Quantum Crypto

MTAT.07.024

Team:

— Dr. Dirk Oliver Theis (assoc.prof. TCS)
— Shahla Novruzova

What we'll cover

- Review of the basics of basic quantum information theory
  ➜ take FunQ as starting point
- Quantum crypto / communication
  ➜ up to QKD (BB84)
- Shor's algorithm
  ➜ Quantum Fourier transform

Fill in math background:

- Start from what's covered in FunQ
- More about Hilbert space operators
- More about spectral theory
- Finite Fourier transform

1.

Quantum mechanics for quantum information processing (today).

2.

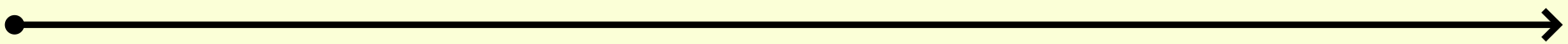
Quantum circuit model of quantum information processing.

3.

QKD.

4.

Shor's algorithm.



A.

Hilbert-space operators.

B.

Spectral theory.

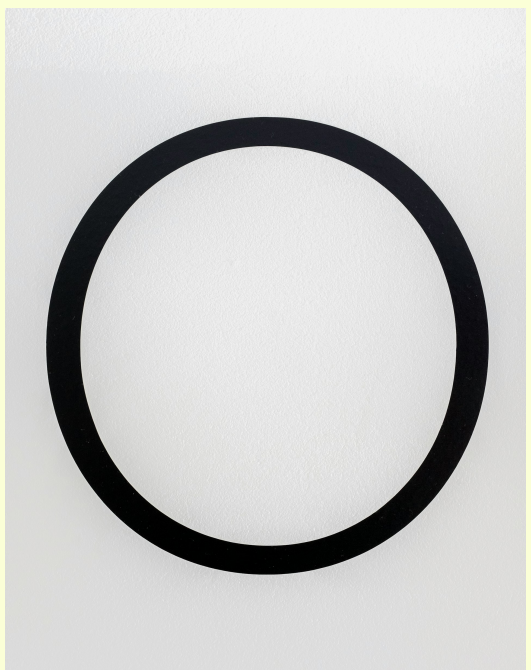
Γ.

Finite Fourier transform.

Course Organization

- Seven homework assignments:
  - Feb27, Mar12, Mar26, Apr9, Apr23, May7, May21
  - One week to solve.
  - No HW cheating/copying 👉 "NaN"
  - No HW team work 👉 "NaN"
- Course grade = average of HW marks
  - Average containing NaN = NaN = F
- Course communication: GitHub
  - `github.com/dojt/Q-crypto-2024`
  - Send your GitHub avatars to:

    `shahla.novruzova@ut.ee`
  - Slides + HW will be made available there



Rooms...?

- Mon 12:15-13:45 1022
- Tue 10:15-11:45 2045