Defense Energy Seminar Series

Quantum Security for Microgrids

Peng Zhang

Stony Brook University

9/10/2024

Stony Brook Power Lab

Our Mission

Transform today's power grids into tomorrow's **autonomic networks** and **flexible services** towards self-configuration, self-healing, self-optimization, and self-protection against grid changes, renewable power injections, faults, disastrous events and cyber-attacks.

Strategic Directions

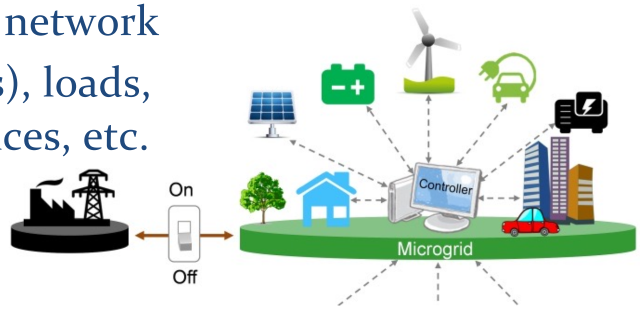
- **AI-Enabled Resilient Power Grids**
- **Quantum Engineered Resilient Grids**
- **Microgrids & Networked Microgrids**
- **Software Defined, Programmable Smart Grid**
- **Grid Resiliency, Cybersecurity, and Stability**
- **Grid Forming and Renewable Energy Integration**

Stony Brook University

Background

NAVAL POSTGRADUATE SCHOOL

- Microgrid
  - Localized autonomous distribution network
  - Distributed energy resources (DERs), loads, storage, controllers, protection devices, etc.



- Networked Microgrids (NMs)
  - Enhanced electric system resilience
  - Reduced economic and emission costs
  - Facilitated integration and coordination of DERs

- Secure data transmission
  - Within a microgrid
  - Among different microgrids

- Existing microgrid communication:
  - Cryptographic systems
  - Relies on <u>classical public key systems</u>
  - <u>Challenges:</u> Vulnerable to attacks from quantum computers

- Diffie-Hellman key exchange (DH)
- Rivest-Shamir-Adleman (RSA)

Mathematical assumptions:
- Discrete logarithm problem
- Factoring problem

FAR BEYOND

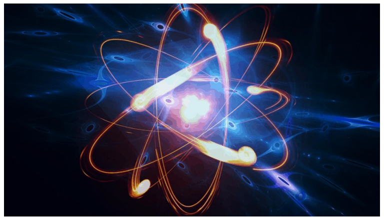
Outline

Quantum Bit

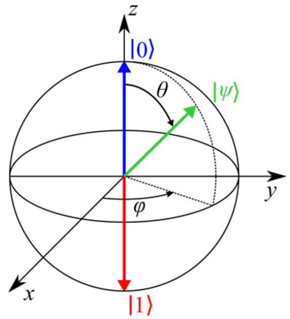
- Classical binary bit
  - ❑ Either 0 or 1
- Quantum bit, or "qubit"
  - ❑ A two-state quantum-mechanical system
  - ❑ Coherent superposition of both states simultaneously

Binary bit

vs.



Qubit

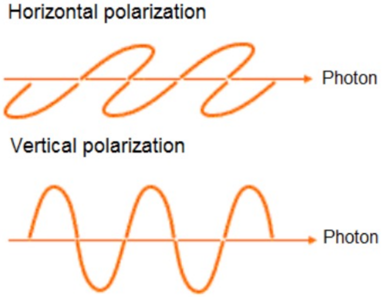


The superposition state is:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $|\alpha|^2 + |\beta|^2 = 1$

- Implementation of qubits
  - ❑ Polarization of a single photon
    - ➢ Horizontal polarization (Z basis)
    - ➢ Diagonal polarization (X basis)

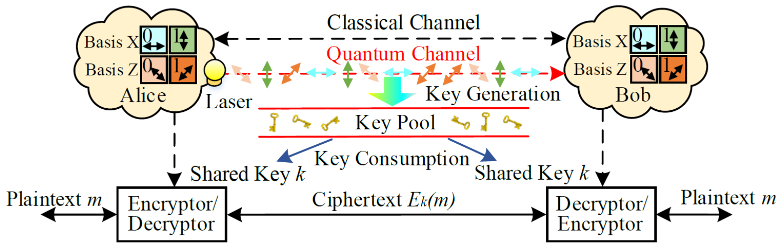


Sender and receiver:
- Same basis:
  - ✓ Same result
- Different bases:
  - ✓ Different results

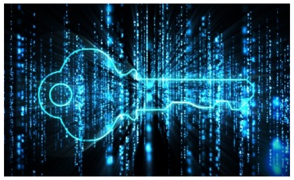
FAR BEYOND

Quantum Key Distribution

- The general setting of a QKD system
  - Quantum channel: Transmit quantum states
  - Classical channel: Post processing, encryption and authentication



The general setting of a QKD system.

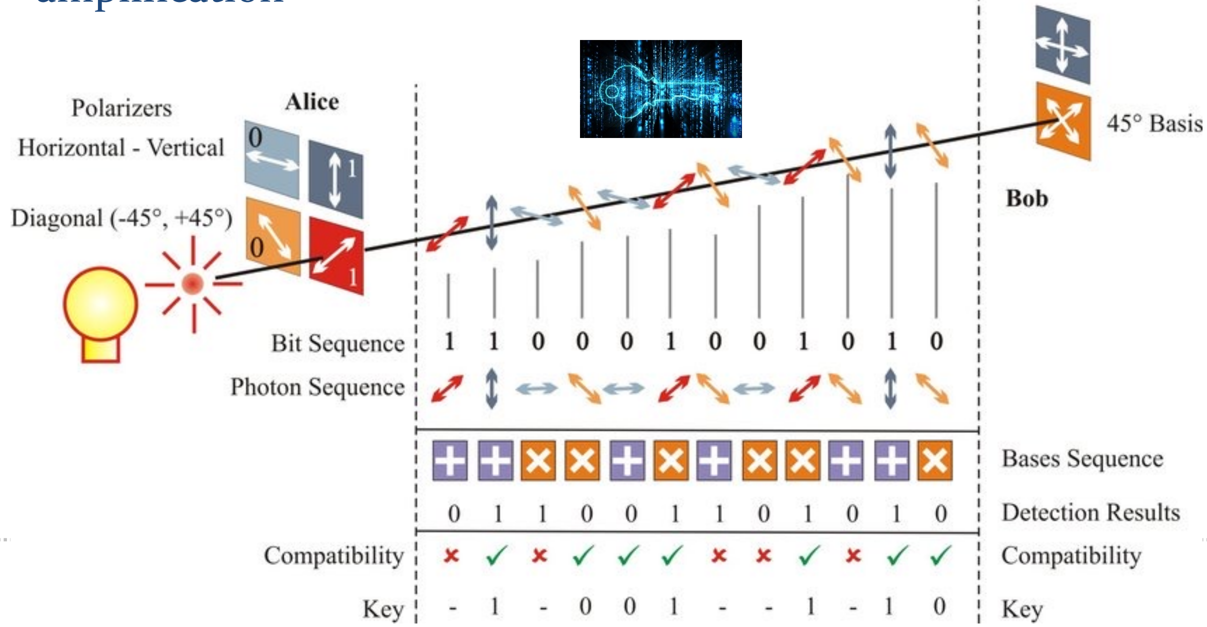


- The unique property
  - Measuring an unknown qubit will change that state
  - The two parties can detect the occurrence of an eavesdropper who is trying to gain knowledge of the keys

The generated keys will be theoretically secure.

Decoy-State BB84 QKD Protocol

- QKD protocols
  - BB84, decoy-state, six-state, Ekert91, BBM92, etc.
- Decoy-state BB84 QKD protocol
  - Preparation, measurement, basis reconciliation, raw key generation, error estimation, error correction, error verification, and privacy amplification



FAR BEYOND

Stony Brook University

Outline

NAVAL POSTGRADUATE SCHOOL

- Introduction
- Quantum Communication
- Quantum-Secure Microgrid
  - Literature Review
  - QSM Architecture
  - QSM Testing Environment
  - Experimental Results
- Quantum-Secure Networked Microgrids
- Programmable Quantum Networked Microgrids
- Conclusion and Future Work

1. Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure microgrid," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1250-1263, 2021.
2. Z. Tang, P. Zhang, and W. O. Krawec, "A quantum leap in microgrids security: The prospects of quantum-secure microgrids," *IEEE Electrification Magazine*, vol. 9, no. 1, pp. 66-73, 2021.

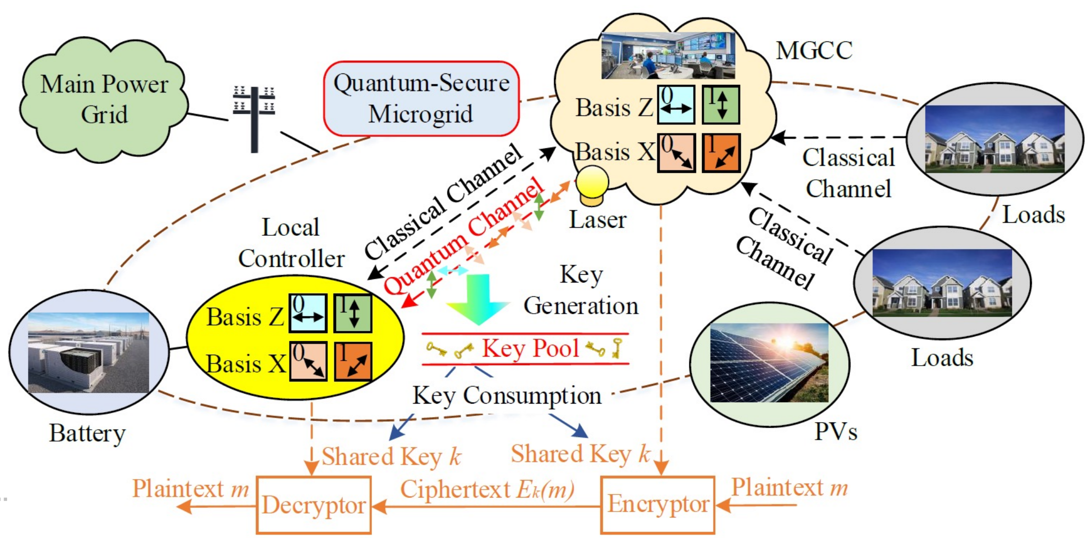
QSM Architecture (1/2)

Microgrid control center (MGCC):

- Collect data from different loads through classical communication
- Send control signals to local controller(s) through quantum communication
- The quantum keys are stored in key pool(s)

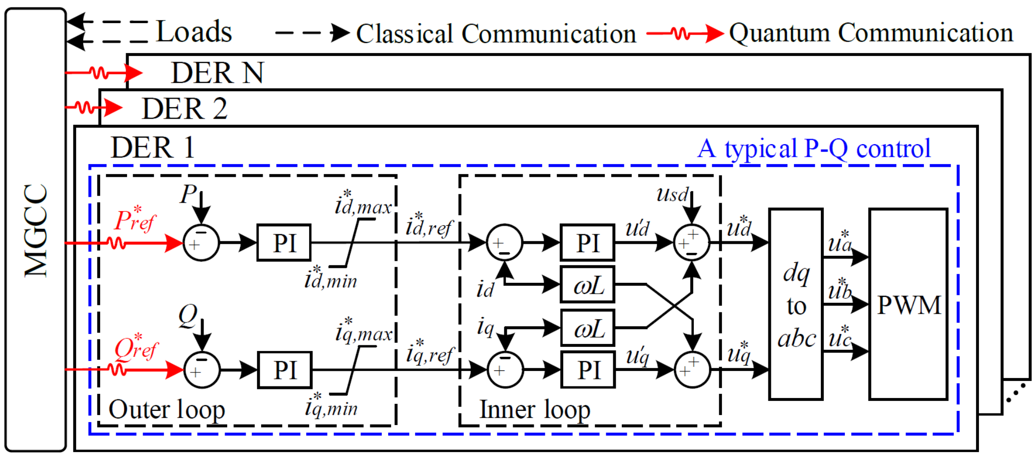
Local controller(s):

- Battery: P-Q control
- Receive control signals from MGCC



QKD-enabled quantum-secure microgrid architecture.

QSM Architecture (2/2)



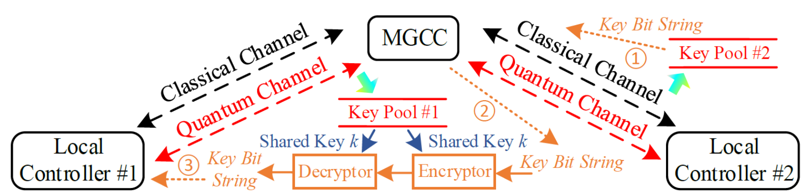
Scheme of the quantum-secure microgrid control.

Quantum-secure microgrid control:

- P-Q control
- Quantum: Control signals
  - Active and reactive power references
  - From MGCC to controller
- Classical: Loads
  - From loads to MGCC

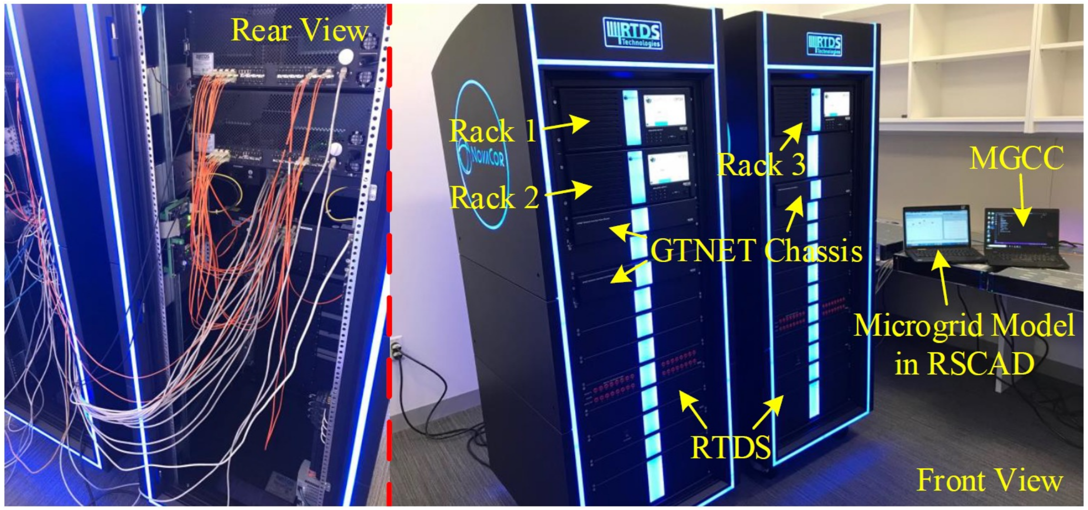
The key pool sharing (KPS) strategy:

- Multiple quantum channels
- Separate key pools
- Key pools can share keys with each other



An example of the KPS strategy.

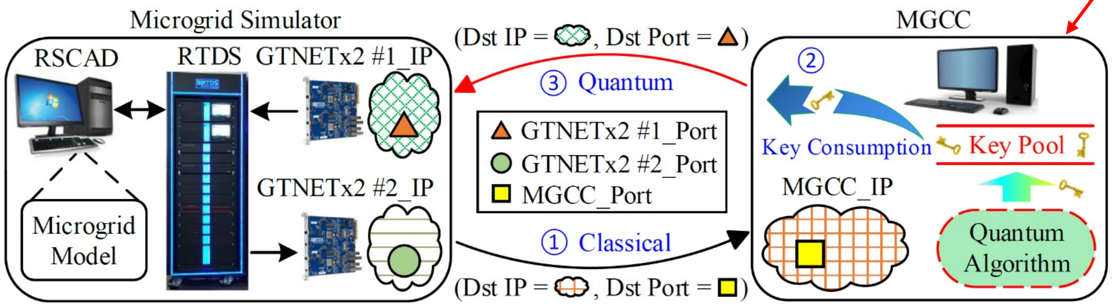
QSM Testing Environment (1/2)



Experimental setup in RTDS.

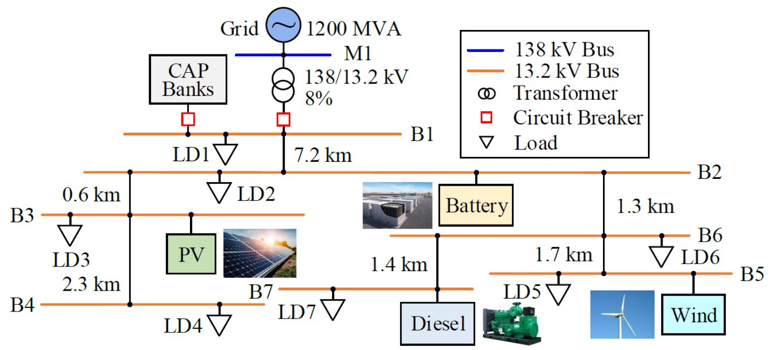
High-level design:

A remote server



High-level design of the testbed.

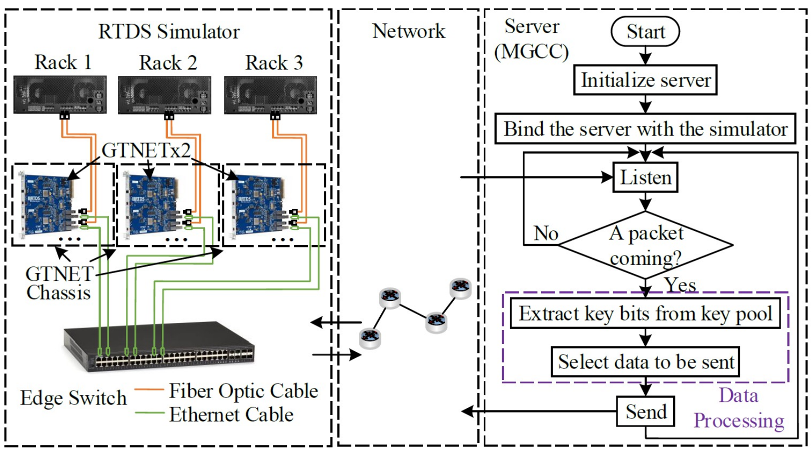
QSM Testing Environment (2/2)



One-line diagram of the microgrid model.

Microgrid modeling:

- A 5.5 MW diesel generator
- A 1.74 MW PV system
- A 2 MW doubly-fed induction generator wind turbine system
- A lithium-ion battery storage
- ……



Network connection of the main components in the RTDS and a flow chart of the algorithm running in the MGCC.

QKD-based microgrid communication network:

- MGCC: listening and sending
- Once a packet is received by MGCC, a certain number of key bits are consumed in the key pool.
- Key bits are generated continuously in the key pool.

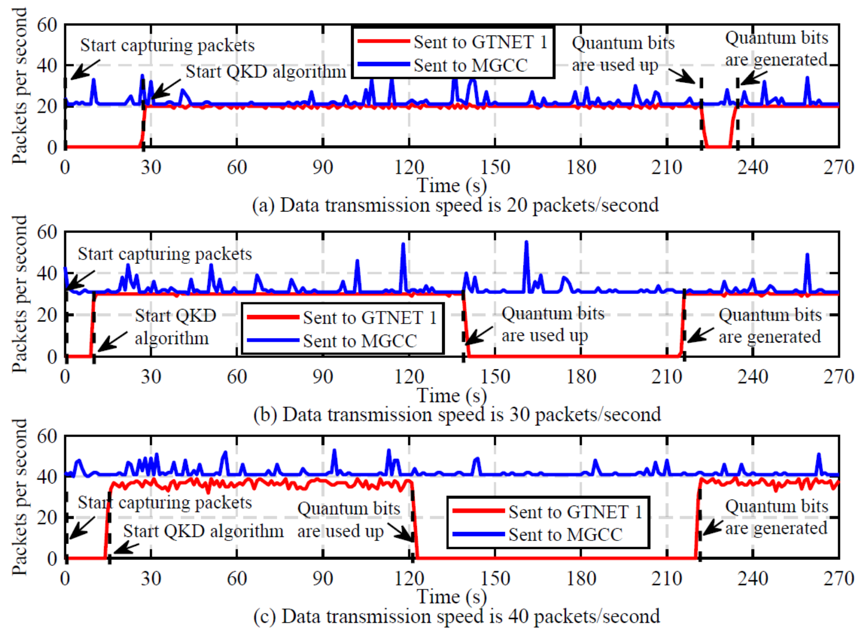
Stony Brook University

Experimental Results (1/7)

NAVAL POSTGRADUATE SCHOOL

- A speed larger than the key generation speed can result in the exhaustion of key bits in a key pool, eventually causing the failure of data communication.
- Wireshark: monitor the traffic
  - The data transmission speed has a large impact on the QKD-based microgrid.
  - The larger the data transmission speed, the sooner the quantum bits will be consumed.

Case 1: Effect of data transmission speed



Traffic monitoring under different data transmission speeds.

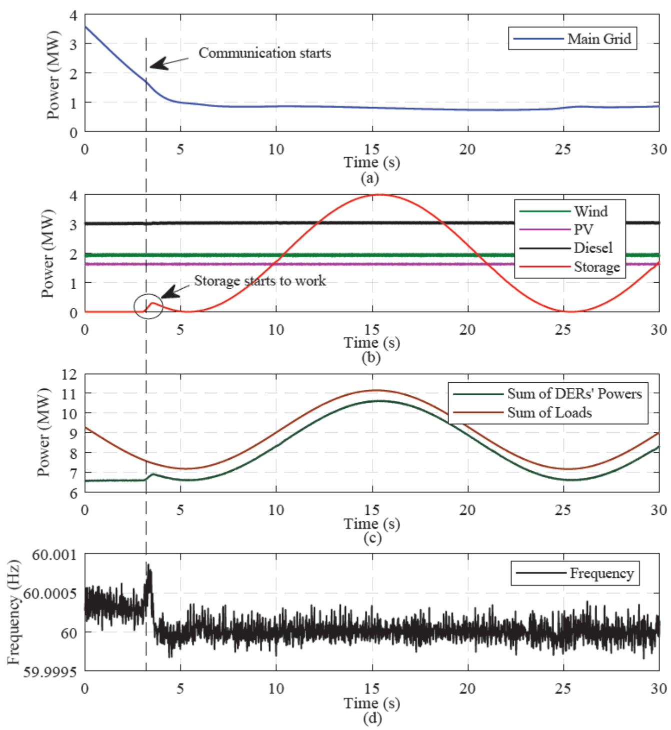
FAR BEYOND

Experimental Results (2/7)

Stony Brook University

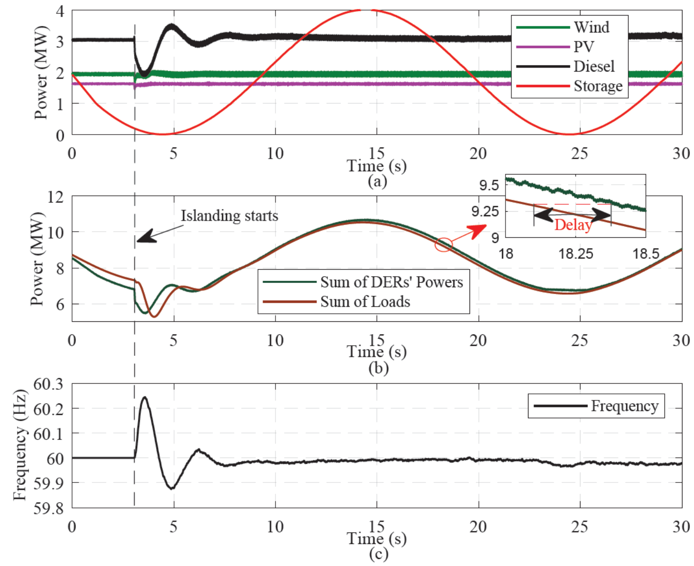
NAVAL POSTGRADUATE SCHOOL

Case 2: Baseline test



The microgrid performance before and after the communication starts to work during grid-connected mode.

The effectiveness of the communication



The microgrid performance during islanding mode.

- The storage responds to the change of loads due to the communication.
- The balance of the total power generation and the sum of the loads can be maintained.

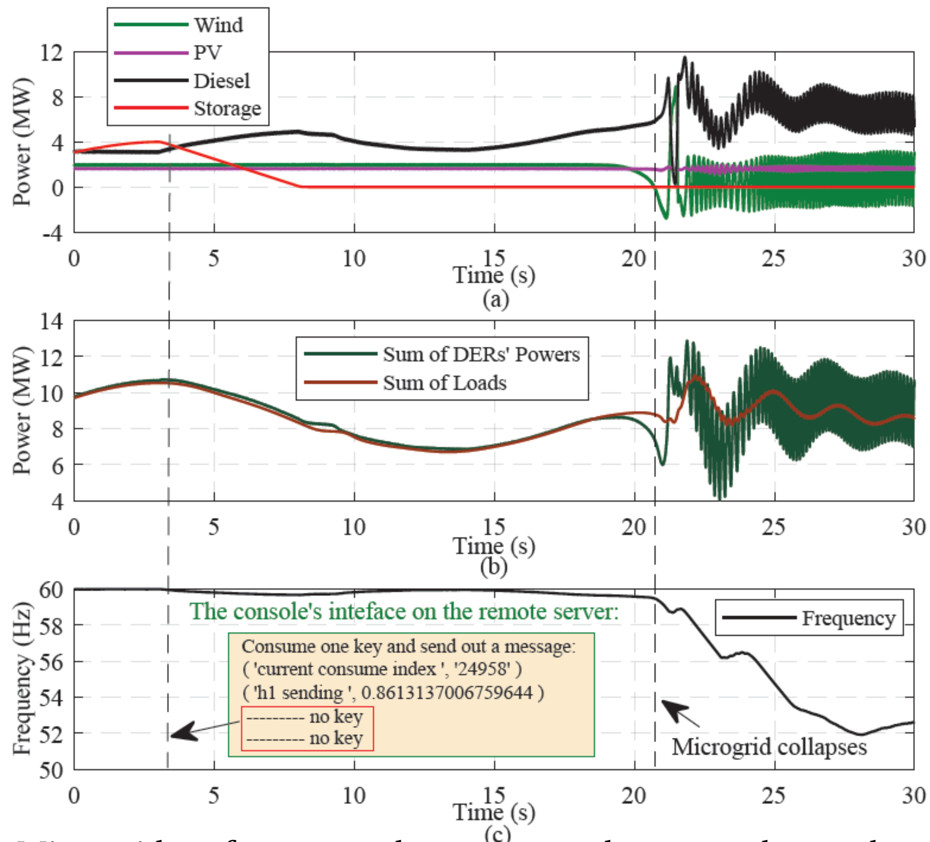
FAR BEYOND

Experimental Results (3/7)

Stony Brook University

NAVAL POSTGRADUATE SCHOOL

Case 3: Microgrid performance when quantum keys are exhausted



Microgrid performance when quantum keys are exhausted.

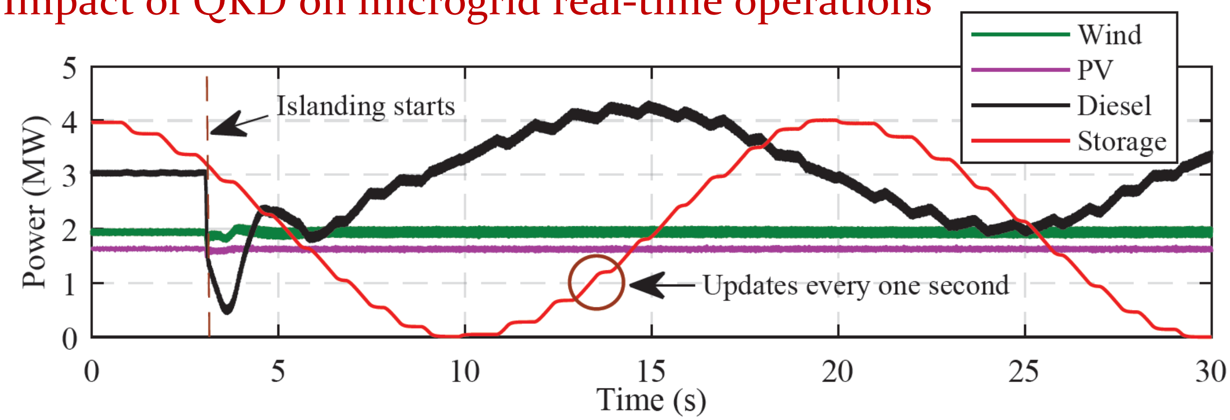
FAR BEYOND

Stony Brook University

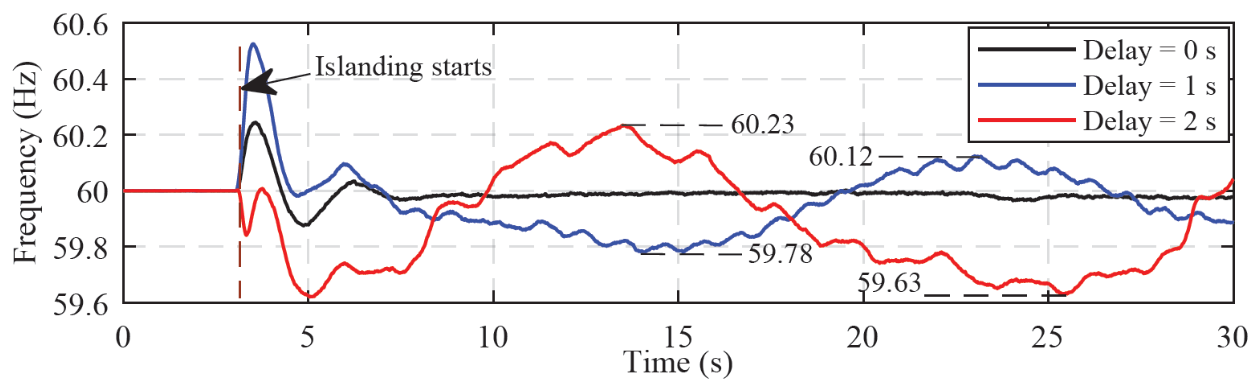
Experimental Results (4/7)

NAVAL POSTGRADUATE SCHOOL

Case 4: Impact of QKD on microgrid real-time operations



The output power from each DER when the delay is 1 s before and after microgrid islands.



Comparison results of the system frequency with different delays.

- The larger the delay is, the more unstable the system will be.

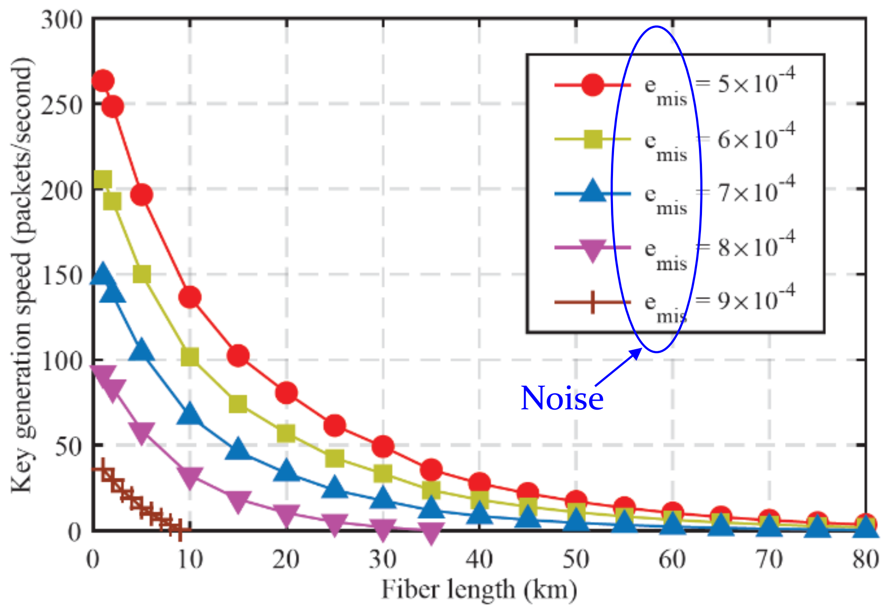
FAR BEYOND

Experimental Results (5/7)

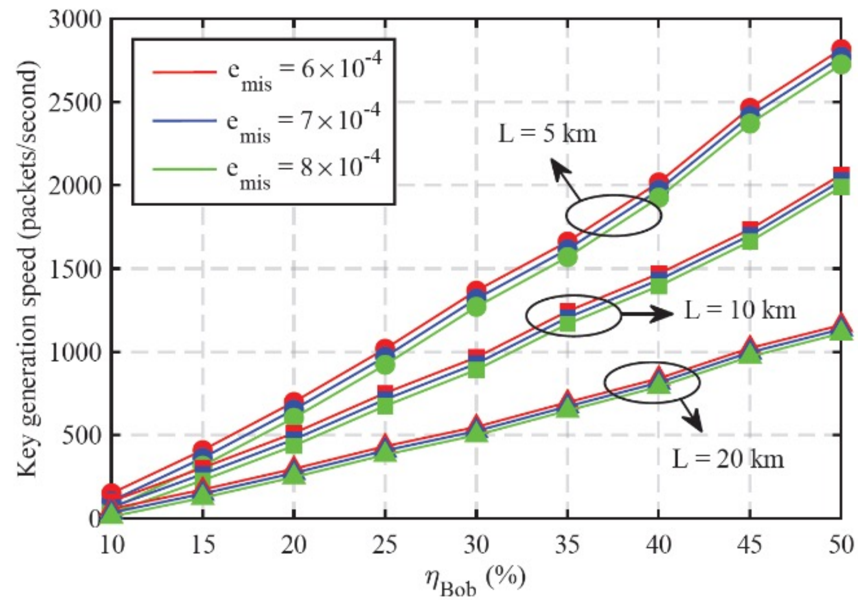
Stony Brook University

NAVAL POSTGRADUATE SCHOOL

Case 5: Key generation speed



Quantum key generation speeds under different Ls and e_{mis}s.

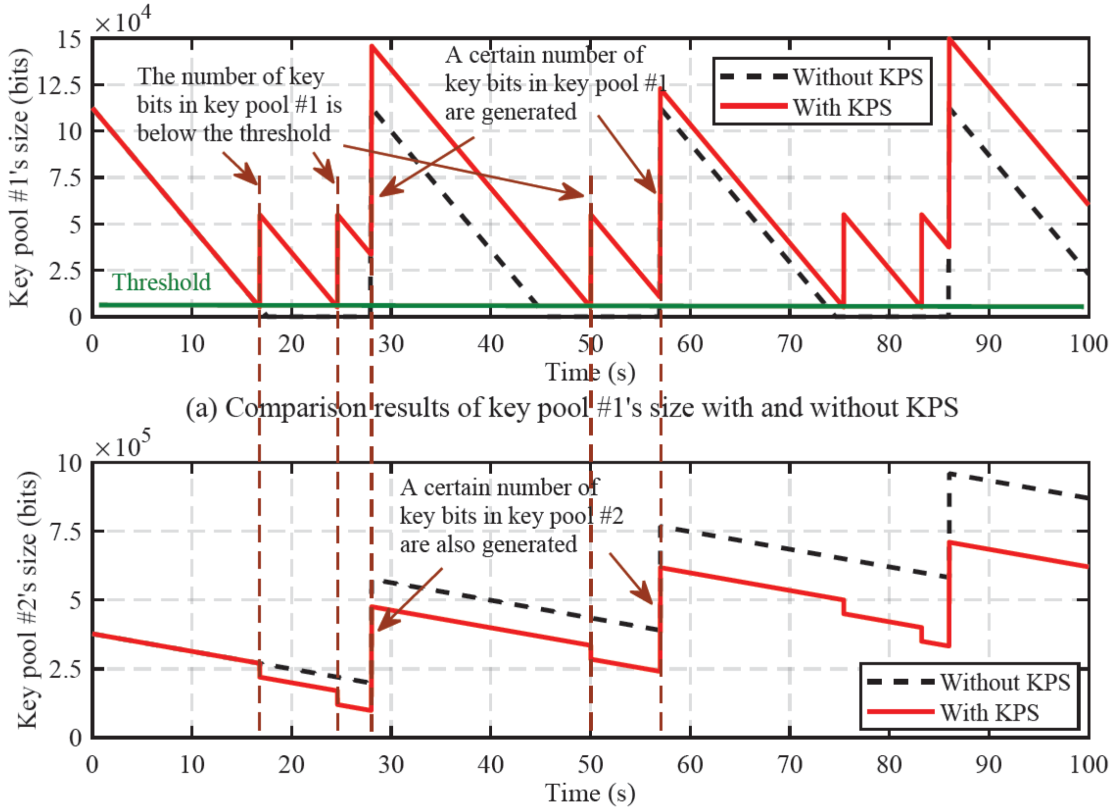


Quantum key generation speeds under different detection efficiencies.

FAR BEYOND

Experimental Results (6/7)

Case 6: KPS performance



(a) Comparison results of key pool #1's size with and without KPS

(b) Comparison results of key pool #2's size with and without KPS

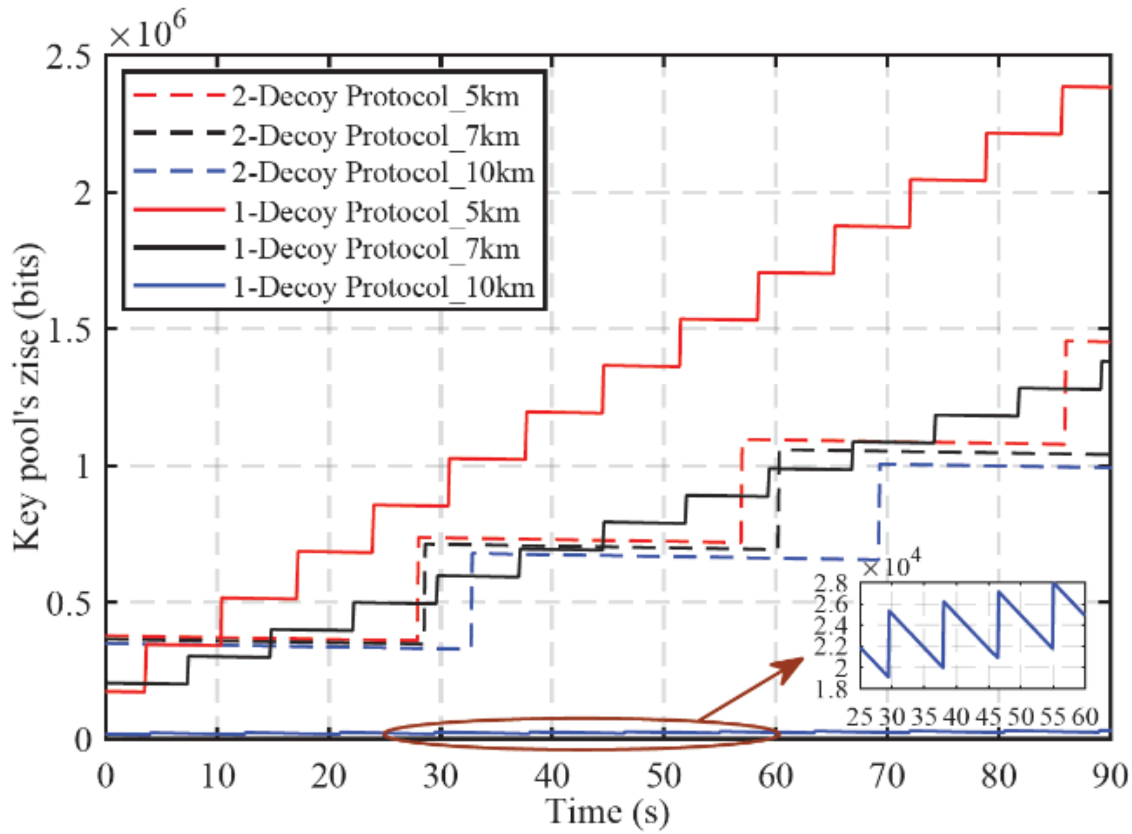
Comparison results of the numbers of key bits in key pools #1 and #2 with and without KPS.

Stony Brook University

Experimental Results (7/7)

NAVAL POSTGRADUATE SCHOOL

Case 7: Different QKD protocols



Comparison results of the 2-decoy state protocol and 1-decoy state protocol with different fiber lengths.

FAR BEYOND

Stony Brook University

Outline

NAVAL POSTGRADUATE SCHOOL

- Introduction
- Quantum Communication
- Quantum-Secure Microgrid
- Quantum-Secure Networked Microgrids
  - QSNMs Architecture
  - QSNMs Testing Environment
  - Experimental Results
- Programmable Quantum Networked Microgrids
- Conclusion and Future Work

1. Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure networked microgrids," in *IEEE Power and Energy Society General Meeting*, Montreal, Quebec, Canada, Aug. 2020. **Best Paper Award.**

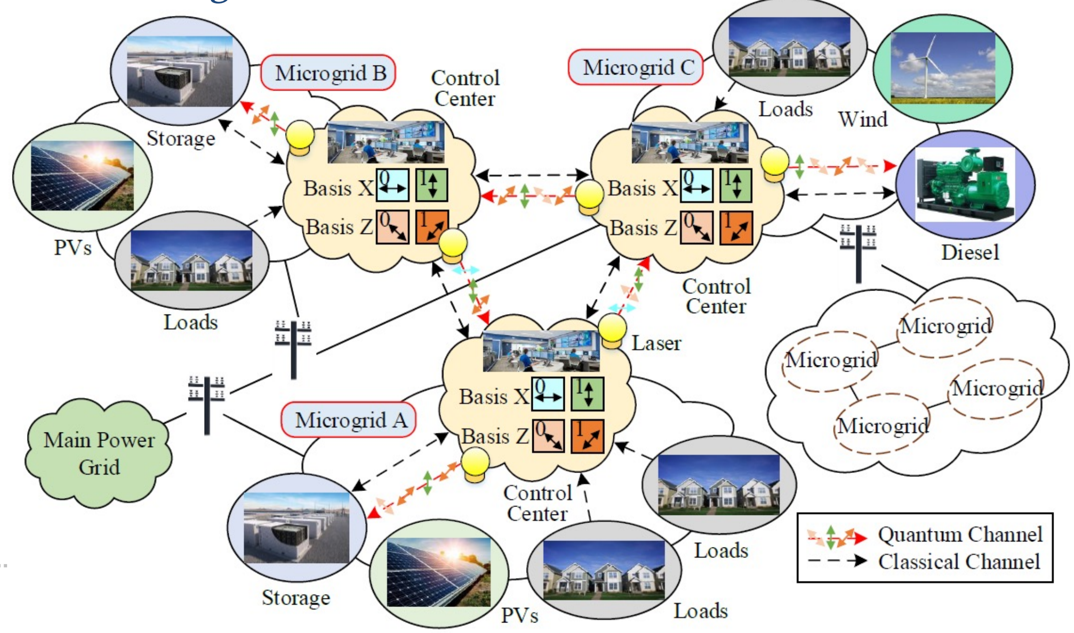
QSNMs Architecture

Microgrid control center (MGCC):

- Collect data from different loads through classical communication
- Send control signals to local controller(s) through quantum communication
- Send and receive control signals to and from other MGCCs

Local controller(s):

- Receive control signals from MGCC



An overview of the QKD-enabled quantum-secure NMs communication architecture.

FAR BEYOND

The TLKPS Strategy

The two-level key pool sharing (TLKPS) strategy:

- When the # of bits in KP_{ij} is below a threshold:
  - ❑ If there is an intermediate KP: use the first level of TLKPS strategy;
  - ❑ If there is no intermediate KP: use the second level of TLKPS strategy.

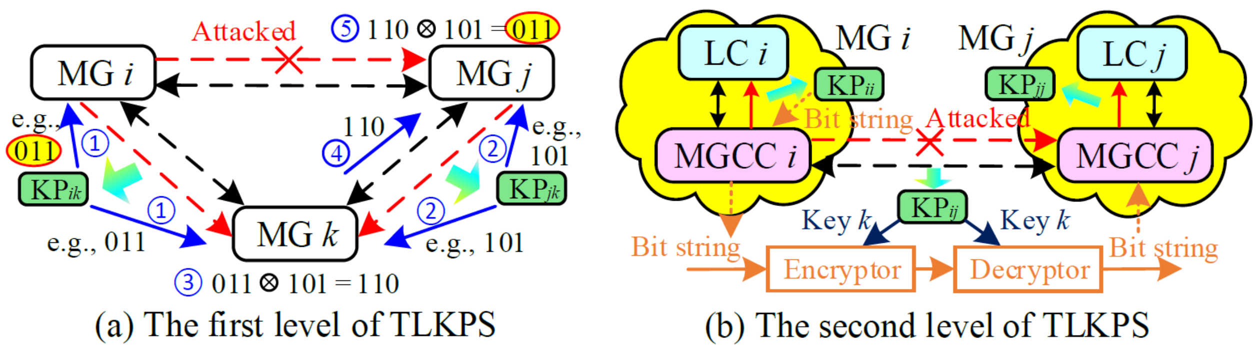
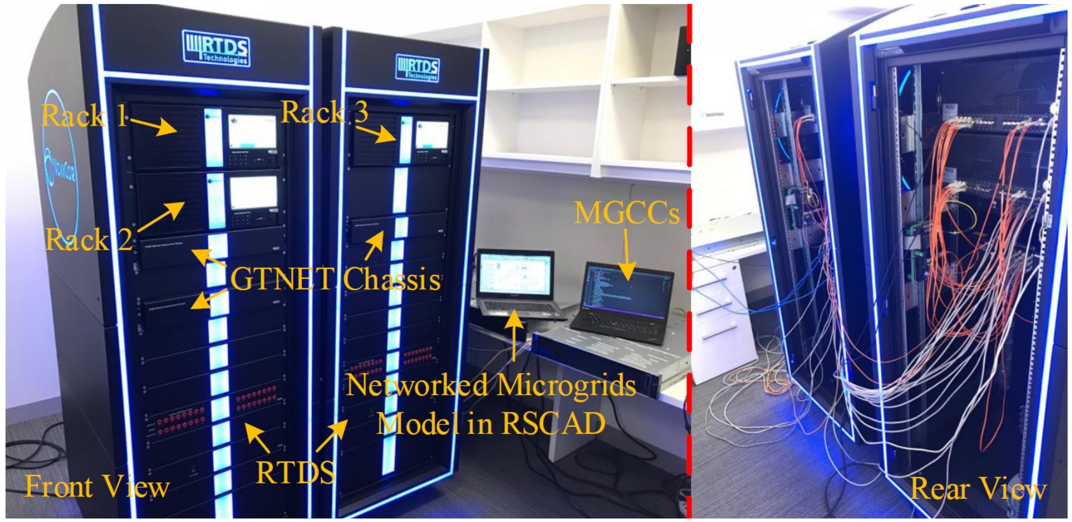


Illustration of the TLKPS strategy.

QSNMs Testing Environment (1/3)

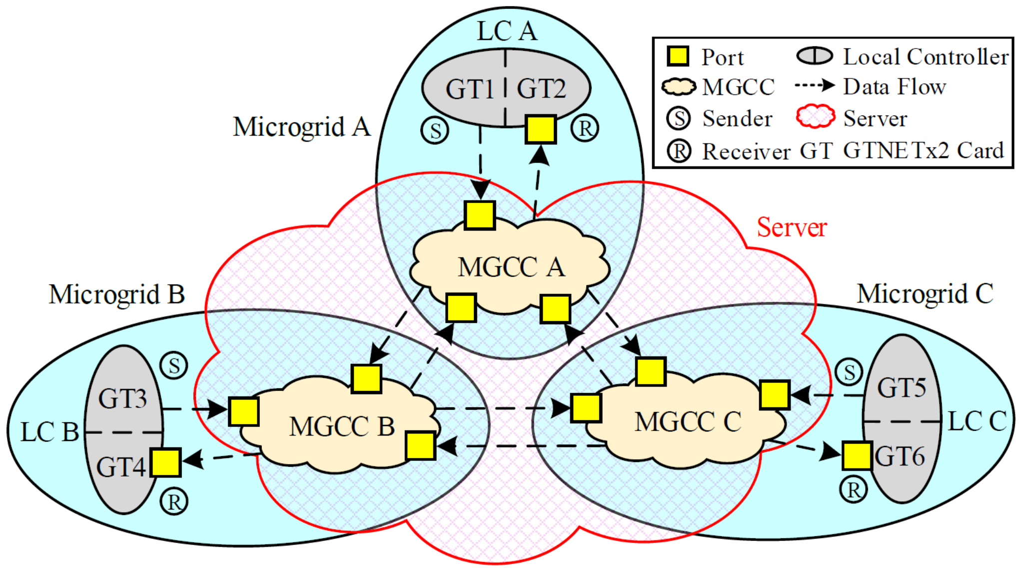


Testbed setup for quantum-secure NMs in RTDS.

High level design:

- Microgrid model is developed and compiled in RSCAD.
- Measurements from the RTDS are transmitted through a GTNETx2 card and are sent to the MGCC via a communication network.
- MGCCs: run on a remote server.
- For each microgrid, two GTNETx2 cards are used:
  - GTNETx2 card #1: used to receive signals from MGCC and to send them to the RTDS.
  - GTNETx2 card #2: used to transmit data from the RTDS to the MGCC.

QSNMs Testing Environment (2/3)



Network topology for the QKD-enabled quantum-secure NMs.

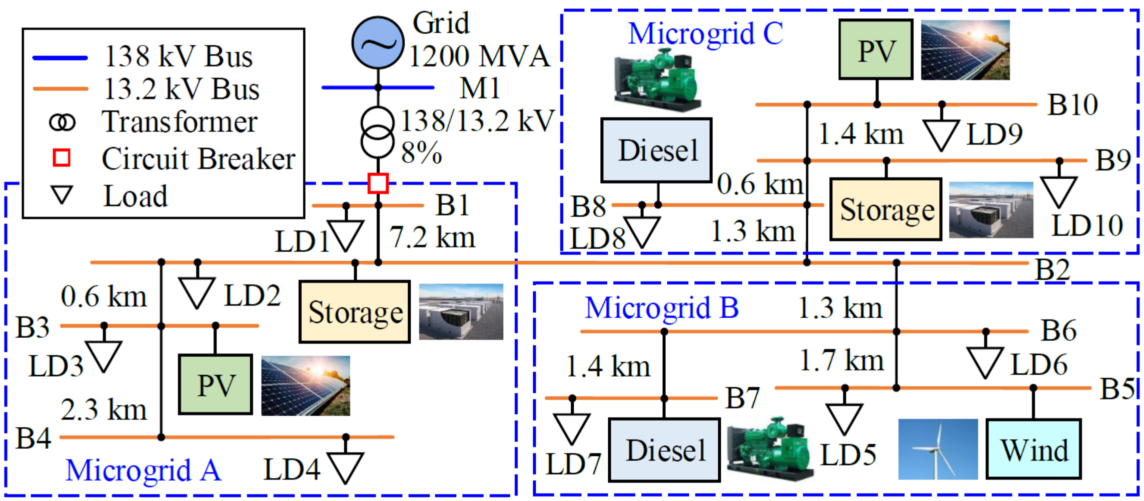
- User Datagram Protocol (UDP): IP & port
- Separate QKD algorithms & separate KPs
- Key bits are continuously generated in each KP with a different speed.
- When there is a need to use keys, a certain # of bits are consumed from the corresponding KP.

FAR BEYOND

QSNMs Testing Environment (3/3)

NMs modeling:

- Three microgrids are interconnected with each other.
  - ❑ Two 5.5 MW diesel generator
  - ❑ Two 1.74 MW PV system
  - ❑ A 2 MW doubly-fed induction generator wind turbine system
  - ❑ Two lithium-ion battery storage



One-line diagram of the NMs model.

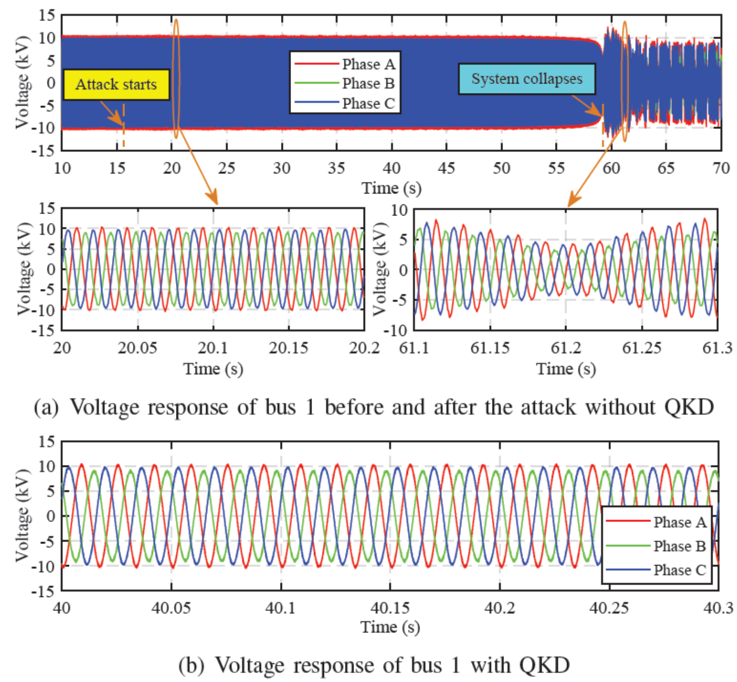
Experimental Results (1/2)

Stony Brook University

NAVAL POSTGRADUATE SCHOOL

Impact of cyberattacks on the microgrid:

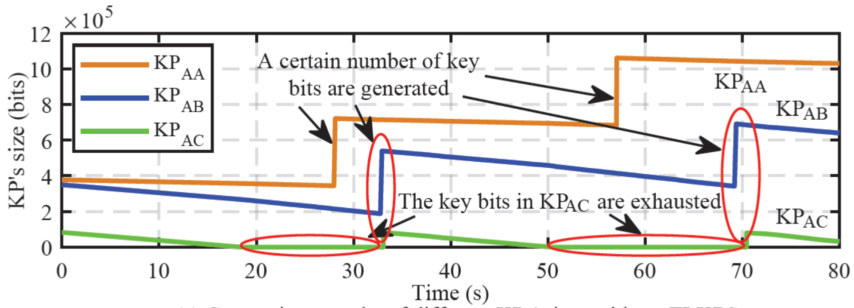
- The real power reference of the P-Q control for the storage at Bus 2 was changed from the initial value, 0, to -6 MW at time t=16s during the islanded mode.
    - 1) The magnitude of voltage gradually decreases.
    - 2) The frequency also decreases.
    - 3) At time t=59s, the system eventually collapses.
- If QKD is employed: impossible to break the encryption or authentication.



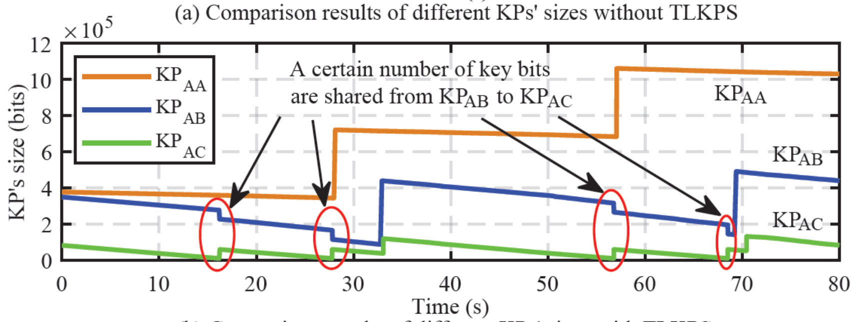
Voltage response of bus 1 with and without QKD.

FAR BEYOND

Experimental Results (2/2)



(a) Comparison results of different KPs' sizes without TLKPS



(b) Comparison results of different KPs' sizes with TLKPS

Comparison results of the numbers of key bits in KPAA, KPAB and KPAC with and without TLKPS when only the quantum channel between MG A and MG C is attacked.

Effectiveness of TLKPS:

- e_{mis} for KPAC is 8×10^{-4} to simulate a strong attack.
- e_{mis} for other KPs is 5×10^{-4} to simulate a weak attack.
- Threshold: 10,000
  - 1) Without TLKPS, there is a shortage of key bits in KP_{AC}.
  - 2) With TLKPS, the shortage issues of KP_{AC} are well addressed.

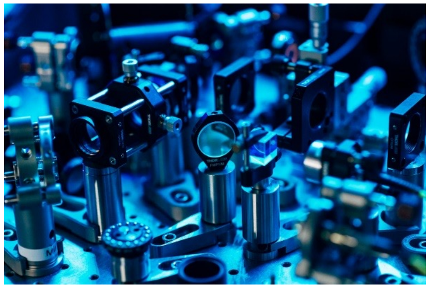
FAR BEYOND

Stony Brook University

NAVAL POSTGRADUATE SCHOOL

Future Work

1. Experimental Demonstration of QKD in Microgrids
2. Novel Practical QKD Protocols for Microgrids
3. Software-Defined Quantum Microgrid



FAR BEYOND