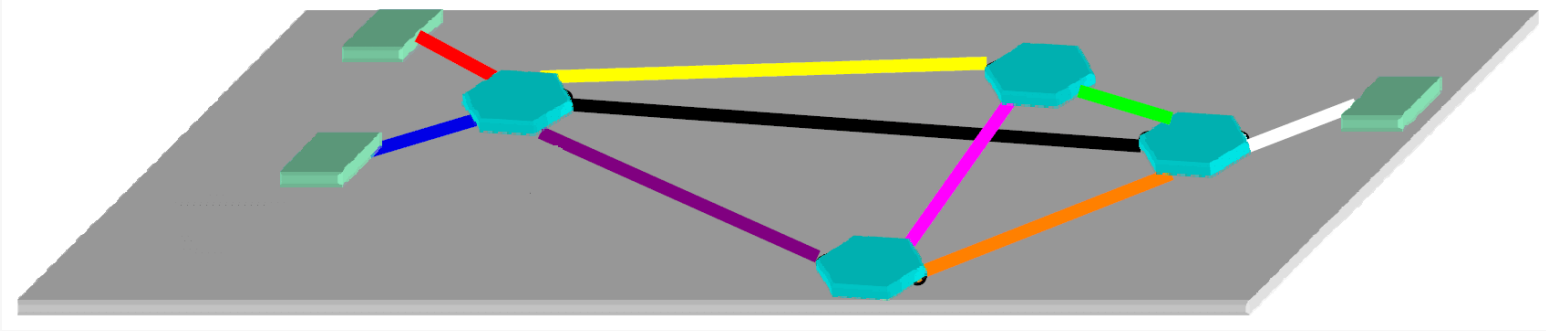
Towards Quantum Communication Networks



Quantum Communication

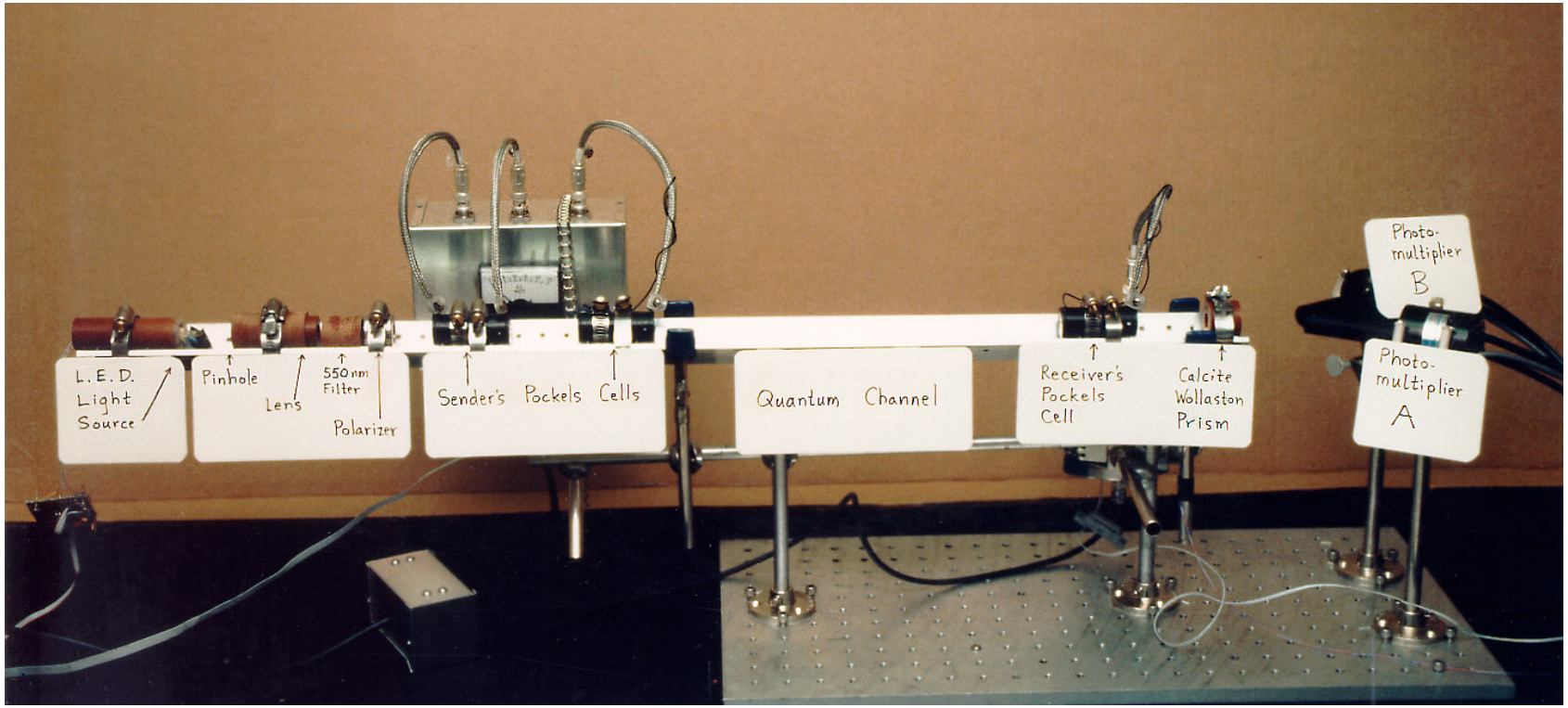
- applications
- today's networks
- future – quantum – networks

applications

- Quantum Key Distribution
  for secure communication
- cryptographic primitives:
  coin-tossing, secret-sharing, etc.
- communication complexity tasks, quantum games, quantum metrology
- quantum teleportation, entanglement swapping → distribute entanglement
- quantum internet → quantum-data links between quantum computation nodes

Quantum Key Distribution

- QKD enables quantifiable security



BB84: errors in key are measure for the information of a potential eavesdropper

commercial systems

- Id Quantique
  www.idquantique.com

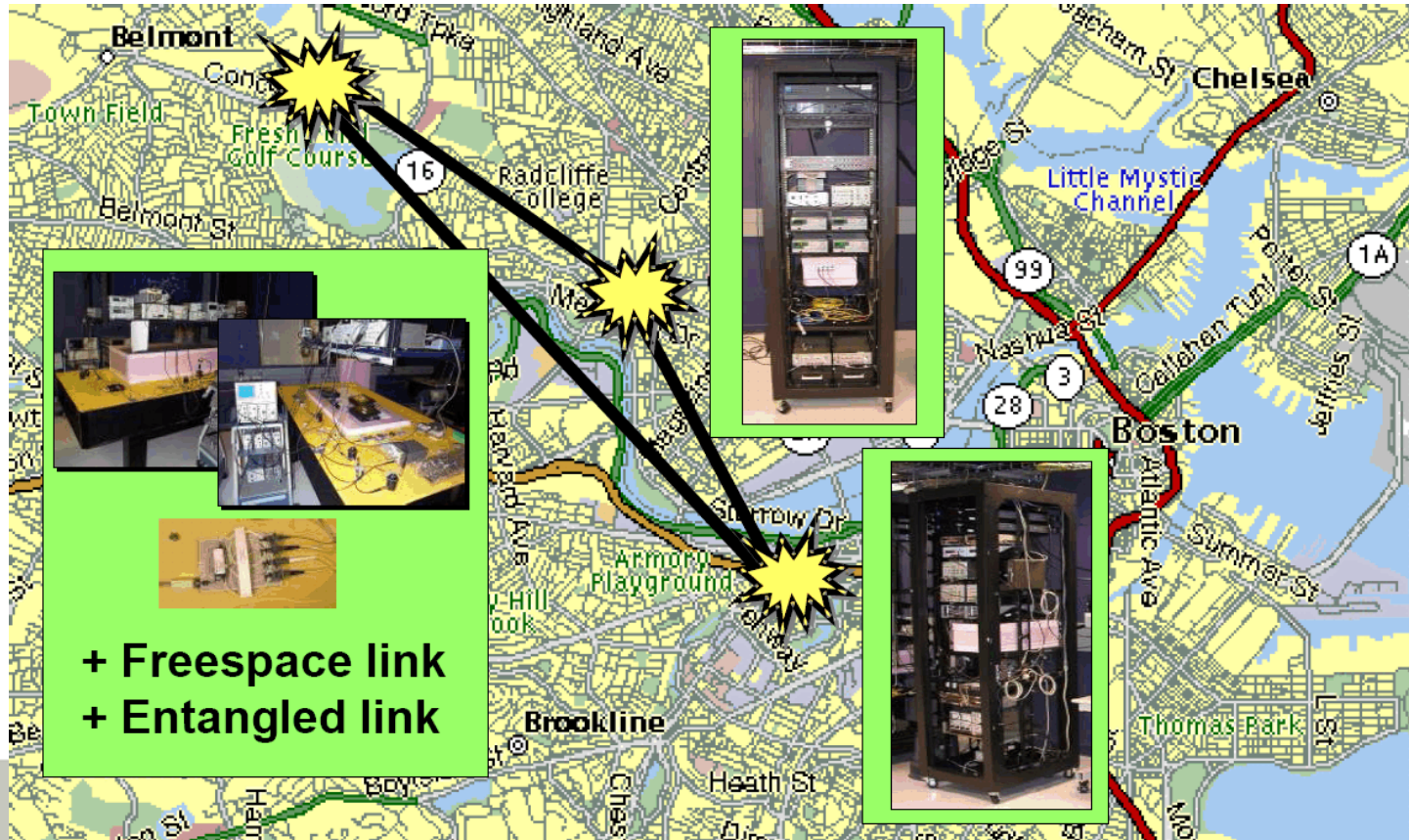
- MagiQ

→Toshiba

- smart-quantum

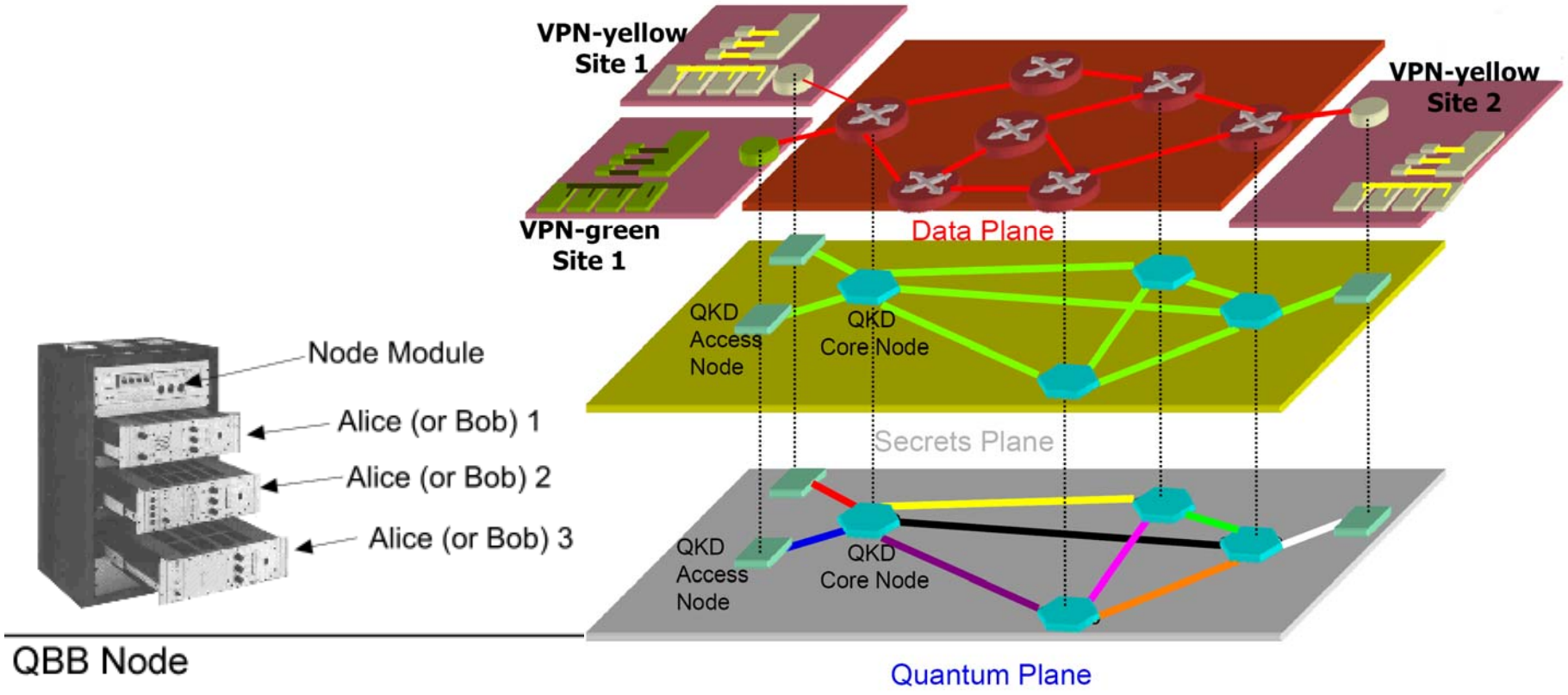
QKD in networks

- trusted repeater schemes
- DARPA network
  - Boston area; BBN, Harvard, Boston University; 2005



SECOQC network

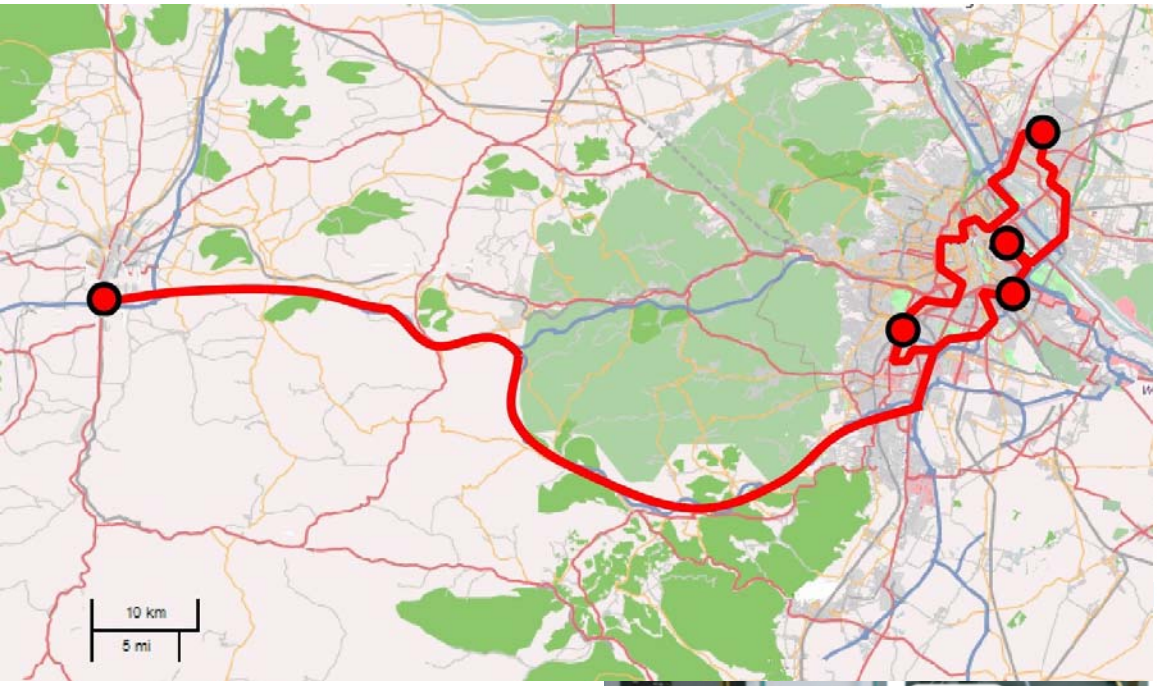
- seamless integration into multi-layer communication structure

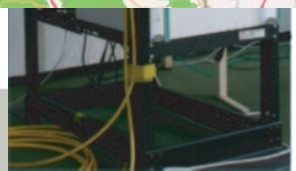


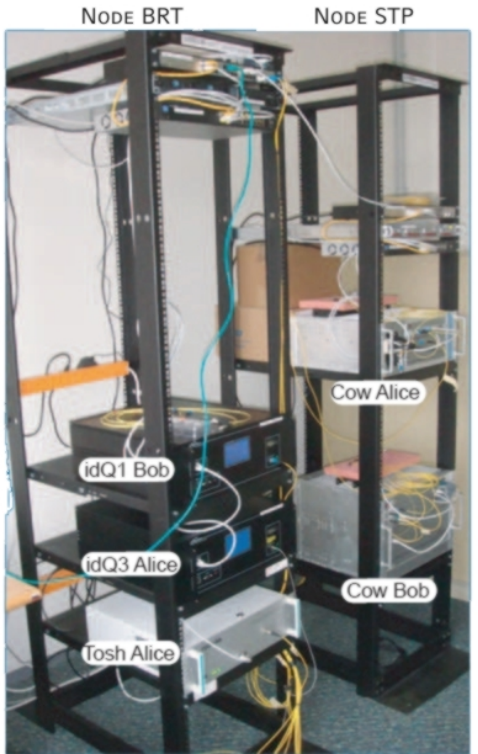
CHIST-ERA
QUANTUM
NETWORK

SECOQC network

- highly integrated systems (19")
- operated in standard telecom infrastructure + daylight free-space link; continuously for 1 month







SECOQC network

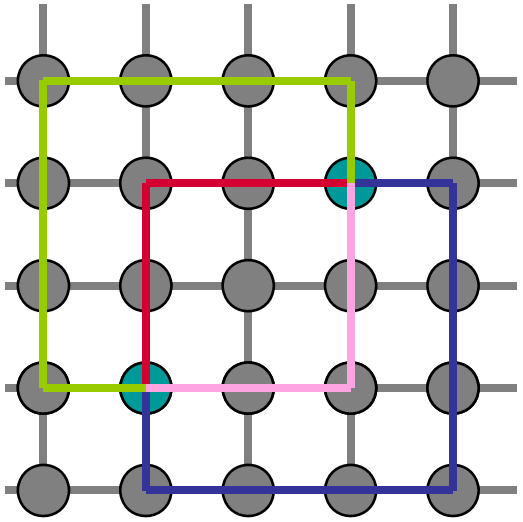
- seamless integration into multi-layer communication structure

– Increase distance and secret rate capacity

–Less initial secret has to be distributed: full covering joint tree is sufficient [*O(n) instead of O(n^2)*] OR
Links running out of authentication key can recover

–Key is a network-wide asset and can be optimally redistributed

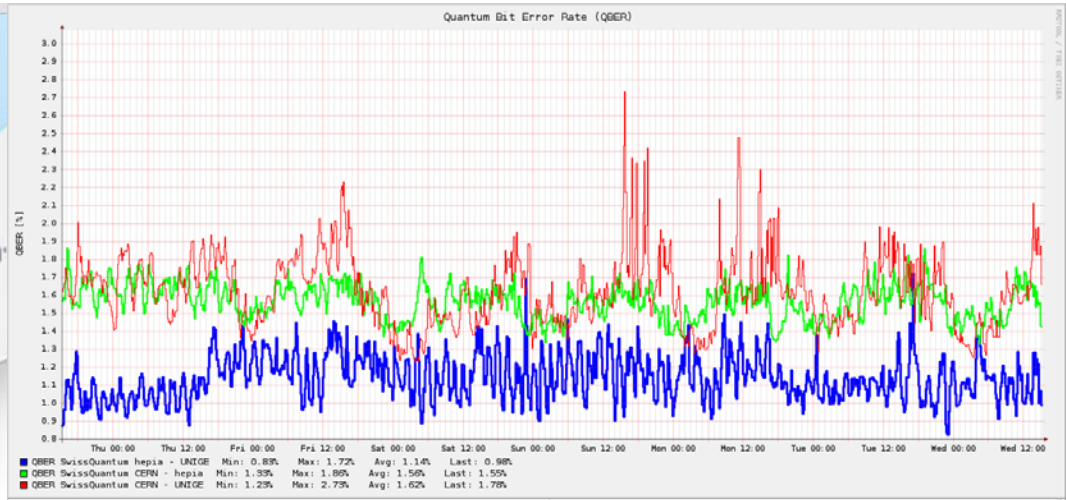
–Combining disjoint paths can ensure **information-theoretic security for a bounded adversary** (secret sharing)

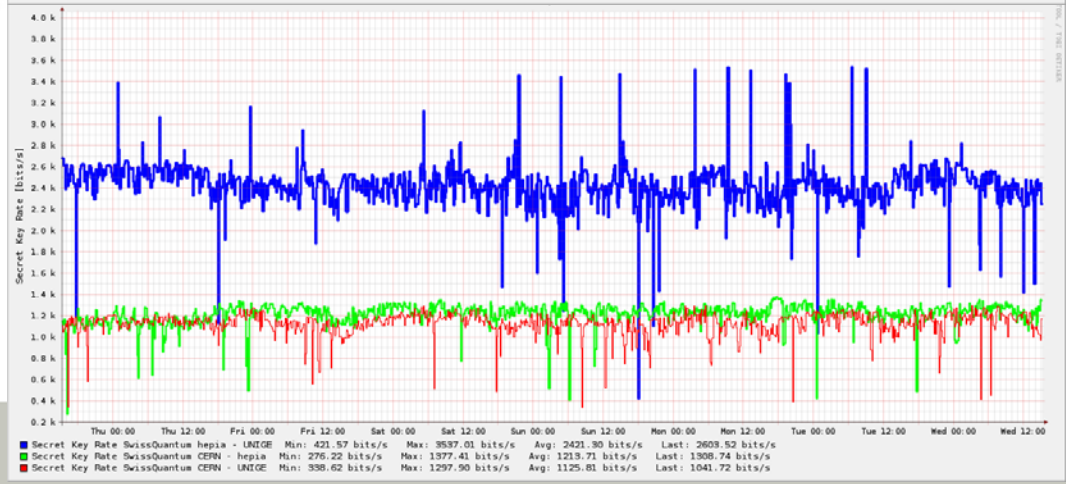


CHIST-ERA
QUANTUM
NETWORK

swiss quantum

- secure links for Geneva election system (since 2007)
- 3 node network, continuous operation since 07/2009





- Univ. Geneva
  Univ. of Appl. Science
  CERN, id Quantique

http://www.swissquantum.com/

current projects

- in Durban, during World-Cup 2010
  University of KwaZulu Natal, id Quantique

- Tokyo QKD Network Oct. 2010
  JGN2plus, NICT, NEC, Mitsubishi Electric, NTT , Toshiba, id Quantique

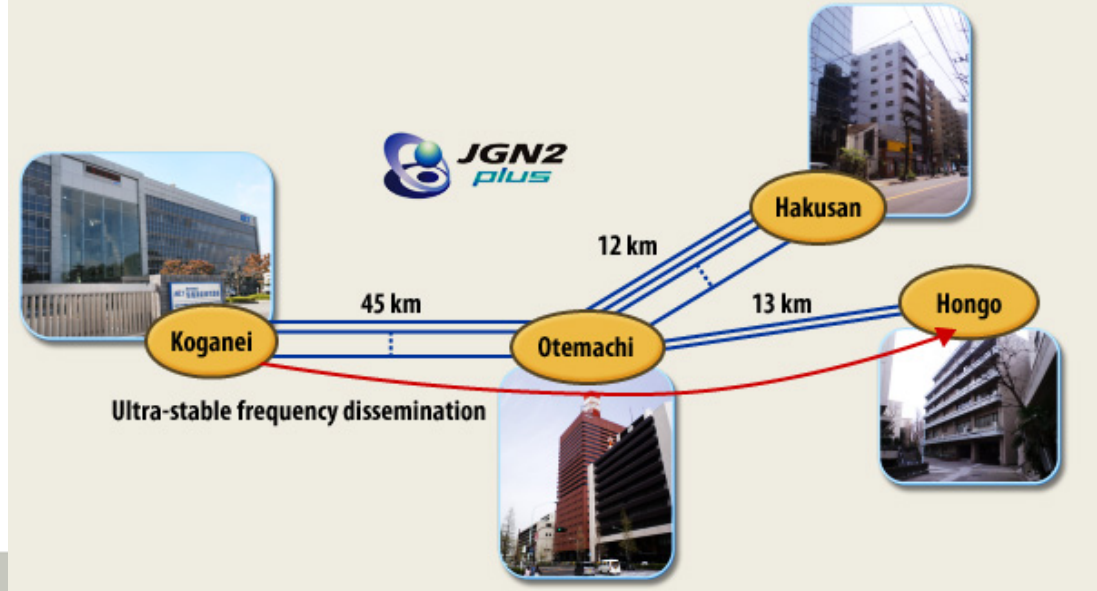
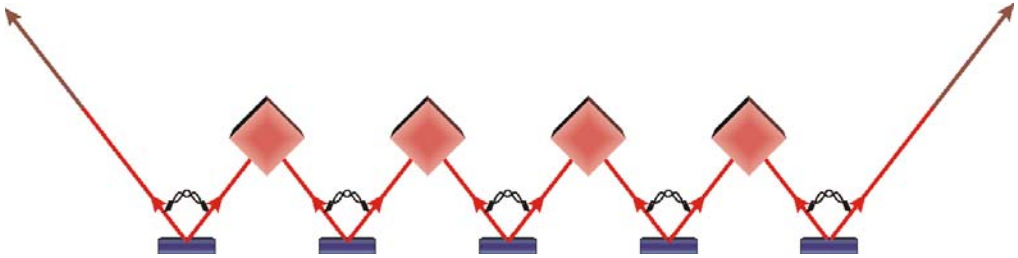


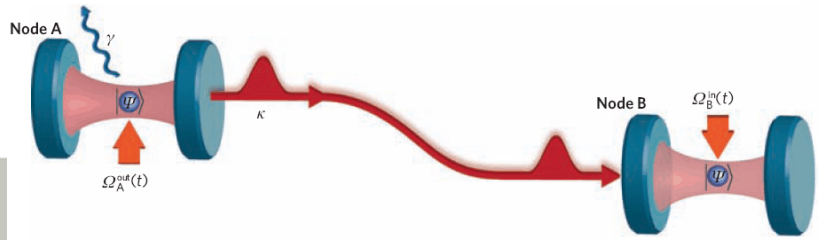
Fig. 1 Network Topology of the Tokyo QKD Network

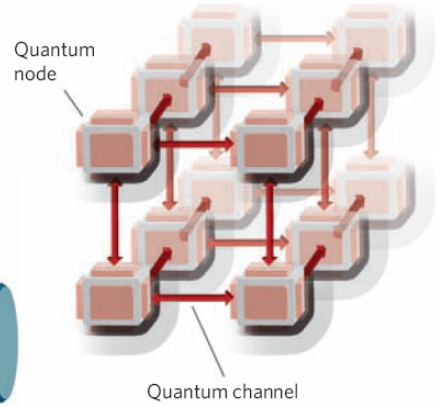
future networks

- long distance communication enabled by quantum repeater



- sources of entangled qubits are conected via repeater nodes performing error correction and storage.
- quantum internet

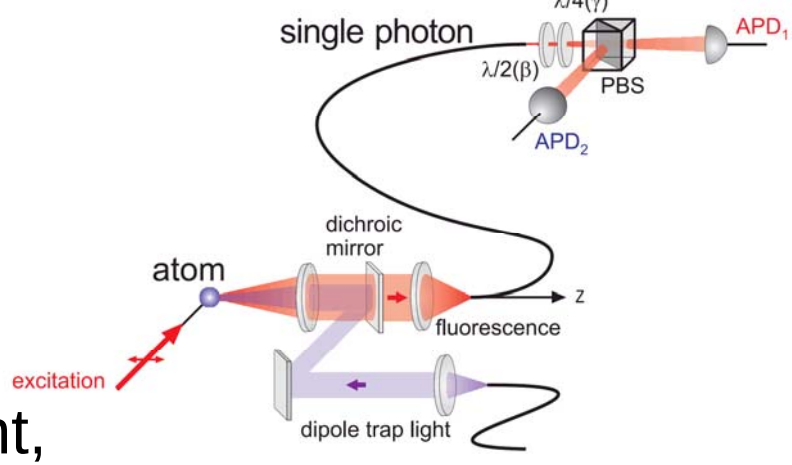


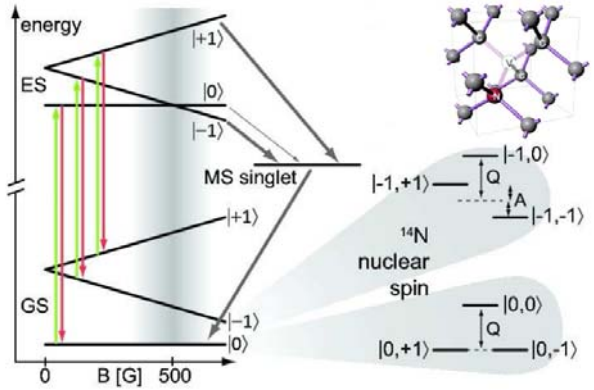


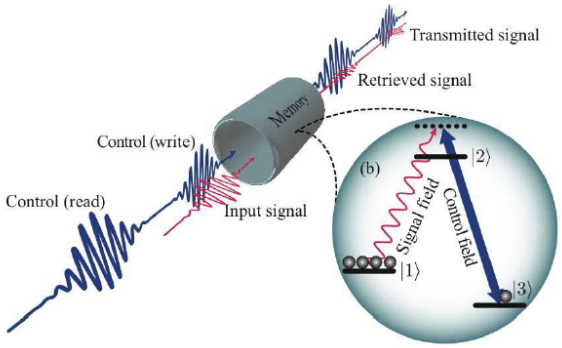
CHIST-ERA QUANTUM NETWORK

components

- sources of entanglement
  - photon pairs, cv-states of light,
    atom-photon states,
    quantum logic elements
- quantum memory
  - atoms, atomic clouds,
    rare earth doped glass fiber,
    solid state e^- and nuclear spin states
- quantum interfaces
  - light-matter interface,
    hybrid systems....
- small scale quantum logics
  - Rydberg coupling, collisions, ion trap, SC-circuits....

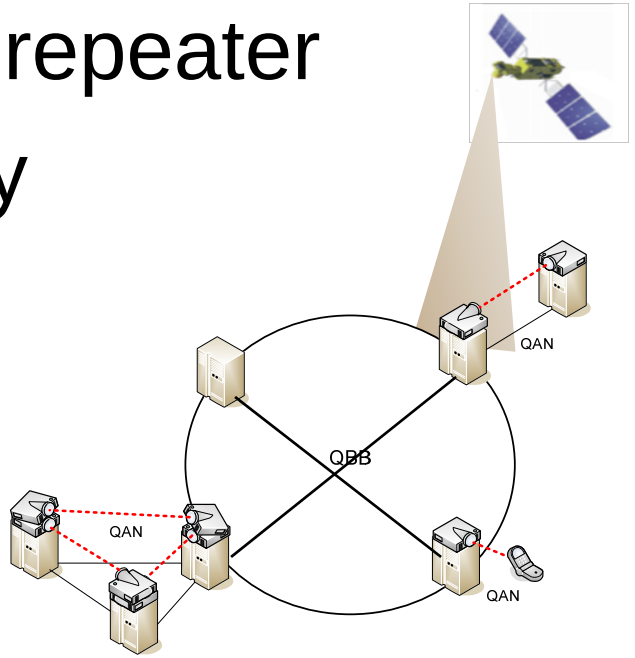






where to go

- high rate, long distance QKD
- components for quantum repeater
- analysis of device security
  (in real world scenarios)
- networking structures



- basis for:
  world wide secure communication
  quantum internet, quantum simulators...