IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 December 2024, accepted 19 January 2025, date of publication 24 January 2025, date of current version 29 January 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3533942

RESEARCH ARTICLE

Quantum Key Distribution Applicability to Smart Grid Cybersecurity Systems

WARREN GRICE[1], MOHAMMED OLAMA[1], (Senior Member, IEEE), ANNABELLE LEE[2], (Member, IEEE), AND PHILIP G. EVANS[1], (Member, IEEE)

[1]Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA
[2]Nevermore Security, Evergreen, CO 80439, USA

Corresponding author: Mohammed Olama (olamahussemm@ornl.gov)

This work was supported by the U.S. Department of Energy (DOE), Office of Electricity (OE), through UT-Battelle, LLC, under Contract DE-AC05-00OR22725.

ABSTRACT To meet the increasing demand for electricity and to have a more reliable and resilient electric grid against conventional and extreme events, grid modernization is more crucial now than ever before. This will require the development and deployment of devices that provide advanced communication capabilities. The overall efficiency, reliability, and resilience of the smart grid will be inextricably linked to the exchange of information between these devices. Unfortunately, the increased information flow will increase the potential attack surface and introduce new vulnerabilities. While a smarter grid will depend critically on information flow, these benefits will be accrued only if that information can be protected. Nowadays, information is secured in smart grids primarily through cryptography. However, with the increasing number of sophisticated attacks as well as the increasing computational power, the security of the ''classical'' cryptographic algorithms is threatened. Quantum information science offers solutions to this problem, specifically quantum key distribution (QKD), which provides a means for the generation and secure distribution of symmetric cryptographic keys. The security of QKD stems ultimately from the very nature of quantum physics. In this paper, we investigate the applicability of QKD to the various smart grid sectors and specific use cases. We have identified 18 smart grid use cases of interest for QKD suitability together with 7 QKD factors used for the assessment of the various use cases. For each use case, the impact to security of the loss of confidentiality, integrity, and/or availability is specified. In addition, the suitability of QKD is assessed for each use case with respect to multiple factors.

INDEX TERMS Smart grid security, symmetric and asymmetric cryptography, quantum key distribution.

I. INTRODUCTION

The electric power industry is embarking upon an infrastructure transformation that will result in a more reliable and resilient electric power grid—in essence, a smarter grid [1]. The transition to a more connected electric grid will be enabled by the development of a variety of devices that communicate with one another. Ultimately, the overall efficiency, reliability, and resilience of the grid will be inextricably linked to this exchange of information.

Modernizing the grid to make it ''smarter'' and more resilient using cutting-edge technologies, equipment, and controls that communicate and work together to deliver electricity more reliably and efficiently can greatly reduce the frequency and duration of power outages, reduce the impact of extreme weather events, and restore service faster when outages occur [2]. Consumers can better manage their own energy consumption and costs, because they will have easier access to their own data. Electric power utilities also will benefit from a modernized grid, including reduced peak loads, increased integration of renewables, and lower operational costs [3].

''Smart grid'' technologies are made possible by two-way communication technologies, control systems, and computer processing. These advanced technologies include advanced sensors — such as phasor measurement units (PMUs) — that

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed F. Zobaa.

allow operators to assess grid stability, advanced metering infrastructure (AMI) that collects detailed metering information from consumers in real time and automatically reports outages, relays that sense and recover from faults in the substation automatically, automated feeder switches that re-route power around faulted lines, and batteries that store excess energy and make it available later to the grid to meet customer demand [4].

Increased information flow and connectivity will also bring potential new vulnerabilities and an increased attack surface [5]. Poor information security could lead to, for example, compromised consumer information or system-wide attacks by adversaries. Thus, while a smarter grid will depend critically on information flow, these benefits will be accrued only if that information can be protected.

The most widely used technique to protect information is cryptography. There are three cryptographic functions [6]: symmetric cryptography, asymmetric cryptography, and secure hash. Symmetric cryptography is primarily used for data confidentiality and the same secret key is used for both the encryption of plaintext and the decryption of ciphertext. The secret key should not be shared among individuals or devices. The secret key encryption allows the use of a provably secure one-time pad encryption method, whereby each key is used only once before being disposed of, but at the cost of insecurity of the key distribution process. Asymmetric cryptography, typically implemented in a public key infrastructure (PKI), uses a private key and associated public key. These keys are mathematically related. The private key is associated with an individual/device and is not shared. The public key may be shared with other devices/individuals. Public key encryption allows for widespread distribution of the public key, hence negating trust issues associated with the distribution of shared secret keys. The security of public key encryption is based on computational complexity. With increasing computational power, attacking the mathematical functions at the heart of public key cryptography becomes more tractable and less computationally expensive. Asymmetric cryptography is commonly used to digitally sign data.

The third cryptographic function is secure hashing, which generates a cryptographic checksum/hash on data. A hash algorithm has the property that it is computationally infeasible to find a message that corresponds to a given message digest, or to find two different messages that produce the same message digest. A secure hash uses a symmetric key to detect both accidental and intentional modifications of the data. For hash functions, the input is called the message, and the output is called the (message) digest or the hash value. The length of the message can vary, while the length of the digest is fixed.

With the increasing number of sophisticated attacks as well as the increasing computational power, the security of classical asymmetric cryptographic algorithms is threatened. In addition, with the rapid advancement of quantum computing technology [7], traditional asymmetric cryptographic methods face the risk of becoming obsolete as quantum computers may be capable of efficiently breaking classical asymmetric algorithms. By utilizing quantum-resistant cryptographic techniques and quantum key distribution protocols, power grid systems can mitigate such cyber threats and ensure the long-term security of communication channels. Quantum communication technologies offer robust defenses against various cyber threats, including eavesdropping, data tampering, and man-in-the-middle attacks [7]. By implementing quantum-secured communication channels, power grid operators can significantly reduce the vulnerability of the grid infrastructure to cyber threats and enhance overall system resilience. Quantum communication can play a crucial role in supporting the deployment of smart grid technologies, such as distributed energy resources (DERs), AMIs, PMUs, and demand response systems. By providing secure and reliable communication links between grid components, quantum communication enables seamless integration of smart grid devices, enhances grid visibility and control, and enables the implementation of advanced grid optimization algorithms.

Quantum information science offers a solution for the generation and secure distribution of symmetric cryptographic keys. Quantum key distribution (QKD) is a quantum communications protocol that generates randomness intended to protect data or information shared between two different entities. Because the shared random bit strings are generated remotely and because they can be used as a resource for conventional security tools such as encryption, QKD provides a powerful capability for helping to secure the electric grid. QKD therefore offers the advantages of ''classical'' private and public key cryptography [6], namely the realization of provably secure keys using variations of a one-time pad, the distribution of such keys over untrusted communication channels where eavesdroppers are assumed to be present, and keys that are not based on computational complexity but are truly random.

The security of QKD stems ultimately from the very nature of quantum physics. Unlike classical cryptographic methods, which rely on mathematical algorithms that could potentially be broken by advancements in computing power or algorithmic breakthroughs, quantum communication provides unconditional security based on the laws of physics. Because the light is encoded in quantum states, any attempts to acquire information during the key generation process will alter the states in a way that can be detected by legitimate users. That is, an eavesdropper cannot gain information without leaving some trace. As one of the most mature quantum protocols, QKD is a proven technology, and complete systems are commercially available. This enhanced security is particularly crucial for protecting sensitive data, critical control commands, and infrastructure information within power grids from cyber threats and attacks.

Although QKD has not seen widespread implementation in applications requiring secure communication, the electric grid offers some intriguing use cases for which QKD can be seen as an attractive solution. This is because many of QKD's shortcomings are less problematic in the grid. For example, several communication links in the grid are short enough to

be serviced by a single QKD link, obviating the need for quantum repeaters, which are not yet practical with today's technology. Another potential synergy between the grid and QKD is the inherent point-to-point nature of both. Most QKD protocols allow key distribution between only two parties, and this is viewed as a limitation in most contexts. However, many components in a smart grid infrastructure only need to communicate with a very limited subset of devices, and the relationships between devices may not change over the lifetime of the network.

The cost of commercially available QKD systems is a potential impediment to implementation. However, this type of concern is typical of nascent technologies, and, with increased adoption, it is almost certain that QKD component costs will come down. The primary question for QKD and the smart grid is not whether QKD can offer better security, but rather which QKD solutions are best and where on the grid they should be implemented.

In this paper, we investigate the applicability of QKD to the various smart grid sectors (or domains) and specific use cases. We conduct an analysis of commercial QKD capabilities and smart grid security needs with the goal of identifying the highest value security needs that can be met by QKD. For each use case, the impact to security of the loss of confidentiality, integrity, and/or availability is specified. In addition, the suitability of QKD is assessed for each use case with respect to several factors. The main contributions of the research in this paper are summarized as follows:

- Selection of 18 smart grid use cases of interest for QKD suitability assessment.
- Identification of 7 QKD factors (considerations) for the assessment of the various use cases.
- Assessment of the selected 18 smart grid use cases based on the 7 QKD factors and presentation of the results.
- High-level recommendations (after consultation with power utilities) for the applicability of QKD to the various smart grid domains.

This paper is organized as follows: Section II presents an overview of QKD including QKD basics, QKD approaches, QKD limitations, and the future of QKD on the smart grid. Section III presents the selection criteria for the grid use cases of interest, in addition to a description of the analysis methodology used in their assessment with respect to QKD suitability. Section IV presents a detailed description of the assessment outcome for each use case, which is organized by smart grid domain. Finally, Section V summarizes the main outcomes of this study and suggests directions for future work.

II. QUANTUM KEY DISTRIBUTION (QKD)

Quantum information science offers security solutions that can be realized using technologies based solely on classical physics. At the forefront of information security is quantum cryptography, which acknowledges that information must inherently manifest in physical form. More fundamentally, the physics of information is necessarily quantum physics. This has broad implications for information security. The most mature example is QKD, which provides a means for the generation and secure distribution of identical cryptographic keys [8].

Despite the fundamental advantages of QKD, quantum cryptography has yet to be widely implemented in cybersecurity applications. This is due, in part, to a need for stable and low-cost infrastructure components, such as quantum light sources and detection stations, that can be deployed in a variety of settings (e.g., in existing telecom infrastructures). Included in this section is a brief introduction to QKD and identification of the components necessary for developing a quantum cryptographic infrastructure to support future smart grid devices.

A. QKD BASICS

Two spatially separated parties, traditionally referred to as Alice and Bob, wish to communicate securely in the presence of a suspected eavesdropper, Eve. There exists a quantum channel over which the quantum key is shared, and a classical channel over which the quantum-key secured information is exchanged using a standard symmetric encryption method, such as the Advanced Encryption Standard (AES) [9]. Eve is assumed to have access to both the quantum and classical channel. This is illustrated in Fig. 1.

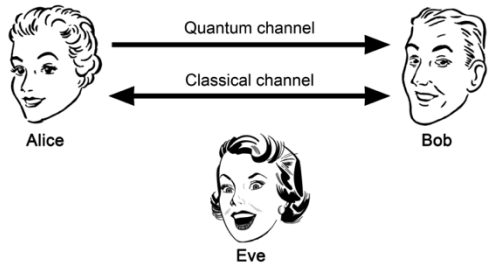

FIGURE 1. Alice, Bob and Eve. Classical and quantum channels.

At the heart of QKD is the generation, transmission and detection of quantum states of light. Typically, the light is prepared and measured in either of two complementary bases. In single-photon QKD, Alice randomly chooses a bit value and a preparation basis, while Bob randomly chooses a measurement basis. If Bob's basis choice is the same as Alice's, then he will be able to measure the value of the bit prepared by Alice. However, if they choose different bases, then Bob's measurement result will be completely uncorrelated with Alice's bit value. As an example, the information might be carried in the polarization of a single photon: the rectilinear basis comprises orthogonal states of horizontal (H) and vertical (V) polarization, while the complementary diagonal basis has orthogonal states of 45° (+) and −45° (−) polarization. Suppose Alice prepares a "V" photon. If Bob measures in the H/V basis, then his measurement result will be "V." However, if he measures in the +/− basis, then he will record either

"+" or "−" each with 50% probability. Once Alice and Bob have prepared and measured a suitable number of photons, they publicly compare their basis choices (but not the bit values) and discard all of the cases (roughly 50%) for which they had chosen different bases. Barring errors, the remaining data are perfectly correlated: Bob knows what Alice sent, and Alice knows what Bob measured.

Alice and Bob assume Eve has access to both the classical and quantum communication channels. There are several attacks Eve can deploy in an attempt to gain information of the secret key passed between Alice and Bob. One of the most straightforward is the classic intercept-resend attack, in which Eve intercepts Alice's photon destined to Bob, applies her own measurement, and then attempts to recreate the same state that she measured for retransmission to Bob. However, this is in direct violation of the no-cloning theorem [10], which states that it is impossible to create identical copies of an arbitrary quantum state. In essence, Eve's strategy works only when she guesses the same basis as Alice and Bob. When she guesses incorrectly, she ends up sending the wrong state to Bob, leading to a detectable increase in the number of errors in the raw key. The presence of information leakage to Eve, can be detected by comparing a certain subset of their remaining bit strings and analyzing errors. Eve has at her disposal a variety of attacks to gain more information about the secret key shared by Alice and Bob. However, any attempt by Eve to gain a useable amount of information is revealed by an increase in the quantum bit error rate (QBER) detected by Alice and Bob.

As long as the QBER is not too high, any information leakage due to Eve's eavesdropping can be minimized by performing reconciliation [11] and privacy amplification [12] steps on the shared bit string. The end result is a shared key that is known only to Alice and Bob. This key can then be used for secure information transfer between Alice and Bob, perhaps using a standard such as the AES. Ideally, the secret key is used only once in a one-time pad scheme, requiring a new QKD session to be initiated before any new message is sent. However, the same key may be used for a limited number of messages (or a limited time) before a new key is required, but at the risk of higher probability of the secret key being discovered by Eve.

The preceding example assumes ideal hardware and conditions. In reality, QKD systems are hampered by losses, less-than-ideal photon sources and detectors, and by engineering flaws, all of which negatively impact the QBER and the amount of information leaked to Eve. These imperfections place limits on the security proofs of practical QKD systems.

B. QKD APPROACHES

In principle, QKD can be carried out using any type of quantum state. In the case of photons, the information can be encoded into any of a number of degrees of freedom and the photons can be generated and detected at any wavelength. Three common QKD approaches are discussed below.

1) SINGLE-PHOTON QKD

In the example given in the preceding subsection, information was encoded into the polarization of single photons. This works well for transmission through free space, but it is more problematic through fiber links, which do not typically preserve polarization information. It is possible to correct for polarization effects in fiber, but a simpler alternative is time-bin QKD, in which information is encoded into a photon's time of emission [13]. Because true single-photon sources—capable of high speed, low timing jitter, true single photon emission into a well-defined spatial mode—are not yet commercially viable, early experimental and current commercial QKD demonstrations use a practical approximation to the single photon source by strongly attenuating the light emitted from a typical laser. This results in a weak-coherent state, with a Poissonian distribution in photon number.

2) CONTINUOUS-VARIABLE QKD

In addition to discrete variables such as polarization, information can also be encoded into continuous variables (CVs) in QKD [14]. CVs can consist of amplitude, phase, position, momentum, and, in the case of light, quadratures, which can be written as a linear combination of the amplitude and phase operators. The quadratures can be measured in several ways. Amplitude can be inferred by measuring optical power, which is done by directly detecting a beam of light with a photodiode or power meter. The generalized quadrature can be measured through homodyne detection or heterodyne detection.

In the case of homodyne or heterodyne detection, the phase or amplitude of the field can be inferred, giving access to a two-dimensional phase space (while direct detection measures only along one dimension). Access to this phase space provides variables that can act as information carriers, just as polarization can carry information in the discrete case. Coherent states, which are the light states emitted by lasers, can occupy any position in this phase space, with some uncertainty dictated by quantum mechanics. Modulation on this position can be used as a signal, which can be demodulated through homodyne or heterodyne detection.

3) ENTANGLED-PHOTON QKD

Entangled-photon pairs possess the property that identical measurements performed separately on the two photons yield correlated results. In entangled photon QKD schemes (such as [15]), a discrete entanglement source sends photons to Alice and Bob (each receives one of the two entangled photons), who then carry out measurements in randomly chosen bases. The protocol proceeds just as with single-photon QKD, except that Alice's role changes from "prepare and transmit" to "receive and measure." One advantage of entangled-photon QKD is that the source does not have to be located with Alice or Bob, because they can perform Bell inequality measurements [15] in order to determine that their photon source truly is entangled and hasn't been compromised (or that an eavesdropper is not present). Another

advantage is that both Alice and Bob will have truly random data, and so no random number generator is needed for data encoding.

C. QKD LIMITATIONS

QKD, in all its forms, has limitations. One of the most important concerns is the optical losses in the quantum channel; higher losses result in lower secure key rates. For the most conservative security proofs, one must assume any transmission loss is a tap on the quantum channel, providing quantum information to Eve. The dominant contributor to loss is the distance between Alice and Bob; other sources of loss include poor or degraded optical fiber, poor splices and connections, or excessive reflection at patch panel connectors.

Another limitation to QKD is cost. Fiber optic cables are expensive to deploy, and though telecommunications infrastructures are present and growing, it is not clear how much overlap there will be with the electric grid. Building an additional parallel fiber network for use solely by the grid is possible, but a difficult value proposition considering a cost of several dollars per foot. Free space links can mitigate this expense, but due to the necessity of line of sight, effective distances in the real world would be limited using this method.

The detection apparatus is also quite costly. For both single- and entangled-photon QKD, detectors capable of registering the arrival of a single photon are required. As with the variety of photon sources available, there exists a considerable variety of proven and experimental single-photon detectors, all with their relative merits. In general, single-photon detectors can be fast, efficient, or cost-effective; but, thus far, these three traits cannot be found in a single package. Depending on the efficiency, which directly affects key rate, single-photon detectors at telecom wavelengths can cost $20,000 or more. They are considerably cheaper (and generally more efficient) for visible wavelengths, but visible photons typically do not propagate well over telecom fiber links. Single photon detection is not required for CV QKD schemes, and so detectors are considerably less costly. However, these savings are offset by the additional complexity of transmitting (or generating) a local oscillator for homodyne or heterodyne detection.

D. THE FUTURE OF QKD IN THE SMART GRID

Because QKD generates identical keys at separate locations, they are especially well-suited to symmetric encryption and secure hash. The former is primarily used for data confidentiality and the same key is used for both encryption and decryption. The recommended symmetric key algorithm is AES with a key size of 256 or 512 bits. Secure hashing is used to generate a cryptographic checksum/hash on data. A hash algorithm has the property that it is computationally infeasible to infer a message that corresponds to a given message digest or to find two different messages that produce the same message digest. A secure hash uses a symmetric key to detect both accidental and intentional modifications of the data. The recommended message authentication and data integrity algorithms are hash-based message authentication code (HMAC) [16] and Galois message authentication code (GMAC) [17]. These cryptographic authentication techniques use a hash function and a secret key to generate and verify an authentication tag on data. When these algorithms are used, the message is not encrypted. The hash is recomputed at the receiving end and compared to the hash generated at the transmission end. The hash function should be Secure Hash Algorithm-2 (SHA-2) or SHA-3.

Despite the promise of better security, QKD has not seen widespread implementation in applications requiring secure communication, however, it may be a good fit for the grid. The main reason is that QKD's biggest shortcoming—short operation distance—is not as much of a limitation on the grid. After all, a smart meter needs to be able to communicate with devices on the local power network, not with a device on the other side of the planet. Another potential synergy between the grid and QKD is the inherent point-to-point nature of both. The QKD protocols described above allow key distribution between only two parties, and this is viewed as a limitation in most contexts. However, most components in a smart grid infrastructure will only need to communicate with a limited subset of devices, and the relationships between devices may not change over the lifetime of the network. Using QKD, it is possible, for example, to have secure communication between a consumer smart meter and a power substation independent of the rest of the network.

It is almost certain that QKD component costs will come down. Therefore, the real question for QKD and the grid is not whether QKD can offer better security, but rather which QKD solutions are best. It is unlikely that a single solution will work for all parts of the grid. For every place that QKD is considered, engineers will need to evaluate factors such as the existing infrastructure, the distance between nodes, bandwidth requirements, etc. Differing security requirements should also be taken into account. Consumer information, for example, is not critical for maintaining the availability of the grid but must be kept confidential for a very long period of time. Alternatively, the integrity of communications related to real-time control of the grid is critical at the time of execution, but the long-term confidentiality is not as critical. For these reasons, it is expected that QKD security solutions for the grid will take many forms. In some places, it will be possible to take advantage of existing fiber links for QKD at telecom wavelengths. In others, it might make more sense to implement short free-space links. The challenge is to find the best match between the many QKD solutions and the many smart grid needs.

Hybrid quantum technologies, for example, consisting of a quantum 'backbone' and wireless local area links, may offer unique solutions for the grid. It is not yet clear whether hybridized quantum-classical technologies will offer the provably secure communication as purely quantum technologies can.

III. QKD USE CASE SELECTION AND ANALYSIS METHOD

QKD offers capabilities that may provide improved security for critical infrastructures, including the energy sector. However, it is not expected that QKD can or should be adopted as a wholesale replacement of existing security tools. Rather, QKD should be viewed as a complementary technology and should be deployed where it offers a clear advantage over other approaches. In this section, we outline our method for selecting energy sector use cases where QKD has potential viability. We start with the framework described in the National Institute of Standards and Technology (NIST) Special Publication 1108r4, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0* [18], which organizes the energy sector into complementary domains, each with several use cases to be considered. We further focus the analysis by selecting only those use cases for which the loss of confidentiality and/or data integrity would have a high or moderate impact on grid operations. Finally, the remaining use cases are analyzed in the context of the suitability of QKD as a potential solution.

The remainder of this section provides additional detail on the use case framework, the down-selection criteria, and the QKD suitability factors used for the use case analysis. Detailed descriptions of the use cases and the resultant analysis is presented in Section IV.

The generation and distribution of symmetric keys via QKD may be used to address the following security objectives in the grid: confidentiality and integrity. Confidentiality addresses limiting information access and disclosure and system access to only authorized users, as well as preventing access by, or disclosure to, unauthorized parties. With QKD implementations, this means the data/information is encrypted with a symmetric key. If the data/information is improperly accessed by an unauthorized individual, the data is illegible unless the individual also has the symmetric key. Confidentiality includes means for protecting personal privacy and proprietary information. Integrity means guarding against improper information modification or destruction, and it also includes ensuring information non-repudiation and authenticity.[1] QKD integrity should include both data integrity and message authentication.

A. SELECTION OF QKD USE CASES

This section provides an overview of the conceptual model and domains defined in the NIST publication [18] and the objectives of cybersecurity as applicable to the power grid and deployment of QKD. This content is used in the selection, organization, and analysis of potential QKD use cases.

The NIST Smart Grid Conceptual Model [18] describes the overall composition of electric grid systems and applications. In its latest version (Release 4.0), the model reflects large increases in the number and types of DERs used throughout the grid, the increasing importance and automation of distribution systems, new customer interactions and assets, and the role of service providers in distribution systems. The model is illustrated in Fig. 2, and it identifies seven domains within the smart grid: Transmission, Distribution, Operations, Generation including DERs, Markets, Customer, and Service Provider.

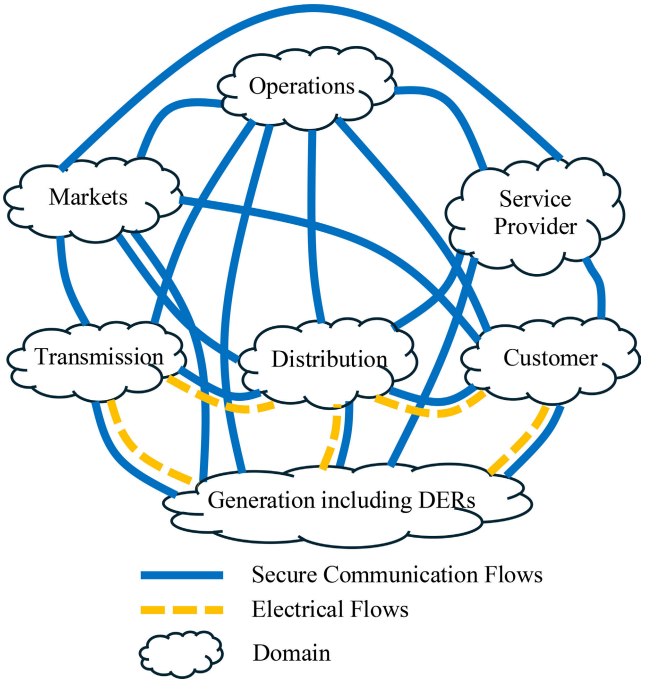

FIGURE 2. Smart grid conceptual model [18].

QKD is a secure key distribution protocol whose security stems from the very nature of quantum physics. Combined with the existing encryption algorithms, QKD offers high confidentiality of the channel data. QKD can detect tampering of the quantum channel and discard the currently generated key, which results in high integrity data transmission. Use of QKD systems with a low-key rate may be limited to applications with moderate data availability requirements. These features of QKD may be used in the selection of a use case. The security impact of the loss of confidentiality, integrity, and/or availability is summarized in Section IV for each selected use case. The impacts are rated as High, Moderate, or Low according to the following definitions, which are extracted from [19]:

- **High Impact**: The loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals.
- **Moderate Impact**: The loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals.
- **Low Impact**: The loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals.

[1] These definitions are based on the definitions from NIST publications.

QKD solutions are best suited for use cases in which confidentiality and/or integrity are important. Accordingly, we adopted the color scheme in Table 1 in the summary tables for the use case analysis in Section IV.

TABLE 1. The color scheme of the security impact considered in this study.

Confidentiality, Integrity, and Availability	
HIGH	The loss of [Confidentiality, Integrity] is deemed to have a High Impact for this use case.
MODERATE	The loss of [Confidentiality, Integrity] is deemed to have a Moderate Impact for this use case.
LOW	The loss of [Confidentiality, Integrity] is deemed to have a Low Impact for this use case.
Not Rated	No color is shown for Availability, since the impact of loss of availability has little effect on the suitability of QKD for a given use case.[2]

Applying the Confidentiality and Integrity filters to the use cases from NIST SP 1108r4 in [18] resulted in 18 use cases for analysis in the context of QKD functionality. As described above, the selection of these use cases is based on the criticality of high confidentiality and/or high integrity of the data, as these use cases may benefit the most from QKD technology. These use cases are listed briefly below, organized by the smart grid domains described in Fig. 2.

- Customer Domain:
  - Remote connect/disconnect of meter
  - Load management
  - Utility controls customer's distributed resources
- Service Provider Domain: No suitable use cases identified
- Markets Domain:
  - Bulk power electricity market
  - Retail power electricity market
- Operations Domain:
  - Distribution analysis using distribution power data flows
  - Wide area monitoring, protection, and control (WAMPAC) historical data
  - Substation field devices and automated responses
- Generation including DERs Domain
  - Distributed energy resources management (DERMs)
  - Regional transmission organization (RTO)/ independent system operator (ISO) management of central generators and storage
  - DER supervisory control and data acquisition (SCADA) systems
  - Microgrid operations
- Transmission Domain
  - Real-time normal transmission operations using energy management system (EMS) applications and SCADA data
  - Real-time emergency transmission operation
  - Wide area synchrophasor system (WAMPAC)
- Distribution Domain
  - Distribution automation within substations
  - Distribution automation controlling and monitoring feeder equipment
  - Utility performs localized load reduction to relieve circuit and/or transformer overloads

These use cases are described in greater detail in Section IV.

[2]However, the availability requirement was evaluated in this study.

B. QKD EVALUATION CRITERIA AND METHOD

To evaluate selected use cases for QKD applicability, a list of critical QKD operational considerations was established and is presented in this subsection. Some of these considerations follow from the limitations of QKD technology (e.g., distance), while others are related to the use cases themselves. All these factors must be considered when assessing the suitability of QKD for a given use case. The operational considerations are evaluated for each of the use cases discussed in Section IV and each factor is assigned a rating of GOOD, MODERATE, or POOR to indicate how well QKD technology is aligned to the use case requirements with respect to that factor. The meanings of these ratings are given in the descriptions of the operational considerations below. But, in general, the ratings can be interpreted as described in Table 2.

TABLE 2. High-level rating guide for the QKD considerations.

GOOD	QKD technology is a GOOD match for this use case—commercially available QKD systems should provide good performance.
MODERATE	QKD technology is a MODERATELY GOOD match for this use case. Minor modifications to the use case and/or the commercially available QKD system would likely be needed.
POOR	QKD technology is a POOR match for this use case. Technological advances are needed before QKD should be considered for this use case.

Finally, as QKD technology matures, it is expected that many of the current limitations will become less restrictive. For example, the requirement for single mode dark fiber may not be needed in the near future, allowing for a much wider use of QKD systems in the smart grid.

C. FACTORS AFFECTING QKD OPERATION

1) AVAILABILITY OF SINGLE MODE DARK FIBER

Because QKD involves the generation, transmission, and detection of very weak optical fields, dedicated fiber links with no additional traffic (i.e., 'dark' fiber) is preferred. Most commercial QKD systems perform best with two fibers—one

for the quantum signal and one for the classical communication between Alice and Bob. Moreover, the quantum link must not include any amplifiers or classical repeaters. However, QKD solutions employed with in-use fiber are possible at the expense of the key rate and the maximum distance, and they are dependent on the specific QKD system employed. Unavailability of fiber, either due to no excess capacity (dark or in-use), or non-existence of deployed optical fiber, severely impacts deployment of QKD with all use cases. For each use case analyzed in Section IV, the suitability of QKD with respect to *Fiber Availability* will be rated according to the guide provided in Table 3.

TABLE 3. Rating guide for the "Fiber Availability" QKD consideration.

Fiber Availability	
GOOD	Dark fiber is typically available between the QKD nodes for this use case.
MODERATE	Fiber is typically available between the QKD nodes for this use case, but the fiber carries other communication traffic.
POOR	Fiber is typically not available between the QKD nodes for this use case.

2) COMMUNICATION NETWORK ARCHITECTURE

Single-photon QKD solutions inherently assume point-to-point network connections. Other network architectures can be realized by linking multiple point-to-point connections and/or through the use of switches. However, this introduces additional complexity. For each use case analyzed in Section IV, the suitability of QKD with respect to *Communication Network Architecture* will be rated according to the guide provided in Table 4.

TABLE 4. Rating guide for the "Communication Network Architecture" QKD consideration.

Communication Network Architecture	
GOOD	One or more unchanging point-to-point QKD links are sufficient for this use case (1-to-1 connectivity).
MODERATE	Point-to-point QKD links are sufficient for this use case, but node pairings may change (any-to-any connectivity).
POOR	Point-to-point QKD links are not adequate for this use case (e.g., broadcast) or would require overly complex network management schemes.

3) QKD LINK DISTANCE

Because QKD involves the transmission of very weak optical fields, QKD solutions perform best over short distances, where loss is not significant. While the distance between the nodes in some commercial QKD systems can exceed 100 km, the secret key rates are much lower. Distances less than 50 km can easily be realized with commercially available QKD systems. Distances up to 250 km can be realized with "trusted-node" links or with advanced QKD techniques. Distances greater than 250 km would require lengthy trusted-node links. In general, the effective distance for QKD solutions operating on used/lit fiber is much shorter. For each use case analyzed in Section IV, the suitability of QKD with respect to *QKD Link Distance* will be rated according to the guide provided in Table 5.

TABLE 5. Rating guide for the "QKD Link Distance" QKD consideration.

QKD Link Distance	
GOOD	The distance between QKD nodes is less than 50 km for this use case.
MODERATE	The distance between QKD nodes is more than 50 km but less than 250 km for this use case.
POOR	The distance between QKD nodes is greater than 250 km for this use case.

4) SECRET KEY RATE

The maximum quantum secret key rates for the key distribution in existing commercial systems are on the order of Mbits/second on relatively short dark fiber connections, and less for longer distances. In general, a secret key rate of 10 bps is easily achieved (assuming moderate distances and dark fiber availability). This rate is sufficient for the exchange of two 256-bit keys per minute. For each use case analyzed in Section IV, the suitability of QKD with respect to *Secret Key Rate* will be rated according to the guide provided in Table 6.

TABLE 6. Rating guide for the "Secret Key Rate" QKD consideration.

Secret Key Rate	
GOOD	A secret key rate of 10 bps is sufficient for this use case.
MODERATE	The secret key rate for this use case must be greater than 10 bps but does not need to exceed 10 kbps.
POOR	A secret key rate of 10 kbps is insufficient for this use case.

5) COMPUTE CAPACITY AT EACH NODE

The QKD protocols require computing resource availability at each node to run dedicated key distillation software [20]. It is likely that the existing processing resources at the nodes used for data encryption and transmission can accommodate the key distillation compute requirements. For each use case analyzed in Section IV, the suitability of QKD with respect to *Compute Capacity at Each Node* will be rated according to the guide provided in Table 7.

TABLE 7. Rating guide for the "Compute Capacity at Each Node" QKD consideration.

Compute Capacity at Each Node	
GOOD	The compute capacity at the QKD nodes for this use case is sufficient for QKD functions (e.g., desktop/laptop machine, Raspberry Pi, etc.).
MODERATE	The sites for the QKD nodes in this use case typically have limited compute capacity (e.g., legacy equipment).
POOR	Computing resources are unavailable at the QKD node locations for this use case.

6) OPERATING TEMPERATURE AND RELATIVE HUMIDITY

Existing photon generating and detection components are sensitive to the environment. The requirements for the operating temperature and relative humidity are therefore more stringent than those for general electronics. For each use case analyzed in Section IV, the suitability of QKD with respect to *Operating Temperature and Relative Humidity* will be rated according to the guide provided in Table 8.

TABLE 8. Rating guide for the "Operating Temperature and Relative Humidity" QKD consideration.

Operating Temperature and Relative Humidity	
GOOD	The sites for the QKD nodes for this use case are in environmentally controlled spaces (i.e., data center equivalent).
MODERATE	The sites for the QKD nodes for this use case are in interior unconditioned spaces (e.g., telecom room).
POOR	The sites for the QKD nodes for this use case are exterior spaces (e.g., pole or cabinet).

7) QKD RESOURCES REQUIRED

Full implementation of a given use case will be expensive, not only because of the cost of QKD systems but also because of the number of systems required. While the resource requirements will scale with the size of the utility or transmission operator, this metric will make it possible to compare use cases for a given operator. For each use case analyzed in Section IV, the suitability of QKD with respect to *QKD Resources Required* will be rated according to the guide provided in Table 9.

TABLE 9. Rating guide for the "QKD Resources Required" QKD consideration.

QKD Resources Required	
GOOD	A full implementation of this use case in a *medium-sized* operator would require fewer than 100 QKD nodes.
MODERATE	A full implementation of this use case in a *medium-sized* operator would require more than 100 but fewer than 500 QKD nodes.
POOR	A full implementation of this use case in a *medium-sized* operator would require more than 500 QKD nodes.

IV. ANALYSIS AND DISCUSSION OF QKD USE CASES

The selection of the 18 smart grid use cases is based on the criticality of high confidentiality and/or high integrity of the data as these cases may benefit the most from QKD technology. They are organized using the smart grid domains illustrated in Fig. 2. The analysis results presented in this section are based on subject matter experts' (SMEs) opinions and have been verified with SMEs at two power utilities.

A. CUSTOMER DOMAIN

The customer is ultimately the stakeholder that the entire grid was created to support. This is the domain where electricity is consumed but is increasingly a domain where electricity is actively managed and generated as well. Typically, three customer types are defined: residential, commercial, and industrial. Actors in the Customer domain enable customers to manage their energy usage and generation. Some actors also provide control and information flow between the Customer domain and the other domains. The boundaries of the Customer domain are typically considered to be the utility meter and the energy services interface (ESI). The ESI provides a secure interface for utility- or service provider-to-customer interactions. The ESI in turn can act as a bridge to facility-based systems, such as a building automation system (BAS) or a customer's premise management system.

The primary requirements in the customer domain are for data confidentiality to ensure that user data is not improperly accessed and data integrity to ensure that commands are not maliciously altered. Currently, smart meter cryptography is configured and maintained/updated by the vendor. Meters include both symmetric and asymmetric cryptography. There are various state privacy laws that define a utility's role, including management of behind-the-meter devices. This may include appliances. The majority of home-based DERs/renewable energy devices, such as solar photovoltaic (PV) and windmills, do not include cyber security controls. Included herein are three Customer domain use cases:

1) C1. REMOTE CONNECT/DISCONNECT OF METER

The connect/disconnect of the meter is performed remotely for the following reasons: move-in, reinstatement on payment, move-out, nonpayment, or emergency load control. Also, the control of the meter may be executed as a broadcast message to multiple users at a time which violates the point-to-point requirement.

2) C2. LOAD MANAGEMENT

Utility controls customer appliances such as air conditioners, water heaters, and pool pumps. A utility also executes direct load control and load shedding, demand side management,

load shift scheduling, curtailment planning, and selective load management through home area networks.

3) C3. UTILITY CONTROLS CUSTOMER'S DERS

A utility can use customer's DERs to provide energy back to the electrical system assuming the customers are enrolled in utility programs that allow their DERs to be used for load support or to assist in maintaining power quality.

A summary of results for the Customer domain is presented in Table 10. The suitability of QKD for these use cases is either Moderate or Good for most of the factors analyzed. However, all three use cases are rated Poor for Fiber Availability since most utilities are unlikely to have widespread fiber to the home, although this is expected to improve in the future. In addition, full implementation of these use cases would require a QKD node at each customer served by a given utility. For this reason, all three use cases are rated Poor for QKD Resources Required.

B. SERVICE PROVIDER DOMAIN

Actors in the Service Provider domain perform services to support the business processes of power system producers, distributors, and customers. These business processes range from traditional utility services, such as billing and customer account management, to enhanced customer services, such as management of energy use and home energy generation. There are no use cases included in this domain. The tasks are included in the Customer and Markets domains.

C. MARKETS DOMAIN

Markets are where grid assets and services are bought and sold. Some markets yet to be created may be instrumental in defining the smart grid of the future, particularly with DERs and aggregated DERs. Entities in the Markets domain exchange price information and balance supply and demand within the power system. The boundaries of the Markets domain include the edge of the Operations domain where control happens, the domains supplying assets (Generation including DERs, Transmission, and Distribution), the Service Provider domain, and the Customer domain. In short, the Markets domain interfaces with all domains of the smart grid. Included herein are two Markets domain use cases:

1) M1. BULK POWER ELECTRICITY MARKET

The bulk power wholesale market is conducted through RTOs and ISOs and is handled independently from actual operations. Even though there are no direct operational security impacts, there may be significant financial security impacts. Federal Energy Regulatory Commission (FERC) Order No. 2222 [21] instructs RTOs and ISOs to allow DER aggregations to participate directly in the wholesale markets and establish a new category of market participants—namely DER aggregators (DERAs). The order removes the barriers preventing DERs from competing on a level playing field in the organized capacity, energy and ancillary services markets run by regional grid operators.

2) M2. RETAIL POWER ELECTRICITY MARKET

The retail power electricity market is currently small, compared to the bulk power market. It typically involves aggregators and energy service providers bidding customer-owned generation or load control into both energy and ancillary services.

A summary of results for the Markets domain is presented in Table 11. The suitability of QKD for these use cases is either Moderate or Good for most of the factors analyzed, but each use case is rated Poor for at least one factor. For the Bulk Power Electricity Market use case, the QKD Link Distance factor is rated Poor because the participants are likely to be spread across a large geographic area. In addition, the Secret Key Rate factor is rated Poor because, although the amount of data needed to execute bidding and transactional communication may be modest, the nature of competitive markets is such that the system may need to accommodate high *peak* rates for real-time markets. Lastly, because the Retail Power Electricity Market use case involves communication between independent organizations, fiber availability is likely to be inconsistent across QKD nodes. Accordingly, the Fiber Availability factor is rated Poor for this use case.

D. OPERATIONS DOMAIN

Actors in the Operations domain are responsible for the smooth operation of the power system. Today, the majority of such operation functions are the responsibility of a regulated utility. The security requirements include both confidentiality and integrity. Confidentiality is important to ensure that the power flow models and historical data are not maliciously altered. Integrity is required for the substation field devices. Included herein are three operations domain use cases:

1) O1. DISTRIBUTION ANALYSIS USING DISTRIBUTION POWER FLOW MODELS

Distribution analysis software applications use models of the power system to validate the raw data, assess real-time and future conditions, and issue the appropriate actions. The applications may be located in the field equipment for local assessments and control, and/or may be centralized for global assessment and control.

2) O2. WIDE AREA MONITORING, PROTECTION, AND CONTROL (WAMPAC) HISTORICAL DATA

The Data Historian is a time-stamped database that stores real-time operational data that can be accessed and used for a wide range of purposes such as visualization, event tracking, production reporting, and consumption by other systems for Advanced Analytics and Asset Performance Management.

TABLE 10. Summary of results for the customer domain.

Customer Domain								
Use Case	Security Impact	QKD Suitability Considerations						
		Fiber	Network Arch.	Distance	Rate	Compute	Temp. / Humid.	Resources
Remote Connect / Disconnect of Meter	C: H I: H A: M	POOR	GOOD	GOOD	GOOD	MOD	POOR	POOR
Load Management	C: L I: H A: M	POOR	GOOD	GOOD	GOOD	MOD	GOOD	POOR
Utility Controls Customer's DERs	C: H I: H A: L	POOR	GOOD	GOOD	GOOD	MOD	MOD	POOR

TABLE 11. Summary of results for the markets domain.

Markets Domain								
Use Case	Security Impact	QKD Suitability Considerations						
		Fiber	Network Arch.	Distance	Rate	Compute	Temp. / Humid.	Resources
Bulk Power Electricity Market	C: H I: H A: M	MOD	MOD	POOR	POOR	GOOD	GOOD	GOOD
Retail Power Electricity Market	C: H I: H A: M	POOR	MOD	GOOD	MOD	MOD	GOOD	MOD

TABLE 12. Summary of results for the operations domain.

Operations Domain								
Use Case	Security Impact	QKD Suitability Considerations						
		Fiber	Network Arch.	Distance	Rate	Compute	Temp. / Humid.	Resources
Distribution Analysis using Distribution Power Flow Models	C: L I: H A: H	MOD	GOOD	GOOD	MOD	GOOD	MOD	MOD
WAMPAC Historical Data	C: H I: H A: L	MOD	GOOD	POOR	POOR	GOOD	GOOD	GOOD
Substation Field Devices and Automated Responses	C: M I: H A: M	POOR	GOOD	GOOD	GOOD	POOR	POOR	MOD

3) O3. SUBSTATION FIELD DEVICES AND AUTOMATED RESPONSES

Data inputs from field devices at substations (as well as in the field) are used by the distribution management system (DMS) to report system state. This data is used to initiate automated responses.

A summary of results for the Operations domain is presented in Table 12. The suitability of QKD for these use cases is either Moderate or Good for most of the factors analyzed, but two of the use cases are rated Poor for two or more factors. For the WAMPAC Historical Data use case, the Distance and Rate factors are rated Poor because the repository may be located far from the participating sites and because the amount of data delivered to the repository is expected to be large. The Substation Field Devices and Automated Responses use case is rated Poor for three factors, all related to the fact that the use case involves data from field devices, which are less likely to have adequate fiber available and are unlikely to have adequate environmental controls and computing resources. The Distribution Analysis using Distribution Power Flow Models use case is notable in this domain as having *all* factors rated either Moderate

or Good. These ratings assume the existence of QKD links between substations and a control center, all within a single utility. If the links extend to field equipment, then the rating should be downgraded to Poor for several factors.

E. GENERATION INCLUDING DER DOMAIN

Electricity generation is the process of creating electricity from other forms of energy and is the first process in delivering electricity to customers. At a logical level, ''generation'' includes traditional large-scale technologies usually attached to the transmission system, such as conventional thermal generation, large-scale hydro generation, and utility-scale renewable installations usually attached to transmission. DERs are associated with generation, storage, and demand response provided in the customer and distribution domains, and with service provider-aggregated energy resources. As the primary electricity supply for the electrical grid, the Generation including DERs domain is electrically connected to the Transmission or Distribution or Customer domain, and shares communications interfaces with all other domains. Included herein are four Generation Including DERs domain use cases:

1) G1. DISTRIBUTED ENERGY RESOURCES MANAGEMENT

The Distributed Energy Resources Management System (DERMS) is a utility system that manages the requests and commands to the DER systems. The DERMS is also responsible for the database of interconnection permits and registrations of DER systems. The DERMS includes load forecasting, real-time monitoring, feeder reconfiguration, virtual and logical microgrids, and distribution planning. In addition, the management provides direct monitoring and control of DERs, shutdown or islanding verification for DERs, plug-in electric vehicle (PEV) management as load, storage, and generation resource, electric storage fill/draw control, renewable energy DERs with variable generation, and small fossil resource management such as backup generators to be used for peak shifting.

2) G2. RTO/ISO MANAGEMENT OF CENTRAL GENERATION AND STORAGE

Both ISOs and RTOs are independent entities, not affiliated with other market players, and the functions of each include day-to-day grid operations, long-term regional planning, billing and settlements, and other wholesale electric market services. RTOs/ISOs coordinate, control, and monitor the electric grid in a specific geographical, multi-state areas. ISOs tend to be smaller in geographic size and some are not subject to FERC jurisdiction (e.g., Canada and central Texas). FERC Order No. 2222 [21] instructs RTOs and ISOs to allow DER aggregations to participate directly in the wholesale markets and establishes a new category of market participants—namely DER aggregators. The order removes the barriers preventing DERs from competing on a level playing field in the organized capacity, energy and ancillary services markets run by regional grid operators.

3) G3. DER SCADA SYSTEMS

DER systems are cyber-physical systems that provide energy and ancillary services to the power grid, typically through the distribution system. This includes solar PV, wind, geothermal and hydroelectric. DER systems can be generators, storage devices, and PEVs if their chargers are capable of managing the charging and discharging processes. SCADA systems are required to manage and control the generation and interconnection of these generation systems.

4) G4. MICROGRID OPERATIONS

As defined by the US Department of Energy [22], a microgrid is a group of interconnected loads and DERs within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island-mode.

A summary of results for the Generation Including DERs domain is presented in Table 13. The QKD suitability factors for three of the four use cases are rated either Good or Moderate for *all* factors. These three use cases involve communication between a utility and either local microgrids or local generation resources. As a result, the distances are likely to be reasonable for QKD. In addition, the microgrids and generation resources are likely to include adequate infrastructure for environmental control, computing resources, etc. The remaining use case, RTO/ISO Management of Central Generation and Storage, was rated Poor for only one factor, QKD Link Distance. The reason is that central generation and storage facilities can be widely spaced.

F. TRANSMISSION DOMAIN

Transmission is the bulk transfer of electrical power from generation sources to distribution through multiple substations. A transmission network is typically operated by a transmission-owning utility, RTO, or ISO, whose primary responsibility is to maintain stability on the electric grid by balancing generation (supply) and load (demand) across the transmission network. Examples of physical actors in the Transmission domain include remote terminal units, substation meters, protection relays, power quality monitors, PMUs, sag monitors, fault recorders, and substation user interfaces. The security requirement primarily focuses on integrity. Included herein are three Transmission domain use cases:

1) T1. REAL-TIME NORMAL TRANSMISSION OPERATIONS USING ENERGY MANAGEMENT SYSTEM (EMS) APPLICATIONS AND SCADA

Real-time operations involve monitoring and controlling the transmission system using the SCADA and EMS. The types of information exchanged include monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy). In addition, the operator command and

TABLE 13. Summary of results for the generation including DERs domain.

Generation Including DERs Domain								
Use Case	Security Impact	QKD Suitability Considerations						
		Fiber	Network Arch.	Distance	Rate	Compute	Temp. / Humid.	Resources
Distributed Energy Resources Management	C: H I: H A: L	MOD	GOOD	GOOD	GOOD	MOD	MOD	MOD
RTO/ISO Management of Central Generators and Storage	C: L I: H A: H	MOD	GOOD	POOR	GOOD	GOOD	GOOD	GOOD
DER SCADA Systems	C: M I: H A: M	MOD	GOOD	GOOD	MOD	MOD	POOR	MOD
Microgrid Operations	C: L I: H A: M	MOD	GOOD	GOOD	MOD	MOD	MOD	GOOD

TABLE 14. Summary of results for the transmission domain.

Transmission Domain								
Use Case	Security Impact	QKD Suitability Considerations						
		Fiber	Network Arch.	Distance	Rate	Compute	Temp. / Humid.	Resources
Real-Time Normal Trans. Ops using EMS Applications & SCADA	C: L I: H A: H	MOD	GOOD	POOR	MOD	GOOD	GOOD	GOOD
Real-Time Emergency Transmission Operation	C: L I: H A: H	MOD	GOOD	POOR	MOD	GOOD	GOOD	GOOD
Wide Area Synchrophasor System	C: L I: H A: H	MOD	GOOD	POOR	POOR	GOOD	GOOD	GOOD

control actions include supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions. Also, closed-loop actions include protective relays tripping circuit breakers upon power system anomalies as well as controlling voltage, volt-ampere reactive (VAR) power, and real power.

2) T2. REAL-TIME EMERGENCY TRANSMISSION OPERATION

Emergency transmission operations include automated actions taken by the power system as well as the operator-controlled actions. The automated actions are emergency operations handling under-frequency load/generation shedding, under-voltage load shedding, load tap changer control/blocking, shunt control, series compensation control, system separation detection, and wide area real-time instability recovery. The operator-controlled actions include managing emergency alarms and system restoration. SCADA systems also respond to emergencies by running disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers, and pre-arming of fast acting emergency automation.

3) T3. WIDE-AREA SYNCHROPHASOR SYSTEM

Currently, the wide area synchrophasor system (or WAMPAC) provides synchronized and time-tagged voltage and current phasor measurements as a monitoring function. Using the synchrophasor data for automated corrective action is hobbled by not having access to the phase angles between local and remote measurements. WAMPAC systems often center around synchrophasor technology and the devices that generate, receive, and utilize this synchrophasor data. WAMPAC systems should be setup to include all components from the PMUs to the WAMPAC applications leveraging that data, including other intermediate devices such as the servers that manage the PMUs, devices that provide alignment services like Phasor Data Concentrators

TABLE 15. Summary of results for the distribution domain.

Distribution Domain								
Use Case	Security Impact	QKD Suitability Considerations						
		Fiber	Network Arch.	Distance	Rate	Compute	Temp. / Humid.	Resources
Dist. Automation within Substations	C: L I: H A: H	MOD	GOOD	GOOD	MOD	GOOD	GOOD	GOOD
Dist. Automation Control/Monitor Feeder Equipment	C: L I: H A: H	POOR	GOOD	GOOD	GOOD	MOD	MOD	MOD
Utility-Directed Localized Load Management	C: H I: H A: H	POOR	GOOD	GOOD	GOOD	MOD	MOD	MOD

(PDCs), phasor gateways, phasor data stores, and other such components.

A summary of results for the Transmission domain is presented in Table 14. The QKD suitability factors for all use cases are rated either Good or Moderate for most factors. However, all three use cases require QKD between a transmission control center and transmission substations. Because these distances can be quite large, all three use cases are rated Poor for QKD Link Distance.

G. DISTRIBUTION DOMAIN

The Distribution domain is the electrical interconnection between the Transmission domain, the Customer domain, and the metering points for consumption, distributed storage, and distributed generation. Similar to the Generation including DERs domain, the Distribution domain may contain DERs, such as electrical storage, peaking generation units, or other medium-scale assets such as community solar installations. The electrical distribution system may be arranged in a variety of structures, including radial, looped, or meshed. The reliability of the distribution system varies depending on its structure, the types of configuration and control devices that are implemented, and the degree to which those devices communicate with each other and with entities in other domains. The primary security objective is integrity with confidentiality as a secondary objective for one use case. Included herein are three Distribution domain use cases:

1) D1. DISTRIBUTION AUTOMATION (DA) WITHIN SUBSTATIONS

DA within substations involves monitoring and controlling of the following equipment: SCADA distribution equipment, substation distribution equipment, substation protection equipment, and reclosers. This involves over-the-network monitoring and controlling of equipment in distribution substations.

2) D2. DISTRIBUTION AUTOMATION MONITORING AND CONTROLLING FEEDER EQUIPMENT

Operators and distribution applications monitor the feeder equipment and determine whether any actions should be taken. The list of possible actions includes remotely open or close automated switches, remotely switch capacitor banks in and out, remotely raise or lower voltage regulators, block local automated actions, send updated parameters to feeder equipment, interact with equipment in underground distribution vaults, retrieve power system information from smart meters, automate emergency response, and provide dynamic rating of feeders.

3) D3. UTILITY PERFORMS LOCALIZED LOAD REDUCTION TO RELIEVE CIRCUIT AND/OR TRANSFORMER OVERLOADS

Localized load reduction is performed to temporarily curtail the load in a specific area to reduce the impact on specific equipment. This scenario describes the integrated use of the AMI system, the demand response system, other load reduction systems, and the SCADA/EMS to achieve this goal.

A summary of results for the Distribution domain is presented in Table 15. The suitability of QKD for these use cases is either Moderate or Good for most of the factors analyzed. In fact, only Fiber Availability was rated Poor for these use cases, and only for two of the three. The Distribution Automation within Substations use case requires QKD between a control center and substations. Because the nodes are utility-owned, fiber availability is likely to be consistent across nodes and Fiber Availability is rated Moderate for this use case. This factor is rated Poor for the other two use cases because QKD would be needed between a control center and the equipment below substations, where fiber is less likely to be available.

V. CONCLUSION

As the electric power industry is actively working towards a smarter grid, with numerous sensors and controls across

various segments of the grid, information transmission across several points in the grid will exponentially increase. There is an urgent need for novel solutions to secure the information for protecting the confidentiality, integrity, and availability of various grid subsystems. This study examined the use of QKD to provide secure communic ations between different points of the grid. This study also identified 7 QKD metrics (factors) along with 18 smart grid use cases of interest for QKD suitability assessment. It provides a basis for developing QKD-centric solutions for smart grid applications.

The biggest drawbacks to QKD solutions on the grid are cost and the current requirement of dark (unused) optical fiber that serves as the quantum channel in all QKD schemes of note. While utilities own a great deal of the existing optical fiber infrastructure, the cost associated with setting aside an individual fiber solely for QKD applications may not necessarily make a worthwhile business case irrespective of the security improvements. Therefore, the utility must perform a realistic cost-benefit analysis with QKD technologies as part of their cybersecurity plan. As the QKD solutions mature and as the cost comes down, one can envision deployment of QKD for energy delivery systems.

Future work is to expand the presented assessment analysis to include a numerical scoring scheme and cost estimate for the applicability of QKD to the various smart grid applications. The ultimate outcome is the development of an application programming interface (API) that provides a quantitative assessment score and cost information about the suitability of QKD to assist energy delivery stakeholders.

ABBREVIATIONS

AES	Advanced encryption standard.
AMI	Advanced metering infrastructure.
API	Application programming interface.
BAS	Building automation system.
CV	Continuous variable.
DA	Distribution automation.
DERs	Distributed energy resources.
DERAs	DER aggregators.
DERMS	Distributed energy resources management system.
DMS	Distribution management system.
DOE	Department of Energy.
EMS	Energy management system.
ESI	Energy services interface.
FERC	Federal Energy Regulatory Commission.
FIPS	Federal Information Processing Standard.
GMAC	Galois message authentication code.
HMAC	Hash-based message authentication code.
ISOs	Independent system operators.
NIST	National Institute of Standards and Technology.
PDCs	Phasor data concentrators.
PEV	Plug-in electric vehicle.
PKI	Public key infrastructure.
PMUs	Phasor measurement units.
PV	Photovoltaic.
QBER	Quantum bit error rate.
QKD	Quantum key distribution.
RTOs	Regional transmission organizations.
SCADA	Supervisory control and data acquisition.
SHA	Secure hash algorithm.
SMEs	Subject matter experts.
VAR	Volt-ampere reactive.
WAMPAC	Wide area monitoring, protection, and control.

ACKNOWLEDGMENT

The authors would like to thank Southern Company for the valuable discussion and feedback on verifying the results presented in this article. This manuscript has been authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the U.S. Department of Energy (DOE). The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes. DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (https://www.energy.gov/doe-public-access-plan).

REFERENCES

[1] P. Surarapu, "Emerging trends in smart grid technologies: An overview of future power systems," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 3, no. 1, pp. 17–24, 2016.

[2] T. Woolf, "Grid modernization," Synapse Energy Econ., Cambridge, MA, USA, Tech. Rep. Synapse Energy Economics, 2024. [Online]. Available: https: //www.synapse-energy.com/expertise/electric-system-planning-wholesale-markets/grid-modernization#:~:text=Grid%20modernization%20incorporates%20new%20technologies,service%20faster%20when%20outages%20occur

[3] K. Amasyali, Y. Chen, B. Telsang, M. Olama, and S. M. Djouadi, "Hierarchical model-free transactional control of building loads to support grid services," *IEEE Access*, vol. 8, pp. 219367–219377, 2020.

[4] U.S. Dept. Energy (DOE), Office Electr. *Grid Modernization and the Smart Grid*. Accessed: Dec. 1, 2024. [Online]. Available: https: //www.energy.gov/oe/grid-modernization-and-smart-grid#:~:text=The%20U.S.%20electric%20grid%20is,just%20generation%20and%20transmission%20infrastructure

[5] X. Zhang, Z. Y. Dong, Z. Wan, C. Xiao, and F. Luo, "Quantum cryptography based cyber-physical security technology for smart grids," in *Proc. 10th Int. Conf. Adv. Power Syst. Control, Operation Manage. (APSCOM)*, Nov. 2015, pp. 1–6.

[6] J. Abulizi, H. Qingsheng, and W. Wei, "Quantum cryptography technology and application in smart grid," in *Proc. IEEE 22nd Int. Conf. Commun. Technol. (ICCT)*, Nov. 2022, pp. 1213–1217.

[7] L. Malina, P. Dobias, J. Hajny, and K.-K.-R. Choo, "On deploying quantum-resistant cybersecurity in intelligent infrastructures," in *Proc. 18th Int. Conf. Availability, Rel. Secur.*, Aug. 2023, pp. 1–10.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[9] *Advanced Encryption Standard (AES)*, Standard FIPS PUB 197, NIST, May 2023.

[10] M. S. Zubairy, "No-cloning theorem and quantum copying," in *Quantum Mechanics for Beginners: With Applications To Quantum Communication and Quantum Computing*. Oxford, U.K.: Oxford Academic, 2020.

[11] D. Dieks, "Communication by EPR devices," *Phys. Lett. A*, vol. 92, no. 6, pp. 271–272, Nov. 1982.

[12] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology—EUROCRYPT* (Lecture notes in computer science), vol. 765. Berlin, Germany: Springer, 1994, pp. 410–423.
[13] A. Müller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," *Appl. Phys. Lett.*, vol. 70, no. 7, pp. 793–795, Feb. 1997.
[14] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A, Gen. Phys.*, vol. 61, no. 1, Dec. 2000, Art. no. 010303.
[15] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.
[16] M. Bellare, "New proofs for NMAC and HMAC: Security without collision resistance," *J. Cryptol.*, vol. 28, no. 4, pp. 844–878, Oct. 2015.
[17] M. Dworkin, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Standard 800-38D, NIST Special Publication, 2007.
[18] A. Gopstein, C. Nguyen, C. O'Fallon, N. Hastings, and D. Wollman, "NIST framework and roadmap for smart grid interoperability standards," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 1108r4, 2021.
[19] *Standards for Security Categorization of Federal Information and Information Systems*, Standard FIPS PUB 199, NIST, Feb. 2004.
[20] J. Constantin, R. Houlmann, N. Preyss, N. Walenta, H. Zbinden, P. Junod, and A. Burg, "An FPGA-based 4 mbps secret key distillation engine for quantum key distribution systems," *J. Signal Process. Syst.*, vol. 86, no. 1, pp. 1–15, Jan. 2017.
[21] *Participation of Distributed Energy Resource Aggregations in Markets Operated By Regional Transmission Organizations and Independent System Operators*, Standard FERC Order 2222, FERC, Sep. 2020.
[22] "Microgrid overview," Dept. U.S. Dept. of Energy, Grid Deployment Office, Tech. Bull., Jan. 2024. [Online]. Available: https://www.energy.gov/sites/default/files/2024-02/46060_DOE_GDO_Microgrid_Overview_Fact_Sheet_RELEASE_508.pdf

WARREN GRICE received the B.S. degree from Western Kentucky University, in 1989, and the Ph.D. degree from the Institute of Optics, University of Rochester, USA, in 1998. He is currently a Distinguished Research Scientist with the Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN, USA. He has numerous publications (including journals, conference proceedings, book chapters, and technical reports) in addition to numerous presentations at professional conferences and international symposia. His research interests include quantum information science, specializing in quantum light sources.

MOHAMMED OLAMA (Senior Member, IEEE) received the B.S. and M.S. (Hons.) degrees in electrical engineering from the University of Jordan, Amman, Jordan, in 1998 and 2001, respectively, and the Ph.D. degree from the Electrical Engineering and Computer Science (EECS) Department, The University of Tennessee at Knoxville, Knoxville TN, USA, in 2007. He is currently a Senior Research Scientist with the Computational Sciences and Engineering Division, Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, USA. He is also an Adjunct Associate Professor with the EECS Department, The University of Tennessee at Knoxville. At ORNL, he has led and participated in several projects under various DOE, DOD, and DHS programs. He has been involved in various modeling, simulations, controls, and communications projects for improved critical infrastructure efficiency, reliability, and security including the smart grid and healthcare. He has more than 180 archival publications (including journals, conference proceedings, book chapters, and technical reports) in addition to numerous presentations at professional conferences and international symposia. His research interests include smart power grids and smart buildings, smart grid communications and control, building-to-grid integration, renewable energy integration, wide-area monitoring and control, microgrid operation and control, cyber-physical systems, complex systems, wireless communications, data analytics, statistical signal processing, and machine learning.

ANNABELLE LEE (Member, IEEE) is currently the Chief Cyber Security Specialist of Nevermore Security. Her experience comprises over 45 years of technical experience in information technology and system design and implementation; 20 years in operational technology and cyber security for the electric sector; and 40 years of cyber security design, specification development, and testing. She has authored or co-authored many documents on cyber security, cryptography, and testing. Currently, she is a Consultant focusing on cyber security for the energy sector. She has worked with utilities around the world. Her areas of expertise include cyber security: strategy and risk management; design and architecture; specification, guidance, and requirements development; assessments against standards; training; and applied cryptography.

PHILIP G. EVANS (Member, IEEE) received the Master of Physics (M.Phys.) degree from the University of Bath, U.K., in 2001, and the Ph.D. degree in physics from The University of Tennessee at Knoxville, in 2007. From 2007 to 2010, he was a Postdoctoral Researcher with the Quantum Information Science Team, Later Group, Oak Ridge National Laboratory, Oak Ridge, TN, USA. In 2010, he joined the Quantum Information Science Group as a Research and Development Staff Member. He is currently a member of the Optical Society of America and the American Physical Society. He has been awarded the ORNL Significant Event Awards twice, the Department of Energy Outstanding Mentor Award, and the UT-Battelle Outstanding Scholarly Output (Team) Award.