2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) | 979-8-3503-1360-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISGT59692.2024.10454235

Post-Quantum Cryptography (PQC)-Grade IEEE 2030.5 for Quantum Secure Distributed Energy Resources Networks

Kalyan Nakka, Seerin Ahmad, Taesic Kim*, Logan Atkinson, and Habib M. Ammari
Electrical Engineering and Computer Science, Texas A&M University-Kingsville, Kingsville, TX, 78363 USA
{venkata_swamy_kalyan.nakka; seerin.ahmad; logan.atkinson}@students.tamuk.edu, taesic.kim@tamuk.edu, habib.ammari@tamuk.edu

***Abstract*—Quantum era is near and advanced quantum computing will pose a huge threat to the security of the current cryptographic systems in distributed energy resources (DER)-rich power grids. It is necessary to prepare now to combat quantum computing attacks with serious real-world consequences in the years ahead. Recently, post-quantum cryptography (PQC) is considered as one of the major candidates of quantum attack defense strategies, and the adoption of PQC for DER systems has not been fully studied yet. This paper discusses the adoption of PQC in a standard DER network protocol (i.e., IEEE 2030.5-PQC), and proposes a real-time hardware-in-the-loop co-simulation PQC testbed consisting of a DER physical system simulation and a cyber system simulation such as DER gateways and DER management system (DERMS) server. Universal custom-made PQC client and server software are developed to meet the compliant with IEEE 2030.5-2018 standard and implemented in the DER gateways and the DERMS server, respectively. Finally, the feasibility of the proposed PQC-grade DER network is validated by using the real-time co-simulation testbed.**

Keywords—Cybersecurity, distributed energy resources, hardware-in-the-loop testbed, post quantum cryptography.

I. Introduction

Today's power grid is transitioning to distributed energy resources (DER)-rich power grid due to the high penetration of DER such as renewable energy systems, energy storage systems, electric vehicle charging infrastructures, and controllable loads in distribution and sub-transmission systems [1], [2]. The growing penetration of DER will provide cheaper and cleaner power and ultimately reach the nation's goals of 100% clean electrical grid by 2035 and net-zero carbon emissions by 2050 [3]. Several roadmaps, standards and regulations for DER cybersecurity were recently developed (e.g., photovoltaic (PV) systems [5] and wind turbine (WT) systems [6] released in 2017 and 2020, respectively). The roadmaps summarize cybersecurity best practices, looking to the future, a list of possible next steps for strengthening cyber resiliency. IEC 62351 [7] contains provision to ensure the integrity, authenticity and confidentiality for different network protocols used in power system. IEEE 1547-2018 [8] defines the interconnection and interoperability requirements for DER connected to grids (e.g., IEEE 2030.5) and recommends transport layer security (TLS) and certificates provided by the authorized issuers. Such TLS and certificates (e.g., SunSpec public key infrastructure (PKI) certificate [9]) will improve protection against eavesdropping and replay, man-in-the-middle (MitM) security risk and spoofing [4], [10].

This research was supported in part by National Science Foundation under award No. CNS-2219733.

It is observed that current security best practices and industry standards for DER systems largely rely on public key cryptography-based authentication and authorization, AES-based encryption, and hash-based data integrity check. However, the advent of quantum computing will create a huge threat to the security of the current cryptographic systems adopted in DER network systems [11]. It is also anticipated that more than half of cryptography will be easily broken by quantum cryptanalytic attacks using quantum computing resources and algorithms by 2030 [12], [13]. This will push a new phase in the eternal race between defenders and attackers [14].

To address the increasing concerns of quantum cryptanalytic attacks, two emerging technologies have been mainly studied: 1) Quantum key distribution (QKD)-based secret key distribution methods and 2) Post quantum cryptography (PQC). In power grid applications, QKD methods have been widely investigated [15-19]. Compared to QKD methods, a few PQC cryptography-based solutions have been proposed [20], [21]. The earliest approach of PQC in smart grids utilizes lattice-based cryptography that is based on finding almost orthogonal vector (i.e., the shortest vector problem to encrypt messages as noisy lattices [21]). In July 2022, NIST announced four public-key PQC algorithms to be standardized.

This paper extends the work of [23] to develop a practical PQC-grade DER network protocol (i.e., IEEE 2030.5-PQC). The candidates of public-key PQC algorithms selected by NIST replace the key exchange algorithm and digital signature algorithm in TLS 1.3 protocol and evaluated by using the real-time hardware-in-the-loop (HIL) co-simulation PQC testbed which consists of a DER physical system simulation and a real cyber and network system. To the authors' best knowledge, this paper may be one of the few practical studies for designing and evaluating the PQC-grade IEEE 2030.5 DER network protocol.

II. PQC-grade IEEE 2030.5 DER Network

Fig. 1 shows an example of DER communication architecture using the PQC-grade IEEE 2030.5. PQC-grade IEEE 2030.5 applies to communications between the utility DERMS and DER systems through connections via DER facility controller, an aggregator, or direct connections. In the direct DER communications, either the smart inverter control unit (SMCU) or a separate gateway/control unit will be the PQC-grade IEEE 2030.5 client. The DER aggregator manages small DER as a PQC-grade IEEE 2030.5 server and communicates with DERMS as a client.

The technical elements of IEEE 2030.5-2018 that correspond to the Open Systems Interconnection (OSI) layer

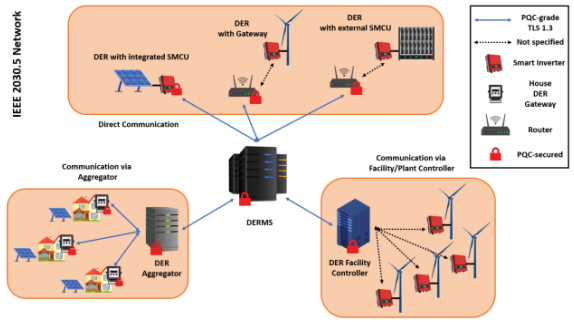


Fig. 1. Utility-to-DER communication architecture using PQC-grade IEEE 2030.5.

are as follows:1) an IP-based network that combines different link layer technologies (such as Wi-Fi and ZigBee) to promote interoperability; 2) the proposed PQC-grade TLS v1.3; 3) representation state transfer (REST) HTTP architecture over TCP/IP for a client-server interaction; and 4) extensible markup language (XML) schema; 5) multicase DNS (mDNS) for host discovery on a local area network (LAN) and DNS-SD for resource discovery; and 6) application profile sources elements to direct DER controls support defined in IEEE 1547-2018. Clients and servers perform mutual authentication using digital certificates (i.e., PQC-grade X.509 v3) during handshake through verification with the Root-CA using the PQC DSA algorithm. RESTful protocols allow HTTP actions. CSIP defines the operation of IEEE 2030.5 in the California Rule 21 use case. For example, POST (create) and DELETE (remove) can be used to create or remove DER end-devices or DER controllers.

III. Proposed PQC-grade IEEE 2030.5 DER Network Testbed

This section provides the details of our real-time HIL PQC testbed, where a real-time physical system simulation is discussed in section III.A and a real cyber system using network hardware and a server is discussed in section III.B.

Fig. 2 shows the experimental setup performing evaluation of the PQC algorithm candidates in a DER system. The real-time hardware-in-the-loop (HIL) DER system testbed consists of a DER physical system simulator using an OPAL-RT's OP-4510 with MATLAB/Simulink and a real-time DER network including DER gateways, a DERMS server, and a router. Custom-made DER gateways and DERMS are implemented in Raspberry Pi 4Bs. A custom-made CA program is designed to provide Root-CA public key. It is noted that the custom-made PQC-grade IEEE 2030.5 program can be universal and implemented in other types of gateway hardware and OS settings.

A. DER Physical System Modeling and Simulation

Fig. 3 illustrates a DER system in IEEE 13 Node Test Feeder circuit where the DER system consists of multiple smart inverters, a swing bus, a WT system, a PV system, an energy storage system (ESS) and loads. The system bus frequency is 60Hz and the nominal voltage is 4.16kV. Smart inverters of WT and PV perform maximum power point tracking (MPPT) controls. The WT of the 634 bus is applied with the permanent magnet synchronous generator (PMSG) model and the rated power is 2.2 MVA. The PV is located on bus 675 and the rated output is 1MW. The ESS capacity of bus 680 is 1 MWh and a lithium-ion battery model is used. Except for the bus where the generators are connected, the resistive, inductive, and capacitive loads are evenly connected to the other buses, where the real power demand of the distribution system is 3.5 MW; the reactive power demand of inductive loads is 2.102 MVAR; and the reactive power demand of capacitive loads is 0.7 MVAR. The impedance values between the buses are chosen based on the IEEE 13 bus system [23].

Fig. 4 illustrates the inverter control model for the ESS. The primary controller controls the voltage, current, active, and reactive power flow of the ESS inverter. A droop control is applied for primary control of the controller. Combination of active/reactive (P/Q) power calculation and droop control determines $I_{edq0,ref}$ (= $I_{ed,ref}$ and $I_{eq,ref}$) which can be expressed as follows:

$$I_{ed,ref} = \frac{2}{3}\frac{P_{eref}}{V_{ed}} \quad (1)$$

$$I_{eq,ref} = -\frac{2}{3}\frac{Q_{eref}}{V_{ed}} \quad (2)$$

where P_{eref} and Q_{eref} are the active and reactive power references, respectively; and V_{ed} is the measured line voltage. Through the P/Q calculation and droop control, P_{eref} and Q_{eref} are computed as follows:

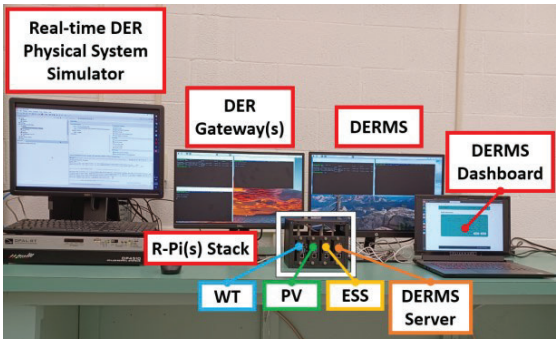
$$P_{eref} = P_{eref,a} + \Delta P_{edroop} \quad (3)$$

$$Q_{eref} = Q_{eref,a} + \Delta Q_{edroop} \quad (4)$$

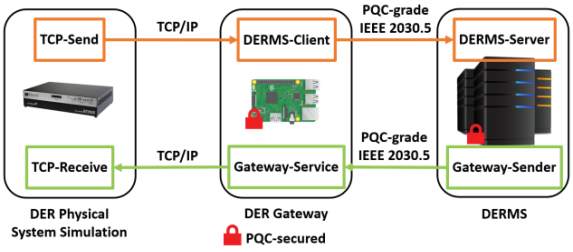
$$\Delta P_{edroop} = -\frac{f - f_0}{K_{eP}} \quad (5)$$

$$\Delta Q_{edroop} = -\frac{V - V_0}{K_{eQ}} \quad (6)$$

where $P_{eref,a}$ and $Q_{eref,a}$ are active and reactive power control commands from DERMS, respectively; ΔP_{edroop} and



(a)



(b)

Fig. 2. PQC-grade DER network testbed: (a) real-time HIL DER system testbed and (b) PQC-grade IEEE 2030.5 implementation in the tested.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

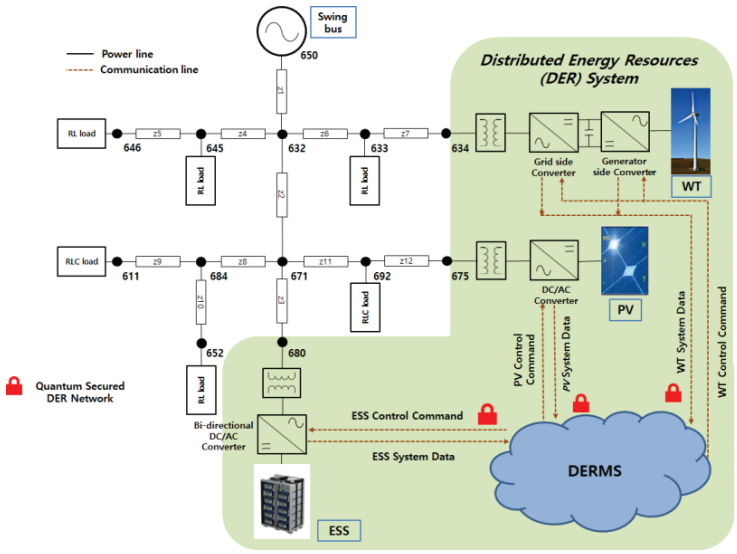


Fig. 3. DER system in IEEE 13 node test feeder circuit, monitored and controlled by a utility DERMS.

ΔQ_{edroop} denote the variations of P and Q, respectively; f_0 and V_0 are nominal frequency and voltage of the system; f *and* V are measured inverter output frequency and voltage, respectively; and K_{eP} and K_{eQ} are droop coefficients. The DER system described is simulated in MATLAB/Simulink environment and run by the real-time simulator.

B. Real Cyber System using PQC-grade IEEE 2030.5

Each DER gateway is connected to the WT, PV, and ESS running in the real-time simulator via TCP/IP. The custom-made DERMS server receives the DER data from the DER gateways and sends control commands to the DER gateway as shown in Fig. 2(b). PQC-grade cryptographic protocols are programmed using OpenSSL of Open Quantum Safe project [24] and liboqs library [25]. The CA utilizes the PQC candidate algorithms to sign certificates of the DERMS server.

The DERMS server is hosted on Raspberry Pi 4B that uses the Nginx HTTPS server for reverse-proxy and routing. To comply with the technical requirements of IEEE 2030.5-2018 standard, Python 3.6.9 and Flask REST Framework are utilized to develop the server. For the lightweight execution, we leverage a docker platform deploying and running these applications. The DERMS server comprises of two docker containers: PQC-grade TLS 1.3-based Nginx docker container and a DERMS web-application docker container. The

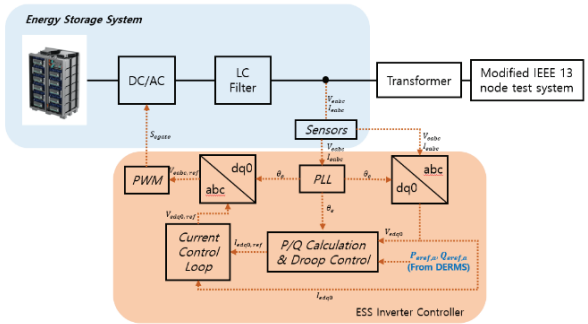


Fig. 4. DER system in IEEE 13 node test feeder circuit, monitored and controlled by a utility DERMS.

DERMS Nginx docker is the point of contact to all the incoming client connections ensuring PQC-grade communication, while the incoming communication data is decrypted and sent to the DERMS web-application. This incoming real-time DER systems data is processed and saved on the server in a local SQLite3 database. By utilizing a Short-Form Device Identifier (SFDI), these details are mapped to each of the DERs. Using the Python module pyplot from matplotlib, these data are shown in real time as a graph on DERMS web-application. Control commands from DERMS are sent to each of the DER gateways using PQC-grade curl ensuring PQC-grade encryption of the control command.

The DER Gateway is also hosted on Raspberry Pi 4B that uses DERMS Client software and Gateway Service software, which comprises of two docker containers: a PQC-enabled TLS 1.3-based Nginx docker container and a Gateway API docker container. PQC is enabled at all software communication points of DER Gateway and DERMS, ensuring PQC-grade encryption in 2-way communication between DER gateway and the DERMS server.

C. DER Network Operation

Once the TLS network is established, the DER gateways and DERMS server carry out CSIP operation. In order to control the DER gateways, the DERMS server sends commands such as autonomous function (for example, vol-var, volt-watt, and Freq-watt), immediate control (e.g., active power curtailment, fixed reactive power, and fixed power factor), and protection setting (e.g., high/low voltage ride-through and high/low frequency ride-through), through the intervention of DERMS operator. The DER gateways transmit system data, including DER nameplate ratings and settings, DER alerts and status, and DER measurements to the DERMS server (e.g., active power, reactive power, voltage, current, power factor, and frequency). In practice, more DERMS functions and software modules can be integrated as microservices in a cloud environment.

IV. Validation

In order to evaluate the feasibility of the PQC-grade IEEE 2030.5 into DER network operations over TLS 1.3, we intend to conduct network performance (i.e., size and time of TLS

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

handshake) and monitoring and control tests using the proposed tested. Among the NIST selected algorithms, total six candidates of PQC cipher suites were selected and implemented to the IEEE 2030.5 protocol by replacing the current cipher suite which is vulnerable to quantum computing attacks (i.e., ECDHE_ECDSA).

A. PQC Handshake Evaluation

Table I shows the comparison of handshake message size for the chipper suites. It is noted that the sizes of the Server Certificate and Key Exchange have grown by two orders of magnitude as a direct result of the larger size of `Falcon1024`, `Dilithium5`, and `Dilithium5-AES` signatures. The Server Certificates of both `Dilithium5` and `Dilithium5-AES` signatures are of same size, 20736 bytes, which is larger than that of `Falcon1024` (14344 bytes). There is slight difference observed in Server Key Exchange messages size between `Kyber1024` and `Kyber1024-90s` algorithms. Since the Client Key Exchange mostly comprises the client's key exchange data (a Kyber cipher text), the message size only increased over thrice of classical one. Overall, PQC algorithms require large message size, while `Kyber1024_Falcol1024` and `Kyber1024-90s_Falcol1024` are the best choice in terms of message size among the PQC cipher suits.

Table II shows the runtime of initial handshake and session ID reuse handshake for all use cases. The TLS handshake utilizing classical cryptography takes about 33.16 ms for initial handshake and takes a minimum of 33.53 ms for session ID reuse. All the PQC cipher suites outperform the classical one by minimum of 4 times and maximum of 12 times differences. Among all the PQC cipher suites, `Kyber1024_Falcon1024` has the best runtime for both initial and session ID reuse handshakes, which are 2.78 ms and 4.07 ms respectively, and are almost 12 times and 8 times respectively faster than the current cipher suit (ECDHE_ECDSA).

TABLE I.
COMPARISON OF HANDSHAKE MESSAGE SIZES OF ALL CIPHER SUITES

Cipher Suite	Server		Client Key Exchange
	Certificate	Key Exchange	
KYBER1024_FALCON1024	14344 B	6330 B	1973 B
KYBER1024-90S_FALCON1024		6340 B	
KYBER1024_DILITHIUM5	20736 B	13784 B	
KYBER1024_DILITHIUM5-AES			
KYBER1024-90S_DILITHIUM5		13796 B	
KYBER1024-90S_DILITHIUM5-AES			
ECDHE_ECDSA (current)	521 B	970 B	538 B

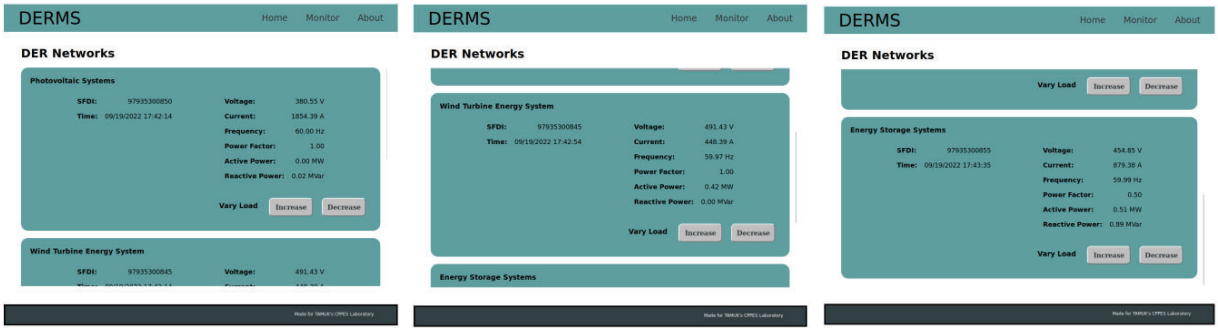
TABLE II.
COMPARISON OF HANDSHAKE RUNTIME FOR ALL CIPHER SUITES

Cipher Suite	Handshake (ms)	
	Initial	Session ID reuse
KYBER1024_FALCON1024	**2.78**	**4.07**
KYBER1024-90S_FALCON1024	3.46	4.55
KYBER1024_DILITHIUM5	3.73	4.94
KYBER1024-90S_DILITHIUM5	4.46	8.48
KYBER1024_DILITHIUM5-AES	6.17	6.79
KYBER1024-90S_DILITHIUM5-AES	6.49	7.35
ECDHE_ECDSA (current)	33.16	33.53

B. Monitoring and Control in DERMS

Based on the evaluation of TLS handshake, we have decided to implement the `Kyber1024_Falcon1024` for further studying and understanding the DER monitoring and control capabilities. The real-time DER data from the physical system simulator is sent from DER Gateway to DERMS Server utilizing the PQC-grade TLS 1.3 network. Fig. 5 illustrates the real-time data from PV, WT and ESS in DERMS Server, which is relayed through the DER Gateway with one second sampling rate. It is practically observed that the DERMS Server is able to monitor the real-time DER system data through the PQC-grade TLS 1.3 network.

Fig 6(a) shows the voltage sag at PCC caused by increased inductive load after 13 seconds. Since DERMS has the capability to manage the DER, the DERMS operator was able to send the control command to ESS from DERMS by clicking on the Increase button in ESS control to provide the requested reactive power after some delay at 16 seconds. In a practical DERMS, this patch can also be automatically executed to achieve a control automation. By providing the requested $Q_{eref,a}$ ESS recovers the voltage at PCC. Therefore, the PCC voltage returns to the original value. Fig 6(b) shows the



(a) (b) (c)

Fig. 5. Real-time DER data monitoring in the custom-made DERMS server (a) PV, (b) WT and (c) ESS.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

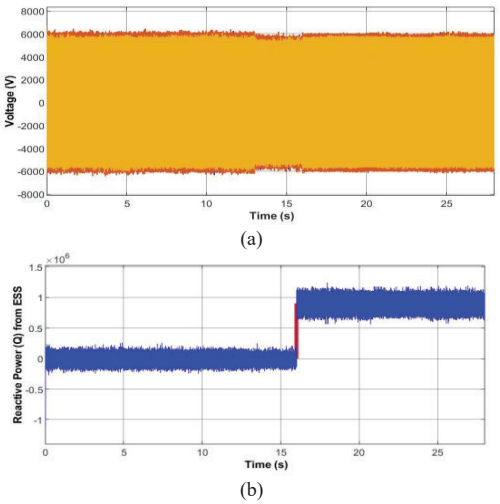


Fig. 6. Experimental results: (a) voltage waveform and (b) ESS control.

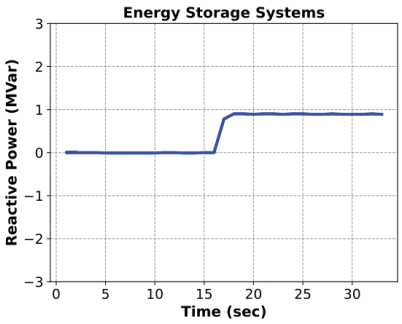


Fig. 7. Reactive power output of the ESS in DERMS.

measured reactive power from the *ESS* (shown in blue) to recover the voltage at PCC which fully follows the reference set value (shown in red). We were able to monitor these reactive power changes of ESS due to the new control command sent by DERMS web application as shown in Fig. 7. Therefore, the PQC-grade DER protocol does not interrupt DER monitoring and operation.

V. Conclusion

Quantum technology will give rise to greater threats and provides opportunities for more secure encryption in the DER network. New attacks can be developed by employing a quantum computer capable of readily breaking present encryption techniques. Therefore, security researchers must monitor quantum computing trends. This paper provides a PQC-grade DER network architecture and investigated the best PQC cipher suite using the real-time HIL DER testbed. The custom-made PQC-grade tools can be applied to various types of DER gateways and DERMS servers. Finally, we recommend `Kyber1024_Falcon1024` cipher suite among NIST PQC finalist for secure DER networks.

References

[1] B. Kroposki *et al.*, "Achieving a 100% renewable grid: Operating electric power systems with extremely high levels of variable renewable energy," *IEEE Comput. Applic. Power*, vol. 15, no. 2, pp. 61–73, 2017.

[2] D. Michelle, *et al*. "U.S solar market insight", Tech. Reports, Wood Mackenzie and Solar Energy Industries Association (SEIA), Dec 2021.

[3] NREL Analysis. [Online]. Available: https://www.nrel.gov/analysis/100-percent-clean-electricity-by-2035-study.html. [Accessed: 23-Aug-2023].

[4] D. Saleem and C. Carter, "Certification procedures for data and communications security of distributed resources," National Renewable Energy Laboratory, Tech. Rep., NREL/TP-5R00- 73628, Jul. 2019.

[5] J. Johnson, "Roadmap for photovoltaic cyber security," Sandia National Laboratories, Tech. Rep. SAND2017-13262, Dec. 2017.

[6] Roadmap for wind cybersecurity, Tech, Rep. DOE/GO 102020 8441 8220, U.S. Department of Energy, July 2020.

[7] IEC 62351, [Online]. Available: https://webstore.iec.ch/publication/6912

[8] IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, IEEE Std. 1547-2018, Feb. 2018.

[9] "SunSpec public key infrastructure (PKI)," *SunSpec Alliance*, 08-Sep-2019. [Online]. Available: https://sunspec.org/sunspec-public-key-infrastructure/. [Accessed: 23-Aug-2023].

[10] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *2019 Resilience Week (RWS)*, 2019.

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

[12] "IBM blog," IBM Blog, 28-May-2013. [Online]. Available: https://www.ibm.com/blogs/research/2021/02/quantum-development-roadmap. [Accessed: 23-Aug-2023].

[13] T. C. Clancy, R. W. McGwier, and L. Chen, "Post-quantum cryptography and 5G security: Tutorial," in *Proc. the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019.

[14] D. Leprince-Ringuet, "Quantum computers could soon reveal all of our secrets. The race is on to stop that happening," ZDNET, 02-Nov-2020. [Online]. Available: https://www.zdnet.com/article/quantum-computers-could-one-day-reveal-all-of-our-secrets. [Accessed: 23-Aug-2023].

[15] D. Flessnerm, "Tennessee utility uses quantum tech for cybersecurity," Chattanooga Times, Mar. 2020.

[16] P.-Y. Kong, "A review of quantum key distribution protocols in the perspective of smart gird communication security," *IEEE Systems Journal*, vol. 16, no. 1, pp. 41–54, Mar. 2022.

[17] W. Lardier, Q. Varo, and J. Yan, "Quantum-Sim: An open-source co-simulation platform for quantum key distribution-based smart grid communications," in *Proc. 2019 IEEE international Conference on Communications, Control, and Computing Technologies for Smart Grids*, pp. 1–6.

[18] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure microgrid," *IEEE Trans. Power Systems*, vo. 36, no. 2, pp. 1250–1263, Mar. 2021.

[19] Z. Tang, P. Zhang, W. O. Krawec, and Z. Jia ng, "Programmable quantum networked microgrids," *Trans. Quantum Engineering*, vol. 1, pp. 1–13, Aug. 2020.

[20] A. R. Abdallah and X. S. Shen, "A lightweight lattice-based security and privacy-preserving scheme for smart grid," in *Proc. IEEE Global Communications Conference*, Austin, TX, USA, 2014. pp. 668–674.

[21] A. Abdallah and X. S. Shen, "A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 396-405, Jan. 2018.

[22] J. Ahn, *et al.*, "Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD)," *Energies*, vol. 15, 714, Jan. 2022.

[23] J. Kim *et al.*, "Real-time hardware-in-the-loop distributed energy resources system testbed using IEEE 2030.5 standard," in *2021 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia)*, 2021.

[24] Openssl: Fork of OpenSSL that includes prototype quantum-resistant algorithms and ciphersuites based on liboqs, *Github.com*. [Online]. Available: https://github.com/open-quantum-safe/openssl. [Accessed: 23-Aug-2023].

[25] liboqs: C library for prototyping and experimenting with quantum-resistant cryptography, *Github.com*. [Online]. Available: https://github.com/open-quantum-safe/liboqs. [Accessed: 23-Aug-2023.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE