Quantum Secured Traveling Wave Protection

Siyun Wang, Ruoyan Fan, Yacov Shamash, and Peng Zhang

***Abstract*—This paper introduces a quantum-secured traveling-wave protection (QDTWP) framework that enhances the cybersecurity of relay-to-relay communication in modern power grids. QDTWP enables direct protection signaling over standard packet networks instead of dedicated fibers while preserving the ultra-high-speed response required by traveling-wave relays. Our contributions include: 1) Developing a lightweight HMAC-based authentication layer tailored for traveling-wave relay communication; 2) Integrating real-time quantum keys to achieve information-theoretic message integrity and resistance to eavesdropping. Experimental results demonstrate millisecond-level end-to-end latency and complete protection against message tampering, validating the feasibility of using Quantum Key Distribution (QKD) to secure ultra-fast protection channels in future quantum-resilient power grids.**

***Index Terms*—Quantum key distribution (QKD), traveling wave protection, cyber-physical security, Hash-based Message Authentication Code (HMAC).**

I. Introduction

Traveling-wave protection (TWP) has gained increasing significance in modern power grids, as traveling-wave relays (TWRs) can identify and locate faults within 1–5 ms by exploiting the initial wavefront of transient voltage and current signals [1]. This fast detection capability helps prevent disturbance propagation and enhances system stability [2]. In large interconnected networks, such rapid response is crucial under severe disturbances or cascading fault conditions. Recent large-scale disturbances, such as the Iberian Peninsula blackout in 2025, have demonstrated how quickly transients can escalate in low-inertia grids [3], further emphasizing the necessity of ultra-fast protection methods like TWP.

Traveling-wave protection can be implemented in either single-ended or double-ended forms. Single-ended TWP relies solely on local measurements and must identify reflected wavefronts, making it less reliable under complex reflections or waveform distortion [4]. In contrast, double-ended TWP uses synchronized measurements from both line ends, eliminating the need for reflection identification and reducing errors caused by system non-uniformity or coupling effects [5]. Given these robustness and accuracy benefits, this work adopts the double-ended TWP scheme.

In double-ended traveling-wave protection schemes, relays at each terminal use the travelling-wave arrival information locally to determine breaker tripping [1]. Each relay also sends a transfer trip signal to the opposite terminal. However, if the local relay fails to operate, the scheme must rely on the remote relay's transfer trip signal to trip the breaker [6]. This remote trip signal is therefore important and must be protected to prevent breaker misoperation.

Beyond the breaker–relay wiring used for local tripping, the relay-to-relay communication in existing TWR implementations usually rely on direct fiber-optic links. Although these approaches ensure deterministic latency, they require high installation and maintenance costs due to dedicated infrastructure, antennas. In existing commercial implementations, dedicated optical interfaces are typically used for protection signaling. These interfaces provide reliable low-latency communication, but are limited to short-range, point-to-point connections, which increases installation cost and reduces deployment flexibility.

To address these limitations, this work presents a quantum-secured traveling-wave protection (QDTWP) framework, as shown in Fig. 1, featuring:

- Secure relay-to-relay signaling using QKD-generated keys and lightweight HMAC authentication;
- A low cost communication path implemented over standard UDP/IP links.

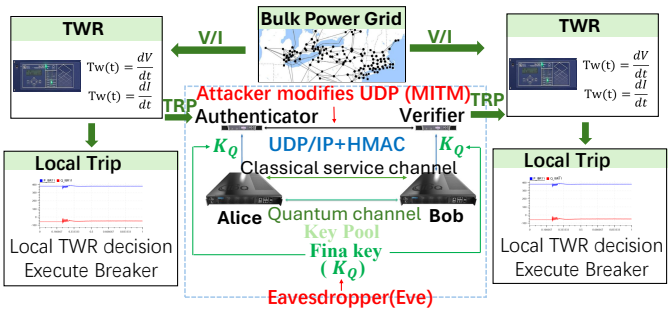


Fig. 1: Entire system setup

II. Quantum Secured Double-Ended TWP

This section introduces the implemented QDTWP framework. Section II-A outlines the system architecture, including the double-ended TWR configuration and communication model used for exchanging the remote trip signals. Section II-B reviews the QKD security foundation, and Section II-C explains how quantum-generated keys are integrated with HMAC^Q to enable authenticated relay communication.

A. Double-Ended TWR Signal Mode

In a double-ended TWR scheme, a fault introduces a sudden change in voltage and current that launches traveling waves toward both terminals at the line propagation velocity v. Each

This work relates to the Department of Navy award N000142512374 issued by the Office of Naval Research. The United States Government has a royalty-free license throughout the world in all copyrightable material contained herein. *Corresponding Author: Peng Zhang.*

The authors are with the Department of Electrical and Computer Engineering, Stony Brook University, NY 11794-2350 USA (e-mails: siyun.wang, ruoyan.fan, p.zhang@stonybrook.edu).

relay, located at Terminals A and B, detects the first wavefront arrival and records the corresponding timestamp t_i. The fault location, measured from Terminal A, is obtained by comparing the two arrival times:

$$d = \frac{l + (t_B - t_A)v}{2}, \tag{1}$$

where l is the total line length and t_A and t_B represent the wavefront arrival times measured at Terminals A and B, respectively [7] .

Each terminal performs local fault detection based on its measured wavefront arrival time. A local tripping decision TRP_i^L is formed according to the estimated fault location, and this decision is represented by a binary value: TRP_i^L ($i \in \{A, B\}$).

$$TRP_i^L = \begin{cases} 1, & \text{if fault is within protection zone,} \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

If $TRP_i^L = 1$, the relay issues a local trip command to its circuit breaker. For dependable operation, each relay also sends a remote trip signal TRP to the opposite terminal. When the local trip cannot be executed because of communication loss, missed wavefront detection, or internal blocking, the relay uses the remote TRP received from the opposite terminal to initiate breaker tripping. This exchanged binary signal forms the protection message that requires secure transmission in the implemented QDTWP framework.

The communication between relays is implemented as a UDP/IP link that exchanges message frames:

$$P = [TRP,\ Seq,\ HMAC^Q], \tag{3}$$

where Seq denotes a sequence counter for packet tracking, and $HMAC^Q$ is the integrity tag computed using the Q-key generated from the QKD process. This lightweight communication layer is designed to maintain deterministic end-to-end latency below 5 ms while guaranteeing message authenticity and integrity [1].

B. QKD Security Foundation

QKD provides the physical-layer security for the implemented QDTWP framework by generating Q-key [8], [9]. Its security is founded on two fundamental principles:

- **Measurement–Disturbance Relation:** The key bits are encoded in quantum states, and any attempt to probe them introduces detectable errors. Such disturbances increase the Quantum Bit Error Rate (QBER), allowing the legitimate users to detect any attempt to obtain the Q-key required to forge the authenticated TRP message [10], [11].
- **No-Cloning Theorem:** Since arbitrary quantum states cannot be copied, an adversary cannot create a duplicate of the transmitted quantum signals to extract the Q-key offline. Any replication attempt requires interaction with the original states, producing detectable disturbances. As a result, the Q-key remains inaccessible to an intruder [12].

C. Q-Key Integration with HMAC^Q

To achieve low-latency message authentication, the QDTWP employs a HMAC^Q using a Q-key. The lightweight nature of HMAC^Q arises from two aspects.

- **Computational Level:** HMAC^Q retains the efficiency of standard HMAC–SHA256 through the following two properties: First, SHA-256 relies only on lightweight bitwise operations (XOR, shifts, additions) and executes a fixed 64-round structure with constant runtime on embedded relay processors. Second, HMAC invokes SHA-256 twice without introducing additional algorithmic stages, resulting in deterministic latency and linear computational cost $O(n)$ [13]. The two SHA256 steps are:

$$H_{\text{in}} = \text{SHA256}((K_Q \oplus \text{ipad}) \,\|\, M)\,, \tag{4}$$

$$T = \text{SHA256}((K_Q \oplus \text{opad}) \,\|\, H_{\text{in}})\,, \tag{5}$$

  where T is the resulting HMAC^Q authentication tag. M is the transmitted relay message containing the TRP signal and Seq. And the Q-key, denoted by K_Q, is the synchronized quantum key shared between the two terminals.
- **Management Level:** The use of Q-key simplifies key handling at the management level. The Q-key are continuously refreshed by the QKD module and stored in a key pool [14], eliminating manual key distribution or periodic renewal. This autonomous key supply reduces operational overhead and avoids the control delays associated with traditional key management.

As a result, message integrity is verified at the receiver by recomputing T using the same Q-key. Since Q-key refresh occurs asynchronously in the background, the authentication procedure introduces no observable delay to the real-time requirements of the TWP scheme.

III. Implementation and Experimental Setup

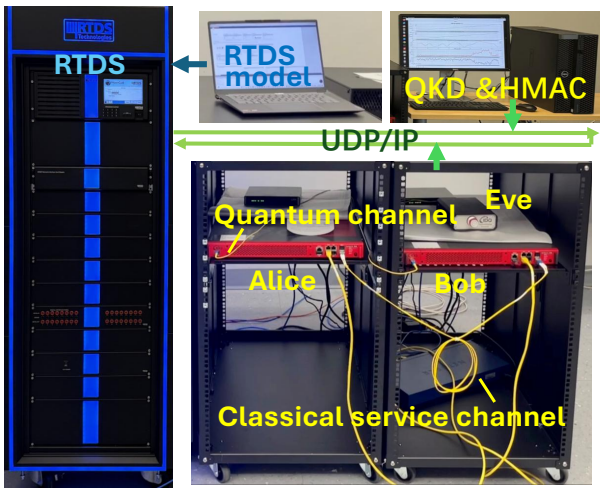


Fig. 2: HIL setup for verifying QDTWP

This section presents the hardware-in-the-loop (HIL) testbed developed to evaluate the QDTWP framework under realistic real-time operating conditions. As shown in Fig. 2, the testbed

integrates RTDS-based double-ended TWR protection environment, a QKD system for Q-key generation, and a lightweight HMAC authentication module.

- **RTDS-based Protection Environment:** The RTDS simulates a modified NPCC system, where the QDTWP is deployed at both terminals of a selected transmission line. The TWP logic runs inside two virtual relays in the RTDS environment. The relay output, including the local trip decision and the TRP message, is forwarded to an external authentication module running on a host PC. In this module, each UDP packet is tagged and verified using the current Q-key before being returned to the RTDS environment. Meanwhile, the QKD system continuously supplies synchronized Q-key to both terminals, ensuring that the sender and verifier operate with the same key. This data flow links the RTDS protection logic, the authentication module, and the QKD system into integrated and real-time QDTWP test environment.
- **QKD System Integration:** The QKD system is implemented as an Alice–Bob pair connected via a quantum channel and an authenticated classical channel. The device performs the standard BB84 post-processing procedures, including sifting, error correction, and privacy amplification, and outputs synchronized Q-key at both nodes [15] [16]. This Q-key is delivered to the protection-layer modules of the testbed and used as the authentication keys in the QDTWP workflow.
- **HMAC Authentication Module:** A lightweight HMAC^Q module runs on an external host PC, interfacing with both the RTDS and the QKD node to authenticate relay-to-relay trip messages. The authentication workflow operates as follows:
  A lightweight HMAC^Q module runs on an external host PC, interfacing with both the RTDS relays and the QKD node to authenticate relay-to-relay trip messages. When Relay A issues a UDP trip frame, the PC intercepts the packet, computes a 256-bit HMAC^Q tag using the current Q-key, and appends this tag before returning the authenticated packet to the RTDS environment for delivery to Relay B. For each packet destined for Relay B, the PC recalculates the HMAC^Q with the same Q-key and compares it with the received tag; only packets with a valid HMAC^Q are forwarded, while any forged or altered packets are immediately discarded. An MITM attacker module is also deployed on the same PC to modify the TRP signals for security–testing purposes.

Two attack scenarios are implemented to evaluate the security of QDTWP.

- In the first scenario, an eavesdropper (Eve) is introduced on the quantum channel to test whether the system can prevent compromised keys from entering the protection workflow. The intrusion causes a visible increase in QBER; once the QBER exceeds the preset threshold, the QKD module halts the key generation process and discards the affected key round. This ensures that only the uncompromised Q-key is supplied to the HMAC^Q module, thereby guaranteeing that the TRP messages are never authenticated with insecure key.
- The second scenario introduces a MITM adversary on the UDP channel to test whether the system can withstand manipulation of the trip messages. Using Q-key, the HMAC^Q module rejects all altered or injected packets, while only authenticated trip messages are accepted.

IV. Case Study

This section evaluates the effectiveness and real-time performance of QDTWP. All experiments are conducted on an RTDS-based test system configured with two TWRs, Relay A and Relay B, representing opposite ends of a protected transmission line. The RTDS GTNET-SKT module is employed to emulate a packet-based communication channel between relays.

In this environment, the trip signal generated by the transmitting relay is sent as a single Boolean value over a UDP path. Accordingly, this study focuses on message tampering, evaluating whether the integrity of this trip signal can be maintained during communication.

Three experiments are conducted to validate the QDTWP framework: Section IV-A presents QKD-based eavesdropping detection results; Section IV-B describes HMAC^Q verification performance under an MITM attack; and Section IV-C evaluates the system-level stability of a modified NPCC test system by comparing the protection response with and without the QDTWP scheme under fault conditions.

A. QKD-based Eavesdropping Detection

This test verifies that any attempt to obtain the Q-key used for HMAC^Q is promptly exposed by the QKD channel, demonstrating that the QDTWP framework can reliably detect key-extraction attacks.

Fig. 3 shows the behavior of the QKD channel under normal and eavesdropping conditions. The observations are summarized below:

- Under normal conditions, both QBER and visibility remain stable, typically below 5% for QBER and a high visibility above 95%. In this state, the quantum signals arrive with consistent polarization, allowing Alice and Bob to generate matching keys.
- When an eavesdropper is introduced, the QBER increases sharply from below 5% to more than 20% in a short interval. At the same time, visibility drops from around 96% to below 40%, reflecting the loss of quantum coherence and the polarization disturbance on the quantum channel. These deviations are indicative of an eavesdropping attempt.

This confims that real-time monitoring of QBER and visibility enables the QDTWP framework to detect eavesdropping early. As a result, compromised Q-key is never used for protection signaling, and only secure keys participate in HMAC^Q-based authentication.

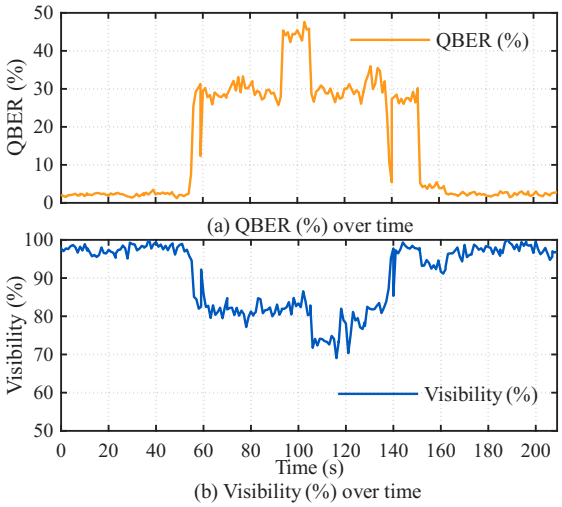


Fig. 3: QBER variation under normal and eavesdropping conditions

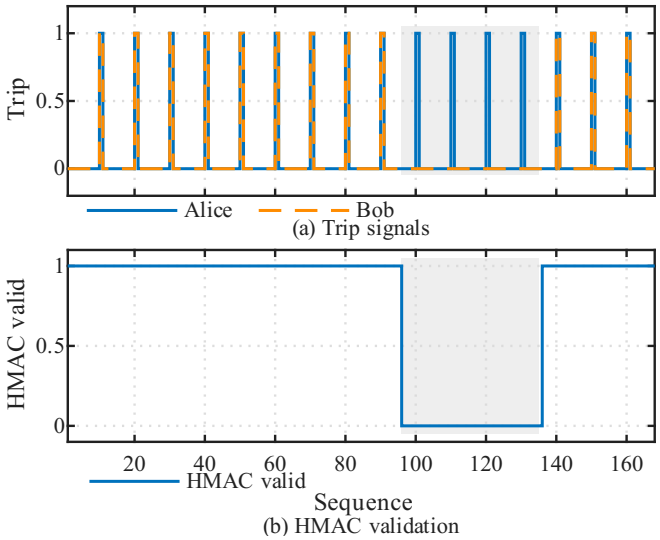


Fig. 4: Trip and HMAC validation under both normal and MITM attack conditions.

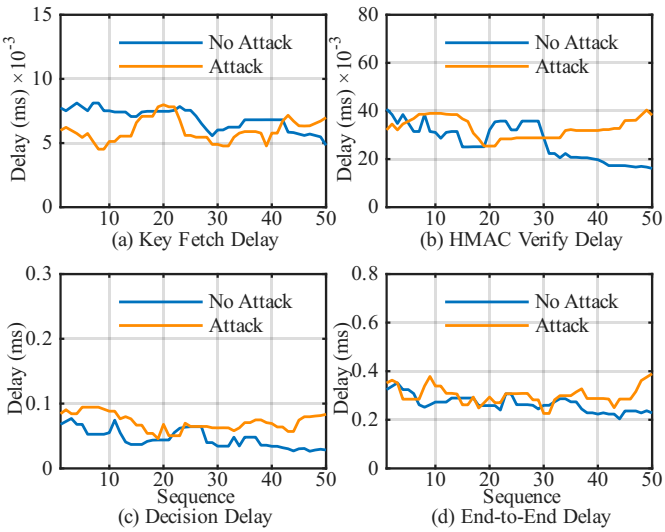


Fig. 5: Latency under normal and attack conditions

B. Message Integrity Validation

This test evaluates whether the implemented QDTWP framework can detect message tampering on the TRP signal. On the sender side, Alice transmits a trip signal which is encapsulated into a UDP frame together with an HMAC^Q tag computed using the current Q-key. On the receiver side, Bob verifies each incoming message by recalculating the HMAC^Q with his locally obtained Q-key and comparing it with the received tag.

Fig. 4 shows the system behavior under both normal and attack conditions. As the packet sequence increases, an MITM attack occurred at around the 95th packet and maintained for about 40 packets. In Fig. 4 (a), the UDP-based trip signals recorded at Alice and Bob remain identical during the normal operating operation, indicating successful synchronization and message authentication. Once the MITM attack is initiated, Bob's trip signal is modified to 0 while Alice continues transmitting the messages. During the attack period as shown in Fig. 4 (b), highlighted in gray, the HMAC^Q validity drops to 0, indicating that the tampered messages are successfully detected. And a post detection logic will decide whether to discard this tampered packet. Together, Fig. 4 confirm that the quantum-key-derived HMAC^Q ensures reliable authentication and resilience against MITM attacks.

Fig. 5 compares the latency components under normal and MITM attack conditions. The key fetch and HMAC verification delays remain in the microsecond range, showing that the security layer adds minimal computational overhead. A slight increase is observed in decision delay during attack due to the integrity verification process. Overall, the end-to-end delay stays within 0.25–0.4 ms, demonstrating that the QDTWP scheme maintains deterministic low-latency performance.

C. System Level Stability Validation

The protection architecture is validated on a modified NPCC system, which is a reduced model for the power grid of the northeastern United States and Canada. The single line diagram of the system is shown in Fig. 6. Each synchronous generator is modeled along with its speed governor, exciter and the associated automatic voltage regulator. Three aggregated IBRs, each rated at 0.3 GW (0.9 GW in total), are connected to the system to account for the effects of increasing inverter-based resources in modern power systems. The IBRs adopt a grid-following-based double loop control, and their locations can be found in Fig. 6.

The double-ended traveling-wave protection is deployed at both terminals of the 500 kV transmission line, as indicated by the blue box in Fig. 6. A single-phase short-circuit fault is applied within the TWR protection zone to evaluate the scheme. The fault is modeled as a 0.15s permanent fault, which reflects the real-world behavior of fault arcs that do not self-extinguish and must be cleared only when the circuit breakers isolate the faulted section.

Fig. 7 (a) shows that with the QDTWP method, the TRP message is successfully authenticated and executed, both re-

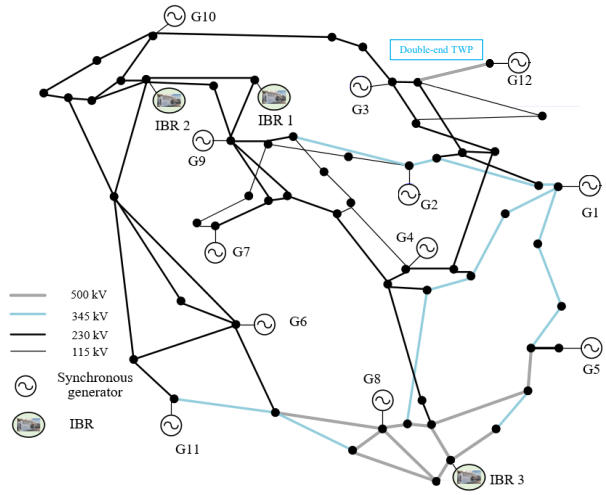
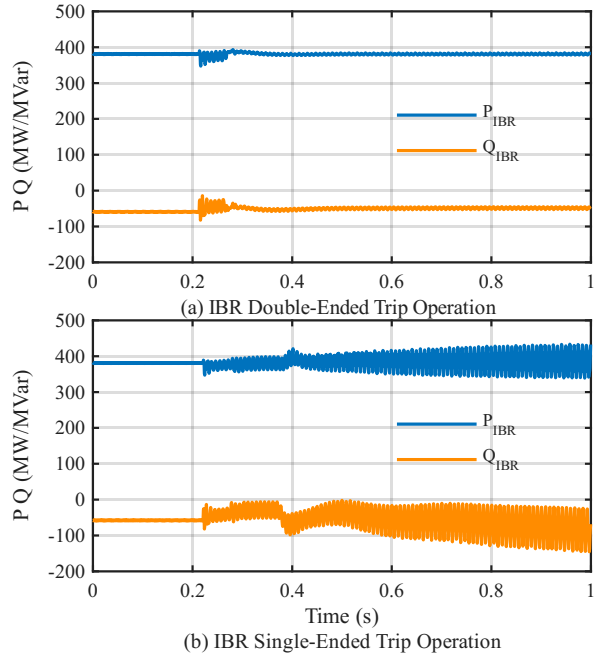


Fig. 6: Single line diagram of the IBR-integrated NPCC system



(a) IBR Double-Ended Trip Operation

(b) IBR Single-Ended Trip Operation

Fig. 7: NPCC test results.

lays trip simultaneously. The fault was quickly cleared, and the active and reactive power exhibit only a brief disturbance and then settle smoothly, indicating stable system behavior. In contrast, Fig. 7 (b) shows that without the QDTWP method, when an attacker block the TRP message so that only one terminal operates after the fault, the power signals experience sustained oscillations and eventually lead to collapse. These results demonstrate that coordinated tripping enabled by reliable TRP delivery is essential for maintaining system level stability.

V. Conclusion

This paper presents a QDTWP framework for securing TWR communication using HMAC^Q. The implemented method achieves low-latency deterministic protection performance and reliability over packet-switched networks. Simulation results verify that the HMAC^Q layer effectively detects message tampering, ensures the integrity of TRP signal transmissions, and maintains stable end-to-end delay under both normal and attack conditions. The results confirm that the scheme provides a practical and cost-effective solution for secure TWR communication without relying on dedicated optical links.

Future work will evaluate the QDTWP performance under practical grid communication conditions, including background traffic, transient disturbances, and realistic packet-loss patterns. The robustness of the scheme will also be examined under traffic surges caused by multi-line fault events, which impose significant stress on protection communication. Validation with commercial traveling-wave relays will further establish the applicability of the proposed framework to field-deployed protection systems.

References

[1] F. Wilches-Bernal, A. Bidram, M. J. Reno, J. Hernandez-Alvidrez, P. Barba, B. Reimer, R. Montoya, C. Carr, and O. Lavrova, "A survey of traveling wave protection schemes in electric power systems," *IEEE Access*, vol. 9, pp. 72949–72969, 2021.

[2] D. Etingov, P. Zhang, Z. Tang, and Y. Zhou, "AI-Enabled Traveling Wave Protection for Microgrids," *Electric Power Systems Research*, vol. 210, p. 108078, 2022.

[3] ENTSO-E, "Report on the iberian peninsula blackout of 28 april 2025," tech. rep., European Network of Transmission System Operators for Electricity, 2025.

[4] F. Deng, X. Li, and X. Zeng, "Single-ended travelling-wave protection algorithm based on full-waveform in the time and frequency domains," *IET Generation, Transmission & Distribution*, vol. 12, no. 15, pp. 3680–3691, 2018.

[5] ENTSO-E, "Use of Travelling Waves Principle in Protection Systems and Related Automations," tech. rep., ENTSO-E Technical Report, 2021.

[6] "IEEE Guide for Protective Relay Applications to Transmission Lines," *IEEE Std C37.113-2015 (Revision of IEEE Std C37.113-1999)*, pp. 1–141, 2016.

[7] P. Zhang, *Microgrids: Theory and Practice*. John Wiley & Sons, 2024.

[8] Y. Zhou, Z. Tang, N. Nikmehr, P. Babahajiani, F. Feng, T.-C. Wei, H. Zheng, and P. Zhang, "Quantum computing in power systems," *iEnergy*, vol. 1, no. 2, pp. 170–187, 2022.

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

[10] Z. Tang, P. Zhang, W. O. Krawec, and Z. Jiang, "Programmable quantum networked microgrids," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–13, 2020.

[11] L. Wang, P. Zhang, Z. Tang, and Y. Qin, "Programmable crypto-control for iot networks: An application in networked microgrids," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7601–7612, 2023.

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

[13] A. Soni, S. K. Sahay, and V. Soni, "Hash based message authentication code performance with different secure hash functions," in *2025 10th International Conference on Signal Processing and Communication (ICSC)*, pp. 104–109, 2025.

[14] Z. Tang, P. Zhang, W. O. Krawec, and L. Wang, "Quantum networks for resilient power grids: Theory and simulated evaluation," *IEEE Transactions on Power Systems*, vol. 38, no. 2, pp. 1189–1204, 2023.

[15] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, (Bangalore, India), pp. 175–179, 1984.

[16] Z. Tang, P. Zhang, and W. O. Krawec, "Enabling resilient quantum-secured microgrids through software-defined networking," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–11, 2022.