Security assessment and key management in a quantum key distribution network

Xiongfeng Ma
xma@tsinghua.edu.cn
Center for Quantum Information
In collaboration with Hongyi Zhou, Kefan Lyu, Longbo Huang

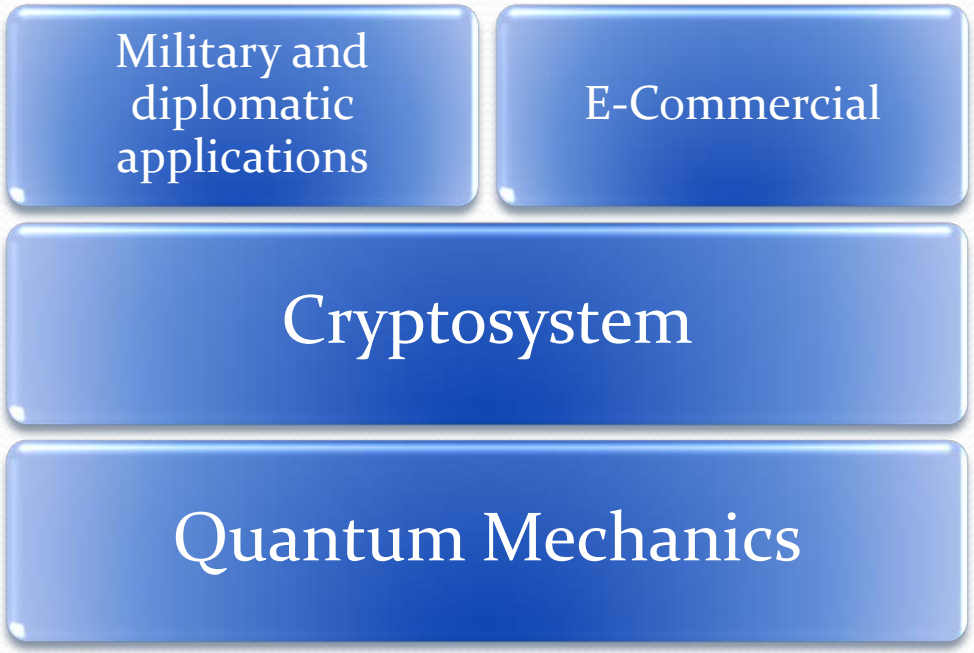
Outline

- Background
  - Quantum key distribution (QKD)
  - Current implementations
  - Field tests of QKD networks
- Security assessment
- Key management

Background

Quantum Cryptography

- Quantum communication
  - Quantum key distribution, teleportation, secret sharing, …
- Quantum cryptography
  - Secure against quantum computing, information-theoretical
- Quantum key distribution cannot replace current communication means
  - Many other tasks, such as authentication and signature, done well with classical means
- In near future, quantum communication cannot replace classical ones



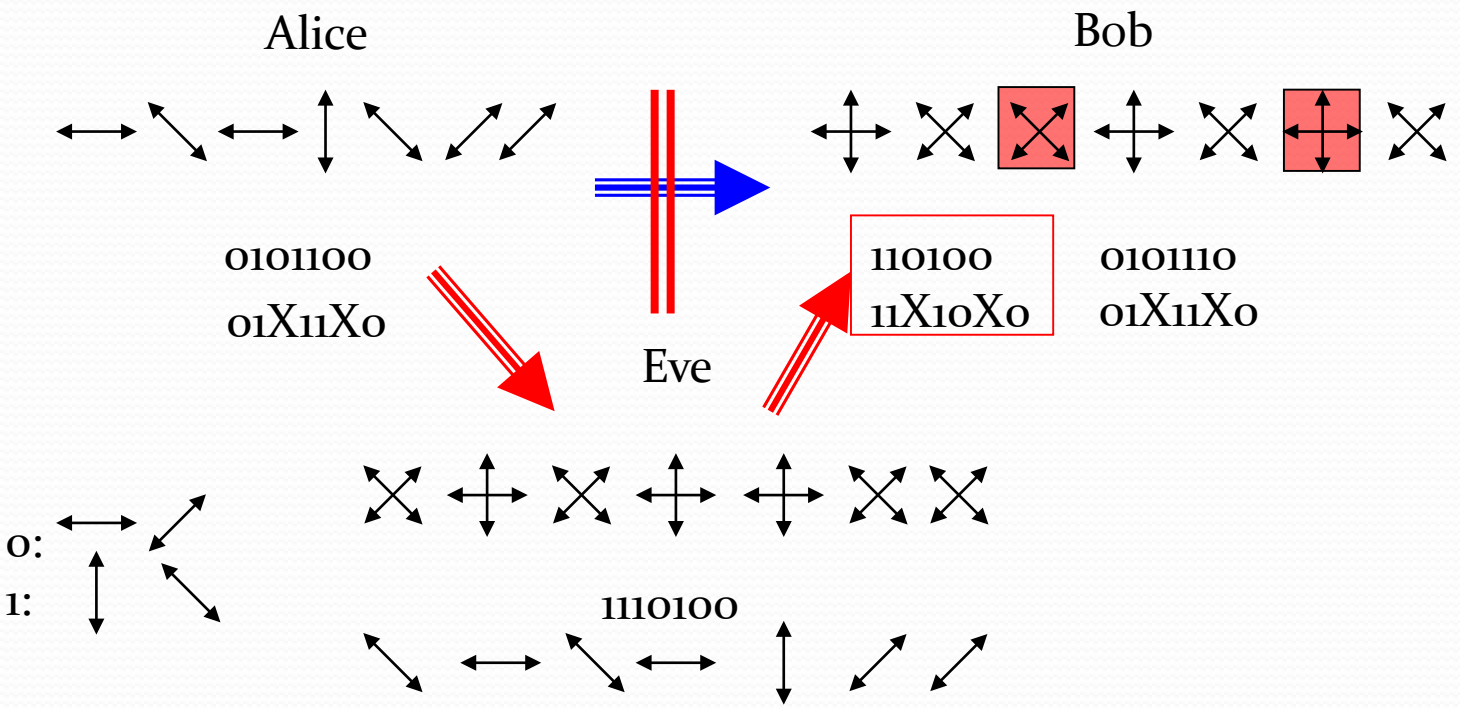
Quantum key distribution (QKD)

- BB84 (Bennett & Brassard 1984)

  Point-to-point protocol

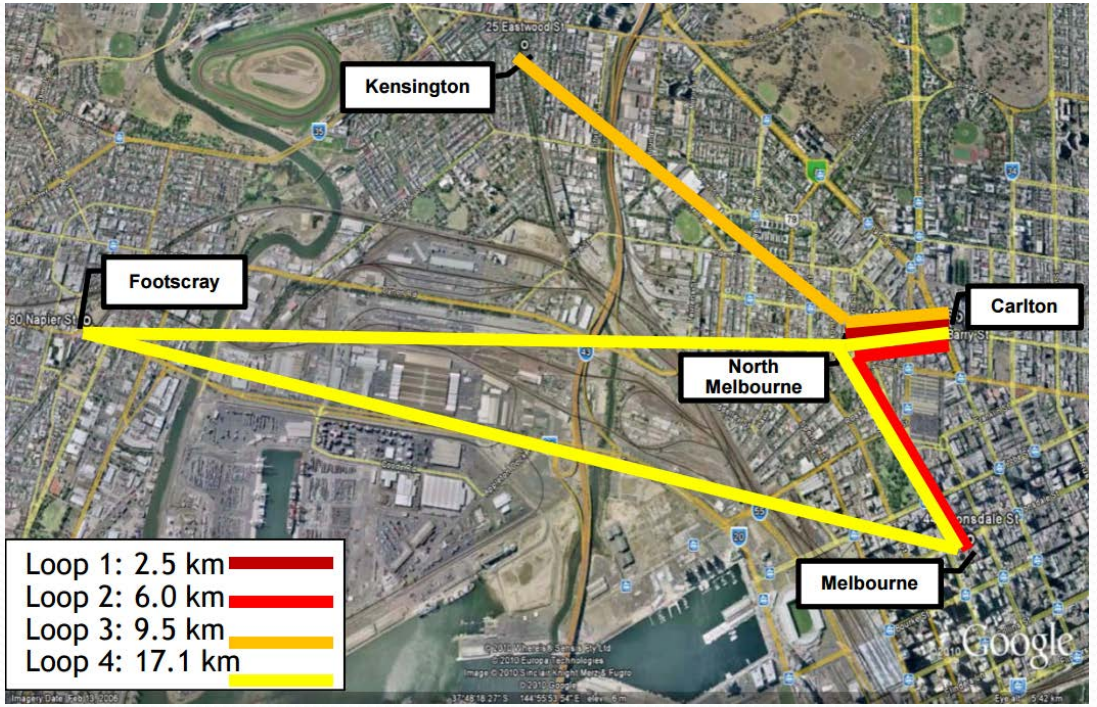
- What if introducing multiple users?

  QKD network



Current implementations

- USA QKD network: DARPA, Battelle, Smartgrid, Since 1004
- Japan: Tokyo network, 2015
- Europe: SECOQC, 2008
- Switzerland: Geneva network, 2009
- South Africa: Durban, 2009
- Australia: Melbourne network, 2010



6

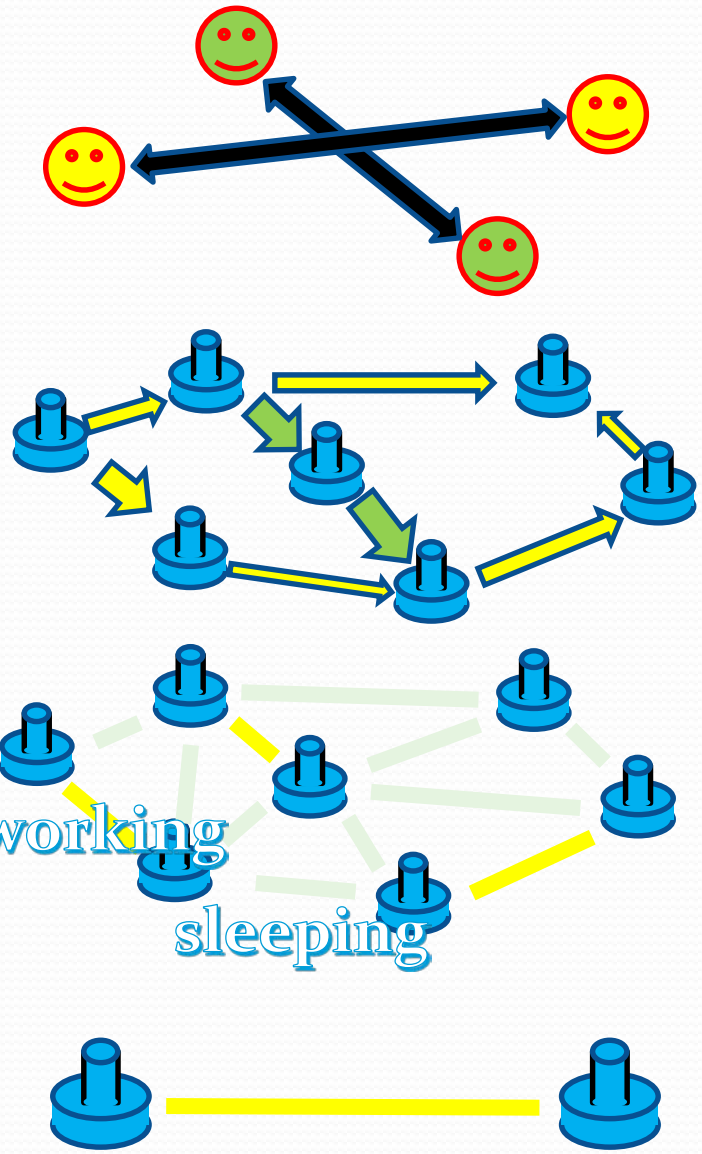
China's Quantum Secure Backbone project

- Total length 2000 km
  - 2013.6-2016.12
  - 32 trustable relay nodes and 31 fiber links
  - GDP 35.6% and population 25.8%
- Metropolitan networks
  - Existing: Hefei, Jinan
  - New: Beijing, Shanghai
- Customers
  - China Industrial & Commercial Bank; Xinhua News Agency; China Banking Regulatory Commission …

Practical Tasks in QKD Network

QKD Network Structure

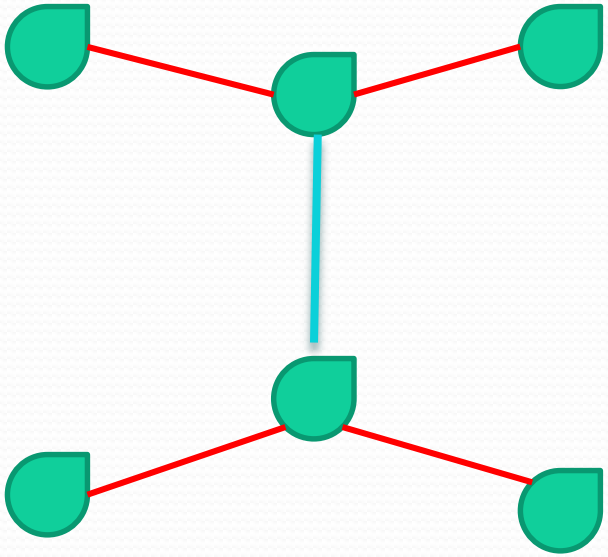
- Host layer
- Key Management Layer
- QKD Network Layer
- QKD Link Layer



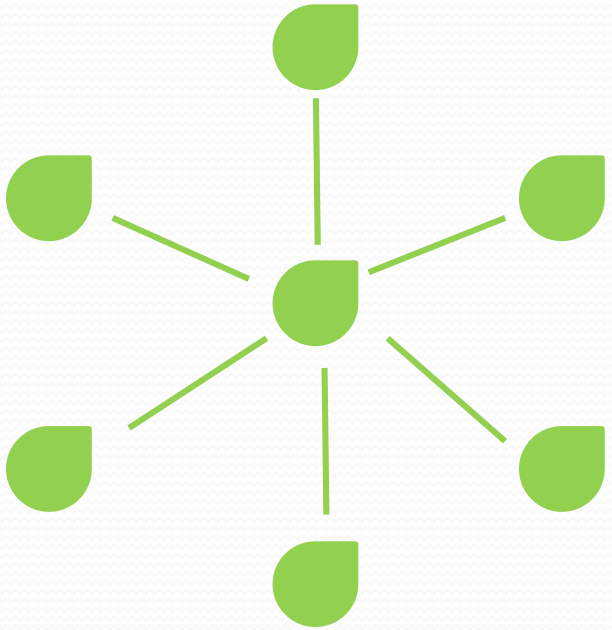
Tysowski et al. Quantum Science and Technology, 2018, 3(2): 024001.

Network topological settings

- Different scenarios employ different settings



Backbone networks

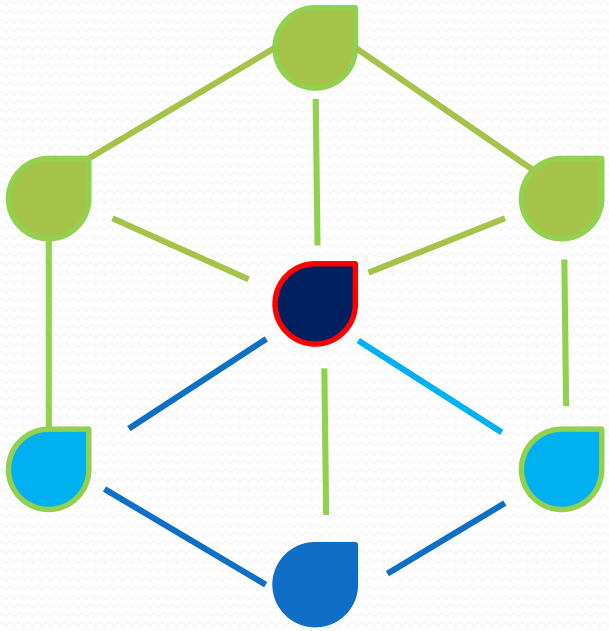


Star-type networks

Alleaume, Roueff, Diamanti, Lutkenhaus, New J. Phys. 11 075002 (2009)

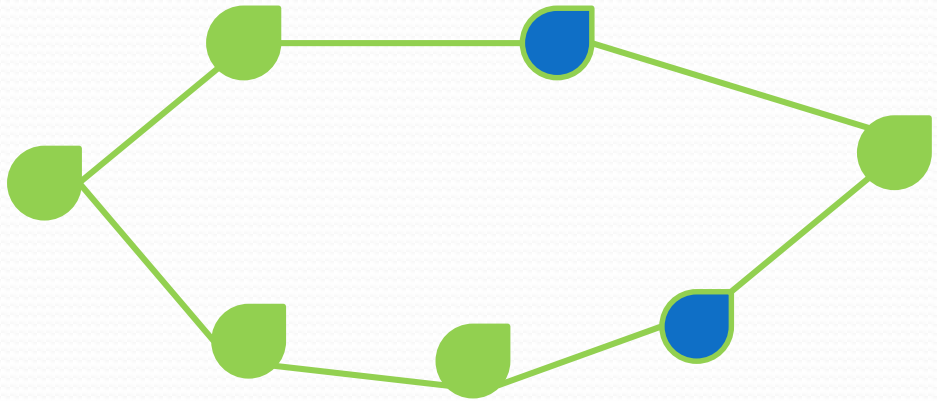
Practical Tasks

- Network issues
  - Latency, reliability, scalability, cost
  - Security
  - Key consumption
- Two simple examples
  - In trusted nodes scenario, some of the nodes may be compromised, where the keys are insecure
  - Balance key distribution and consumption
  - Data routing and scheduling



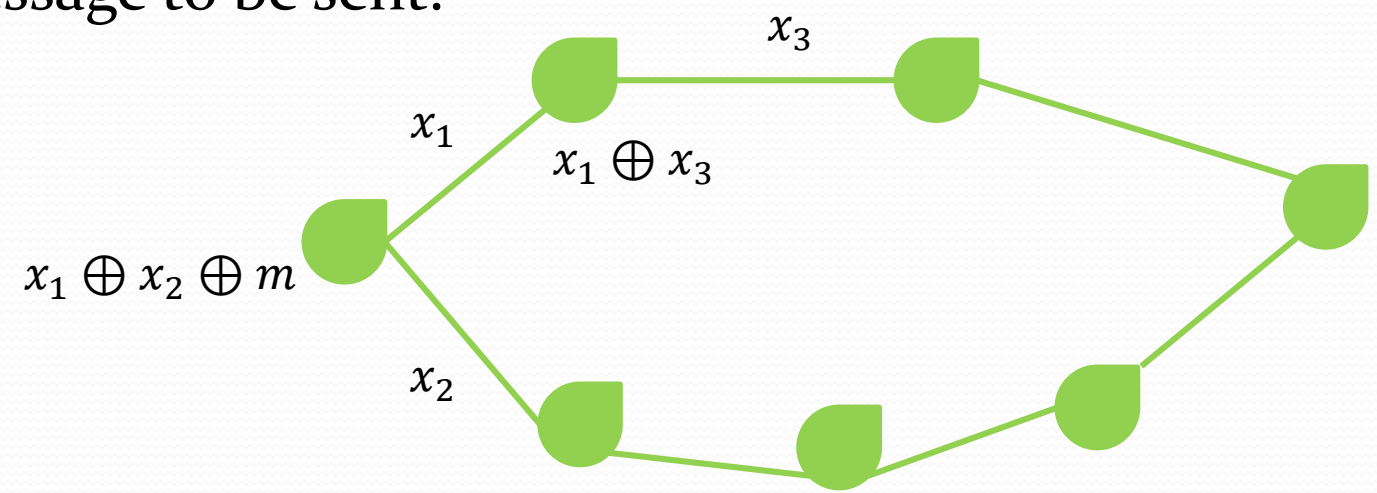
Task I: compromised nodes

- Designing the classical communication scheme in highest security level with sufficient keys
- Strongest attack
  - Eve may eavesdrop arbitrary nodes and obtain their keys
  - The strongest attack is a cut between Alice and Bob in the graph
  - Eve's strategy: minimum cut problem in graph theory



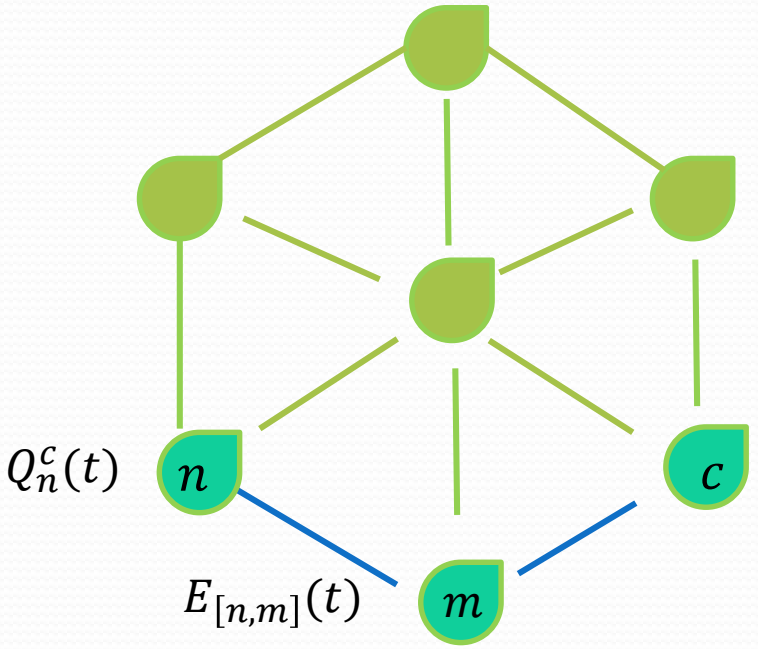
Communication in highest security

- Communication scheme in highest security level can only be hacked by the strongest attack
  - Each node (except Alice and Bob) broadcast the exclusive-or result of all keys from connected channels.
  - Alice broadcasts the exclusive-or result of all keys from connected channels and the message to be sent.



Task II: Key management and data scheduling

- QKD network: graph description $G = \{N, L\}$
  - User: node
  - Distributed key: edge
- Share key => transfer message along a single link
- QKD network state at time t
  - For nodes $n \in N$, how much data to transfer to $c \in N$, $Q_n^c(t)$?
  - For channels $[n, m] \in L$, how much key stored, $E_{[n,m]}(t)$?



Utility optimization

- Data transmission from n to c: $R_n^c(t)$
- Utility: the value of the transmitted data: $U_n^c\left(R_n^c(t)\right)$
  - Concave with $R_n^c(t)$
  - Defined according to practical cases: e.g. $\log_2 R_n^c(t)$
- Utility optimization: Optimize data scheduling $R_n^c(t)$ and key management $P_{[n,m]}(t)$ to maximize the total utility $\sum_{n,c} U_n^c(R_n^c(t))$,

$$\max_{R_n^c(t),P_{[n,m]}(t)} \sum_{\substack{n,c \\ \tau}} U_n^c(r_n^c)$$

$$r_n^c = \lim_{t\to\infty} \frac{1}{t} \sum_{\tau=0} R_n^c(\tau)\,,$$

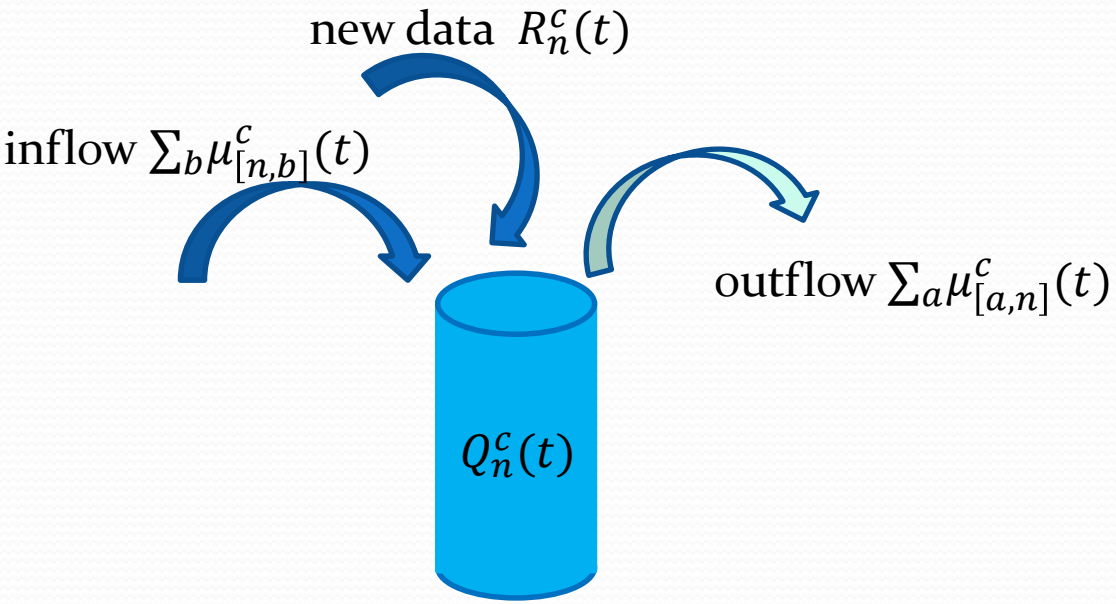
given the following dynamics and constraints.

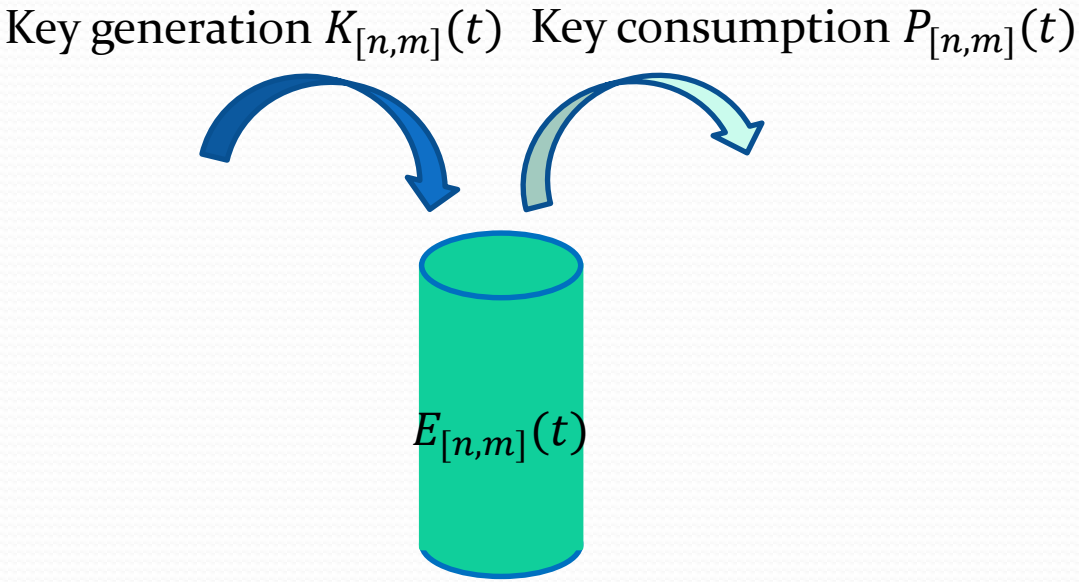
Dynamics

- Dynamic queue: how the data (key) size in t+1 evolves from t

$$Q_n^c(t+1) = Q_n^c(t) + \sum_b \mu_{[n,b]}^c(t) - \sum_a \mu_{[a,n]}^c(t) + R_n^c(t)$$

$$E_{[n,m]}(t+1) = E_{[n,m]}(t) + K_{[n,m]}(t) - P_{n,m}(t)$$





Constraints

- Stability constraint: a well-defined problem in field of network -- residual data is convergent with time

$$\bar{Q} = \limsup_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{n,c} Q_n^c(\tau) < \infty$$

Solution: Lyapunov Function and drift,

$$L(t) = \frac{1}{2} \sum_{n,c} [Q_n^c(t)]^2 + \frac{1}{2} \sum_{[n,m]} [E_{[n,m]}(t) - \theta_{[n,m]}]^2$$

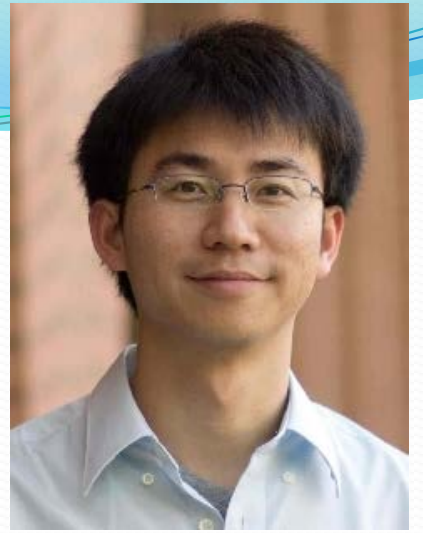
$$\Delta(t) = L(t+1) - L(t)$$

- Key availability constraint: consumption is less than storage

$$P_{[n,m]}(t) \le E_{[n,m]}(t)$$

Tanaka K, Hori T, Wang H O. A multiple Lyapunov function approach to stabilization of fuzzy control systems[J]. IEEE Transactions on Fuzzy Systems, 2003, 11(4):582-589.

Optimization algorithm



- Target function

$$\Delta(t) - \sum_{n,c} U_n^c\left(R_n^c(t)\right) \le B + C + D + E$$

- Main idea:
  - Minimize target function
  - Obtain optimal data scheduling $R_n^c(t)$ and key management $P_{[n,m]}(t)$
  - Decouple $R_n^c(t)$ and $P_{[n,m]}(t)$

B =constant

$$C = \sum_{[n,m]} (E_{[n,m]}(t) - \theta_{[n,m]}) K_{[n,m]}(t)$$

$$D = -\sum_{n,c} \left[V U_n^c\left(R_n^c(t)\right) - Q_n^c(t) R_n^c(t)\right]$$

$$E = -\sum_{[n,m]} \{\mu_{[n,m}(t)[Q_n^c(t) - Q_b^c(t)] + (E_{[n,m]}(t) - \theta_{[n,m]}) P_{[n,m]}(t)\}$$

Huang L, Neely M J. Utility optimal scheduling in energy-harvesting networks[J]. IEEE/ACM Transactions on Networking (TON), 2013, 21(4): 1117-1130.

Optimization algorithm

- **Input of the algorithm.** Initialize $\theta_{[n,m]}$. At every time slot t, observe $Q_n^c(t), E_{[n,m]}(t)$.
- **Key generation.** Minimize C. Obtain an optimized key generation strategy $K_{[n,m]}(t)$.
- **Data transmission.** Minimize D. Obtain an optimized data scheduling strategy $R_n^c(t)$.
- **Key management.** Minimize E. Obtain an optimized key management strategy $P_{[n,m]}(t)$.
- **Queue update.** Use the dynamics of data queue and key storage queue. Obtain $Q_n^c(t+1), E_{[n,m]}(t+1)$.

Conclusion and Outlook

- More network issues should be taken into account
- Current graph theory techniques can be employed in QKD network
- Current network techniques can be employed in QKD network
- Generalized to quantum network
  - Entanglement layer
  - Quantum computing

Thank you!

- International graduate student fellowships are available!
- Welcome to join and visit!