Cyber Layer Upgrade in Power Systems to Support Semi-Quantum Key Distribution

Mariam Gado* and Muhammad Ismail*
*Department of Computer Science, Tennessee Technological University, Tennessee, USA
Emails: {mmgado42, mismail}@tntech.edu

***Abstract*—This paper investigates semi-quantum key distribution between local control centers and the substations in power systems to encrypt and decrypt critical measurements and control commands. We study the problem of allocating a minimal number of quantum servers and fiber links on a pre-existing cyber layer to satisfy the minimum required key rate in the presence of an attacker. The problem is formulated as a binary optimization program that upgrades the classical cyber layer of power systems to support semi-quantum key distribution. Due to the complexity of the allocation problem, we developed an optimal allocation strategy following a genetic algorithm. We examined the proposed allocation strategy on the cyber layer of the IEEE 14-bus and IEEE 39-bus test systems. Our results demonstrate that the target key rate can be achieved at different attack levels with a number of quantum servers and fiber links that is 33% and 21%, respectively, less than a benchmark for the IEEE 14-bus system. Our results demonstrate that the target key rate can be achieved at different attack levels with a number of quantum servers and fiber links that is 67% and 19%, respectively, less than a benchmark for the IEEE 39-bus system. Our results also demonstrate that the proposed solution requires 52.17% and 54.65% less upgrades compared with QKD for the IEEE 14-bus and IEEE 39-bus systems, respectively.**

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

I. Introduction

Power systems require security against false data and command injection attacks, this can be achieved by encryption algorithms such as the advanced encryption system (AES) [1]. Date encryption and decryption can by achieved by secret keys, which are exchanged by key-sharing mechanisms. Rivest-Shamir-Adleman (RSA) [2] and Diffie-Hellman key exchange [3] are two of the most common key-sharing mechanisms, which depend on the complexity of solving mathematical problems [4]. Classical computers fail to solve these problems in a reasonable time. However, they can be solved by quantum computers revealing the secret keys and leading to security breaches [5]. To address this concern, post-quantum key exchange strategies have been proposed, offering the capability to secure the systems against both classical and quantum adversaries, under computational assumptions. Other strategies, namely, quantum key distribution (QKD) and semi-QKD (SQKD) provide the unique advantage of unconditional security for key distribution, based on the laws of quantum mechanics.

This work was supported by NSF award #2220346.

The consequences of breaching the power system security can be severe leading to blackouts, which result in losses varying from financial losses to even threatening human lives. To support QKD and SQKD, quantum servers/nodes are needed to generate, measure, and manipulate qubits. Also, fiber optical links are needed to transmit the qubits from one point to another. However, the cyber layer of the power system is not equipped with these capabilities. Hence, there is a need to upgrade the cyber layer of the power system to include quantum servers and fiber links, thus, supporting QKD and SQKD. Hence, exploring cyber layer's upgrade solutions to support QKD and SQKD is necessary.

A. Related Works

A satellite quantum network is used to mitigate cyber attacks on the Chinese power system, which provides secure communication between the national emergency command center in Bejing and the power grid of Fujian [6]. QKD is used in recent works for secret key sharing and data authentication in power systems [7]–[9]. The BB84 protocol [10] and B92 [11] protocol are among many adopted QKD protocols, which require all nodes in the cyber layer to be upgraded to quantum servers with full quantum capabilities, i.e., quantum bit (qubit) generation, transmission, and measurement in the Z basis or the X basis. On the other hand, SQKD made it possible to share unconditionally secure keys between nodes that do not have the full quantum capabilities unlike QKD [12], [13]. In SQKD, a few number of nodes have the full quantum capabilities, while the rest of the nodes have limited quantum capabilities, e.g., transmit and measure qubits in the Z basis. Hence, a near-term deployment of unconditionally secure keys can be supported by SQKD for its cost effectiveness. Various SQKD protocols have been proposed in the literature [13]. One of the most robust SQKD protocols against noiseless attacks, which can be applied in practice is the mirror protocol [14]. The work in [15] studied the practical collective attacks on the mirror protocol, while mitigating the remaining general attacks is still an open problem. A greedy algorithm is proposed in [16] to select a minimal number of quantum servers to support SQKD in power systems, assuming a fiber network based cyber layer.

B. Limitations, Challenges, and Contributions

This paper focuses on sharing unconditionally secure keys in the power system between the local control center and the power substations. However, the existing works in the literature on quantum-secure power grids, e.g., [6], [7], [16], suffer from the following limitations:

- The considered power systems comprise a small number of power substations that are closely located, which does not guarantee the scalability of the QKD solution for larger transmission power systems that span tens to hundreds of kilometers.
- The existing QKD-based solutions require the cyber layer to be equipped with full quantum servers for each cyber node inside the system, which makes the upgrading cost higher. This requirement obstructs adopting QKD solutions in the near-term.
- There is only one work that investigates the upgrade of the cyber layer of power systems to support SQKD, as a cost effective solution compared with QKD. However, this work focuses on allocating only quantum servers while assuming that the network is a fiber-based one, which is not the case in the existing power systems [17]. Instead, existing power systems have a mixture of classical links (e.g., microwave, radio, etc.) and fiber links.

Hence, a cost-effective solution is needed to support unconditionally secure key sharing by upgrading a pre-existing cyber layer in a large-scale transmission power system. The following features are needed for a near-term solution: (a) the proposed solution should require a minimal number of cyber nodes to be upgraded to quantum servers and a minimal number of links to be upgraded to fiber links. Noting that the quantum servers using fiber links have full quantum capabilities (i.e., qubit generation, qubit transmission, and qubit measurement in both the X basis and Z basis), while the remaining cyber nodes have limited quantum capabilities (i.e., qubit transmission and measurement in the Z basis); (b) The proposed solution should be applicable to large-scale transmission power system, while satisfying the target key rate for long distances.

Toward this objective, we carried out the following:

- We formulated a binary optimization problem to allocate quantum servers and fiber links, thus, upgrading a power system's classical cyber layer to support SQKD. The formulated problem aims to upgrade a minimal number of cyber nodes to be fully quantum servers and a minimal number of fiber links in the presence of an attacker while satisfying the minimum target key rate. Due to the computational complexity, we propose an allocation strategy based on a genetic optimization algorithm.
- We examined the proposed allocation strategy on the cyber layer of the IEEE 14-bus and IEEE 39-bus test systems. Our results demonstrate a quantum server reduction of up to 33% and $\%67$ compared with a benchmark for the IEEE 14-bus and the IEEE 39-bus test systems, respectively. Also, our results compared with QKD demonstrate that only 20% and 3% of power substations should be upgraded with full quantum capabilities while the rest can have limited capabilities for IEEE 14-bus and IEEE 39-bus systems, respectively. A fiber link reduction of 21% and 19% is achieved compared with a benchmark and QKD, while satisfying the minimum target key rate for different attack levels for the IEEE 14-bus and IEEE 39-bus systems, respectively.

The rest of this paper is organized as follows. Section II gives a brief background about SQKD. Section III presents the system model. Section IV introduces the problem formulation and the proposed allocation strategy. Section V illustrates the numerical results. Section VI concludes our paper.

II. Semi-Quantum Key Distribution Protocol

This paper adopts the mirror protocol [14] for SQKD since it was proven to be robust against all noiseless attacks along with a set of practical attacks in [15]. The mirror protocol in [14] defines the full quantum node as Bob, who can generate, transmit, and measure qubits in both the Z and the X bases, while Alice is the semi-quantum node with limited quantum capabilities such as qubit transmission and measurement in the Z basis only. The SQKD mirror protocol's steps are as follows:

1) Bob prepares a $|+\rangle$ state and sends it to Alice.
2) Alice receives the $|+\rangle$ state and applies one of the following steps randomly:
   a) Alice leaves all photons undisturbed and transmits them back (reflects) towards Bob without measuring them. This is called a test round.
   b) Alice reflects all the photons in the $|0\rangle$ state and measures all the photons in the $|1\rangle$ state. This is called a raw key round.
   c) Alice reflects all the photons in the $|1\rangle$ state and measures all the photons in the $|0\rangle$ state. This is called a raw key round.
   d) Alice measures all the photons and does not reflect any photons towards Bob. This is called a swap-all round.
3) Bob receives the state from Alice if any (e.g., excluding the swap-all rounds) and measures it either in the Z basis or in the X basis randomly.

In order for Alice and Bob to share a qubit in raw key rounds, Alice has to choose 2b) or 2c) while detecting no photon after she measures the corresponding photons. Also, Bob has to use the Z basis for measurement in order to share a qubit. For more information about the mirror protocol, the reader is referred to [14]. We assume the existence of an attacker Eve between Alice and Bob in this setup. Eve has the ability to perform no attack on the system or a single attack

represented by a noise injection level on the communication channel 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

The physical layer of the power system consists of a set of transmission lines connecting a set of generation and load buses (substations). Sensing devices monitor each substation to measure active and reactive powers, three-phase voltages, etc. Additionally, each substation has a local network that is connected via a wide-area network to its local control center. The cyber layer is used to share the measurements of each substation with its local control center to define the optimal operation strategy and, hence, define and send back the control signals to the power substations.

Fig. 1 illustrates the physical layer of the IEEE 14-bus test system. The IEEE 14-bus and the IEEE 39-bus test systems will be used for performance evaluation of the proposed allocation strategy.

B. Cyber Layer

A set of routers and links connecting the power substations with local controllers form the cyber layer. Fig. 1 illustrates the cyber layer of the IEEE 14-bus system based on [18]. Since they are closely located, power substations 5 and 6 submit their measurements and receive control signals through a single cyber node (router) 4. Similarly, power substations $4, 7, 8$, and 9 have a common cyber node (router) 3. The rest of the buses have dedicated routers. The dominant majority of links are classical according to the report in [17], hence, we assume that there are no fiber links in the cyber layer of both the IEEE 14-bus and the IEEE 39-bus test systems.

This paper aims to identify upgrades of the cyber layer in terms of full quantum servers (i.e., red circles in Fig. 1) and fiber links (i.e., red lines in Fig. 1) to support SQKD between the local control center and the power substations. The rest of the cyber nodes will be semi-quantum servers with limited quantum capabilities and the rest of the links will be classical links. The generated keys will be used to encrypt and decrypt the messages (measurements and command signals) between the local control center and the power substations.

C. SQKD Rate

The optimal number and locations of quantum servers and fiber links are necessary for the produced key distribution rate $r_{n,n'}$ between a fully quantum server at n and a semi-quantum server at n'. Nodes n and n' use a fiber link set $\mathcal{E}_{n,n'}$, which covers all intermediate links that establish a path between nodes n and n' to generate unconditionally secure keys to satisfy the minimum required key generation rate $r_{\min}$. The channel connecting n and n' can be a noisy channel.

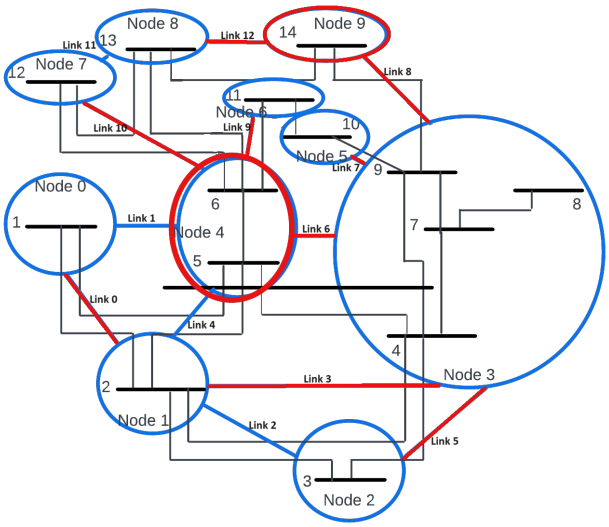

Fig. 1: Top view of the physical layer of IEEE 14-bus system (in black) and the cyber layer (in blue). The cyber layer is based on [18]. The red cyber nodes represent the node upgrade into a full quantum server and the red links represent the link upgrade into a fiber link.

We assume that the noise is representing the existence of an attacker E.

The attacker affects the communication session between the quantum server n and the semi-quantum server n' by injecting noise, hence, the attained key rate is reduced. The attained key rate $r_{n,n'}$ in bits per second (bps) can be described as in [15], [16]

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

where in (1), r_n is the source rate of the fully quantum server in photons per second, which is the rate of state creation and sending of a photon (i.e., the state $|+\rangle$) from the quantum server n (Bob) to the semi-quantum server n' (Alice). In (1), $M_{n,n'}$ denotes the probability that both nodes n and n' successfully generate raw key bits, which is described as [15]

$$M_{n,n'} = \frac{1}{2} \times 10^{\frac{-2\alpha L_{n,n'}}{10}}, \tag{2}$$

where in (2), α denotes the fiber link attenuation loss per kilometer and $L_{n,n'}$ is the length of the fiber link between nodes n and n' in kilometer, which is equivalent to the summation of the lengths of all fiber links in $\mathcal{E}_{n,n'}$. The last term in (1) represents the difference between two terms, which gives the total rate of the SQKD algorithm including mismatched raw key bits. The first term is the Von Neumann entropy $S(n'|E)$ between the semi-quantum server at n' and the attacker E. The second term is the entropy $H(n'|n)$ between the quantum server n and the semi-quantum server n'. The reader is referred to Appendix B to calculate $(S(n'|E) - H(n'|n))$.

Algorithm 1 computes the final key rate $r_{n,n'}$ based on [15] and [16]. The final key rate in (1) varies depending on the source rate of photon r_n, the distance of the fiber link $L_{n,n'}$ and the noise level $Q_x = Q_z$ since we consider a dependent noise model to maximize the noise tolerance of the SQKD algorithm to 11% [15]. This paper is using the final key rate to generate its results.

Algorithm 1 Key Rate Calculation

Input: $\alpha, L_{n,n'}, Q_z, Q_x, r_n$
Initialize: $\eta \to \infty$, $k = 0$
Compute $\langle P_0|P_0\rangle_E = \langle P_3|P_3\rangle_E$, $\langle P_1|P_1\rangle_E = \langle P_2|P_2\rangle_E$ from (15) and (16), respectively
Compute $M_{n,n'}$ using (17)
Compute $\zeta =$ the interval result of (9)
{Compute a lower bound on $S(n'|E)$}
for $\mathcal{R}\langle P_1|P_2\rangle_E \in \zeta$ **do**
  Compute a lower bound on $\mathcal{R}\langle P_0|P_3\rangle_E$ using (10) and subject to (8)
  Compute a lower bound γ on $S(n'|E)$ using (4)
  if $\gamma < \eta$ **then**
    $\eta = \gamma$
  end if
  $\mathcal{R}\langle P_1|P_2\rangle_E += 10^{-3}$
end for
Compute $\rho = H(n'|n)$ using (11)
$\nu = \eta - \rho$
$r_{n,n'} = r_n \times M_{n,n'} \times \nu$
Output: $r_{n,n'}$

IV. The Allocation of Quantum Servers and Fiber Links

The problem formulation to minimize the cost of upgrading the cyber layer of the power system to generate unconditionally secure keys is presented in this section. Then, we introduce our proposed strategy for allocating a minimum number of quantum servers and fiber links. We refer to the quantum servers and fiber links allocation problem as the allocation problem in this paper.

A. Problem Formulation

We model the cyber layer as an undirected, connected, weighted, acyclic graph $G(\mathcal{N}, \mathcal{E})$. $\mathcal{N}$ represents the set of all cyber nodes and $\mathcal{E}$ represents the set of pre-existing links between nodes, which can be (radio, microwave, etc.). The weights of $\mathcal{E}$ are based on the lengths of these links. We assume that the network does not have any fiber links. The minimum number of nodes $\in \mathcal{N}$ to be upgraded to fully quantum servers and edges $\mathcal{E}$ to be upgraded to fiber optics links is identified by the allocation problem. The minimum required key generation rate $r_{\min}$, is used as a constraint. The allocation problem can be described as follows

$$\begin{aligned} \min_{x_n, y_{i,j}} \quad & \sum_{n=1}^{N} x_n + \sum_{i=1}^{N}\sum_{j=1}^{N} y_{i,j} \\ \text{s.t.} \quad & r_{n,n'} \geq r_{\min} \\ & y_{i,j} \in \mathcal{E}_{n,n'}, \\ & \qquad \forall n \in \hat{\mathcal{N}}, n' \in \mathcal{N}/\hat{\mathcal{N}}, \\ & \qquad \forall i, j \in \mathcal{N} \\ & \qquad i \neq j, n \neq n', \\ & \qquad x_n \in \{0, 1\}, \\ & \qquad y_{i,j} \in \{0, 1\}, \end{aligned} \tag{3}$$

where x_n is a binary quantum server allocation decision variable such that $x_n = 1$ indicates that this cyber node is to be upgraded to a quantum server, where $n \in \hat{\mathcal{N}}$, where $\hat{\mathcal{N}}$ is the set of quantum servers, else $x_n = 0$ and this node is going to be a semi-quantum server, where $\mathcal{N}/\hat{\mathcal{N}}$ is the set of semi-quantum servers. $y_{i,j}$ is a binary fiber link allocation decision variable such that $y_{i,j} = 1$ indicates that the link between i and j is to be upgraded to a fiber link to support SQKD, otherwise, $y_{i,j} = 0$ and this link is not going to be upgraded to a fiber link. The minimum required key rate $r_{\min}$ is maintained by the first constraint in (3), where $r_{n,n'}$ is calculated from Algorithm 1. The second constraint maintains that $y_{i,j}$ is upgraded only if it belongs to a path $\mathcal{E}_{n,n'}$ between n and n'.

The allocation problem presented in (3) is an NP-complete binary program [16]. Hence, we propose an allocation strategy based on genetic algorithm to solve the problem and to reduce the complexity of finding an optimal solution to (3).

B. Proposed Allocation Strategy

Genetic algorithms (GA) are of the metaheuristic algorithms, which use operations that are inspired from nature such as selection, mutation, and crossover. GA are considered as a candidate to solve optimization problems with lower complexity [19]. In this paper, we use GA to propose a solution to the proposed allocation problem.

The distance between a given cyber node (Alice) and its corresponding quantum server (Bob) determines the key distribution rate as in (1), assuming the source rate and other probabilities are fixed. Each edge/link is a candidate to be upgraded to a fiber link. Similarly, each node in the cyber layer is a candidate to be upgraded to a quantum server. We model our solution to the problem as variant of the one-max problem [20] in which a chromosome has the length of the summation of the number of cyber nodes and the number of links between nodes. The population is constructed from input such as the chromosome length, population size, number of iterations/generations, crossover rate, mutation rate, and the objective function. To construct a feasible search space that minimizes the the objective function value, two main constrains are checked in order for a solution to be accepted

after the quantum network graph G' is constructed based on the chromosome. These constraints are: (a) graph connectivity, which is related to the second constraint in (3) (b) minimum key rate satisfaction $r_{\min}$, which is selected depending on the requirements of the used encryption/decryption algorithm (i.e., AES), which is related to the first constraint in (3).

Algorithm 2 Constrained Objective Function Value

Input: c, G
G' = **Construct**(c)
con1 = **Check-Con**(G')
con2 = **Check-R**(G')
if con1 = con2 = 1 **then**
  score = **UpgradesN**(c)
else
  score = ∞
end if
Output: score

Algorithm 2 shows the pseudo-code of the constrained objective function value, where the inputs are the chromosome c and the cyber network graph G, and the output is a score giving the fitness of this chromosome. **Construct**(c) function constructs the graph G' based on the locations of 1s in the chromosome c. **Check-Con**(G') function gets the constructed graph G' as an input and checks whether the graph is connected. This is done by checking if each node is accessible from all other nodes in the graph G' using Dijkstra's Algorithm. **Check-R**(G') function has two goals. The first goal is to assign a quantum server for each semi-quantum node in the graph. For each semi-quantum node, the assigned quantum server must be the nearest quantum server, which has the largest key generation rate in this chromosome. The second goal is to check if the key rate for all nodes in the graph is satisfying the minimum required key rate $r_{\min}$. The two outputs of the two functions are binary. If all the functions' outputs are 1s, then the score is calculated by function **UpgradesN**(c), which takes the chromosome as an input and outputs the number of the required quantum servers and fiber links upgrades and their specific locations, otherwise, the score of this chromosome is infinity, i.e., not a feasible solution.

Algorithm 3 summarizes the proposed allocation strategy, where the following terms are provided as inputs: the minimum required key rate $r_{\min}$, the cyber layer topology $G(\mathcal{N}, \mathcal{E})$, the number of iterations $iter$, chromosome length $clen$, population size $psize$, crossover probability $cross$, and mutation probability mut. The function **Construct-Pop**($clen, psize$) is called to generate a $psize$ population size of chromosomes with length $clen$ and the result population is stored in pop and $npop$ lists. The algorithm iterates for the number of iteration $iter$; For each iteration $iter$, each chromosome c in the population has a score according to the output of Algorithm 2. Algorithm 3 checks the solution, if the current chromosome c has a fitness score $score$ that is less than the previous chromosome's fitness score, then the current chromosome c is the new solution. The function **Construct-npop**($pop, scores, cross, mut$) has the input of the previous population pop and its scores $scores$ for each chromosome, the probability of crossover $cross$, and the probability of mutation mut. Then it generates a new population $npop$ to be used in the next iteration $iter$. The output of Algorithm 3 is the chromosome with the lowest number of upgrades and their corresponding locations, which is the solution to the allocation problem.

The complexity of the algorithm is O($iter$*$psize$($\mathcal{E}$*log($\mathcal{N}$)+1+2$clen$)), where $\mathcal{E}$ and $\mathcal{N}$ are the number of fiber links and cyber nodes in the cyber layer, respectively.

Algorithm 3 Proposed Allocation Strategy

Input: $r_{\min}$, $G(\mathcal{N}, \mathcal{E})$, $iter$, $clen$, $psize$, $cross$, mut
Initialize: Empty lists pop, $npop$
min $\rightarrow \infty$
pop = $npop$ = **Construct-Pop**($clen$, $psize$)
for $i \in iter$ **do**
  pop = $npop$
  $scores$ = []
  for $c \in psize$ **do**
    $score$ = call Algorithm 2 with inputs (c, G)
    $scores$.add($score$)
    if $score \leq$ min **then**
      solution = c
    end if
  end for
  $npop$ = **Construct-npop** (pop, $scores$, $cross$, mut)
end for
Output: solution

V. Numerical Results

This section presents the numerical results of the allocation strategy on the cyber layer of the IEEE 14-bus test system shown in Fig. 1 [18] and on the cyber layer of the IEEE 39-bus test system [21] assuming that each substation has a dedicated router. The technical notes in [22] and [21] are used as link lengths for the IEEE 14-bus and the IEEE 39-bus test systems, respectively. The attenuation coefficient α is set to 0.2 dB/km [23]. Using Algorithm 3, the number of iterations is set as $iter = 1000$, the chromosome length is set as $clen = 23$ (10 servers +13 edges), $clen = 86$ for the IEEE 14-bus and the IEEE 39-bus test systems, respectively. The population size is $psize = 200$. The crossover rate is $cross = 0.9$. The mutation rate is $mut = \frac{1}{23}$.

A. IEEE 14-bus Test System

This subsection illustrates the numerical results of Algorithm 3 on the IEEE 14-bus test system.

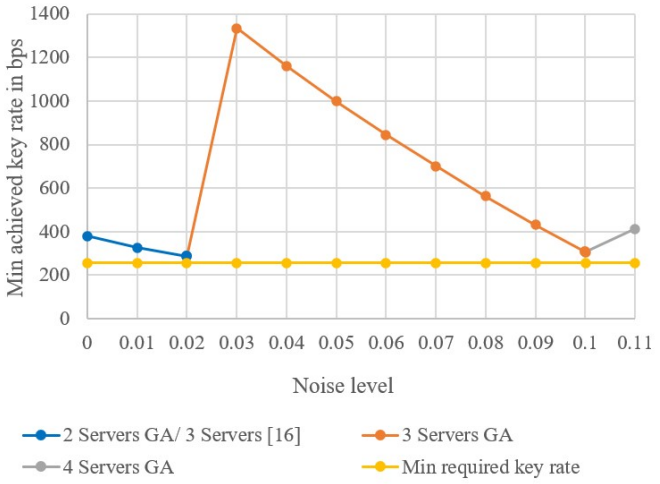

Fig. 2: A comparison of minimum achieved key rate $r_{n,n'}$ between the proposed algorithm and the benchmark in [16] on the IEEE 14-bus system cyber layer for a source rate of 10^7 photon per second for different attack levels. GA represents the proposed allocation strategy and [16] represents the benchmark in [16].

Fig. 2 illustrates the numerical results for the required number of quantum servers in the cyber network for a source rate of 10^7 pps. Fig. 2 shows that at least 2 servers are required to be upgraded to fully quantum servers in the presence of an attacker, for a noise level of $[0, 0.02]$, which are located at Node 3 and Node 7 and the following links are to be upgraded to fiber links: $0, 4, 5, 6, 7, 8, 9, 11$, and 12. This result demonstrates a reduction of 33% and 80% in the number of quantum servers compared with the benchmark in [16], and QKD solutions respectively. This result also demonstrates 31% reduction in the number of fiber links compared with both the benchmark in [16] and the QKD solutions. The work in [16] was not successful to mitigate attacks above 2% for a source rate of 10^7 photon per second (pps), hence, no comparison is provided beyond this attack level. The number of servers that are required to be upgraded to fully quantum servers for noise level $[0.02, 0.10]$ is 3, which are located at Node 4, Node 7 and Node 9 and the following links are to be upgraded to fiber links: $1, 4, 5, 6, 7, 8, 9, 11$, and 12. This result demonstrates a reduction of 70% in the number of quantum servers compared with QKD solutions. This result also demonstrates 31% reduction in the number of fiber links compared with QKD solutions. The number of quantum servers that are required to be upgraded to fully quantum servers for noise level $[0.10, 0.11]$ is 4, which are located at Node 1, Node 4, Node 7, and Node 9 to satisfy $r_{\min}$ and the following links are to be upgraded to fiber links: $0, 2, 4, 6, 7, 9, 10, 11$, and 12. This result demonstrates a reduction of 60% in the number of quantum servers compared with QKD solutions. This result also demonstrates 31% reduction in the number of fiber links compared with QKD solutions.

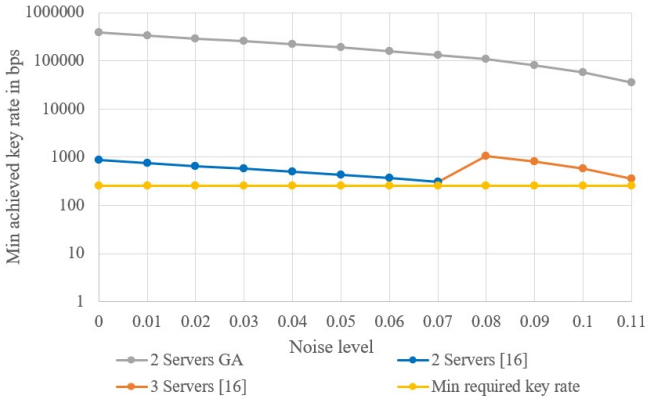

Fig. 3: A comparison of minimum achieved key rate $r_{n,n'}$ between the proposed algorithm and the benchmark in [16] on the IEEE 14-bus system cyber layer for a source rate of 10^8 photon per second for different attack levels. GA represents the proposed allocation strategy and [16] represents the benchmark in [16].

Fig. 3 illustrates the numerical results of the required number of quantum servers in the cyber network for a source rate of 10^8 pps. Fig. 3 shows that at least 2 nodes are required to be upgraded to fully quantum servers in order to satisfy $r_{\min} = 256$ bps under the presence of an attacker with a noise level $\in [0, 0.11]$, where the two nodes are Node 3 and Node 8 in the cyber layer and the following links are to be upgraded to fiber links: $1, 3, 5, 6, 7, 8, 9, 10$, and 11. This result demonstrates a reduction of 33% and 80% in the number of quantum servers compared with the benchmark in [16] and QKD solutions, respectively. Fig. 3 also shows the previous work results, where at least 2 nodes are required to be upgraded to quantum server under the presence of an attacker with a noise level $\in [0, 0.07]$, where Node 4 and Node 7 are required to be upgraded in the cyber layer. Although both of the proposed algorithm and the benchmark have 2 quantum server upgrades to mitigate the attacks $\in [0, 0.07]$, our proposed algorithm offer more key generation rate compared with the benchmark in [16]. In the benchmark in [16], it is required to upgrade at least 3 quantum servers in the presence of an attacker with a noise level $\in [0.07, 0.11]$, which are Node 3, Node 4 and Node 7. The number of link upgrades is 31% less for all noise levels compared with QKD and the benchmark in [16]. From Fig 3, it is shown that the proposed algorithm requires a less number of upgrades compared with both the benchmark in [16] and QKD for this test case.

Fig. 4 illustrates the numerical results for the required number of quantum servers in the cyber network for a source rate of 10^{10} pps. Fig. 4 shows that at least 1 server is required to be upgraded to a fully quantum server in the presence of an attacker, with a noise level of $[0, 0.05]$, which is located at Node 4 and the following links are to be upgraded to fiber

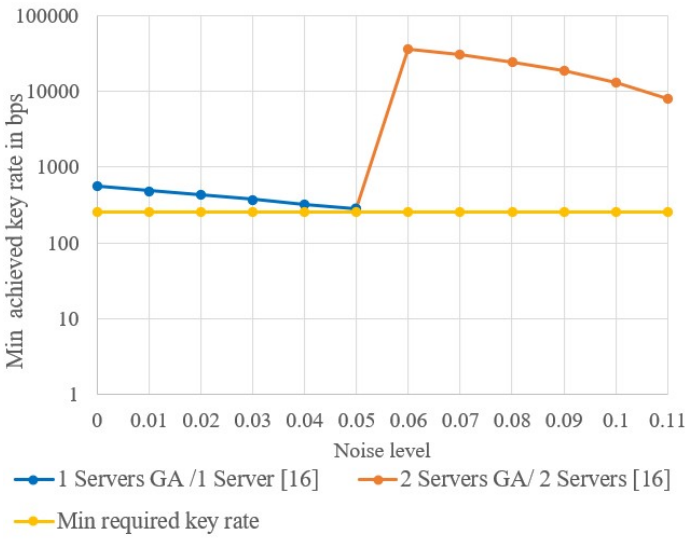

Fig. 4: A comparison of minimum achieved key rate $r_{n,n'}$ between the proposed algorithm and the benchmark in [16] on the IEEE 14-bus system cyber layer for a source rate of 10^{10} photon per second for different attack levels. GA represents the proposed allocation strategy and [16] represents the benchmark in [16].

links: $1, 2, 5, 6, 7, 8, 9, 10$, and 11. This result demonstrates a reduction of 90% in the number of quantum servers compared with QKD solutions. It is required to upgrade at least 2 nodes to fully quantum servers for noise level $[0.05, 0.11]$, which are Node 4 and Node 8 to satisfy $r_{\min}$ and the following links are to be upgraded to fiber links: $0, 1, 5, 6, 7, 8, 9, 11$, and 12. This result demonstrates a reduction of 80% in the number of quantum servers compared with QKD solutions. The results show that both our proposed strategy and the benchmark in [16] has the same number and locations of the quantum servers. However, the number of link upgrades is 31% for all noise levels compared with QKD and the benchmark in [16].

The results demonstrate that the number of the required link upgrades is equal to $\mathcal{N} - 1$ in G', which is the minimum number of link upgraded to keep the graph G' connected under all noise levels and with different source rates. The attack level influences the key generation rate, hence, more servers are required to mitigate a stronger attack as shown in the results. The source rate intensity also affects the key generation rate, hence, the lower the source rate intensity, the larger the number of the required quantum servers and vice versa.

The resilience level of the cyber network and the quantum source rate determines the number of the required full quantum servers and fiber links. As shown in the numerical results, 2 quantum servers are required for a source rate of 10^8 pps and 10^{10} pps, respectively, while 4 quantum servers are required for a source rate of 10^7 pps using our proposed algorithm to mitigate an attack up to 11%, which is the maximum achieved resistance by the SQKD algorithm in [14].

B. IEEE 39-bus Test System

This subsection presents the numerical results of Algorithm 3 on the cyber layer of the IEEE 39-bus test system.

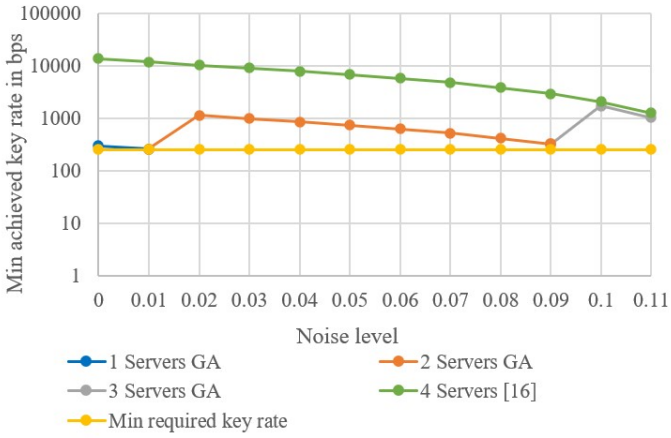

Fig. 5: A comparison of minimum achieved key rate $r_{n,n'}$ between the proposed algorithm and the benchmark in [16] on the IEEE 39-bus system cyber layer for a source rate of 10^7 photon per second for different attack levels. GA represents the proposed allocation strategy and [16] represents the benchmark in [16].

Fig. 5 illustrates the numerical results for the required number of quantum servers in the cyber network of the IEEE 39-bus test system for a source rate of 10^7 pps. Fig. 5 shows that at least 1 server is required to be upgraded to a fully quantum server in the presence of an attacker, for a noise level of $[0, 0.01]$. This result demonstrates a reduction of 75% and 97.44% in the number of quantum servers compared with the benchmark in [16] and QKD solutions, respectively. The number of servers that are required to be upgraded to fully quantum servers for noise level $[0.01, 0.09]$ is 2. This result demonstrates a reduction of 50% and 94.87% in the number of quantum servers compared the benchmark in [16] and QKD solutions, respectively. The number of quantum servers that are required to be upgraded to fully quantum servers for noise level $[0.09, 0.11]$ is 3. This result demonstrates a reduction of 25% and 92.31% in the number of quantum servers compared the benchmark in [16] and QKD solutions, respectively. Fig. 5 shows that the benchmark in [16] requires at least 4 quantum servers to be upgraded for noise $[0, 0.11]$. The the number of link upgrades for the IEEE 39-bus test system is 19% less for all noise levels compared with both the benchmark in [16] and QKD solutions.

Fig. 6 illustrates the numerical results for the required number of quantum servers in the cyber network of the IEEE 39-bus test system for a source rate of 10^8 pps. Fig. 6 shows that at least 1 server is required to be upgraded to a fully quantum server in the presence of an attacker, for a noise level

of $[0, 0.11]$. This result demonstrates a reduction of 66.7% and 97.44% in the number of quantum servers compared with the benchmark in [16] and QKD solutions, respectively. The number of link upgrades for the IEEE 39-bus test system is 19% less for all noise levels compared with both the benchmark in [16] and QKD solutions.

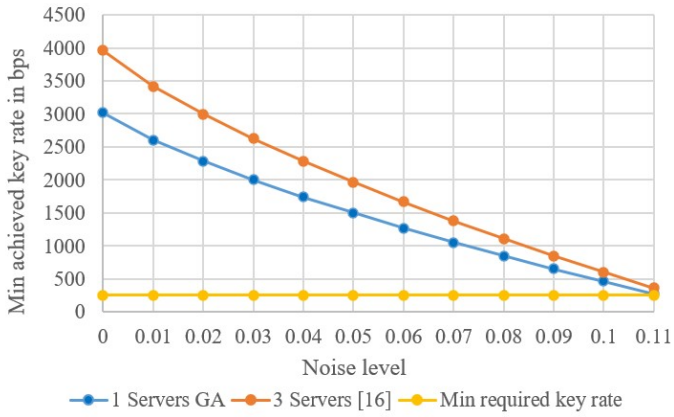

Fig. 6: A comparison of minimum achieved key rate $r_{n,n'}$ between the proposed algorithm and the benchmark in [16] on the IEEE 39-bus system cyber layer for a source rate of 10^8 photon per second for different attack levels. GA represents the proposed allocation strategy and [16] represents the benchmark in [16].

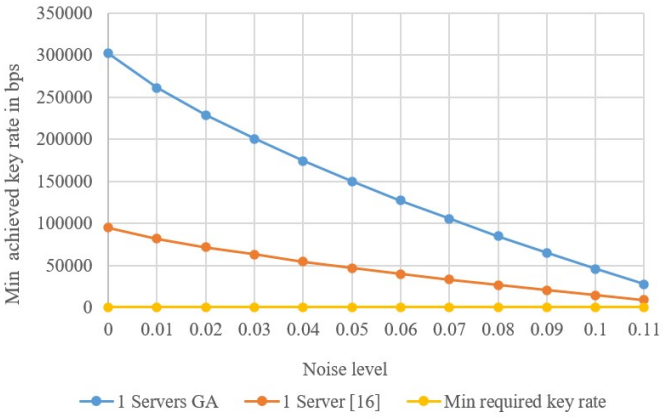

Fig. 7: A comparison of minimum achieved key rate $r_{n,n'}$ between the proposed algorithm and the benchmark in [16] on the IEEE 39-bus system cyber layer for a source rate of 10^{10} photon per second for different attack levels. GA represents the proposed allocation strategy and [16] represents the benchmark in [16].

Fig. 7 illustrates the numerical results for the required number of quantum servers in the cyber network of the IEEE 39-bus test system for a source rate of 10^{10} pps. Fig. 7 shows that at least 1 server is required to be upgraded to a fully quantum server in the presence of an attacker, for a noise level of $[0, 0.11]$. This result demonstrates a reduction of 97.44% in the number of quantum servers compared with QKD solutions. Although both of the proposed algorithm and the benchmark have the 1 quantum server upgrade to mitigate the attacks, our proposed algorithm offers more key generation rate compared with the benchmark in [16]. The the number of link upgrades for the IEEE 39-bus test system is 19% less for all noise levels compared with both the benchmark in [16] and QKD solutions.

VI. Conclusion

This paper studied the problem of upgrading the existing cyber layer of a transmission power system to generate unconditionally secure keys using semi-quantum key distribution. In this work, only a subset of cyber nodes and transmission links are required to be upgraded to full quantum servers and fiber links, respectively, while the other cyber nodes have limited quantum capabilities. The cyber layer upgrade problem is formulated as a binary optimization problem and a genetic algorithm is proposed to provide a solution to reduce the computational complexity. In the IEEE 14-bus test system, for a source rate of 10^7 pps, 10^8 pps, and 10^{10} pps, the proposed algorithm requires 31.25%, 31.25%, and 26.27% less upgrades compared with the benchmark in [16], respectively. Also, for source rate of 10^7 pps, 10^8 pps, and 10^{10} pps, the proposed algorithm requires 43.48%, 52.17%, and 52.17% less upgrades compared with the QKD solutions for the IEEE 14-bus test system. In the IEEE 39-bus test system, for a source rate of 10^7 pps, 10^8 pps, and 10^{10} pps, the proposed algorithm requires 19%, 23%, and 0% less upgrades compared with the benchmark in [16], respectively. Although our algorithm shows that key generation rate is 319% of the benchmark for the case where the same number of servers is used. Also, for source rate of 10^7 pps, 10^8 pps, and 10^{10} pps, the proposed algorithm requires 52.33%, 54.65%, and 54.65% less upgrades compared with the QKD solutions. Our future work will examine larger IEEE systems beyond the IEEE 14-bus and the IEEE 39-bus test systems to verify the scalability of the approach.

Appendix

A. Quantum States and Measurements

Qubits are the basic building blocks 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 the following equality: $|\alpha|^2+|\beta|^2 = 1$. Classical bits can exist in one of the following two states: state 0 or state 1, qubits on the other hand can exist in state 0 or state 1 or a superposition of both states at the same time.

Qubits are represented by photons in the SQKD systems, and the quantum state is represented by the polarization of the photon(s). There are two polarization bases that are considered in this paper as follows: the Z basis (i.e., computational basis) and the X basis (i.e., diagonal basis). The Z basis has two states $|0\rangle$ and $|1\rangle$, and the X basis has two states $|+\rangle$ and $|-\rangle$, where the state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and

the state $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. In quantum systems, both the sender and the receiver must agree on the same basis to encode and decode the qubit successfully, thus, receiving the corresponding information. Measuring qubits $|0\rangle$ and $|1\rangle$ in the computational Z basis results in the classical bits 0 and 1, respectively. Measuring qubits $|+\rangle$ and $|-\rangle$ in the diagonal X basis results in the classical bits 0 and 1, respectively.

B. Calculating $(S(n'|E) - H(n'|n))$

A bound on the conditional Von Neuman entropy $S(n'|E)$ can be calculated from (4) as in [15] using the probabilities defined in Table I as follows

$$\begin{aligned} &S(n'|E) \geq \\ &\frac{\langle P_0|P_0\rangle_E + \langle P_3|P_3\rangle_E}{M_{n,n'}} \times \\ &[H_2(\frac{\langle P_0|P_0\rangle_E}{\langle P_0|P_0\rangle_E + \langle P_3|P_3\rangle_E}) - H_2(\lambda_1)] \\ &+ \frac{\langle P_1|P_1\rangle_E + \langle P_2|P_2\rangle_E}{M_{n,n'}} \times \\ &[H_2(\frac{\langle P_1|P_1\rangle_E}{\langle P_1|P_1\rangle_E + \langle P_2|P_2\rangle_E}) - H_2(\lambda_2)], \end{aligned} \tag{4}$$

where

$$\lambda_1 \triangleq \frac{1}{2} + \frac{\sqrt{(\langle P_0|P_0\rangle_E - \langle P_3|P_3\rangle_E)^2 + 4\mathcal{R}^2 \langle P_0|P_3\rangle_E}}{2(\langle P_0|P_0\rangle_E + \langle P_3|P_3\rangle_E)^2}, \tag{5}$$

$$\lambda_2 \triangleq \frac{1}{2} + \frac{\sqrt{(\langle P_1|P_1\rangle_E - \langle P_2|P_2\rangle_E)^2 + 4\mathcal{R}^2 \langle P_1|P_2\rangle_E}}{2(\langle P_1|P_1\rangle_E + \langle P_2|P_2\rangle_E)^2}, \tag{6}$$

where

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x), \tag{7}$$

$\mathcal{R}\langle P_0|P_3\rangle_E$ and $\mathcal{R}\langle P_1|P_2\rangle_E$ are subject to three constraints in (8)-(10) in a noisy channel, i.e., in the presence of an attacker E, where

$$\mathcal{R}\langle P_0|P_3\rangle_E \leq \frac{1}{4}(1-K_{n,n'})^2(1-Q_z), \tag{8}$$

$$\mathcal{R}\langle P_1|P_2\rangle_E \leq \frac{1}{4}(1-K_{n,n'})^2 Q_z, \tag{9}$$

$$\mathcal{R}(\langle P_0|P_3\rangle_E + \langle P_1|P_2\rangle_E) \geq (1-K_{n,n'})^2(\frac{1}{4} - \frac{1}{2}Q_x), \tag{10}$$

where Q_x and Q_z are the noises on the quantum channel. Q_x is the probability that $|0\rangle$ is flipped to $|1\rangle$ and vice versa in raw key generation rounds. Q_z is the probability that the state $|+\rangle$ is flipped to $|-\rangle$ and vice versa in test rounds [15].

The term $H(n'|n)$ can be calculated as follows:

$$H(n'|n) = H(n'n) - H(n), \tag{11}$$

Probability	Definition	Formula
$\langle P_0\|P_0\rangle_E$	Alice and Bob get raw key bits $0,0$, respectively	(15)
$\langle P_1\|P_1\rangle_E$	Alice and Bob get raw key bits $0,1$, respectively	(16)
$\langle P_2\|P_2\rangle_E$	Alice and Bob get raw key bits $1,0$, respectively	(16)
$\langle P_3\|P_3\rangle_E$	Alice and Bob get raw key bits $1,1$, respectively	(15)
$M_{n,n'}$	Probability that both Alice and Bob get raw key bits	(17)
$K_{n,n'}$	Fiber channel loss rate	(18)

TABLE I: Definitions of probabilities and their corresponding formulas.

where

$$H(n'n) = H(\frac{\langle P_0|P_0\rangle_E}{M_{n,n'}}, \frac{\langle P_1|P_1\rangle_E}{M_{n,n'}}, \frac{\langle P_2|P_2\rangle_E}{M_{n,n'}}, \frac{\langle P_3|P_3\rangle_E}{M_{n,n'}}), \tag{12}$$

$$H(n) = H(\frac{\langle P_0|P_0\rangle_E + \langle P_2|P_2\rangle_E}{M_{n,n'}}, \frac{\langle P_1|P_1\rangle_E + \langle P_3|P_3\rangle_E}{M_{n,n'}}), \tag{13}$$

where

$$H(x_1, x_2, ...x_n) = -\sum_{j=1}^{k} x_j \log_2(x_j), \tag{14}$$

$$\langle P_0|P_0\rangle_E = \langle P_3|P_3\rangle_E = \frac{1}{4}(1-K_{n,n'})^2(1-Q_z), \tag{15}$$

$$\langle P_1|P_1\rangle_E = \langle P_2|P_2\rangle_E = \frac{1}{4}(1-K_{n,n'})^2 Q_z, \tag{16}$$

$$M_{n,n'} = \sum_{i=0}^{3} \langle P_i|P_i\rangle_E, \tag{17}$$

$$K_{n,n'} = 1 - 10^{\frac{-\alpha \mathbf{L}_{n,n'}}{10}}, \tag{18}$$

where (2) is equivalent to (17) according to the following proof,

$$\begin{aligned} &M_{n,n'} \\ &= \sum_{i=0}^{3} \langle P_i|P_i\rangle_E \\ &= \langle P_0|P_0\rangle_E + \langle P_1|P_1\rangle_E + \langle P_2|P_2\rangle_E + \langle P_3|P_3\rangle_E \\ &= 2(\frac{1}{4} \times (1-K_{n,n'})^2(1-Q_z)) + 2 \times (\frac{1}{4} \times (1-K_{n,n'})^2 Q_z) \\ &= \frac{1}{2} \times (1-K_{n,n'})^2(1-Q_z+Q_z) \\ &= \frac{1}{2} \times (1-(1-10^{\frac{-\alpha \mathbf{L}_{n,n'}}{10}}))^2 \textbf{ from } (18) \\ &= \frac{1}{2} \times (10^{\frac{-\alpha \mathbf{L}_{n,n'}}{10}})^2 \end{aligned} \tag{19}$$

REFERENCES

[1] 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, 12 2022.

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

[3] 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.

[4] 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.

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

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

[7] 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.

[8] 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.

[9] 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.

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

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

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

[13] 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.

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

[15] 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.

[16] M. Gado, M. Ismail, and W. O. Krawec, "Upgrading the cyber layer of power systems to support semi-quantum key distribution," in *2024 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2024, pp. 1–5.

[17] M. Soetan, Z. Mao, and K. Davis, "Statistics for building synthetic power system cyber models." Institute of Electrical and Electronics Engineers Inc., 4 2021.

[18] 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.

[19] S. Katoch, S. S. Chauhan, and V. Kumar, "A review on genetic algorithm: past, present, and future," *Multimedia Tools and Applications*, vol. 80, pp. 8091–8126, 2 2021.

[20] C. Qian, C. Bian, W. Jiang, and K. Tang, "Running time analysis of the (1 + 1)-ea for onemax and leadingones under bit-wise noise," *Algorithmica*, vol. 81, pp. 749–795, 2 2019.

[21] Manitoba Hydro International. (2018) PSCAD TM IEEE 39 Bus System. [Online]. Available: https://www.pscad.com/knowledge-base/article/28

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

[23] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure microgrid," *IEEE Transactions on Power Systems*, vol. 36, pp. 1250–1263, 3 2021.