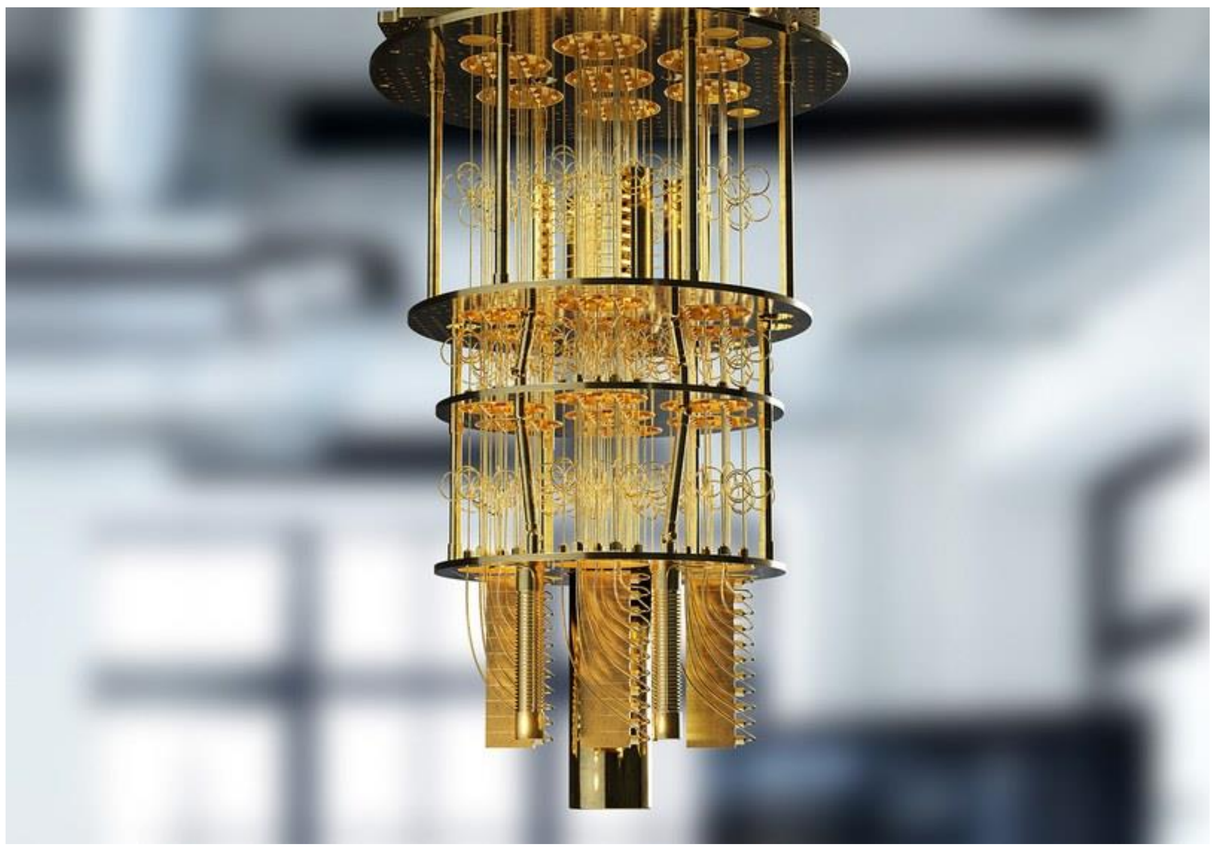
QUANTITY
Quantum-Assisted Cryptanalysis

We are examining the security of cryptosystems in an era where quantum computers are becoming increasingly capable. Alongside established quantum algorithms relevant to cryptography, we will also explore and modify additional algorithms to assess their potential effects on the security of cryptosystems.

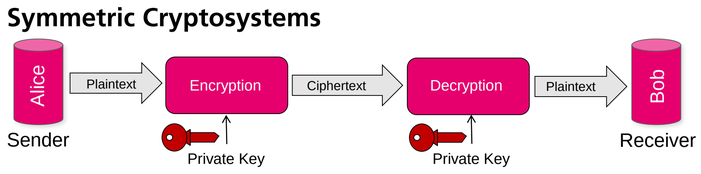
- Quantum-Resistant Cryptography
- Quantum Algorithms
- Classical and Quantum-assisted Cryptanalysis
- Symmetric and Asymmetirc Cryptography



Motivation: Long-term protection of transmitted and stored data in the age of quantum computers

Can someone else read the message?	Confidentiality	⇨ Symm. / asymm. Cryptosystem
Has the information been modified?	Integrity	⇨ Digital Signatures (mainly asymm. Cryptosystem)
How can I be sure, that the person is who they claim to be?	Authenticity	
Can the sender deny having sent the message?	Non-repudiation	

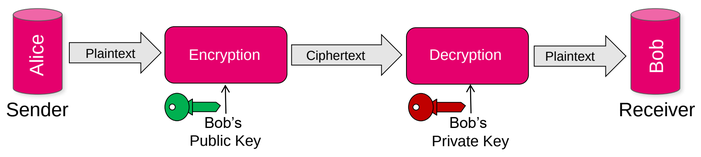
Symmetric Cryptosystems



☺ Used for high data rate transmission

☹ Secure key exchange and key storage required

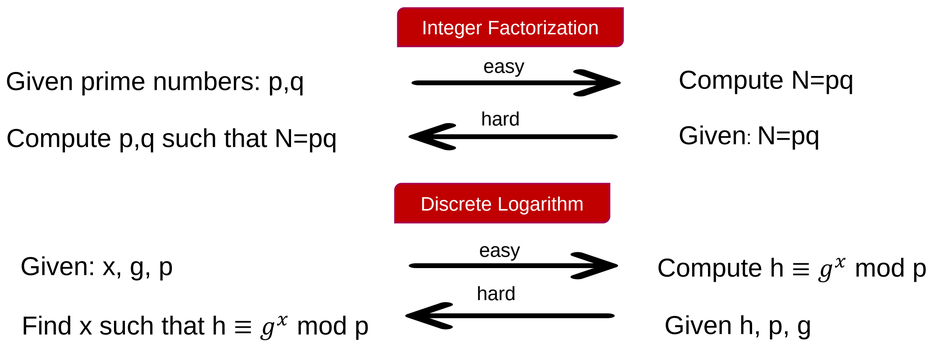
Asymmetric Cryptosystems



Can be used for key exchange and digital signatures

Trusted authority for key distribution required

One way functions



Threats:

In 1994, Peter W. Shor developed an algorithm capable of solving both the discrete logarithm problem and the integer factorization problem in polynomial time, provided a sufficiently large quantum computer becomes available. Since most public-key cryptosystems (PKCs) rely on these problems for security, Shor's algorithm poses a significant threat to them. In 1996, Lov Grover introduced a search algorithm that can weaken both symmetric and asymmetric cryptosystems. However, the vulnerability in symmetric cryptosystems can be countered by simply doubling the key size.

Goal:

Harden the term „Quantum Resistant"

Currently, the term "quantum resistant" primarily means "resistant to attacks using Shor and Grover." However, this covers only a very small portion of the potential attack methods using quantum algorithms.

To determine the security level of encryption methods, the most efficient attacks from both classical and quantum computers must be considered.
A promising approach is the combination of classical cryptanalysis methods with new or existing quantum algorithms.
The analysis and development of cryptographically relevant quantum algorithms thus make an important contribution to determining the long-term security level of encryption methods.

We need to know

- *…which* problems are hard for quantum computers?
- *…how hard* certain problems/operations are for quantum computers
- …the crypto-relevance of existing quantum algorithms (apart from Shor and Grover)
- …the relevance of potential quantum-assisted cryptanalysis methods

Overview

The security of cryptosystems is based on hard problems (i.e. problems that can be proven / are believed to be hard to solve).

The security level of the developed quantum-resistant cryptosystem is determined by the most efficient attack on both, classical and quantum computers.

Apart from Shor's and Grover's algorithm only little is known about the potential effect of quantum algorithms on the security level of cryptosystems.

Roadmap

Analysis of classical cryptanalysis methods for quantum-resistant cryptosystems

- Analysis of crypto-relevant quantum algorithms
  - Analysis of quantum algorithms regarding their potential to speed up crypto-relevant operations
    - e.g. Harrow-Hassidim-Lloyd (HHL), Quantum Algebraic Attack (QAA), Quantum Approximate Optimization Algorithm (QAOA)
  - Definition of adequate complexity metrics for quantum algorithms
- Development of quantum-assisted cryptanalysis algorithms
  - Adaptation of the identified quantum algorithms for new quantum-assisted cryptanalysis methods
  - Complexity analysis of the developed quantum-assisted algorithms
- Proof-of-Concept implementation of the developed algorithms
  - Implementation of the classical parts
  - Implementation of the quantum parts

Industry Cooperation

- **Analysis of existing quantum algorithms** regarding their cryptographic relevance
- **Derivation of complexity metrics** for quantum algorithms that are well-suited to derive the security level of existing and future cryptosystems
- **Complexity analysis** of the developed quantum algorithms with respect to the developed complexity metrics
- **Proof-of-concept implementation** of the quantum part of the developed algorithms

NIST Standardization for Post-Quantum Cryptography

- *Round 1* (Nov. 2017): 82 submission, resulting in 69 candidates
- *Round 2* (Jan. 2019): 26 candidates
- *Round 3* (Jul. 2020): 7 finalists, 8 alternates
- 4 algorithms selected for standardization (Jul. 2022)
- *Round 4* candidates announced (Jul. 2022)
- Draft released for three of the standards for public comments/feedback (2023)
- Three of the standards are now finalized and ready to use (August 2024)

Broken by classical (!!!) attacks

	PKC/KEM	Type	Signature	Type	
finalists	Classic McEliece	code	CRYSTALS-DILITHIUM	lattice	
	CRYSTALS-KYBER	lattice	FALCON	lattice	
	NTRU	lattice	Rainbow	multivariate	
	SABER	lattice			
alternates	BIKE	code	GeMSS	multivariate	
	FrodoKEM	lattice	Picnic	hash	
	HQC	code	SPHINCS+	hash	
	NTRU Prime	lattice			
	SIKE	isogeny			

More information about the project on our website

A project of

DLR Institute of Communications and Navigation

Industry partner

HQS QUANTUM SIMULATIONS

Contact

Dr. Hannes Bartz
Cornelia Ott

DLR | QCi

Get in touch.
We enable quantum!

Supported by:

Federal Ministry for Economic Affairs and Climate Action

on the basis of a decision by the German Bundestag