Quantum Digital Signature

Group “Hanko”

Who we are

- Shota Nagayama
- Hirotaka Nakajima
- Shinnosuke Ozawa

Goal

- Design quantum digital signature “protocol” rather than “algorithm”

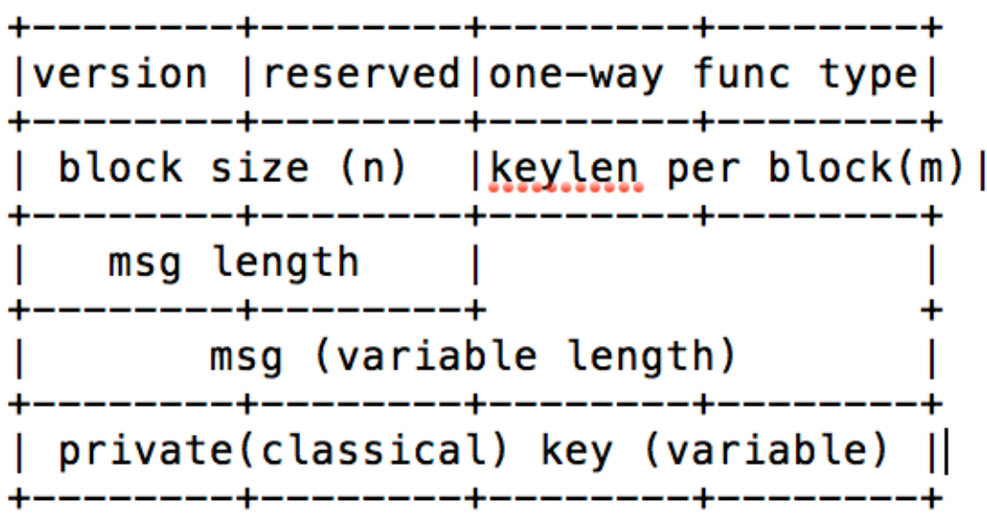
- Implement the protocol

Which QDS algorithms?

- Gottesman-Chuang (2-party)
  - arXiv:quant-ph/0105032
- “Secure quantum signatures using insecure quantum channels” (3-party)
  - Phys. Rev. A 93, 032325 (2016)

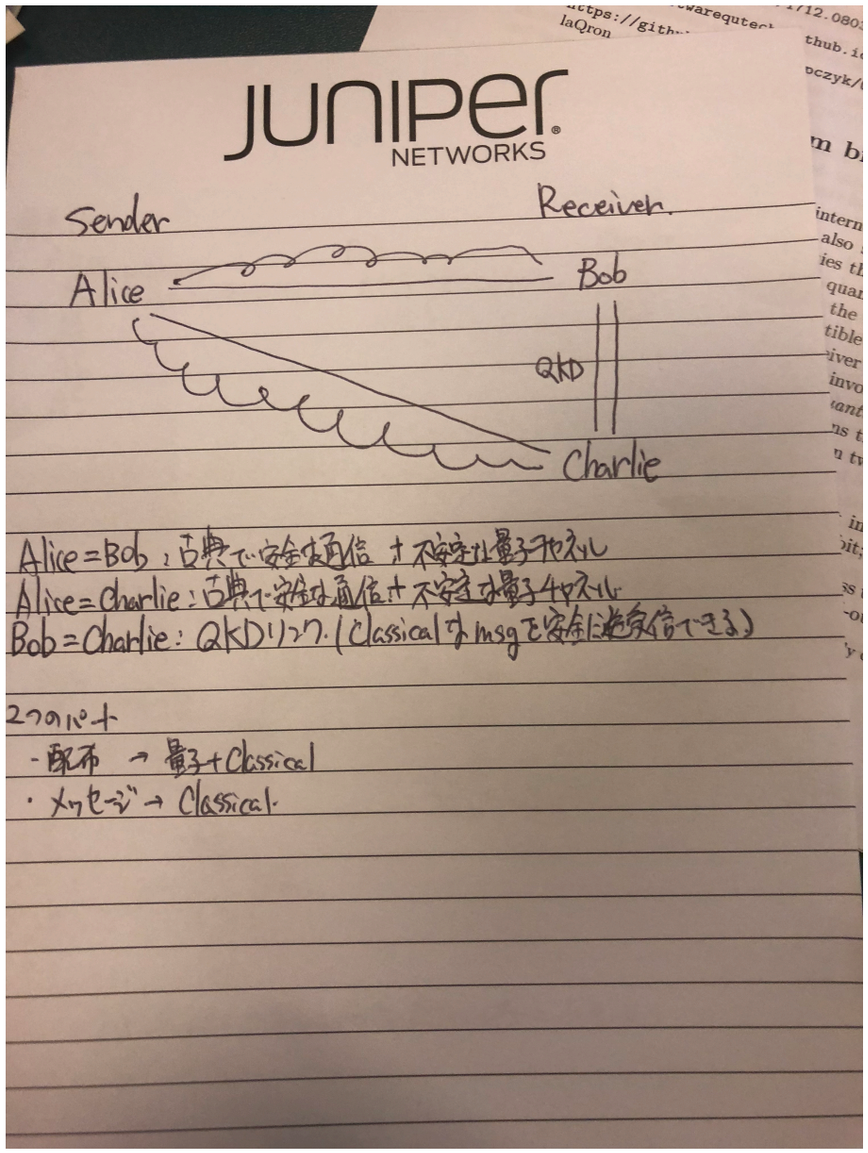
2-party protocol Results

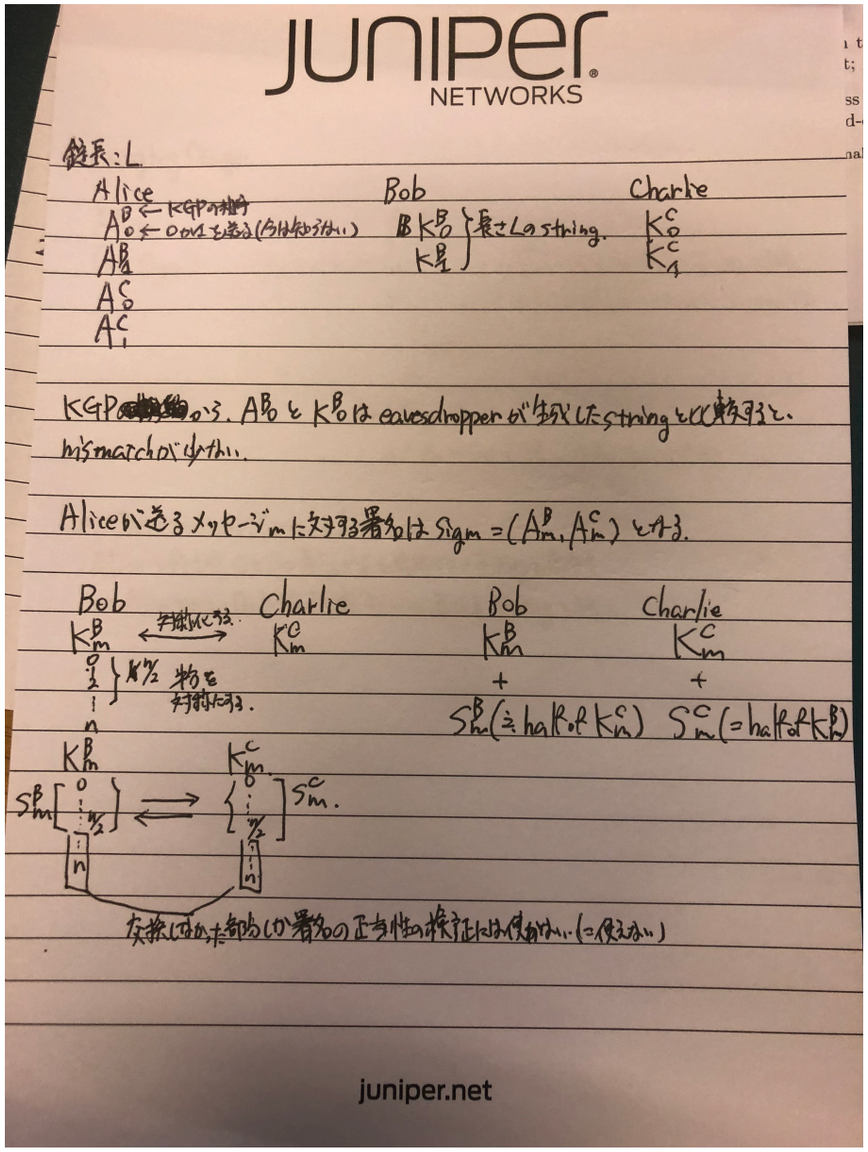
- https://github.com/ngym/quantum_digital_signature
- achievement
  - implementation
    - variable key length, variable msg length,
      simple stabilizer states quantum one-way function
  - protocol format
    - draft for the 2-party protocol
- follow-up
  - implementation of the 2-party protocol
  - other quantum one-way functions



3-party protocol
Results

- achievement
  - prototype of the implementation





Lesson

- QDS is not space-efficient

- “Fragmented” transfer of quantum signature would work for early stage of the Quantum Internet