Post-quantum cryptography

Overview

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Summary: current state of the art

- Currently used crypto (check the lock icon in your browser) starts with elliptic-curve Diffie-Hellman (ECDH), RSA, or Diffie-Hellman (DH) in finite fields.
- Older standards are RSA or elliptic curves from NIST (or Brainpool), e.g. NIST P256 or ECDSA.
- Internet currently moving over to Curve25519 and Ed25519
- For symmetric crypto TLS (the protocol behind https) uses AES or ChaCha20 and some MAC, e.g. AES-GCM or ChaCha20-Poly1305. High-end devices have support for AES-GCM, smaller ones do better with ChaCha20-Poly1305.
- Security is getting better. Some obstacles: bugs; untrustworthy hardware; let alone anti-security measures such as laws restricting encryption in China, Iran, Russia, but also western countries like Australia and UK. Even NL has attempts to weaken encryption.

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as a polynomial in the size of the input. The class of prob-

U.S. National Academy of Sciences report

Quantum Computing: Progress and Prospects (2019)

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

Quantum Computing: Progress and Prospects (2019)

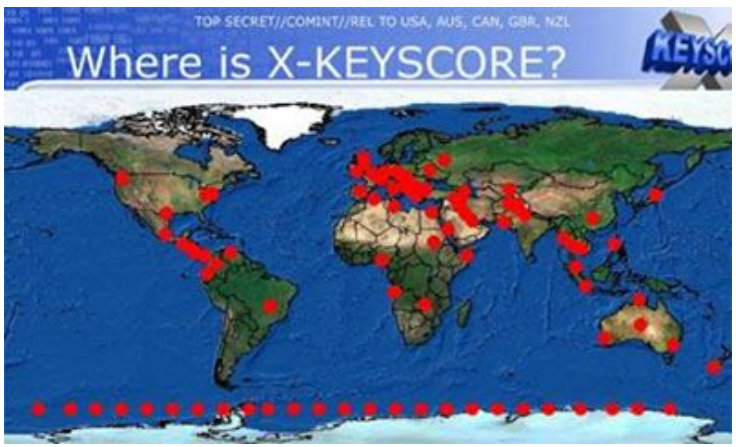
Don't panic. "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

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."

Post-quantum cryptography:
Cryptography designed
under the assumption that
the **attacker** (not the user!)
has a large quantum computer.

High urgency for long-term confidentiality

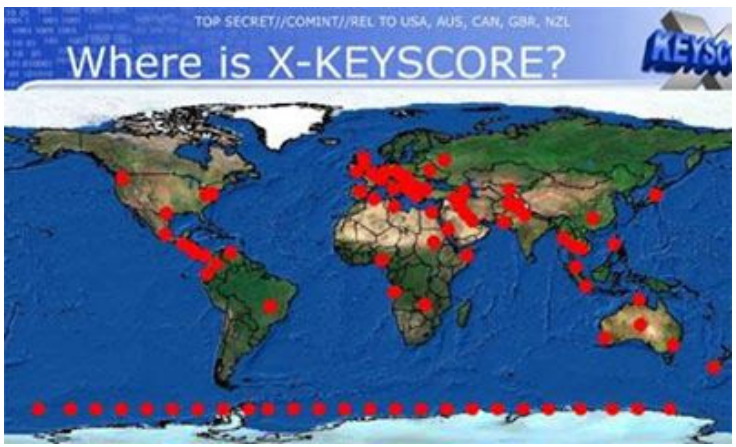
- Today's encrypted communication is being stored by attackers and will be decrypted years later with quantum computers. Danger for human-rights workers, medical records, journalists, security research, legal proceedings, state secrets, ...



- Signature schemes can be replaced once a quantum computer is built – but there will not be a 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 not be a public announcement ... and an important function of signatures is to protect operating system upgrades.
- Protect your upgrades *now* with post-quantum signatures.

Mathematical foundations of systems expected to survive

- **Code-based** encryption: McEliece cryptosystem has survived since 1978. Short ciphertexts and large public keys. Security relies on hardness of decoding error-correcting codes.
- **Hash-based** signatures: very solid security and small public keys. Require only a secure hash function (hard to find second preimages).
- **Isogeny-based** encryption: new kid on the block, promising short keys and ciphertexts and non-interactive key exchange. Security relies on hardness of finding isogenies between elliptic curves over finite fields.
- **Lattice-based** encryption and signatures: possibility for balanced sizes. Security relies on hardness of finding short vectors in some (typically special) lattice.
- **Multivariate-quadratic** signatures: short signatures and large public keys. Security relies on hardness of solving systems of multivariate equations over finite fields.

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

We have a good understanding of what a quantum computer can do, but new systems need more analysis.

Deployment issues & solutions

- Different recommendations for rollout:
  - 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.

  These recommendations match different risk scenarios.
- 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, but mostly for experiments, not production quality.
- Google and Cloudflare experimented with including post-quantum systems into TLS.

Deployment issues & solutions

- Different recommendations for rollout:
  - 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.

  These recommendations match different risk scenarios.
- 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, but mostly for experiments, not production quality.
- Google and Cloudflare experimented with including post-quantum systems into TLS.
- NIST (National Institute for Standards and Technology, US) is running competition to select standards for PQC.
  Narrowed field to 15 candidates, currently in hot phase.

Links

- NIST PQC competition https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
- Post-quantum cryptography course with video lectures and lots of exercises http://hyperelliptic.org/tanja/teaching/pqcrypto21/. Next edition: Spring 2022 in Mastermath.
- Quantum Threat Timeline from Global Risk Institute, 2019.
- PQCRYPTO EU project https://pqcrypto.eu.org:
  - Expert recommendations.
  - Free software libraries (libpqcrypto, pqm4, pqhw).
  - Lots of reports, scientific papers, (overview) presentations.
- PQCRYPTO summer school 2017 with 21 lectures on video + slides + exercises. https://2017.pqcrypto.org/school:
- https://pqcrypto.org: Survey site by Daniel J. Bernstein & TL
  - Many pointers: e.g., PQCrypto conference series.
  - Bibliography for 4 major PQC systems.