Aalto University

Applications of Quantum Key Distribution (QKD)

Olav Tirkkonen, Iikka Elonsalo, Jari Lietzen, Teemu Manninen, Ilkka Tittonen, Roope Vehkalahti

Departments of Communications and Networking & Micro and Nano,

Aalto University

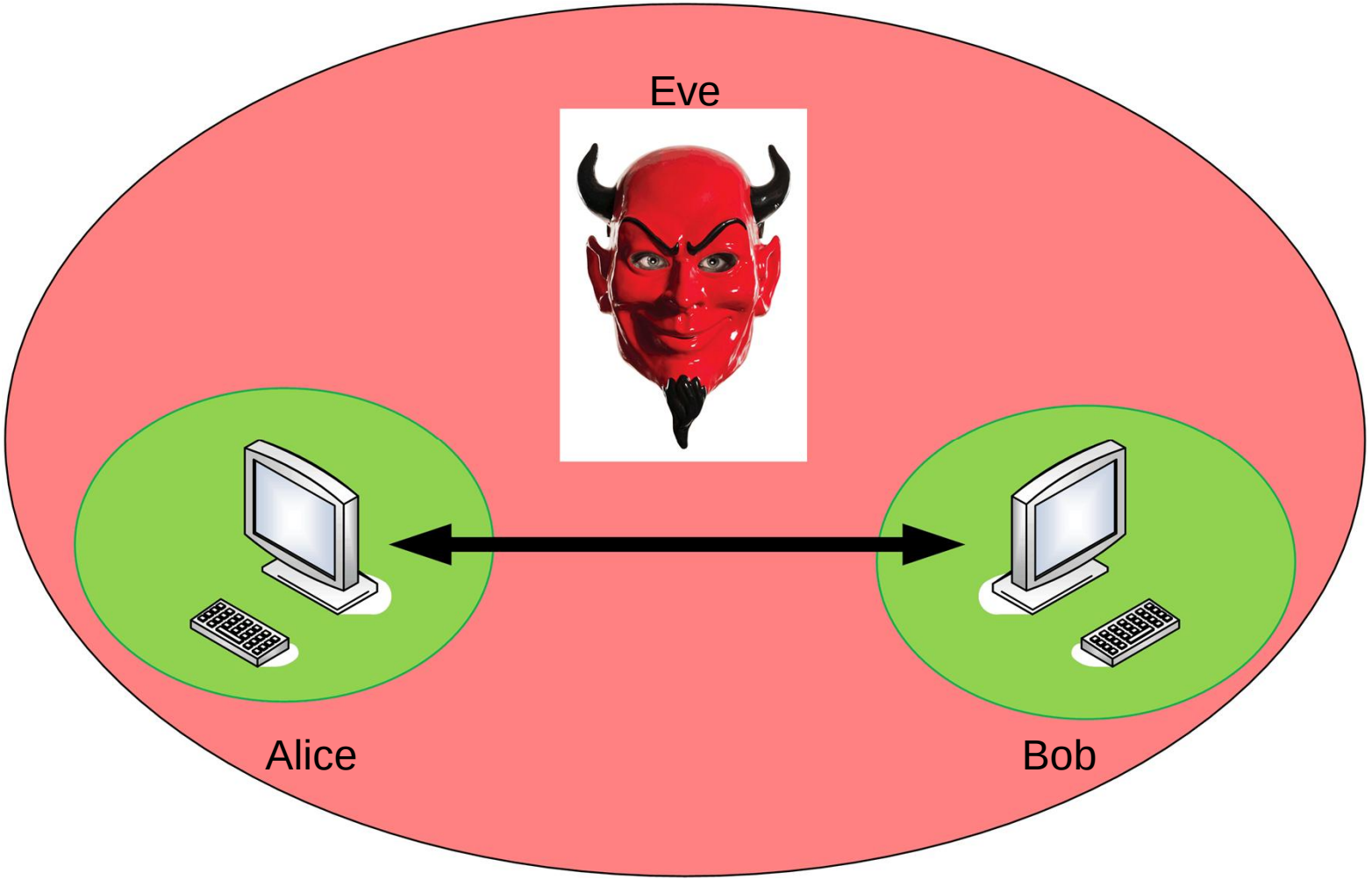
16.11. 2017

Quantum

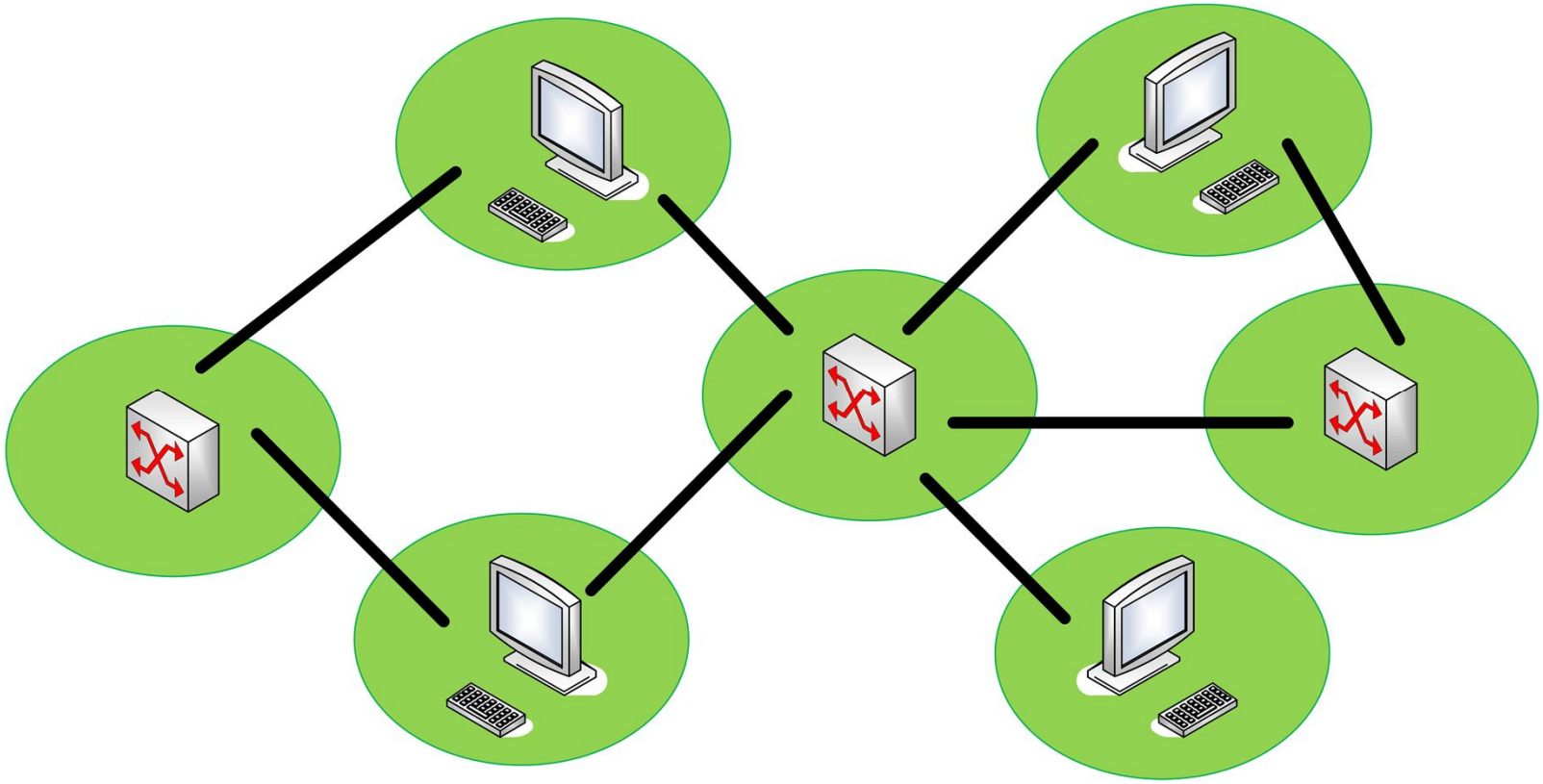
- Quantum communication
  - Communicate bits in absolute security
- Quantum key distribution
  - Generate keys of a priori unknown bits in absolute security
- Security guaranteed by laws of nature
  - Not hypotheses on problem hardness
  - Principles of quantum mechanics have been under doubt for the better part of 100 years
  - Proven to be more fault tolerant than most laws of nature
- Quantum:
  - communication with definitely non-macroscopic number of particles,
  - and non-macroscopic energy

    è this is fragile

Point-to-point



Trusted Node Network

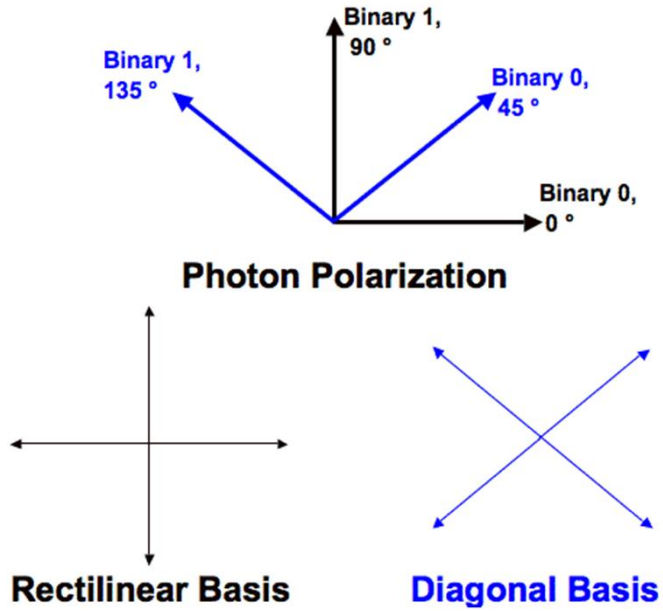


- Caveat:
  - Assume that green blobs completely isolated, except for the communication links puncturing them

What's Up in the World?

- China:
  - QKD-satellite (August 2017)
  - 2000 km QKD-network (August 2017)
- ID Quantique (Switzerland)
  - > 100 QKD systems soled (by 2017)
  - New Clavis3: 3 kbps over 50 km, max distance 100 km
- Toshiba
  - 2 Mbps over 50 km, 10 Mbps over 10 km
  - Trusted node networks under construction
  - Ultimate goal: quantum internet

Quantum Security



- Based on

1. transmissions in quantum basis unknown to Eve and Bob

2. and collapse of wave function during measurement
   - To get hold of the information, one has to measure

   è An eavesdropper on line leaves signature of presence

3. and no-cloning theorem:
   - Eavesdropper cannot clone an unknown state and then collapse it

- Quantum hacking happens in the engineering domain

Prototype Protocol: BB84

Alice sends to Bob photons with X(V/H) and Z(D^{45}/D^{135}) polarization.

Bob chooses a base and measures incoming photons.

XZ XXZ X Z XZ Z XZ X Z X Z X X Z bases

results

Bob sends the basis he used for each photon over a classical channel.

XZ XXZ X Z XZ Z XZ X Z X Z X X Z

Alice tells Bob which ones are correct over a classical channel.

X XZ X Z XZ X X Z X

Bob examines the ones they agree upon (if no eavesdropping).

Bob decodes the photons.

1 1 0 0 1 1 1 1 0 0 0

Alice sends Bob the parity of a selected subset.

1 1 0 0 1 1 1 1 0 0 0 Parity of 1,4,5,9,11.. =EVEN

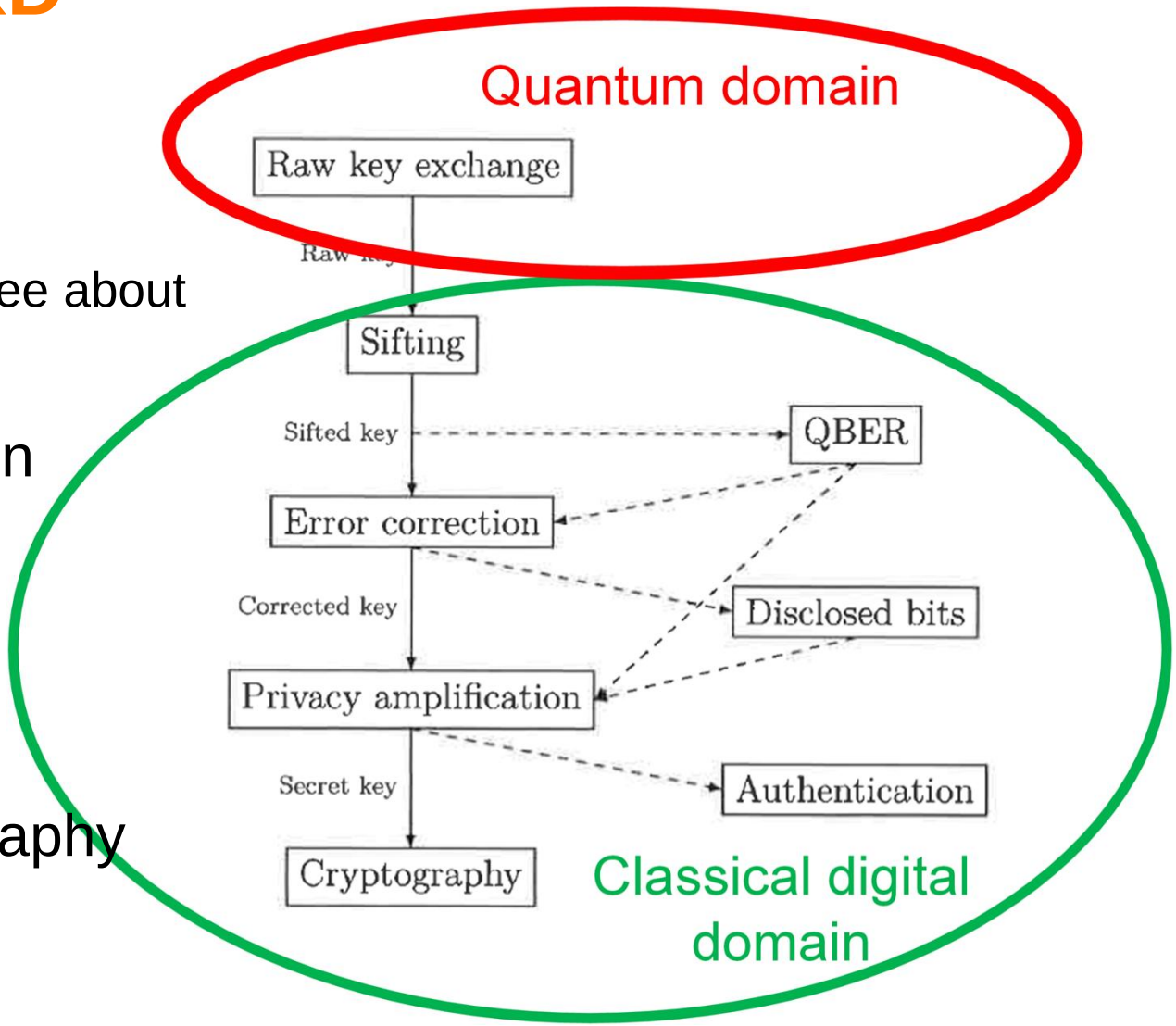
Bob verifies the parity of a selected subset.

1 1 0 0 1 1 1 1 0 0 0 Parity of 1,4,5,9,11.. = OK

1 0 1 1 1 0 Secret Key

Stages of QKD

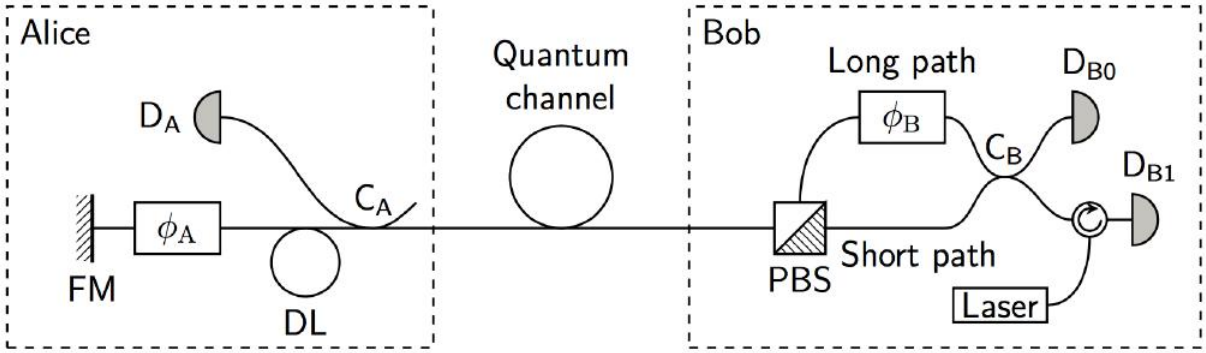
- Generate raw keys
- Sifting
  - Agree what you agree about
- Correct errors
- Privacy Amplification
  - Compress away information that Eve may have
- Authenticate
- Use key in cryptography



Hardware and Software

- Hardware
  - Low-loss fiber Truly random number generators
  - Light sources (attenuated lasers)
  - Single photon detectors
  - è To increase range: invest in expensive fiber, or cooling of detectors
    - Non-zero key rate at 404 km [Yin 2016]
    - ultra-low loss fiber, superconducting detectors

- Quantum protocols
  - Generating, transmitting and receiving quantum states



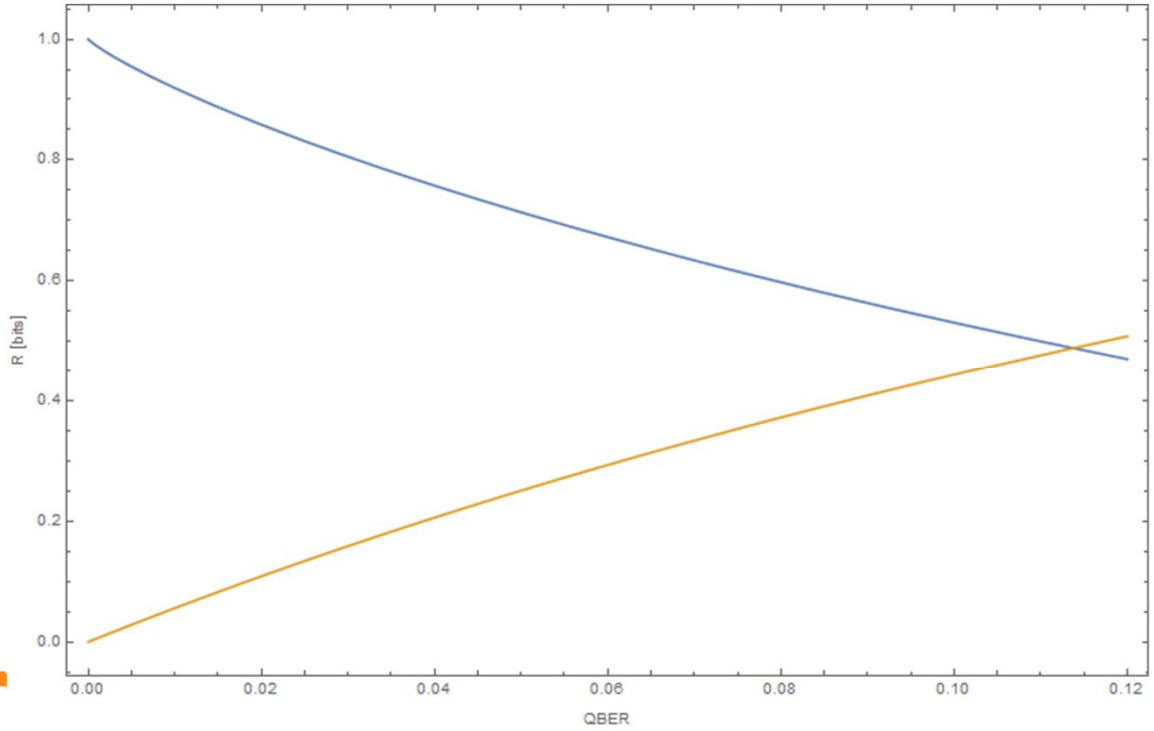
- Classical protocols
  - Error correction, privacy amplifiation, authentication
  - Increase range: invest in digital innovation

Error Correction & Privacy Amplification

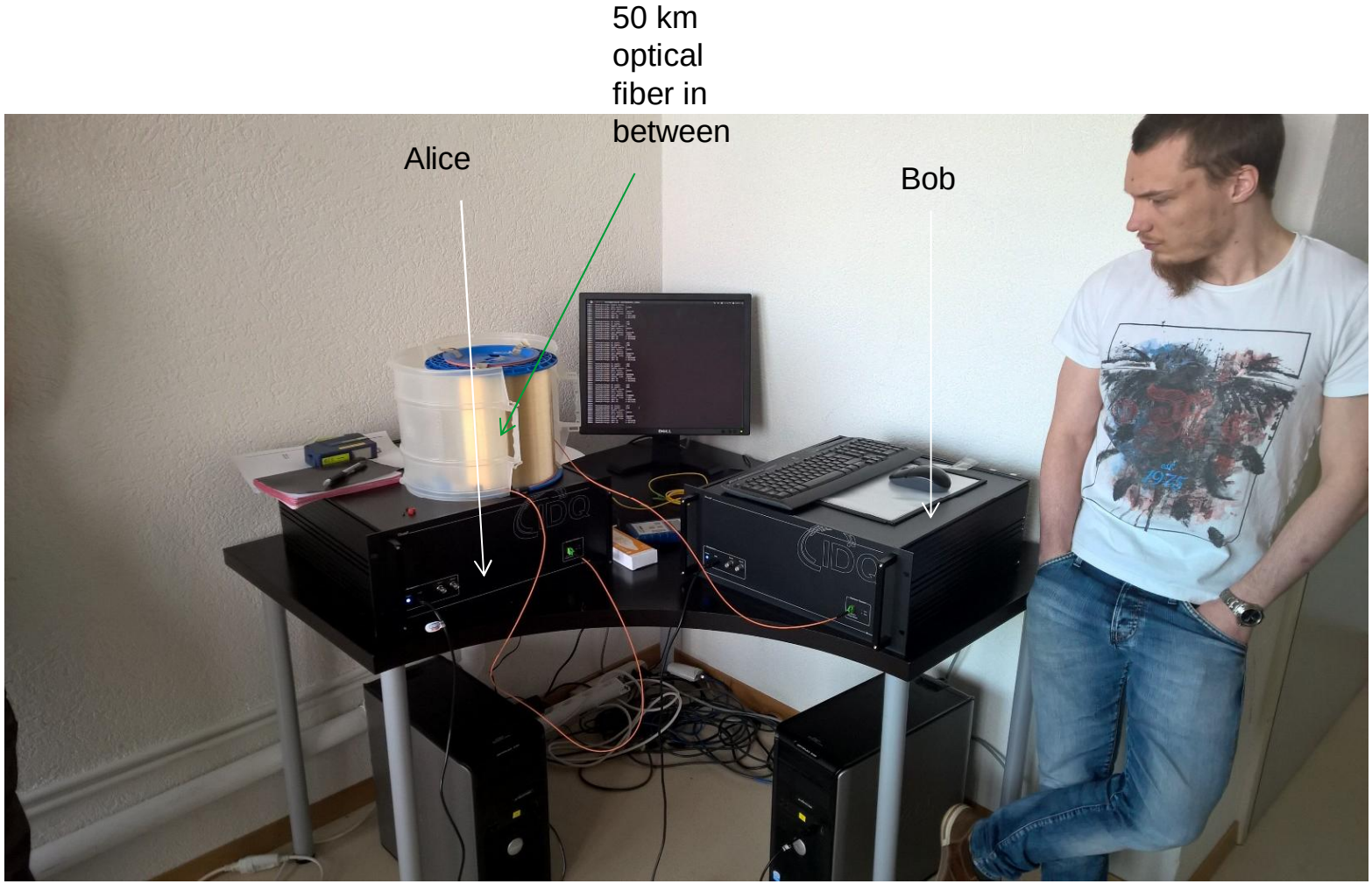
- The channel may cause errors in the sifted bits: QBER
- Correcting errors: Alice and Bob want the same secret
  - Errors have to be corrected
  - Classical error correction coding
  - A fraction of the sifted bits are lost in this
- Privacy amplification
  - All errors assumed to be caused by Eve

  è part of bits discarded
- Conventional method:
  - If QBER > 11%

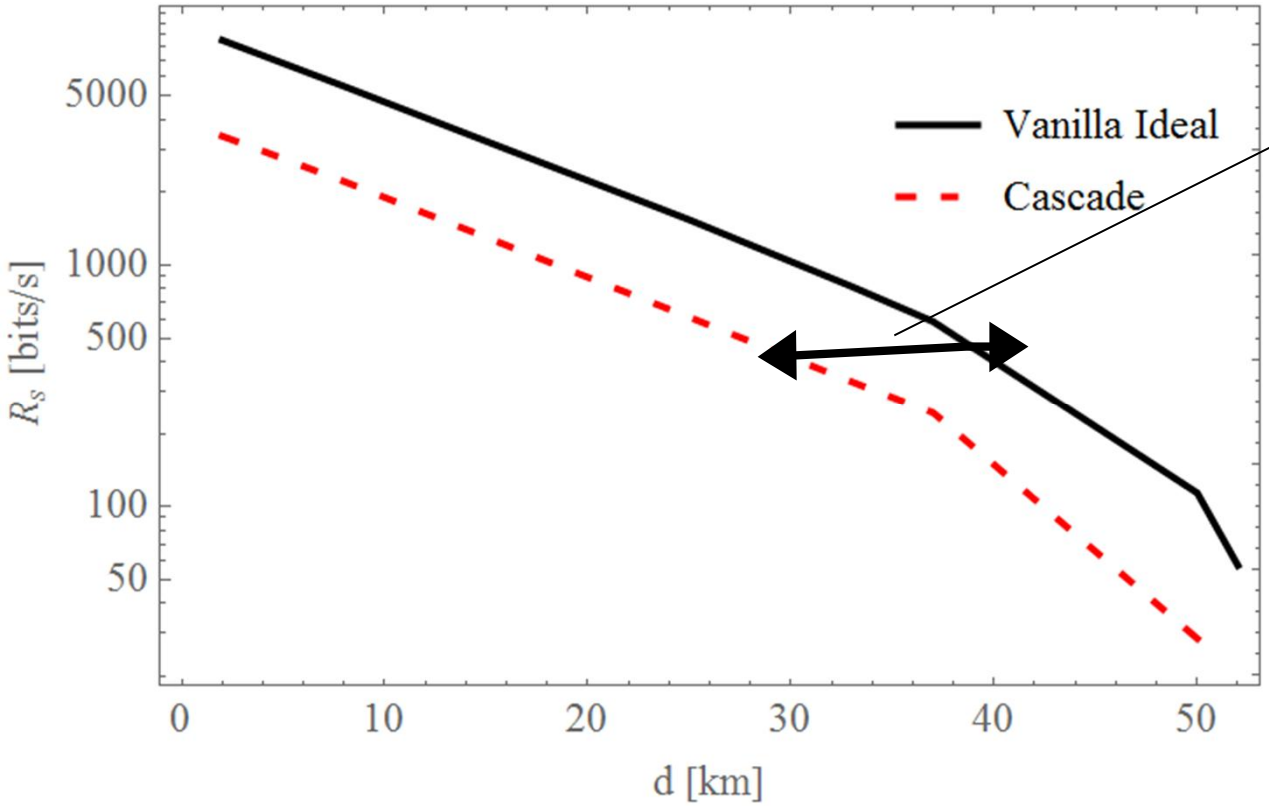
  è key rate = 0



IDQuantique QKD setup



Measurement Results



- Gap between theory and practice:
  - Coding inefficiency (can be shrunk a bit)
  - Authentication

- ID Quantique commercial product Clavis2
- Error correction based on Cascade
- Key production runs lasting days
  - Fluctuations in performance observed

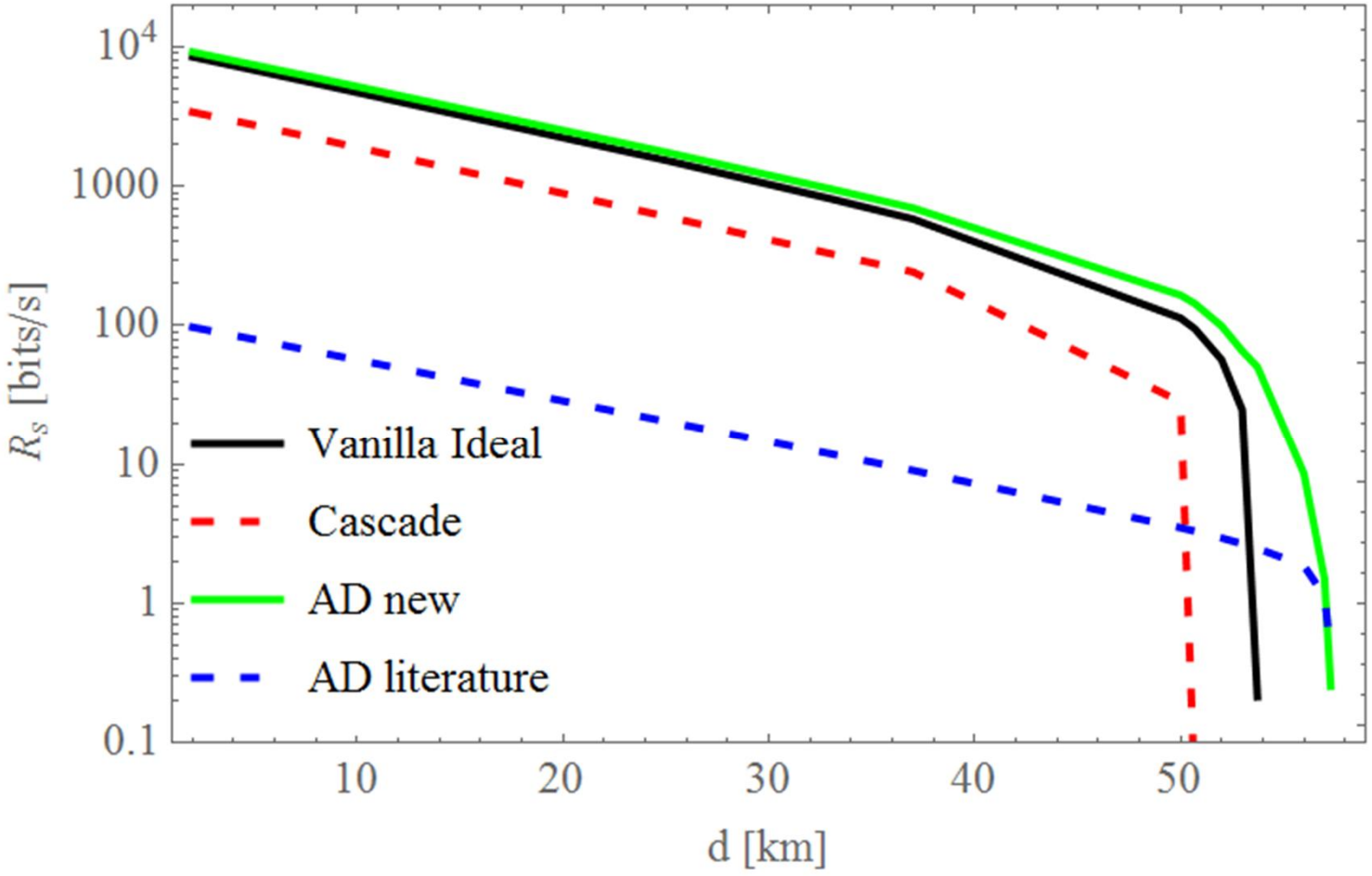
Advantage Distillation

- The conventional scheme (and QBER < 11% bound) is based on assumption that Bob reconstructs the whole key before privacy amplification
- Relaxing this it is possible to construc two-way protocols that work up to QBER 20% [Chau 2002, Renner 2005]
- Advantage Distillation:
  - Discard some part of the sifted key where there is a higher density of errors
  - Concentrate on correcting a part with a lower density of errors
- Two-way key exchange enables longer distances

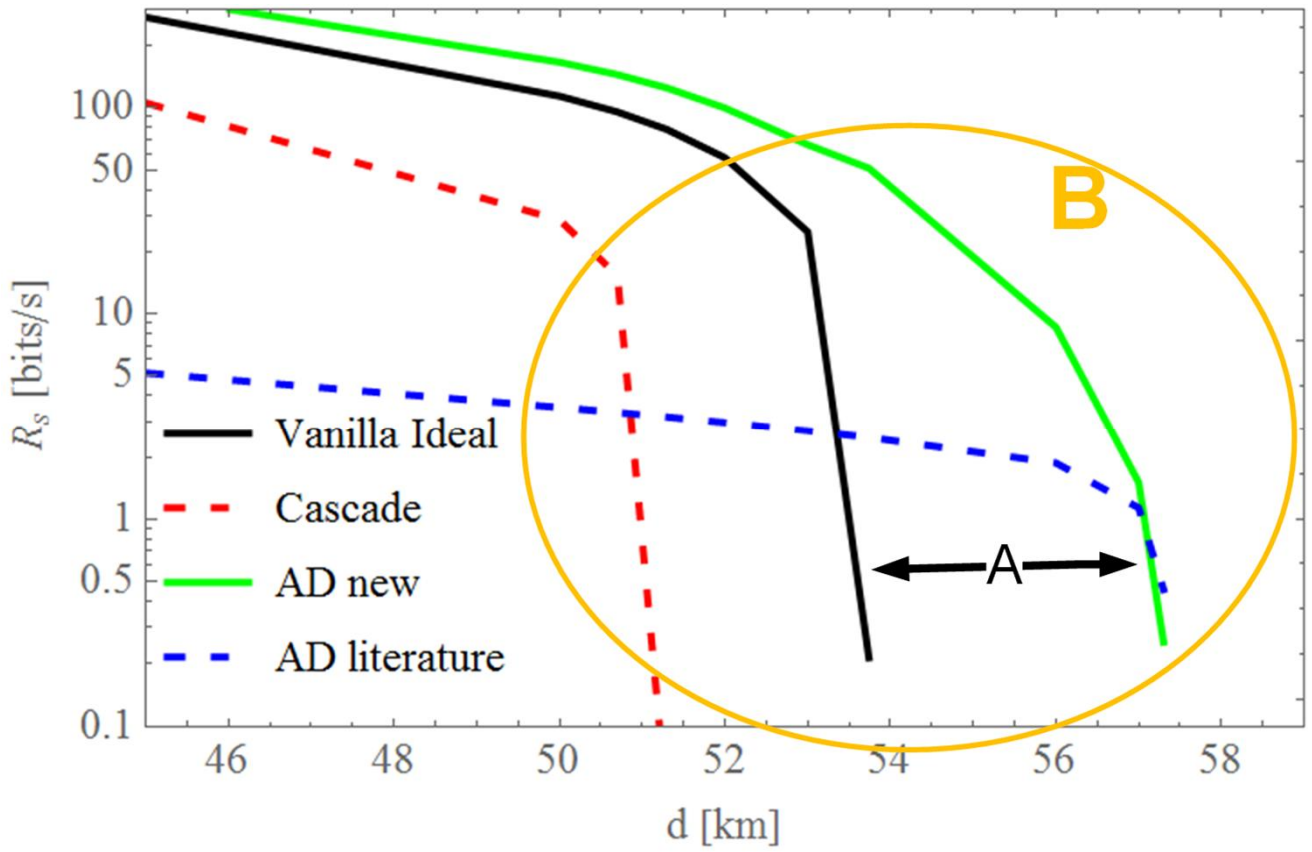
Problems of Two-way Protocols

- Why does, e.g., ID Quantique not use two-way protocol?
- Conventional wisdom about two-way protocols:
  - when QBER is low, they produce low key rate [Scarani 2009]
- This wisdom holds with current protocols
- We do not see any fundamental reason why this should be so.

Projected Perfromance of Advantage Distillation



Zoom



A. Potential range increase from advantage distillation
B. Problematic range where detector dark count dominates QBER

(cooling helps)

Summary

- Discussed Quantum key distribution
- Reported measurement results from key production runs lasting days
- Reported work on error correction in Quantum Key Distribution
- Novel error correction & privacy amplification that can be used with any quantum key generation protocol
- Applying on top of state of the art commercial equipment would increase range by ~10% (almost for free)
- The best protocol in classical part with any QBER
- High potential to further increase range, if cooling applied to reduce detector-induced errors