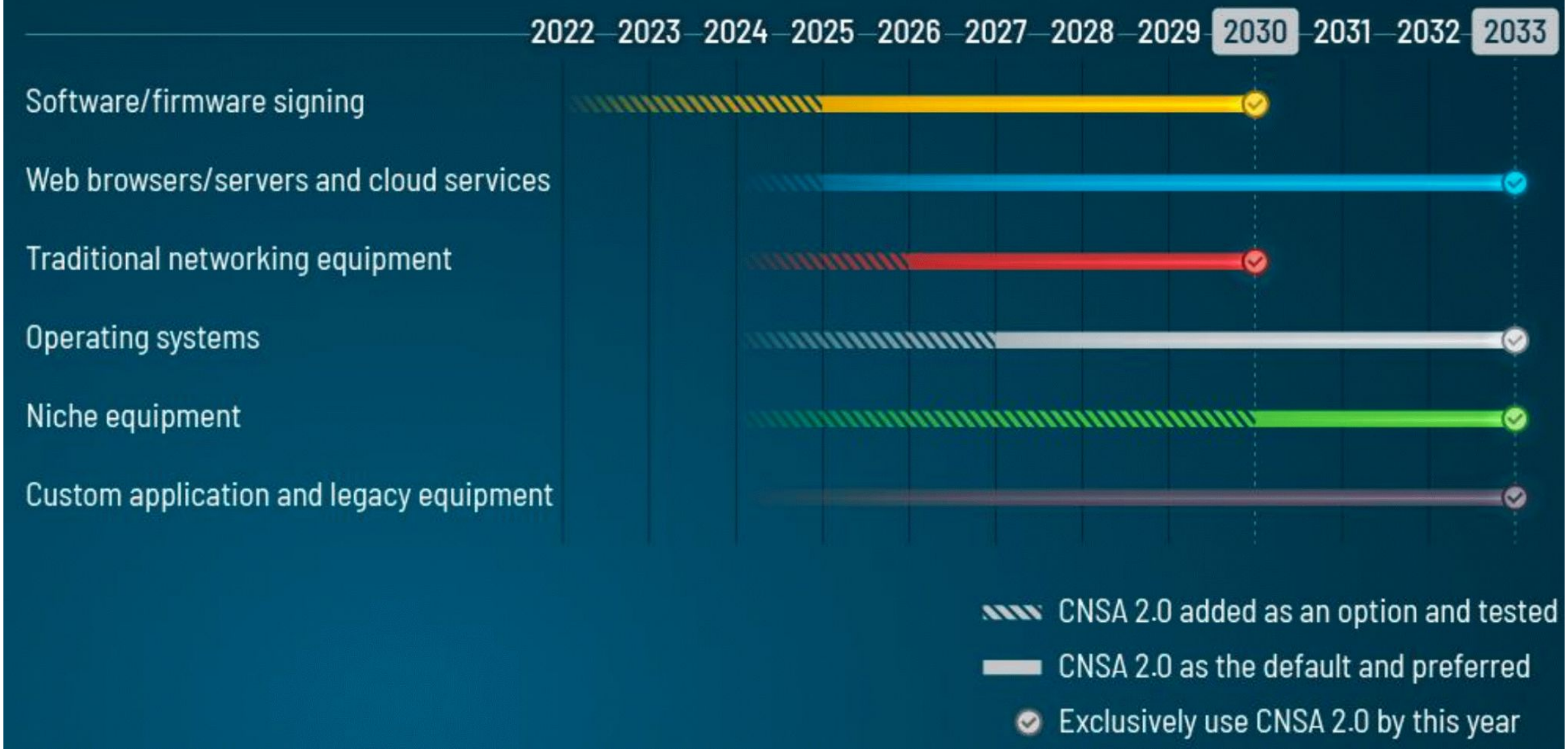
BRIEFING ROOM

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035. Currently, the Director of the National Institute of

CNSA 2.0 Timeline



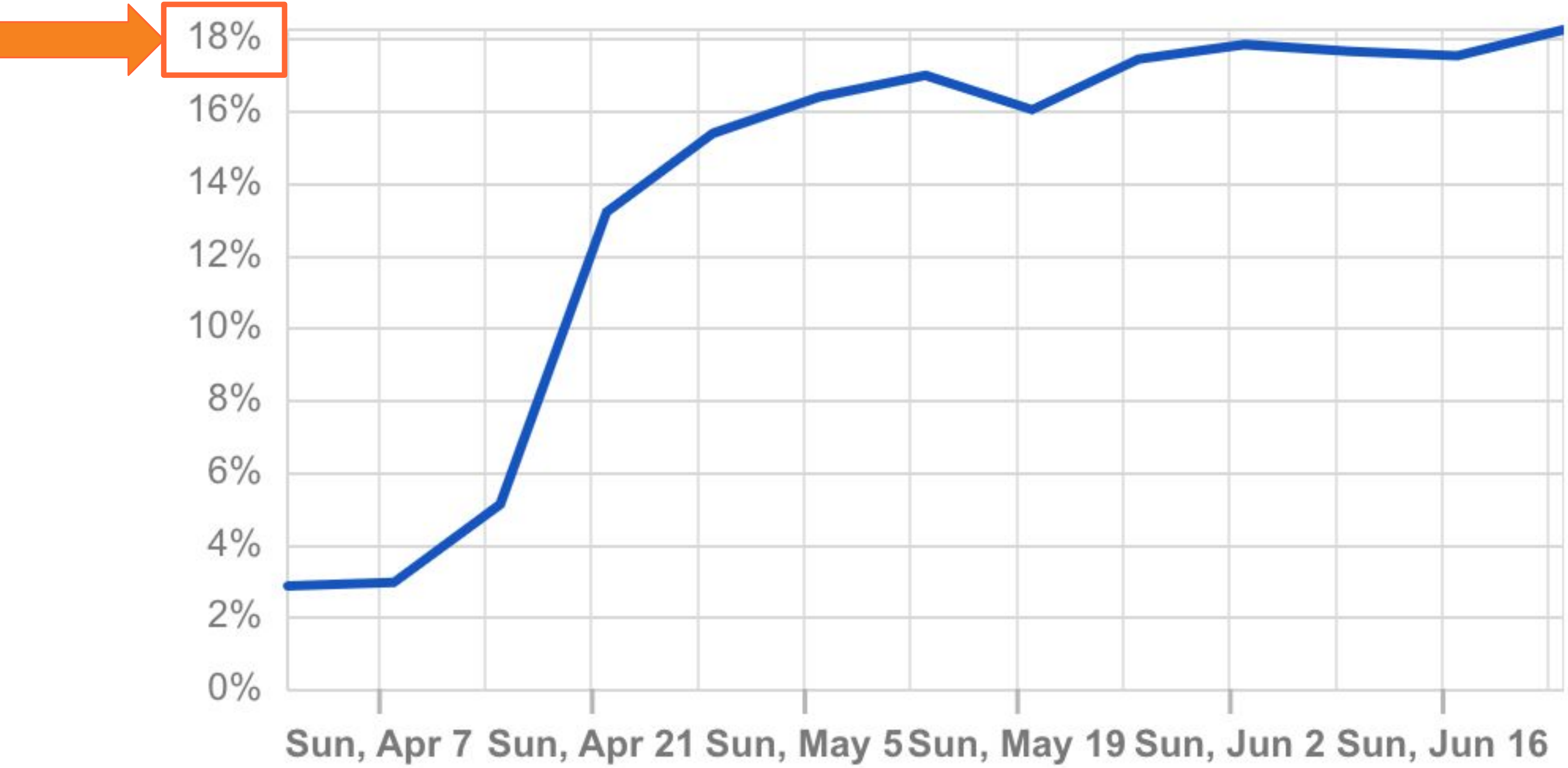
1. Key agreement 🤝

Communication can be recorded today and decrypted in the future. We need to upgrade as soon as possible.

2. Signatures 🖋️

Less urgent: need to be replaced before the arrival of cryptographically-relevant quantum computers.

(AES128 / SHA256 are fine. No need to double bitlengths.)



Client PQE adoption on Cloudflare Radar

			Sizes (bytes)		CPU time (lower is better)	
		PQ	Public key	Signature	Signing	Verification
Classical	Ed25519	❌	32	64	1 (baseline)	1 (baseline)
	RSA-2048	❌	256	256	70	0.3
NIST	ML-DSA-44	✅	1,312	2,420	4.8	0.5
	FN-DSA-512 ⚠️	✅	897	666	8 ⚠️	0.5
	SLH-DSA-128s	✅	32	7,856	8,000	2.8
	SLH-DSA-128f	✅	32	17,088	550	7
Sample from signatures onramp	MAYO$_{\text{one}}$	✅	1,168	321	4.7	0.3
	MAYO$_{\text{two}}$	✅	5,488	180	5	0.2
	SQISign I	✅	64	177	60,000	500
	UOV Is-pkc	✅	66,576	96	2.5	2
	HAWK512	✅	1,024	555	2	1

Thank you!

Further reading:

- State of the post-quantum Internet (‘24)
- Google’s writing