Post-Quantum Cryptography

Sergey Abrahamyan

Institute for Informatics and Automation Problems

Of NAS RA

AUA

2024

Two types of cryptography

- **Symmetric**
- allows two parties to communicate secretly on a public channel, only if they exchanged a secret key on a private channel before
- Efficient both in hardware and software
- Usually more trusted
- **Asymmetric**
- allows two parties to communicate secretly on a public channel, even if they never communicated before
- Significantly less efficient than symmetric crypto •
- Based on mathematical problems that are hard to solve

Two types of cryptography

- **Symmetric**
- AES(128,192,256) Blowfish, SAFER+ , TripleDES
- **Asymmetric**
- RSA-2048,4096 ECC-256 DSA, ECDSA

Asymmetric Cryptography

- Diffie-Hellman function

  Discrete Logarithm problem

  $$y = g^x$$

  where g is the generator of a prime order cyclic group (finite field element or elliptic curve point)

- RSA function (one-way **trapdoor** function)

  RSA/Factorization problem

  $$y = x^e \bmod N$$

  where N is the product of two primes of roughly the same size

One-way functions

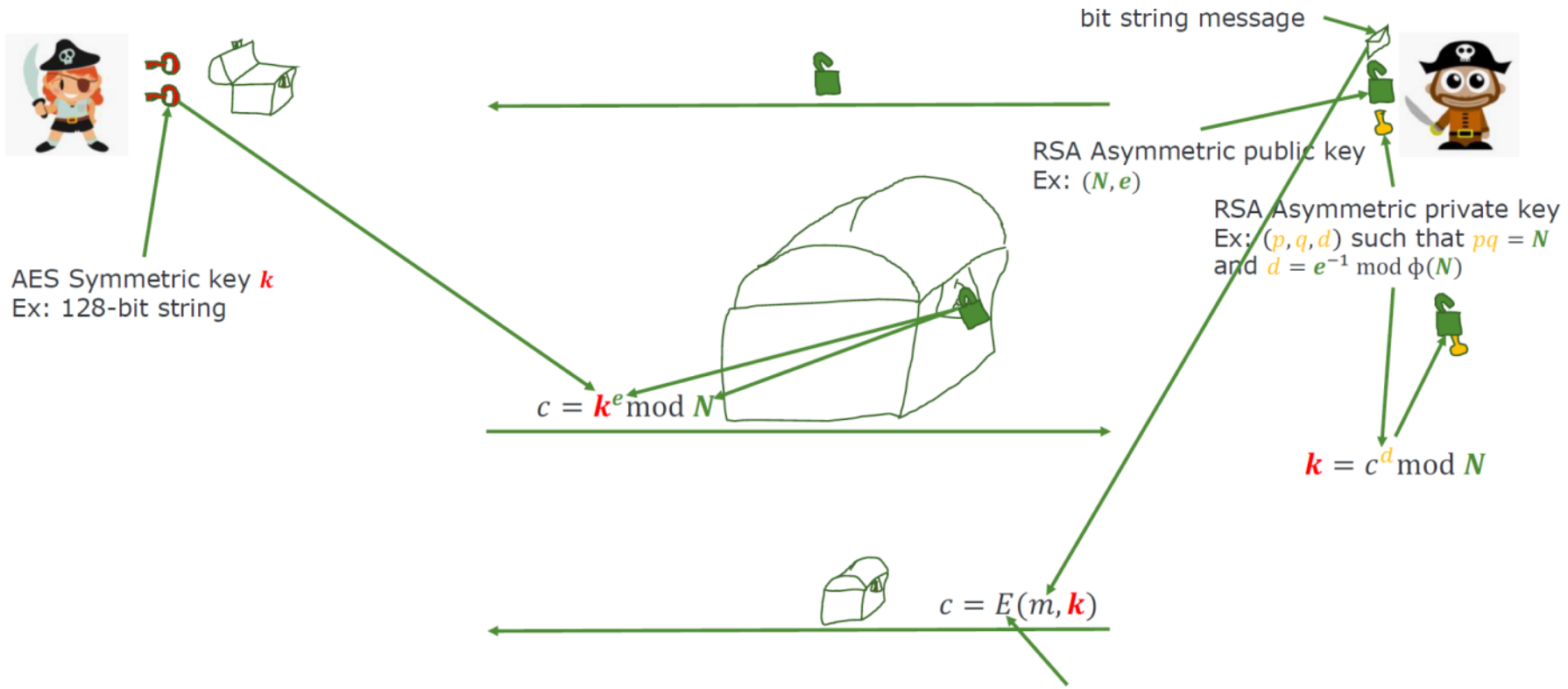
- A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input (this property is called pre-image resistance).
- SHA2 SHA3, MD5

Digital signatures

- A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.
- A valid digital signature gives a recipient reason to believe that
- The message was created by a known sender (authentication),
- The sender cannot deny having sent the message (non-repudiation),

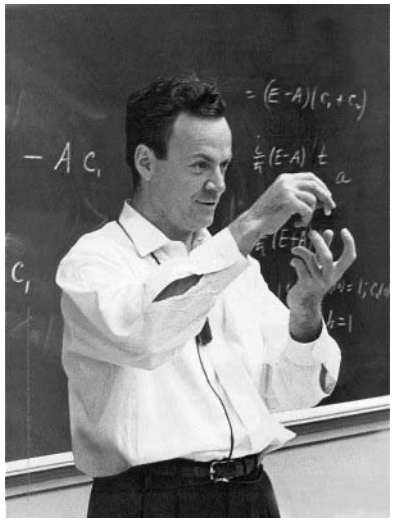
The message was not altered in transit (integrity).

Digital certificates are based on symmetric and asymmetric cryptosystems



Quantum computers

- "I think I can safely say that nobody understands quantum mechanics" - Feynman



- 1982 - Feynman proposed the idea of creating machines based on the laws of quantum mechanics instead of the laws of classical physics.
- 1985 - David Deutsch developed the quantum turing machine, showing that quantum circuits are universal.
- 1994 - Peter Shor came up with a quantum algorithm to factor very large numbers in polynomial time.
- 1997 - Lov Grover develops a quantum search algorithm with O(√N) complexity

Quantum supremacy

- **Quantum supremacy** or "quantum advantage" is the potential ability
- of quantum computing devices to solve problems that classical computers
- practically cannot.
- In computational complexity-theoretic terms, this generally means providing a
- superpolynomial speedup over the best known or possible classical algorithm.
- **So far, quantum supremacy has not been reached yet!**
- Google previously announced plans to demonstrate quantum supremacy before
- the end of 2017 by solving this problem with an array of 49 superconducting
- qubits.
- In October 2017, IBM demonstrated the simulation of 56 qubits on a conventional
- supercomputer, increasing the number of qubits needed for quantum supremacy.
- Then, on march 2018, Google announced Bristlecone, a new 72 qubits quantum
- processor, but it is still trying to make it work…

Quantum computers VS classical crypto

- If a practical quantum computer would exist, it would break all classical factorization and discrete log based public key crypto

  (because of **Shor's algorithm**)

And would force doubling the key sizes of symmetric key cryptography.

- (because of **Grover's algorithm**)
- Not many other quantum algorithms are known… yet!
- So… what solutions should we adopt?

Shor’s algorithm

- **Shor’s algorithm** solves integer factorization and discrete logarithms in polynomial time on a quantum computer. More generally, Shor’s algorithm efficiently solves the hidden subgroup problem for finite Abelian groups. This directly breaks cryptographic primitives that are based on integer factorization, e.g., RSA, and the discretelogarithm problem, e.g., DiffieHellman and ECC

Grover’s algorithm

- **Grover’s algorithm** for quantum computers gives a square root speedup on search problems. This improves brute force algorithms that check every possible key. The square root factor halves the exponent of the time complexity.
- This means, that for example a brute force attack on AES-128 with a cost of at most 2^{128}AES operations on a classical computing system can be finished with about 2^{64} AES operations on a quantum computer .

Grover’s algorithm

- The impact of Grover’s algorithm can practically be averted by doubling security parameters. Doubling the key length of AES from 128bit (AES128) to 256bit (AES256) gives a cost of at least 2^{128} operations on a quantum computer and therefore is considered secure.

Alternatives

- The physicists say:
- “Use quantum technologies to fight quantum technology!”
- **QUANTUM CRYPTOGRAPHY**

- ● The mathematicians say:
- “Just base your crypto on math that quantum computers can’t break.”
- **QUANTUM RESISTANT or POST QUANTUM CRYPTOGRAPHY**

Quantum cryptography in practice

- mainly limited to *quantum key distribution*,
- provides no authentication (apart from PUF technologies),
- requires direct fiber-optical connection or line of sight,
- has a problem with large distances,
- needs new infrastructure and new technology,
- does not work for mobile phones, sensor networks, cars, ...
- does not scale well,

- Quantum computer do not solve **all hard** problems…

- **PQC** consists of classical algorithms that
- run efficiently on classical computers in terms of time, memory, and communication
- are hard to break both by classical and quantum algorithms,
- rely on **different mathematical problems** than integer factorization or discrete logarithms.

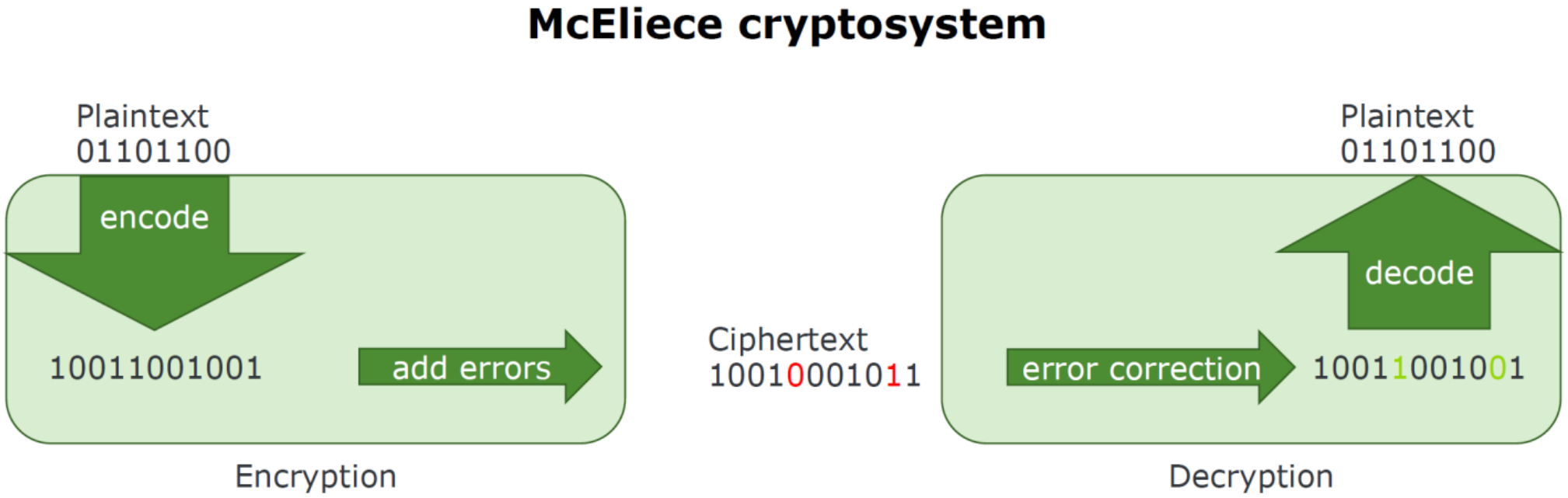
NIST Post-quantum competition

- Feb. 2016 Announcement at PQCrypto 2016
- April 2016 NIST releases NISTIR 8105 - Report on Post-Quantum Cryptography
- Dec. 2016 Formal Call for Proposals
- Nov. 2017 Deadline for submissions
- Early 2018 Workshop — Submitter's Presentations
- 3-5 years Analysis Phase — NIST will report findings
- 1-2 workshops during this phase
- 2 years later Draft Standards ready

Families of PostQuantum Schemes

- The cryptographic community is discussing five different families of postquantum cryptography,
- namely:
- Code-based cryptography,
- lattice-based cryptography,
- Hash-based cryptography,
- multivariate cryptography, and
- supersingular ellipticcurve
- isogeny cryptography.

Error correction to encryption scheme



- Thank you