# Quantum-Secure Networked Microgrids

Zefan Tang, Yanyuan Qin, Zimin Jiang, Walter O. Krawec, Peng Zhang

***Abstract*—The classical key distribution systems used for data transmission in networked microgrids (NMGs) rely on mathematical assumptions, which however can be broken by attacks from quantum computers. This paper addresses this quantum-era challenge by using quantum key distribution (QKD). Specifically, the novelty of this paper includes 1) a QKD-enabled communication architecture it devises for NMGs, 2) a real-time QKD-enabled NMGs testbed it builds in an RTDS environment, and 3) a novel two-level key pool sharing (TLKPS) strategy it designs to improve the system resilience against cyberattacks. Test results validate the effectiveness of the presented strategy, and provide insightful resources for building quantum-secure NMGs.**

***Index Terms*—Networked microgrids, quantum key distribution, quantum communication, cyber security**

## I. Introduction

ALL classical public key systems used in networked microgrids (NMGs) to distribute keys for two communicating parties are secured based on the assumed limits on an adversary's power, i.e., the mathematical problems such as the discrete logarithm problem [1] or the factoring problem [2] cannot be efficiently solved even by the fastest modern computers with any existing algorithms. This mathematical assumption however can be broken by attacks from quantum computers, as quantum computing promises to efficiently solve mathematical problems [3]. Although today's quantum computers are still noisy and their advent on a degree powerful enough to break current cryptographic systems is perhaps still decades away, their sudden appearance will leave microgrid organizers little time to adapt.

A potent solution to tackle this quantum-era challenge is to use the quantum key distribution (QKD) [4]–[6]. QKD provides information-theoretic security through the laws of physics. Those laws have been fairly heavily tested, and provide a more solid foundation than computational assumptions. Different protocols have been proposed to implement QKD including the well-known BB84, decoy-state, six-state, Ekert91, and BBM92. However, while QKD has been extensively analyzed and widely applied in areas such as computer networks [7], online banking [8], ATM transactions [9], e-voting systems [10], and portable applications [9], the microgrid community is unfortunately largely silent on the topic of developing quantum-secure NMGs. In the context of quantum-secure NMGs, the existing QKD systems however cannot be directly applied. With multiple data transmission channels existing in NMGs, it was unclear how the QKD's performance will be in the system. A real-time QKD-enabled NMGs simulation testbed for evaluating the performance of the system is significantly needed but does not yet exist.

Furthermore, the key generation speed in a QKD system is affected by various factors such as the distance between two communicating parties and the noise, which can be either natural or caused by an adversary, on quantum optic equipment. A large distance or a strong attack on the QKD equipment can unfortunately reduce the speed, detrimentally causing keys to be exhausted. A proper strategy is therefore needed to improve the cyberattack resilience for the system.

To bridge the gaps, we devise a QKD-based communication architecture for NMGs in this paper. A practical decoy-state protocol is utilized to implement QKD. This protocol has been one of the most widely used schemes in the QKD community, and its security and feasibility have been well-demonstrated by different experimental groups. We then show in detail how to build a QKD-integrated quantum-secure NMGs testbed in an RTDS environment, including the hardware connection, communication network design, and QKD integration. Further, we present a novel two-level key pool sharing (TLKPS) strategy to improve the system's cyberattack resilience. Extensive tests are implemented on the testbed. Test results validate the effectiveness of the presented strategy, and provide insightful resources for building quantum-secure NMGs.

The remainder of this paper is organized as follows: Section II describes the presented QKD-enabled NMGs architecture and the TLKPS strategy. Section III elaborates the testbed design in the RTDS environment. The results of our investigation are reported in Section IV. Section V concludes the paper.

## II. Quantum-Secure NMGs Architecture

### A. Quantum Key Distribution

The general setting of a QKD-based communication system is illustrated in Fig. 1. It consists of a quantum channel and a classical one. The quantum channel allows two parties, commonly named Alice and Bob, to share quantum bits (or qubits) for creating secure and secret keys. With the created keys, the information to be transmitted is encrypted and later decrypted over the classical channel. The keys generated are stored in a key pool (KP), and will be extracted later from the KP for encryption and decryption. The security of a QKD protocol, in a way, takes advantage of this: by encoding a classical bit string using different, randomly-chosen bases, an adversary who is unaware of the basis choice can never be truly certain of the information being transmitted. Furthermore, any attempt to actually learn this information causes noise in the quantum channel which can be detected by the two parties later.

This work was supported by the National Science Foundation under Grant ECCS-1831811.

Z. Tang, Z. Jiang and P. Zhang are with the Department of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY 11794, USA (e-mail: p.zhang@stonybrook.edu).

Y. Qin and W. O. Krawec are with the Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269, USA.

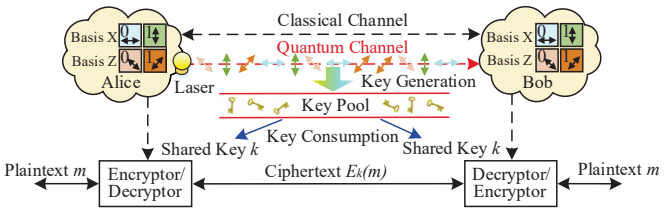



Fig. 1. The general setting of a QKD-based communication system.

In this study, we consider a practical decoy-state QKD protocol to implement QKD. Parameters of this QKD system are adopted from [11]. The technology to create a stable QKD link (as we simulated) is available today and the simulator parameters take into account standard devices used today. There are several experimental and commercial groups with this hardware capability. Bit generation rates are continuing to increase while cost is continuing to decrease, leading to the potential for even more practical systems in the near future.

### B. Attack Model

Adversaries have complete control over all quantum communication channels along with perfect quantum memories. In addition, they are free to perform an optimal attack on the quantum communication utilizing any computational capability available now or in the future (e.g., using quantum computers). The security guarantees the QKD-produced keys are information theoretic in that they do not make any assumptions on the computational abilities of the adversary. Thus, the keys derived are secure even against future computational or algorithmic breakthroughs. We do assume that devices internal to communication nodes (e.g., quantum sources and quantum measurement devices) are trusted and cannot be tampered with by the adversary. As future work, we may explore relaxing this assumption moving towards device-independent models of security; however for this work, we assume trusted devices. Finally, we assume an authenticated classical channel connects two parties. Such channels are needed for QKD systems to operate and provide information theoretic authentication (but not secrecy). These authentication tags, being also information theoretic secure, are secure against future computational or algorithmic breakthroughs (e.g., they are secure against a future quantum computer).

### C. QKD-Enabled NMGs Architecture

We present a QKD-based quantum-secure NMGs architecture in this paper. As shown in Fig. 2, the NMGs system consists of multiple interconnected MGs. Within each MG, a microgrid control center (MGCC) collects information from customers and sends corresponding control signals to local controllers. In this architecture, QKD is utilized to generate keys for communications between each MGCC and local controllers in the same MG, while the communications between each MGCC and customers in the same MG are established over classical channels. The keys used for the communication between two MGCCs in different MGs are also generated using QKD. Note that this design is practical and reasonable,

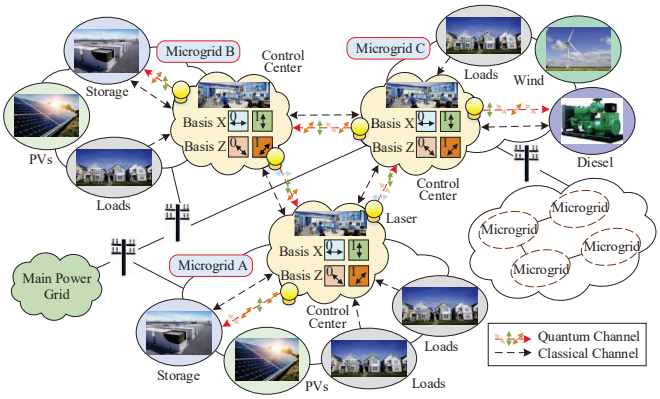



Fig. 2. An overview of the QKD-enabled quantum-secure NMGs architecture.

**Algorithm 1:** The TLKPS Strategy

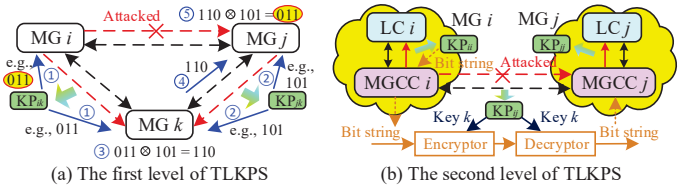
**Input:** $T_h$, $N_s$, QKD configurations
**Results:** The number of bits in each KP is above $T_h$
initialize NMGs system configuration;
**for** *each* $KP_{ij}$ *between MG* $i$ *and MG* $j$ **do**
  **if** $N_{ij} < T_h$ **then**
    **if** *there exists MG* $k$ && $N_{ik} > (T_h + N_s)$ && $N_{jk} > (T_h + N_s)$ **then**
      Share $N_s$ bits from $KP_{ik}$ and $KP_{jk}$ to $KP_{ij}$;
    **else**
      **if** $N_{ii} < N_{jj}$ **then**
        Share $N_s$ bits from $KP_{jj}$ to $KP_{ij}$;
      **else**
        Share $N_s$ bits from $KP_{ii}$ to $KP_{ij}$;
      **end**
    **end**
  **end**
**end**

because from the economic perspective, building a quantum link is costly; therefore, quantum channels are only allocated for important communications. Keys generated by different quantum channels are stored in separate KPs.

### D. The TLKPS Strategy

Ideally, the key generation speed in a QKD system has to be large enough to guarantee there are always enough keys in the KP. However, this speed can be affected by a variety of factors such as the distance between two communicating parties and the attack on quantum optic equipment. To maintain normal operations in the QKD-enabled NMGs, a proper strategy is needed in case the bits in any KP are used up.

In this paper, we develop a two-level key pool sharing (TLKPS) strategy. The procedures are formalized in Algorithm 1. A threshold $T_h$, which restricts the minimum number of bits in a KP, is first determined. If the number of bits in each KP is below $T_h$, a given number of bits will be shared from other KPs. Let $KP_{ij}$ be the KP between MG $i$ and MG $j$, $N_{ij}$ the number of bits in $KP_{ij}$, and $N_s$ the number of bits sent to $KP_{ij}$. Then, if $N_{ij}$ is below $T_h$, $N_s$ bits will be sent to $KP_{ij}$.




(a) The first level of TLKPS (b) The second level of TLKPS

Fig. 3. Illustration of the TLKPS strategy.

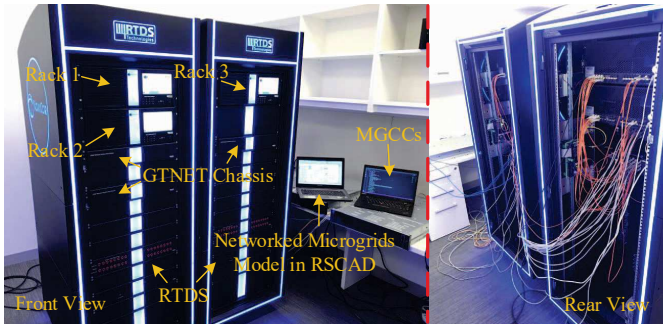



Fig. 4. Testbed for QKD-enabled quantum-secure NMGs in RTDS.

Fig. 3 gives an illustration of the TLKPS strategy. It consists of two levels of bit-sharing from other KPs to $\text{KP}_{ij}$. When there exists MG $k$ that establishes KPs with both MG $i$ and MG $j$, and the numbers of bits in $\text{KP}_{ik}$ and $\text{KP}_{jk}$ are both above $(T_h + N_s)$, $N_s$ bits can be shared to $\text{KP}_{ij}$ using the first level of TLKPS. In this case, MG $k$ is utilized as an intermediate node to distribute keys between MG $i$ and MG $j$. The procedures are formalized in Fig. 3 (a). MG $k$ and MG $i$ both extract a string of bits (i.e., $N_s$ bits) from $\text{KP}_{ik}$, and MG $k$ and MG $j$ both extract the same number of bits from $\text{KP}_{jk}$. MG $k$ then XORs the extracted two bit strings, and sends the result to MG $j$. MG $j$ XORs the received bit string with the bit string extracted previously from $\text{KP}_{jk}$. The result obtained by MG $j$ will be exactly the same as the bit string extracted by MG $i$ from $\text{KP}_{ik}$. In this way, a string of bits is securely transferred from $\text{KP}_{ik}$ and $\text{KP}_{jk}$ to $\text{KP}_{ij}$. Note that this first level of TLKPS still maintains information-theoretic security, and therefore is given the first priority in TLKPS.

However, it is common that in some cases there is no such intermediate MG, or attacks are performed on multiple links, making intermediate MGs fail to share enough bits. The second level of TLKPS is thus established. As shown in Fig. 3 (b), instead of using an intermediate MG to share keys to $\text{KP}_{ij}$, the second level of TLKPS utilizes the KP inside MG $i$ (denoted as $\text{KP}_{ii}$) or the KP inside MG $j$ (denoted as $\text{KP}_{jj}$). When $N_{ij}$ is below $T_h$, a string of bits is extracted from $\text{KP}_{ii}$ (or $\text{KP}_{jj}$ depending on which KP has more bits). This bit string is then used as a plaintext, encrypted by MGCC $i$ via a key extracted from $\text{KP}_{ij}$ (note there are still some keys left in $\text{KP}_{ij}$), and sent to MGCC $j$. MGCC $j$ uses the same key from $\text{KP}_{ij}$ to decrypt the received message and obtains the bit string. A bit string is thus transferred from $\text{KP}_{ii}$ and is securely shared to $\text{KP}_{ij}$. Note that this AES-based key distribution loses information-theoretic security, and is performed when the first level of TLKPS fails. But it is still better than relying on public key systems because AES is considered quantum-secure.

## III. Quamtum-Secure NMGs Testing Environment

### A. QKD-Enabled Quantum-Secure NMGs Testbed

Fig. 4 gives the design of our testbed for the QKD-enabled quantum-secure NMGs in RTDS, a real-time power system simulator. Specifically, the model of the NMGs is developed and compiled in RSCAD, a power system simulation software designed to interact with the RTDS simulation hardware. The RTDS in our testbed consists of three racks, which can be either used separately for small-scale power systems or combined together to provide more cores for a large-scale system. In this study, rack 1 is utilized to simulate the NMGs in real-time, where the six cores in that rack are sufficient to provide high fidelity for our test results.

The measurements from the RTDS simulator are sent to a remote server using GTNETx2 cards, which can either receive data from the RTDS and send it to external equipment, or receive data from the network and send it back to the RTDS, depending on whether they are designed to be in sending or receiving mode. The MGCCs in the NMGs run on the same remote server (they can also run on different servers). The server receives load measurements from the RTDS, and sends signals back to RTDS, with a 1 Gbps Ethernet connection.

A QKD simulator capable of simulating the decoy-state BB84 protocol is developed in Python in the remote server. It simulates the probabilities of various events occurring such as multiple photon emission, photons being lost in the channel, phase errors, and detector imperfections. The simulator assumes quantum signals are continually being sent from end-nodes building a raw-key pool. When the simulator is called, it determines how many signals could have been sent from the last call (based on the speed of the simulated laser source and detector dead times), what the user's choices were for those signals (e.g., basis and intensity choices), and whether the receiver got a measurement outcome. If a sufficient number of signals have been sent the error correction and privacy amplification results are simulated leading to the generation of a simulated secret key of the actual size that would be generated under these conditions in practice. These secret key bits are added to the respective key pool.

### B. Quantum-Secure NMGs Communication Network

The network topology for the QKD-enabled NMGs is illustrated in Fig. 5. In this testbed, the keys used for communications between two MGs and between a MGCC and a local controller (LC) are generated using separate QKD algorithms, and are stored in separate KPs. When there is a need to use keys, a certain number of bits are consumed from the corresponding KP. Two GTNETx2 cards are utilized for the communication between a LC in the RTDS simulator and each MGCC on the remote server. The User Datagram Protocol (UDP) is used in our simulation to transmit and receive data.

The measurements in each MG are transmitted to its MGCC through one GTNETx2 card with a fixed speed set in RSCAD.

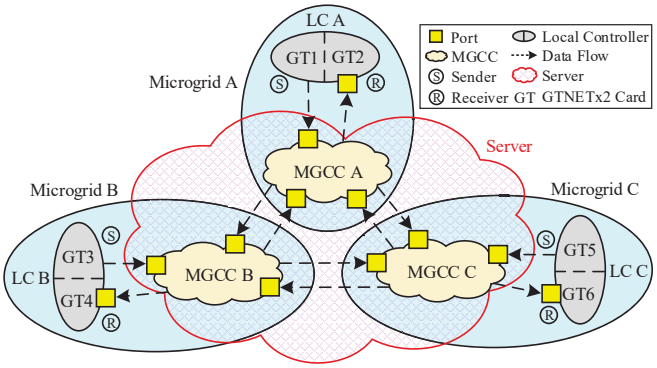



Fig. 5. Network topology for the QKD-enabled quantum-secure NMGs.

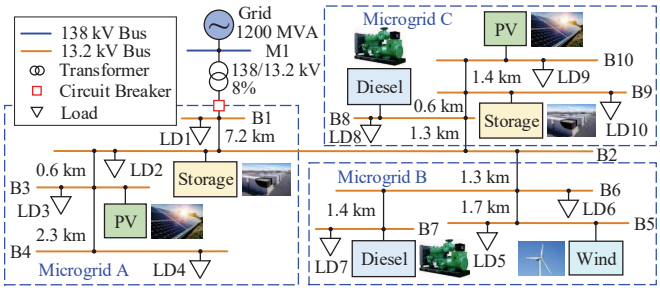



Fig. 6. One-line diagram of the NMGs model in this study.

The destination IP address is set as the IP address of the server, and the destination port is a specific number for the MGCC. Another GTNETx2 card is used for the LC to receive data from MGCC. Any UDP packet whose destination IP and port match those of this GTNETx2 card, will be received.

From the MGCC side, each MGCC is receiving any UDP packet whose destination IP is the server's IP and destination port match the MGCC's port. When each MGCC receives a data packet from the RTDS, it sends out messages to other two MGCCs and a control signal to its LC. Two other ports are set for each MGCC to receive UDP packets from other two MGCCs. When each MGCC receives a data packet from another MGCC, a certain number of bits in the KP between the two MGCCs are deducted.

### C. NMGs Modeling

A typical NMGs system shown in Fig. 6 is modeled to evaluate the performance of the QKD-enabled NMGs. This system is designed based on a medium-voltage MG from [12]. Three MGs are interconnected with each other. MG A contains a photovoltaic (PV) system and a battery storage. A P-Q control is designed to regulate the output power of the battery, the value of which is determined by the real and reactive power references transferred from MGCC A. MG B contains a diesel generator and a wind turbine. A droop control is utilized to regulate the output power of the diesel, the value of which is determined by the real and reactive power references transferred from MGCC B. MG C contains a diesel generator, a PV system and a storage, where the storage uses a P-Q control whose real and reactive power references are given by MGCC C. Both the PV and wind turbine in the NMGs use the

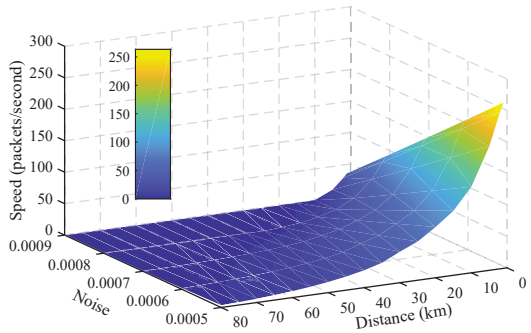



Fig. 7. Key generation speed with different distances and noises. Each packet consists of 64 bits.

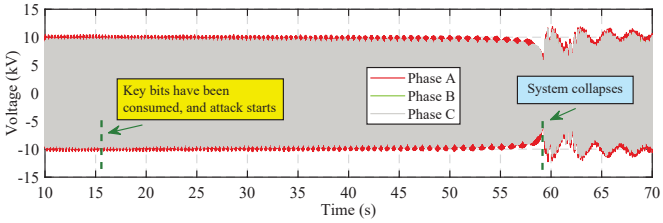



Fig. 8. Voltage response of bus 1 before and after the key bits are used up.

Maximum Power Point Tracking (MPPT) control to maximize their output powers. The information shared between two MGs includes the total power generation and the total load in each MG. For more details on the design of the NMGs, readers are referred to [12].

## IV. Experimental Results

### A. Key Generation Speed with Different Distances and Noises

The key generation speed is a critical metric in a QKD-based system, as it determines the maximum data transmission speed. Fig. 7 gives the experimental results of the key generation speed under different distances and noises, where each packet consists of 64 bits. It can be seen that 1) a small distance exhibits great superiority over a large one under the same noise, which gives valuable insights that two QKD parties should not be too far from each other; and 2) a large noise dramatically decreases the speed even with a small distance; this indicates that a proper strategy is significantly needed to improve the system's resilience against attacks.

### B. Impact of Attacks on NMGs

The impact of attacks on NMGs is evaluated in this subsection. For a classical communication or a quantum communication when keys are exhausted, the security of the communication can be easily broken by using quantum computers. The control signals sent from the MGCC to the LC can thus be intercepted and falsified by an adversary. The impact of a malicious control signal on the NMGs system is illustrated in Fig. 8, where the real power reference of the P-Q control for the battery in MG A is changed from 0 to -6 MW at time $t = 16$ s during the islanded mode. It can be observed that 1) the voltage's magnitude decreases, 2) the frequency also decreases, and 3) at time $t = 59$ s, the system collapses. It is thus of great importance to have enough key bits in the KP.

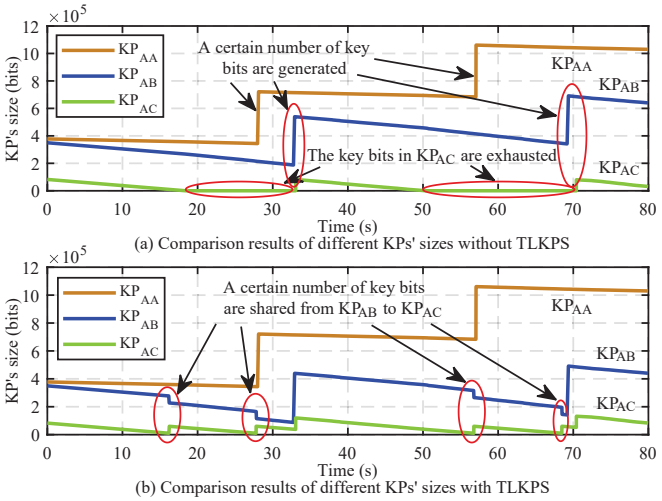



Fig. 9. Comparison results of the numbers of key bits in $\mathrm{KP}_{AA}$, $\mathrm{KP}_{AB}$ and $\mathrm{KP}_{AC}$ with and without TLKPS when only the quantum channel between MG A and MG C is attacked.

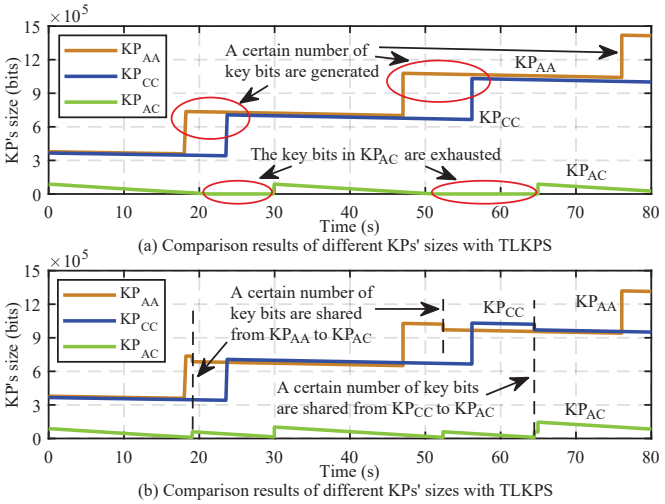



Fig. 10. Comparison results of the numbers of key bits in $\mathrm{KP}_{AA}$, $\mathrm{KP}_{CC}$ and $\mathrm{KP}_{AC}$ with and without TLKPS in multi-attack scenario.

### C. Effectiveness of TLKPS in Single-Attack Scenario

Fig. 9 gives the comparison results of the numbers of bits in $\mathrm{KP}_{AA}$, $\mathrm{KP}_{AB}$ and $\mathrm{KP}_{AC}$ with and without TLKPS when only the quantum channel between MG A and MG C is attacked. The noise for the quantum channel between MG A and MG C is set at $8 \times 10^{-4}$ to simulate a strong attack, while the noises for other quantum channels are $5 \times 10^{-4}$. The distance between two MGs is set at 10 km, and the distance between each MGCC and its LC is 5 km. For the TLKPS strategy, the threshold is set at 10,000, meaning that once the number of bits in any KP is below 10,000, a given number of bits (which is set at 50,000) will be shared to that KP.

It can be seen that 1) without TLKPS, there is a shortage of bits in $\mathrm{KP}_{AC}$ while at the same time other KPs do not have the shortage issues; and 2) with TLKPS, the shortage issue can be well solved; when the number of bits in $\mathrm{KP}_{AC}$ is below 10,000, 50,000 bits are sent from $\mathrm{KP}_{AB}$ to $\mathrm{KP}_{AC}$.

### D. Effectiveness of TLKPS in Multi-Attack Scenario

Fig. 10 gives the comparison results of the numbers of bits in $\mathrm{KP}_{AA}$, $\mathrm{KP}_{CC}$ and $\mathrm{KP}_{AC}$ with and without TLKPS in multi-attack scenario. The noises for the quantum channel between MG A and MG B, and the quantum channel between MG A and MG C are both set at $8 \times 10^{-4}$ to simulate strong attacks, while the noises for other quantum channels are $5 \times 10^{-4}$ for weak attacks or no attack. The distance between MGCC A and LC A is set at 5 km, while the distance between MGCC C and LC C is 7 km for a slight difference in the numbers of bits in $\mathrm{KP}_{AA}$ and $\mathrm{KP}_{CC}$. The distance between MG A and MG C is set at 9 km. The setting for the TLKPS strategy is the same as in the previous subsection.

It can be seen that 1) without TLKPS, there is a shortage of bits in $\mathrm{KP}_{AC}$; and 2) with TLKPS, when the number of bits in $\mathrm{KP}_{AC}$ is below 10,000, 50,000 bits are shared from either $\mathrm{KP}_{AA}$ or $\mathrm{KP}_{CC}$ to $\mathrm{KP}_{AC}$ depending on which KP ($\mathrm{KP}_{AA}$ or $\mathrm{KP}_{CC}$) has more bits; the shortage issue is well solved.

## V. Conclusion

In this paper, a QKD-enabled architecture is devised for NMGs. It ensures an unconditional security by using the laws of quantum-mechanics. Detailed instructions are provided for developing a QKD-integrated NMGs testbed in an RTDS environment, and the TLKPS strategy is further established to enhance the system's attack resilience. Future work could be done on investigating the system's performance with the testbed under more scenarios and improving the TLKPS strategy to further enhance the resilience of the system.

## References


[1] K. S. McCurley, "The discrete logarithm problem," in *Proc. of Symp. in Applied Math*, vol. 42. USA, 1990, pp. 49–74.

[2] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms," *IEE Proceedings-Computers and Digital Techniques*, vol. 141, no. 3, pp. 193–195, 1994.

[3] J. R. Friedman, V. Patel, W. Chen, S. Tolpygo, and J. E. Lukens, "Quantum superposition of distinct macroscopic states," *nature*, vol. 406, no. 6791, p. 43, 2000.

[4] C.-H. F. Fung, X. Ma, and H. Chau, "Practical issues in quantum-key-distribution postprocessing," *Physical Review A*, vol. 81, no. 1, p. 012318, 2010.

[5] G.-L. Long and X.-S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Physical Review A*, vol. 65, no. 3, p. 032302, 2002.

[6] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure microgrid," *arXiv preprint arXiv:2001.02301*, 2020.

[7] M. Geihs, O. Nikiforov, D. Demirel, A. Sauer *et al.*, "The status of quantum-key-distribution-based long-term secure internet communication," *IEEE Transactions on Sustainable Computing*, 2019.

[8] J.-L. Zhang, M.-S. Hu, Z.-J. Jia, L.-P. Wang *et al.*, "A novel E-payment protocol implented by blockchain and quantum signature," *International Journal of Theoretical Physics*, vol. 58, no. 4, pp. 1315–1325, 2019.

[9] S. Cobourne *et al.*, "Quantum key distribution protocols and applications," *Surrey TW20 0EX, England*, 2011.

[10] H. Alshammari, K. Elleithy, K. Almgren, and S. Albelwi, "Group signature entanglement in e-voting system," in *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*. IEEE, 2014, pp. 1–4.

[11] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Physical Review A*, vol. 89, no. 2, p. 022307, 2014.

[12] N. Onyinyechi, "Real time simulation of a microgrid system with distributed energy resources," 2015.