The Mathematics of Post-Quantum Cryptography

Max Planck Institute for Mathematics, Bonn
December 4, 2024

Welcome

- Speakers: please upload your slides in case you haven't done so. (Ask one of the organizers in case you lost the link.)
- All participants: please sign the participant list!
- Coffee/tea: there will be coffee, tea, fruit and water in the tea room on the 4th floor,
- Additionally, cakes and cookies for the 4pm breaks.
- **Please note: no food or drinks (except water) are allowed in the lecture hall!**

Conference Dinner

- Only registered participants (registered for dinner) can participate.
- Please inform Pieter if you registered for dinner but are not able to come.
- We meet at the reception at **18:30** to walk to the restaurant.
- Restaurant: Nees (in front of Poppelsdorfer Schloss), Meckenheimer Allee 169.
- Dinner starts at 19:30.
- For all dinner questions: ask Pieter!

Introduction

- Public-Key cryptography: usually relies on **computational hardness assumptions**.
- That means essentially: we assume, a certain problem cannot be solved efficiently (in polynomial time).

Example 1 (RSA problem)

Given a composite positive integer n, exponent $e \in \mathbb{Z}$ and

$$c = m^e \pmod{n}$$

(for secret m), find m.

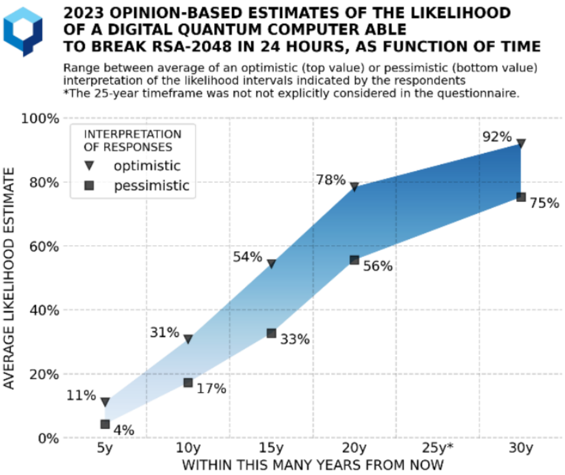
- This is easy if factoring integers is easy.

Example 2 (Discrete logarithm problem)

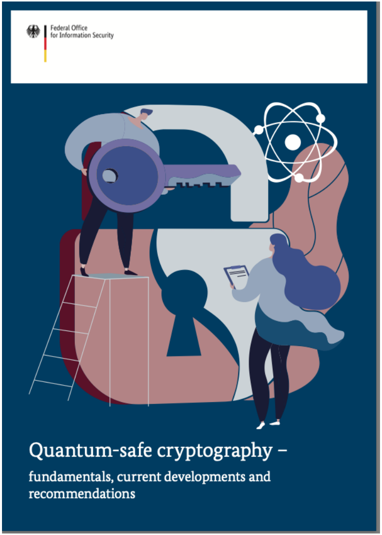
Given elements a, b of a group G, with $b = a^k$ find k.

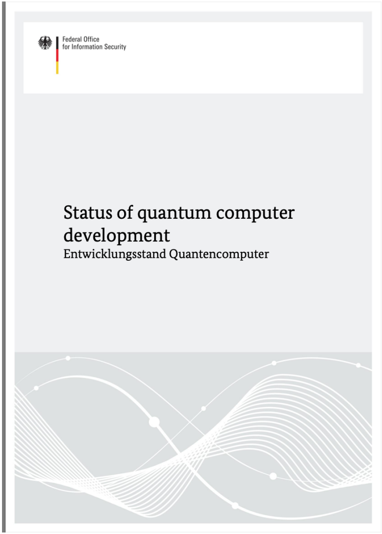
Introduction

- For **Quantum computers**, there are algorithms (Shor, 1994), that solve these problems (factoring, DLP) in polynomial time.



BSI publications





Post-Quantum Cryptography

- **Post-Quantum cryptography** instead relies on the assumed quantum and computational hardness of certain mathematical problems:
- Lattice problems: Shortest Vector Problem, Closest Vector problem
- Decoding problems: For a (linear, binary code), solve the decoding problem
- Problems related to isogenies between elliptic curves
- Systems of multivariate polynomial equations
- Group actions
- Equivalence/Isomorphism problems
- ....?

A look at our program: today

- 13:20: Wouter Castryck: Interpolating **isogenies** between elliptic curves: destructive and constructive applications
- 14:25: Peter Stevenhagen: **Lattices** in Number Theory
- 15:15: Leo Ducas: Principles of **Lattice** Cryptography, and cryptanalysis by lattice reduction
- 16:40: Monika Trimoska: Algebraic cryptanalysis applied to **equivalence problems**
- 17:30: problem session

A look at our program: tomorrow

- 9:00: Hugues Randriam: The syzygy distinguisher (**codes**)
- 9:45: Sabrina Kunzweiler: **Isogeny**-based **group actions** in cryptography
- 11:00: Aurel Page: Hardness of **isogeny problems** and equidistribution
- 14:05: Severin Barmeier: Utility and usability of projective resolutions (somewhat related to Hugues talk)
- 15:00: Wessel van Woerden: Dense and smooth **lattices** in any genus