Share experience. Build resilience

Welcome to SECCON NL 22

digital trust center.

Connect2Trust

HSD securitydelta.nl

CYBERVEILIG NEDERLAND

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

telindus
a Proximus company

avit

CISCO SECURE

Quantum hurdles

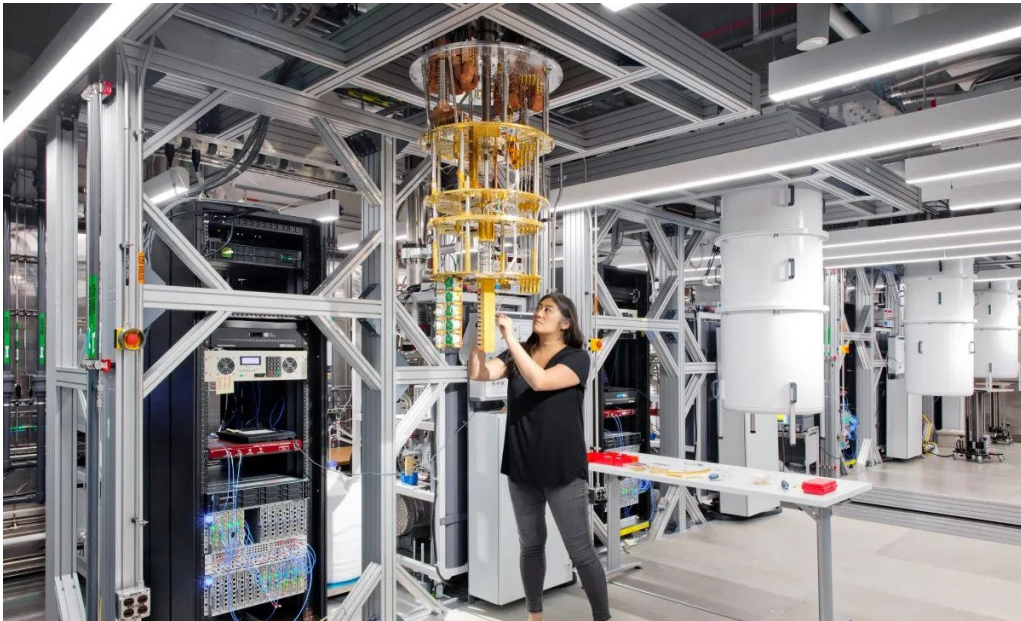
An optimistic view of post-quantum security

Sander Dorigo
Senior security architect @ Fox-IT
September 22, 2022

Crypto @ Fox-IT

We invent, create and manage cryptographic products for media and file encryption, network security, domain separation, secure mobile communications, and encryption key management.

- Separate entity, 100% Dutch, owned by Fox-IT
- Customers already demand quantum-proof solutions



d resilience.

1994

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

2001

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M.K. Vandersypen[†,*], Matthias Steffen[*,†], Gregory Breyta[†],
Costantino S. Yannoni[†], Mark H. Sherwood[†] and Isaac L. Chuang[*,†]

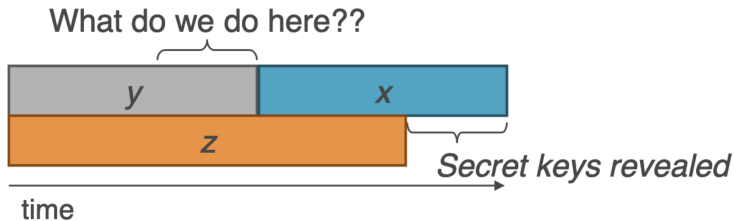
[†] *IBM Almaden Research Center,*
San Jose, CA 95120
[*] *Solid State and Photonics Laboratory,*
Stanford University,
Stanford, CA 94305-4075

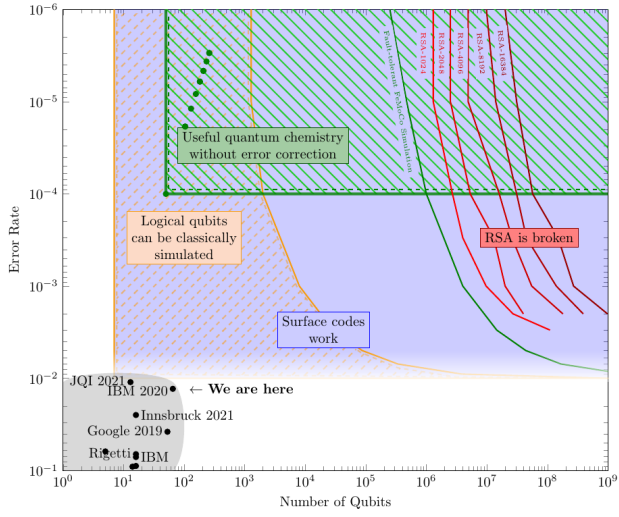
Quantum resilience efforts

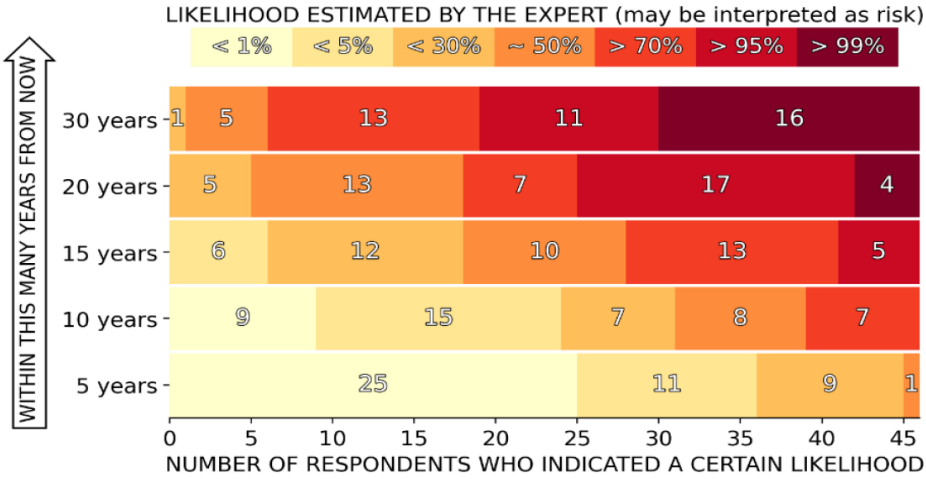
- Public-key encryption and key-establishment algorithms
  - Encryption without face-to-face shared secret (PKI)
  - Post-compromise security
- Digital signature algorithms
  - Digital signatures and authentication

How soon do we need to worry?

- How long do you need encryption to be secure? (x years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (y years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance)? (z years)




Error Rate
Number of Qubits
10^{-6}
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
10^{0}
10^{1}
10^{2}
10^{3}
10^{4}
10^{5}
10^{6}
10^{7}
10^{8}
10^{9}
Useful quantum chemistry without error correction
Fault-tolerant FeMoCo simulation
RSA-1024
RSA-2048
RSA-4096
RSA-8192
RSA-16384
Logical qubits can be classically simulated
RSA is broken
Surface codes work
JQI 2021
IBM 2020
← We are here
Innsbruck 2021
Google 2019
Rigetti
IBM


LIKELIHOOD ESTIMATED BY THE EXPERT (may be interpreted as risk)
< 1%
< 5%
< 30%
~ 50%
> 70%
> 95%
> 99%
WITHIN THIS MANY YEARS FROM NOW
30 years
20 years
15 years
10 years
5 years
1
5
13
11
16
5
13
7
17
4
6
12
10
13
5
9
15
7
8
7
25
11
9
1
0
5
10
15
20
25
30
35
40
45
NUMBER OF RESPONDENTS WHO INDICATED A CERTAIN LIKELIHOOD

National Institute of Standards and Technology

Round 3 finalists

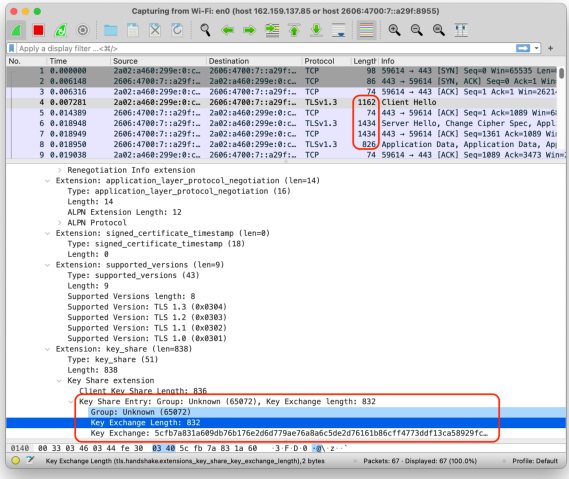
- Public-key Encryption and Key-establishment Algorithms
  - Classic McEliece, CRYSTALS-KYBER, NTRU, SABER
  - BIKE, FrodoKEM, HQC, NTRU Prime, ~~SIKE~~
- Digital Signature Algorithms
  - CRYSTALS-DILITHIUM, FALCON, ~~Rainbow~~
  - GeMSS, Picnic, *SPHINCS+*

OpenSSH

* ssh(1), sshd(8): use the hybrid Streamlined NTRU Prime + x25519 key exchange method by default ("sntrup761x25519-sha512@openssh.com"). The NTRU algorithm is believed to resist attacks enabled by future quantum computers and is paired with the X25519 ECDH key exchange (the previous default) as a backstop against any weaknesses in NTRU Prime that may be discovered in the future. The combination ensures that the hybrid exchange offers at least as good security as the status quo.

  We are making this change now (i.e. ahead of cryptographically-relevant quantum computers) to prevent "capture now, decrypt later" attacks where an adversary who can record and store SSH session ciphertext would be able to decrypt it once a sufficiently advanced quantum computer is available.

Cloudflare PQ experiments (August 2022)



The current state

- Lots of algorithms
- Lots of experiments
- Quantum computers are still far away...

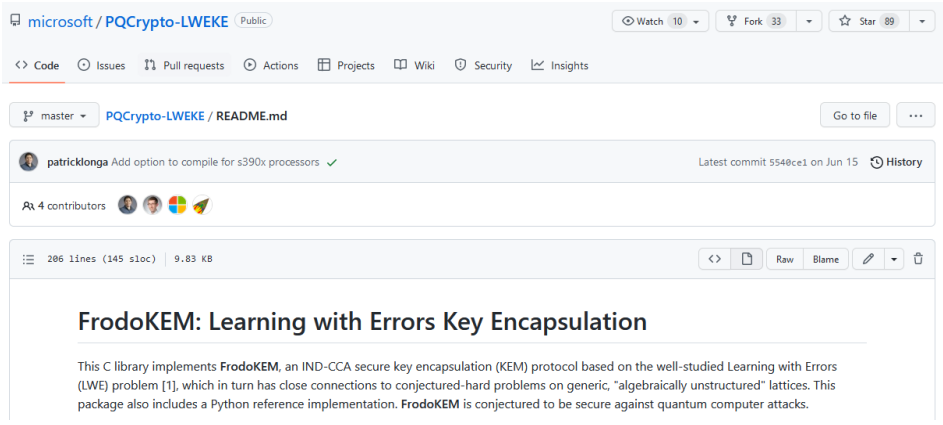
APTs and other (cryptographic) threats

- Steal now, decrypt later

APTs and other (cryptographic) threats

- Steal now, decrypt later
- Weak points in (custom) libraries, tools and protocols
  - Timing and side-channel attacks

APTs and other (cryptographic) threats



APTs and other (cryptographic) threats

return value of randombytes() not checked #29

Closed **dorssel** opened this issue on Jun 1 · 1 comment

dorssel commented on Jun 1

For example during key generation:

PQCrypto-LWEKE/src/kem.c
Line 35 in 4210d53

```
35      randombytes(randomness, CRYPTO_BYTES + CRYPTO_BYTES + BYTES_SEED_A);
```

`randombytes()` can fail on Windows, which will go unnoticed and will lead to an insecure (possibly completely deterministic) key!

Additionally: the code in `randombytes.c` is not very well written for other reasons. On Linux, the code will simply deadlock if `\dev\urandom` is not available. And if you ever compile without either WINDOWS or NIX, then it defaults to returning `passed` instead of `failed`. But that last point doesn't actually matter, since the return value is not checked anyway...

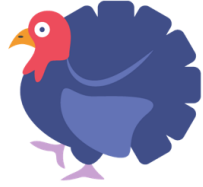
👀 1

APTs and other (cryptographic) threats

- Steal now, decrypt later
- Weak points in (custom) libraries, tools and protocols
  - Timing and side-channel attacks
- Using broken (post quantum) cryptographic algorithms.

APTs and other (cryptographic) threats

CECPQ2 = HRSS + X25519



CECPQ2b = SIKE + X25519

Future steps

- We know the timelines (sort of)
- We know the threats (mostly)
- What can I do?

Canaries in the coal mine

- Quantum-powered chemistry research
  - Molecule design and viability simulation, simulating protein dynamics (folding@home)

Canaries in the coal mine

- Quantum-powered chemistry research
  - Molecule design and viability simulation, simulating protein dynamics (folding@home)
- Quantum-powered models for pharmacy use cases
  - ADME, toxicity predictions and safety simulations

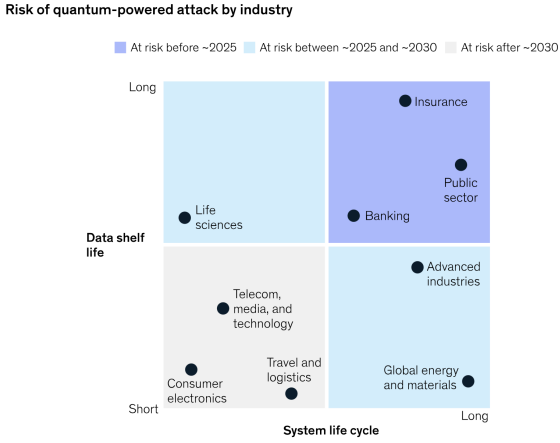
Canaries in the coal mine

- Quantum-powered chemistry research
  - Molecule design and viability simulation, simulating protein dynamics (folding@home)
- Quantum-powered models for pharmacy use cases
  - ADME, toxicity predictions and safety simulations
- Artificial intelligence and machine learning
  - Quantum ML models

Future steps

- We know the timelines (sort of)
- We know the threats (mostly)
- **What can I do?**

What's your risk?



What is this “Crypto Agility“ you speak of?

1. The ability of your tech-stack to switch to new cryptographic components
   - Algorithms, protocols, implementations, security strength
   - Platform compatibility, migrations, retirement of legaccy
2. The ability of your organisation to classify its data and assets
   - Risk-based, value based, “treasure trove”

Open Quantum Safe

The ability of your tech-stack to switch to new cryptographic components

The Open Quantum Safe (OQS) project is an open-source project that aims to support the development and prototyping of quantum-resistant cryptography.

`https://openquantumsafe.org/`

HAPKIDO

The ability of your tech-stack to switch to new cryptographic components

- **H**ybrid
- **A**pproach for
- quantum-safe **P**ublic **K**ey **I**nfrastructure **D**evelopment for
- **O**rganisations

An initiative to help (large) organisations migrate their (internal) PKI and research how you could do certificate management with post quantum algorithms.

Intelligence agencies

The ability of your organisation to classify its data and assets

AIVD, BSI, ANSSI, GHCQ, NSA

Intelligence agencies

The ability of your organisation to classify its data and assets

- 🇳🇱 AIVD, 🇩🇪 BSI, 🇫🇷 ANSSI, 🇬🇧 GHCQ, 🇺🇸 NSA
- Use long symmetric keys, research and use symmetric protocols, do not rely on quantum key distribution alone. Determine how *long* data needs to be safe. Protect that data accordingly.

Intelligence agencies

The ability of your organisation to classify its data and assets

- 🇳🇱 AIVD, 🇩🇪 BSI, 🇫🇷 ANSSI, 🇬🇧 GHCQ, 🇺🇸 NSA
- Start a data protection and asset classification program. Write a data governance policy. Discuss data retention policies with your employer. Mention the GDPR.

Are you crypto agile?

- Find the shortest (ie RSA 1024) certificate in your organisation (and replace it)
- Scan your network for servers that accept TLS 1.0 connections (and disable them)

Are you crypto agile?

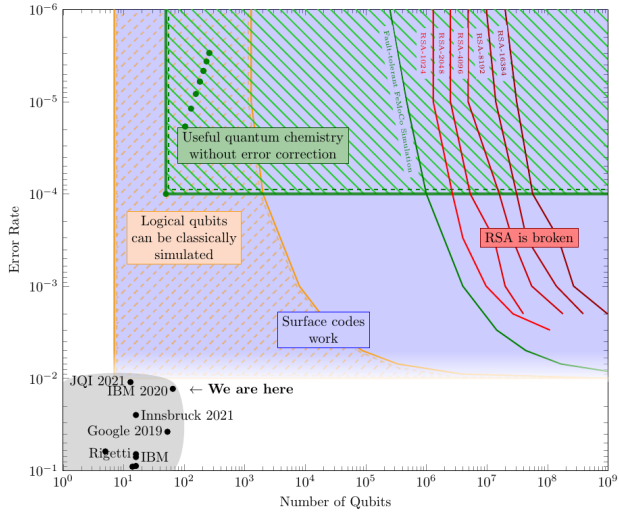
- Find the shortest (ie RSA 1024) certificate in your organisation (and replace it)
- Scan your network for servers that accept TLS 1.0 connections (and disable them)
- Mention the word “upgrade” to a Websphere sysadmin

Are you crypto agile?

- Find the shortest (ie RSA 1024) certificate in your organisation (and replace it)
- Scan your network for servers that accept TLS 1.0 connections (and disable them)
- Mention the word “upgrade” to a Websphere sysadmin
- Suggest we “unflatten the network” to a network admin

Experiment with PQC

- Can you generate a quantum safe SSH keypair, and use it?
- Can you submit a quantum safe CSR to Let's Encrypt?
- Can you join the Cloudflare PQC experiment with a (sub)domain?
- Can you encrypt your backups using symmetric algorithms only?


Error Rate
Number of Qubits
10^{-6}
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
10^{0}
10^{1}
10^{2}
10^{3}
10^{4}
10^{5}
10^{6}
10^{7}
10^{8}
10^{9}
Useful quantum chemistry without error correction
Fault-tolerant FeMoCo simulation
RSA-1024
RSA-2048
RSA-4096
RSA-8192
RSA-16384
Logical qubits can be classically simulated
RSA is broken
Surface codes work
JQI 2021
IBM 2020
← We are here
Innsbruck 2021
Google 2019
Rigetti
IBM

Conclusion

- The utility of quantum computers in code-breaking and other number theoretical problems is WAY over hyped

Conclusion

- The utility of quantum computers in code-breaking and other number theoretical problems is WAY over hyped
- Proper data classification and governance is a good idea either way

Conclusion

- The utility of quantum computers in code-breaking and other number theoretical problems is WAY over hyped
- Proper data classification and governance is a good idea either way
- Crypto agility is also a “low-regret move”

Conclusion

- The utility of quantum computers in code-breaking and other number theoretical problems is WAY over hyped
- Proper data classification and governance is a good idea either way
- Crypto agility is also a “low-regret move”
- Familiarize yourself with the new quantum resilient algorithms because learning is fun

Conclusion

- The utility of quantum computers in code-breaking and other number theoretical problems is WAY over hyped
- Proper data classification and governance is a good idea either way
- Crypto agility is also a “low-regret move”
- Familiarize yourself with the new quantum resilient algorithms because learning is fun
- Don’t panic

Ask me anything

Share experience. Build resilience.

Ask me anything

Sander Dorigo
sander.dorigo@fox-it.com

https://f0x.nl/seccon22