energies

MDPI

Article

Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD)

Jongmin Ahn [1], Hee-Yong Kwon [1], Bohyun Ahn [2], Kyuchan Park [1], Taesic Kim [2], Mun-Kyu Lee [1], Jinsan Kim [1] and Jaehak Chung [1,*]

[1] Department of Electrical Engineering and Computer Science, Incheon, INHA University, 100, Inha-ro, Michuhol-gu, Incheon 22212, Korea; anjong3@naver.com (J.A.); heeyong.kr@gmail.com (H.-Y.K.); kyuchan100@gmail.com (K.P.); mklee@inha.ac.kr (M.-K.L.); jskim@nsl.inha.ac.kr (J.K.)

[2] Department of Electrical Engineering and Computer Science, Texas A&M University-Kingsville, MSC 192, 700 University Blvd, Kingsville, TX 78363, USA; bohyun.ahn@students.tamuk.edu (B.A.); Taesic.Kim@tamuk.edu (T.K.)

* Correspondence: jchung@inha.ac.kr

Abstract: Quantum computing is a game-changing technology that affects modern cryptography and security systems including distributed energy resources (DERs) systems. Since the new quantum era is coming soon in 5–10 years, it is crucial to prepare and develop quantum-safe DER systems. This paper provides a comprehensive review of vulnerabilities caused by quantum computing attacks, potential defense strategies, and remaining challenges for DER networks. First, new security vulnerabilities and attack models of the cyber-physical DER systems caused by quantum computing attacks are explored. Moreover, this paper introduces potential quantum attack defense strategies including Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC), which can be applied to DER networks and evaluates defense strategies. Finally, remaining research opportunities and challenges for next-generation quantum-safe DER are discussed.

Keywords: distributed energy resources; post-quantum cryptography; quantum computing attack; quantum key distribution

check for updates

Citation: Ahn, J.; Kwon, H.-Y.; Ahn, B.; Park, K.; Kim, T.; Lee, M.-K.; Kim, J.; Chung, J. Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). *Energies* **2022**, *15*, 714. https://doi.org/10.3390/en15030714

Academic Editors: Jay Johnson, Craig Rieger, Danish Saleem and Paul Skare

Received: 16 December 2021
Accepted: 12 January 2022
Published: 19 January 2022

1. Introduction

Distributed Energy Sources (DER) such as wind turbines and solar panels are being added to the power system as carbon-neutral policies are promoted around the world. Over the past decade, the proportion of PV and wind-turbine power generation has increased. In California, power generated by PV accounted for 21% of the total power supply [1–3]. The number of DERs is on the rise, and the need for a network to control the DER system has increased for the stable operation of the entire system [1–3].

Wind speed and solar radiation cannot be controlled, and the amount of power generated by the DER system entirely relies on these meteorological phenomena. Thus, if the DER system is added to the entire power system without control, the DER system induces active power imbalance between generation and demand sides [4–6]. The need for security of the DER network increases because active power imbalance can shut down or damage the entire system [4–8]. The DER network connects DER devices to DER management systems (DERMS) in order to monitor the current state of DER and control the active power supply of DER. The DER network also connects DERMS to utilities to keep the entire system stable [4–8]. As the amount and importance of information transmitted and received in the DER network also increase, the interest and importance of DER network security also increases [4–15]. Many standards have been established for the security of DER networks [10,16–27]. Essentially, these standards protect the DER network with security protocols based on encryption technology [10,16–28]. However, the development of quantum computing poses a significant threat to the security of current cryptographic systems adopted in DER systems.

Quantum processors have powerful calculation capabilities and can dramatically decrease the time to break existing encryption algorithms [29–32]. According to [32], half of the existing encryption algorithms will become useless because of quantum computing attacks. Despite a new wave in cryptography technology, quantum attack strategy, method, model, and solution have not been researched yet. It is necessary to predict future quantum attacks and identify vulnerabilities of the DER network to protect the DER network against future quantum attacks [4]. In addition, depending on the vulnerability, new encryption and security technologies should be appropriately applied to the DER network [4].

In order to prepare for the quantum era, this paper analyzes the DER network attack model using quantum attacks, and we also predict when quantum attacks become possible. Then, in order to protect these quantum attacks on the DER network, we consider a method to introduce new encryption and security technologies (i.e., quantum key distribution (QKD) and post-quantum cryptography (PQC)) into the DER network. Conventional studies have, respectively, applied PQC or QKD to DER, and their practicality is low [33–41]. In this paper, we consider the practical problems (i.e., network delay, network structure, and cost) when PQC and QKD are simultaneously applied to the DER network. The contributions of the paper are summarized as follows:

1. Estimate when quantum attacks can be possible by analyzing current quantum computing technology trends;
2. Predict the possible quantum attacks on the DER network;
3. When PQC is applied to the DER network, analyze the network delay and compare this delay with the IEEE 2030.5 protocol;
4. To apply QKD to the DER network and analyze QKD in terms of communication distance, data rate, and cost;
5. When PQC and QKD are simultaneously applied to the DER network, we propose a new DER network structure by considering network delay and implementation cost.

This paper is organized as follows. In Section 2, we analyze the current state of quantum computer development and predict when a quantum attack becomes possible. We also estimate what types of quantum attacks are possible for the DER network and analyze the impact of those attacks on the entire power system in Section 2. Section 3 introduces technologies to defend against the predicted quantum attack in Section 2. We also analyze the issues to be considered when applying this technology to DER. Section 4 concludes and describes future research by the DER network to prepare for the quantum era.

2. Prediction of Future Quantum Attacks on DER Network

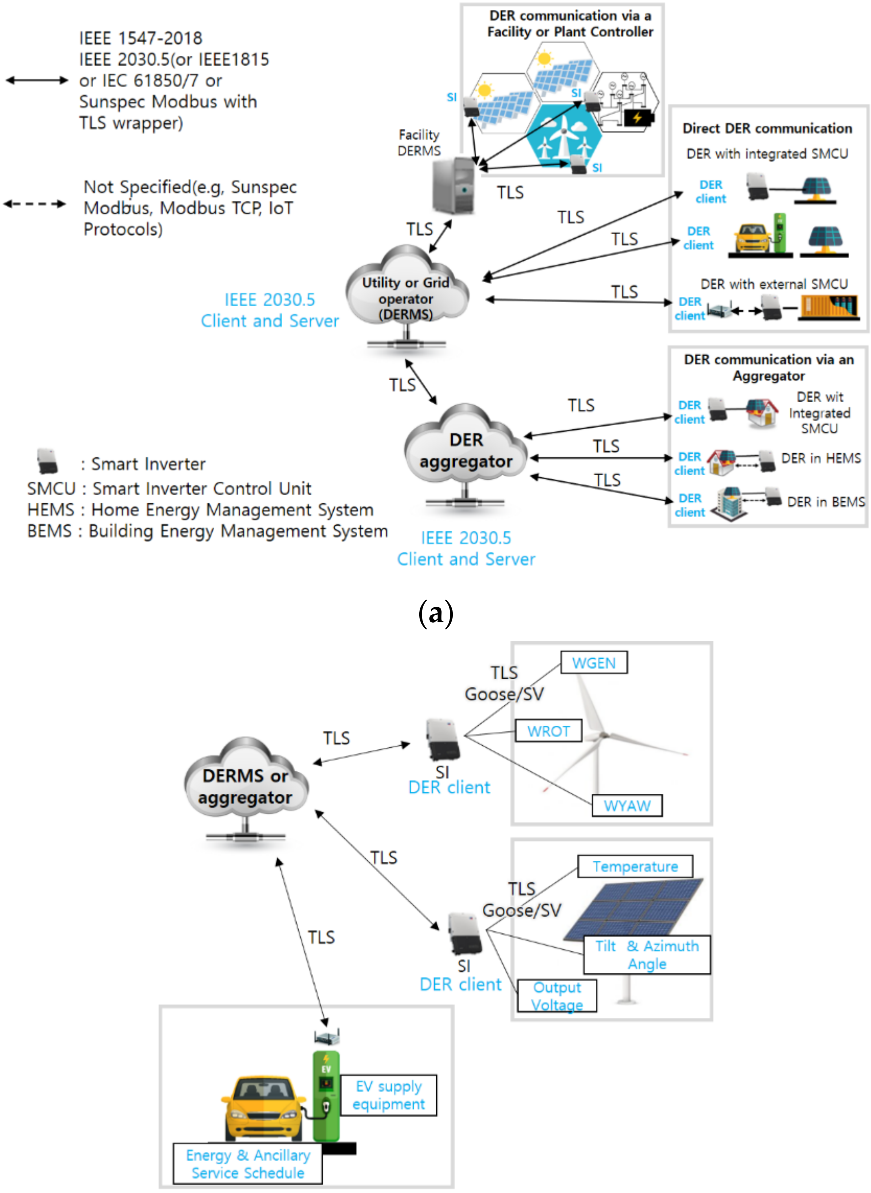
This section estimates when encryption algorithms used in the DER network protocol will become insecure according to the trend of quantum computer development. First, the security protocol and encryption algorithm used in the DER network will be described. Then, with the development of quantum computers, we will predict when the current security protocol will not guarantee safety.

2.1. The Security Protocol of the DER Network

DER networks are huge networks that connect DER devices and control devices (SCADA and DERMS) and power plants for the stable operation of the entire system and DER systems. In addition, the DER network is a combination of a sensor network and an existing data communication network for monitoring the current state of the DER device and to control it appropriately. In order to secure the DER network, many standards have been established according to the type of DER system [10,16–28].

IEEE 1547-2018 mandates DER communication protocols including IEEE 2030.5 (i.e., Smart Energy Profile 2.0 (SEP2)), IEEE 1815 (DNP3), IEC 61850, and SunSpec Modbus. Specifically, California Rule 21 mandates that new DER interconnection with Electric Power

Systems (EPS) in California must be ready to communicate to a host utility using the IEEE 2030.5-2018 standard [16]. Figure 1a shows an example of a DER network structure in compliance with IEEE 2030.5 [10], where DER devices are monitored and controlled by a utility's DER management system (DERMS) or by a DER aggregator (for behind-the-meter (BTM) DER such as home DER and building DER). DERMS and aggregators monitor each part of the DER device in order to keep the DER system stable, which is referred to as a logical node (LN) [42–48]. LNs in wind turbines and solar panels are represented in Figure 1b.



(**a**)

(**b**)

Figure 1. A DER network structure: (**a**) overall network structure; (**b**) specific network structure of DER device monitoring and control.

In Figure 1a, DER devices are monitored and controlled by a utility or by a DER aggregator (for behind-the-meter (BTM) DER such as home DER and building DER). DERMS and a DER aggregator monitor DER devices and sends control commands (e.g., set points/operating points and on/off commands) to these smart inverters by using the SEP2 protocol. Figure 1b shows the specific network structure of DER device monitoring and control network. The sensor value measured at each LN of the DER device is regularly transmitted to the Smart Inverter (SI) and DERMS by using a message in a goose or SV type. DERMS checks the state and output of the DER device based on the received sensor value and controls DER devices.

DER network data are encrypted and authenticated by TLS with SunSpec PKI certificates that are provided by the authorized issuers to fulfill California Rule 21 compliance. Moreover, IEC 61,850 and IEE 1547 protocols utilize TLS-based encrypted traffic (i.e., HTTPS) and X-509 digital certificates for server and client authentications. Although SunSpec Modbus and Modbus TCP implementations do not generally support TLS, incorporating TLS wrapper (e.g., Modbus TLS [17]) enables the use of TLS. Analysis of the current DER network standards shows that the current DER network relies on TLS for security.

TLS is a security protocol that verifies each other (client and server) and encrypts data. By using signature and authentication algorithms, client and server verify one another. Then, the client and server exchange symmetric keys to encrypt data. This process is called a handshake. After the handshake, encrypted data are transmitted. The version of TLS used for each protocol is summarized in Table 1 [10,16–28].

Table 1. TLS version for DER security protocol.

Protocol	Version of TLS
IEC 61850 IEC 60870-5 IEC 61968 IEEE 1815 DNP3-SA	TLS 1.1/TLS 1.2
IEEE 2030.5 (SEP2)	TLS 1.3

The latest version of TLS is 1.3., and it is only introduced in IEEE 2030.5 [16]. TLS 1.3 uses Authenticated Encryption with Associated Data (AEAD), which performs encryption and authentication at the same time. The key exchange, AEAD, and the signature algorithm used in TLS 1.3 are described in Table 2 [43,49].

Table 2. Encryption and signature algorithm of TLS 1.3.

AEAD		Key Exchange	Signature and Certification
Bulk Encryption	**Hashing**		
AES-128 GCM	SHA 256	ECDHE	RSA
AES-128 CCM	SHA 256		ECDSA(X. 509)
AES-256 GCM	SHA 384		EdDSA

If the algorithms in Table 2 become insecure due to quantum attacks, the security of the DER network is not guaranteed either. The next subsection describes future quantum attacks on the DER network.

2.2. Predicting Possible Quantum Attacks

Future quantum attacks on the DER network are analyzed based on current attack methods and strategies. In the future, even if an attacker can break the encryption algorithm of the DER network by using a quantum computer, the purpose of the attack is not much different from present purposes. Thus, by analyzing the strategy of the current attack on the DER network, a quantum attack on the DER system can be predicted more realistically in the future.

The main purpose of attacking the DER network is to shut down the entire power system, obtain confidential information, or gain illegal benefits [43–46]. In order to achieve these goals, attackers set up strategies. Security experts are studying attack models and strategies to prevent the attack and find vulnerabilities of the DER network [6,14,50–52].

The attack model is generally divided into 9–12 steps [6,14,50–52]. However, these steps can be briefly summarized as four steps according to certain goals: 1. collecting information and analyzing vulnerabilities; 2. selecting target, route, and means of attack; 3. attacking; and 4. eliminating traces. This strategy is shown in Figure 2.

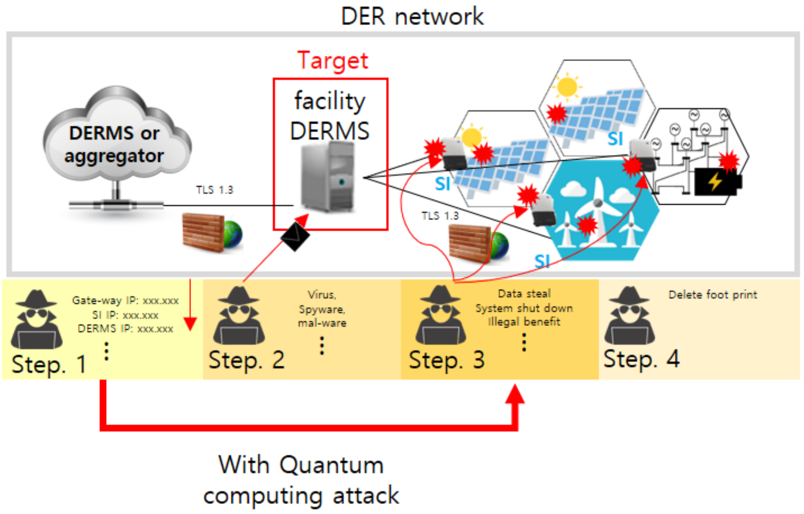


Figure 2. DER network attack model and effect of quantum computing attack.

In Figure 2, if the DER network is protected by TLS 1.3, the attacker uses a method to bypass the firewall. In the first step, port scanning tools such as Nmap or sniffing tools such as wire shark or packet capture can be utilized to collect information. The attacker can understand the network structure of the system by using the collected information and find the attack route by using port numbers or packets containing user IDs and passwords. In the second stage, the attacker sets the target and delivers attack tools such as worm, virus, trojan horse, adware, and spyware to the target system. Delivery methods can be websites, apps (APP), emails, P2P, and also be physical connections such as USBs, external hard drives, and stick PCs [51,52]. If the attacker invades the target system by using a rootkit or desired malware, an attacker can obtain confidential information or administrative authority of the target system.

The defense methods are different for each step from step 1 to step 3. The defense methods for the first and second steps are for preventing invasion in networks and extortion of authentication [51,52]. In the third step, since the attack on DER has already happened, defense methods are focused on the detection and restoration of abnormalities in the system [51,52]. Thus, quantum attacks can be utilized to break the first and second steps. When quantum attack is feasible, the attacker does not have to bypass the TLS 1.3 firewall, and the attacker can succeed in the attack only with the first step because the quantum attack renders TLS 1.3 encryption for the DER network useless. Therefore, this paper considers the attack model, which invades from the outside of the DER network and does not consider the bypass attack model that induces leakage of the encryption key inadvertently.

In order to predict future quantum attacks, assume that the attacker attacks DERMS or DER server in Figure 1a. When the encryption of each part of the TLS 1.3 protocol is broken, it analyzes what types of attack is possible. If the attacker can break only the key-exchanging algorithm, the attacker can obtain the Encryption Key (EK) from DERMS and SI handshake. If an attacker can break AEAD using a quantum attack, the attacker can obtain confidential information only with a communication message between DERMS and SI. In addition, obtaining the communication message is easy. If the DER network uses Wi-Fi, Raspberry Pi, or Modbus, attackers can easily sniff messages exchanged between devices in the DER network using packet capture or wire shark. Thus, when AEAD and key-expending algorithms are broken by quantum attacks, privacy security in the DER network is not guaranteed. Figure 3 shows the future quantum attack process based on a sniffing attack.

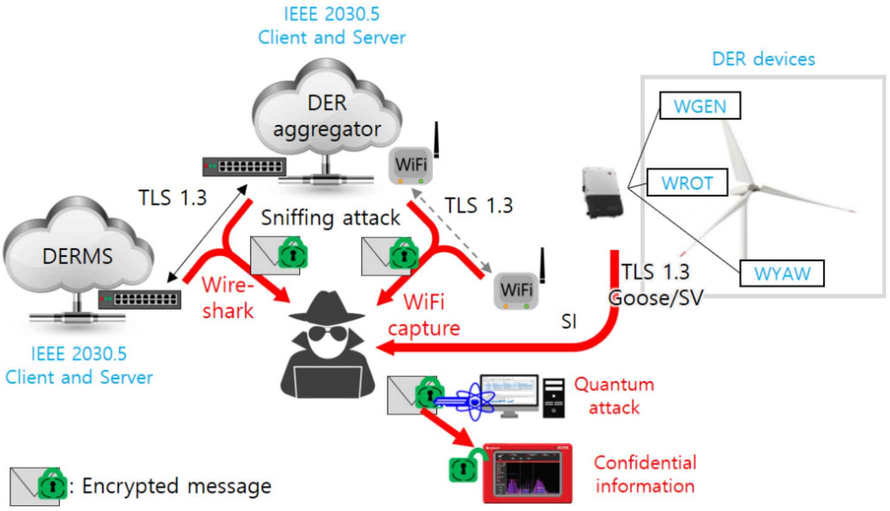


Figure 3. Sniffing attack on the DER network.

Let us assume that quantum computing attacks break not only AEAD and key exchanging algorithms but also signature and certification (X.509). The attackers can perform a Man in The Middle (MiTM) attack by pretending to be SI on the DERMS or pretending to be DERMS on the SI. In this case, an attacker may not only steal confidential information but also shut down the entire power system or gain illegal benefits. For example, the attackers can earn illegal benefits by manipulating the amount of curtailment or unit price. In addition, the attacker can shut down the entire power system by manipulating the output during valley load filling or peak load clipping. Figure 4 shows future MiTM quantum attack processes.

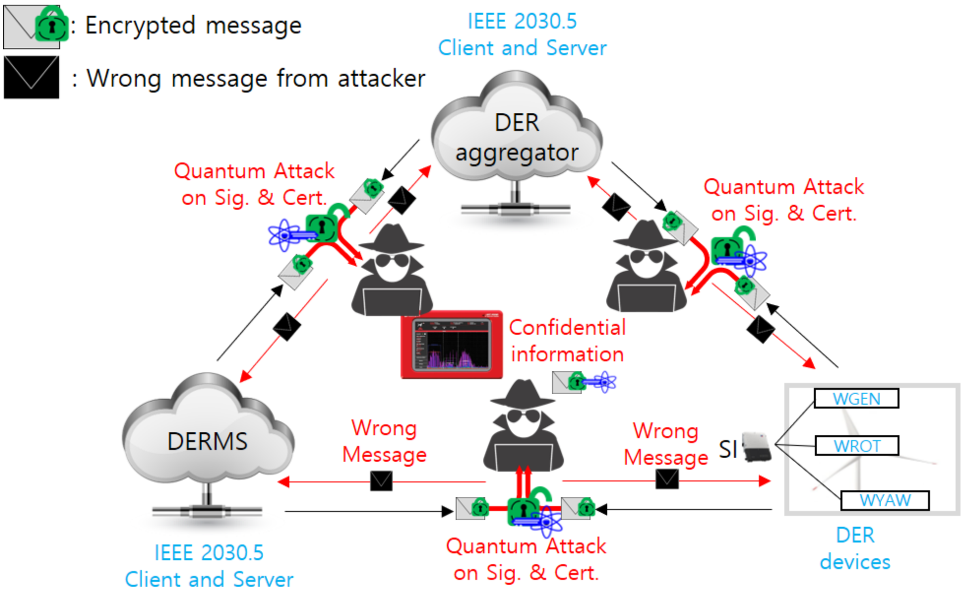


Figure 4. MiMT attack on the DER network.

As shown in Figures 3 and 4, the method and purpose of the attack vary depending on which part of the TLS 1.3 security protocol is broken by a quantum attack. Table 3 shows possible attack methods according to parts of the TLS 1.3 security protocol.

Table 3. Future quantum attack on DER depending on TLS 1.3.

Key Exchange	AEAD	Signature and Certification	Attack Methods
○	×	×	The private key is exposed to an adversary. Compromise a user's private key.
×	○	×	All data (data in transit and data at rest) are decrypted.
○	○	×	Session keys are exposed to an adversary. All data are decrypted.
○	○	○	Private keys are exposed to enemies. Certificate modification. Pretend to be an authenticated user.

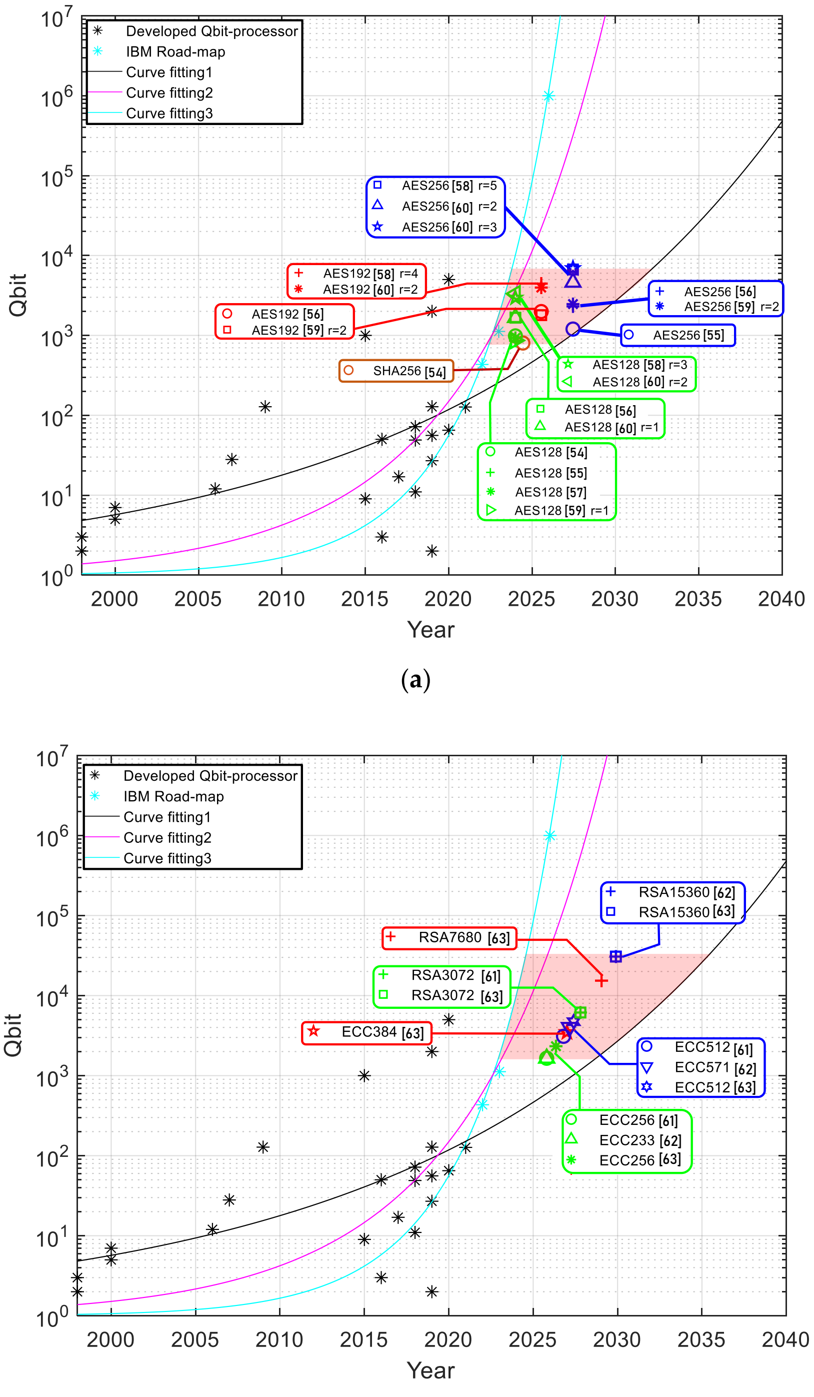
In the next subsection, we predict when quantum attacks will become possible based on the current status of quantum computer development.

2.3. Predicting When Quantum Attacks Become a Reality

Quantum computers calculate using the principle of quantum entanglement or superposition. The unit of information processed by quantum computers is called Q-bit, which is the same concept as a bit in existing computers. Q-bit can represent 0 and 1 at the same time while the bit represents 0 and 1, respectively. Conventional computers can calculate n bit at once while a quantum computer can calculate 2^n bit. Thus, quantum computers have faster computational speeds than a conventional computer, and problems that take trillions of years on conventional computers can be calculated in seconds on quantum computers [53–63]. However, the fast computational speed of quantum computers is a major threat to cryptographic algorithms.

Existing cryptographic algorithms use mathematical or computational complexity to obtain security. However, if a quantum computer has a large number of Q-bits for easily solving the encryption algorithm in Table 2, the security of the DER network is not guaranteed. It is necessary to predict the development trend of quantum computers in order to know when quantum attacks become possible. There was a previous study predicting quantum computer development trends in 2009 [64]. However, in 2009, quantum computer research was in its infancy, and actual quantum computer developments were rare; thus, the current development situation and predicted results in [64] are very different. After that, the trend of quantum computer development was predicted based on Moore's law, and most of the results predict that processors with a Qbit of 10^5 will be developed by 2030 [65–67]. IBM's roadmap aims to develop a mega-Qbit (10^6) processor after 2026 [68]. This paper predicted development trends based on currently developed quantum processor specifications [69] and the IBM quantum computer development roadmap [68]. We also predicted when the algorithm in Table 2 was broken based on the quantum processor development trend. The results are represented in Figure 5.

In Figure 5, the black asterisk represents the number of Q-bits of the already developed quantum processor, and cyan colored asterisks represent the roadmap presented by IBM. In this paper, the current development status and IBM roadmap results were curve-fitted with 95% reliability to predict the quantum processor development trend. When performing curve fitting, the exponential function is utilized as a base model in accordance with Moore's law. As a result, three curve fitting results (black, cyan, and magenta line) were obtained. The black line in Figure 5 is the result of curve fitting using the currently developed quantum processor (black asterisk). The magenta line is the result of curve fitting using the current developed quantum processor (black asterisk) and IBM roadmap (cyan asterisk). The cyan line is the result of curve fitting only with IBM's development results and roadmap. The prediction results show that the mega Qbit processor will be developed as early as 2026 and 2040 at the latest.



(**a**)

(**b**)

Figure 5. Quantum road map and expected quantum attack timing: (**a**) symmetric-k algorithm (AEAD); (**b**) key exchange and signature and certification.

In Figure 5, the marker color represents the security level of the encryption algorithm. Red, green, and blue represents one, three, and five, respectively. Figure 5a,b show symmetric encryption algorithms and key exchange and signature and certification, which are utilized in TLS 1.3, respectively. In Figure 5b, ECDSA, EdDSA, and ECDHE are represented by Elliptic Curves Cryptography (ECC) because they are made based on the same mathematical principle of elliptic curves.

Recent cryptoanalysis studies show that decrypting cryptographic algorithms currently used in DER networks requires processors with thousands of Q-bits [54–63]. Considering this trend of development, the threat of quantum attacks is expected to be realized in a few years. In Figure 5a, the symmetric key algorithm will not guarantee security after 2032. In Figure 5b, all algorithms used for key exchange and signature and certification will be insecure after 2036.

In Figure 5a, the probability of attack success on AES varies depending on the number of plaintext-ciphertext pairs, and it should be considered to prevent quantum attacks on the DER network. In Figure 5, r represents the minimum number of plaintext-ciphertext pairs required for the 100% success of the attack. If the AES key is used less than r-times, an attacker cannot succeed in a quantum attack. However, to operate the DER system stably, monitoring and control messages must be exchanged at very short time intervals. Therefore, it is necessary to analyze whether key distribution delay is less than the minimum delay required by the DER network.

As a result of the analysis, future quantum attacks will be realized after only a few years. In addition, as a result of the quantum attack model on the DER network, the vulnerabilities of the DER network are founded in the first and second steps. In order to increase the security of the DER network, in the first stage, security protocols must prevent the attacker from obtaining or eavesdropping on physical signals. In the second stage, encryption techniques that cannot be broken by quantum attacks are required. Novel protection technologies that meet this purpose include Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD).

PQC is a future encryption technique that is not broken by quantum attacks, and QKD is a physical layer communication technique that uses quantum communication to determine whether physical signals are eavesdropped on or not. Therefore, in order to prepare for future quantum attacks, these two techniques need to be applied to the DER network.

3. Post-Quantum Era Technologies

In this section, PQC and QKD are briefly described, and the feasibility of the DER network of these two technologies is analyzed in terms of network performance and implementation cost.

3.1. Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) is a novel encryption algorithm that can guarantee safety against quantum computer attacks. The National Institute of Standards and Technology (NIST) has been conducting quantum-resistant cryptography contests since 2016 to develop PQC. By implementing this contest, NIST aims to complete a standard for quantum-resistant cryptography by 2022, and the target algorithms include the signature Key Exchange Mechanism (KEM). Note that the symmetric encryption algorithm is not included as a target. In July 2020, NIST selected 15 algorithms as a candidate for three rounds. Among 15 algorithms, seven algorithms were selected as final candidates. The remaining eight are alternative candidates, and these algorithms are preliminary algorithms in case defects are found in the final candidate algorithm. Currently developed quantum-resistant cryptography is divided into five types (Lattice, Code, Hash, Isogeny, and Multivariate). Table 4 shows the advantages and disadvantages of algorithms [70].

As shown in Table 4, the problems with applying PQC to the DER network are larger signatures, key sizes, and slower computational speeds compared to current encryption algorithms. For example, the Rainbow algorithm has a 1200-times larger public key size than ECDHE of TLS 1.3 [39,40,71,72].

The larger the size of the key and signature, the more data there are to be transmitted and received between SI and DERMS. In addition, the processing speed is slowed down due to the increased size of the key and signature. This delay increases handshake time, and it can be a big problem considering future quantum attack characteristics in Section 2. Previously, in Section 2, the probability of quantum attack success depends on the number of plaintext–ciphertext pairs (r). Therefore, the number of usages of the encryption key must be less than r, and the key must be destroyed after being utilized r times. Then, all devices must receive a new key. Since continuous monitoring is required to operate the DER grid stably, it is difficult to apply PQC to the DER network when the time for the key distribution is greater than the time required for stable operation of the DER grid. Therefore, when PQC is applied to the DER network, the time required for key distribution should be analyzed.

Table 4. PQC algorithms in NIST round 3.

Type	Advantage	Disadvantage	Algorithm	
Lattice	Fast operation speed	Difficult setting parameter	Sig.	CRYSTALS-DILITHIUM, FALCON
			KEM	CRYSTALS-KYBER, NTRU, NTRU prime, SABER, FRODO
Code	Small signature size Fast operation speed	Large key size	Sig.	—
			KEM	Classic McEliece, BIKE, HQC
Multivariate	Fast encryption and decryption speed	Large key size	Sig.	Rainbow
			KEM	—
Isogeny	Small key size	Slow operation speed	Sig.	—
			KEM	SIKE
Hash	Safety proof possible	Large signature size	Sig.	SPHINCS+, PICNIC
			KEM	

In this paper, in order to analyze which PQC algorithm can be applied to the DER network, the key distribution delay according to the number of devices in the DER network is analyzed. In order to analyze the key distribution delay, assume a DER network, as shown in Figure 6. Each DER device is connected to an SI, and it is connected to DERMS. It is assumed that SIs are divided into sectors, and SIs existing in the same sector are connected by a network hub. The network assumed wired ethernet, which follows the 802.3z protocol.

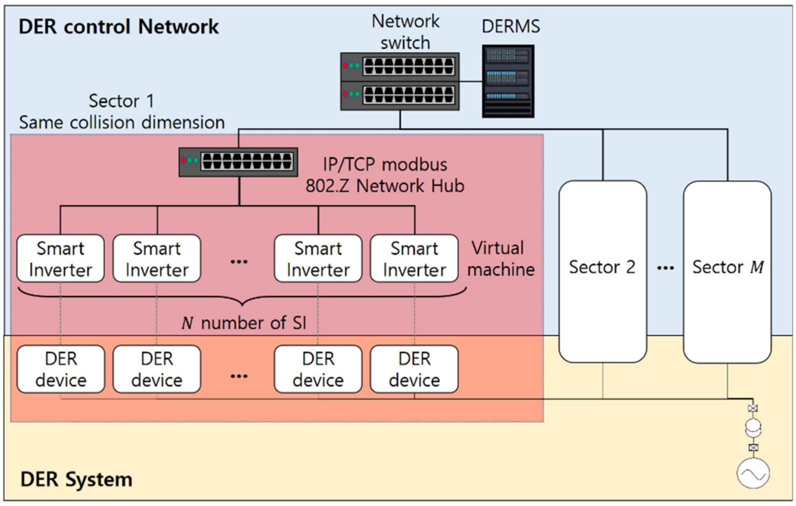


Figure 6. The structure of the DER network.

The actual DER grid senses several LNs, but in this paper, it is assumed that the DER network monitors only the Voltage Regulating part for simplicity of the experiment. Referring to the DER grid using the IEEE 2030.5 protocol, the Voltage Regulating Device (VRD) reporting cycle is 2 s~5 s [73,74].

SI and DERMS were implemented using a virtual machine. The virtual machine was made into an Ubuntu (64-bit) operating system with 2Gram on a computer equipped with AMD Ryzen 53500U. The PQC applied TLS1.3-based DER network is implemented with OQS-OpenSSL. X.509 was utilized as certification. The cipher suite was configured with PQC KEM and the Signature with the same security level. AES 128, 192, and 256 are adopted as the symmetric algorithm according to the security level. In this network, according to the cipher suit and the number of devices, the time required to distribute keys is measured, and the results are shown in Figure 7.

In Figure 7, the results show that the key distribution delay is more affected by the Signature algorithm than the KEM algorithm. In Figure 5, the minimum r for AES 128 is 1, and for AES 192 and 256, the minimum r is 2. If the security level is one, the key can only be used once, and if the security level is three or five, the key can only be used twice. Therefore, keys must be distributed every 2 to 5 s when the security level is one, and the key distribution period is 4~10 s when the security level is three or five. Figure 7a,b show that the key distribution delay is all less than 2 s; thus, QKD with a security level of one and three is expected to be applicable to the current DER network. In the case of using Rainbow-5 in Figure 7c, a key distribution delay is 9 s when the number of SI is 50. If Rainbow 5 (Blue group in Figure 7c) is to be written as the signature algorithm, the number of SI must be set to less than 50. Therefore, in order to apply PQC to the DER network, it is necessary to determine an appropriate security level according to the importance of information to be transmitted and select an appropriate PQC algorithm according to the size of the DER grid.

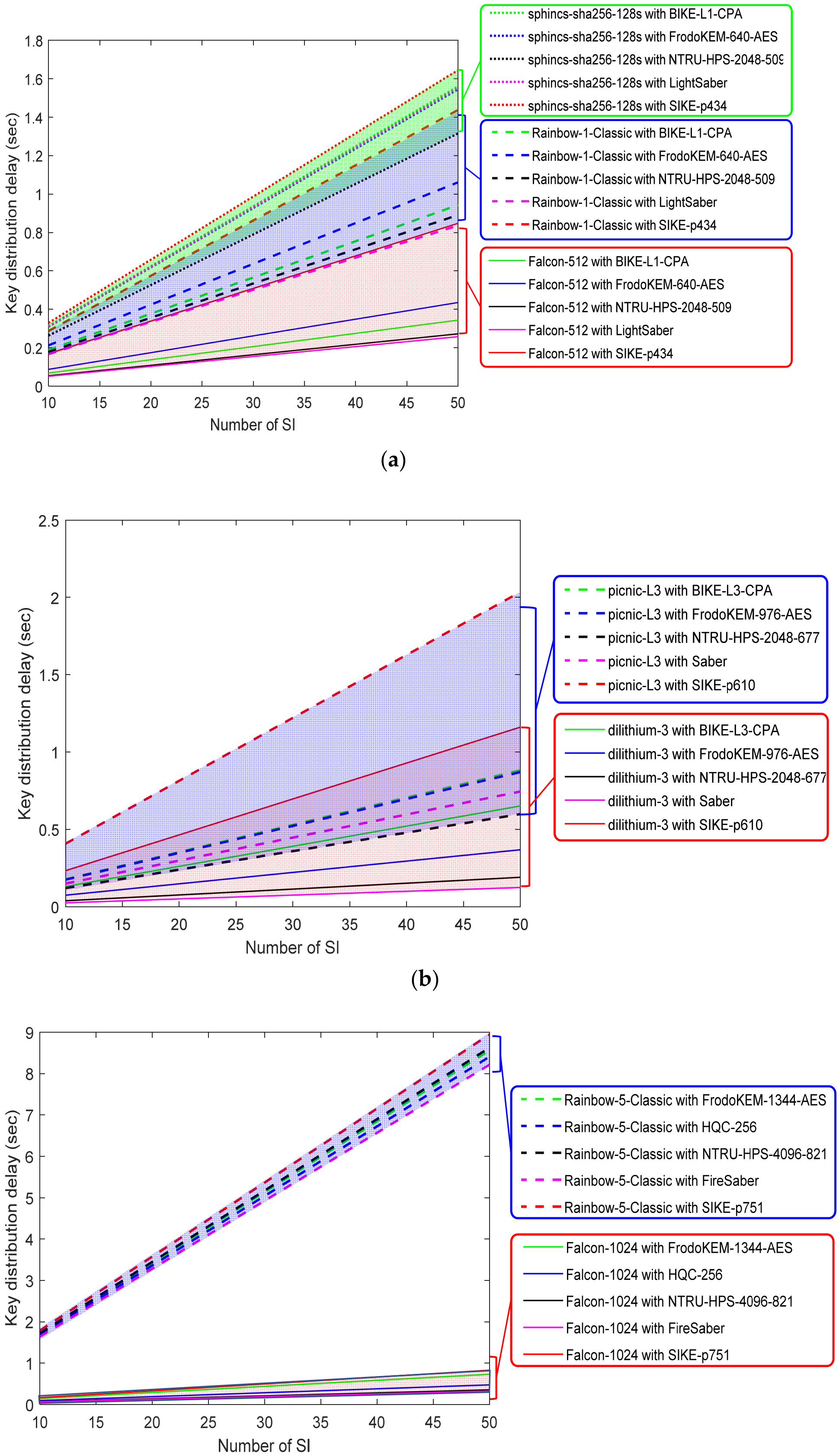
In this paper, only a VRD cycle is considered as an example. However, the practical DER system requires several millisecond delays to react when controlling critical factors such as Load Frequency Control (LFC) [10,25–28]. In this case, the algorithm that satisfies this condition is only based on the lattice of security level one. Therefore, it is necessary to make a PQC lighter to apply to the DER system. Figure 7 shows that the key distribution delay of Lattice-based algorithms, such as Falcon, Saber, NTRU, and Frodo, showed less and better performance than other algorithms. As the grouped results in Figure 7 show, the signature algorithm plays a more important role than the KEM algorithm on network performance of key distribution delay.

Therefore, it is feasible to apply a lattice-based algorithm to the current DER network. However, if a new quantum computing algorithm is developed that can speed up the calculation of lattice, the security of lattice-based algorithms is threatened; thus, research should be conducted for application to other types of PQC.

Although PQC can prevent quantum attacks, attackers can steal keys by inducing negligence in key management. Moreover, as mentioned in Section 2, it is safer to prevent signal sniffing in advance when quantum attacks become possible in the future. Therefore, in the next section, QKD technology that can increase the security of the physical layer communication is explained.

3.2. Quantum Key Distribution and Application

QKD is a protocol for distributing encryption keys through the quantum channel (Q-channel). If encryption keys are completely secret and random, the quantum attack cannot conduct cryptanalysis on the ciphertext, and it is theoretically proven [75]. The Q-channel can determine whether the transmitted signal has been eavesdropped or not by utilizing quantum physics laws [76]. Since Wi-Fi, Raspberry Pi, or Modbus cannot know whether there is eavesdropping occuring, network information such as IP is leaked when an attacker attempts to eavesdrop on the network packet using sniffing devices such as wire-shark or packet capture. Since the QKD network can know the presence of eavesdropping, the attacker cannot obtain any network information. When the attacker attempts to eavesdrop, the network stops data transmission to prevent information leakage. Thus, unlike conventional networks (Wi-Fi, Raspberry Pi, or Modbus), applying QKD to the DER network can prevent attackers from stealing r number of messages required to break AEAD. QKD can be categorized into two methods depending on the encoding method of the Q-bit: Prepare and Measurement (PM) [77] and Quantum Entangle base (EB) method [78].



(**a**)

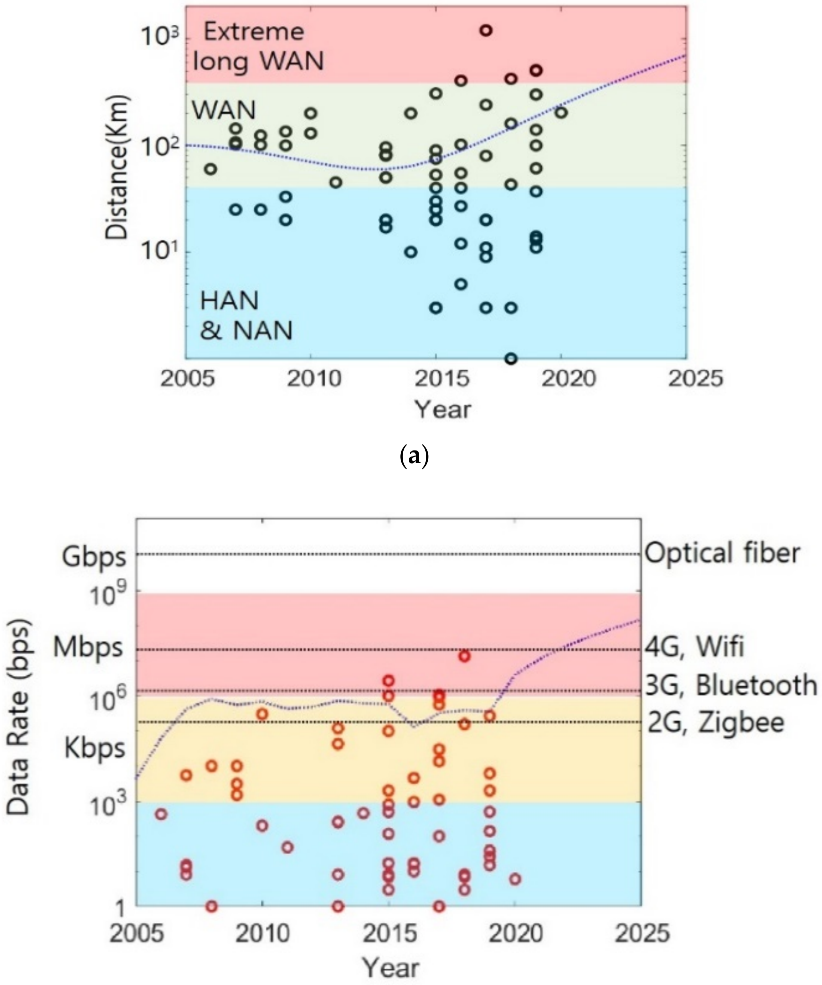
(**b**)

(**c**)

Figure 7. Key distribution delay of PQC-DER network according to security level: (**a**) 1; (**b**) 3; (**c**) 5.

PM can be implemented by using an optical fiber network and has a higher secret key rate (SKR) than EB when the distance is short. Thus, the PM-based method is usually applied to the DER network [79,80]. However, QKD has a shorter communication distance, lower transmitting speed, and much higher cost than the current public network [81–86]. In addition, QKD only protects physical networks, does not encrypt data, and uses public networks. Thus, the latest encryption technologies, i.e., PQC must be applied simultaneously to the DER network [4].

In this paper, in order to analyze the applicability of QKD's DER network, the communication performance of QKD in the future was predicted based on the data in [81–86]. The prediction results are shown in Figure 8.



(**a**)

(**b**)

Figure 8. The performance of QKD: (**a**) communication distance; (**b**) data rate.

Figure 8a shows the distance by year, and (b) shows the data rate. Looking at Figure 8a, it can be observed that existing QKD networks have been able to communicate over 300 km and have an Mbps data rate since 2015. Although it does not meet the speed of LTE, 4G, and Wi-Fi, which are widely used today, QKD shows sufficient speed because it is used only for key distribution. Moreover, it is predicted that it will show a similar speed to the current general communication equipment within 2025. In Section 2, quantum attacks will become possible after 2025, and QKD can be applied at the proper time. Therefore, when applying QKD to the DER network, the consideration is the cost and the applicability of PQC.

In order to reduce the number of quantum transceivers in a cost-effective QKD network, not all DER or SI devices are connected to the quantum channel [81–86]. Figure 9 shows the cost-efficiency QKD network structure.

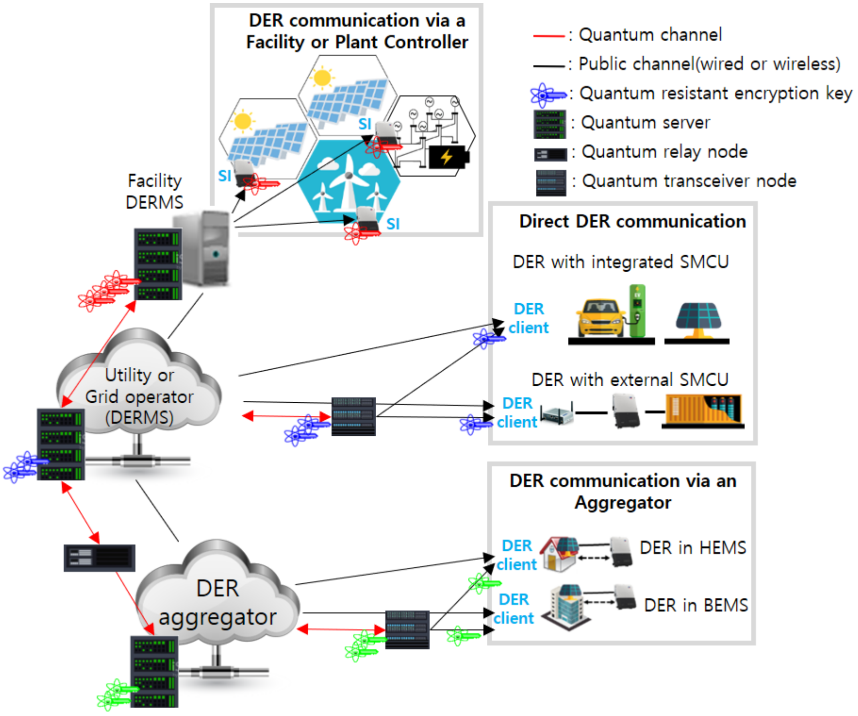


Figure 9. The cost-efficiency QKD network for DER.

In Figure 9, only a DERMS/DER aggregator and quantum transceiver node are connected to each other by using quantum channels. SIs are connected to DERMS by using a public channel such as a conventional network, but DERMS distributes quantum-resistant encryption keys for DER/SI through a public channel. The structure of Figure 9 is cost-effective because not all SIs and DER devices are equipped with quantum transceivers. SKT, South Korea's wireless communication service provider, commercialized QKD with this network structure [84,85]. As the number of DER/SI connected to one quantum node (i.e., quantum server and quantum transceiver node) increases, the cost of installing QKD decreases. The network structure of Figure 9 reduces security because DER and SI are not guaranteed security by quantum channels. Therefore, when using such a QKD network structure, it is essential to apply PQC. The SKT increased security by applying AES-256 encryption to the QKD network. In a cost-efficiency QKD network, as the number of DER/SI connected to one quantum node increases, the number of keys to be distributed by one quantum server also increases. In other words, the security and communication performance of the network and the installation cost have a tradeoff relationship.

In this paper, in order to analyze DER applicability of QKD, key distribution delay and QKD network installation costs were analyzed according to the size of the QKD network. The QKD installation cost is shown in the following equation [86].

$$\text{Cost} = C_Q \times N_Q + C_S \times N_S + C_R \times N_R + C_W \times D_s \tag{1}$$

In Equation (1), N_Q, N_S, and N_R represent the number of quantum devices required to configure the QKD network. D_L is the total length of fibers of the QKD network. Other variables are shown in Table 5 below. The price of quantum equipment is referenced in the paper [86,87].

Table 5. The cost of a quantum device [86,87].

C_Q: Cost of Quantum transceiver	40,000 USD
C_S: Cost of Quantum Server	50,000 USD
C_R: Cost of Quantum relay node	5000 USD
C_W: Cost of fiber per kilometer	8 USD

According to the latest quantum network study, one quantum server can be connected to a maximum of four quantum transceiver nodes through a quantum channel with a data rate as 2 Kbps [88,89]. Based on Equation (1) and the result of the latest quantum server research, we can calculate the cost of the QKD network for DER in Figure 9. Let us assume N_{QN-SI} is the number of SIs connected to one quantum transceiver. Then, N_Q can be represented as $\left\lceil \frac{100}{N_{Q-SI}} \right\rceil$. As described above, since one quantum server can be connected to up to four quantum transceiver nodes, N_S can be rewritten as $\lceil N_Q/4 \rceil$. It is assumed that one quantum relay node is added whenever two quantum servers are added, and N_R can be rewritten as $[N_R/2]$. Thus, the cost required to install QKD varies depending on how many SIs are connected to one quantum transceiver node. For example, the total number of SI (N_{SI}: 100) is 100, and five SIs are connected to one quantum transceiver node (N_{QN-SI} : 5). Twenty quantum transceiver nodes (N_Q : 20), five quantum servers (N_S: 5), and three quantum relay nodes (N_R: 3) are required to implement the QKD network. Therefore, the cost of installing QKD in Equation (1) may be expressed as shown in Equation (2).

$$\text{Cost} = C_Q \times \left\lceil \frac{N_{SI}}{N_{Q-SI}} \right\rceil + C_B \times \left\lceil \frac{N_{SI}}{N_{Q-SI}/4} \right\rceil + C_T \times \left\lceil \frac{N_{SI}}{N_{Q-SI}/8} \right\rceil + C_W \times D_s \quad (2)$$

The QKD network is assumed, as shown in Figure 10. In Figure 10, the network between the quantum transceiver and SIs is the same as the DER network to which the PQC of Section 3 is applied. The total number of SI (N_{SI}) constituting the network is 100.

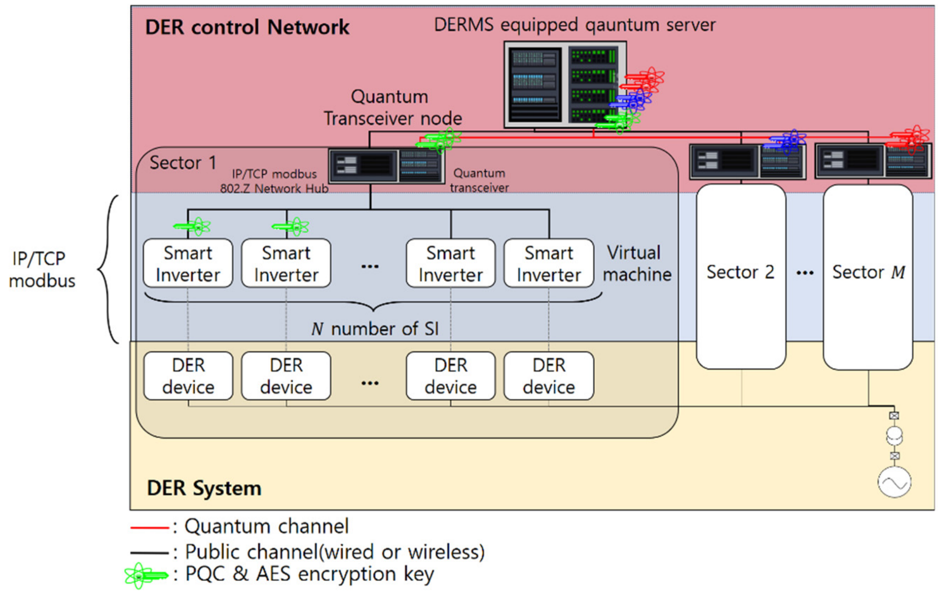


Figure 10. Cost-efficiency QKD network for simulation.

The optical fiber length required for network configuration was fixed at 100 km. At this time, the cost of installing key distribution delay and QKD according to the number of SI accepted by the quantum transceiver node was analyzed and shown in Figure 11.

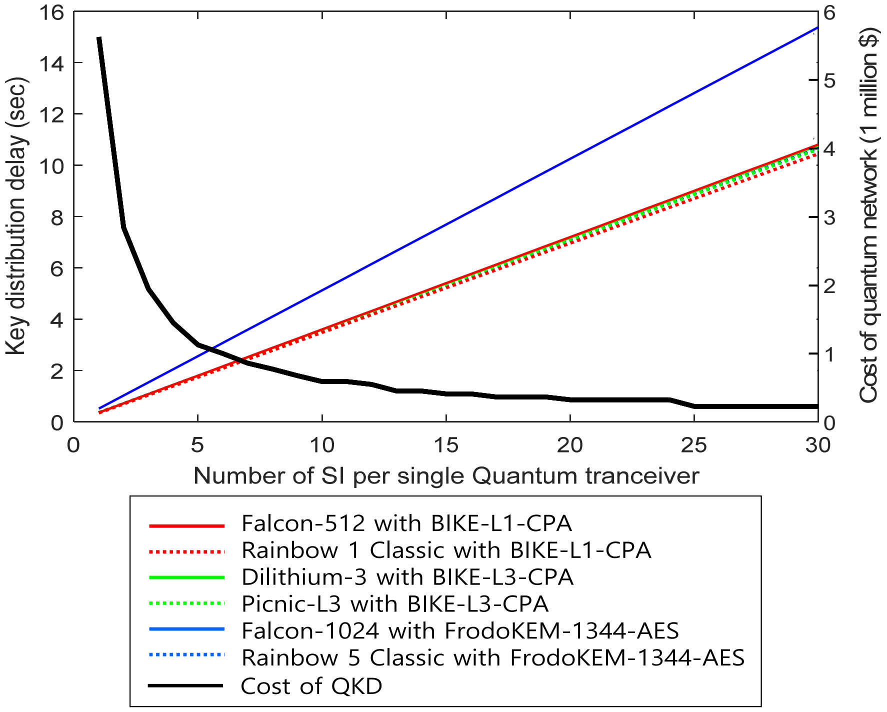


Figure 11. Cost of QKD network and key distribution delay.

According to analysis results in Figure 11, as the number of SI connected to single quantum transceiver node increases, key distribution delay increases linearly, while cost decreases nonlinearly. In particular, when the number of SI connected to a single quantum transceiver node is between three and five, cost decreases dramatically. If the number of SI is seven or higher, the cost does not decrease significantly, even if the number of SI increases.

In Figure 11, the implementation cost is 5.5 million dollars to connect quantum channels to all SIs, and DER can be stably operated because key distribution delay is less than 1 s. If five SIs are connected to the quantum transceiver node, the key distribution delay is 1.5 s to 3.5 s, which can still reliably operate the DER. In addition, cost will be reduced to less than about a million dollars. If 15 to 20 SIs are connected to the quantum transceiver node, the price decreases to 0.2 to 0.3 million dollars, but DER is unable to operate stably because the key distribution delay is greater than 10 s. Therefore, in order to apply QKD to the DER network, optimal cost and network configuration should be researched in terms of the actual cost and key distribution delay.

Comparing the results in Figure 11 with those in Figure 5, the key distribution delay be smaller when QKD and PQC are simultaneously applied to the DER network because the data rate of the QKD network is slower than the conventional network. Therefore, as predicted in Figure 8, the improvement of the data rate of the QKD network is expected to be more advantageous in applying QKD to the DER system.

4. Conclusions and Future Works

Quantum technology will induce greater threats and provides opportunities for more secure encryption in the DER network. New attacks will be created by using a quantum computer that easily breaks current encryption algorithms. Therefore, security researchers need to pay attention to quantum computing trends. This paper analyzes possible quantum attacks in the future and predicts feasible timing. The results show that quantum attacks will be feasible in only three to five years.

In order to protect the DER network from future quantum attacks, this paper investigated the case of simultaneously applying PQC and QKD to the DER network. In addition, we analyzed problems that occur when these two technologies are applied simultaneously in terms of network performance and installation cost.

Future research includes cost-effective and high-performance quantum-safe network DER networks using server-based QKD and lightweight PQC. The network delay of TLS 1.3 currently used in the DER network is measured in several milliseconds [14]. In the case of control critical factors such as load frequency, the DER system requires an immediate response of several milliseconds or less [90]. Therefore, research will be needed to change PQC to being lightweight in order to enable key distribution within milliseconds. In the future, setting appropriate security levels depending on the importance of each part of the DER system also will be researched.

Currently, the QKD network is expensive. In addition, the DER system is usually established in a large area. Thus, there may be an isolated DER system that is hard to apply QKD. Thus, QKD should be priorly applied to important parts of the DER system, and a cost-effective QKD network structure will be researched. If QKD has a cost-effective network structure, as shown in Figure 9, the DER network inevitably uses a public network. In this case, it is necessary to study methods for securing the public network.

Similarly to conventional attack models, DoS or bypassing attack models inadvertently render leakage of the encryption key. Thus, a more in-depth study about future quantum attack models is needed, and a study to score risks according to the quantum attack for each part of the DER system is needed.

Author Contributions: Forma analysis, Methodology and Visualization, J.A.; Data curation, J.A., H.-Y.K., B.A., K.P., T.K. and J.K.; Software, J.A. and H.-Y.K.; Validation, H.-Y.K., B.A., K.P., T.K., J.K. and J.C.; Supervision, T.K. and J.C.; Project administration, M.-K.L. and J.C.; Funding acquisition, Investigation and Resources, M.-K.L.; Writing-original draft, review and editing, J.A. All authors have read and agreed to the published version of the manuscript.

Funding: MSIT: Korea, Institute for Information & communication Technology Planning & evaluation (IITP) grant number: 2020-0-01540) and MSIT, Korea, National Research Foundation of Korea (NRF), No. 2020R1A2C2013089.

Data Availability Statement: Not applicable.

Acknowledgments: This research was supported in part by the MSIT, Korea, under the High-Potential Individuals Global Training Program (grant number: 2020-0-01540) supervised by the IITP. This research was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1A2C2013089).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Feldman, D.; Margolis, R. *Q1/Q2 2020 Solar Industry Update*; Technical Reports; National Renewable Energy Lab: Golden, CO, USA, 2020.
2. Michelle, D.; Clin, S.; Bryam, W.; Rachel, G.; Xiaojing, S.; Molly, C.; Gregson, C.; Ravi, M.; Shawn, R.; Colin, S.; et al. *U.S Solar Market Insight*; Technical Reports; Wood Mackenzie and Solar Energy Industries Association (SEIA): Washington, DC, USA, 2021.
3. Cook, J.J.; Ardani, K.B.; O'Shaughnessy, E.J.; Margolis, R.M.; Smith, B. *Expanding PV Value: Lessons Learned from Utility-Led Distributed Energy Resource Aggregation in the United States*; Technical Reports; National Renewable Energy Lab: Golden, CO, USA, 2018.
4. Ahn, J.M.; Chung, J.H.; Kim, T.S.; Ahn, B.H.; Choi, J.C. An overview of quantum security for distributed energy resources. In Proceedings of the 12th IEEE Symposium on Power Electronics for Distributed Generation Systems, Chicago, IL, USA, 28 June–1 July 2021.
5. Alhelou, H.; Paul, C. A Dynamic State Estimator Based Tolerance Control Method against Cyberattack and Erroneous Measured Data for Power Systems. *J. Trans. Ind. Inform.* **2021**. Early access.
6. Ahn, B.H.; Kim, T.S.; Choi, J.C.; Park, S.W.; Park, K.C.; Won, D.J. A Cyber Kill Chain Model for Distributed Energy Resources (DER) Aggregation Systems. In Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–18 February 2021.
7. Chavez, A.R.; Lai, C.; Jacobs, N.; Hossain-McKenzie, S.; Jones, C.B.; Johnson, J.; Summers, A. Hybrid intrusion detection system design for distributed energy resource systems. In Proceedings of the IEEE Cyber PELS Workshop, Knoxville, TN, USA, 29 April–1 May 2019.

8. Kong, P.Y. Routing in communication networks with interdependent power grid. *J. IEEE/ACM Trans. Netw.* **2020**, *28*, 1899–1911. [CrossRef]
9. Qi, J.; Hahn, A.; Lu, X.; Wang, J.; Liu, C.-C. Cybersecurity for distributed energy resource and smart inverters. *J. IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 28–39. [CrossRef]
10. Obert, J.; Cordeiro, P.; Johnson, J.; Lum, G.; Tansy, T.; Pala, M.; Ih, R. *Recommendations for Trust and Encryption in DER Interoperability Standards*; Technical Reports; Sandia National Laboratories: Albuquerque, NM, USA; Livermore, CA, USA, 2019.
11. Lai, C.; Jacobs, N.; Shamina, H.M.; Carter, C.; Cordeiro, P.; Onunkwo, I.; Johnson, J. *Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators*; Technical Reports; Sadia National Laboratories: Albuquerque, NM, USA, 2017.
12. Hamedani, K.; Liu, L.; Atat, R.; Wu, J.; Yi, Y. Reservoir computing meets smart grids: Attack detection using delayed feedback networks. *J. IEEE Trans. Ind. Inform.* **2018**, *14*, 734–743. [CrossRef]
13. Nghia, L.T.; Chin, W.; Chen, H. Standardization and Security for Smart Grid Communications Based on Cognitive Radio Technologies—A Comprehensive Survey. *J. IEEE Commun. Surv. Tutor.* **2017**, *19*, 423–445. [CrossRef]
14. Johnson, J.; Onunkwo, I.; Cordeiro, P.; Wright, B.J.; Jacobs, N.; Lai, C. Assessing DER network cybersecurity defences in a power communication co-simulation environment. *J. IET Cyber Phys. Syst.* **2020**, *5*, 274–282. [CrossRef]
15. Hossain, M.M.; Peng, C. Cyber physical security for on-going smart grid initiatives: A survey. *J. IET* **2020**, *5*, 233–244. [CrossRef]
16. Rule 21 Interconnection. Available online: https://www.cpuc.ca.gov/Rule21/ (accessed on 8 December 2021).
17. Modbus Organization. *Modbus/TCP Security Protocol Specification*; Technical Reports; Modbus Organization: Hopkinton, MA, USA, 2018; Available online: https://modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf (accessed on 30 October 2021).
18. Communication Networks and Systems for Power Utility Automation-Part 7-420: Basic Communication Structure–Distributed Energy Resources Logical Nodes. Available online: https://webstore.iec.ch/preview/info_iec61850-7-420%7Bed1.0%7Den.pdf (accessed on 30 November 2021).
19. Communication Networks and Systems for Power Utility Automation-Part 8-2: Specific Communication Service Mapping (SCSM)—Mapping to Extensible Messaging Presence Protocol (XMPP). Available online: https://webstore.iec.ch/publication/34345 (accessed on 30 November 2021).
20. Communication Networks and Systems for Power Utility Automation-Part 90-7: Object Models for Power Converters in Distributed Energy Resources (DER) Systems. Available online: https://webstore.iec.ch/publication/6027 (accessed on 30 November 2021).
21. Communication Networks and Systems for Power Utility Automation-Part 90-12: Wide Area Network Engineering Guideline. Available online: https://webstore.iec.ch/publication/63706 (accessed on 30 November 2021).
22. Telecontrol Equipment and Systems-Part 5-104: Transmission Protocols-Network Access for IEC 60870-5-101 Using Standard-transport Profiles. Available online: https://webstore.iec.ch/publication/25035 (accessed on 30 November 2021).
23. Application Integration at Electric Utilities-System Interfaces for Distribution Management-IEC 61968-3-Part 3: Interfaces for Network Operations. Available online: https://cimug.ucaiug.org/WG14/61968-3/57-61968-3-Ed2-IS-FDIS-11-02-2016.docx (accessed on 30 November 2021).
24. Munir, M.; Francesco, P.P.; Duminda, W. DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework. In *Advances in Computer, Information, and System Sciences, and Engineering*; Springer: New York, NY, USA, 2007; pp. 227–234. ISBN 978-1-4020-5261-3.
25. IEEE1815-2012-IEEE Standard for Electric Power Systems Communication-Distributed Network Protocol (DNP3). Available online: https://ieeexplore.ieee.org/document/6327578 (accessed on 30 November 2021).
26. Saleem, D.; Carter, C. *Certification Procedures for Data and Communications Security of Distributed Energy Resources*; Technical Reports; National Renewable Energy Laboratory: Golden, CO, USA, 2019.
27. Hussain, S.M.S.; Ustun, T.S.; Kalam, A. A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. *J. IEEE Trans. Ind. Inform.* **2020**, *16*, 5643–5654. [CrossRef]
28. IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads. Available online: https://www.researchgate.net/file.PostFileLoader.html?id=56d9bfe9217e206a1677bbff&assetKey=AS%3A335962107334669%401457111016976 (accessed on 30 November 2021).
29. Mailoux, L.O.; Lewis, C.D.; Rings, C.; Grimaila, M.R. Post-quantum cryptography: What advancements in quantum computing mean for IT professinals. *J. IEEE IT Prof.* **2016**, *18*, 42–47. [CrossRef]
30. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994.
31. Boneh, D.; Lipton, R. Quantum cryptanalysis of hidden linear functions. In Proceedings of the Crypto' 95, Santa Barbara, CA, USA, 27–31 August 1995.
32. Mosca, M. Cybersecurity in an Era with quantum computers: Will we be ready? *J. IEEE Secur. Priv.* **2018**, *16*, 38–41. [CrossRef]
33. Kong, P.Y. A review of quantum key distribution protocols in the perspective of smart gird communication security. *J. IEEE Syst.* **2020**, 1–14, Early access. [CrossRef]
34. Kaur, M.; Kalra, S. Security in IoT-based smart grid through quantum key distribution. *J. Avd. Intell. Syst. Comput.* **2017**, *554*, 523–530.

35. Lardier, W.; Varo, Q.; Yan, J. Quantum-Sim: An open-source co-simulation platform for quantum key distribution-based smart grid communications. In Proceedings of the 2019 IEEE international Conference on Communications, Control, and Computing Technologies for Smart Grids, Beijing, China, 21–23 October 2019.
36. Tang, Z.; Qin, Y.; Jiang, Z.; Krawec, W.O.; Zhang, P. Quantum-secure microgrid. *J. IEEE Trans. Power Syst.* **2021**, *36*, 1250–1263. [CrossRef]
37. Tang, Z.; Zhang, P.; Krawec, W.O.; Jiang, Z. Programmable quantum networked microgrids. *J. Trans. Quantum Eng.* **2020**, *1*, 1–13. [CrossRef]
38. Abdallah, A.R.; Shen, X.S. A lightweight lattice-based security and privacy-preserving scheme for smart grid. In Proceedings of the IEEE Global Communications Conference, Austin, TX, USA, 8–12 December 2014; pp. 668–674.
39. Jani, S.; Adrian, K.; Jari, K.; Sami, L. Evaluating the efficiency of physical and cryptographic security solutions for quantum immune IoT. *J. Cryptogr.* **2018**, *2*, 5.
40. Malina, L.; Popelova, L.; Dzurenda, P.; Hajny, J.; Martinasek, Z. On feasibility of post quantum cryptography on small devices. *J. IFAC* **2017**, *51*, 462–467. [CrossRef]
41. Wang, W.; Han, J.; Xie, Z.; Huang, S.; Zeng, X. Cryptography coprocessor design for IoT sensor nodes. In Proceedings of the 2016 International SoC Design Conference (ISOCC), Jeju, Korea, 23–26 October 2016.
42. Premaratne, U.; Samarabandu, J.; Sidhu, T.; Beresh, R.; Tan, J.C. Security analysis and auditing of IEC61850-based automated substations. *J. IEEE Trans. Power Del.* **2021**, *25*, 2346–2355. [CrossRef]
43. Hong, J.; Liu, C.C.; Govindarasu, M. Detection of cyber intrusions using network-based multicast messages for substation automation. In Proceedings of the Innovation Smart Grid Technology, ISGT 2014, Washington, DC, USA, 19–22 February 2014.
44. Kush, E.; Ahmed, N.; Branagan, E.; Foo, M. Poisoned GOOSE: Exploiting the GOOSE protocol. In Proceedings of the 12th Australasian Information Security Conference, Auckland, New Zealand, 20–23 January 2014.
45. Silva, L.E.; Coury, D.V. A new methodology for real-time detection of attacks in IEC 61850-based systems. *J. Electr. Power Syst. Res.* **2017**, *143*, 825–833. [CrossRef]
46. Etamaly, A.M.; Mohamed, A.A.; Majed, A.A.; Alolah, A.I.; Kim, Y.C. Performance of Communication Network for Monitoring Utility Scale Photovoltaic Power Plants. *J. Energy* **2020**, *13*, 5527.
47. Jse, M.P.P.; Antonio, M.A.; Guilermo, S.N.; Maria, C.B.; Angel, M.G. PV Module Monitoring System Based on Low-Cost Solutions: Wireless Raspberry Application and Assessment. *J. Energy* **2018**, *11*, 3051.
48. Mohamed, A.A.; Kim, C.H. Communication Architecture for grid integration of cyber physical wind energy systems. *J. Appl. Sci.* **2017**, *7*, 1034.
49. Transport Layer Security (TLS) Parameters. Available online: https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml (accessed on 30 November 2021).
50. Park, G.C.; Ahn, B.H.; Kim, J.S.; Won, D.J.; Noh, Y.T.; Choi, J.C.; Kim, T.S. An Advanced Persistent Threat (APT)-Style Cyberattack Testbed for Distributed Energy Resources (DER). In Proceedings of the 2021 IEEE Design Methodologies Conference (DMC), Bath, UK, 14–15 July 2021.
51. Eric, M.H.; Michael, J.C.; Rohan, M.A. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In Proceedings of the 6th International Conference on i-Warfare and Security, Washington, DC, USA, 17–18 March 2011.
52. Shin, K.Y.; Kim, K.M.; Lee, J.K. A study on the Concept of Social Engineering Cyber Kill Chain for Social Engineering based Cyber Operations. *J. Korea Inst. Inf. Secur. Cryptol.* **2018**, *28*, 1247–1257.
53. Bae, E.; Kim J., S.; Lee, S.J. Research trends in quantum computational algorithm for cryptanalysis. *J. Korean Opt. Photonics* **2018**, *29*, 53–57.
54. Kim, P.; Han, D.; Jeong, K.C. Time–space complexity of quantum search algorithms in symmetric cryptanalysis: Applying to AES and SHA-2. *J. Quantum Inf. Processing* **2018**, *17*, 1–39. [CrossRef]
55. Bonnetain, X.; Naya-Plasencia, M.; Schrottenloher, A. Quantum security analysis of AES. *J. IACR Symmetric Cryptol.* **2019**, *2*, 55–93. [CrossRef]
56. Davenport, J.H.; Pring, B. Improvements to quantum search techniques for block ciphers with applications to AES. In Proceedings of the Selected Areas in Cryptography 2020, Halifax, NS, Canada, 21–23 October 2020.
57. Almazrooie, M.; Samsudin, A.; Abdullah, R.; Mutter, K.N. Quantum reversible circuit of AES-128. *J. Quantum Inf. Processing* **2018**, *17*, 1–30. [CrossRef]
58. Grassl, M.; Langenberg, B.; Roetteler, M.; Steinwandt, R. Applying grover's algorithm to AES: Quantum resource estimates. In Proceedings of the PQCrypto, FuKuoka, Japan, 24–26 February 2016.
59. Langenberg, B.; Pham, H.; Steinwandt, R. Reducing the cost of implementing AES as a quantum circuit. *J. IEEE Quantum Eng.* **2016**, *1*, 1–12.
60. Jaques, S.; Michael, N.; Martin, R.; Fernando, V. Implementing grover oracles for quantum key search on AES and LowMC. *J. Adv. Eurocrypt* **2019**, *12106*, 280.
61. Proos, J.; Zalka, C. Shor's discrete logarithm quantum algorithm for elliptic curves. *arXiv* **2003**, arXiv:0301141. [CrossRef]
62. Banegas, G.; Bernstein, D.J.; Van Hoof, I.; Lange, T. Concrete quantum cryptanalysis of binary elliptic curves. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2021**, *1*, 451–472. [CrossRef]

63. Roetteler, M.; Naehrig, M.; Svore, K.M.; Lauter, K. Quantum resource estimates for computing elliptic curve discrete logarithms. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hongkong, China, 3–7 December 2017.
64. Jaime, S.; Jess, C.R. Forecasting timelines of quantum computing. *arXiv* **2009**, arXiv:2009.05045.
65. Septhen, S. IBM's Quantum Computing Ambitions Get Exponential Like Moore's Law, Online Article. Available online: https://www.cnet.com/news/ibms-quantum-computing-ambitions-get-exponential-like-moores-law/ (accessed on 9 January 2022).
66. Nicholas, Y. Moore's Law of Moore's Law of Quantum Computing, Online Article. Available online: https://nickyoder.com/moores-law-quantum-computer/ (accessed on 9 January 2022).
67. Press Released from IBM; IBM Achieves Highest Quantum Volume to Date, Establishes Roadmap for Reaching Quantum Advantage, Online Article. Available online: https://www.quantaneo.com/%E2%80%8BIBM-Achieves-Highest-Quantum-Volume-to-Date-Establishes-Roadmap-for-Reaching-Quantum-Advantage_a44.html (accessed on 9 January 2022).
68. Jay, G.; Ismael, F.; Kari, W. IBM's Roadmap for Building an Open Quantum Software Ecosystem, Online Article. Available online: https://research.ibm.com/blog/quantum-development-roadmap (accessed on 9 January 2022).
69. IEEE GRSS Working Group HDCRS, Physical Qubits Roadmap for Quantum Computers, Online Article. Available online: https://www.hdc-rs.com/quantum-computing (accessed on 9 January 2022).
70. NIST, Post Quantum Cryptography 3rd Round Submissions—3rd Round Finalists. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (accessed on 9 January 2022).
71. Borrghany, A.; Sarmadi, S.B.; Jalili, R. On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards. *J. ACM Trans. Embed. Comput. Syst.* **2015**, *14*, 1–25. [CrossRef]
72. Khalid, A.; McCarthy, S.; O'Neill, M.; Liu, W. Lattice-based Cryptography for IoT in A Quantum World: Are We Ready? In Proceedings of the 2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI), Otranto, Italy, 13–14 June 2019.
73. Joseph, A.; Smedley, K. Secure High DER Penetration Power Distribution via autonomously Coordinated Volt/VAR Control. *J. IEEE Power Deliv.* **2020**, *35*, 2272–2284. [CrossRef]
74. Blooming, T.M.; Carnovale, D.J. Capacitor application issues. *J. IEEE Trans. Ind. Appl.* **2008**, *44*, 1013–1026. [CrossRef]
75. Mailloux, L.O.; Grimaila, M.R.; Hodson, D.D.; Baumgartner, G.; McLaughlin, C. Performance Evaluations of Quantum Key Distribution System Architectures. *J. IEEE Secur. Priv.* **2015**, *13*, 30–40. [CrossRef]
76. Wootters, W.K.; Hubert, W. A single quantum cannot be cloned. *J. Nat.* **1982**, *299*, 802–803. [CrossRef]
77. Bennett, C.; Brassard, G. Quantum cryptography: Key distribution and coin tossing. In Proceedings of the International Conference Computer, System Signal Process, Bangalore, India, 9–12 December 1984.
78. Ekert, A.K. Quantum cryptography based on Bells' theorem. *J. Phys. Rev. Lett.* **1991**, *67*, 661. [CrossRef]
79. Sharma, V.; Thapliyal, K.; Pathak, A.; Banerjee, S. A comparative study of protocols for secure quantum communication under noisy environment: Single-qubit-based protocols versus entangled-state-based protocols. *J. Quantum Inf. Process.* **2016**, *15*, 4681–4710. [CrossRef]
80. Fang-Yi, L.; Dong, W.; Shuang, W.; Mo, L.; Zhen-Qiang, Y.; Hong-Wei, L.; Zheng-Fu, H. Effect of electromagnetic disturbance on the practical QKD system in the smart grid. *J. Chin. Phys. B* **2014**, *23*, 12.
81. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *J. Am. Phys. Soc.* **2020**, *92*, 025002. [CrossRef]
82. Diouvu, R.C.; Agee, J.T. Enhancing the security of a cloud-based smart grid AMI network by leveraging on the features of quantum key distribution. *J. Trans. Emerg. Telecommun. Technol.* **2019**, *30*, 1–21. [CrossRef]
83. Borges, F.; Santos, R.A.M.; Marquezino, F.L. Preserving privacy in a smart grid scenario using quantum mechanics. *J. Secur. Comm. Netw.* **2015**, *8*, 2061–2069. [CrossRef]
84. Kim, T.H.; Cho, S.B.; Cho, J.S.; Choi, J.W.; Kwak, S.H. Development of quantum communication technologies in SK telecom. In Proceedings of the 17th Opto-Electronics and Communications Conference, Busan, Korea, 2–6 July 2012.
85. Kim, T.H. Status of QKD System Deployment and Ion Trap Development at SK Telecom. Available online: http://www2.yukawa.kyoto-u.ac.jp/~{}rqin-2017/slides/Taehyun_Kim.pdf (accessed on 30 November 2021).
86. Cao, Y.; Zhao, Y.; Wang, J.; Yu, X.; Ma, Z.; Zhnag, J. Cost-Efficient Quantum Key Distribution (QKD) Over WDM Networks. *J. Opt. Commun. Netw.* **2019**, *11*, 285–298. [CrossRef]
87. Bista, A.; Sharma, B.; Galvez, E.J. A demonstration of quantum key distribution with entangled photons for the undergraduate laboratory. *J. Am. Phys.* **2021**, *89*, 111–120. [CrossRef]
88. Park, B.; Woo, M.; Kim, Y.; Cho, Y.; Moon, S.; Han, S. User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a 1 × N quantum key distribution network system. *J. Photonics Res.* **2020**, *8*, 296–302. [CrossRef]
89. Woo, M.; Park, B.; Kim, Y.; Cho, Y.; Jung, H.; Lim, H.; Kim, S.; Han, S. One to Many QKD Network System Using Polarization-Wavelength Division Multiplexing. *J. IEEE Photonics Soc.* **2020**, *8*, 194007–194014. [CrossRef]
90. Hassan, H.A.; Mohamad, E.H.G.; Nikos, D.H. A Decentralized Functional Observer Based Optimal LFC Considering Unknown Inputs, Uncertainties, and Cyber-Attacks. *J. IEEE Trans. Power Syst.* **2019**, *34*, 4408–4417.