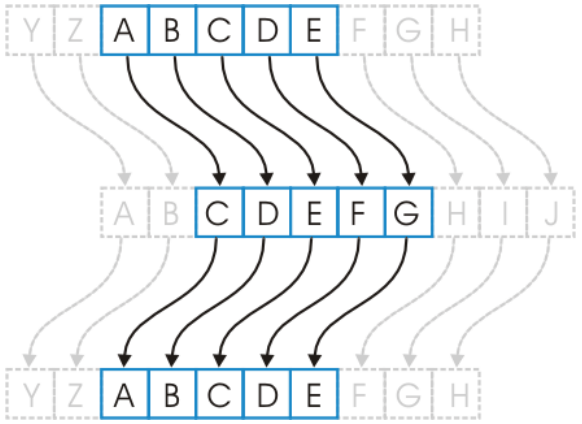
THE QUANTUM THREAT TO OUR DIGITAL SOCIETY

Thijs Laarhoven, PhD

Migrating towards quantum-secure cryptography

TNO innovation for life

SECURE COMMUNICATION



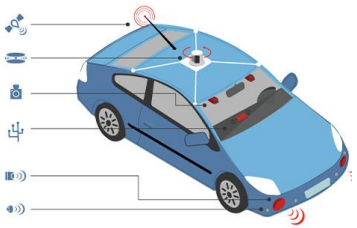
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

RSA SECURITY™

ECDSA

safe secure https://

OneDrive



PayPal

zoom

THREATS TO OUR (DIGITAL) SOCIETY

'A' for Angela

GCHQ and NSA Targeted Private German Companies and Merkel

Documents show that Britain's GCHQ intelligence service infiltrated German Internet firms and America's NSA obtained a court order to spy on Germany and collected information about the chancellor in a special database. Is it time for the country to open a formal espionage investigation?

Von Laura Poitras, Marcel Rosenbach und Holger Stark
29.03.2014, 14.55 Uhr

NIEUWS | *07 oktober 2021*

Industrieconcern VDL plat door cyberaanval

Leestijd van ongeveer 1 minuut

Hackers en spionnen zitten vuistdiep in Nederlandse systemen, Onderzoeksraad slaat alarm

VIDEO **Tot op de dag van vandaag hebben aanvallers toegang tot digitale systemen van Nederlandse bedrijven en organisaties. Het kabinet moet ingrijpen, zegt de Onderzoeksraad voor Veiligheid in een vernietigend rapport.**

TECHNOLOGY

Suspected Chinese hackers target telecoms, research in Taiwan, Recorded Future says

French Supreme Court raises constitutional questions over EncroChat hacking secrecy

Conseil Constitutionnel to decide whether 'defence secrecy' over state EncroChat cryptophone hacking breaches French constitution

IoT's Market Growth Outpaces Security and Hackers are Loving It

Natali Tshuva / 28 Feb 2022 / Data and Security / IoT

Hackers Destroyed Data at Key Ukraine Agency Before Invasion

- Ministry of Internal Affairs oversees the national police
- Large volume of telecom data also stolen amid troop buildup

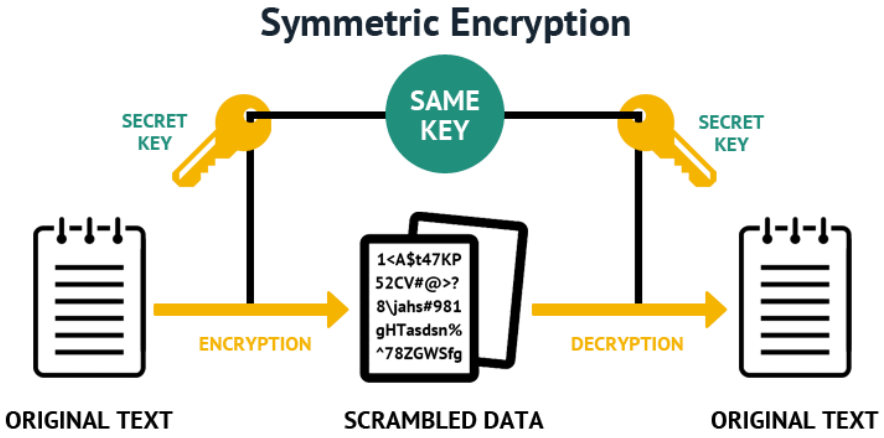
World News

Anonymous hack sees Ukraine national anthem played on Russian state's channels

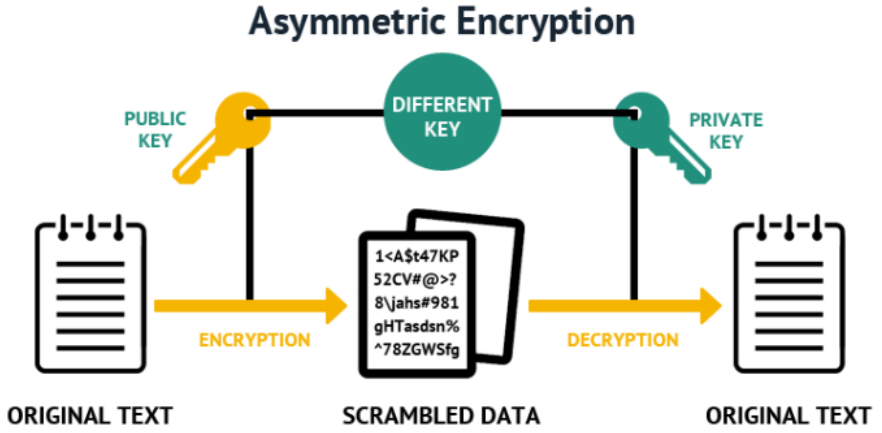
They sent a warning to Putin

MODERN CRYPTOGRAPHY

- Symmetric cryptography
  - Single key for both encryption and decryption
  - Requires agreeing upon a shared key beforehand
  - Examples: *AES*, *DES*, *Blowfish*, *Salsa20*, *ChaCha20*

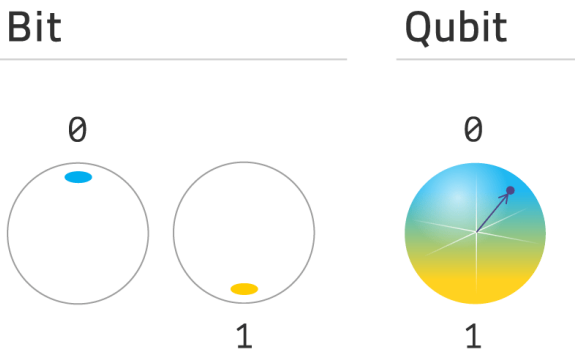


- Asymmetric ("public-key") cryptography
  - Keys for encryption (*public key*), decryption (*private key*)
  - Security based on hard computational problems
  - Can be used to generate a shared (symmetric) key
  - Examples: *RSA*, *DSA*, *ECDSA*, *Diffie-Hellman key exchange*

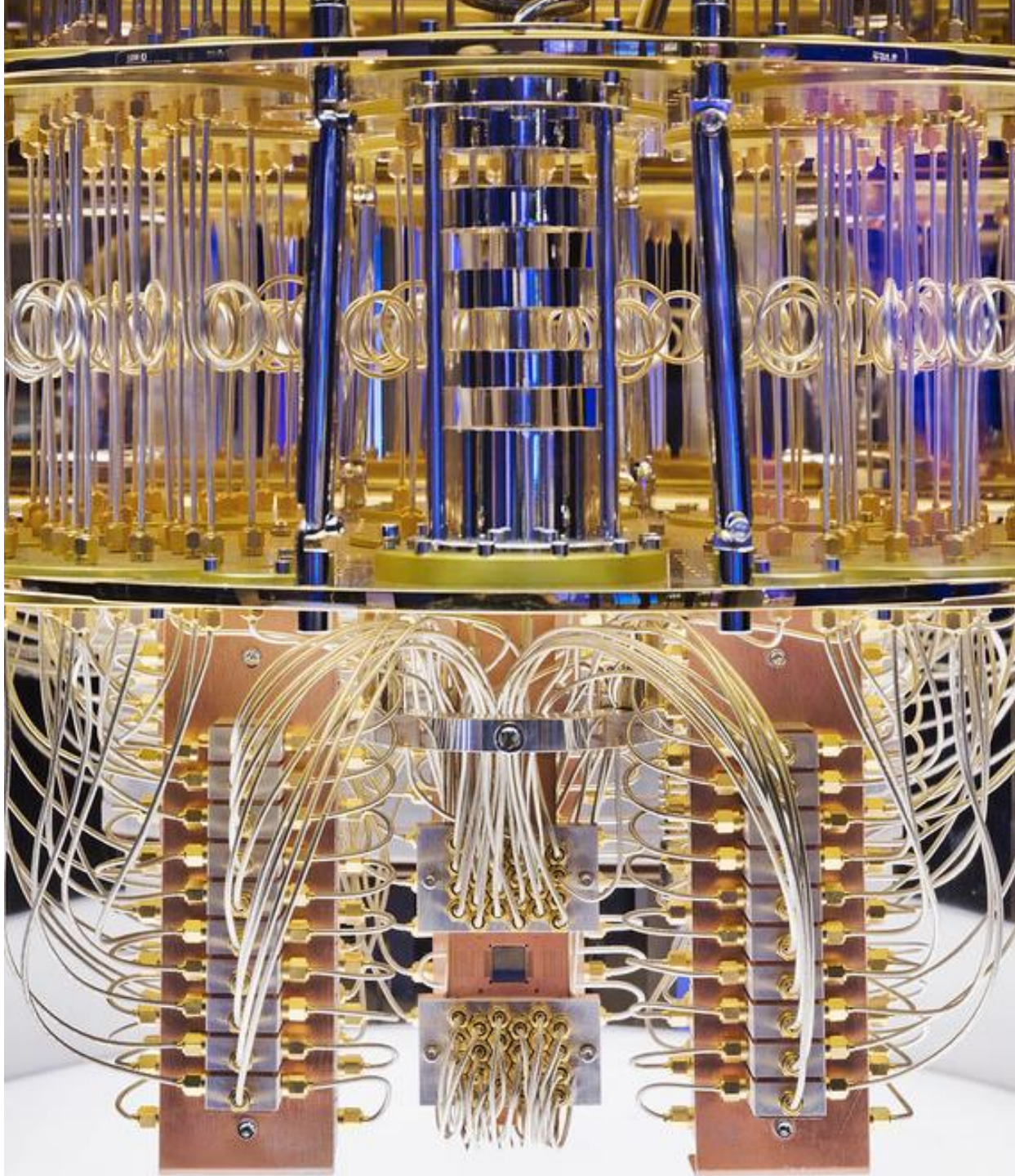


QUANTUM COMPUTERS

- Fundamentally different way of computation
- Makes use of so-called qubits rather than bits



- Various challenges: coherence, stability, scalability, error-correction
- Redefines which problems are “hard”



POWER OF QUANTUM COMPUTING

- Grover (1996): efficiently searching an unstructured list

$$a[i] = 00000000001000000000000000$$

$$a[11] = 1$$

- Shor (1994): efficiently factoring large integers, computing discrete logarithms, …

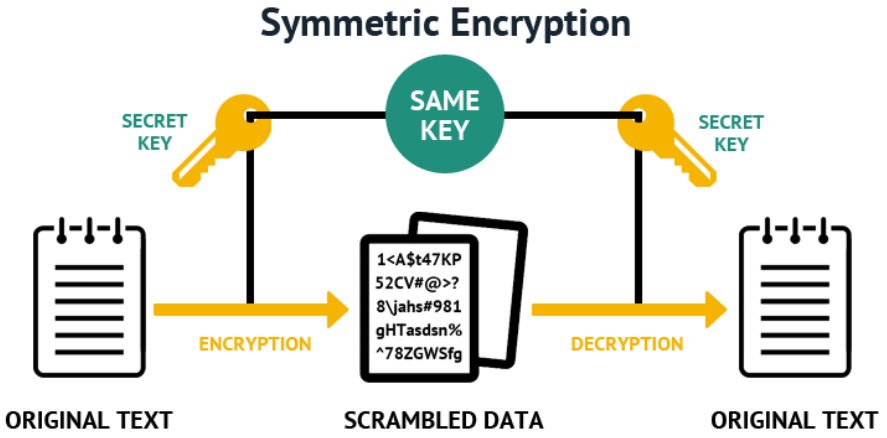
$$n = 5126641943039633$$

$$n = 54271853 \cdot 94462261$$

QUANTUM THREAT TO MODERN CRYPTOGRAPHY

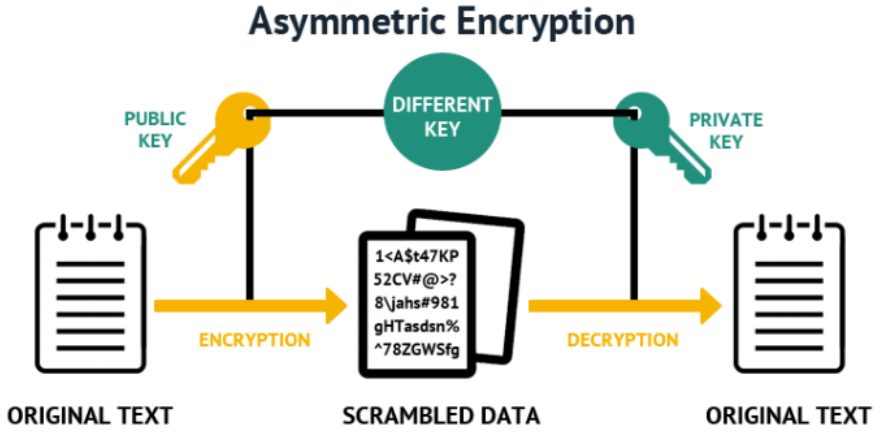
- Symmetric cryptography
  - Single key for both encryption and decryption
  - Requires agreeing upon a shared key beforehand
  - Examples: *AES*, *DES*, *Blowfish*, *Salsa20*, *ChaCha20*

Weakened by quantum attacks (Grover)



- Asymmetric ("public-key") cryptography
  - Keys for encryption (*public key*), decryption (*private key*)
  - Security based on hard computational problems
  - Can be used to generate a shared (symmetric) key
  - Examples: *RSA*, *DSA*, *ECDSA*, *Diffie-Hellman key exchange*

Completely broken by quantum attacks (Shor)



TOWARDS A LARGE-SCALE QUANTUM COMPUTER

NEWS | 23 October 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

Amazon, IBM and Microsoft race to bring global access to quantum computing

Quantum computing could help companies without billion-dollar budgets design superbatteries, create complex chemicals and understand the universe.

India to invest $1bn in quantum computing

India plans to invest $1bn over the next five years to advance its capabilities in quantum technology, but it will need to have a tailored approach and to address the skills gap to succeed

By **Pratima Harigunani** Published: **14 Feb 2022 8:31**

NEWS FEATURE | 02 October 2019

Quantum gold rush: the private funding pouring into quantum start-ups

A *Nature* analysis explores the investors betting on quantum technology.

TECHNOLOGY NEWS MAY 11, 2021 / 10:52 AM / UPDATED 10 MONTHS AGO

Germany to support quantum computing with 2 billion euros

By Reuters Staff 2 MIN READ

US begins $1 billion quantum computing plan to get ahead of 'adversaries'

The government is funding basic research in AI, too.

Microsoft just upped its multi-million bet on quantum computing

Microsoft pours millions into a new Station Q outpost in Copenhagen.

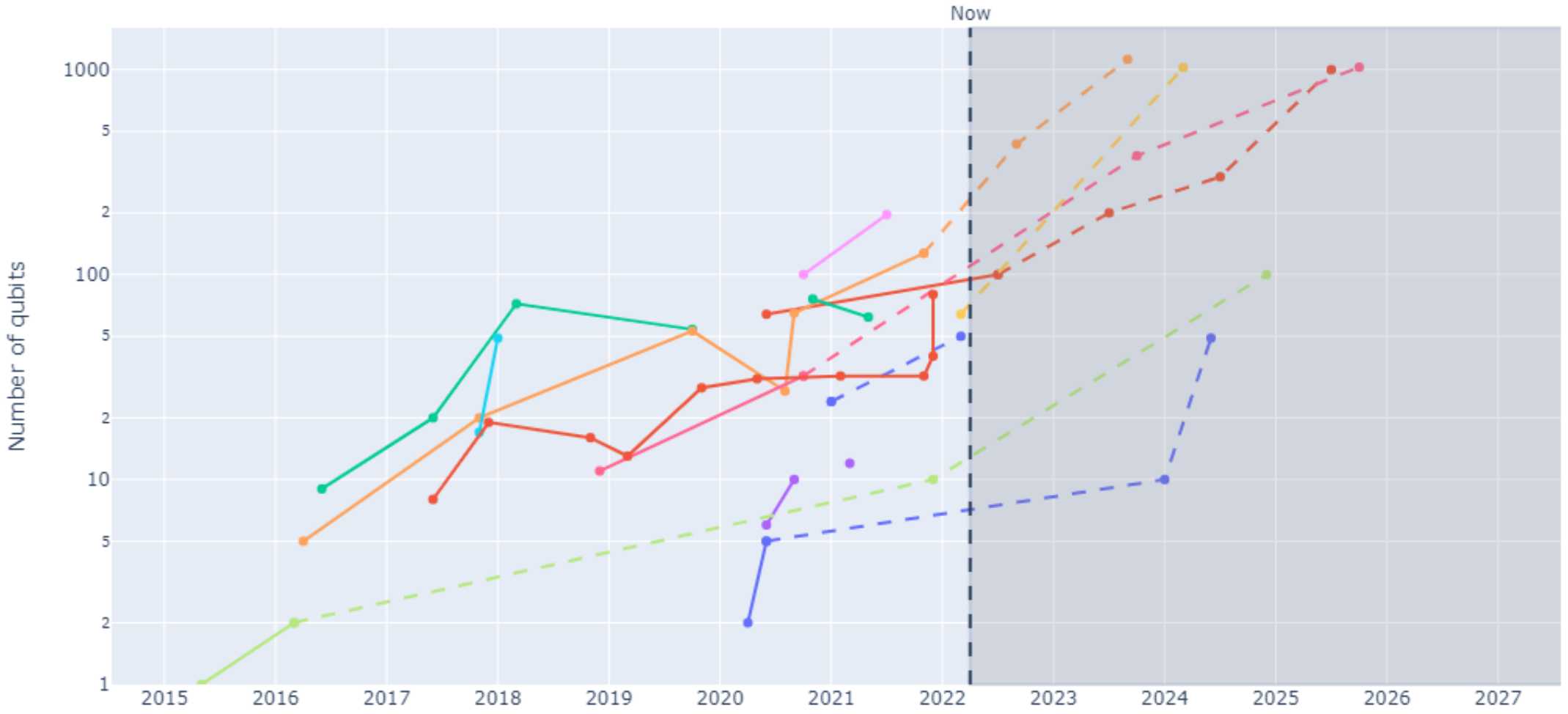
January 31, 2022

IBM Unveils 127-Qubit Quantum Computer

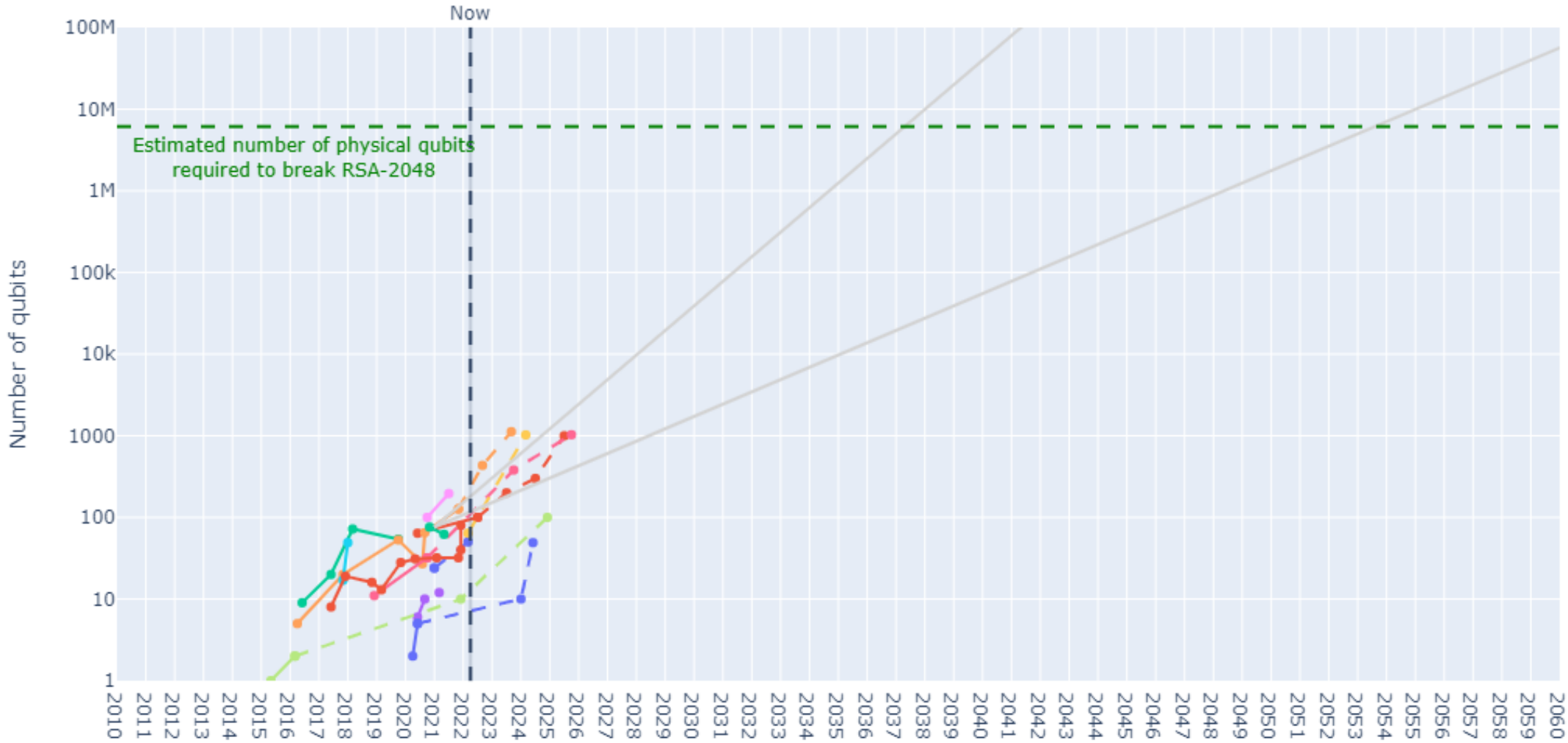
Hold on. This is Going to Make Your Head Hurt

by Steven Leibson

TOWARDS A LARGE-SCALE QUANTUM COMPUTER

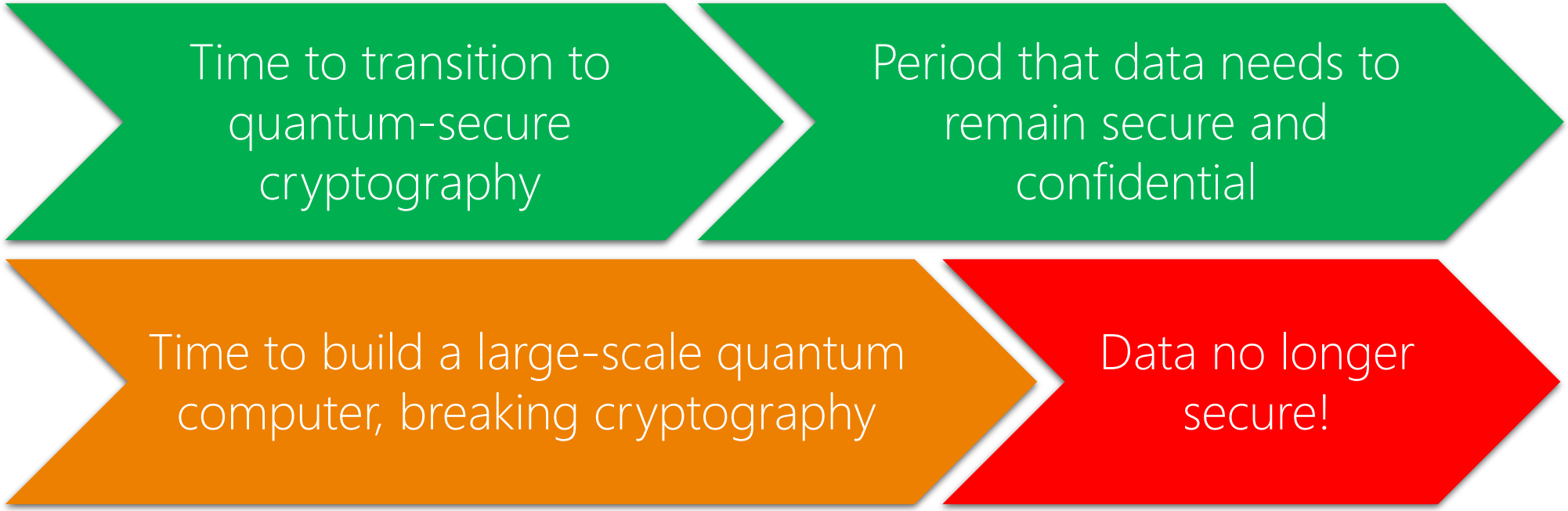


TOWARDS A LARGE-SCALE QUANTUM COMPUTER

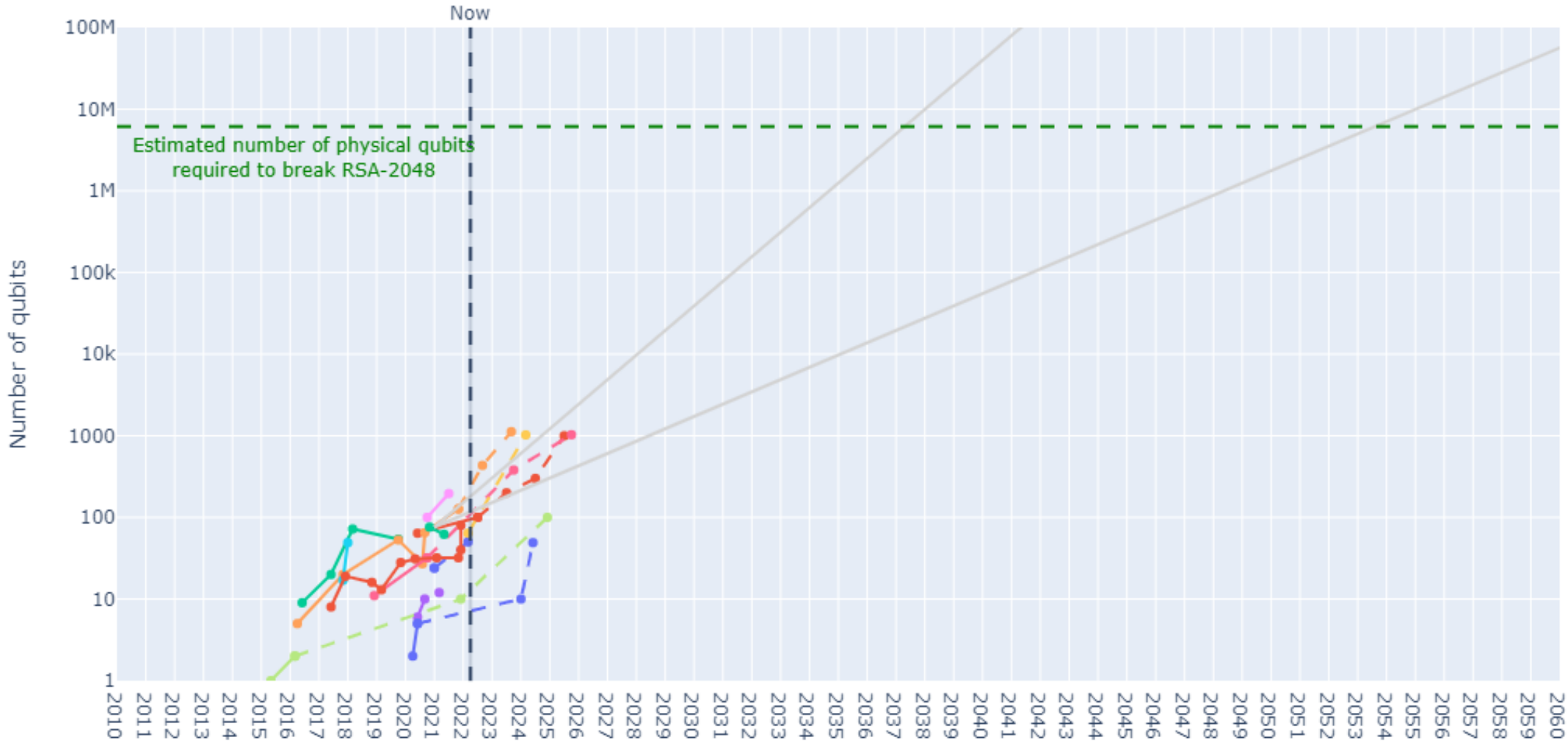


WHY SHOULD WE CARE NOW?

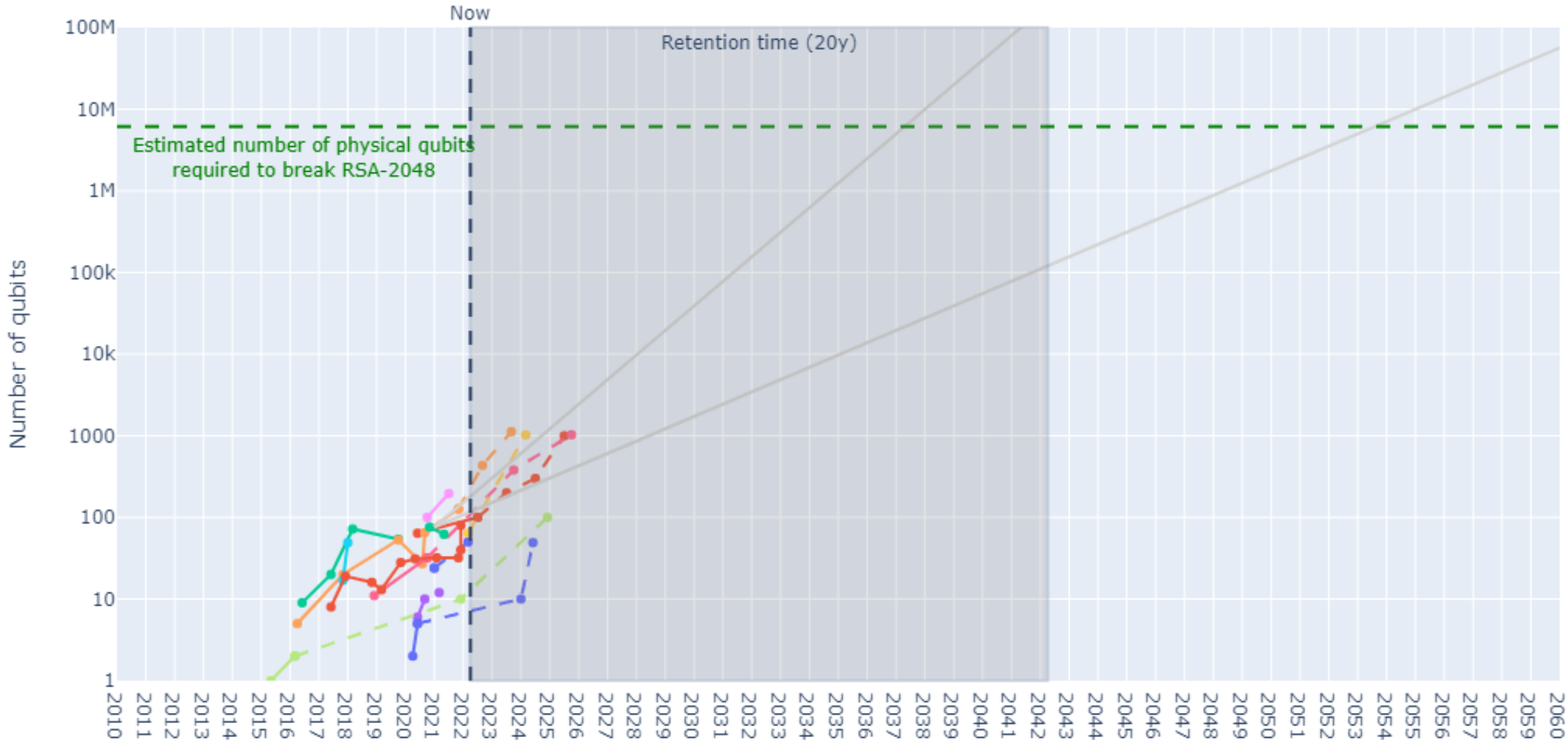
- **Mosca's inequality**: assessing urgency to transition (2015)



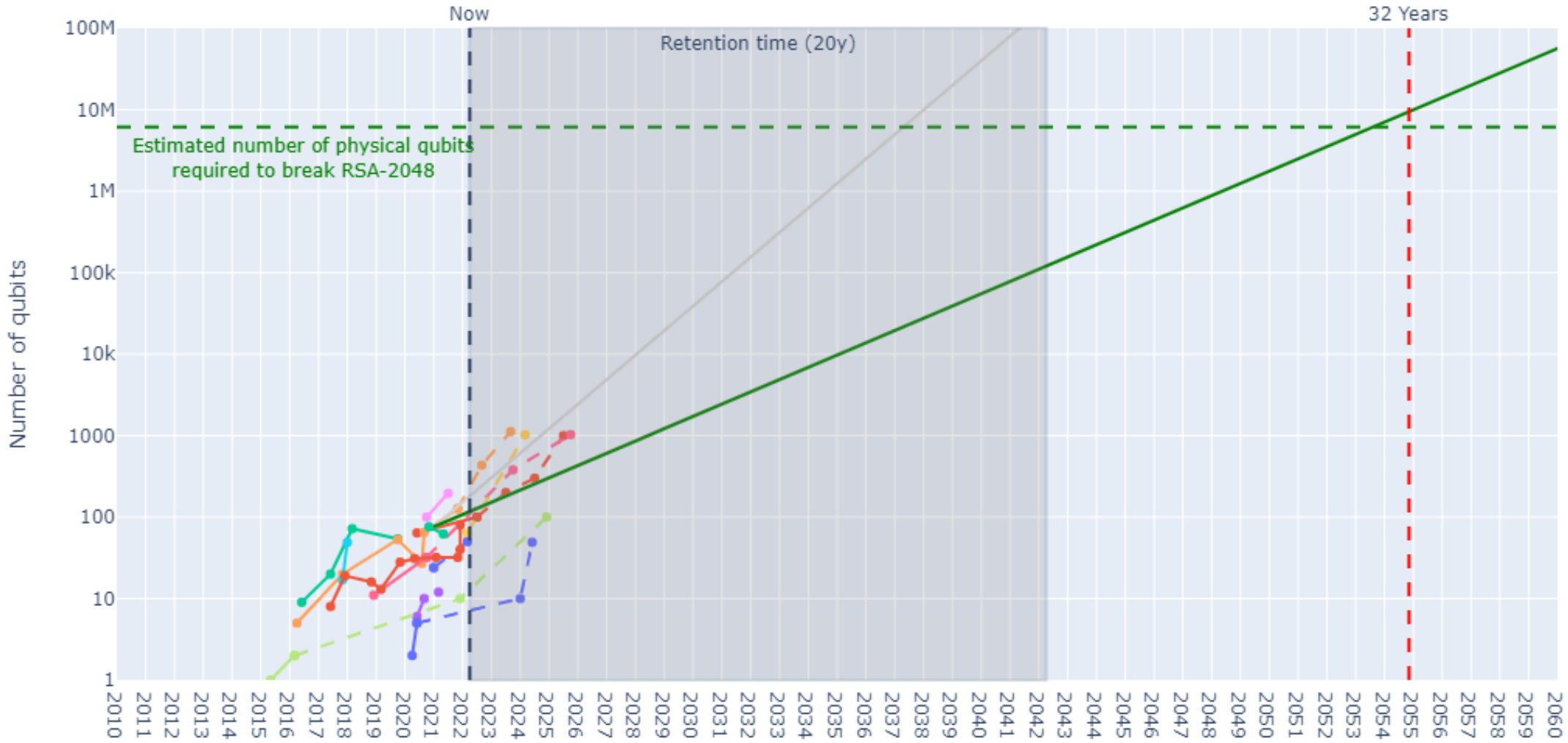
QUANTUM COMPUTING PREDICTIONS



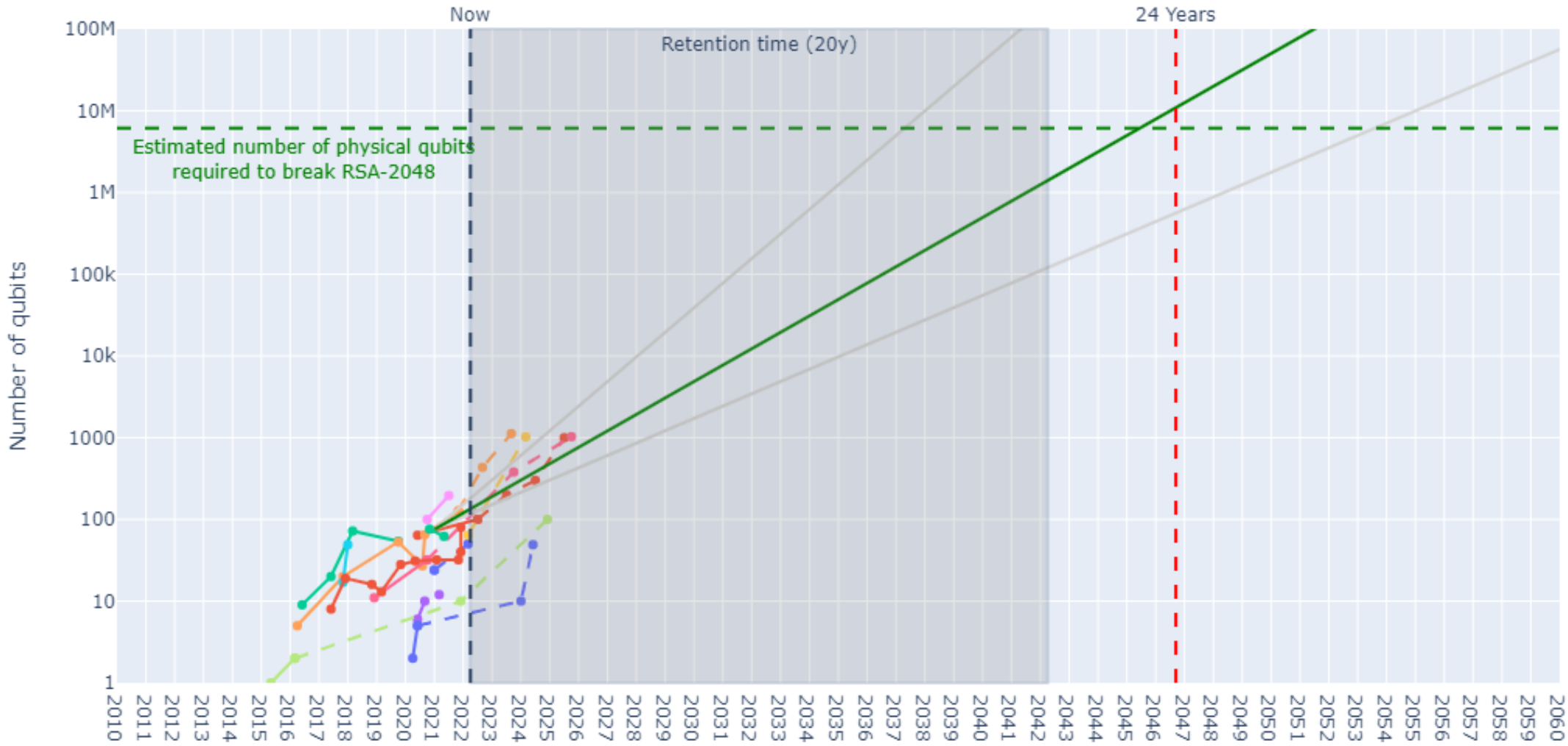
QUANTUM COMPUTING PREDICTIONS



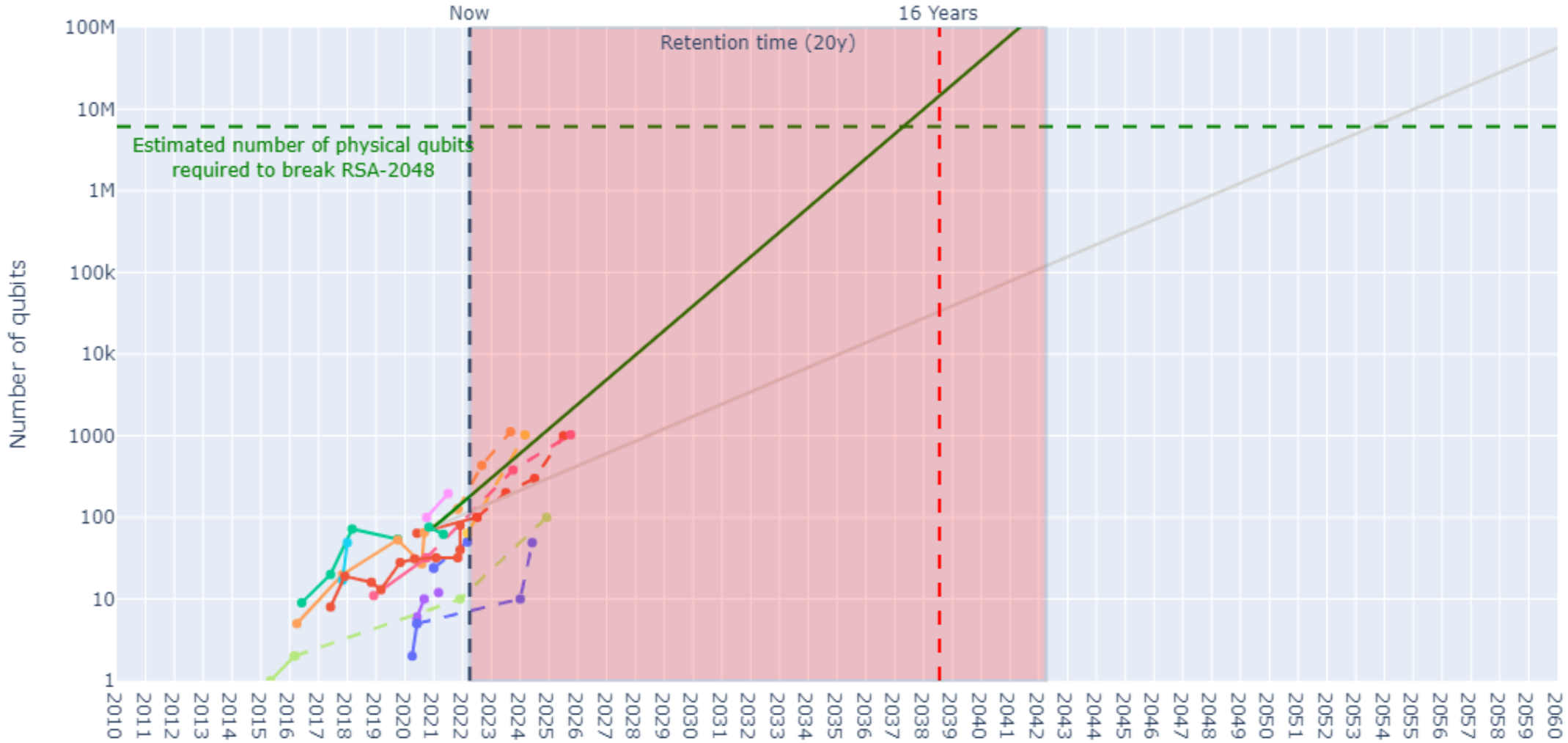
QUANTUM COMPUTING PREDICTIONS (X2 EVERY 2YR)



QUANTUM COMPUTING PREDICTIONS (X2 EVERY 1.5YR)

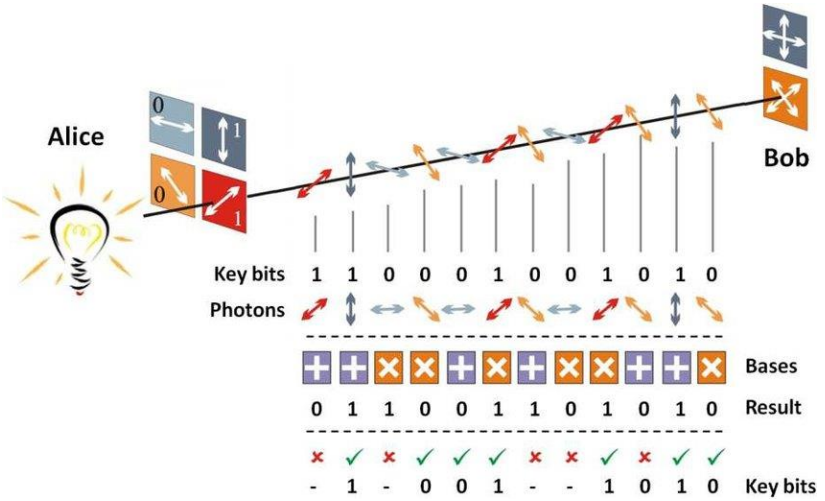


QUANTUM COMPUTING PREDICTIONS (X2 EVERY 1YR)

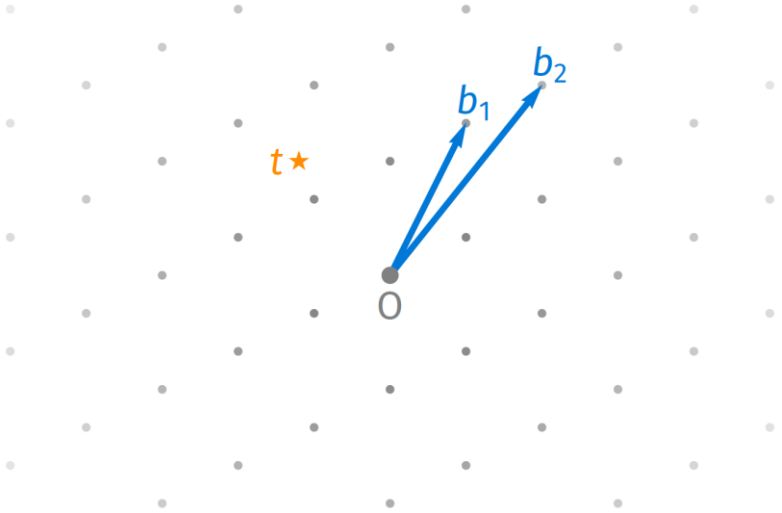


WHAT CAN WE DO?

- "Quantum" cryptography
  - Uses quantum physics: **Requires quantum hardware!**
  - Perfect security in high-profile applications
  - Not practical for most real-world applications



- "Post-quantum" (or "quantum-secure") cryptography
  - Does not use quantum computing: **Can already be used now!**
  - Based on lattices, codes, and other mathematical objects
  - In general, small efficiency loss compared to "classical" methods



POST-QUANTUM CRYPTOGRAPHY – COMPARISON

	Features			Speed			Memory		
	Post-Q	Mature	Versatile	KeyGen	Encrypt	Decrypt	PubKey	PrivKey	CT/Sig
Factoring									
Discrete log									
Elliptic curves									
Lattices									
Codes									
Multivariate									
Hash-based									
Isogenies									

POST-QUANTUM CRYPTOGRAPHY – TIMELINE

- Past timeline
  - **Feb 2016:** NIST report on post-quantum cryptography
  - **Dec 2016:** NIST call for submissions
  - **Nov 2017:** Deadline for submissions
  - **Dec 2017:** Round 1 – 69 candidates
  - **Jan 2019:** Round 2 – 26 candidates
  - **Jul 2020:** Round 3 – 7 finalists, 8 alternates

- Future timeline
  - **Mar 2022**: Round 4
  - **2023/24**: NIST standards announced
  - **2023/24+**: Other standards (ETSI, IETF, IEEE, ISO, …)

SUMMARY

- Hacking efforts and cyber warfare intensifying

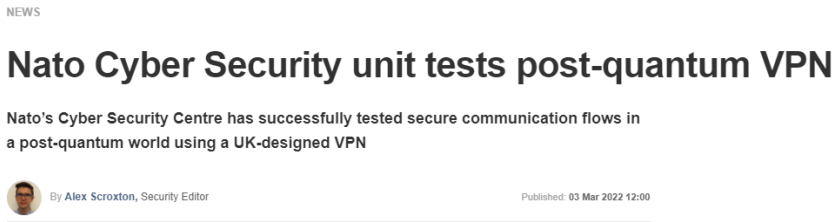
- **Quantum threat** is looming, needs to be addressed urgently
  - **Symmetric cryptography**: increase (double) key sizes
  - **Asymmetric cryptography**: need new cryptographic algorithms

- **Mosca's theorem**: act before it is too late
  - **Defensive side**: estimate **retention time** and **transition time**
  - **Attacking side**: stay updated on quantum computing predictions

- **Post-quantum cryptography** solutions exist, and will soon be standardized

TOWARDS POST-QUANTUM CRYPTOGRAPHY

- High security, long-term confidentiality: **start migrating soon!**
  - Use hybrid of classical and post-quantum cryptography
  - Secure, good reputation: **code-based encryption** (*McEliece*)


NEWS

Nato Cyber Security unit tests post-quantum VPN

Nato's Cyber Security Centre has successfully tested secure communication flows in a post-quantum world using a UK-designed VPN

By Alex Scroxton, Security Editor

Published: 03 Mar 2022 12:00

- Other use cases: **raise awareness, and prepare for upcoming standards**
  - Either use hybrid or wait for mature standards
  - Emphasis on efficiency: **structured lattices** (*NTRU*, *Kyber*, *Saber*, *Dilithium*, *Falcon*)
  - Emphasis on security: **unstructured lattices** (*Frodo*)
  - Making fewer assumptions: **hash-based/symmetric signatures** (*SPHINCS*, *Picnic*)


THANK YOU FOR
YOUR ATTENTION
TNO
innovation
for life