Quantum computers

–

the future attack that breaks today's messages

Tanja Lange

12 Feb 2020

Eindhoven University of Technology

U.S. National Academy of Sciences report

Don't panic. "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

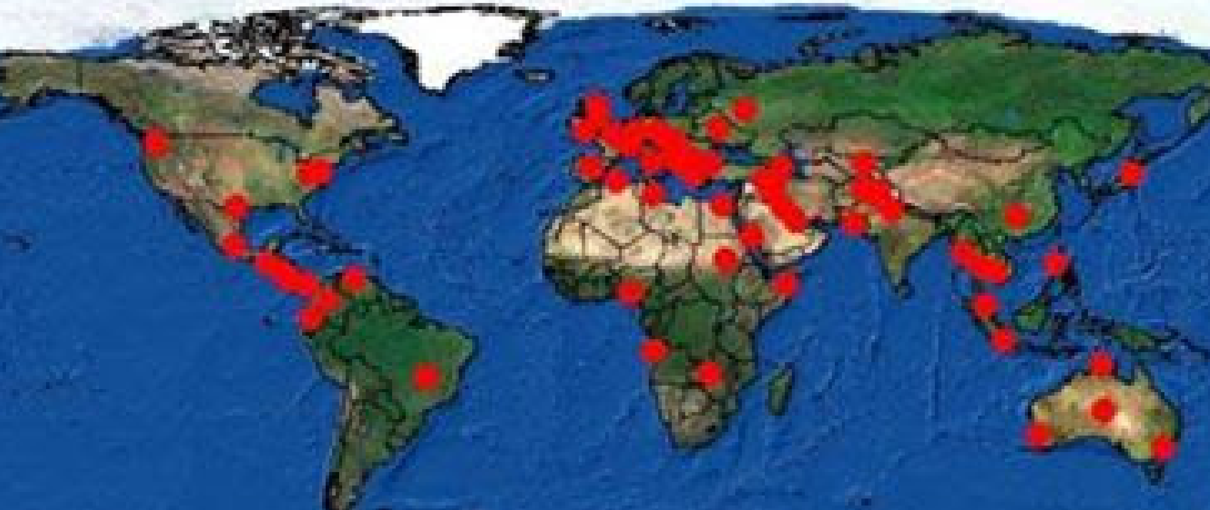
U.S. National Academy of Sciences report

Don't panic. "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

Panic. "Key Finding 10: Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster."

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?



High urgency for long-term confidentiality

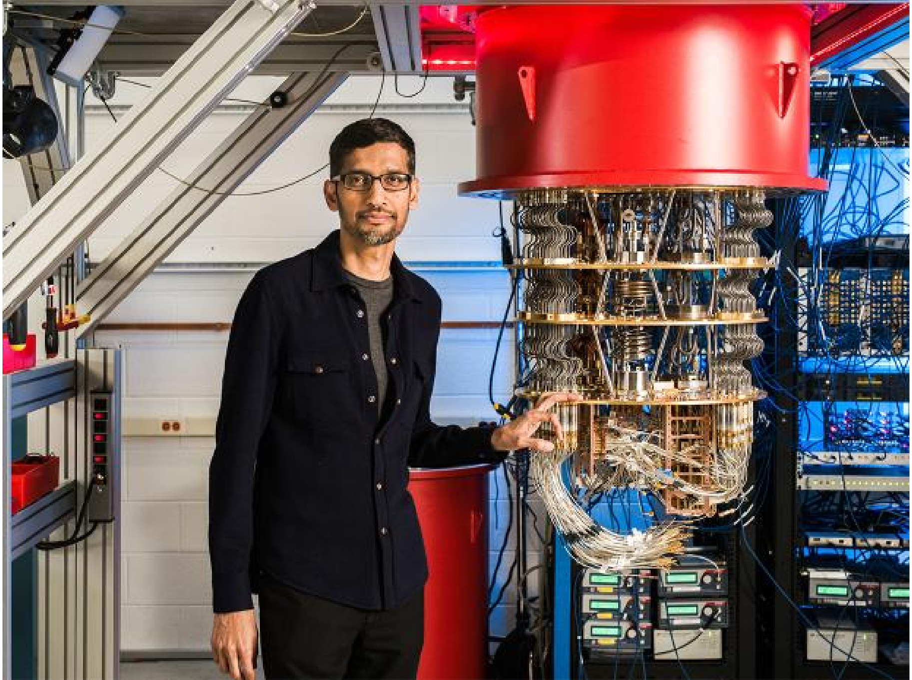
- Today's encrypted communication is being stored by attackers and will be decrypted years later with quantum computers. Danger for human-rights workers, medical records, journalists, security research, legal proceedings, state secrets, . . .

- Signature schemes can be replaced once a quantum computer is built – but there will be no public announcement

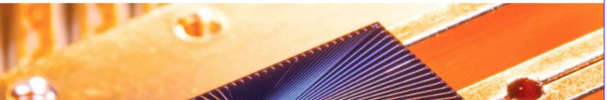
High urgency for long-term confidentiality

- Today's encrypted communication is being stored by attackers and will be decrypted years later with quantum computers. Danger for human-rights workers, medical records, journalists, security research, legal proceedings, state secrets, ...

- Signature schemes can be replaced once a quantum computer is built – but there will be no public announcement ... and an important function of signatures is to protect system upgrades.
- Protect your upgrades *now* with post-quantum signatures.



Quantum computing could end encryption within five years, says Google boss



Mr Pichai said a combination of artificial intelligence and quantum would "help us tackle some of the biggest problems we see", but said it was important encryption evolved to match this.

"In a five to ten year time frame, quantum computing will break encryption as we know it today."

This is because current encryption methods, by which information such as texts or passwords is turned into code to make it unreadable, rely upon the fact that classic computers would take billions of years to decipher that code.

Quantum computers, with their ability to be

Many stages of research from design to deployment

- Define the goals
- Explore space of cryptosystems
- Study algorithms for the attackers
- Focus on secure cryptosystems
- Study algorithms for the users
- Study implementations on real hardware
- Study side-channel attacks, fault attacks, etc.
- Focus on secure, reliable implementations
- Focus on implementations meeting performance requirements
- Integrate securely into real-world applications

Is post-quantum crypto moving quickly enough?

1994: Shor's algorithm.

PQCrypto 2006: International Workshop on Post-Quantum Cryptography. (Coined phrase in 2003.)

Is post-quantum crypto moving quickly enough?

1994: Shor's algorithm.

PQCrypto 2006: International Workshop on Post-Quantum Cryptography. (Coined phrase in 2003.) PQCrypto 2008, 2010, 2011, 2013, 2014, 2016, 2017, 2018, 2019, upcoming 2020.

Is post-quantum crypto moving quickly enough?

1994: Shor's algorithm.

PQCrypto 2006: International Workshop on Post-Quantum Cryptography. (Coined phrase in 2003.) PQCrypto 2008, 2010, 2011, 2013, 2014, 2016, 2017, 2018, 2019, upcoming 2020.

2014: EU solicits grant proposals in post-quantum crypto.

2014: ETSI starts working group on "Quantum-safe" crypto.

2015: NIST hosts workshop on post-quantum cryptography.

After public input, NIST calls for submissions of public-key systems to "Post-Quantum Cryptography Standardization Project". Deadline 2017.11.

2017: Submissions to the NIST competition

21 December 2017: NIST posts 69 submissions from 260 people.

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some submissions are broken within days

By end of 2017: 8 out of 69 submissions attacked.

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some less secure than claimed; some smashed; some attack scripts.

Do cryptographers have any idea what they're doing?

By end of 2018: 22 out of 69 submissions attacked.

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some less secure than claimed; some smashed; some attack scripts.

Do cryptographers have any idea what they're doing?

By end of 2019: 30 out of 69 submissions attacked.

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some less secure than claimed; some smashed; some attack scripts.

An attempt to explain the situation

People often categorize submissions. Examples of categories:

- Code-based encryption and signatures.
- Hash-based signatures.
- Isogeny-based encryption.
- Lattice-based encryption and signatures.
- Multivariate-quadratic encryption and signatures.

This list is based on the best known attacks (as always).

These are categories of mathematical problems;
individual systems may be totally insecure
if the problem is not used correctly.

Some attempts to explain the situation

"What's safe is using the portfolio from the European PQCRYPTO project." — Are you sure?

Some attempts to explain the situation

"What's safe is using the portfolio from the European PQCRYPTO project." — Are you sure?

The portfolio: BIG QUAKE. BIKE. Classic McEliece. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. FrodoKEM. Gui. KINDI. LUOV. MQDSS. NewHope. NTRU-HRSS-KEM. NTRU Prime. Picnic. qTESLA. Rainbow. Ramstake. SABER. SPHINCS+.

Some attempts to explain the situation

"What's safe is using the portfolio from the European PQCRYPTO project." — Are you sure?

The portfolio: BIG QUAKE. BIKE. Classic McEliece. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. FrodoKEM. Gui. KINDI. LUOV. MQDSS. NewHope. NTRU-HRSS-KEM. NTRU Prime. Picnic. qTESLA. Rainbow. Ramstake. SABER. SPHINCS+.

69 submissions = **denial-of-service attack against security evaluation**. Maybe cryptanalysts were focusing on submissions from outside the project.

An attempt to explain the situation

“What’s safe is lattice-based cryptography.”

An attempt to explain the situation

"What's safe is lattice-based cryptography."

2006 Silverman: "Lattices, SVP and CVP, have been intensively studied for more than 100 years, both as intrinsic mathematical problems and for applications in pure and applied mathematics, physics and cryptography."

An attempt to explain the situation

"What's safe is lattice-based cryptography."

2006 Silverman: "Lattices, SVP and CVP, have been intensively studied for more than 100 years, both as intrinsic mathematical problems and for applications in pure and applied mathematics, physics and cryptography."

2017 Peikert: "The underlying worst-case problems—e.g., approximating short vectors in lattices—have been deeply studied by some of the great mathematicians and computer scientists going back at least to Gauss, and appear to be very hard."

Reality: SVP hardness is poorly understood

Best SVP algorithms known by 2000:
time $2^{\Theta(N \log N)}$ for almost all dimension-N lattices.

Best SVP algorithms known today: $2^{\Theta(N)}$. Huge change!

Reality: SVP hardness is poorly understood

Best SVP algorithms known by 2000:
time $2^{\Theta(N \log N)}$ for almost all dimension-N lattices.

Best SVP algorithms known today: $2^{\Theta(N)}$. Huge change!

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.

Reality: SVP hardness is poorly understood

Best SVP algorithms known by 2000:
time $2^{\Theta(N \log N)}$ for almost all dimension-N lattices.

Best SVP algorithms known today: $2^{\Theta(N)}$. Huge change!

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.
0.384: 2011 Wang–Liu–Tian–Bi.

Reality: SVP hardness is poorly understood

Best SVP algorithms known by 2000:
time $2^{\Theta(N \log N)}$ for almost all dimension-N lattices.

Best SVP algorithms known today: $2^{\Theta(N)}$. Huge change!

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.
0.384: 2011 Wang–Liu–Tian–Bi.
0.378: 2013 Zhang–Pan–Hu.

Reality: SVP hardness is poorly understood

Best SVP algorithms known by 2000:
time $2^{\Theta(N \log N)}$ for almost all dimension-N lattices.

Best SVP algorithms known today: $2^{\Theta(N)}$. Huge change!

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.
0.384: 2011 Wang–Liu–Tian–Bi.
0.378: 2013 Zhang–Pan–Hu.
0.337: 2014 Laarhoven.

Reality: SVP hardness is poorly understood

Best SVP algorithms known by 2000:
time $2^{\Theta(N \log N)}$ for almost all dimension-N lattices.

Best SVP algorithms known today: $2^{\Theta(N)}$. Huge change!

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.
0.384: 2011 Wang–Liu–Tian–Bi.
0.378: 2013 Zhang–Pan–Hu.
0.337: 2014 Laarhoven.
0.298: 2015 Laarhoven–de Weger.
0.292: 2015 Becker–Ducas–Gama–Laarhoven.

Lattice security is even more poorly understood

Lattice-based crypto has many more attack avenues than SVP.

Lattice-based submissions: Compact LWE.
CRYSTALS-DILITHIUM. CRYSTALS-KYBER.
Ding Key Exchange. DRS. EMBLEM and R.EMBLEM. FALCON.
FrodoKEM. HILA5. KINDI. LAC. LIMA. Lizard. LOTUS.
NewHope. NTRUEncrypt. NTRU-HRSS-KEM. NTRU Prime.
Odd Manhattan. OKCN/AKCN/CNKE. pqNTRUSign. qTESLA.
Round2. SABER. Titanium.

Lattice security is even more poorly understood

Lattice-based crypto has many more attack avenues than SVP.

Lattice-based submissions: Compact LWE.
CRYSTALS-DILITHIUM. CRYSTALS-KYBER.
Ding Key Exchange. DRS. EMBLEM and R.EMBLEM. FALCON.
FrodoKEM. HILA5. KINDI. LAC. LIMA. Lizard. LOTUS.
NewHope. NTRUEncrypt. NTRU-HRSS-KEM. NTRU Prime.
Odd Manhattan. OKCN/AKCN/CNKE. pqNTRUSign. qTESLA.
Round2. SABER. Titanium.

Lattice security estimates are so imprecise that nobody is sure whether the remaining submissions are damaged by a 2019 paper solving a lattice problem "more than a million times faster".

Urgency of post-quantum recommendations

- If users want or need post-quantum systems **now**, what can they do?

Urgency of post-quantum recommendations

- If users want or need post-quantum systems **now**, what can they do?
- Post-quantum secure cryptosystems exist (to the best of our knowledge) but are under-researched – we can recommend secure systems now, but they are big and/or slow

Urgency of post-quantum recommendations

- If users want or need post-quantum systems **now**, what can they do?
- Post-quantum secure cryptosystems exist (to the best of our knowledge) but are under-researched – we can recommend secure systems now, but they are big and/or slow hence the logo of the PQCRYPTO project.

PQCRYPTO
ICT-645622

Urgency of post-quantum recommendations

- If users want or need post-quantum systems **now**, what can they do?
- Post-quantum secure cryptosystems exist (to the best of our knowledge) but are under-researched – we can recommend secure systems now, but they are big and/or slow hence the logo of the PQCRYPTO project.

PQCRYPTO
ICT-645622

- PQCRYPTO was an EU project in H2020, running 2015 – 2018.
- PQCRYPTO designed a portfolio of high-security post-quantum public-key systems, and improved the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet.

Initial recommendations of long-term secure post-quantum systems

Daniel Augot, Lejla Batina, Daniel J. Bernstein, Joppe Bos, Johannes Buchmann, Wouter Castryck, Orr Dunkelman, Tim Güneysu, Shay Gueron, Andreas Hülsing, Tanja Lange, Mohamed Saied Emam Mohamed, Christian Rechberger, Peter Schwabe, Nicolas Sendrier, Frederik Vercauteren, Bo-Yin Yang

Initial recommendations

- **Symmetric encryption** Thoroughly analyzed, 256-bit keys:
  - AES-256
  - Salsa20 with a 256-bit key
- **Symmetric authentication** Information-theoretic MACs:
  - GCM using a 96-bit nonce and a 128-bit authenticator
  - Poly1305
- **Public-key encryption** McEliece with binary Goppa codes:
  - length $n = 6960$, dimension $k = 5413$, $t = 119$ errors
- **Public-key signatures** Hash-based (minimal assumptions):
  - XMSS with any of the parameters specified in CFRG draft
  - SPHINCS-256

Deployment issues & solutions

- Different recommendations for rollout in different risk scenarios:
  - Use most efficient systems with ECC or RSA, to ease usage and gain familiarity.
  - Use most conservative systems (possibly with ECC), to ensure that data really remains secure.
- Protocol integration and implementation problems:
  - Key sizes or message sizes are larger for post-quantum systems, but IPv6 guarantees only delivery of $\leq$ 1280-byte packets.
  - Google experimented with larger keys and noticed delays and dropped connections.
  - Long-term keys require extra care (reaction attacks).
- Some libraries exist, quality is getting better.
- Google and Cloudflare are running some experiments of including post-quantum systems into TLS.