Upgrading the Cyber Layer of Power Systems to Support Semi-Quantum Key Distribution

Mariam Gado*, Muhammad Ismail*, and Walter O. Krawec†
*Department of Computer Science, Tennessee Technological University, Tennessee, USA
†Department of Computer Science, University of Connecticut, Connecticut, USA
Emails: {mmgado42, mismail}@tntech.edu and walter.krawec@uconn.edu

***Abstract*—This paper investigates upgrading the classical cyber layer of power systems to support semi-quantum key distribution. With such an upgrade, only a few cyber nodes are required to have full quantum capabilities (i.e., generation, transmission, and measurement of qubits) while the rest of the cyber nodes are required to have limited quantum capabilities (i.e., transmission and measurement of qubits). As a result, unconditionally secure keys can be shared between the control center and the power substations to encrypt and decrypt critical measurement and control data. We study the problem of allocating the minimum number of quantum servers (i.e., nodes with full quantum capabilities) on the pre-existing cyber layer to satisfy the required key distribution rate in an attacker's presence. Due to the associated computational complexity, we propose a greedy algorithm to solve the allocation problem. We examine the proposed allocation algorithm on the cyber layer of the IEEE-14 bus test system. Our results demonstrate that the target key rate can be satisfied at different attack levels.**

***Index Terms*—Quantum key distribution, semi-QKD, smart grid, power system, and secret key generation.**

I. Introduction

One effective way to secure power systems against false data and command injection attacks can be attained by encryption, e.g., using the advanced encryption system (AES). In this context, key-sharing mechanisms are used to exchange secret keys between the communicating cyber nodes to encrypt and decrypt the data. Commonly used key-sharing mechanisms include Rivest-Shamir-Adleman (RSA) [1] and Diffie-Hellman key exchange [2], which depends on the difficulty of solving specific mathematical problems [3]. These problems are hard to solve using classical computers, however, quantum computers have the capability to break them and reveal the shared secret keys, which will lead to security breaches [4]. While post-quantum key exchange methods provide robust security against both classical and quantum adversaries, under computational assumptions, QKD and S-QKD solutions remain valuable as they offer the unique advantage of providing unconditional security, based on the laws of quantum mechanics, for key distribution. This makes exploring upgrade solutions to the cyber-layer of the power system to support QKD and S-QKD solutions particularly important where the consequences of a breach in such a critical infrastructure could lead to large scale blackouts, hence, posing not only significant financial losses but also grave threats to human lives.

This work was supported by NSF award #2220346.

A. Related Works

To mitigate cyber-attacks on its power system, recent reports indicated that China uses a satellite quantum network to provide secure communication between the power grid of Fujian and the national emergency command center in Bejing [5]. Furthermore, a few recent works studied the use of quantum key distribution (QKD) to distribute secret keys and use them to encrypt and authenticate data in power systems [6]–[8]. Several QKD protocols have been proposed in the literature such as the BB84 [9] and the B92 [10] protocols. Unlike QKD, semi-QKD (S-QKD) protocols have been proposed to enable key distribution between nodes that do not have full quantum capabilities [11], [12]. Hence, in S-QKD, a few nodes are able to generate, transmit, and measure quantum bits (qubits), while the rest of the nodes offer limited quantum capabilities, e.g., transmit and measure qubits. Thus, S-QKD presents a cost-effective means for near-term deployment compared to QKD. In literature, several works proposed various S-QKD protocols [12]. The S-QKD algorithm in [13] can be applied practically and it is robust against the noiseless attacks; [14] analyzed practical collective attacks, while the rest of the general attacks mitigation is still an open problem.

B. Limitations, Challenges, and Contributions

The existing few works on quantum-secure power grids suffer from the following limitations: (a) the considered systems represent a small number of closely located nodes, which do not guarantee a scalable solution that covers a transmission power system spanning tens to hundreds of kilometers, and (b) the existing solutions are based on QKD, which requires a cyber layer with full quantum capabilities, hence, increasing the upgrade cost of the existing classical cyber layers and hinders the adoption of such solutions in the near term.

Hence, there is a need for a cost-effective solution that upgrades the classical cyber layer to support sharing unconditionally secure keys in large-scale transmission power systems. Toward a near-term solution, the following features are needed: (a) for cost-effectiveness, the proposed solution should require a minimum number of cyber nodes to have full

quantum capabilities (i.e., generation, manipulation, transmission, and measurement of qubits) while the rest of the cyber nodes have limited quantum capabilities (i.e., measurement and transmission of qubits), and (b) to be applicable to large-scale transmission power system, the target key generation/distribution rate should be satisfied over long distances.

To address the aforementioned limitations and provide a near term cost-effective solution, we carried out the following:

- We formulate a quantum server allocation problem that upgrades the classical cyber layer of a transmission power system to support S-QKD. The formulated problem upgrades the minimum number of cyber nodes to be full quantum nodes while satisfying the target key rate in the presence of an attacker. The problem is formulated as a binary program. Then, we propose a greedy allocation algorithm to overcome the computational complexity.
- We examined the proposed algorithm on the cyber layer of the IEEE 14-bus test system. Our results demonstrate that the target key distribution rate can be satisfied at different attack levels.

The rest of this paper is organized as follows. Section II gives a brief background about quantum systems and S-QKD. Section III presents the system model. Section IV covers the problem formulation and solution. Section V presents the numerical results. Conclusions are made in Section VI.

II. Preliminaries

This section reviews quantum systems and S-QKD.

A. Quantum States and Measurements

Qubits are the basic unit of information in quantum systems. A qubit can be represented by a state vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. While classical bits can exist in one state at a time (0 or 1), a qubit can be in a superposition of both states.

In what follows, we describe S-QKD systems where photons are used to represent qubits and the polarization of the photon corresponds to a quantum state. We consider two main bases, namely, the Z basis (i.e., horizontal and vertical polarization) and the X basis (i.e., diagonal polarization). Formally, the Z basis corresponds to $|0\rangle$ and $|1\rangle$, and the X basis corresponds to $|+\rangle$ and $|-\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. If both sender and receiver use the same basis to encode and decode the qubit, information will be received successfully, else, information may not be received correctly.

In the Z basis, measuring qubits $|0\rangle$ and $|1\rangle$ result in classical bits 0 and 1, respectively. In the X basis, measuring qubits $|+\rangle$ and $|-\rangle$ result in classical bits 0 and 1, respectively.

B. Semi-Quantum Key Distribution Protocol

This paper adopts the S-QKD protocol of [13] as its security was proven against a set of practical collective attacks along with the previously proven noiseless attacks in [14]. In [13], Bob represents a full quantum node that can generate, transmit, and measure qubits, while Alice is a limited (semi) quantum node that can only measure in the Z basis and transmit qubits. The S-QKD protocol can be described as follows:

1) Bob creates and sends a qubit/photon in $|+\rangle$ to Alice.
2) Alice applies randomly one of the following:
   a) Alice transmits back (reflects) all qubits (photons) toward Bob without any measurement. This is considered a testing round.
   b) Alice reflects all photons in the $|0\rangle$ polarization toward Bob and measures all qubits in the $|1\rangle$ polarization. This is considered a raw key round.
   c) Alice reflects all photons in the $|1\rangle$ polarization toward Bob and measures all qubits in the $|0\rangle$ polarization. This is considered a raw key round.
   d) Alice measures all photons without reflecting any toward Bob. This is considered a swap-all round.
3) Bob measures the received qubit (photon) from Alice randomly in the Z or the X bases.

In order to share a secret bit, Alice has to choose 2b) or 2c) and detect no photon at her end, while Bob has to measure in the Z basis. The reader is referred to [13] for more details about the protocol. In this setup, an attacker Eve is assumed between Alice and Bob. Eve can perform no attack or a single attack represented by a noise injection level on the communication between Alice and Bob.

III. System Model

This section describes the physical and cyber layers of the power system and the design requirements.

A. Physical Layer

In its physical layer, the power system consists of a set of generation and load buses (substations) connected by a set of transmission lines. Each power substation is monitored by sensing devices to measure active and reactive powers, three-phase voltages, etc. Also, each substation has a local network that is connected via a communication network (cyber layer) with the control center. The measurements of each substation are shared via the cyber layer with the control center to specify optimal operation strategies, and hence, send command/control signals back to the power substations. Fig. 1 illustrates the physical layer of an IEEE-14 bus test system, which will be used to evaluate the performance of the proposed quantum server allocation algorithm. It should be highlighted that the proposed algorithm is applicable to any system size and the IEEE 14-bus test system is just used as an illustration example.

B. Cyber Layer

The cyber layer consists of a set of routers and links that connect the local networks of the power substations with the control center. Fig. 1 illustrates the cyber layer of the IEEE 14-bus test system based on [15]. As shown in Fig. 1, closely located power substations such as buses 5 and 6 submit their measurements and receive control signals through a common

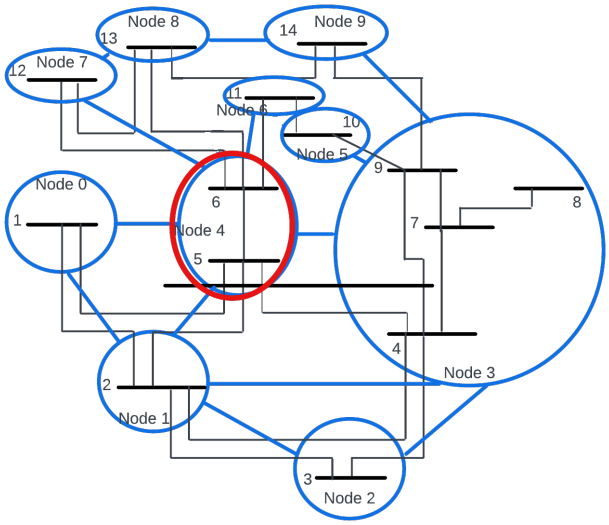

Fig. 1. Top view of the IEEE 14-bus system's physical layer (in black) and cyber layer (in blue). The cyber layer is based on [15]. The highlighted cyber node in red exemplifies a node upgraded into a full quantum server.

router (Node 4), and buses 4, 7, 8, and 9 have a common router (Node 3). Other buses have dedicated routers. As a first step of research, this paper assumes that all the communication links connecting the routers are based on optical fibers.

For the system under consideration, the goal is to identify which of the cyber nodes (in blue) will be upgraded to full quantum servers (Bob) capable of generating, transmitting, and measuring qubits and which will only be equipped with semi-quantum servers (Alice). Full quantum servers will engage with the other nodes to share secret keys. The measurements and control signals going through a given router will be encrypted and decrypted with the shared key between the respective substation and the control station.

C. S-QKD Rate

The optimal number and location of the full quantum servers ensure that the attained key distribution rate $r_{n,n'}$ between a full quantum server at node n and a semi-quantum server at node n' satisfies the minimum required key generation rate $r_{\min}$ in the presence of an attacker E. The attacker disturbs the session between nodes n and n' by noise injection, hence, reducing the attained key rate. The key rate $r_{n,n'}$ in bits per second (bps) can be described as [14]

$$r_{n,n'} = r_n \times M_{n,n'} \times (S(n'|E) - H(n'|n)), \tag{1}$$

where r_n is the source rate in photons per second, which is the rate at which the quantum server at node n (Bob) creates and sends a photon in the $|+\rangle$ state to the semi-quantum server at node n' (Alice). In (1), $M_{n,n'}$ denotes the probability that both nodes n and n' successfully get raw key bits, which is described as [14]

$$M_{n,n'} = 0.5 \times 10^{\frac{-2\alpha l_{n,n'}}{10}}, \tag{2}$$

with α denoting the fiber link attenuation loss per kilometer and $l_{n,n'}$ is the length of the link between nodes n and n' in kilometer. The last term in (1) provides the difference between the Von Neuman entropy between the semi-quantum server at node n' and the attacker, $S(n'|E)$, and the entropy between the quantum server at node n and the semi-quantum server at node n', $H(n'|n)$. To compute $S(n'|E)$ and $H(n'|n)$, Algorithm 1 in [14] is used. Eventually, the key rate $r_{n,n'}$ depends on the source rate, link distance, and attack (noise injection) level.

IV. Allocation of Quantum Servers

In this section, we present the problem formulation to minimize the upgrade cost for an unconditionally secure key sharing within the cyber layer then we present our proposed solution of allocating a minimum number of quantum servers in strategic locations only.

A. Problem Formulation

The cyber layer is modeled as an undirected, connected, weighted, acyclic graph $G(\mathcal{N}, \mathcal{E})$ where $\mathcal{N}$ denotes the set of cyber nodes (routers) and $\mathcal{E}$ denotes the set of cyber edges (fiber links) whose weights are based on the lengths of the links. The allocation problem is to identify the minimum number of nodes $\in \mathcal{N}$ that should be upgraded to a full quantum server such that the attained rates over all edges $\in \mathcal{E}$ are at least $r_{\min}$. Formally, the quantum server allocation problem can be described as

$$\begin{aligned} \min_{x_n} \quad & \sum_{n=1}^{N} x_n \\ \text{s.t.} \quad & r_{i,j} \geq r_{\min} \qquad \forall i \in \hat{\mathcal{N}}, j \in \mathcal{N}/\hat{\mathcal{N}}, \\ & x_n \in \{0, 1\}, \end{aligned} \tag{3}$$

where x_n is a binary allocation decision variable such that $x_n = 1$ indicates that nodes $n \in \mathcal{N}$ should be upgraded to a quantum server, else $x_n = 0$. The first constraint in (3) ensures that the optimal allocation results in a key distribution rate that satisfies the minimum rate requirement $r_{\min}$. The set $\hat{\mathcal{N}}$ includes only the full quantum servers (i.e., with $x_n = 1$).

The allocation problem in (3) is an NP-complete binary program. Hence, we propose a greedy algorithm that solves (3) with a reduced computational complexity.

B. Proposed Greedy Algorithm

The attained key distribution rates in (1) are proportional to the distance between the quantum server and the other nodes in the cyber layer. Since every node in the cyber layer is a candidate for a quantum server upgrade, we first use the Dijkstra algorithm to determine the shortest path and the sum distance between every node n and the rest of the nodes in the cyber layer $\mathcal{N}/n$. Then, we select node n with the least sum

distance to the rest of the nodes $\mathcal{N}/n$ to be a quantum server. Next, we calculate the rates $r_{n,\mathcal{N}/n}$. If all rates satisfy $r_{\min}$, no additional quantum servers are needed. If the target rate $r_{\min}$ is not satisfied, additional quantum servers are allocated close to the rate-deprived nodes (those nodes that cannot be served by the existing server). This is done by using the Dijkstra algorithm to identify the location of an additional quantum server that is closest to the rate-deprived nodes. Specifically, the Dijkstra algorithm is applied and the sum distance from all nodes to the rate-deprived nodes is calculated. Then, the node with the least sum distance is chosen for the additional quantum server. We keep iterating the two steps of selecting nodes as quantum servers and checking the rate constraints until no further quantum servers are needed. Since the selected locations of the quantum server nodes are closest to the rest of the nodes, the effect of the attenuation due to the link distance is minimized. Hence, the minimum number of quantum server nodes that satisfy the target key rate are allocated.

Algorithm 1 summarizes the greedy allocation strategy, where the minimum target key rate $r_{\min}$ and the topology of the cyber layer are provided as inputs. A function **Dijkstra**($\mathcal{N}[i]$) is called to find the shortest path for node i to all the nodes in the cyber layer. The sum distance from node i to all the nodes in the cyber layer is calculated using function call **sumDijkstra**($\mathcal{N}[i]$), which is then stored in the list V. The selected node to be upgraded to a quantum server m is the position in V with the minimum sum distance value. The selected node is stored in a list Q. Then, the key rate is calculated from the server node to all the remaining nodes. For the nodes with a rate less than $r_{\min}$, function **minDijkstra**($\mathcal{N}[j]$) is called to find candidate locations close to these rate-deprived nodes, which are added to the list of quantum servers Q. The output of the algorithm provides a list of nodes to be upgraded to quantum servers Q, which satisfies the target minimum rate $r_{\min}$ for all the remaining nodes in the cyber layer.

The proposed algorithm uses a greedy approach to solve the quantum server allocation problem with reduced computational complexity. The complexity of the algorithm is $O(EN\log(N))$, where E and N are the number of edges and nodes in the cyber layer, respectively.

V. Numerical Results

This section presents the numerical results of the allocation algorithm on the cyber layer of the IEEE-14 bus test system based on the configuration in [15]. The attenuation coefficient $\alpha = 0.2$ dB/km [6], [14] and the lengths of the fiber links in the cyber layer are calculated based on [16] and summarized in Table I. Two case studies are presented with source rates $r_n = 10^8$ and $r_n = 10^{10}$ photon per second. The case studies consider the presence of an attacker with noise injection levels $\in [0, 11\%]$. Also, we consider $r_{\min} = 256$ bps aiming for AES-256 encryption with a key refresh rate of 1 second.

Algorithm 1 Quantum server allocation

Input: $r_{\min}$, $G(\mathcal{N}, \mathcal{E})$
Initialize: Empty lists V, Q
for $i \in \mathcal{N}$ **do**
  sum = 0
  Dijkstra($\mathcal{N}[i]$)
  sum = **sumDijkstra**($\mathcal{N}[i]$)
  $V[i] =$ sum
end for
$m = \arg\min(V)$
Q.add(m)
for $j \in \mathcal{N}$ **do**
  Calculate $r_{m,j}$ $\forall j \neq m$
  if $r_{m,j} \leq r_{\min}$ **then**
    $n =$ **minDijkstra**($\mathcal{N}[j]$)
    Q.add(n)
  end if
end for
Output: Q

TABLE I
Lengths of the fiber links in the cyber layer of the IEEE 14-bus test system in kilometers.

From Node	To Node	Line length (km)
0	1	22.5
0	4	84.9
1	2	75.4
1	3	67
1	4	66.3
2	3	65.1
3	4	16
3	5	32.2
3	9	103
4	6	75.8
4	7	97.5
7	8	76.2
8	9	133

Fig. 2 and Fig. 3 show the minimum achieved key rate in the cyber layer for source rates of $r_n = 10^8$ and $r_n = 10^{10}$ photon per second, respectively. The minimum achieved rate in the cyber layer is found by calculating the least $r_{n,n'}$ for all n and n' representing full quantum and semi-quantum servers, respectively. As shown in Fig. 2, at least 2 nodes should be upgraded to a full quantum server so that the achieved rate is greater than or equal to $r_{\min} = 256$ bps. These two selected nodes are Node 4 and Node 7 in the cyber layer. As the attack (noise injection) level increases, the minimum achieved rate in the cyber layer is reduced, until the target $r_{\min}$ cannot be satisfied (attack/noise level $[0, 7\%]$). Beyond a noise level of 7%, an additional node should be upgraded into a full quantum server, which is Node 3. This increases the minimum achieved key rate in the cyber layer beyond $r_{\min}$ (attack/noise level

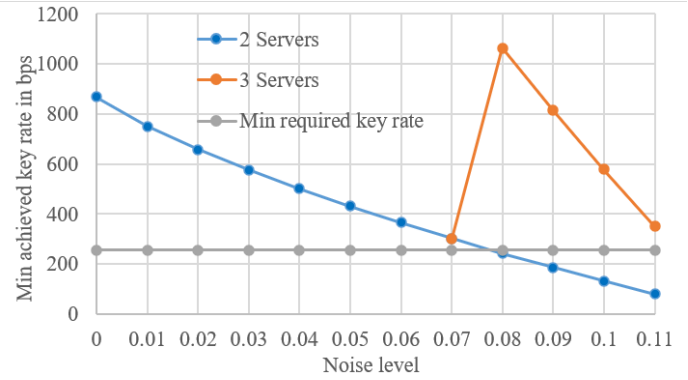

Fig. 2. Minimum achieved key rate in the cyber layer for a source rate of 10^8 photon per second for different attack (noise injection) levels.

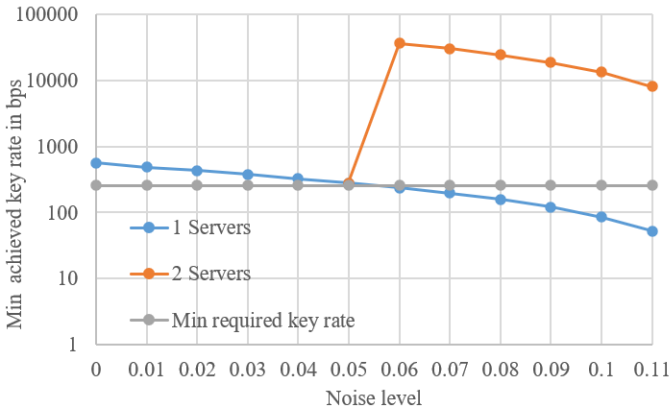

Fig. 3. Minimum achieved key rate in the cyber layer for a source rate of 10^{10} photon per second for different attack (noise injection) levels.

$[8\%, 11\%]$). For the case presented in Fig. 3, a higher source rate is considered for the quantum server, hence, for the same noise range $[0, 11\%]$, less number of full quantum servers is required. Specifically, only one quantum server is sufficient for the noise range $[0, 5\%]$, which is located at Node 4. Starting 6% noise level, an additional full quantum server is allocated at Node 7 to satisfy $r_{\min}$. As outlined, the quantum source rate and the desirable resilience level (i.e., resistance to a noise injection level) affect the number of required full quantum servers. For instance, to be able to satisfy $r_{\min}$ while resisting attacks with noise injection levels up to 8%, 3 servers are required if the source rate is 10^8 photon per second while only 2 servers are sufficient if the source rate is 10^{10} photon per second.

VI. Conclusion

This paper studied the upgrade of the existing cyber layer of a transmission power system to be able to support semi-quantum key distribution. In this case, only a subset of nodes are required to be upgraded to a full quantum server (i.e., capable of generating, transmitting, and measuring qubits) while the rest of the nodes can have limited quantum capabilities. The upgrade of the cyber layer is formulated as a binary optimization problem and a greedy algorithm is proposed to solve the problem with a reduced computational complexity. Our results demonstrated that the number of required full quantum servers depends on the quantum source rate (i.e., the number of generated photons per second on a diagonal basis) and the desirable resistance level to noise injection attacks. Our future work will examine the joint decision of the number, location, and source rate of the full quantum servers given some budget constraints. Also, our future work will relax the assumption that all pre-existing communication links are fiber links. Finally, our future work will consider evaluating larger systems beyond IEEE-14 bus test system to verify the scalability of the approach.

References

[1] R. A. Mollin, *RSA and Public-Key Cryptography*. USA: CRC Press, Inc., 2002.

[2] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-hellman key distribution extended to group communication," in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, 1996, pp. 31–37.

[3] J. Suo, L. Wang, S. Yang, W. Zheng, and J. Zhang, "Quantum algorithms for typical hard problems: a perspective of cryptanalysis," *Quantum Information Processing*, vol. 19, pp. 1–26, 2020.

[4] C. Easttom, "Quantum computing and cryptography," in *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. Springer, 2022, pp. 397–407.

[5] AZO Quantum. How the 'Mozi' Satellite Grants Quantum Security From Space. [Online]. Available: www.azoquantum.com/Article.aspx?ArticleID=308

[6] Z. Tang, P. Zhang, and W. O. Krawec, "A quantum leap in microgrids security: The prospects of quantum-secure microgrids," *IEEE Electrification Magazine*, vol. 9, no. 1, pp. 66–73, 2021.

[7] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure networked microgrids," in *2020 IEEE Power Energy Society General Meeting (PESGM)*, 2020, pp. 1–5.

[8] M. Alshowkan, P. G. Evans, M. Starke, D. Earl, and N. A. Peters, "Authentication of smart grid communications using quantum key distribution," *Scientific Reports*, vol. 12, no. 1, p. 12731, 2022.

[9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020.

[10] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical review letters*, vol. 68, no. 21, p. 3121, 1992.

[11] H. Iqbal and W. O. Krawec, "Semi-quantum cryptography," *Quantum Information Processing*, vol. 19, pp. 1–52, 2020.

[12] S. Mutreja and W. O. Krawec, "Improved semi-quantum key distribution with two almost-classical users," *Quantum Information Processing*, vol. 21, no. 9, p. 319, 2022.

[13] M. Boyer, M. Katz, R. Liss, and T. Mor, "Experimentally feasible protocol for semiquantum key distribution," *Physical Review A*, vol. 96, 12 2017.

[14] W. O. Krawec, T. Mor *et al.*, "Security proof against collective attacks for an experimentally feasible semiquantum key distribution protocol," *IEEE Transactions on Quantum Engineering*, 2023.

[15] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, 2015.

[16] Manitoba Hydro International. IEEE 14 Bus System. [Online]. Available: https://www.pscad.com/knowledge-base/article/26