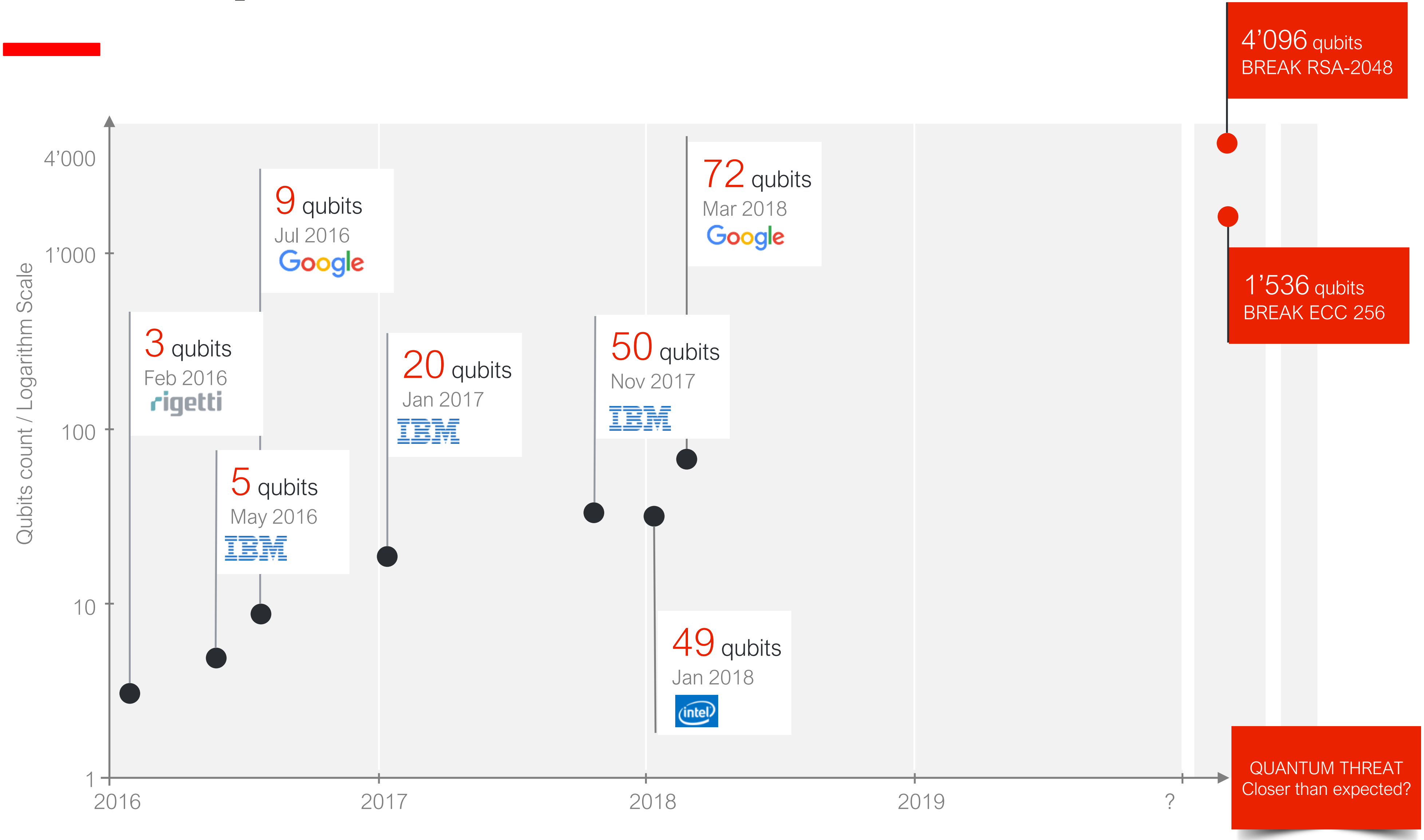
Post-Quantum Cryptography

Tomislav Nad | contact@tnad.at

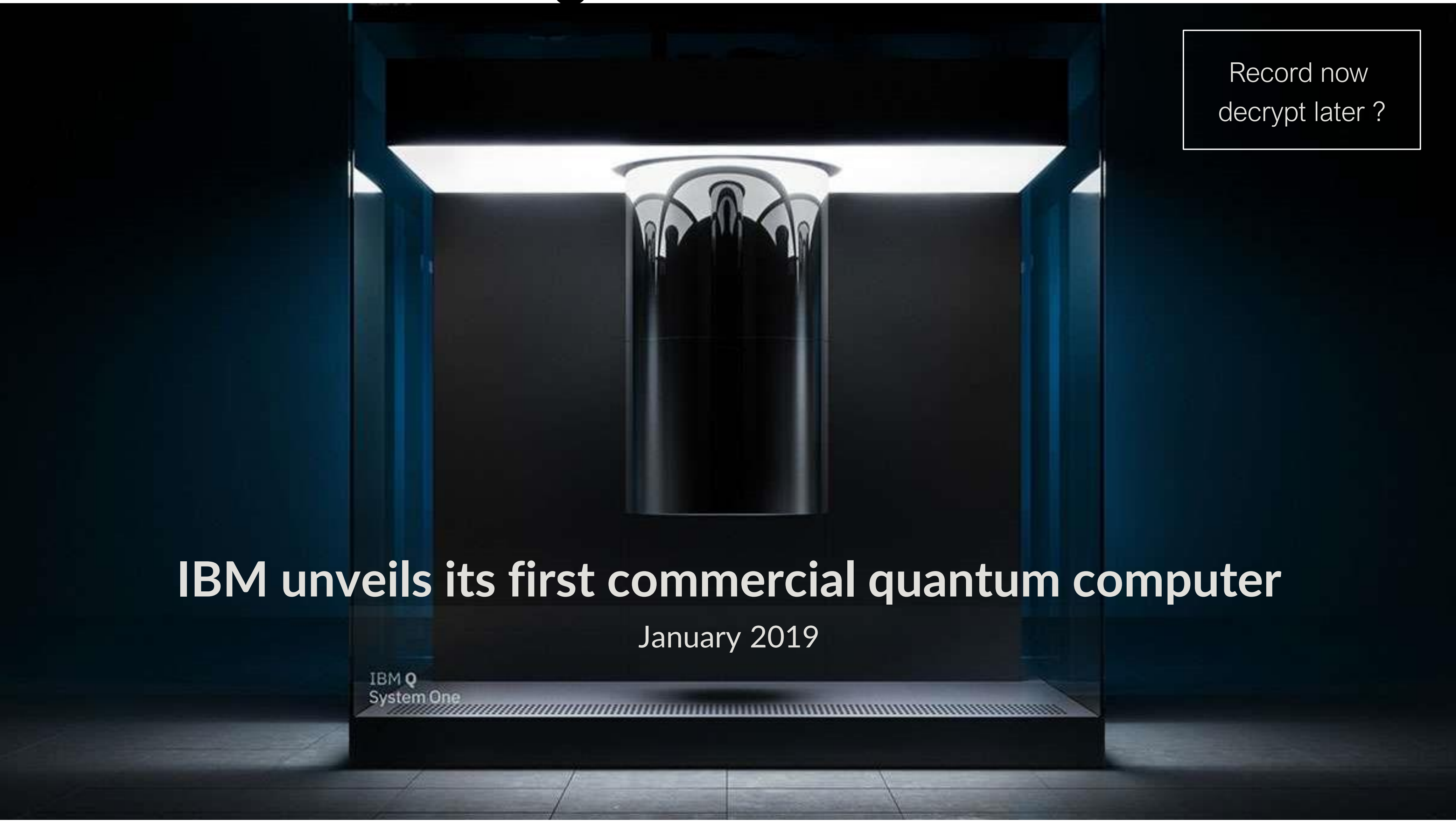
Quantum Computer

- Ongoing practical research and development paves the way for building large-scale quantum computers.
- Small scale quantum computers already exist.
- In about 10-20 years, large-scale quantum computers could become a reality.

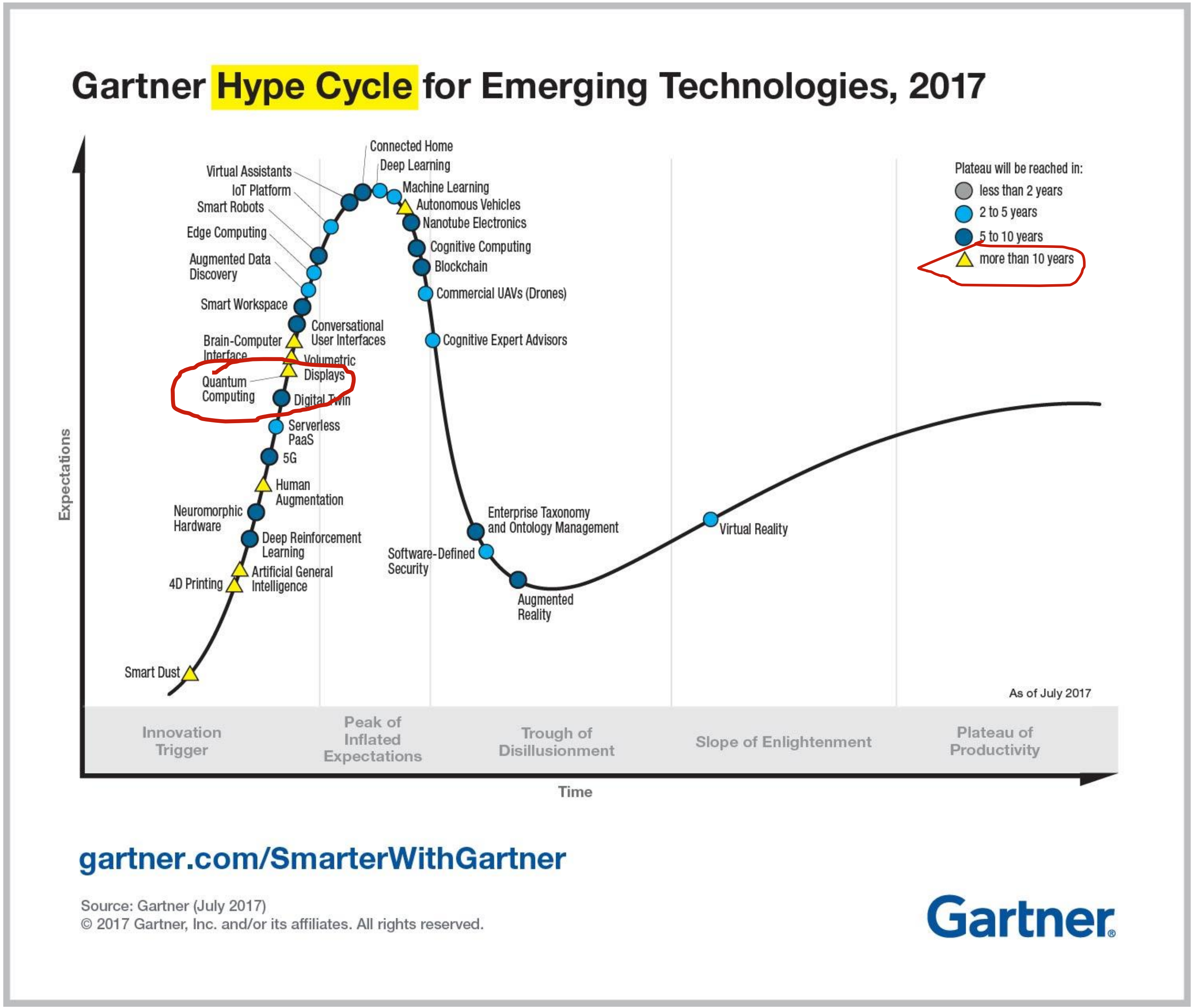
Development



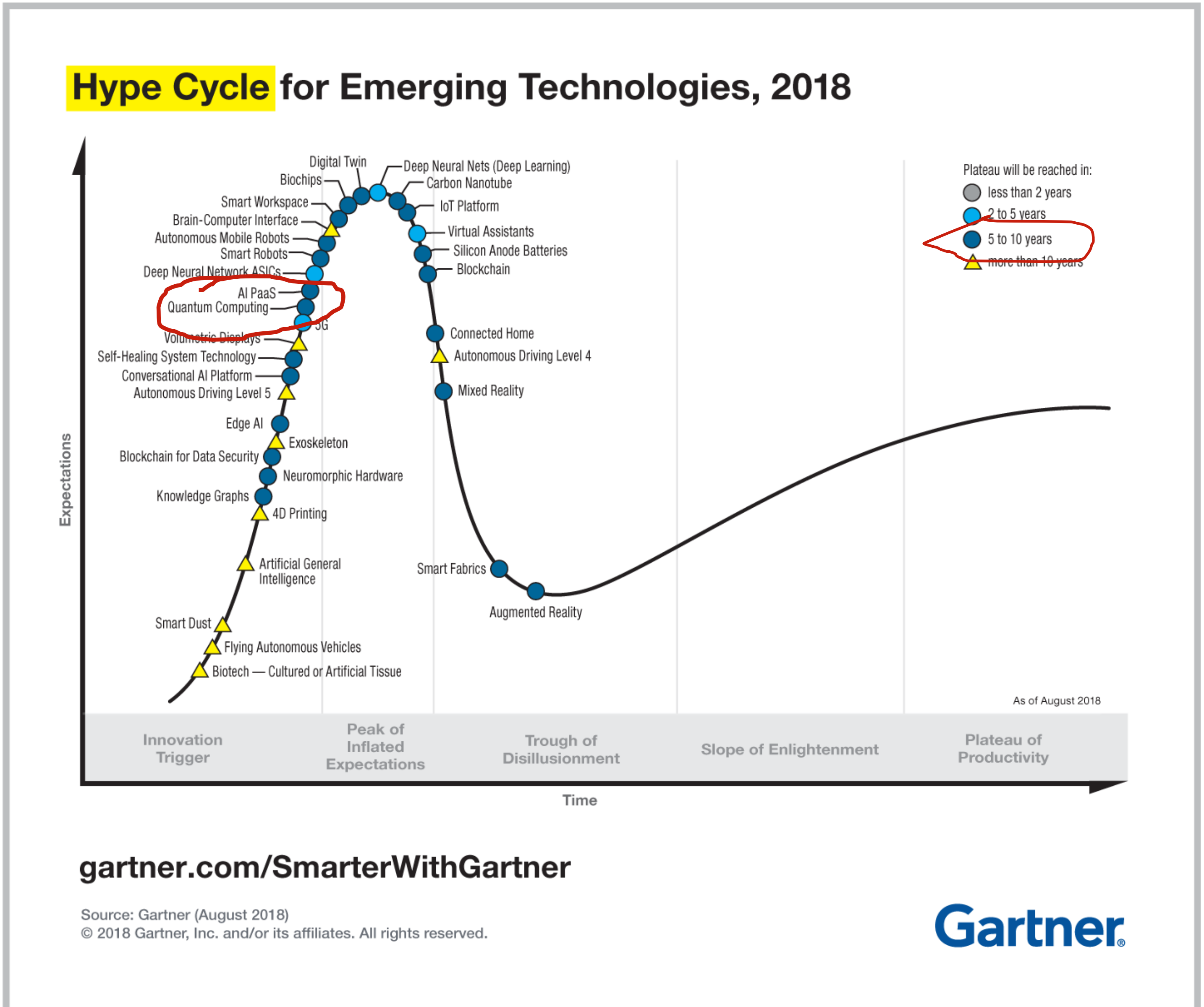
Commercialising



Gartner Hype Cycle 2017



Gartner Hype Cycle 2018



Global Initiatives (just examples)

- Quantum Flagship

- Centre For Quantum Computation and Com. Technology

- National Quantum Initiative Act

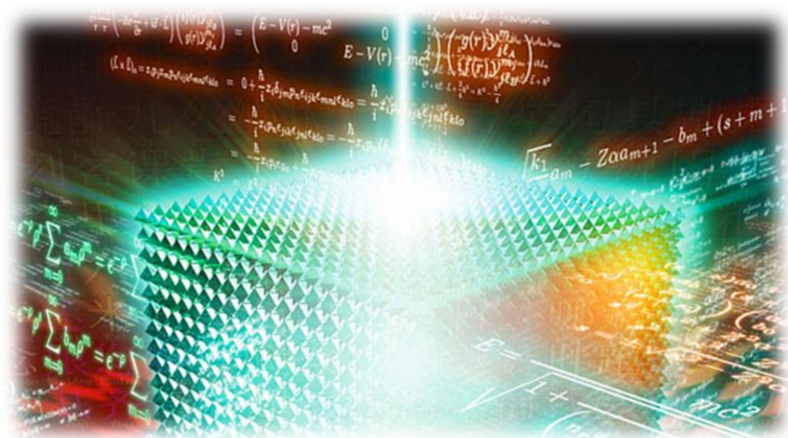
- National Laboratory for Quantum Information Sciences

Companies

- Too many to list…

Capabilities of Quantum Computers

- Quantum computers will be able to perform computations much faster.
- Search algorithms can be performed in square root time (Grover's algorithm).
- Factorization and discrete logs can be computed in polynomial time (Shor's algorithm)



How is Cryptography Affected?

Symmetric:

- Generic square root quantum search algorithms apply.
- Need to double the key length.

Public-Key:

- Schemes, whose security is based on integer factorization (RSA), can be broken in quantum polynomial time.
- Schemes, based on DLOG problem, can be broken in quantum polynomial time.
- All of the currently standardized asymmetric cryptography (RSA, ECC) can be efficiently broken by a quantum adversary!
- No ‘easy fix’ as for symmetric cryptography.

How is Cryptography Affected?

Algorithm	Key length	Security Level Conventional Computer		Security Level Quantum Computer	
RSA-1024	1024 bits	80 bits	BROKEN	0 bits	BROKEN
RSA-2048	2048 bits	112 bits	VIABLE	0 bits	BROKEN
ECC-256	256 bits	128 bits	VIABLE	0 bits	BROKEN
ECC-384	384 bits	256 bits	VIABLE	0 bits	BROKEN
AES-128	128 bits	128 bits	VIABLE	64 bits	BROKEN
AES-256	256 bits	256 bits	VIABLE	128 bits	VIABLE

MATERIAL IMPACT EXPECTED

Problem | Quantum Computer Threat # Today

Record Now, Decrypt Later

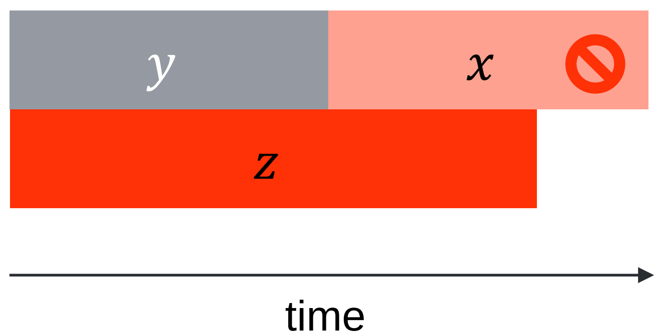
https://www.sciencenews.org/article/google-moves-toward-quantum-supremacy-72-qubit-computer

Transition Period

By Michele Mosca, https://eprint.iacr.org/2015/1075.pdf

- How long does your information need to be secure (x)
- How long to deploy quantum safe solutions (y)
- How long until a large-scale quantum computer (z)

If $x + y > z$ then worry



Prepare for the Quantum Computer

Create a Crypto Inventory

Know your vulnerabilities

Move to a Crypto Agile System

Do the effort once

Use standard crypto for now

Move to NIST standards

NIST published its standards

Risk Assessment

When do I need to worry?

Move to PQC

Use todays PQC algorithms

Monitor Crypto Threats

Ready for future crypto challenges

Today → **Quantum Computer Risk**

Post-Quantum Cryptography

Quantum Safe Cryptosystems

CO

Code Based Cryptosystems

Security is based on the difficulty of decoding linear codes. It is famous for being the oldest public key encryption scheme that is potentially quantum safe.

HA

Hash Based Cryptosystems

Security is based on hash functions. The most famous schemes are XMSS and SPHINCS.

LA

Lattice Based Cryptosystems

Security is based on the shortest vector problem in a lattice. The most famous schemes include NTRU or cryptosystems based on Learning With Errors (LWE).

IS

Isogeny Based Cryptosystems

Security is based on the problem to find an isogeny between supersingular elliptic curves. The most famous scheme is SIDH.

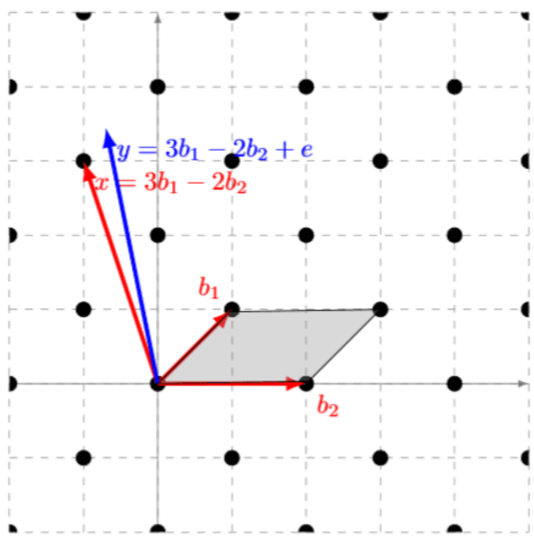
MU

Multivariate Based Cryptosystems

Security is based on the problem of solving a set of non-linear equations. The most famous scheme is the Hidden Field Equations cryptosystems.

Lattice-Based

- Many lattice-based approaches exist, depending on the underlying hard problem: Closest Vector Problem (CVP), Learning With Errors (LWE), Ring-LWE (RLWE) and others
- Used for signatures, encryption, KEM



Code-Based

- Based on error-correcting codes
- The hard problem is based on hardness of decoding general linear code (NP-hard)

- Used for signatures, encryption, KEMs

Isogeny-Based

- Supersingular elliptic curve isogeny cryptography
- Extension of elliptic curve cryptography
- Hard problem is based on the difficulty of computing the isogeny between curves

- Used for key encapsulation

Hash-Based

- One-time and few-time signatures form the building blocks
- Use a tree structure
- Security only depends on the security of the underlying hash function

- Used for signatures

Multivariate-Based

- Based on multivariate polynomials over a finite field F
- Uses affine transformations and affine endomorphisms
- Hard problem is solving the system of multivariate polynomial equations

- Used for signatures

NIST Competition

- Submission deadline: Nov 30, 2017
- 69 round 1 candidates
- April 2018: first NIST PQC Workshop
- Second round began January 2019
- August 2019: second NIST PQC Workshop
- 2020/2021 - Select algorithms or start a 3rd Round
- 2022-2024 - Draft standards available

- Note: Standard organizations such as ETSI, IETF, ISO, and X9 are all working on recommendations.

NIST Competition

- Submissions

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multivariate	7	2	9
Symmetric/Hash-based	3	0	3
Isogeny-based	0	1	1
Other	2	4	6
Total	19	45	64

NIST Competition

- Round 2

	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based	0	7	7
Multivariate	4	0	4
Symmetric/Hash-based	2	0	2
Isogeny-based	0	1	1
Other	0	0	0
Total	9	17	26

- https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions

Benchmarks

- https://bench.cr.yp.to/supercop.html
- https://www.safecrypto.eu/pqclounge/

Signature Algorithm

- CPU cycles and bytes

Category	Scheme	Key generation	Sign	Verify	Signature
Hash-based	Sphincs+-SHA256-128f	7’170’350	238’582	9’951’241	16’976
Lattice	Dilithium	227’254	910’911	291’116	2’044
Multivariate	MQDSS-48	2’579’234	252’403’091	185’066’255	32’886
Code	pqsigRM412	18’062’152’610	33’057’982’128	301’873’276	528

Key Encapsulation Mechanism

- CPU cycles

Category	Scheme	Key generation	Encapsulation	Decapsulation
Isogeny ECC	SIKEp503	82’329’570	133’880’410	142’428’861
Lattice	NewHope512-CCA	513’054	776’525	874’199
Multivariate	DME-(3,2,48)	445’585’460	2’114’390	10’845’706
Code	Classic McEliece 6960119	2’406’818’088	1’756’816	498’750’958

PQC and PKI

PKI

- Quantum computing strikes at the heart of the security of the global public key infrastructure
- All certificates become obsolete
- Root CAs operate for 20+ years
- Transition to new cryptosystem takes 10+ years (see SHA-1)

Multiple Public-Key Algorithm X.509 Certificates

- X.509 Extensions
- Adds a PQC algorithm and signature to the certificate

```
             [ ... omitted for brevity ... ]
    X509v3 extensions:
         X509v3 Basic Constraints:
             CA:FALSE
         Netscape Cert Type:
             SSL Server
         Netscape Comment:
             OpenSSL Generated Server Certificate
         [ ... omitted for brevity ... ]

         Alt-Signature-Algorithm:
             sha512WithHSS

         Subject-Alt-Public-Key-Info:
             Leighton-Micali Hierarchical Signature System
             Public Key:
                 00:00:00:01:00:00:00:07:00:00:00:03:1c:ba:ef:
                 [ ... omitted for brevity ... ]
             Winternitz Value:   3 (0x3)
             Tree Height:   7 (0x7)

         Alt-Signature-Value:
             Signature:
                 30:82:0a:74:[ ... omitted for brevity ... ]

Signature Algorithm: ecdsa-with-SHA256
     30:45:02:21:[ ... omitted for brevity ... ]
```

https://datatracker.ietf.org/doc/draft-truskovsky-lamps-pq-hybrid-x509/

Conclusion

- Quantum Computer risk is real
- Do your risk assessment
- Move towards crypto agile systems
- Be ready in case QC becomes real