Reminder:

RSA and ECC are (almost) dead

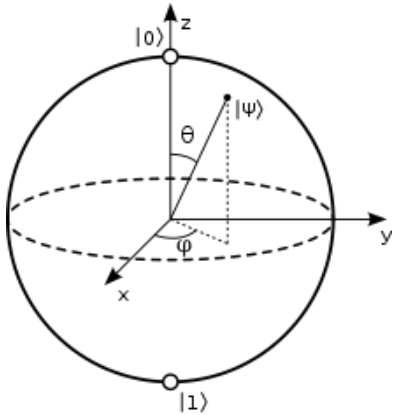
Quantum computers

Do not try to understand it by intuition !

Qubit ?

Ou Qu-bit, or Qbit (/'kju:bɪt/)

Various technologies: Superconducting, Trapped ion, Photonic, Silicon-based, Topological, Neutral atom, …



Funny properties

It's a kind of ~~magic~~ quantic

It is NOT

Future of computing

« a computer which computes all values simultaneously »

Just a question of « how much qubits »

Quite good news

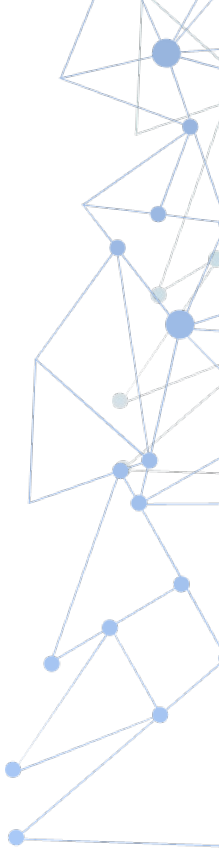
Hash Algorithms

No known efficient attack
Works in progress ?

Symmetric encryption

Grover algorithm ?

AES128 → 64 bits of security
AES256 → 128 bits of security



Asymetric cryptography

Shor's algorithm

Will **Break** (a few days ? Hours ? Minuts ?)

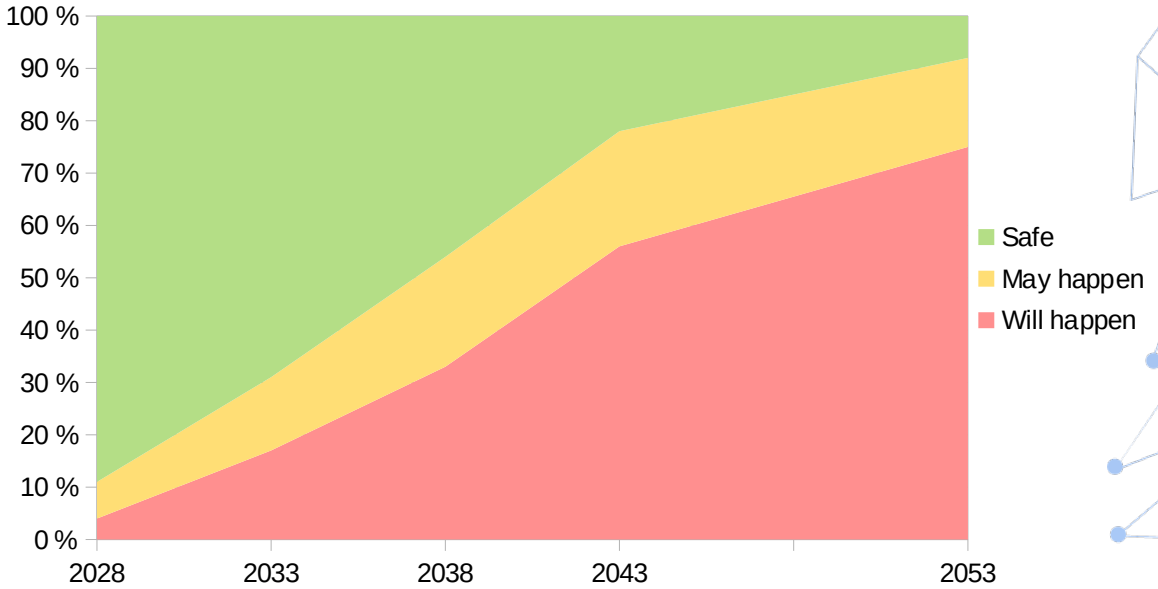
- RSA
- Elliptic Curves (ECC)
- Diffie-Hellman

That was spoiled in the first slide !

When will it happen ?

One day

Almost certain

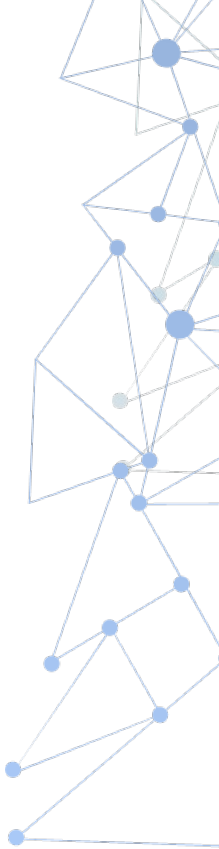


Opinion estimation on the risk that a quantum computer will break an RSA-2048 key in less than 24 hours (Global Risk Institute / 2023)

And this is not just a matter of « I have enough Qubits »……

Consequences

- Authentication → Identity spoofing
- Signature → Sign arbitrary documents
- Encryption → Read private / sensitive data !
  « Store now, decrypt later »



Mosca's Theorem

Y
Time to standardize and adopt

X
Data confidentiality duration

Z
Time before a quantum computer attack

X + Y > Z = Problem !

Solution: Post-quantum algorithms

Other mathematical problems

Lattice

Multivariate polynoms

Hash-based

Supersingular elliptic curves

Code based (including error correcting)

Old good Preshared keys ……

Can run on your computer

Standardization

Encryption

CRISTALS-Kyber (NIST, Lattice)

- « ML-KEM », « FIPS 203 »

FrodoKEM (ISO, Lattice)

Other candidates

Signature

CRISTALS-Dilithium (NIST, Lattice)

- « ML-DSA », « FIPS 204 »

SPHINCS+ (NIST, hashes)

- « SLH-DSA », « FIPS 205 »

Falcon (NIST, Lattice)

Other candidates

NIST: final versions in ~~2024~~ ~~Q2~~ ~~April~~ ~~Q2~~ ~~July~~ August ?

Security agencies guidelines

Quickly move to PQSafe algorithms
« To be completed by 2035 »

Not enough feedback on new algorithms

→ Do not use them alone for now

Hybrid mode: (RSA|ECC) + PQSafe

PQSafe alone « later » (2030+ ?)

Complex migration

Confidence level / **Hybrid mode**

→ New RFCs….

Keys / data size

→ New RFCs….

CPU / RAM ?

What should I do now ?

Be aware !

Crypto inventory

Crypto agility

Product’s roadmaps ?

Encryption first !

Thank you

STORMSHIELD