Quantum-Secure Microgrid

Zefan Tang, *Student Member, IEEE,* Yanyuan Qin, *Student Member, IEEE,* Zimin Jiang, *Student Member, IEEE,* Walter O. Krawec, Peng Zhang, *Senior Member, IEEE*

***Abstract*—Existing microgrid communication relies on classical public key systems, which are vulnerable to attacks from quantum computers. This paper uses quantum key distribution (QKD) to solve these quantum-era microgrid challenges. Specifically, this paper makes the following novel contributions: 1) it devises a novel QKD simulator capable of simulating QKD protocols; 2) it offers a QKD-based microgrid communication architecture for microgrids; 3) it shows how to build a quantum-secure microgrid testbed in an RTDS environment; 4) it develops a key pool sharing (KPS) strategy to improve the cyberattack resilience of the QKD-based microgrid; and 5) it analyzes the impacts of critical QKD parameters with the testbed. Test results provide insightful resources for building a quantum-secure microgrid.**

***Index Terms*—Microgrid, quantum key distribution, quantum computer, cyber security, communication, testbed**

NOMENCLATURE

χ_n	The probability that the laser sends a n-photon state
$\delta_{Z,1}$	The number of bit errors of single-photon Z events in the raw key
ℓ	The length of the extracted secret key
η_{Bob}	The receiver's detection efficiency
η_{ec}	Error correction efficiency
η_{tr}	The transmittance that is related to the fiber length L
λ_{ec}	Specifies how much information leaked during error correction
ϕ_X	Phase error rate of single-photon X events in raw key
ε_c	The probability that keys extracted by the two parties are not identical
ε_s	The maximum failure probability
$\xi_{X,0}$	The number of vacuum X events in the raw key
$\xi_{X,1}$	The number of single-photon X events in the raw key
$\xi_{Z,0}$	The number of vacuum Z events in the raw key
$\xi_{Z,1}$	The number of single-photon Z events in the raw key
B	Block size for post processing
b_k	The probability of having a bit error for intensity k
e_{mis}	Error rate due to optical errors
k_i	The i^{th} intensity; $i = 1, 2, 3$
L	The fiber length
$m_{Z,k}$	The number of error events in the raw key with the Z basis for intensity k
N_b	The number of raw-key signals in the "buffer"
N_r	The number of signals needed to be sent before the post processing can start
N_s	Key pool size
N_t	The total number of signals that have been sent by the laser within $(t_c - t_p)$
$n_{X,k}$	The number of X signals received using intensity k
$n_{Z,k}$	The number of Z signals received using intensity k
$n_{Zr,k}$	The number of error events in Z basis for intensity k
p_x	The probability of choosing the X basis by the sender
p_{ap}	After-pulse probability
p_{d_k}	The probability that a signal with intensity k is received by the receiver
p_{dc}	Dark count probability
p_{k_i}	The probability of intensity k_i
P^*_{ref}	Active power reference
Q^*_{ref}	Reactive power reference
R_c	The rate of correctly-received raw-key signals
r_k	The expected detection rate
$R_{X,k}$	Expected transmission rate of X signals for k
$R_{Z,k}$	Expected transmission rate of Z signals for k
$R_{Zr,k}$	Expected transmission error rate in the Z basis for k
t_c	The current time
t_p	The last calling time
v_s	The speed of the laser sending signals

This work was supported in part by the National Science Foundation under Grant ECCS-1831811 and in part by the Office of the Vice President for Research, Stony Brook University.

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.

I. INTRODUCTION

SECURING data transmission in microgrid is critical for maintaining normal grid operations and achieving desirable benefits, e.g., fast recovery during a main grid blackout, improved system reliability and resilience, and economic power supply to customers [1]–[3]. Existing methods on this topic largely rely on cryptographic systems such as the Advanced Encryption Standard (AES) [4]. AES and similar methods use a key for all encryptions within a given time period [5]. It therefore requires that the key, which is preshared by two parties, has to be kept secret. This secure key distribution process is mostly achieved by public-key cryptographic methods such as the Diffie-Hellman key exchange (DH) [6] and Rivest-Shamir-Adleman (RSA) [7].

However, the security of all classical public key systems is only guaranteed based on the assumed limits on an adversary's power. For instance, some mathematical problems such as the discrete logarithm problem [8] or the factoring problem [9] cannot be effectively solved even by the fastest modern computers using any existing algorithms [10]. These assumptions however are still unproven, and if proven false, the current cryptographic systems will no longer be secure [11].

Further, even if these assumptions remain true, the development of quantum computers will lead to security breaks [12], [13]. Quantum computing promises to efficiently solve mathematical problems by using quantum-mechanical phenomena such as superposition [14] and entanglement [15]. Note that

although today's quantum computers are still noisy and their advent on a scale large enough to break current cryptographic systems is perhaps still decades away, their sudden appearance will leave microgrid stakeholders little time to adapt.

A potent solution to tackle this quantum-era challenge is the use of quantum key distribution (QKD) [16]. It uses laws of quantum mechanics to securely generate keys for two parties. Because those laws have been fairly heavily tested, they provide a more solid foundation than computational assumptions. However, although QKD has been widely applied in such areas like computer networks [17], online banking [18], and ATM transactions [19], the microgrid community is unfortunately largely silent on the topic of developing a quantum-secure microgrid. Part of the reason for this stems from the fact that the existing QKD systems cannot be directly applied in microgrid. With multiple communication channels and different transmission requirements existing in microgrid, it was unclear how QKD performs and whether it is applicable under various circumstances. A real-time QKD-integrated microgrid simulation testbed for evaluating the performance of the QKD-based microgrid is critical but does not yet exist.

Building a real-time QKD-integrated microgrid simulation testbed is however challenging. There are currently no existing resources indicating how to integrate QKD systems into a real-time microgrid simulator. For instance, most cyber-physical power system testbeds focus on power sources, control systems, communication bandwidths, delays, and cyberattacks [20]–[22], neither of which is related with quantum cryptography. In addition, no existing QKD simulators or real systems can be directly integrated into an existing microgrid simulator. To properly integrate QKD systems into a real-time microgrid simulator, the critical concerns are summarized as follows: 1) the system should have the capability to flexibly modify QKD parameters for simulating different scenarios, e.g., with different fiber lengths and noise levels; 2) the system should be easily extensible to employ different QKD protocols with different principles, theories and configurations; and 3) the system should be capable of simulating multiple quantum channels and even multiple microgrids.

Further, the key generation speed in a QKD system is affected by a number of variables like 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 reduce this speed, detrimentally causing keys to be exhausted. As the frequency of data transmission in microgrid is much faster than that in many other areas, keys in microgrid are more likely to be exhausted. A proper strategy is significantly needed to enhance the resilience of the system.

To bridge the gaps, in this paper, we develop a QKD-integrated microgrid testbed in Real Time Digital Simulator (RTDS). Specifically, a QKD simulator is developed in Python capable of simulating QKD systems in practice. This simulator is not only able to flexibly modify QKD parameters, but also easily extensible for different QKD protocols and quantum channels. Key components of the testbed like hardware connection, communication network, and QKD integration are designed and presented in detail. To evaluate the performance of the QKD-enabled microgrid, extensive case studies are conducted. Building this QKD-integrated microgrid real-time testing environment is an important step towards constructing a realistic QKD-enabled microgrid in practice. The real-time communication between the RTDS simulator and a remote server enabled by the QKD algorithm is the salient feature of this testbed. Main contributions of this paper are as follows:

- A novel QKD simulator is developed capable of simulating QKD protocols with great flexibility to modify QKD parameters and ease of extensibility for different QKD protocols and quantum channels.
- A novel QKD-enabled communication architecture is devised for microgrids. Instead of using classical public key systems to distribute keys for two communicating parties, it uses quantum cryptography with an information-theoretic security. This architecture is also easily extensible for more QKD systems and more microgrids.
- A QKD-integrated microgrid testbed is built in RTDS. Key components like hardware connection, communication network, and QKD integration are designed. This is the first real-time power systems testbed that integrates both microgrid and quantum cryptography features.
- A novel key pool sharing (KPS) strategy is designed to further enhance the system's resilience to cyberattacks. It is not only quantum-secure but also ensures that the information-theoretic one-time pad (OTP) is used up until the last 128 or 256 bits are available maximizing the security of the overall system.
- The impacts of critical QKD parameters like quantum fiber length, data transmission speed, attack level, and detection efficiency are evaluated with the testbed. The impact of QKD systems on microgrid and the comparison of different QKD protocols are also investigated.

The rest of this paper is organized as follows: Section II describes quantum communication and offers the design of the QKD simulator. The QKD-based microgrid architecture and the KPS strategy are presented in Section III. Section IV elaborates the testbed design. Our evaluation results are reported in Section V, and Section VI concludes the paper.

II. Quantum Communication and A QKD Simulator

In this section, we will first give a brief overview of quantum communication including quantum states, the general setting of a QKD system, and a practical decoy-state protocol. We will then present the novel QKD simulator capable of simulating QKD protocols, and the benefits of using QKD for microgrids.

A. Quantum Communication

1) Quantum States: Instead of using binary bits to encode information as in classical communication systems, quantum communication utilizes quantum states, or "qubits". A qubit is a two-state quantum-mechanical system, whose state is commonly represented by the spin of an electron or the polarization of a photon. Unlike a binary bit, which has to be in one state or the other, a qubit can be in a coherent superposition of both states [23]. For QKD systems, photons are the primary practical implementation of qubits. For the

QKD system we consider, the polarization of the photon will be used to encode a quantum state. We will consider two *Bases*, namely horizontal polarization (denoted as the Z basis later) and diagonal polarization (denoted as the X basis later). If a source and its receiver both operate in the same basis, information can be transmitted deterministically; however, if different bases are used, the information received will be uncorrelated with the transmitted information.

2) General Setting: The general setting of a QKD-based communication system consists of a quantum channel and a classical one. The quantum channel allows two parties to share quantum signals for creating a secure and secret key. With the created key, the information to be transmitted is encrypted and later decrypted over the classical channel. The *key generation rate* of a QKD protocol is an important statistic and is affected by numerous parameters, most importantly the noise in the quantum channel (caused, perhaps, by an adversary or natural noise) and the distance between the two parties.

An important and unique property of QKD is that the two parties can detect when an eavesdropper is trying to gain knowledge of the keys. This is due to the quantum-mechanical property that measuring an unknown quantum state will, in general, change that state. This ensures that a non-secret key will never be used, making QKD-based encryption and authentication theoretically secure. It is worth noting that QKD is only used to generate keys through the quantum channel; data messages are still transmitted using classical encryption methods over the classical channel. In reality, QKD can be associated with either one-time pad (OTP) or some other symmetric key algorithms such as AES.

3) Practical QKD Protocol: Different protocols have been proposed to implement QKD such as the well-known BB84, decoy-state, six-state, Ekert91, and BBM92 (see [24] for a survey). In this paper, we consider a practical decoy-state QKD protocol [24], [25]. This protocol has been one of the most widely used schemes in the QKD community because of its ability to tolerate high channel loss and to operate robustly even with today's hardware. Its security and feasibility have been well-demonstrated by several experimental groups, and theoretical security analyses including the evaluation of concise and tight finite-key security bounds have been provided.

The idea of this protocol is as follows: The information is encoded into qubits and then sent out by one party, commonly named Alice, using weak coherent laser pulses. With today's technology, the production of a single qubit is not practical; instead, weak coherent laser pulses are used. However, these pulses contain, with non-zero probability, multiple qubit signals that would cause a break in security. To tackle this challenge, the decoy-state protocol varies the intensity of each laser pulse randomly using one of three intensities k_1, k_2 and k_3, which are the intensities of the signal state, decoy state and vacuum state, respectively. Two bases X and Z are selected with probabilities p_x and $1-p_x$, respectively. Recall that these bases refer to the polarization setting of the qubit. The other party, named Bob, measures the qubits by randomly selecting bases from X and Z. If Alice and Bob choose the same basis, they share information since sending and receiving qubits in the same basis, as mentioned, leads to a deterministic outcome; otherwise, the iteration is discarded. By repeating this numerous times, the two parties share a so-called *raw-key*, which is partially correlated and partially secret. Error correction is then performed (leaking additional information to the adversary which must be taken into account) followed by privacy amplification, yielding a secret key of size ℓ.

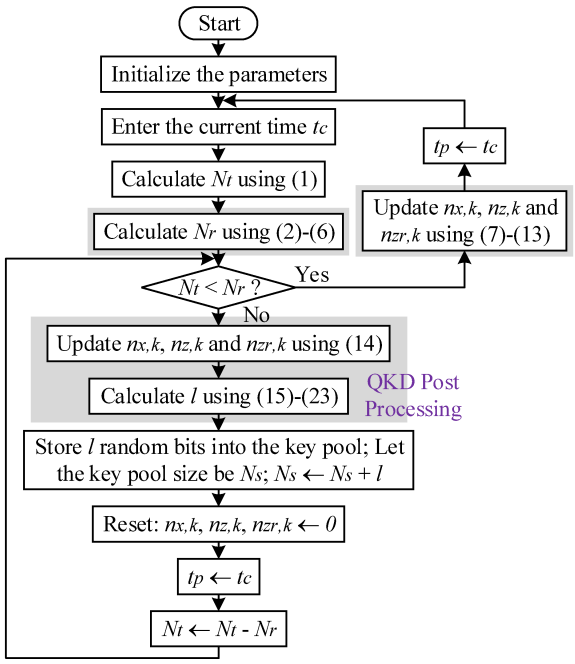


Fig. 1. The flow chart of the QKD simulator.

B. QKD Simulator

To integrate QKD systems into a real-time microgrid simulation testbed, we develop a QKD simulator using Python in this paper capable of simulating QKD protocols. The flow chart of the simulator capable of simulating the decoy-state protocol is given in Fig. 1. Note that this simulator is easily extensible for different QKD protocols.

In this simulator, we use time as the indicator to determine whether a sufficient number of key signals have been sent by the laser for generating the secret key of size ℓ. Let the current time be t_c, and the last calling time be t_p. Then, within the interval $(t_c - t_p)$, the number of signals that have been sent by the laser, N_t, can be obtained as

$$N_t = v_s(t_c - t_p), \tag{1}$$

where v_s is the speed of the laser sending signals, a constant value assumed in this study.

The post measured signals received by Bob are temporarily stored in a classical "buffer". When a sufficient block size of signals have been received, the post processing will start. Let the block size for post processing be B which is set by the users, and the number of signals needed to be sent before the post processing can start be N_r. Then,

$$N_r = \frac{B - N_b}{R_c}, \tag{2}$$

where N_b is the number of raw-key signals in the "buffer", and R_c is the rate of correctly-received raw-key signals, i.e.,

the ratio of the number of correctly-received signals (leading to a useful raw key) and the number of signals actually sent. Specifically, R_c can be calculated as follows [26]:

$$R_c = \sum_{k\in\{k_1,k_2,k_3\}} p_k p_x^2 p_{d_k}, \tag{3}$$

where p_{d_k} is the probability that a signal with intensity k is received by Bob. It can be expressed as

$$p_{d_k} = (1+p_{ap})r_k,\ \forall k \in \{k_1,k_2,k_3\}, \tag{4}$$

where p_{ap} is the after-pulse probability. r_k is the expected detection rate (excluding after-pulse contributions) for intensity k, and can be calculated as follows:

$$r_k = 1-(1-2p_{dc})e^{-\eta_{tr}\eta_{Bob}k},\ \forall k \in \{k_1,k_2,k_3\}, \tag{5}$$

where p_{dc} is the dark count probability and η_{Bob} is Bob's detection efficiency. η_{tr} is the transmittance that is related to the fiber length L as follows:

$$\eta_{tr} = 10^{-0.2L/10}, \tag{6}$$

where the fibers are assumed to have an attenuation coefficient of 0.2 dB/km.

When the simulator is called, N_t and N_r are calculated and compared. Based on the comparison result of N_t and N_r, two cases exist as described below:

1) Case 1: If N_t is smaller than N_r, the post processing will not start, and the value of t_c will be assigned to t_p. Note that t_c is continuously increasing. Meanwhile, a certain number of signals within the time interval $(t_c - t_p)$ will be added into the "buffer". Let $n_{X,k}$ be the number of X signals received using intensity k. Then, of course, n_X, the size of the raw key in the "buffer" with the X basis, is simply the sum of all $n_{X,k}$ over all the intensities used. Specifically, $n_{X,k}$ can be updated as follows:

$$n_{X,k} \leftarrow n_{X,k} + N_t R_{X,k},\ \forall k \in \{k_1,k_2,k_3\}, \tag{7}$$

where $R_{X,k}$ is the expected transmission rate of X signals for intensity k. It can be expressed as

$$R_{X,k} = p_k p_x^2 p_{d_k},\ \forall k \in \{k_1,k_2,k_3\}. \tag{8}$$

Similarly, the number of Z signals received using intensity k, $n_{Z,k}$, can be updated as follows:

$$n_{Z,k} \leftarrow n_{Z,k} + N_t R_{Z,k},\ \forall k \in \{k_1,k_2,k_3\}, \tag{9}$$

where $R_{Z,k}$ is the expected transmission rate of Z signals for intensity k, and can be expressed as

$$R_{Z,k} = p_k(1-p_x)^2 p_{d_k},\ \forall k \in \{k_1,k_2,k_3\}. \tag{10}$$

The size of the raw key in the "buffer" with the Z basis, n_Z, is the sum of all $n_{X,k}$ over all the intensities used.

For our simulation, we assume a standard fiber channel and practical settings for devices. In this case, the probability of having a bit error for intensity k, b_k, is as follows:

$$b_k = p_{dc} + e_{mis}(1-e^{-\eta_{tr}k}) + \frac{p_{ap}r_k}{2},\ \forall k \in \{k_1,k_2,k_3\}, \tag{11}$$

where e_{mis} is the error rate due to optical errors. Then, the number of erroneous bits in the Z basis for intensity k, $n_{Zr,k}$, can be updated as follows:

$$n_{Zr,k} \leftarrow n_{Zr,k} + N_t R_{Zr,k},\ \forall k \in \{k_1,k_2,k_3\}, \tag{12}$$

where $R_{Zr,k}$ is the expected transmission error rate in the Z basis for intensity k, and can be expressed as

$$R_{Zr,k} = p_k(1-p_x)^2 b_k,\ \forall k \in \{k_1,k_2,k_3\}. \tag{13}$$

When all the X, Z, and erroneous signals with all the intensities have been added, the simulator goes back to the "listening" mode. As mentioned, t_p becomes t_c, and t_c continuously grows.

2) Case 2: If N_t is greater than or equal to N_r, post processing will start. The simulator will then add all the X, Z, and erroneous signals with all the intensities into $n_{X,k}$, $n_{Z,k}$ and $n_{Zr,k}$, respectively. Specifically, $n_{X,k}$, $n_{Z,k}$ and $n_{Zr,k}$ can be updated in the following way:

$$\begin{cases} n_{X,k} \leftarrow n_{X,k} + N_r R_{X,k} \\ n_{Z,k} \leftarrow n_{Z,k} + N_r R_{Z,k} \\ n_{Zr,k} \leftarrow n_{Zr,k} + N_r R_{Zr,k} \end{cases} \forall k \in \{k_1,k_2,k_3\}. \tag{14}$$

After the post processing is completed, the key is established and can be used by Alice and Bob. The simulator simulates the process by calculating the length ℓ of the extracted secret key that would be generated under the same conditions in practice. The length ℓ of the extracted secret key can be obtained as follows [25]:

$$\ell = \lfloor \xi_{X,0} + \xi_{X,1} - \xi_{X,1}h(\phi_X) - \lambda_{ec} - 6\log_2\frac{21}{\varepsilon_s} - \log_2\frac{2}{\varepsilon_c} \rfloor, \tag{15}$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. $\xi_{X,0}$, $\xi_{X,1}$, and ϕ_X are the number of vacuum events, the number of single-photon events, and the phase error rate of the single-photon events in the raw key with the X basis, respectively. ε_c is the probability that the keys extracted by the two parties are not identical, and ε_s is the user-specified maximum failure probability. λ_{ec} specifies how much information is leaked during error correction. It is set to $n_X\eta_{ec}h(\phi_X)$, where η_{ec} is the error-correction efficiency.

The above parameters cannot be directly observed; however, by using the decoy-state protocol, they can be bounded as shown in [25]. Basically, $\xi_{X,0}$ satisfies

$$\xi_{X,0} \geq \chi_0 \frac{k_2 n^-_{X,k_3} - k_3 n^+_{X,k_2}}{k_2 - k_3}, \tag{16}$$

where χ_n is the probability that Alice sends a n-photon state. This value, using a weak-coherent laser, follows a Poisson distribution and is found to be:

$$\chi_n = \sum_{k\in\{k_1,k_2,k_3\}} e^{-k}k^n p_k/n!, \tag{17}$$

and

$$n^{\pm}_{X,k} = \frac{e^k}{p_k}(n_{X,k} \pm \sqrt{\frac{n_X}{2}\ln\frac{21}{\varepsilon_s}}),\ \forall k \in \{k_1,k_2,k_3\}. \tag{18}$$

TABLE I
INITIAL VALUES OF THE PARAMETERS IN THE QKD SIMULATOR

k_1	k_2	k_3	p_{k_1}	p_{k_2}	p_{k_3}	$n_{X,k}$
0.4	0.1	0.007	1/3	1/3	1/3	0
B	p_x	p_{dc}	ε_c	η_{Bob}	e_{mis}	$n_{Z,k}$
10^7	0.8	6×10^{-7}	10^{-11}	0.1	5×10^{-4}	0
t_p (s)	η_{ec}	p_{ap}	ε_s	L (km)	v_s (bit/s)	$n_{Zr,k}$
0	1.16	4×10^{-2}	10^{-11}	5	4×10^7	0

The number of single-photon events in the raw key with the X basis, $\xi_{X,1}$, satisfies

$$\xi_{X,1} \geq \frac{\chi_1 k_1[n^-_{X,k_2} - n^+_{X,k_3} - \frac{k_2^2-k_3^2}{k_1^2}(n^+_{X,k_1} - \frac{\xi_{X,0}}{\chi_0})]}{k_1(k_2-k_3) - k_2^2 + k_3^2}. \quad (19)$$

Similarly, by using (16)-(19) with statistics from the basis Z, the number of vacuum events in Z_A, $\xi_{Z,0}$, and the number of single-photon events in the raw key with the Z basis, $\xi_{Z,1}$, can also be obtained.

The phase error rate of the single-photon events in the raw key with the X basis, ϕ_X, satisfies [27],

$$\phi_X \leq \frac{\delta_{Z,1}}{\xi_{Z,1}} + f(\varepsilon_s, \frac{\delta_{Z,1}}{\xi_{Z,1}}, \xi_{Z,1}, \xi_{X,1}), \quad (20)$$

where

$$f(a,b,c,d) = \sqrt{\frac{(c+d)(1-b)b}{cd\log 2}\log_2(\frac{c+d}{cd(1-b)b}\frac{441}{a^2})}, \quad (21)$$

and $\delta_{Z,1}$ is the number of bit errors of the single-photon events in the raw key with the Z basis. It is given by

$$\delta_{Z,1} \leq \chi_1 \frac{m^+_{Z,k_2} - m^-_{Z,k_3}}{k_2 - k_3}, \quad (22)$$

where

$$m^{\pm}_{Z,k} = \frac{e^k}{p_k}(m_{Z,k} \pm \sqrt{\frac{m_Z}{2}\ln\frac{21}{\varepsilon_s}}), \ \forall k \in \{k_1,k_2,k_3\}, \quad (23)$$

and $m_Z = \sum_{k\in\{k_1,k_2,k_3\}} m_{Z,k}$. Here, $m_{Z,k}$ is the number of error events in the Z basis.

In this paper, the initial values of the parameters from (1)-(23) are given in Table I.

In sum, this simulator 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 corresponding key pool.

Note that this QKD simulator is able to flexibly alter QKD parameters for simulating different scenarios, e.g., with different fiber lengths and noise levels. The simulator is also easily extensible for different QKD protocols and quantum channels. With a different QKD protocol, only the steps within shaded areas in Fig. 1 need to be changed correspondingly.

C. Attack Model and Security Requirement

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 of 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. For side-channel attacks, such as detector blinding attacks [28], other countermeasures exist. As future work, we may explore relaxing this assumption moving towards device-independent models of security; however for this work, we assume trusted devices. We also 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-theoretically secure, are secure against future computational or algorithmic breakthroughs, e.g., they are secure against attacks from a future quantum computer.

Further, all point-to-point communication systems are assumed to hold an initially-shared secret key (which may be pre-installed when devices are manufactured, or loaded into secure memories by the operator on the first setup). This shared initial key is needed for the authenticated channel to operate; however, it will be continually and automatically refreshed by the QKD system. As for functionality requirements, devices are required to have access to a classical communication network and a point-to-point quantum channel along with the source preparation and measurement devices needed to operate the decoy-state BB84 protocol. See [24] for more information on the needed hardware of a QKD system. This hardware is practical today and commercially available.

The security analysis follows information-theoretic techniques [29]. In particular, it is guaranteed that, except with the negligible probability ε_c, devices will output a secret key that is independent of any adversary, even one that is computationally unbounded. The security proof of the decoy state protocol in [25] guarantees that for any attack from the adversary allowed within the laws of physics, the final key is uniformly random and independent of any adversary.

D. Benefits of Using QKD for Microgrids

QKD has been envisioned as one of the most secure and practical instances of quantum cryptography. Specifically, using QKD provides the following benefits for microgrid:

- Keys generated by QKD are almost impossible to steal even in the face of an adversary with infinite supplies of time and processing power, because by encoding a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2020.3011071, IEEE Transactions on Power Systems

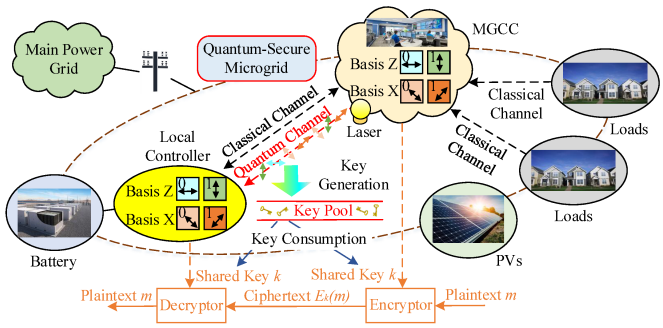


Fig. 2. QKD-enabled quantum-secure microgrid communication architecture.

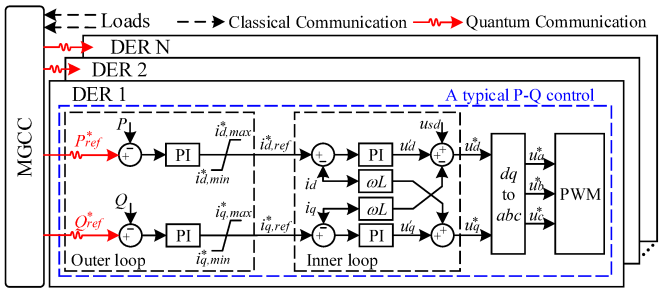


Fig. 3. Scheme of quantum-secure microgrid control.

classical bit using a randomly-chosen basis, an adversary unaware of the basis choice can never be truly certain of the information being transmitted.

- QKD is particularly well-suited to produce a long random key, which makes the OTP more realistic in practice. When QKD is combined with OTPs, both the key generation and encryption are unconditionally secure.
- A QKD-enabled microgrid is able to detect the presence of an eavesdropper trying to gain knowledge of the keys, whereas existing communication systems without this ability will inevitably require extra detection mechanisms. This is because any attempt to learn keys causes noise in the quantum channel which can be detected by users.
- QKD systems have the advantage of automatically generating provably secure keys over those manually distributing keys. This is needed in microgrid to satisfy various continuous data transmission requirements.

Note that there are also post-quantum ways to distribute keys. However, the security of post-quantum systems is always based on assumptions that solving certain mathematical problems (not the discrete logarithm problem or factoring problem, but other problems for quantum computers) is hard. QKD, conversely, does not require these assumptions.

III. Architecture of Quantum-Secure Microgrid

A. Quantum-Secure Microgrid Communication Architecture

Given the great benefits described above, we present a QKD-based communication architecture for microgrids. As illustrated in Fig. 2, the microgrid control center (MGCC) collects data from different loads (denoted as the first type of communication) and sends control signals to local controllers (denoted as the second type of communication). As building a quantum channel is costly, it is practical and reasonable to implement QKD for only those critical communications in microgrid. Compared with the first type of communication, the second type is arguably more critical, because a malicious control signal can directly lead to fateful consequences. The first type of communication is less critical, because when the data are received from different loads by the MGCC, they will typically be dealt with by some anomaly detection methods.

In this study, a QKD-based quantum channel is built between the MGCC and the local controller for a battery's storage. This battery uses a P-Q control to adjust its power output based on the real power reference received from the MGCC. It is worth noting that, QKD is only used for generating keys for two parties in an unconditional secure way; the data encryption process is still achieved using classical cryptographic methods such as AES or OTP. Using AES to encrypt data is considered quantum-secure, as long as the key used for this process is secure [30]. OTP is even more secure (or more accurately, unconditionally secure), because it uses a random key only once and then discards the key. But this requires that the key be as long as the plaintext. Keys generated by a QKD link are stored in a key pool, and when there is a need to transfer data, a certain number of key bits are extracted for encryption.

To properly integrate QKD into microgrid, a critical concern is key generation speed in a QKD system. It has to be larger than the frequency of data transmission to guarantee there are *always* enough keys in the key pool. Different with other applications where there is no strict requirement on the frequency of data transmission, microgrid often needs a high frequency of continuous data transmission to accommodate fast and dynamic changes typically caused by customers or various distributed energy resources (DERs). Before constructing a real QKD system in microgrid, building a real-time simulation testbed to evaluate the performance of the QKD-enabled microgrid under different circumstances is of great importance. In this paper, we show in detail how to build a QKD-integrated microgrid testbed in an RTDS environment. To maintain normal operations of the QKD-enabled microgrid when the key bits in a key pool are used up, we further develop a key pool sharing (KPS) strategy.

B. Quantum-Secure Microgrid Control

The microgrid control strategy is described in this subsection. As shown in Fig. 3, the MGCC collects data from different loads, and sends control signals to local controllers. Note that, in a real microgrid, not all controllers require external communications. For instance, photovoltaic (PV) solar systems and wind turbines can be controlled by the local Maximum Power Point Tracking (MPPT) controller. However, other controls such as the secondary, the tertiary, and the P-Q controls in some environments, can often require a communication channel to transmit control signals.

In this study, control signals are sent from the MGCC to some local controllers for regulating their output powers such that the total power generation matches the sum of loads. As the loads are dynamically changing in reality, the control signals vary correspondingly. A typical P-Q control used in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2020.3011071, IEEE Transactions on Power Systems

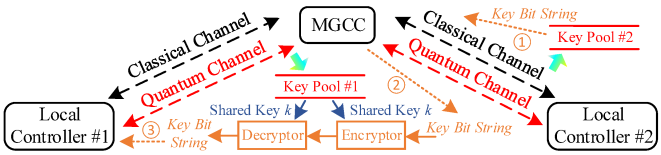


Fig. 4. An example of the KPS strategy.

this study is shown in Fig. 3, where the control signals are the active and reactive power references, i.e., P^*_{ref} and Q^*_{ref}.

Note that while the confidentiality of data might not be obviously critical in microgrid, the integrity of data is of paramount importance, and it is highly dependent on the security of keys. If the keys shared between the MGCC and a certain local controller are obtained by the adversary, the data messages sent from the MGCC to the local controller can be intercepted, decrypted, falsified, re-encrypted, and re-sent to the local controller by the adversary without being detected. A malicious control signal can directly lead to fateful consequences.

A local DER can store keys in a classical computer memory as the keys generated are purely classical bit strings. Any key storage techniques feasible for storing classical keys can be used to store keys generated by a QKD system. For instance, a common way is to encrypt keys via a password such that the keys will not be disclosed.

C. The KPS Strategy

The idea of the KPS strategy is as follows: The MGCC establishes multiple quantum channels with local controllers and uses separate key pools to store keys. Key pools can share keys with each other, meaning that, when the number of key bits in one key pool is below a pre-determined threshold, a certain number of key bits can be shared from other key pools.

An example of the KPS strategy is illustrated in Fig. 4, where two quantum channels are established between the MGCC and two local controllers. When the number of key bits in key pool #1 is lower than a threshold, for instance, a string of key bits is extracted from key pool #2 by the MGCC (represented in ① in Fig. 4). This key bit string is then used as plaintext (represented in ② in Fig. 4), encrypted by the MGCC via a key extracted from key pool #1 (note that there are still some key bits left in key pool #1), and sent to local controller #1. Local controller #1 uses the same key from key pool #1 to decrypt the received message and obtains the key bit string (represented in ③ in Fig. 4). In this way, a string of key bits is transferred from key pool #2 and is securely shared between the MGCC and local controller #1. Although this distribution of keys through AES loses information-theoretic security, it is still better than relying on public key systems, because, as mentioned, AES is considered quantum-secure as long as the key used for the encryption is secure [30]. Note that, unlike an alternative approach employing AES keys for actual data transmission (changing the key every n seconds), our KPS system has the advantage that the information-theoretic OTP may be used up until the last 128 or 256 bits are available maximizing the security of the overall system (switching to computational security only as a last-resort).

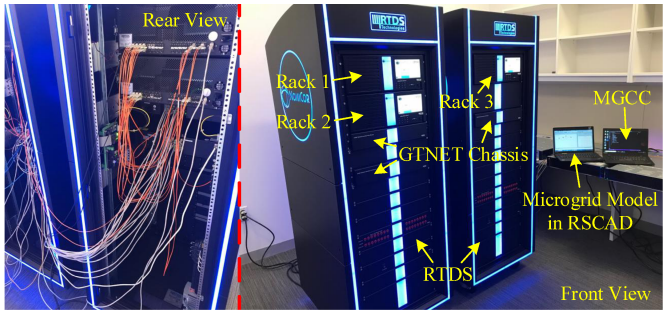


Fig. 5. Testbed setup for a quantum-secure microgrid in RTDS environment.

Overhead analysis: The communication and computation overheads of our KPS strategy are negligible. Assuming the microgrid control signals with a total size of 200k bits that need to be transmitted within 20 seconds, then 200k bits of quantum keys are used to encrypt the data. The required bandwidth for transmitting those key bits from the MGCC to a local controller is therefore only 10 Kbps, which is far less than the link capacity of a common switch (i.e., 1 Gbps). On the other hand, practical encryption schemes such as 128-bit AES can be utilized to transmit quantum keys, where only a few key bits are consumed for encrypting a large number of bits (e.g., 128 bits for a 1500-byte packet). The processing time of the 128-bit AES encryption with the current computing hardware is small. A commercial server with four cores could process AES data with a speed up to 2,804 MB/s [31].

IV. Quantum-Secure Microgrid Test Environment

A. High-Level Design

The test environment is illustrated in Fig. 5. Specifically, the microgrid model 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 our simulation, rack 2 is utilized to simulate the microgrid model in real-time, where the four cores in that rack (running at 3.5 GHz) are sufficient to provide high fidelity for test results in this paper.

The measurements from the RTDS simulator are transmitted through a GTNETx2 card and sent to the MGCC via a communication network. The GTNETx2 card can either receive data from the RTDS and send it to external equipment, or it can receive data from the network and send it back to the RTDS, depending on whether the GTNETx2 card was designed to be in sending or receiving mode. The MGCC runs on a remote server, which can receive load measurements from and send signals back to RTDS with a 1 Gbps Ethernet connection.

The high-level design of the testbed is illustrated in Fig. 6. Two GENETx2 cards are utilized for the purpose of network communication. It should be noted that, although only one quantum channel is established in this case, the principle can be easily extended to cases with multiple quantum channels. GTNETx2 card #2 is used to transmit data from the RTDS to the MGCC, which models the classical communication (represented in ① in Fig. 6) in real-time, i.e., collecting load

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2020.3011071, IEEE Transactions on Power Systems

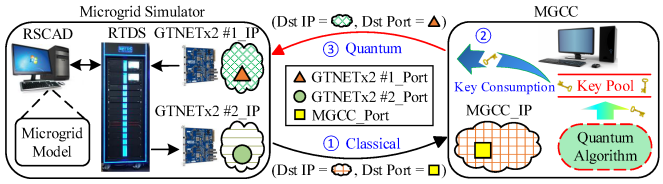


Fig. 6. High-level design of the quantum-secure microgrid testbed.

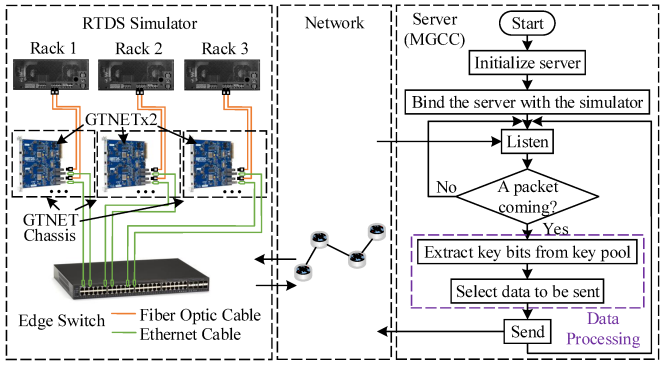


Fig. 7. The network connection of key components in the RTDS simulator and a flow chart of the algorithm running in the MGCC.

measurements to MGCC as shown in Fig. 2. When the data is received by the MGCC, an analysis of the data is conducted, and proper control signals are sent to the local controller. Before a control signal is sent out, a key with the same length is extracted from the key pool. This process (represented in ② in Fig. 6) succeeds only when there are enough key bits.

GTNETx2 card #1 is utilized to receive signals from the MGCC (represented in ③ in Fig. 6) and transfer them to the RTDS. The simulation results with the updated control signals are demonstrated in RSCAD. Note that the QKD system is modeled using the QKD simulator in Fig. 1. Keys are continuously generated by the QKD algorithm, and are stored in a key pool. This real-time communication between the RTDS microgrid simulator and the MGCC using the QKD algorithm is the salient feature of this testbed.

B. QKD-Based Microgrid Communication Network

The network connection of key components in the RTDS simulator and a flow chart of the algorithm running in the MGCC are illustrated in Fig. 7. As shown on the left side of Fig. 7, each RTDS rack is connected to one or more GTNETx2 cards using fiber optic cables. All the GTNETx2 cards are connected with an edge switch through Ethernet cables to transmit and receive data over the network. The User Datagram Protocol (UDP) is used in our simulation.

From the MGCC side, as shown on the right side of Fig. 7, the server enters the *listening* mode after being connected to the simulator. At this stage, the server is receiving any UDP packet whose destination IP and port match those of the server, respectively. Once a packet arrives, a quantum key with the same length of the received data, i.e., 64 bits in this paper, is extracted from the key pool, and corresponding control signals are generated. The server then enters the *sending* mode and starts to send out control signals whose destination IP and port are the IP and port of GTNETx2 card #1 in the RTDS simulator (see Fig. 6), respectively. After controller signals are sent out, the server goes back to the *listening* mode.

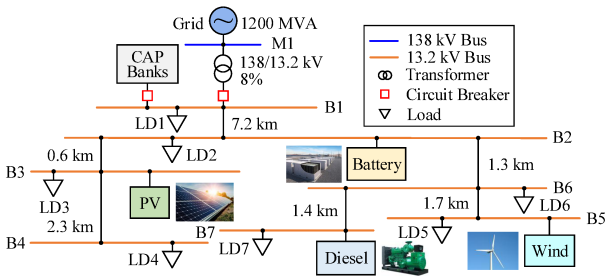


Fig. 8. One-line diagram of the microgrid model.

C. Microgrid Modeling and Simulation

A typical microgrid system shown in Fig. 8 is used to evaluate the performance of the QKD-enabled quantum-secure microgrid in this study. This system is based on a medium-voltage microgrid from [32] with a battery and communication channels added. The buses within the microgrid are rated at 13.2 kV, and the microgrid is connected to the 138 kV main grid through a 138/13.2 kV transformer and a circuit breaker. The microgrid can operate either in islanded mode or in grid-connected mode depending on the state of the circuit breaker. The transformer is $\Delta - Y$ connected and rated at 25 MVA with a 8% impedance.

The DERs in the microgrid include a 5.5 MVA diesel generator, a 1.74 MW PV system, and a 2 MW doubly-fed induction generator wind turbine system. The diesel generator uses the droop control to regulate the microgrid frequency in islanded operation and to provide real and reactive powers in both grid-connected and islanded modes. The PV system and wind turbine both use the MPPT control to maximize their power outputs. Three switched capacitors are connected at bus 1 to facilitate voltage synchronization in the microgrid.

A lithium-ion battery storage is further connected at bus 2 to provide a backup power supply and store extra energy when the microgrid is in islanded operation. The battery model consists of 250 stacks connected in parallel with each one having 250 cells in series. A single cell has a capacity of 0.85 AH, and the initial state of charge in a single cell is set at 85%. 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 the MGCC via a communication channel. The initial values of the real and reactive power references are both set at zero.

The resistance and inductance of a unit length of the lines in the microgrid are 0.2322 Ω/km and 2.355×10^{-3} H/km, respectively, and the lengths of the lines are given in Fig. 8. The power loads at different buses are given in Table II. For more details on the microgrid, readers are referred to [32].

V. Experimental Results

In this section, we evaluate the performance of the QKD-based microgrid with our testbed. This section is organized into two studies. The first study is the single-key-pool scenario where a single key pool is established between the MGCC and the local P-Q controller for the battery in Fig. 8. We

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2020.3011071, IEEE Transactions on Power Systems

TABLE II
POWER LOADS AT DIFFERENT BUSES IN FIG. 8

Load	Phase A KVA	Phase B KVA	Phase C KVA	Power Factor
LD 1	506	506	506	0.9
LD 2	367	367	367	0.95
LD 3	344	344	344	0.9
LD 4	356	356	356	0.9
LD 5	325	625	100	0.95
LD 6	125	725	300	0.95
LD 7	275	625	150	0.95

demonstrate the impact of data transmission speed, effectiveness of QKD-enabled communication, performance of QKD-enabled microgrid when quantum keys are exhausted, impact of QKD on microgrid real-time operations, and performance of quantum key generation speed under different conditions. In the second study, two key pools are established where we first validate the efficacy of the KPS strategy and then present a comparison of two different QKD protocols.

A. Study 1: Single-Key-Pool Scenario

To model the dynamic characteristics of loads, a time-varying load with the magnitude of 2 MW and the frequency of 0.05 Hz is added to Load 2 (see Fig. 8). The value of the varying load is continuously sent from the RTDS to the remote server with a user-specified frequency. When the remote server receives the data packet, it calculates the value of P^*_{ref} and sends it to the local P-Q controller for the battery at bus 2, such that the total power generation matches the sum of loads. The value of Q^*_{ref} is fixed at zero in this study.

1) Case 1: Impact of Data Transmission Speed: Data transmission speed is a critical statistic in a QKD-based microgrid. 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.

We use Wireshark, an open-source packet analyzer, to monitor traffic in the system. Specifically, two types of packets are captured: the packets sent from the RTDS (GTNETx2 #2) to the MGCC and from the MGCC to the RTDS (GTNETx2 #1). The transmission speeds of the two types of packets are set as the same. Namely, once there is a packet received by the MGCC, a packet is sent out from the MGCC.

The impact of the data transmission speed is illustrated in Fig. 9, where the fiber length L (between the MGCC and the local controller) is set at 50 km. The other parameters are the same as those in Table I. Each packet sent from the MGCC to the RTDS consists of 64 binary bits, meaning that 64 key bits are consumed from the key pool when a packet is sent out.

From Fig. 9, it can be observed that:

- The data transmission speed has a large impact on the QKD-based microgrid. With the setting in Fig. 9, a speed larger than 20 packets/second will lead to the exhaustion of key bits in the key pool.
- The larger the data transmission speed is, the sooner the quantum generated key will be consumed. With the setting in Fig. 9, for a speed of 40 packets/second, the exhaustion lasts around 100 seconds within the key generation period. This long shortage can cause serious damage to microgrid operations, as there is no key in the key pool for the encryption and authentication of data messages.

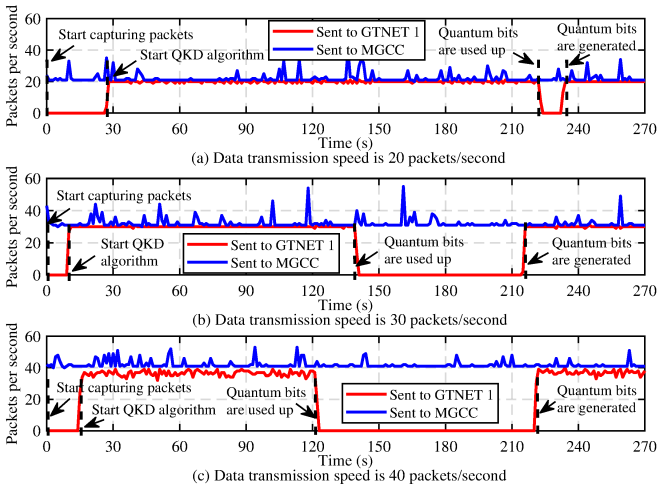


Fig. 9. Traffic monitoring under different data transmission speeds.

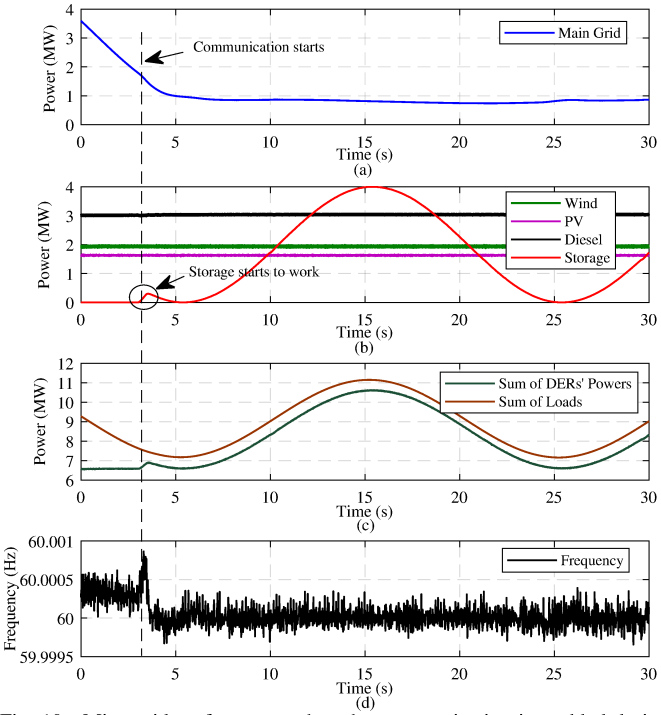


Fig. 10. Microgrid performance when the communication is enabled during grid-connected mode. (a) Power from main grid. (b) Output power from each DER. (c) The sums of DERs' powers and loads. (d) System frequency.

2) Case 2: Effectiveness of QKD-Enabled Communication: Fig. 10 illustrates the microgrid performance before and after the communication starts to work during grid-connected mode. Before time $t = 3$ s, the communication is disabled. The balance of the total power generation and the sum of loads is mainly achieved by the main grid. When the communication is enabled at time $t = 3$ s, the storage starts to respond to the change of loads and the balance can be well-maintained. Similar results can be observed in Fig. 11 where microgrid switches from grid-connected mode to the islanding mode.

3) Case 3: Performance of QKD-Enabled Microgrid When Quantum Keys Are Exhausted: A QKD system mainly poses two impacts on microgrid operations: 1) keys generated by the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2020.3011071, IEEE Transactions on Power Systems

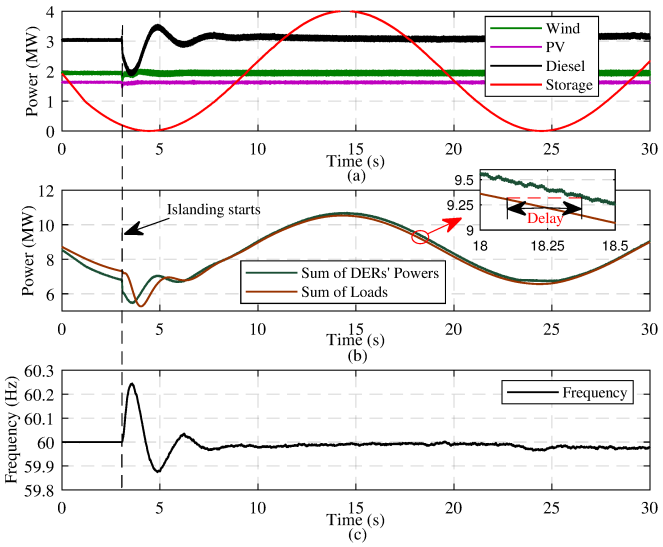


Fig. 11. Microgrid performance during islanding mode. (a) Power from each DER. (b) The sums of DERs' powers and loads. (c) System frequency.

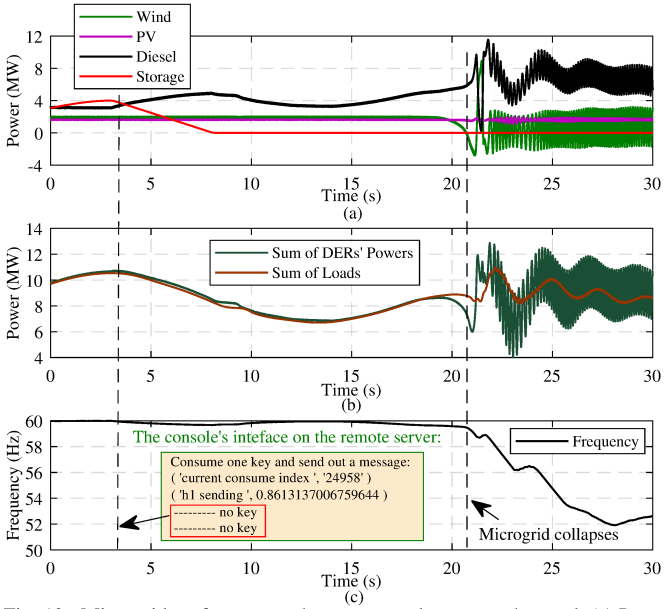


Fig. 12. Microgrid performance when quantum keys are exhausted. (a) Power from each DER. (b) The sums of DERs' powers and loads. (c) Frequency.

QKD system are exhausted, and 2) the delay introduced by a QKD system affects the real-time data transmission.

In this case, the first impact is evaluated. Fig. 12 demonstrates the microgrid performance when keys are exhausted at time $t = 3$ s during the islanding mode. It can be seen that the system eventually collapses at time $t = 21$ s. The console's interface on the remote server is shown in Fig. 12 (c).

4) Case 4: Impact of QKD on Microgrid Real-Time Operations: A QKD system consists of a quantum channel and a classical one. The classical channel is shared by quantum key generation and normal data transmission. Adding a QKD system into microgrid therefore inevitably introduces more traffics into the classical channel. In this case, the impact of the delay caused by a QKD system is evaluated.

Specifically, we manually add a delay in the QKD algorithm on the remote server, meaning when a data packet arrives, the control signal will be sent out with a certain time delay. Fig. 13 gives the output power of each DER when the delay is 1 s.

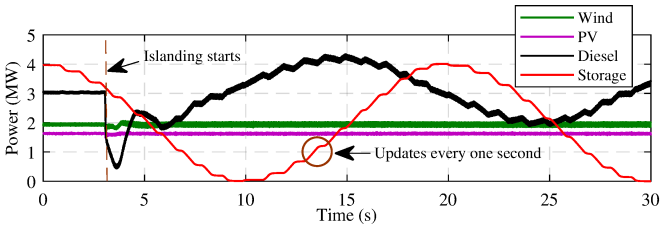


Fig. 13. The output power from each DER when the delay is 1 s before and after microgrid islands.

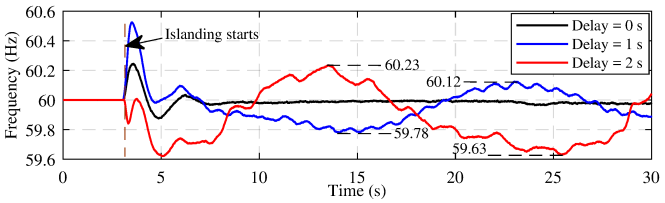


Fig. 14. Comparison results of system frequencies with different delays.

It can be seen that, the storage updates every one second, and due to the delay, the output of the diesel varies significantly. The comparison of the impacts caused by different delays is given in Fig. 14, where the delay is set to be 0 s, 1 s, and 2 s, respectively. It can be seen that the larger the delay is, the more unstable the system will be. An even larger delay, i.e., 3 s, directly leads to collapse of the microgrid during islanding mode as shown in Fig. 15.

5) Case 5: Evaluation of Quantum Key Generation Speed under Different Fiber Lengths and Noise Levels: The speed of quantum key generation determines the maximum data transmission speed in a QKD-based microgrid. The larger the key generation speed, the higher the maximum data transmission speed. However, it was unclear which levels of key generation speed the QKD system could provide for the microgrid under different conditions. In this case, an evaluation of key generation speed under different fiber lengths Ls and noise levels e_{mis}s, is provided. The noise can be either natural or caused by an adversary. A strong attack on the quantum optic equipment is simulated by setting a large e_{mis}.

The real-time simulation results are given in Fig. 16, where L is set from 1 km to 80 km, e_{mis} is set from 5×10^{-4} to 9×10^{-4} with a step of 1×10^{-4}, and each packet consists of 64 binary bits. The other parameters are the same as those in Table I. Key generation speed is calculated as the fraction of the generated key's size ℓ (see (15)) and the time required.

It can be observed that:

- A small L exhibits great superiority over a large L under the same e_{mis}, which gives valuable insights that the MGCC and the local controller should be close to each other in a QKD-based microgrid.
- The key generation speed is sufficient with a small L and a small e_{mis}. But, it decreases dramatically when e_{mis} increases. A proper strategy therefore has to be carried out to improve the system's cyberattack resilience.
- Importantly, Fig. 16 gives valuable resources on which levels the data transmission speed should be set at under different Ls and e_{mis}s. With the setting in Fig. 16, any data transmission speed that is below the corresponding curve (with regards to a certain e_{mis}) in Fig. 16, will have sufficient key bits in the key pool under that e_{mis}.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRS.2020.3011071, IEEE Transactions on Power Systems

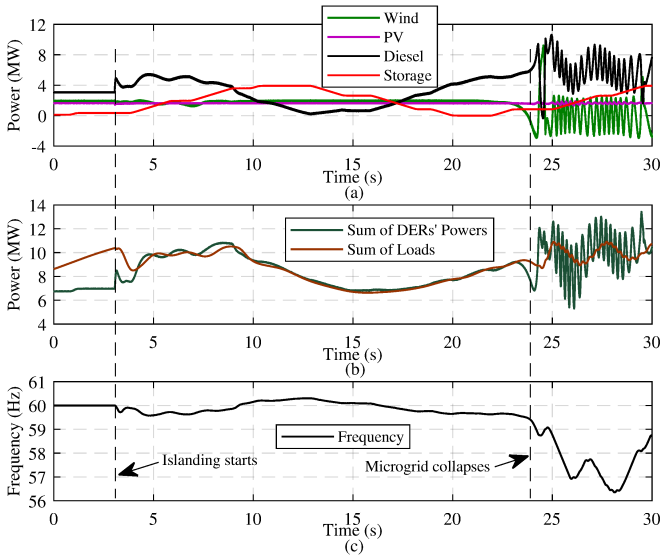


Fig. 15. Microgrid performance when the delay is 3 s before and after microgrid islands. (a) Output power from each DER. (b) The sums of DERs' powers and loads. (c) System frequency.

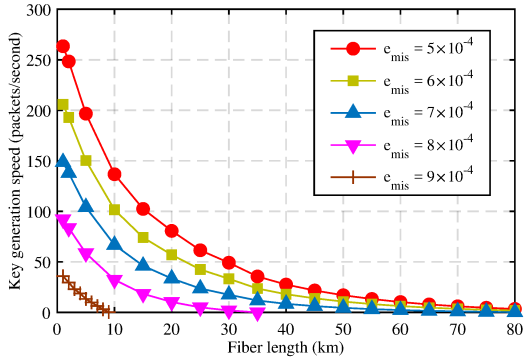


Fig. 16. Quantum key generation speeds under different Ls and e_{mis}s.

6) Case 6: Evaluation of Quantum Key Generation Speed under Different Receiver's Detection Efficiencies: The detection efficiency of the receiver, η_{Bob}, is critical in a QKD system. Detection efficiency refers to the probability that the receiver can successfully detect the photons, which is largely determined by the quality of the detection devices.

The impact of η_{Bob} is evaluated in our real-time testbed. The results are illustrated in Fig. 17, where L is set at 5 km, 10 km, and 20 km, respectively; e_{mis} is set at 6×10^{-4}, 7×10^{-4}, and 8×10^{-4}, respectively; and η_{Bob} is from 10% to 50% with a step of 5%. The other parameters are the same as in Table I.

It can be seen that η_{Bob} has a significant impact on key generation speed. With a given L and a given e_{mis}, a small increase of η_{Bob} results in a great improvement of the speed. This indicates that it is worth improving the quality of detection devices in a QKD-based microgrid.

B. Study 2: Multiple-Key-Pool Scenario

1) Case 7: Effectiveness of The KPS Strategy: The performance of the presented KPS strategy is evaluated using our testbed. In this test case, two key pools are established in the quantum algorithm, and each stores its quantum key bits separately. The QKD parameters for the two key pools are set as the same except that e_{mis} for key pool #1 is 8×10^{-4} to

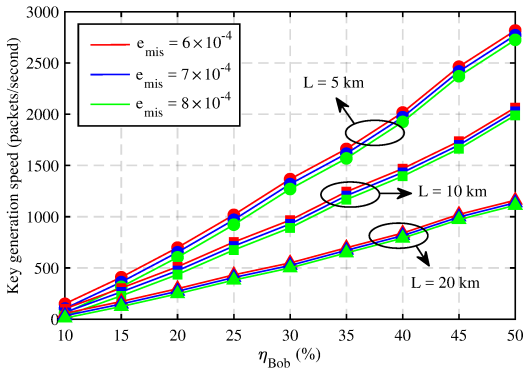


Fig. 17. Quantum key generation speeds under different η_{Bob}s.

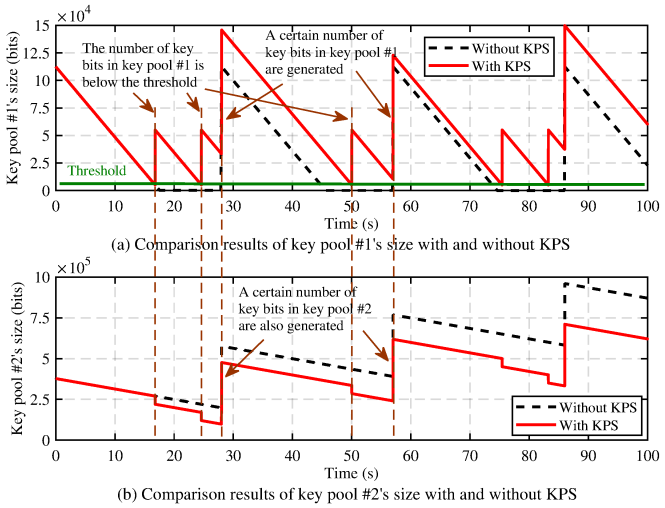


Fig. 18. Comparison results of the numbers of key bits in key pools #1 and #2 with and without KPS.

simulate a strong attack, while e_{mis} for key pool #2 is 5×10^{-4} for a weak attack. The data transmission speed is set at 100 packets/second, where each packet consists of 64 bits.

For the KPS strategy, the threshold is set at 5,000 bits for key pool #1, meaning that once the number of key bits in key pool #1 is lower than 5,000, a given number (which is set at 20,000) of key bits will be shared from key pool #2.

The comparison results of the numbers of key bits in key pools #1 and #2 with and without KPS are illustrated in Fig. 18. It can be observed that:

- Without KPS, there is a shortage of key bits in key pool #1. For instance, at time $t = 17.56$ s, the key bits in key pool #1 are used up (see the black dashed line in Fig. 18 (a)), and the shortage lasts around 10.5 s until a certain number of key bits are generated. Meanwhile, the key bits in key pool #2 do not have shortage issues (see the black dashed line in Fig. 18 (b)).
- With KPS, the shortage issues of key pool #1 are well addressed. At time $t = 16.79$ s, the number of key bits in key pool #1 is below the threshold, and immediately 20,000 key bits are added (see the red solid line in Fig. 18 (a)). Meanwhile, 20,000 key bits are deducted from key pool #2 (see the red solid line in Fig. 18 (b)). But this does not affect the normal operation of key pool #2, as the minimum number of key bits in key pool #2 is still above the threshold.

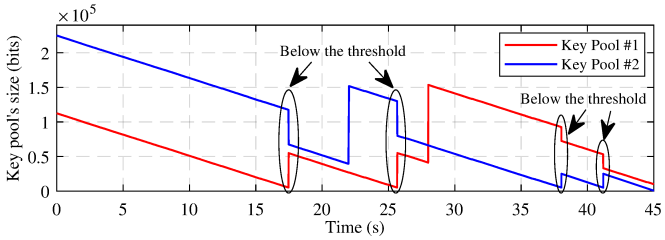


Fig. 19. The effectiveness of the KPS strategy when both key pools are under strong attacks.

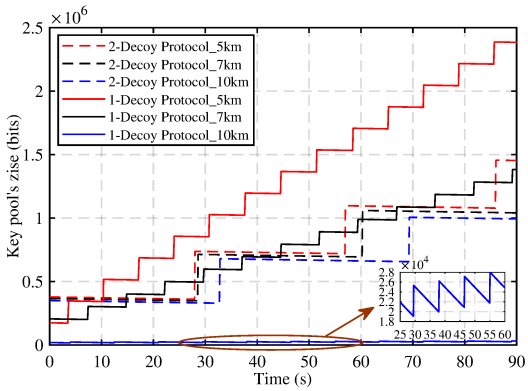


Fig. 20. Comparison results of the 2-decoy state protocol and 1-decoy state protocol with different fiber lengths using the testbed.

2) Case 8: Effectiveness of The KPS Strategy When Both Key Pools Are Attacked: In this test case, both key pools are under strong attacks, i.e., e_{mis}s for key pools #1 and #2 are both set at 8×10^{-4}. The initial number of bits in key pool #2 is twice that in key pool #1. Other settings are the same as in Case 7. Fig. 19 illustrates the effectiveness of the KPS strategy. It can be seen that, 1) without KPS, the key bits in key pool #1 are used up at time $t = 17.56$ s; and 2) with KPS, the key bits in the two key pools are used up at around $t = 45$ s. The KPS strategy maximizes the usage of key bits in each key pool, and greatly extends the time when key bits in any key pool are exhausted.

3) Case 9: Comparison of Different QKD Protocols: In this test case, we use the testbed to compare the performances of two different QKD protocols, namely the 2-decoy state protocol (as described above in this paper) and the 1-decoy state protocol (as presented in [33]). Specifically, key pool #1 stores key bits generated by the 2-decoy state protocol and key pool #2 stores key bits generated by the 1-decoy state protocol. The fiber length is set at 5 km, 7 km, and 10 km, respectively. Other parameters are the same for the two protocols. The comparison results are given in Fig. 20.

It can be observed that the 1-decoy state protocol is more sensitive to the fiber length than the 2-decoy state protocol, and outperforms the 2-decoy state protocol when the fiber length is small. This is reasonable, as the 1-decoy state protocol is more efficient in that there aren't any "vacuum" decoys (which are useless for key-rates); however, due to the lack of vacuum decoys, it's more sensitive to noise and loss.

VI. Conclusion

This paper presents a real-time QKD-enabled microgrid testbed implemented in RTDS. This testbed provides a realistic cyber-physical testing environment in real time with a simulated QKD algorithm integrated. This is an important step towards constructing a real QKD system in microgrid in practice. With this testbed, more research work could be done in the future. Some examples include exploiting the feasibility of more advanced and practical QKD protocols for microgrids, evaluating the QKD-enabled microgrid's performance under more scenarios, and developing methods to further enhance the cyberattack resilience of the QKD-enabled microgrid.

References

[1] M. Farrokhabadi, C. A. Canizares, J. W. Simpson-Porco, E. Nasr, L. Fan, P. Mendoza-Araya, R. Tonkoski, U. Tamrakar, N. D. Hatziargyriou, D. Lagos *et al.*, "Microgrid stability definitions, analysis, and examples," *IEEE Transactions on Power Systems*, 2019.

[2] F. Feng and P. Zhang, "Enhanced microgrid power flow incorporating hierarchical control," *IEEE Transactions on Power Systems*, vol. 35, no. 3, pp. 2463–2466, 2020.

[3] C. W. Ten, C. C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, 2008.

[4] R. Van Meter, *Quantum networking*. John Wiley & Sons, 2014.

[5] S. Banik, A. Bogdanov, and F. Regazzoni, "Compact circuits for combined AES encryption/decryption," *Journal of Cryptographic Engineering*, vol. 9, no. 1, pp. 69–83, 2019.

[6] M. D. Liskov, J. D. Guttman, J. D. Ramsdell, P. D. Rowe, and F. J. Thayer, "Enrich-by-need protocol analysis for Diffie-Hellman," in *Foundations of Security, Protocols, and Equational Reasoning*. Springer, 2019, pp. 135–155.

[7] S. C. Coutinho, *The mathematics of ciphers: number theory and RSA cryptography*. AK Peters/CRC Press, 1999.

[8] K. S. McCurley, "The discrete logarithm problem," in *AMS Proc. Symp. Appl. Math*, vol. 42, 1990, pp. 49–74.

[9] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. IEEE, 1994, pp. 124–134.

[10] S. Y. Yan, "Logarithm based cryptography," in *Cybercryptography: Applicable Cryptography for Cyberspace Security*. Springer, 2019, pp. 287–341.

[11] P. D. M. Lara, D. A. Maldonado-Ruiz, S. D. A. Díaz *et al.*, "Trends on computer security: Cryptography, user authentication, denial of service and intrusion detection," *arXiv preprint arXiv:1903.08052*, 2019.

[12] G. Fano and S. Blinder, "Quantum chemistry on a quantum computer," in *Mathematical Physics in Theoretical Chemistry*. Elsevier, 2019, pp. 377–400.

[13] K. Wright, K. Beck, S. Debnath, J. Amini, Y. Nam, N. Grzesiak, J.-S. Chen, N. Pisenti, M. Chmielewski, C. Collins *et al.*, "Benchmarking an 11-qubit quantum computer," *arXiv preprint arXiv:1903.08181*, 2019.

[14] T. Kovachy, P. Asenbaum, C. Overstreet, C. Donnelly, S. Dickerson, A. Sugarbaker, J. Hogan, and M. Kasevich, "Quantum superposition at the half-metre scale," *Nature*, vol. 528, no. 7583, p. 530, 2015.

[15] I. Bengtsson and K. Życzkowski, *Geometry of quantum states: An introduction to quantum entanglement*. Cambridge university press, 2017.

[16] R. Orús, S. Mugel, and E. Lizaso, "Quantum computing for finance: Overview and prospects," *Reviews in Physics*, p. 100028, 2019.

[17] C. Hong, J. Jang, J. Heo, and H.-J. Yang, "Quantum digital signature in a network," *Quantum Information Processing*, vol. 19, no. 1, p. 18, 2020.

[18] A. Bani-Hani, M. Majdalweieh, and A. AlShamsi, "Online authentication methods used in banks and attacks against these methods," *Procedia Computer Science*, vol. 151, pp. 1052–1059, 2019.

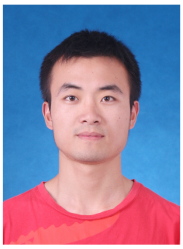
[19] S. Cobourne *et al.*, "Quantum key distribution protocols and applications," *Surrey TW20 0EX, England*, 2011.

[20] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.

[21] L. Wang, Y. Qin, Z. Tang, and P. Zhang, "Software-defined microgrid control: The genesis of decoupled cyber-physical microgrids," *IEEE Open Access Journal of Power and Energy*, vol. 7, pp. 173–182, 2020.

[22] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh, and R. Jin, "Enabling resilient microgrid through programmable network," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2826–2836, 2017.

[23] B. Trauzettel, D. V. Bulaev, D. Loss, and G. Burkard, "Spin qubits in graphene quantum dots," *Nature Physics*, vol. 3, no. 3, p. 192, 2007.
[24] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *arXiv preprint arXiv:1906.01645*, 2019.
[25] 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.
[26] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, no. 6, p. 063027, 2010.
[27] 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.
[28] V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New Journal of Physics*, vol. 11, no. 6, p. 065003, 2009.
[29] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.
[30] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2016.
[31] "AES-NI SSL Performance: A study of AES-NI acceleration using LibreSSL, OpenSSL," [Online available]: https://calomel.org/aesni_ssl_performance.html.
[32] N. Onyinyechi, "Real time simulation of a microgrid system with distributed energy resources," 2015.
[33] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," *Applied Physics Letters*, vol. 112, no. 17, p. 171104, 2018.



Zefan Tang (S'15) received the B.S. degree in mechanical engineering from Zhejiang University, Zhejiang, China, in 2014, and the M.S. degree in electrical and computer engineering from the University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai Jiao Tong University, Shanghai, China, in 2017. He is currently working toward the Ph.D. degree in electrical engineering with Stony Brook University, Stony Brook, NY, USA. His current research interests include microgrids, quantum security, quantum key distribution, quantum networking, and cyber physical security for electric power networks.

Yanyuan Qin (S'15) received the B.S. degree in Automation from the Nanjing University of Aeronautics and Astronautics, China, in 2011, and the M.S. degree in Control Science and Engineering from Shanghai Jiao Tong University, China, in 2014. He is currently pursuing the Ph.D. degree with the Computer Science and Engineering Department, University of Connecticut. His research interests are in software defined networking and wireless networks.

Zimin Jiang (S'16) received the B.S. degree in electrical engineering from Shandong University, Jinan, China, in 2015, where he is working toward the Ph.D. degree at the School of Electrical Engineering. He is currently a Research Support Specialist with the Department of Electrical and Computer Engineering, Stony Brook University, New York, USA. His main research interests are power system stability and control, microgrids, cyber security, renewable energy integration to power system and grid connection testing.

Walter O. Krawec received a Ph.D. in Computer Science from Stevens Institute of Technology, Hoboken NJ USA in 2015 and an MA in Mathematics from the University at Albany, SUNY in 2010. He is currently an Assistant Professor of Computer Science and Engineering at the University of Connecticut, Storrs USA. His research interests are primarily in quantum cryptography and quantum information theory.

Peng Zhang (M'07−SM'10) received the Ph.D. degree in electrical engineering from the University of British Columbia, Vancouver, BC, Canada, in 2009. He is a SUNY Empire Innovation Professor at Stony Brook University, New York. He has a joint appointment at Brookhaven National Laboratory as a Staff Scientist. He was a System Planning Engineer at BC Hydro and Power Authority, Vancouver. His research interests include networked microgrids, power system stability and control, formal methods and reachability analysis, quantum security, quantum computing, and cyber security.
Dr. Zhang is an individual member of CIGRÉ. He is an Editor for the IEEE Transactions on Power Systems, the IEEE Transactions on Sustainable Energy and the IEEE Power and Energy Society Letters, and an Associate Editor for the IEEE Journal of Oceanic Engineering.