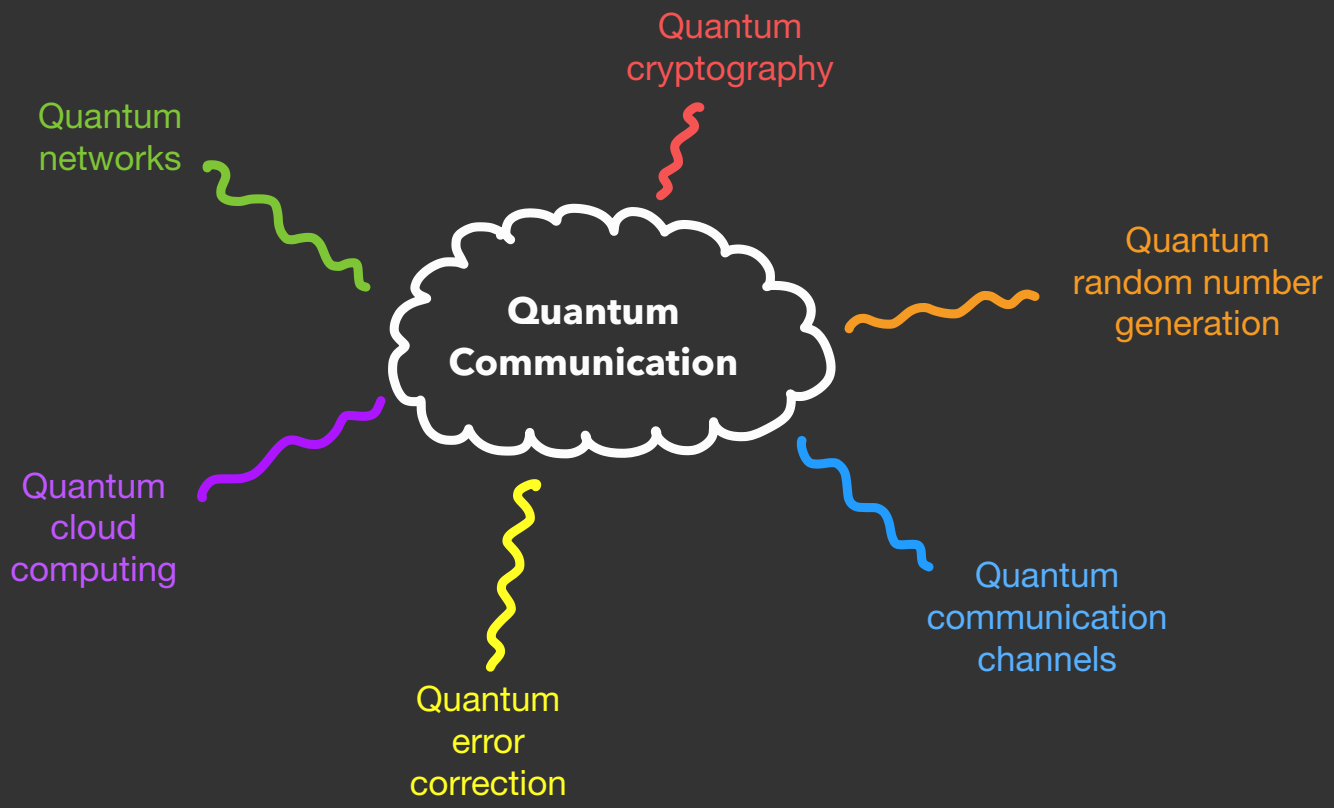
Quantum Communication

Ramona Wolf
University of Siegen

European Quantum Technology Summer School, Strasbourg, July 12th

Universität Siegen


Quantum cryptography
Quantum networks
Quantum random number generation
Quantum Communication
Quantum cloud computing
Quantum communication channels
Quantum error correction

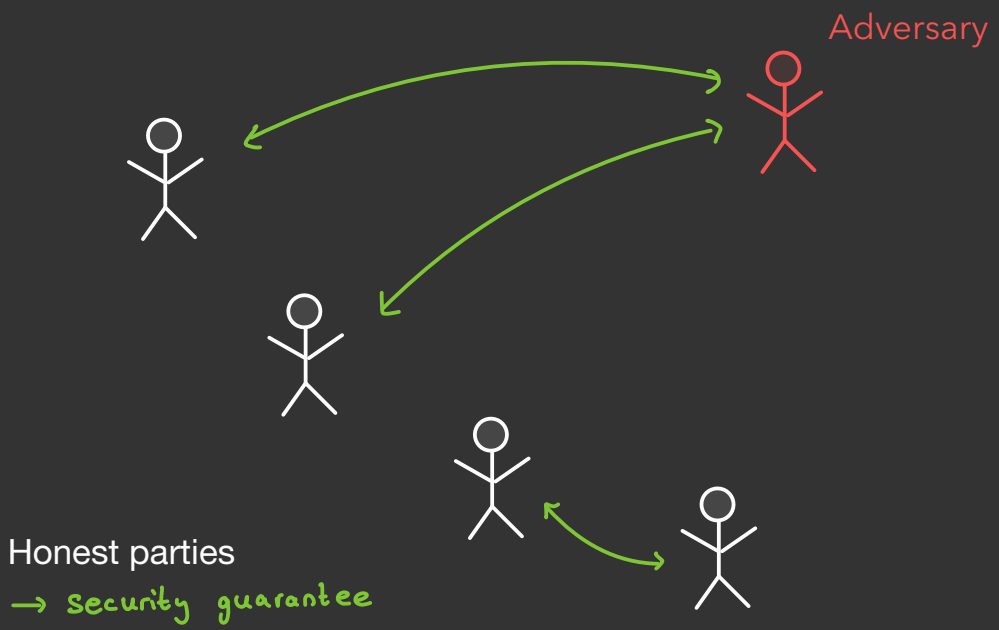
Two types of protocols:

1. Using quantum to enhance efficiency:
   - Super-dense coding ← transmitting two bits of information with one use of the channel
   - Quantum source coding ← efficient compression of quantum information
2. Using quantum to enhance security:
   - Quantum key distribution ← Unbreakable security from quantum principles
   - Quantum random number generation ← Provably unpredictable numbers
   - Cloud computing (e.g. blind quantum computing) ← secret computation on a quantum sever

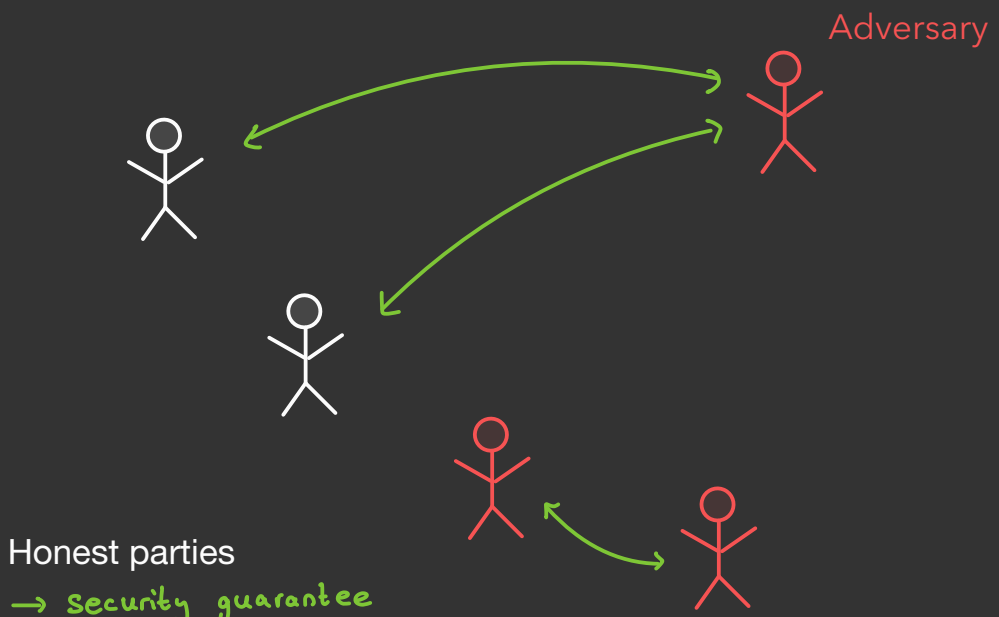
Security in quantum communication

What is security?

What is security?



What is security?

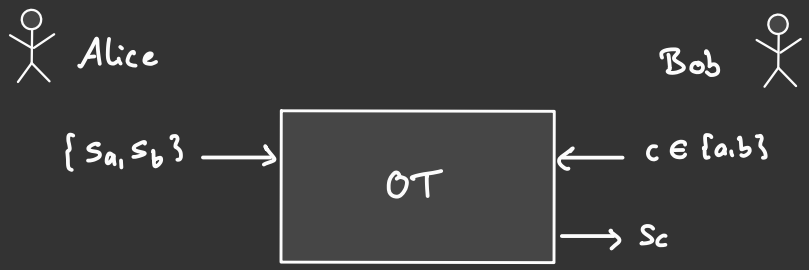


Security proof for a
communication protocol

Assumptions  Security guarantee

Oblivious transfer

universal for two-party cryptography



Security proof for a communication protocol

Assumptions → Security guarantee

Classically: computational assumptions

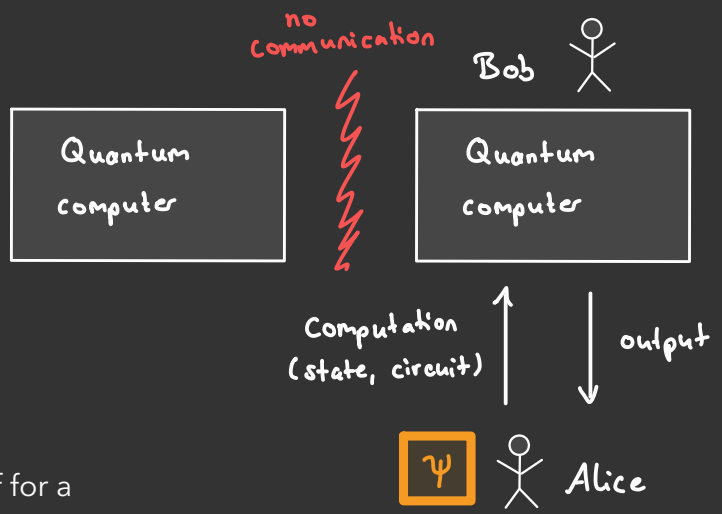
Quantum?

Also not without assumptions :-(

e.g., Bob only has bounded quantum memory

- Bob receives the correct bit
- Bob cannot learn the other bit
- Alice does not learn c

Blind quantum computing



Security proof for a communication protocol

Assumptions

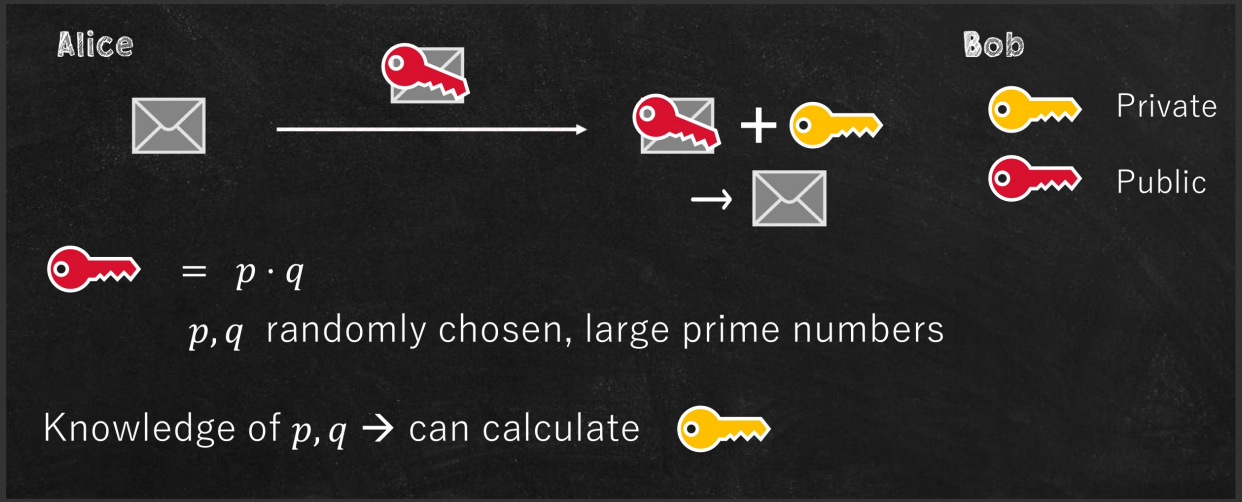
Classically: impossible
Quantum: Alice can prepare quantum states
Classical Alice: Need additional assumption, e.g. second quantum computer

Security guarantee

- The output is correct
- Bob learns nothing about the circuit, the input, and the output

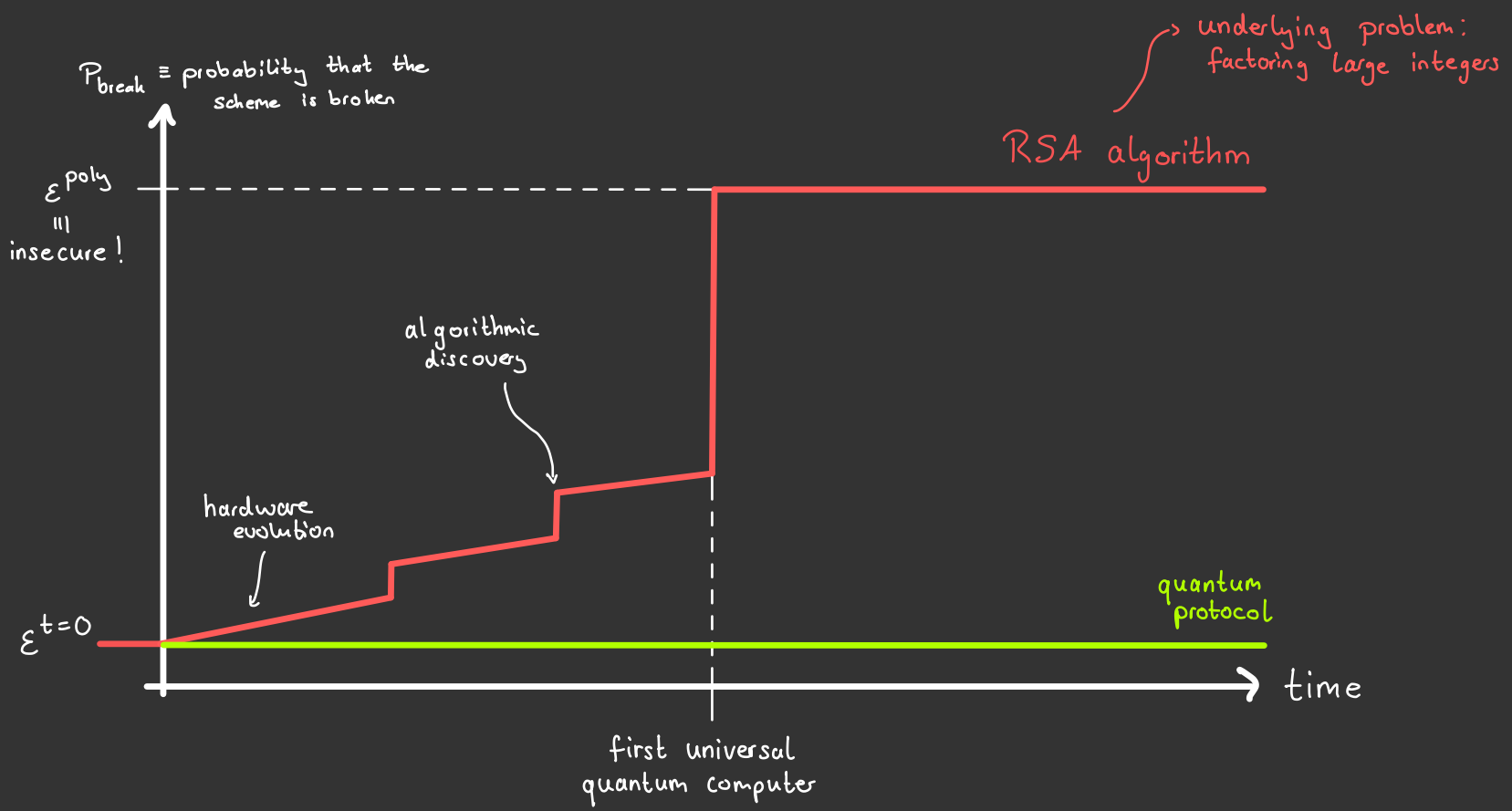
Secure message transmission

Classically: RSA



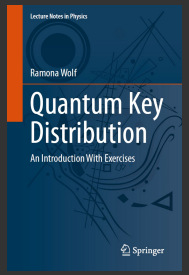
Assumption: Factoring large numbers is hard

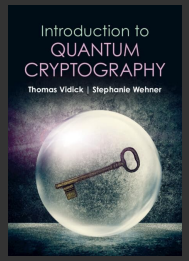
Not for a quantum computer!


P_{break} ≡ probability that the scheme is broken
underlying problem: factoring large integers
RSA algorithm
ε^{poly}
≡
insecure!
algorithmic discovery
hardware evolution
$\varepsilon^{t=0}$
quantum protocol
time
first universal quantum computer

References:

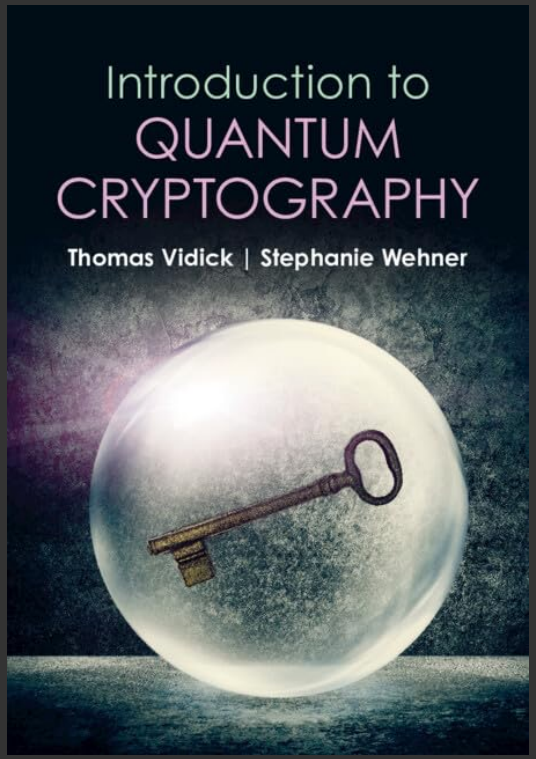
- Textbooks:
  - Thomas Vidick and Stephanie Wehner, "Introduction to quantum cryptography"
  - Ramona Wolf, "Quantum key distribution"





- Articles:
  - R. Renner and C. Portmann, "Security in quantum cryptography", Rev. Mod. Phys. 94, 025008 (2022), arXiv: 2102.00021
    Definition of security, composability
  - R Renner and R. Wolf, "Quantum advantage in cryptography", AIAA Journal 61 (5) (2023), arXiv: 2206.04078
    Non-technical introduction to QKD and current challenges
  - M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof of QKD", Quantum 1 (14) (2017), arXiv: 1506.08458
    Detailed security proof including all steps (technical paper)

More about quantum cryptography:



More about QKD: