The threat of quantum computers for cryptography[1]

Tomáš Fabšič

Faculty of Electrical Engineering and Information Technology
Slovak University of Technology in Bratislava
(FEI STU)

6. July 2022

[1] Support from the NATO SPS Project G5448 is acknowledged.

Outline

Contents

Two types of cryptography used today

- Symmetric cryptography
  - symmetric encryption schemes (e.g. AES)
  - message authentication codes (e.g. HMAC)
- Asymmetric cryptography
  - Diffie-Hellman key exchange
  - digital signatures (e.g. RSA signature)
  - asymmetric encryption schemes (e.g. RSA encryption scheme)
  - key encapsulation mechanisms (KEMs)

Symmetric cryptography - illustration

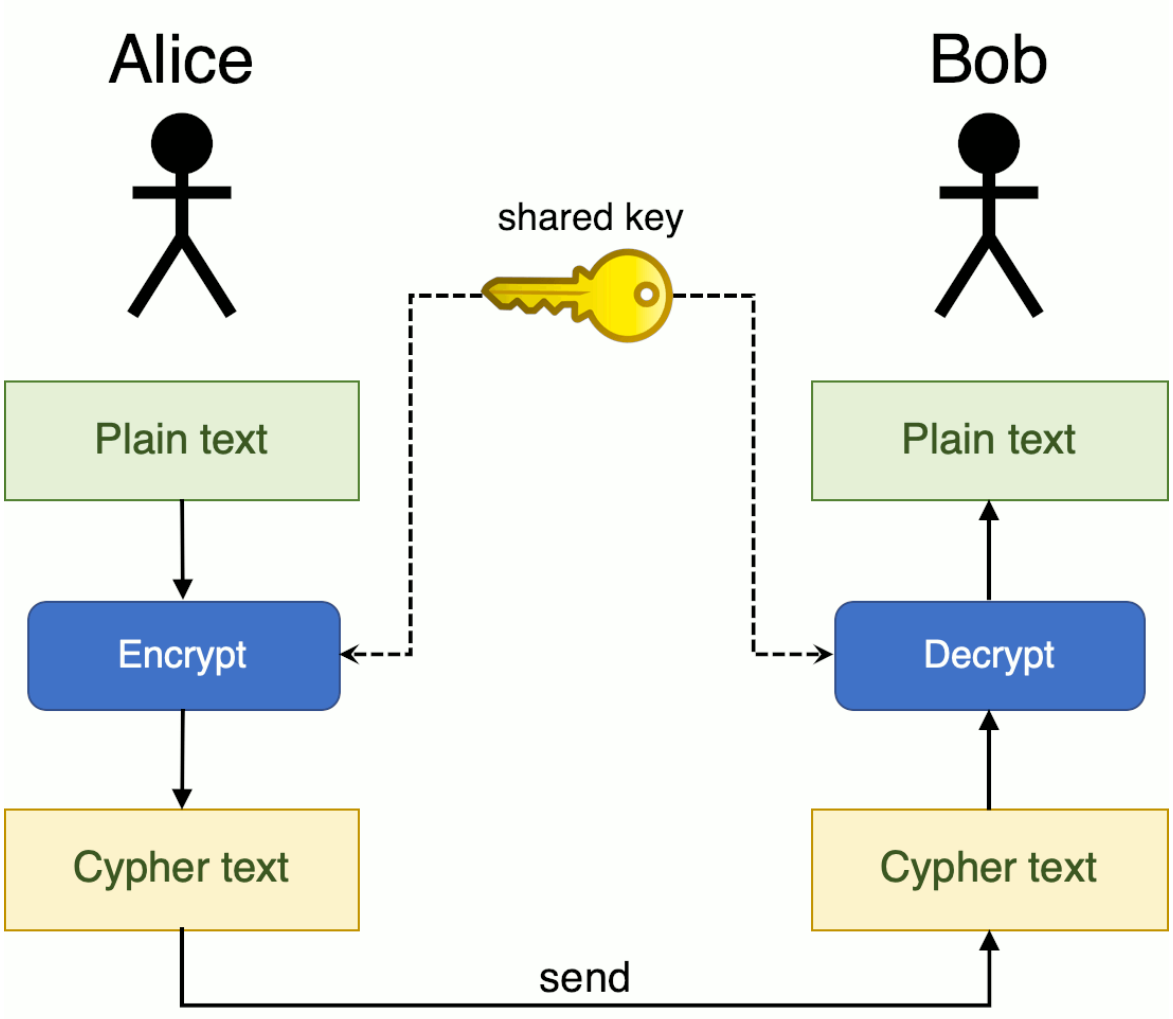


Figure: Source: https://www.coengoedegebure.com/surviving-an-infosec-job-interview-cryptography/

Symmetric cryptography - problem

- Alice and Bob need to share a secret key.
- How can Alice and Bob agree on a secret key?

How can Alice and Bob agree on a secret key?

- By using asymmetric cryptographic primitives!
- Symmetric and asymmetric cryptography are usually used together!

Joint use of symmetric and asymmetric cryptography

- Illustration: HTTPS connection
  - Client and server first use asymmetric cryptography to establish shared secret key (this process is called handshake).
  - Afterwards, client and server use the shared secret key with symmetric cryptography to transfer data.

Asymmetric cryptography - illustration

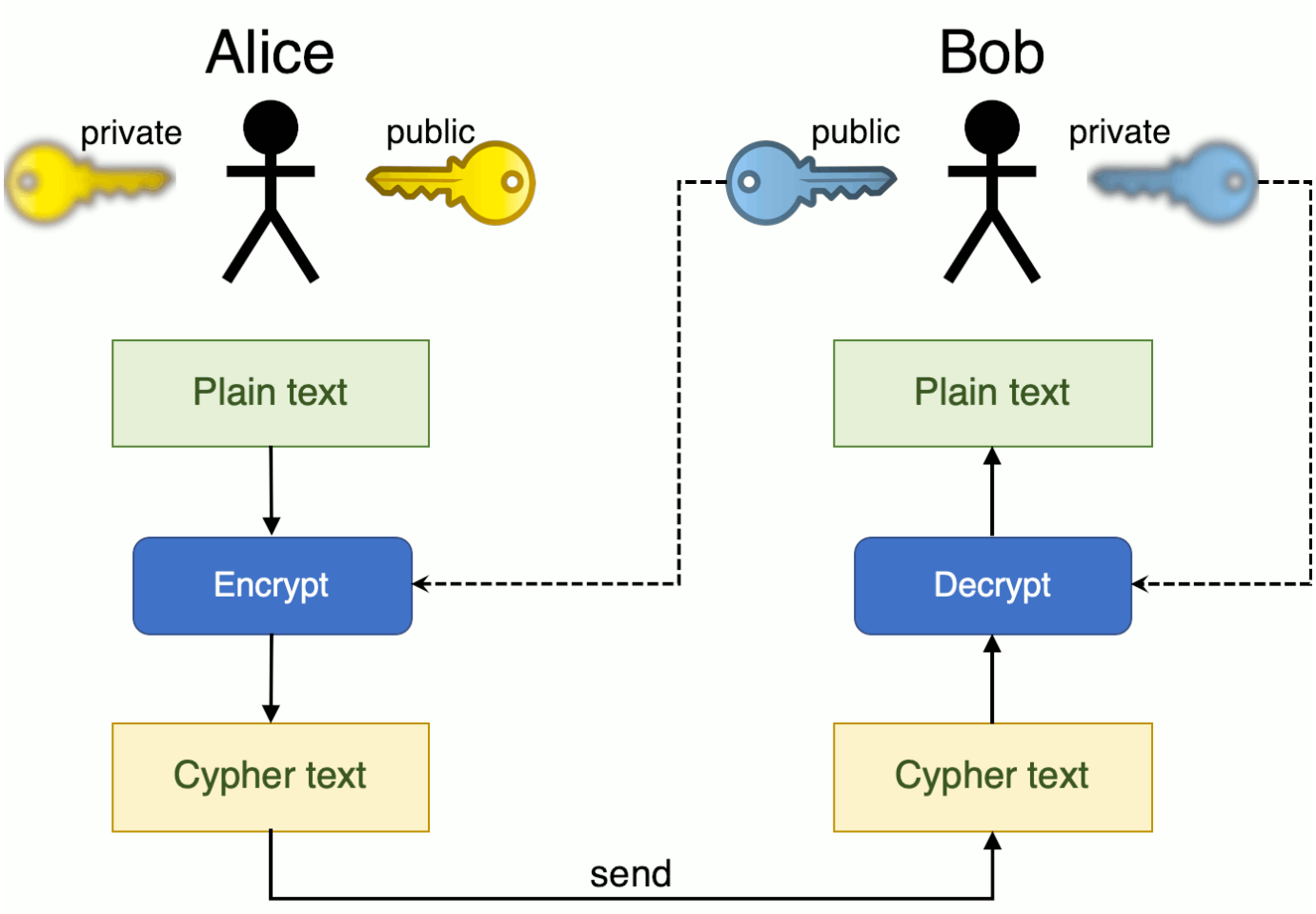


Figure: Source: https://www.coengoedegebure.com/surviving-an-infosec-job-interview-cryptography/

Asymmetric cryptography and hard problems

- It must be difficult for an adversary to compute Bob's private key from his public key.
- Asymmetric cryptography therefore relies on hard problems.

hard problem $=$ computational problem for which the humanity does not have an efficient (polynomial-time) solving algorithm

Example of a hard problem: prime factorization

- Given a large integer it is difficult to express it as a product of primes.
- RSA public key: a large integer n.
- RSA private key: primes p and q such that $n = p \times q$.

Hard problems in asymmetric cryptography today

- Currently deployed asymmetric cryptography relies on hardness of the following problems:
  - prime factorization problem
  - discrete logarithm problem
- Humanity has no efficient algorithms for solving these problems.
- More precisely: Humanity has no efficient classical algorithms for solving these problems.

$$\text{classical algorithm} = \text{an algorithm running on a classical computer}$$

- But humanity has an efficient quantum algorithm for solving these problems!

Contents

The threat of quantum computers

- Humanity has efficient quantum algorithm for solving prime factorization and discrete logarithm problems!
- This algorithm is called Shor's algorithm and was developed by Peter Shor in 1994.

$$\text{quantum algorithm} = \text{an algorithm running on a quantum computer}$$

- This means that if we had a large quantum computer we could break most of asymmetric cryptography used today!

Should we panic?

- NO. No large quantum computers currently exist.
- But rapid progress is being made in their development!

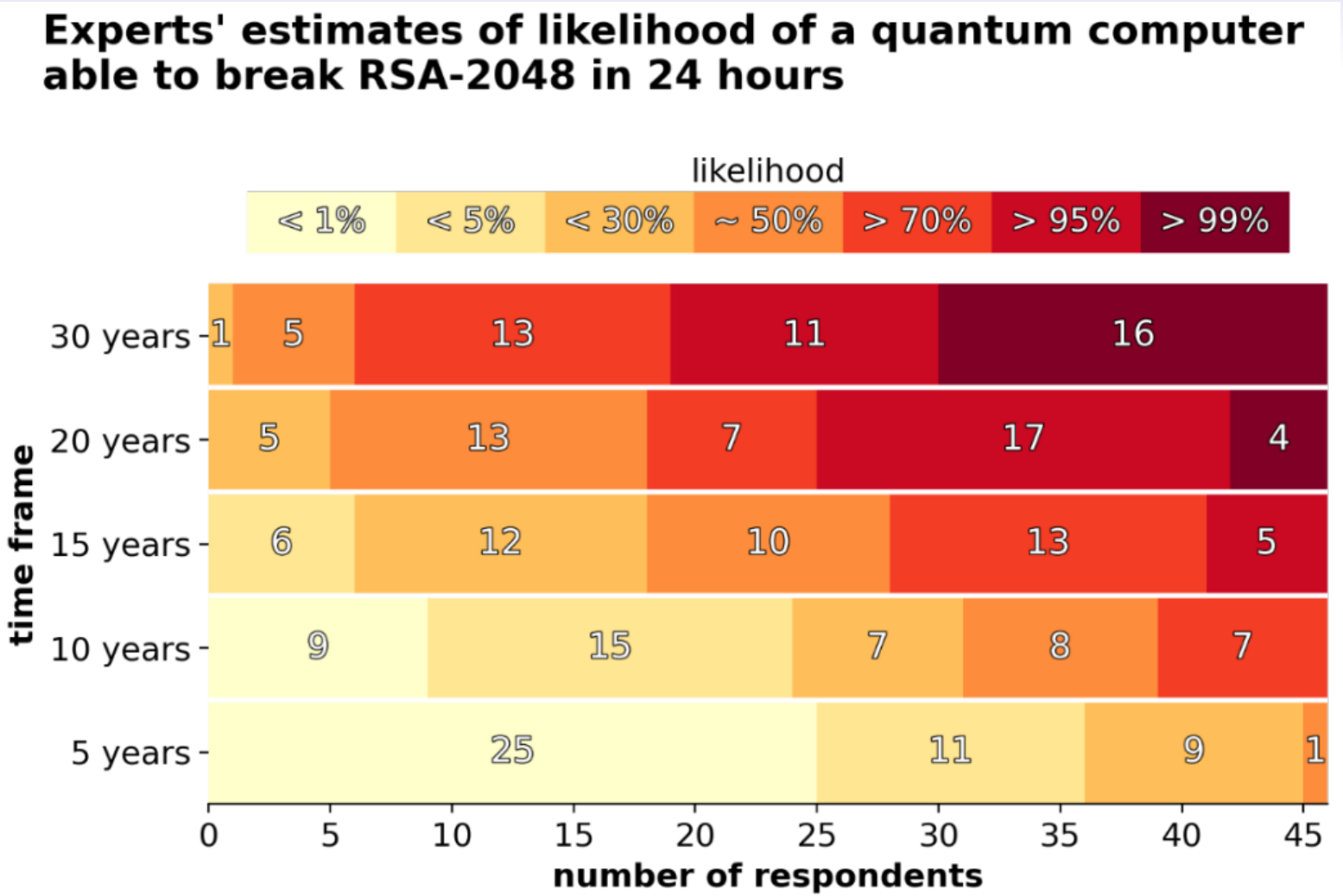


Figure: Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2021 https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

Contents

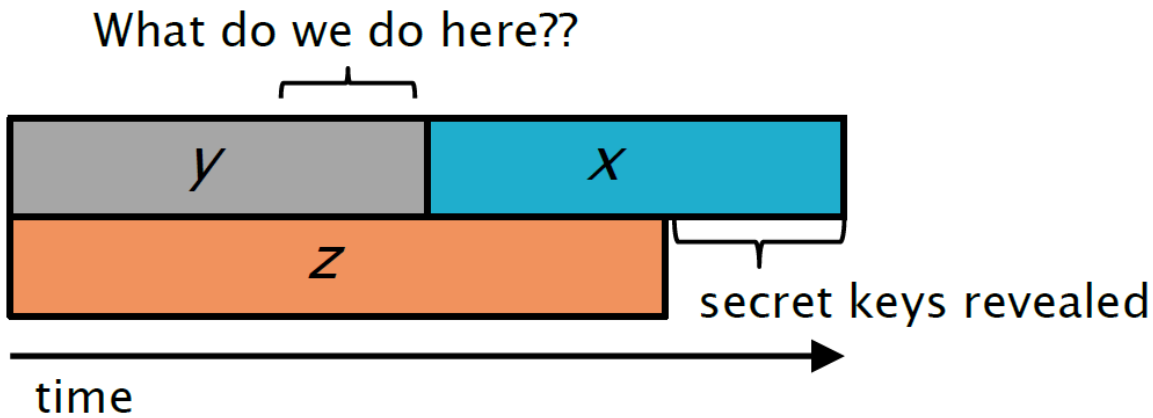
Implications for asymmetric cryptography

- Cryptographers will need to develop new standards for asymmetric cryptography.
- These new standards need to be based on problems which are hard to solve even on a quantum computer.
- Cryptosystems based on such problems are called post-quantum (PQ) cryptosystems.
- Candidates for PQ cryptosystems come from:
  - Lattice-based cryptography
  - Code-based cryptography
  - Multivariate cryptography
  - Hash-based cryptography
  - Isogeny-based cryptography

When do we need to start?

- Now!

Theorem (Mosca): If $x + y > z$, then problem



x – how long data needs to be safe
y – time for standardization and adoption
z – time until quantum computers

Figure: Source: https://csrc.nist.gov/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa

Implications for symmetric cryptography

- The impact on symmetric cryptography is less significant.
- Best known theoretical quantum attacks on symmetric cryptography employ Grover's algorithm.
- Grover's algorithm offers only polynomial speedup in unstructured search, from $O(N)$ to $O(\sqrt{N})$.
- It is therefore believed that the current symmetric cryptographic algorithms can be safely used in the quantum era, only the size of keys may need to increase.

Contents

Call for proposals

- In 2016 NIST launched post-quantum cryptography (PQC) standardization process[2].
- They called for post-quantum asymmetric cryptographic algorithms for new standards.
- Two categories:
  - encryption/ key-establishment
  - digital signatures

[2] https://csrc.nist.gov/Projects/post-quantum-cryptography

2017-2020: rounds 1 & 2

- 2017: submissions
  - NIST received 82 submissions.
  - NIST announced 69 first round candidates.
  - All first round candidates were made public (including implementations).
- 2017-2019: round one
  - First round candidates were analyzed by cryptographic community.
- 2019: second round candidates determined
  - NIST published a report on the first round (NISTIR 8240).
  - NIST announced 26 candidates which proceed to round 2.
- 2019-2020: round two
  - Second round candidates were analyzed by cryptographic community.

2020-2022: round 3

- 2020: NIST published a report on the second round (NISTIR 8309).
- NIST announced 15 candidates which proceed to round 3.
- 2020-2022: Third round candidates were analyzed by cryptographic community.
- Results of round 3 were announced only yesterday!

Round 3 results: algorithms selected for standardization

- *"The primary algorithms NIST recommends be implemented for most use cases are CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signature)."* [3]
- *"... the signature schemes Falcon and SPHINCS+ will also be standardized."* [3]

[3] Announced on PQC forum `https://csrc.nist.gov/Projects/post-quantum-cryptography/Email-List`

Round 3 results: algorithms selected for standardization - CRYSTALS-KYBER

- lattice-based key-establishment mechanism (KEM)
- suitable for most applications

Round 3 results: algorithms selected for standardization - CRYSTALS-Dilithium

- lattice-based digital signature
- uses Fiat-Shamir transform
- suitable for most applications

Round 3 results: algorithms selected for standardization - Falcon

- lattice-based digital signature
- uses *"hash then sign"* approach
- suitable for most applications
- has smaller signatures than CRYSTALS-Dilithium

Round 3 results: algorithms selected for standardization - SPHINCS+

- hash-based digital signature
- Main positive: has very strong security guatantees
- Main negative: slower and larger signatures than CRYSTALS-Dilithium or Falcon

Round 3 results: first set of standards

- NIST plans to release draft standards for public comment in 2022-2023.[4]
- NIST plans to have the first set of standards finalized by 2024.[4]

[4] https://csrc.nist.gov/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa

Round 3 results: algorithms selected for 4th round

- Some algorithms from 3rd round were selected for the 4th round.
- NIST views these algorithms as promising candidates for a later standardization.
- These algorithms are:
  - BIKE (code-based KEM)
  - Classic McEliece (code-based KEM)
  - HQC (code-based KEM)
  - SIKE (isogeny-based KEM)

Round 3 results: algorithms selected for 4th round - BIKE and HQC

- *"Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices."* [5]
- *"NIST expects to select at most one of these two candidates for standardization at the conclusion of the fourth round."* [5]

[5] Announced on PQC forum `https://csrc.nist.gov/Projects/post-quantum-cryptography/Email-List`

Round 3 results: algorithms selected for 4th round - SIKE

- *"SIKE remains an attractive candidate for standardization because of its small key and ciphertext sizes and will continue to study it in the fourth round."* [6]

[6] Announced on PQC forum `https://csrc.nist.gov/Projects/post-quantum-cryptography/Email-List`

Round 3 results: algorithms selected for 4th round - Classic McEliece

- *" Although Classic McEliece is widely regarded as secure, NIST does not anticipate it being widely used due to its large public key size."* [7]
- *"NIST may choose to standardize Classic McEliece at the end of the fourth round."* [7]

[7] Announced on PQC forum `https://csrc.nist.gov/Projects/post-quantum-cryptography/Email-List`

NIST plans for the near future

- For CRYSTALS-KYBER, CRYSTALS-Dilithium, Falcon and SPHINCS+, NIST plans to release draft standards for public comment in 2022-2023.[8]
- NIST plans to have these standards finalized by 2024.[8]
- NIST will continue evaluating candidates in Round 4. (Round 4 will take 18-24 months.[8])
- New call for signatures.
  - By the end of this summer, NIST will issue a new Call for Signatures. [9]
  - The main reason for this call is to diversify the signature portfolio. [9]

[8] https://csrc.nist.gov/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa

[9] Announced on PQC forum yesterday https://csrc.nist.gov/Projects/post-quantum-cryptography/Email-List

Contents

About the project

- Project title: Secure Communication in the Quantum Era
- Project is supported by the NATO Science for Peace and Security Programme.
- Project duration: 2018-2022
- Participants:
  - University of Malta (director is Christian Colombo)
  - The University of Alabama in Huntsville, USA (director is Rainer Steinwandt)
  - Universidad Rey Juan Carlos, Spain (director is María Isabel González Vasco)
  - FEI STU (director is Otokar Grošek)
- Project website: `https://re-search.info/`

Motivation for the project

- The NIST PQC standardization process adresses the issue of post-quantum key-establishment between two parties.
- In certain applications (e.g. conference calls) there is a need for key-establishment between more than two parties.

Main results of the project

- The Spanish and US teams designed a protocol for key-establishment between more than two parties.
- The protocol offers quantum-future security.
- The Maltese and Slovak teams implemented the protocol and created a prototype chat application which uses the protocol and offers quantum-future security.
- The chat application follows the RV-TEE framework[10] for higher security.
- RV-TEE = Runtime Verification enhanced Trusted Execution Environment

[10] Proposed by Mark Vella, Christian Colombo, Robert Abela, and Peter Špaček.

Thank you for your attention!