Quantum Full-Duplex Anonymous Communication in Adversarial Quantum Networks

Awais Khan, Syed Muhammad Abuzar Rizvi, Trung Q. Duong, *Fellow, IEEE*, Een-Kee Hong, *Senior Member, IEEE*, and Hyundong Shin, *Fellow, IEEE*

***Abstract*—Full-duplex communication is a transformative technology in next-generation networks, enabling simultaneous transmission and reception for both high efficiency and low latency. In this paper, we integrate *full duplexity* with quantum anonymous communication (QAC), developing a quantum dimension of full-duplex anonymity to address the stringent demands for communication efficiency, security, and privacy in emerging networks. Specifically, we design two full-duplex QAC (FD-QAC) protocols for the bidirectional, secure, and anonymous exchange of classical information with the help of a server. The first FD-QAC protocol, tailored for ring-type quantum networks, ensures that even an adversary with full network access cannot determine communicating identities—achieving *perfect untraceability*. The second FD-QAC protocol, designed for star-type quantum networks, improves scalability, security, and resilience against dishonest participant attacks. We provide the anonymity analysis demonstrating the robustness of these QAC protocols against external adversaries and malicious participants in adversarial quantum networks. Furthermore, we evaluate the error performance of the protocols in noisy quantum networks, illustrating that this quantum full-duplex anonymity is both reliable and scalable.**

***Index Terms*—Anonymity, full duplexity, quantum anonymous communication, quantum networks.**

I. Introduction

QUANTUM technology is driving the development of the quantum Internet, a network of interconnected quantum processors and sensors designed to achieve unprecedented levels of security, computational power, and sensing accuracy—surpassing the capabilities of classical systems [1]–[6]. This transformative leap is fueled by rapid advancements in quantum information science, which have significantly enhanced security across communication, sensing, and computation domains [7]–[10]. Core protocols such as quantum key distribution (QKD) [11]–[14], quantum secure direct communication [15]–[18], secure quantum metrology [19], [20], blind quantum computation [21]–[24], quantum secret sharing [25]–[27], and distributed secure quantum computation [28], [29] are key to establishing secure quantum networks. While these protocols primarily address message confidentiality—ensuring that only authorized parties can decrypt information—network security extends beyond content protection. Equally important is protecting the identities of communicating parties to preserve privacy. This concealment, known as anonymity, must be guaranteed without relying on any assumptions about adversary computational power [30].

Quantum mechanics provides a foundation for the concept of quantum anonymity through non-classical phenomena such as entanglement and the no-cloning theorem [31]–[33]. By leveraging quantum mechanics principles, quantum anonymity effectively obfuscates the identities of senders and receivers, ensuring that even adversaries with unlimited computational power cannot trace messages to their origin [34]. This property is critical across various domains, including communication, sensing, and computation, where it plays a pivotal role in ensuring data security, enhancing privacy, and preventing unauthorized information tracking in adversarial networks [35]–[38]. Consequently, several prominent applications have emerged, including quantum anonymous teleportation (QAT) [39]–[45], quantum anonymous entanglement (QAE) [46]–[51], quantum anonymous voting (QAV) [52]–[55], quantum anonymous notification (QANO) [56], [57], quantum anonymous conference key agreement (QA-CKA or quantum anonymous CKA) [58]–[60], quantum anonymous collision detection (QACD) [61], [62], quantum anonymous ranking (QAR) [63]–[65], quantum anonymous broadcast (QAB) [38], quantum anonymous group communication (QAGC) [66], quantum anonymous secret sharing (QASS) [67], quantum anonymous information retrieval (QAIR) [68], [69], quantum anonymous sensing (QAS) [37], quantum anonymous identity authentication (QAIA) [70], and quantum anonymous publication (QAP) [71], each capitalizing on inherent anonymity provided by quantum anonymous networks (QANs) [34], [35].

Despite these advancements, most existing quantum anonymous communication (QAC) frameworks operate in a simplex mode, where information flows unidirectionally from sender to receiver. However, emerging communication systems demand efficient, reliable, and interactive exchanges, underscoring the need to transition toward a full-duplex (FD) communication model. While quantum protocols such as quantum dialogue enable bidirectional communication between two parties, the identities of the communicating users are typically known in these protocols [72], [73]. Yet, the concept of *full-duplex*

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (RS-2025-00556064 and RS-2025-25442355), by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2025-RS-2021-II212046) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation), and by the Canada Excellence Research Chair (CERC) Program CERC-2022-00109. *(Corresponding author: Hyundong Shin.)*

A. Khan, S. M. A. Rizvi, E.-K. Hong, and H. Shin are with the Department of Electronics and Information Convergence Engineering, Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Republic of Korea (e-mail: hshin@khu.ac.kr).

T. Q. Duong is with the Faculty of Engineering and Applied Science, Memorial University, St. John's, NL A1C 5S7, Canada, and also with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, Belfast, UK (e-mail: tduong@mun.ca).

TABLE I
EXPANSIONS OF IMPORTANT ACRONYMS

Acronym	Expansion	Acronym	Expansion
CNOT	Controlled-NOT	DEP	Duplex Error Probability
EPR	Einstein–Podolsky–Rosen	FD	Full-Duplex
FD-QAC	Full-Duplex Quantum Anonymous Communication	GHZ	Greenberger–Horne–Zeilinger
LOCC	Local Operations and Classical Communication	MDI	Measurement-device-independent
QAB	Quantum Anonymous Broadcast	QAC	Quantum Anonymous Communication
QACD	Quantum Anonymous Collision Detection	QAE	Quantum Anonymous Entanglement
QAGC	Quantum Anonymous Group Communication	QAIA	Quantum Anonymous Identity Authentication
QAIR	Quantum Anonymous Information Retrieval	QAN	Quantum Anonymous Network
QANO	Quantum Anonymous Notification	QAP	Quantum Anonymous Publication
QAR	Quantum Anonymous Ranking	QAS	Quantum Anonymous Sensing
QASS	Quantum Anonymous Secret Sharing	QAT	Quantum Anonymous Teleportation
QAV	Quantum Anonymous Voting	QA-CKA	Quantum Anonymous Conference Key Agreement
QFDA	Quantum Full-Duplex Anonymity	QKD	Quantum Key Distribution

anonymity in quantum networks remains largely unexplored. The motivation behind this work is to address this gap by designing quantum protocols that enable simultaneous, anonymous, and resource-efficient message transmission in adversarial network environments. In this paper, we design two full-duplex QAC (FD-QAC) protocols for adversarial quantum networks, addressing semi-honest and dishonest participant scenarios. These protocols integrate local operations and classical communication (LOCC) to facilitate secure, untraceable, and bidirectional information transmission. By introducing FD anonymity functionality, we put forth the FD-QAC framework beyond existing simplex models, providing both duplexity and anonymity. The main contributions of this work can be outlined as follows.

- *Full-Duplex Anonymity:* We propose two FD-QAC protocols that allow communicating parties to exchange classical messages anonymously, securely, and simultaneously across two types of quantum networks—one designed for semi-honest participants and the other for dishonest participants. These protocols ensure *untraceability*, meaning that even with full access to network resources, an adversary cannot trace messages back to their original sources. The protocols initially utilize quantum entanglement as a resource to encode classical messages with LOCC for anonymous duplex communication. Then, communicating parties use quantum measurement outcomes to decode duplex messages.
- *Security, Anonymity, and Noise Analysis:* The anonymity analysis of FD-QAC protocols demonstrates their robustness against both external and internal adversarial attacks, preserving the privacy of communicating parties such that their identities remain concealed under a variety of threat models. Furthermore, we evaluate the error performance of the protocols in noisy quantum networks, specifically deriving the duplex error probability (DEP) under depolarizing, bit-flip, and phase-flip noise conditions.

The remainder of the paper is organized as follows. Section II provides the fundamental trustworthiness notions and reviews related works on QAC protocols, outlining their key features and limitations. Section III introduces network models and system properties. Sections IV and V present the FD-QAC protocols for bidirectional classical message transmission and analyze their untraceability, respectively. Section VI discusses the DEP performance of the designed FD-QAC protocols in noisy quantum scenarios. Finally, Section VII concludes the paper. Table I presents key acronyms used in this work.

II. TRUSTWORTHINESS AND RELATED WORK

This section first presents the foundational concepts of security, privacy, and anonymity, which are essential for ensuring trust and protection in emerging networks (see Fig. 1). We then provide a brief overview of prior work on quantum anonymity protocols, outlining their main contributions and limitations.

A. Trustworthiness Notions

1) Security, Privacy, and Anonymity: In communication networks, security refers to the protection of information and system resources from unauthorized access, modification, or disruption. A system is considered *secure* if it preserves confidentiality, integrity, and availability of information, thereby preventing unauthorized access, interception, or manipulation under defined threat conditions. Privacy protects personal or sensitive data such that it remains confidential and is controlled by the legitimate owner. Formally, a system preserves *privacy* when it ensures that users are free from unwanted observation or interference by unauthorized parties and have authority over what information they disclose, and to whom. Anonymity enables users to communicate or interact without disclosing their identities, thereby strengthening privacy and mitigating risks associated with targeted identification. A system preserves *anonymity* when an individual cannot be distinguished within a defined set of users, known as the anonymity set, such that the probability of linking a specific action to a given user remains uniform across all members of the set.

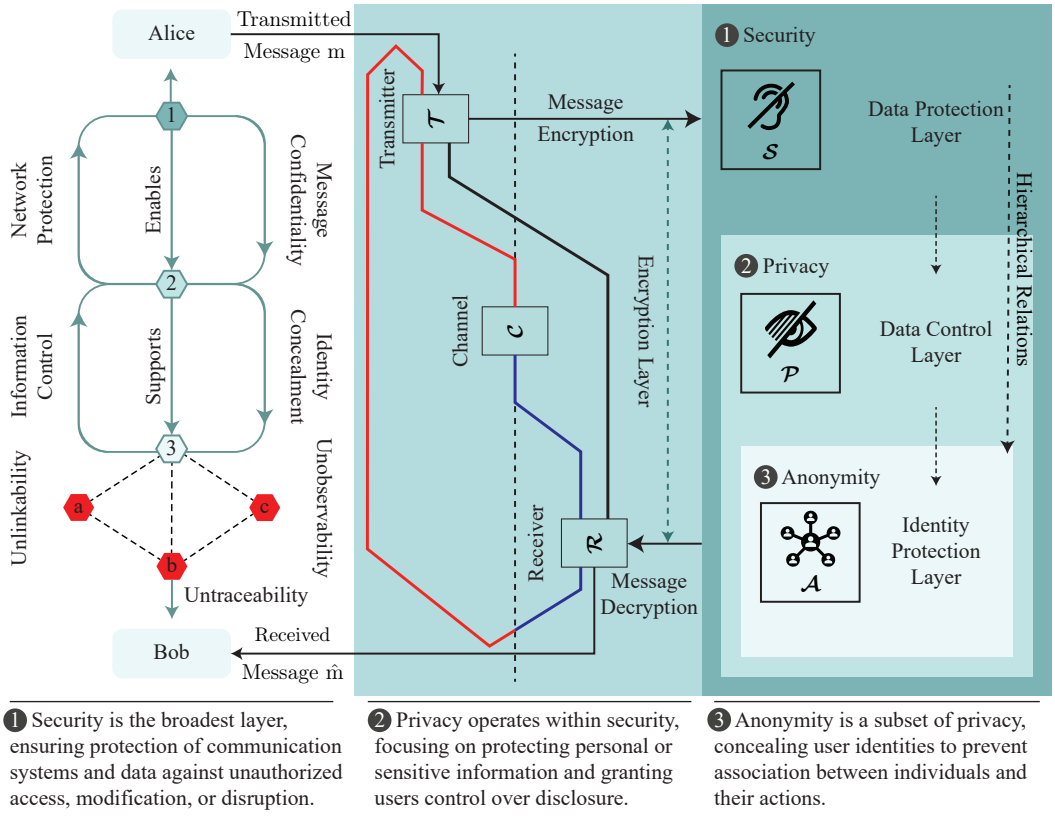


Fig. 1. Trustworthiness notions, properties, and their relations.

2) Untraceability, Unlinkability, and Unobservability: Untraceability prevents an adversary from determining the origin or destination of a message or action. This property ensures that neither the sender nor the receiver can be uniquely identified from observable communication events, even if those events are intercepted or analyzed. A system preserves *untraceability* if, for any given communication or action, the probability of linking it to a specific source or destination remains unchanged before and after observation by an adversary. Formally, untraceability guarantees that an observer cannot infer the mapping between a message and its true sender or recipient beyond random chance. The unlinkability property ensures that multiple communications, transactions, or actions initiated by the same entity cannot be associated or correlated by an adversary. This property prevents observers from deducing relationships between distinct communication events. Formally, a system preserves *unlinkability* if, for any two or more observable items (e.g., messages, sessions, or actions), the probability that they originate from the same user remains invariant before and after adversarial observation or analysis. The unobservability property hides not only the content but also the existence of a communication or action. This property ensures that an adversary cannot distinguish whether communication is taking place at all. Formally, a system preserves *unobservability* if, from an adversary's viewpoint, the occurrence of a specific communication event is statistically indistinguishable from other communication events of the same type, even after observing network traffic or system behavior.

B. Trustworthiness Relations

1) Notion Relations: Security and privacy are interdependent concepts sharing the common objective of data protection. While security emphasizes defense against external threats and unauthorized interference, privacy focuses on selective information disclosure and user control. Anonymity complements security by concealing user identities, thereby reducing exposure to personalized attacks. Privacy is the broader concept encompassing control over personal information, whereas anonymity represents a specific mechanism that conceals identity to achieve privacy. Thus, anonymity operates as a subset of privacy, ensuring that communications cannot be attributed to specific individuals. Anonymity serves as a means to achieve privacy and enhance overall network security, particularly in environments requiring identity protection and confidentiality. A system may provide security without anonymity, but anonymity inherently strengthens both privacy and resilience against tracking or profiling.

2) Property Relations: Untraceability supports anonymity by concealing the source and destination of actions or messages. It prevents adversaries from linking a communication to its initiator, thereby protecting identity within the anonymity set. Unlinkability contributes to both privacy and anonymity by preventing external parties from correlating multiple communications belonging to the same participant. If individual events are unlinkable, tracing behavioral patterns or identifying users becomes infeasible. Unobservability represents the strongest privacy notion. It ensures that communications are

indistinguishable from background activity, thereby implying both untraceability and unlinkability. In highly adversarial environments, unobservability provides complete stealth—concealing both the existence and the source of actions.

C. Fundamental Primitives of QAC protocols

The evolution of the two fundamental primitives of QAC protocols (i.e., QAT and QAE) spans several distinct phases, ranging from foundational anonymity models to adversarially robust and lightweight constructions, and more recently to noise-tolerant and topology-adaptive designs, as summarized in Table II.

1) Foundational Protocols: The concept of anonymity in quantum networks was first established through the QAT protocol introduced in [39], which enables quantum message transmission while concealing the identities of both sender and receiver. The protocol consists of two fundamental subprotocols: i) QAB, which provides anonymous dissemination of classical information, ensuring that the broadcaster's identity remains hidden; and ii) QAE, which generates anonymous entanglement between communicating parties without revealing their identities. By combining QAB and QAE, the protocol supports teleportation-native quantum communication while maintaining identity concealment. This work also introduced the untraceability principle, assuming a perfectly shared Greenberger–Horne–Zeilinger (GHZ) state among all participants. However, this reliance on ideal multipartite GHZ entanglement significantly limits the practicality and scalability of the protocol in realistic quantum networks.

2) Verifiable and Disruption-Resistant Protocols: To overcome the assumptions of foundational QAT [39], subsequent protocols incorporated entanglement-verification procedures, disruption-detection mechanisms, fully symmetric, and denial-of-service-resistant communication [40], [41], [46]. The original protocol was extended in [46] by integrating GHZ-state verification into the QAE subprotocol, enabling participants to detect deviations from the expected entanglement correlations and thereby ensuring QAE correctness. This refinement enabled probabilistic detection of dishonest or malfunctioning participants and preserved message integrity under limited adversarial interference. The protocol achieved one-sided anonymity, allowing either the sender or the receiver to remain anonymous, and offered disruption tolerance characterized by the quantum Gilbert–Varshamov bound. However, its implementation remained complex, required an anonymous classical channel, and assumed a restricted adversarial setting, tolerating only a small fraction of dishonest participants. Building on this variant, the fail-safe teleportation mechanism was introduced in [40], allowing recovery of the transmitted quantum message in the event of disruption or transmission failure. This protocol achieves full (sender and receiver) anonymity and tolerates corrupted participants. However, it remains vulnerable to forced abortion by a single malicious node, incurs high quantum resource overhead, and requires pairwise private quantum channels.

The most substantial advancement in QAT and QAE work was presented in [41], which incorporated trap-based entanglement verification and formalized the detection of malicious disruption under active adversarial models. By employing mediator-assisted coordination that enables anonymous entanglement generation without revealing identity information, this approach significantly improves resilience against denial-of-service (DoS) and collusion-based attacks. Even with these improvements, these protocols remain highly resource-intensive, lack noise modeling, and still continue to rely on high-fidelity multipartite entanglement.

3) Noise-Aware and Practical Protocols: While early refinements in QAT primarily focused on maintaining correctness under idealized or weakly adversarial settings, subsequent research has shifted toward practical, noise-tolerant, and actively secure constructions of QAE. The protocol in [47] addressed a central limitation of earlier schemes by replacing the assumption of a perfectly shared GHZ state with approximate GHZ-state verification. By introducing a statistical test that tolerates photon loss and experimental imperfections, the protocol ensures approximate anonymity and correctness even when the underlying entanglement source is noisy. However, its security guarantees are limited by fidelity thresholds of the verification test, which degrade as the network size increases. Building on this foundation, the correctness analysis for such practical QAE protocols has been revisited in [48], uncovering subtle vulnerabilities in anonymity preservation arising from mode-selection inconsistencies and adversarial manipulation of measurement choices. To overcome these issues, the refined verification model has been introduced to incorporate explicit measurement-mode selection and stricter consistency checks, thereby strengthening correctness against active adversaries and reducing the likelihood of undetected disruption. Nevertheless, this improvement increases communication overhead and amplifies the verification cost for large networks.

The QAE design has been further extended in [50] to noisy-measurement regimes for practicality, where detectors may behave imperfectly or adversarially. By incorporating randomized measurement verification and noise-aware consistency testing, the protocol collectively guarantees both anonymity and correctness even when measurement devices are unreliable. Although this approach significantly improves robustness under realistic experimental conditions, it requires repeated verification rounds, resulting in higher resource consumption. Together, these works mark a transition from idealized theoretical constructions to QAE protocols explicitly designed for practical quantum networks operating under loss, noise, and active adversarial interference.

4) Lightweight Single-Particle Protocols: Beyond GHZ-based constructions, lightweight approaches have been explored for QAE generation without relying on multipartite entangled states. The efficient framework for QAT and QAE has been introduced in [42], which eliminates the need for pre-distributed GHZ entanglement by relying solely on single-particle transmissions and two controlled-NOT (CNOT) operations, enabling anonymous communication in circular quantum networks. Compared with GHZ-based schemes, this approach significantly reduces both quantum resource requirements and physical implementation complexity. The protocol incorporates collision detection, notification, and anonymous broadcast subroutines and proves full anonymity for both

TABLE II
FUNDAMENTAL QAC PRIMITIVES: QAT AND QAE PROTOCOLS

Protocol	Main Contribution	Key Advantage	Adversarial Model	Message Mode	Limitation	Ref.
QAT	Introduced QAT; proposed QAB and QAE subprotocols for QAT	First QAC framework; established untraceability (quantum-unique property)	Passive attacks (semi-honest)	Quantum (simplex)	Requires perfect GHZ; lack of noise modeling or adversarial setting	[39]
	Improved QAT by introducing fail-safe teleportation; full anonymity (sender–receiver)	Tolerates any number of corrupt participants; perfect anonymity and message privacy	Active attacks (dishonest)	Quantum (simplex)	Forced abort; high resource cost; requires pairwise private quantum channels	[40]
	Extended QAT protocols; proposed mediator-assisted QAE by utilizing entanglement swapping and verification	Provides full anonymity without trusted third parties; resistant to DoS attacks	Active attacks (dishonest)	Quantum (simplex)	High communication and quantum resource cost; assumes ideal channels; lack of noise modeling	[41]
	Resource-efficient QAT by establishing QAE with single photons, two CNOT operations, and no preshared GHZ states	Maintains full anonymity; reduces entanglement cost, implementation complexity	Active attacks (dishonest)	Quantum (simplex)	Vulnerable to abortion by malicious participants; no protection against active tampering or DoS	[42]
	Proposed one-sided QAT; established QAE with single particles and CNOT operations, and no preshared GHZ states	Achieves sender anonymity and message privacy; reduced quantum resources cost	Active attacks (dishonest)	Quantum (simplex)	Vulnerable to abortion by the malicious receiver; no protection against DoS	[43]
	Proposed QAT via entanglement relay; established QAE from EPR pairs instead of GHZ states	Maintains full anonymity and message privacy; improves efficiency and robustness	Active attacks (dishonest)	Quantum (simplex)	Lack of noise modeling; aborts under repeated adversarial disruption	[44]
	Proposed counterfactual QAT; established QAE via the quantum Zeno effect and Mach–Zehnder interferometers	Achieves full anonymity and message privacy without transmitting physical particles; immune to Trojan-horse attacks	Active attacks (dishonest)	Quantum (simplex)	Complex experimental realization; decreased efficiency with network size	[45]
QAE	Enhanced QAE by adding entanglement verification and disruption detection mechanisms	Provides one-sided anonymity with disrupter tolerance under the Gilbert–Varshamov bound	Active attacks (dishonest)	Quantum	Complex implementation; requires classical anonymous channels	[46]
	Proposed QAE with practical GHZ verification for lossy and noisy quantum networks	Achieves anonymity under realistic networks; operates without perfect GHZ states	Active attacks (dishonest)	Quantum	Pairwise private classical channels and authenticated quantum links	[47]
	Improved QAE correctness by introducing revised measurement and mode-selection steps	Rigorous correctness model; resistant to DoS attacks under active scenarios	Active attacks (dishonest)	Quantum	Verification overhead; decreased efficiency with network size	[48]
	Proposed QAE using W-state entanglement for noisy quantum networks	Provides noise tolerance and robustness against particle loss; maintains full anonymity for noisy quantum networks	Passive attacks (semi-honest)	Quantum	Vulnerable to abortion or disruption by malicious nodes; unsecure in fully active adversarial model	[49]
	Extended the practical QAE [49] by introducing noisy-measurement model and randomized verification	Correctness, anonymity, and robustness under realistic noisy measurements	Active attacks (dishonest)	Quantum	High resource cost for repeated verification; decreased efficiency with detector noise	[50]
	Proposed MDI QAE utilizing untrusted ancillary nodes	Full anonymity even with untrusted measurement devices; practical deployment	Active attacks (dishonest)	Quantum	Degradation under channel loss and detector inefficiency	[51]

sender and receiver, as well as privacy of the transmitted quantum message even when an active adversary controls an arbitrary number of corrupt participants—provided that the receiver remains honest. However, the protocol is vulnerable to forced abortion or disruption if any participant behaves as an active adversary. In a related direction, the one-sided QAT protocol was proposed in [43], which supports anonymous quantum message transmission from a hidden sender to a publicly known receiver. This protocol has further optimized resource usage by constructing QAE from single-qubit states in a public-receiver setting. While this approach provides anonymity and message privacy for the sender, it similarly lacks robustness against active adversaries, as a malicious receiver can force protocol abortion or disrupt communication. Consequently, although these lightweight single-particle protocols improve feasibility, their applicability remains limited to weakly adversarial quantum network environments.

5) Topology-Driven and Noise-Resilient Protocols: In addition, scalable and robust QAT designs have been proposed by introducing alternative mechanisms and quantum resources for QAE generation that improve scalability and operational

robustness in practical network settings. The entanglement-relay–assisted QAT framework was presented in [44], where QAE is established through the sequential forwarding of Einstein–Podolsky–Rosen (EPR) pairs rather than relying on a globally shared GHZ state. This approach eliminates the need for multipartite entanglement distribution, allowing the protocol to scale effectively across large-scale or dynamically structured networks while preserving full anonymity of both sender and receiver under active adversarial conditions. However, the protocol does not explicitly model noise, and its performance under realistic channel loss or measurement imperfections remains uncharacterized. In contrast, the noise-tolerant QAE construction based on the W-state entanglement was introduced in [49], exploiting its intrinsic robustness to qubit loss and amplitude-damping noise. This design enables anonymous quantum message transmission even when individual qubits are corrupted or lost during distribution, thereby ensuring full anonymity in noisy quantum networks. However, the adversarial model in [49] is limited to semi-honest participants, leaving the protocol susceptible to disruption and other active attacks in fully adversarial environments.

6) Device-Independent and Counterfactual Protocols: Further advances in practical quantum anonymity have focused on mitigating device imperfections and relaxing trust assumptions in networked measurement settings. The measurement-device-independent (MDI) QAE protocol introduced in [51] employs an untrusted ancillary node to perform multipartite GHZ-state measurements while preserving anonymity for both the sender and the receiver. By decoupling security from detector reliability, the protocol mitigates vulnerabilities arising from detector side-channel attacks and enables practical deployment in networks with heterogeneous or imperfect measurement devices. Although the design ensures correctness and anonymity under active adversaries, its performance is sensitive to channel noise and loss, which degrade the fidelity and success probability of anonymous entanglement generation in large-scale implementations.

In a complementary direction, the counterfactual QAT and QAE designs—based on the quantum Zeno effect and the nested Mach–Zehnder interferometers—have been proposed in [45], enabling anonymous entanglement establishment without transmitting information-carrying particles through the communication channel. This counterfactual property enhances security against man-in-the-middle and Trojan-horse attacks while preserving full anonymity and message privacy. The protocol's robustness has been further analyzed under various channel-noise models. However, the protocol imposes substantial experimental complexity, and its efficiency deteriorates as the number of interferometric cycles and channel noise increase, limiting its practical realizability in near-term quantum networks.

7) Direct Anonymous Classical Communication: Despite substantial progress in quantum anonymity, most existing QAC protocols are fundamentally designed for QAE generation and the anonymous transmission of *quantum* messages. In contrast, the problem of directly transmitting *classical* information anonymously over quantum networks remains comparatively underdeveloped, even though classical messages constitute the primary payload in most practical communication tasks. Current QAC frameworks overwhelmingly treat classical information only as an auxiliary component for establishing QAE, rather than as a primary communication payload. While the QA-CKA protocol extends QAC to multiparty settings by first generating conference keys from QAE and subsequently using them to transmit classical information, it still relies on QAE as an initial resource. In contrast, direct anonymous classical communication eliminates this dependency, enabling anonymous delivery of classical messages without prior QAE. Although recent QAC protocols for direct classical message transmission have been proposed for various quantum network topologies, including ring-type, linear, and tree- or graph-mixed networks, they commonly assume that all participants are *semi-honest* (i.e., honest but curious) [74]. However, in realistic adversarial network scenarios, participants may behave dishonestly and launch active attacks that compromise anonymity. Hence, the QAN protocols devised under the semi-honest model are generally impractical for deployment [63]. Moreover, all these previously designed QAC protocols for the QAN tasks—such as QAE, QAT, QAB, QAV, QAR, QANO, QACD, QA-CKA, QAIR, QAGC, QAIA, QAS, and QAP—operate in a *simplex* mode, where information flows in only one direction—from sender to receiver. This simplex operation increases communication overhead, introduces latency, and exposes vulnerability to adversarial attacks, as bidirectional exchange requires multiple independent transmissions. These challenges collectively motivate the design of FD-QAC protocols that support simultaneous bidirectional communication while preserving anonymity, integrity, and robustness under active adversarial conditions. Fig. 2 illustrates the evolutionary timeline of QAC protocols.

III. Models and Properties

In this section, we outline the preliminaries and network models, followed by a discussion of the fundamental properties essential in developing QAC protocols for quantum full-duplex anonymity (QFDA).

A. Quantum Preliminaries

We begin by establishing the mathematical framework of quantum states and extend it to duplex information carrier states, specifically entangled states. The successful realization of FD-QAC depends on the modulation of classical information onto entangled states and its subsequent demodulation to retrieve anonymous messages. Therefore, this subsection also explores the unitary operations that facilitate this process.

1) Quantum States: A quantum bit (qubit) is the fundamental unit of quantum information, defined in a two-dimensional Hilbert space [75], [76]. A qubit can be expressed as a linear combination of the computational basis states:

$$|\psi\rangle = \sum_{j\in\mathbb{Z}_2} \alpha_j |j\rangle \tag{1}$$

where $|j\rangle$, $j \in \mathbb{Z}_2 = \{0, 1\}$, form the computational basis and the complex amplitudes α_j satisfy the normalization condition $\sum_{j\in\mathbb{Z}_2} |\alpha_j|^2 = 1$. In addition, quantum states can also be

Fig. 2. A timeline illustrating the evolution of QAC protocols. Herein, DACC stands for direct anonymous classical communication.

measured in the Hadamard basis. The Hadamard operator $\boldsymbol{H}$ is defined on the computational basis states as follows:

$$\boldsymbol{H} : |j\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{k\in\mathbb{Z}_2} (-1)^{jk} |k\rangle . \tag{2}$$

This transformation provides the Hadamard (or diagonal) basis states:

$$|+\rangle = \boldsymbol{H}|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \tag{3}$$

$$|-\rangle = \boldsymbol{H}|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) . \tag{4}$$

2) Quantum Entanglement: In quantum mechanics, a composite system is considered entangled when its state cannot be expressed as the tensor product of its individual subsystems. This phenomenon serves as a vital resource in quantum information processing and plays a crucial role in key protocols such as quantum teleportation and superdense coding [77], [78]. One of the most widely used examples of a maximally entangled bipartite state is the Bell state $|\mathsf{bell}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ [79]. For N-partite systems, the GHZ state provides a prominent example of genuine entanglement among N qubits as follows [80]:

$$|\mathsf{ghz}\rangle = \frac{1}{\sqrt{2}} \sum_{j\in\mathbb{Z}_2} |j\rangle^{\otimes N} \tag{5}$$

where $\otimes$ is the tensor product. Both Bell and GHZ states serve as indispensable resources in quantum information processing, particularly in QAC.

3) Bit/Phase-Flip Operations: In quantum communication, a quantum system undergoes unitary operations to encode and manipulate quantum information while preserving the coherence of quantum states. In particular, the QAC protocols require the following two essential Pauli operations.

- The Pauli-x (bit-flip) operator flips the bit of the computational basis states and is given by:

$$\boldsymbol{X} = \sum_{j\in\mathbb{Z}_2} |j\oplus 1\rangle\langle j| : |j\rangle \mapsto |j\oplus 1\rangle \tag{6}$$

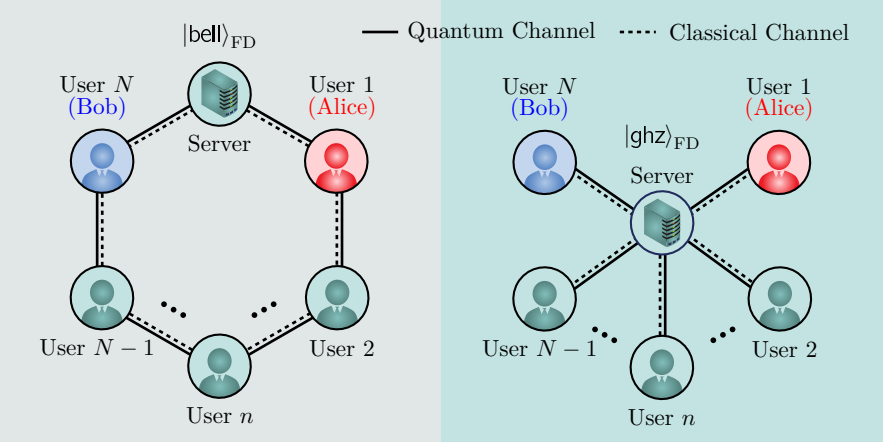


Fig. 3. A FD-QAC network architecture incorporating ring-type and star-shaped topologies. The network consists of N users and a server. The anonymity layer in the full-duplex configuration ensures a secure, anonymous, and simultaneous exchange of classical information between communicating parties (e.g., Alice and Bob). For simplicity, we set the server, Alice, and Bob as the zeroth, first, and Nth parties of the network, respectively.

where $\oplus$ denotes binary addition.

- The Pauli-z (phase-flip) operator shifts the phase of the computational basis states and is defined as:

$$\boldsymbol{Z} = \sum_{j \in \mathbb{Z}_2} (-1)^j |j\rangle\langle j| : |j\rangle \mapsto (-1)^j |j\rangle . \tag{7}$$

Note that the Hadamard operator $\boldsymbol{H}$ conjugates these two Pauli operators as follows: $\boldsymbol{HXH} = \boldsymbol{Z}$ and $\boldsymbol{HZH} = \boldsymbol{X}$. Furthermore, we can express the Hadamard action in the Pauli algebra as $\boldsymbol{H} = (\boldsymbol{X} + \boldsymbol{Z})/\sqrt{2}$.

B. Network Models

The network consists of $N+1$ participants, including two anonymous communicating parties (say, Alice and Bob) and a server (say, Charlie), as illustrated in Fig. 3. Alice and Bob wish to exchange classical messages anonymously and simultaneously. For simplicity, we denote the server, Alice, and Bob as the zeroth, first, and Nth parties in the network, respectively. All network participants are assumed to be capable of performing LOCC. In this work, we consider two network models: a ring-type quantum network for semi-honest users and a star-shaped quantum network for dishonest users.

- *Ring-Type Networks:* The network users and the server are connected in a circular configuration via quantum and classical channels, such that each participant communicates directly only with their immediate neighbors, as depicted in Fig. 3. The server is responsible for distributing Bell states and coordinating the communication process. All participants, including the server, are assumed to be semi-honest in this model.
- *Star-Shaped Networks:* All network users are connected to the server through quantum channels and classically authenticated channels, forming a star-shaped topology (see Fig. 3). The server enables quantum communication by distributing an $(N+1)$-partite GHZ state. The distribution and verification for this state follow the approach proposed in [63]. All participants, except for the server, are considered dishonest, making this model more aligned with practical adversarial scenarios.

C. Key Properties

Now, we formally define key features of FD-QAC protocols, assuming that quantum resources are shared correctly.

- *Correctness:* Both anonymous parties should be able to simultaneously exchange their messages with certainty, ensuring accurate transmission.
- *Anonymity:* The identities of communicating parties remain hidden, regardless of the content or outcome of their exchanged messages.
- *Untraceability:* Even with full adversarial access to all the network resources—including encoded quantum states and classical communication messages—the communicating identities remain completely concealed.
- *Security:* The communicating parties can exchange their messages securely, ensuring protection against adversarial attacks from both internal and external entities.

IV. FD-QAC for Classical Information

In this section, we present the design and operational steps of FD-QAC protocols for ring-type networks with semi-honest users and star-shaped networks with dishonest users. Both protocols enable any two network parties to simultaneously and anonymously exchange classical messages while maintaining key QFDA features. To avoid transmission collisions among N users, the QACD protocol is executed prior to the FD-QAC communication phase. In this step, users anonymously indicate whether they intend to transmit in the current round. The QACD protocol determines the number of participating users without revealing their identities [61], [62]. The FD-QAC protocol proceeds only when exactly two participating users are detected by the QACD protocol. Otherwise, the FD-QAC phase is not initiated, and the QACD procedure is repeated until exactly two users are detected. This mechanism ensures collision-free channel access while preserving the anonymity of communicating parties.

A. Protocol 1: QFDA for Ring-Type Networks

We propose a FD-QAC protocol for classical information exchange in ring-type quantum networks, under the assump-

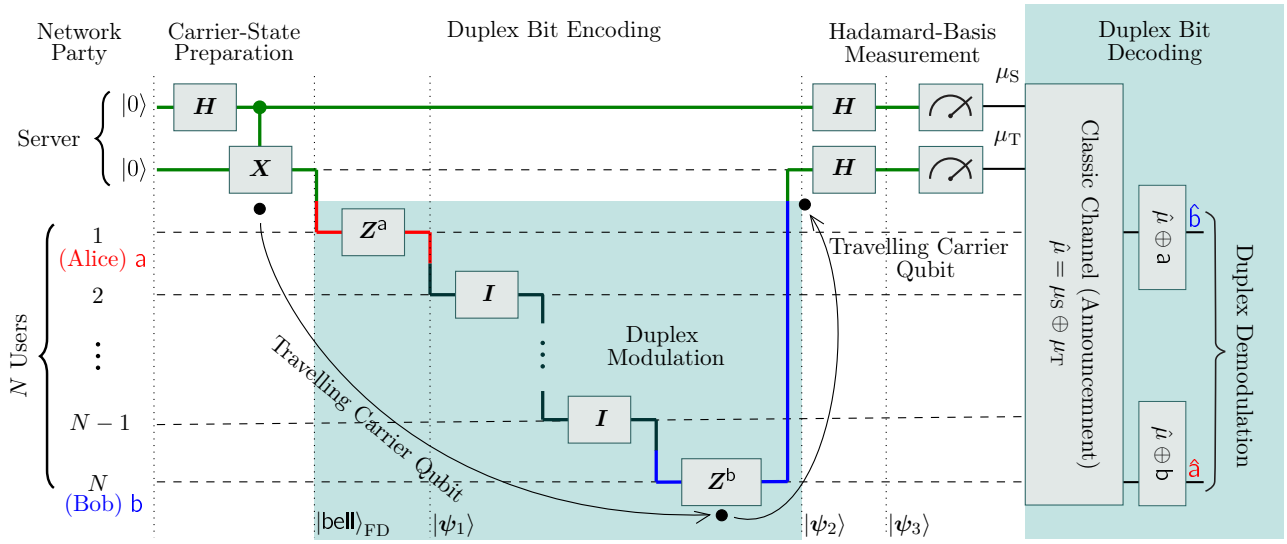


Fig. 4. A FD-QAC protocol in a ring-type topology for classical information (Protocol 1). The protocol involves Bell-state preparation, duplex encoding (phase-flip operations), Hadamard-basis measurements, classical announcements, and duplex decoding (binary additions).

tion that all network participants are semi-honest—i.e., they follow the protocol but may attempt to infer additional information. This protocol enables any two users (e.g., Alice and Bob) to simultaneously and anonymously exchange classical messages $\mathsf{a}, \mathsf{b} \in \mathbb{Z}_2$. Alice encodes her message bit a, and Bob encodes his message bit b, by applying the corresponding phase-flip operators $\boldsymbol{Z}^{\mathsf{a}}$ and $\boldsymbol{Z}^{\mathsf{b}}$ to their information-carrier states, respectively. Specifically, the QFDA protocol takes a series of the following steps under the semi-honest model, as illustrated in Fig. 4.

1) Carrier-State Preparation: The server (Charlie) prepares the Bell pair—called the *QFDA* carrier:

$$|\mathsf{bell}\rangle_{\mathrm{FD}} = \frac{1}{\sqrt{2}} \sum_{j \in \mathbb{Z}_2} |jj\rangle_{\mathrm{ST}} \tag{8}$$

where the subscripts S and T denote the carrier-state qubit held by the server and the carrier-state qubit that travels sequentially to each network user for duplex message encoding, respectively. All the $N+1$ network parties—from the server to N users—perform the eavesdropping check procedure to ensure the secure transmission of the traveling carrier qubit T using the decoy-state method [15], [63]. All the $N+1$ network parties—from the server to N users—perform the eavesdropping check procedure to ensure the secure transmission of the traveling carrier qubit T using the decoy-state method [15], [63]. In typical implementations, a subset of transmitted qubits is randomly selected as decoy states to detect potential eavesdropping. The insertion ratio depends on the desired security level and system parameters. Practical implementations typically use a small fraction of transmitted qubits (e.g., around 10%–20%) as decoy states [81]. The channel security is evaluated using the quantum bit error rate, and the protocol is aborted if the observed error rate exceeds a predefined threshold [82]. The insertion of decoy states slightly reduces the effective secure communication rate, typically by a factor proportional to the decoy-state fraction. Specifically, each party embeds the traveling qubit within a sequence of randomly positioned decoy-state qubits and forwards the entire sequence to the next network participant. Subsequently, random-basis measurements (in either the computational or Hadamard basis) are performed, followed by classical communication of the results. Any mismatch in these outcomes indicates a potential eavesdropping attempt, prompting immediate termination of the protocol. Upon successful verification, all parties leave the traveling qubit T unchanged, except for the anonymous communicating parties—Alice and Bob—who proceed to encode their classical messages using the following duplex modulation procedure.

2) Duplex Modulation: Alice encodes her classical message bit $\mathsf{a} \in \mathbb{Z}_2$ onto the QFDA carrier state (8) by applying the phase-flip operator $\boldsymbol{Z}^{\mathsf{a}}$ to the traveling qubit. Then, the carrier $|\mathsf{bell}\rangle_{\mathrm{FD}}$ transforms into:

$$\begin{aligned} |\psi_1\rangle &= \boldsymbol{I} \otimes \boldsymbol{Z}^{\mathsf{a}} |\mathsf{bell}\rangle_{\mathrm{FD}} \\ &= \frac{1}{\sqrt{2}} \sum_{j \in \mathbb{Z}_2} (-1)^{j\mathsf{a}} |jj\rangle_{\mathrm{ST}} . \end{aligned} \tag{9}$$

After encoding, Alice securely transmits the traveling qubit T to the next network user. The qubit then continues through the network until it successfully reaches Bob. Upon receiving the qubit, Bob encodes the classical message bit $\mathsf{b} \in \mathbb{Z}_2$ onto the state (9) by applying the phase-flip operator $\boldsymbol{Z}^{\mathsf{b}}$ to the traveling qubit, where b is the classical bit Bob intends to send to Alice. This operation transforms the state $|\psi_1\rangle$ into:

$$\begin{aligned} |\psi_2\rangle &= \boldsymbol{I} \otimes \boldsymbol{Z}^{\mathsf{b}} |\psi_1\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{j \in \mathbb{Z}_2} (-1)^{j\mathsf{a} \oplus \mathsf{b}} |jj\rangle_{\mathrm{ST}} . \end{aligned} \tag{10}$$

Finally, Bob securely transmits the traveling qubit to the server.

3) Hadamard-Basis Measurement: The server applies the Hadamard operation $\boldsymbol{H}$ to both qubits of the duplex encoding

state $|\psi_2\rangle$, transforming it into:

$$\begin{aligned}|\psi_3\rangle &= \boldsymbol{H}\otimes\boldsymbol{H}\,|\psi_2\rangle\\ &= \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle_{\rm ST} + (-1)^{\mathsf{a}\oplus\mathsf{b}}\,|{-}{-}\rangle_{\rm ST}\right)\\ &= \frac{1}{\sqrt{8}}\sum_{i,j\in\mathbb{Z}_2}\left(|ij\rangle_{\rm ST} + (-1)^{\mathsf{a}\oplus\mathsf{b}\oplus i\oplus j}\,|ij\rangle_{\rm ST}\right)\\ &= \frac{1}{\sqrt{2}}\sum_{\substack{i,j\in\mathbb{Z}_2\\ i\oplus j=\mathsf{a}\oplus\mathsf{b}}}|ij\rangle_{\rm ST}\,. \end{aligned} \tag{11}$$

Then, the server measures both qubits of the state $|\psi_3\rangle$ in the computational basis and obtain the measurement outcomes $\mu_{\rm S}\in\mathbb{Z}_2$ and $\mu_{\rm T}\in\mathbb{Z}_2$ of the qubits S and T, respectively.

4) Classical Communication: The server announces binary information

$$\hat{\mu} = \mu_{\rm S}\oplus\mu_{\rm T} \tag{12}$$

sequentially to all N users in the ring-type network using the classical channel.

5) Duplex Demodulation: Alice decodes Bob's message by calculating $\hat{\mathsf{b}} = \hat{\mu}\oplus\mathsf{a}$ using the information $\hat{\mu}$ announced by the server and her own message a sent to Bob. Similarly, Bob recovers Alice's message as $\hat{\mathsf{a}} = \hat{\mu}\oplus\mathsf{b}$. Thus, classical information is exchanged anonymously and simultaneously between Alice and Bob, without revealing their identities and message contents to any third party.

Note that the proposed FD-QAC protocol provides efficiency advantages compared with executing two sequential simplex QAC sessions. In the simplex QAC protocol for ring-type networks with N users, bidirectional communication requires two independent protocol executions, resulting in a total consumption of $2N$ Bell pairs, $2N$ qubit transmissions through the quantum channel, and $2N$ Bell-state measurement operations across the network [74]. In contrast, the proposed FD-QAC protocol completes simultaneous bidirectional exchange in a single protocol execution, using a single Bell-pair carrier state prepared by the server and a single traveling qubit that traverses the ring once. The decoding step requires only Hadamard operations followed by single-qubit measurements at the server. Consequently, the FD-QAC framework reduces the required entanglement resources, measurement operations, and overall communication latency compared to two sequential simplex QAC sessions.

B. Protocol 2: QFDA for Star-Shaped Networks

We now design a FD-QAC protocol for N dishonest users in star-shaped networks. This protocol allows any two users (e.g., Alice and Bob) in the network to simultaneously and anonymously exchange classical message bits $\mathsf{a},\mathsf{b}\in\mathbb{Z}_2$ with the help of the server (e.g., Charlie). The server prepares and distributes the multiparty QFDA carrier state—i.e., $(N+1)$-partite GHZ state—among all network participants. The verification of this entangled state follows a variant procedure proposed in [63]. Then, Alice and Bob apply the phase-flip operators to encode their messages on respective qubits for simultaneous bidirectional exchange of classical information. Specifically, the QFDA protocol in star-shaped networks follows a series of following steps under the dishonest model (see Fig. 5).

1) Carrier-State Preparation: All $N+1$ parties in the network, including the anonymous communicating parties (Alice and Bob) share the $(N+1)$-partite GHZ state—called the *multiparty* QFDA carrier:

$$|\mathsf{ghz}\rangle_{\rm FD} = \frac{1}{\sqrt{2}}\sum_{j\in\mathbb{Z}_2}|jj\rangle_{\rm SA}\,|j\rangle^{\otimes N-2}\,|j\rangle_{\rm B} \tag{13}$$

where the subscripts A, B, and S denote Alice, Bob, and the server, respectively.

2) Duplex Modulation: Alice and Bob encode their classical messages $\mathsf{a},\mathsf{b}\in\mathbb{Z}_2$ onto the QFDA carrier state (13) by applying the phase-flip operators $\boldsymbol{Z}^{\mathsf{a}}$ and $\boldsymbol{Z}^{\mathsf{b}}$ to their respective qubits, where a is the message Alice intends to send to Bob and b is the message Bob intends to send to Alice. The remaining network participants apply the identity operator $\boldsymbol{I}$ to their qubits, thereby leaving their qubit states unchanged. Then, the $(N+1)$-partite entangled carrier state $|\mathsf{ghz}\rangle_{\rm FD}$ transforms into:

$$\begin{aligned}|\boldsymbol{\eta}_1\rangle &= \boldsymbol{I}\otimes\boldsymbol{Z}^{\mathsf{a}}\otimes\boldsymbol{I}^{\otimes N-2}\otimes\boldsymbol{Z}^{\mathsf{b}}\,|\mathsf{ghz}\rangle_{\rm FD}\\ &= \frac{1}{\sqrt{2}}\sum_{j\in\mathbb{Z}_2}(-1)^{j\mathsf{a}\oplus\mathsf{b}}\,|jj\rangle_{\rm SA}\,|j\rangle^{\otimes N-2}\,|j\rangle_{\rm B}\,. \end{aligned} \tag{14}$$

3) Hadamard-Basis Measurement: All $N+1$ network participants apply the Hadamard operation $\boldsymbol{H}$ on their respective qubits of the duplex encoding state $|\boldsymbol{\eta}_1\rangle$, transforming it as follows:

$$\begin{aligned}|\boldsymbol{\eta}_2\rangle &= \boldsymbol{H}^{\otimes N+1}\,|\boldsymbol{\eta}_1\rangle\\ &= \frac{1}{\sqrt{2}}\left(|{+}\rangle^{\otimes N+1} + (-1)^{\mathsf{a}\oplus\mathsf{b}}\,|{-}\rangle^{\otimes N+1}\right)\\ &= \frac{1}{\sqrt{2^{N+2}}}\sum_{\boldsymbol{k}\in\mathbb{Z}_2^{N+1}}\left(|\boldsymbol{k}\rangle + (-1)^{\mathsf{a}\oplus\mathsf{b}\oplus\|\boldsymbol{k}\|_1}\,|\boldsymbol{k}\rangle\right)\\ &= \frac{1}{\sqrt{2^N}}\sum_{\substack{\boldsymbol{k}\in\mathbb{Z}_2^{N+1}\\ \|\boldsymbol{k}\|_1=\mathsf{a}\oplus\mathsf{b}}}|\boldsymbol{k}\rangle \end{aligned} \tag{15}$$

where $\|\boldsymbol{k}\|_1$ denotes the ℓ_1 norm of $\boldsymbol{k}$. For the binary vector $\boldsymbol{x}=(x_1,x_2,,\ldots,x_n)\in\mathbb{Z}_2^n$, the ℓ_1 norm of $\boldsymbol{x}$ is specifically defined as the binary sum of all entries, i.e., $\|\boldsymbol{x}\|_1 = x_1\oplus x_2\oplus\cdots\oplus x_n$. Then, all $N+1$ network parties measure their qubits of $|\boldsymbol{\eta}_2\rangle$ in the computational basis and get their measurement outcomes $\boldsymbol{\mu}=(\mu_0,\mu_1,\ldots,\mu_N)\in\mathbb{Z}_2^{N+1}$. The outcome μ_0 corresponds to the measurement result obtained by the server.

4) Classical Communication: All N network users transmit their measurement results $\mu_1,\mu_2,\ldots,\mu_N$ to the server through a classical authenticated communication channel. Then, the server announces the binary sum (ℓ_1 norm)

$$\hat{\mu} = \|\boldsymbol{\mu}\|_1 = \mu_0\oplus\mu_1\oplus\cdots\oplus\mu_N \tag{16}$$

to all N network users using the classical channel.

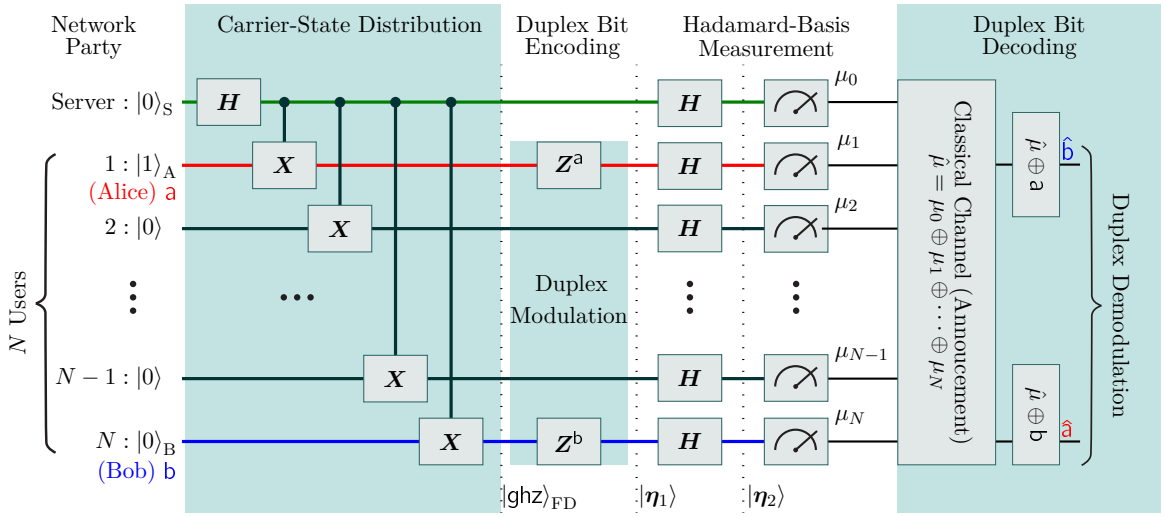


Fig. 5. A FD-QAC protocol in a star-shaped topology for classical information (Protocol 2). The protocol involves GHZ-state preparation, duplex encoding (phase-flip operations), Hadamard-basis measurements, classical announcements, and duplex decoding (binary ℓ_1 norms).

5) Duplex Demodulation: Alice and Bob finally decode their respective messages by taking the same duplex demodulation steps used in Protocol 1 for ring-type networks. Note that in FD-QAC protocols, Alice's message serves as the key to decode Bob's message, and vice versa.

In particular, the entanglement distribution overhead of the proposed protocols depends on the network topology. In the ring-type FD-QAC protocol, only a single Bell-pair carrier state is required, and the traveling qubit interacts sequentially with the network users. Consequently, the entanglement distribution cost remains constant and does not scale with the network size. In contrast, the star-type FD-QAC protocol relies on the $(N+1)$-partite GHZ state distributed by the server to all network participants. Therefore, the entanglement distribution overhead scales linearly with the network size, as the server must distribute one entangled qubit to each user.

V. Security Analysis

The objective of the FD-QAC protocols is to enable two communicating parties to exchange messages anonymously, securely, and simultaneously. Anonymity is preserved as long as the adversary's uncertainty about the identities of the communicating parties remains unchanged. The adversary's goal is to compromise the anonymity or security of the protocol. In this section, we analyze the security of Protocol 1 under the semi-honest network model and Protocol 2 under the dishonest network model. In the semi-honest model, all participants are assumed to follow the protocol faithfully while passively recording all accessible information during execution. In contrast, the dishonest model allows participants to actively deviate from the protocol and engage in malicious behavior. We begin with the analysis of Protocol 1 under the semi-honest model, followed by the analysis of Protocol 2 under the dishonest model.

A. Protocol 1 Under the Semi-Honest Model

We characterize the security of Protocol 1 under the semi-honest model by considering two distinct attack scenarios: i) an external adversary attempts to identify the communicating parties, and ii) an internal adversary exploits the information recorded during the protocol execution to compromise its security. In this protocol, only the server has access to both qubits of the QFDA carrier state. The first qubit S of the state $|\text{bell}\rangle_{FD}$ in (8) is retained by the server at all times, while the second traveling qubit T is sequentially transmitted among the server and N users. The reduced density matrix of the traveling qubit T is given by

$$\begin{aligned}\boldsymbol{\rho}_T &= \text{tr}_S\left(|\text{bell}\rangle_{FD}\langle\text{bell}|\right)\\ &= \frac{1}{2}\left(|0\rangle_T\langle 0| + |1\rangle_T\langle 1|\right) = \frac{1}{2}\boldsymbol{I}.\end{aligned} \tag{17}$$

Clearly, $\boldsymbol{\rho}_T$ is a maximally mixed state and remains invariant under any unitary operation. Consequently, no useful information can be extracted from the traveling qubit T. Moreover, the traveling qubit is securely transmitted across the ring-type quantum network using the decoy-state method. Since the positions of the decoy qubits are known only to the respective senders, an adversary cannot distinguish between the decoy states and the actual carrier qubit. As a result, any eavesdropping attempt inevitably introduces disturbances to the decoy states, which can be detected by the communicating parties, leading to immediate termination of the protocol. Therefore, the protocol is secure against external adversaries and prevents them from obtaining any useful information about the identities of the communicating parties or the transmitted messages.

In the second (internal attack) scenario, any user in the network attempts to compromise the anonymity of the protocol by utilizing information recorded during its execution. However, as previously discussed, the message-carrying qubit remains in a maximally mixed state, ensuring that no useful information can be extracted from it throughout the transmission process. Although the server ultimately gains access to the encoded carrier state $|\psi_2\rangle = (|00\rangle_{ST} + (-1)^{a\oplus b}|11\rangle_{ST})/\sqrt{2}$ at the end of the protocol, it is important to note that this state is independent of the identities of the communicating parties. The

state $|\psi_2\rangle$ depends solely on the binary sum $\mathsf{a} \oplus \mathsf{b}$ of the classical message bits and remains invariant with respect to which two users participated in the communication. In other words, the encoded phase $(-1)^{\mathsf{a}\oplus\mathsf{b}}$ carries no information about user identities. Moreover, the protocol utilizes a technique analogous to the quantum one-time pad, in which the phase information is effectively masked by the classical messages themselves. For example, Alice's classical message a sent to Bob serves as the decoding key for Bob's message b, and vice versa. This ensures that even if the server observes the encoded state, it cannot infer the message content exchanged between the communicating parties or their identities, demonstrating the untraceability property. Consequently, the protocol ensures both anonymity and security against adversaries.

B. Protocol 2 Under the Dishonest Model

We now analyze the security of Protocol 2 under the dishonest model, considering two attack scenarios: i) the server or an external adversary attempts to attack the protocol without any collaboration from network participants, and ii) an adversary colludes with K dishonest participants to compromise the anonymity of the honest communicating participants. The QFDA (GHZ) carrier state is distributed among the network participants according to the procedure detailed in [63]. Any active attack by the server or an external adversary during this distribution phase is easily detectable. Since no further communication occurs over the quantum channel after distribution, the adversary is restricted to passive attacks. The probability of obtaining a specific outcome vector $\boldsymbol{\mu} = \boldsymbol{x} \in \mathbb{Z}_2^{N+1}$ is given by

$$\begin{aligned}\Pr[\boldsymbol{\mu} = \boldsymbol{x}] &= \mathrm{tr}\left(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\, \boldsymbol{H}^{\otimes N+1}\, |\boldsymbol{\eta}_1\rangle\langle\boldsymbol{\eta}_1|\, \boldsymbol{H}^{\otimes N+1}\right) \\ &= \frac{1}{\sqrt{2^{N+2}}}\left[1 + (-1)^{\mathsf{a}\oplus\mathsf{b}\oplus\|\boldsymbol{x}\|_1}\right]^2, \end{aligned} \tag{18}$$

which implies that only 2^N outcome vectors satisfying $\|\boldsymbol{x}\|_1 = \mathsf{a} \oplus \mathsf{b}$ can occur among 2^{N+1} binary vectors, and each such outcome appears uniformly at random with probability $1/2^N$. Therefore, these measurement outcomes reveal no information about individual values of a and b, as well as leak any information regarding the identities of the communicating parties. Consequently, neither an external adversary nor a malicious server can gain any knowledge about the communication pair, ensuring information-theoretic anonymity.

In the second colluding scenario, the adversary may collude with K malicious participants of the network to compromise the anonymity. This type of attack is potentially more effective, as the adversary gains access to the quantum resources, i.e., the reduced density matrix $\boldsymbol{\rho}_{\mathrm{D}}$ of K dishonest participants:

$$\begin{aligned}\boldsymbol{\rho}_{\mathrm{D}} &= \mathrm{tr}_{\mathrm{H,S}}\left(|\mathsf{ghz}\rangle_{\mathrm{FD}}\langle\mathsf{ghz}|\right) \\ &= \mathrm{tr}_{\mathrm{H,S}}\left(|\boldsymbol{\eta}_1\rangle\langle\boldsymbol{\eta}_1|\right) \\ &= \frac{1}{2}\left(|0\rangle_{\mathrm{T}}\langle 0|^{\otimes K} + |1\rangle_{\mathrm{T}}\langle 1|^{\otimes K}\right) = \frac{1}{2}\boldsymbol{I} \end{aligned} \tag{19}$$

where the subscript H denotes the honest participants. To infer the identities of the communicating parties, the adversary attempts to exploit both the quantum information $\boldsymbol{\rho}_{\mathrm{D}}$ available from the malicious users and the classically announced measurement outcomes from the honest users H and the server S. However, (19) shows that the quantum information held by the dishonest users remains in a maximally mixed state both before and after the encoding operation, and is invariant under any unitary transformation. As a result, no information about the identities of the communicating parties can be extracted from this state. Hence, even with access to the quantum states of the dishonest users, the adversary is unable to compromise the protocol's anonymity.

VI. DEP Analysis in Noisy Quantum Networks

In this section, we analyze the error performance of the QFDA protocols in the presence of quantum noise. Specifically, we consider three types of quantum noise channels: bit-flip quantum noise $\mathcal{N}_X$, phase-flip quantum noise $\mathcal{N}_Z$, and depolarizing quantum noise $\mathcal{N}_D$. It is important to note that these noise channels only affect the traveling qubit of the QFDA carrier state—that is, the qubit transmitted through quantum channels during the protocol execution. The stationary qubit, held at the server, remains unaffected. To assess the impact of each noise type on the QFDA protocols, we briefly describe the corresponding quantum noise models.

- *Bit-Flip Noise*: This channel is modeled as a completely positive trace-preserving (CPTP) map, which flips a qubit state $\boldsymbol{\rho}$ with probability p, and leaves it unchanged with probability $1-p$. The channel map is given by

$$\mathcal{N}_X(\boldsymbol{\rho}) = (1-p)\,\boldsymbol{\rho} + p\boldsymbol{X}\boldsymbol{\rho}\boldsymbol{X}. \tag{20}$$

- *Phase-Flip Noise*: A CPTP map that introduces a phase-flip error in a qubit state $\boldsymbol{\rho}$ with probability p, and leaves it unchanged with probability $1-p$. The channel map is given by

$$\mathcal{N}_Z(\boldsymbol{\rho}) = (1-p)\,\boldsymbol{\rho} + p\boldsymbol{Z}\boldsymbol{\rho}\boldsymbol{Z}. \tag{21}$$

- *Depolarizing Noise*: A CPTP map that transforms a quantum state $\boldsymbol{\rho}$ into a convex combination of the original state and the maximally mixed state. The channel map is given by

$$\mathcal{N}_D(\boldsymbol{\rho}) = (1-p)\,\boldsymbol{\rho} + \frac{p}{2}\boldsymbol{I}. \tag{22}$$

Note that for bit-flip $\mathcal{N}_X$ and phase-flip $\mathcal{N}_Z$ noise channels, the noise parameter p is typically considered in the range $0 \leq p \leq 1/2$, as the effect of these channels is limited to flipping the qubit state with a certain probability. Beyond $p = 1/2$, the noise begins to resemble a deterministic inversion. In contrast, the depolarizing channel $\mathcal{N}_D$ spans the full range $0 \leq p \leq 1$, as it represents a convex mixture between the original quantum state and the maximally mixed state, with $p = 1$ corresponding to complete depolarization (i.e., total loss of information).

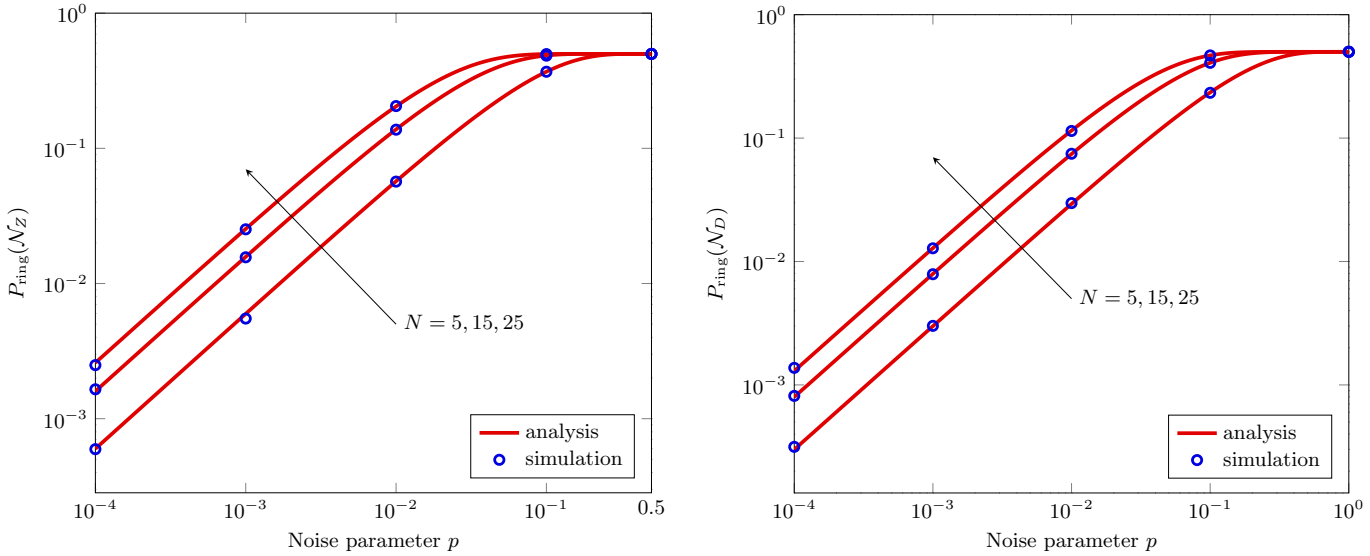


Fig. 6. DEP $P_{\text{ring}}(\mathcal{N})$ for the QFDA Protocol 1 as a function of the noise parameter p when $N = 5, 15, 25$ under phase-flip noise $\mathcal{N}_Z$ (left) and depolarizing noise $\mathcal{N}_D$ (right), respectively.

A. Protocol 1 with Noisy QFDA Carriers

In ring-type quantum networks, the state (8) serves as the carrier state for FD-QAC. The evolution of this QFDA carrier state under noise is given by

$$\begin{aligned}\boldsymbol{\rho}_{\text{bell}}(\mathcal{N}) &= (\boldsymbol{I}\otimes\mathcal{N})^{\otimes N+1}\left(|\mathsf{bell}\rangle_{\text{FD}}\langle\mathsf{bell}|\right)\\ &= \frac{1}{2}\sum_{i,j\in\mathbb{Z}_2}(\boldsymbol{I}\otimes\mathcal{N})^{\otimes N+1}\left(|i\rangle\langle j|^{\otimes 2}\right)\end{aligned} \tag{23}$$

where $\mathcal{N}\in\{\mathcal{N}_X,\mathcal{N}_Z,\mathcal{N}_D\}$ denotes the quantum noise channel acting on the traveling qubit. This formulation captures the cumulative effect of noise on the traveling carrier qubit as it traverses through the quantum channels. With error symmetry and equiprobable *a priori* duplex information, we obtain the DEP $P_{\text{ring}}(\mathcal{N})$ for ring-type networks under the noisy carrier state $\boldsymbol{\rho}_{\text{bell}}(\mathcal{N})$ as follows:

$$\begin{aligned}P_{\text{ring}}(\mathcal{N}) &= \Pr\left[\hat{\mathsf{a}}\neq\mathsf{a}\text{ or quivalently }\hat{\mathsf{b}}\neq\mathsf{b}\mid\boldsymbol{\rho}_{\text{bell}}(\mathcal{N})\right]\\ &= \Pr\left[\hat{\mu}\oplus\mathsf{b}\neq\mathsf{a}\mid\boldsymbol{\rho}_{\text{bell}}(\mathcal{N})\right]\\ &= \Pr\left[\hat{\mu}\neq\mathsf{a}\oplus\mathsf{b}\mid\boldsymbol{\rho}_{\text{bell}}(\mathcal{N})\right]\\ &= \Pr\left[\hat{\mu}\neq 0\mid\mathsf{a}\oplus\mathsf{b}=0,\boldsymbol{\rho}_{\text{bell}}(\mathcal{N})\right].\end{aligned} \tag{24}$$

To decode the duplex information, both qubits of the noisy carrier state (23) are measured in the Hadamard basis, giving $\hat{\mu}=\mu_{\text{S}}\oplus\mu_{\text{T}}$. The projection of $|i\rangle\langle j|$ in the Hadamard basis is given by

$$\langle k|_{\mathcal{H}}|i\rangle\langle j|k|j|k\rangle_{\mathcal{H}} = \frac{1}{2}(-1)^{k(i-j)} \tag{25}$$

where $i,j,k\in\mathbb{Z}_2$ and the eigenstates $|k\rangle_{\mathcal{H}}=\boldsymbol{H}|k\rangle$ belong to the Hadamard basis states $|\pm\rangle$, formed by the Hadamard transforms (3) and (4). In this basis, the action of the quantum channel $\mathcal{N}$ on the diagonal $|i\rangle\langle i|$ and the non-diagonal $|i\rangle\langle j|$ states, with $i\neq j\in\mathbb{Z}_2$, is described as:

$$\langle k|_{\mathcal{H}}\mathcal{N}(|i\rangle\langle i|)|k\rangle_{\mathcal{H}} = 1/2 \tag{26}$$

$$\langle k|_{\mathcal{H}}\mathcal{N}(|i\rangle\langle j|)|k\rangle_{\mathcal{H}} = \frac{D_{\mathcal{N}}}{2}(-1)^{k(i-j)} \tag{27}$$

where the noise-dependent factor $D_{\mathcal{N}}$ is given by

$$D_{\mathcal{N}} = \begin{cases}1, & \mathcal{N}=\mathcal{N}_X\\ 1-2p, & \mathcal{N}=\mathcal{N}_Z\\ 1-p, & \mathcal{N}=\mathcal{N}_D.\end{cases} \tag{28}$$

Using (23)–(28) with the same arguments in [71], the DEP for Protocol 1 under quantum noise $\mathcal{N}$ is given by

$$P_{\text{ring}}(\mathcal{N}) = \frac{1}{2}\left(1-D_{\mathcal{N}}^{N+1}\right) \tag{29}$$

exhibiting its asymptote $P_{\text{ring}}(\mathcal{N}) = (1-D_{\mathcal{N}})(N+1)/2 + o(p)$ as $p\to 0$ in the low-noise regime.

In the presence of bit-flip noise, the Hadamard operation transforms a bit-flip error to a phase-flip error, i.e., $\boldsymbol{HXH}=\boldsymbol{Z}$. Since phase-flip errors do not affect measurement outcomes in the computational basis, this type of noise has no effect on the protocol error performance—i.e., $P_{\text{ring}}(\mathcal{N}_X)=0$. Fig. 6 shows the DEP $P_{\text{ring}}(\mathcal{N})$ for Protocol 1 as a function of the noise parameter p when $N=5,15,25$ under phase-flip noise $\mathcal{N}_Z$ (left) and depolarizing noise $\mathcal{N}_D$ (right), respectively. The results indicate that $P_{\text{ring}}(\mathcal{N})$ exhibits linear scaling with respect to the probability p and the network size $N+1$ in the low-noise regime ($p\ll 1$), as shown in the log-log plots.

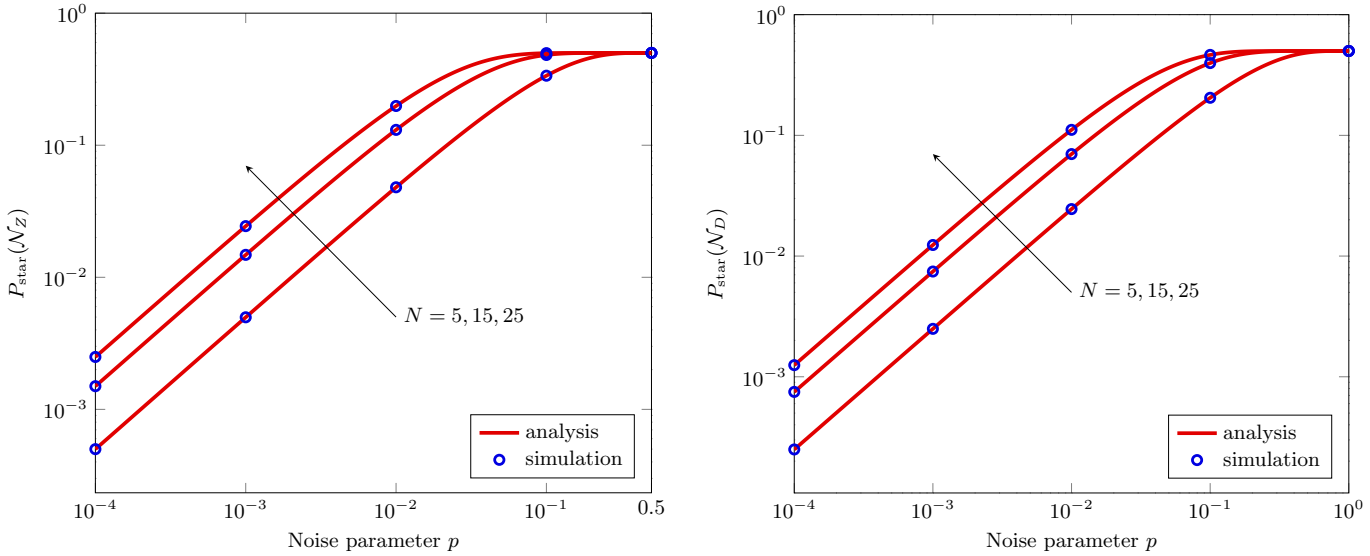


Fig. 7. DEP $P_{\text{star}}(\mathcal{N})$ for the QFDA Protocol 2 as a function of the noise parameter p when $N = 5, 15, 25$ under phase-flip noise $\mathcal{N}_Z$ (left) and depolarizing noise $\mathcal{N}_D$ (right), respectively.

B. Protocol 2 with Noisy QFDA Carriers

In star-shaped quantum networks, the state (13) serves as the QFDA carrier and evolves under noise $\mathcal{N}$ as follows:

$$\begin{aligned}\boldsymbol{\rho}_{\text{ghz}}(\mathcal{N}) &= \boldsymbol{I} \otimes \mathcal{N}^{\otimes N}\left(|\mathsf{ghz}\rangle_{\text{FD}}\langle\mathsf{ghz}|\right) \\ &= \frac{1}{2}\sum_{i,j\in\mathbb{Z}_2} \boldsymbol{I} \otimes \mathcal{N}^{\otimes N}\left(|i\rangle\langle j|^{\otimes N+1}\right) \end{aligned} \tag{30}$$

where the noisy map $\mathcal{N}$ affects only the qubits distributed to the N users, excluding the qubit retained by the server. Under the same assumption and argument as in (24), we obtain the DEP $P_{\text{star}}(\mathcal{N})$ for star-shaped networks with the noisy QFDA carrier $\boldsymbol{\rho}_{\text{ghz}}(\mathcal{N})$ as follows:

$$P_{\text{star}}(\mathcal{N}) = \Pr\left[\hat{\mu} = \|\boldsymbol{\mu}\|_1 \neq 0 \mid \mathsf{a} \oplus \mathsf{b} = 0, \boldsymbol{\rho}_{\text{ghz}}(\mathcal{N})\right]. \tag{31}$$

To decode the duplex information in the star-shaped networks, all $N+1$ qubits of the noisy state (30) are locally measured in the Hadamard basis. Using (30) and (31) along with the projection relations (26)–(28), the DEP $P_{\text{star}}(\mathcal{N})$ for Protocol 2 under quantum noise $\mathcal{N}$ is again given by

$$P_{\text{star}}(\mathcal{N}) = \frac{1}{2}\left(1 - D_{\mathcal{N}}^{N}\right), \tag{32}$$

which behaves as

$$P_{\text{star}}(\mathcal{N}) = \frac{N}{2}\left(1 - D_{\mathcal{N}}\right) + o(p) \quad (p \to 0) \tag{33}$$

in the low-noise asymptotic regime. As in Protocol 1, bit-flip noise $\mathcal{N}_X$ has no effect on the protocol error performance due to its symmetry under Hadamard transformation. Fig. 7 depicts the DEP $P_{\text{star}}(\mathcal{N})$ for Protocol 2 as a function of the noise parameter p under dephasing noise $\mathcal{N}_Z$ (left) and depolarizing noise $\mathcal{N}_D$ (right), confirming its linear scaling properties with respect to both p and N, as similarly observed in Fig. 6 for the ring-type case.

In practical implementations, photon loss does not compromise the anonymity of the protocol but reduces the probability of successful entanglement distribution and photon detection, thereby lowering the effective execution rate of the protocol in large-scale quantum networks. In the ring-type FD-QAC protocol, the traveling carrier qubit sequentially traverses the network participants, and the success probability depends on the transmission efficiency of quantum channels. Similarly, in the star-type FD-QAC protocol, the successful distribution of the $(N+1)$-partite GHZ state depends on the transmission efficiency of the channels connecting the server and the users. Nevertheless, such effects primarily influence the execution efficiency rather than the security of the protocol, and reliable communication can still be achieved through repeated protocol rounds in practical quantum networks [36].

VII. Conclusion

This paper has designed two FD-QAC protocols that enable the simultaneous, secure, and anonymous exchange of classical information in adversarial quantum networks. These QFDA protocols, tailored for ring-type and star-shaped network topologies, exploit quantum entanglement and LOCC to achieve full duplexity, robust anonymity, and perfect untraceability, ensuring that even adversaries with complete network access cannot associate transmitted information with its origin. We have analyzed the robust security of these protocols against both external and internal adversaries, including semi-honest and dishonest participants. Furthermore, the DEP analysis under noisy quantum environments confirms the practicality and reliability of the designed QFDA protocols, exhibiting scalable and noise-resilient behavior across different noise conditions. Specifically, the protocols demonstrate error-free performance under bit-flip noise attributed to the inherent symmetry in the encoding and measurement operations. In contrast, under phase-flip and depolarizing noise, the DEP exhibits linear scaling with both the noise probability and the network size in the low-noise regime. These findings pave the

way for developing scalable and noise-tolerant QAC frameworks, facilitating robust, privacy-preserving, and full-duplex communication in adversarial QANs. There is considerable potential for further advancing FD-QAC protocols. In particular, Protocol 2 relies on multipartite GHZ states to achieve key privacy properties such as anonymity and untraceability. While recent experimental progress has demonstrated the feasibility of generating large multipartite entangled states—for example, 18-qubit GHZ states with a fidelity of 0.708 and a count rate of 55 millihertz using multiple degrees of freedom [83]—the preparation and distribution of such states become increasingly challenging as the network size grows. Consequently, Protocol 2 is expected to be more suitable for small- to medium-scale quantum networks in near-term implementations. Future research can explore alternative quantum resources and optimized protocol designs to further improve scalability while maintaining strong privacy and security guarantees.

REFERENCES

[1] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, "Quantum Internet—Applications, functionalities, enabling technologies, challenges, and research directions," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2218–2247, Sep. 2021.

[2] U. Khalid, J. ur Rehman, S. N. Paing, H. Jung, T. Q. Duong, and H. Shin, "Quantum network engineering in the NISQ age: Principles, missions, and challenges," *IEEE Netw.*, vol. 38, no. 1, pp. 112–123, Jan. 2024.

[3] N. Gisin and R. Thew, "Quantum communication," *Nat. Photon.*, vol. 1, no. 3, pp. 165–171, Mar. 2007.

[4] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018.

[5] F. Zaman, A. Farooq, M. A. Ullah, H. Jung, H. Shin, and M. Z. Win, "Quantum machine intelligence for 6G URLLC," *IEEE Wireless Commun.*, vol. 30, no. 2, pp. 22–30, Apr. 2023.

[6] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Rev. Mod. Phys.*, vol. 89, no. 3, p. 035002, Jul. 2017.

[7] C. Portmann and R. Renner, "Security in quantum cryptography," *Rev. Mod. Phys.*, vol. 94, no. 2, p. 025008, Jun. 2022.

[8] U. Khalid, M. S. Ulum, M. Z. Win, and H. Shin, "Integrated satellite-ground variational quantum sensing networks," *IEEE Commun. Mag.*, vol. 62, no. 10, pp. 20–27, Oct. 2024.

[9] F. Zaman, S. N. Paing, A. Farooq, H. Shin, and M. Z. Win, "Concealed quantum telecomputation for anonymous 6G URLLC networks," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 7, pp. 2278–2296, Jul. 2023.

[10] U. Khalid, U. I. Paracha, Z. Naveed, T. Q. Duong, M. Z. Win, and H. Shin, "Quantum fusion intelligence for integrated satellite-ground remote sensing," *IEEE Wireless Commun.*, vol. 32, no. 3, pp. 46–55, Jun. 2025.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, Jan. 1984, pp. 175–179.

[12] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, Jan. 2022.

[13] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim *et al.*, "A device-independent quantum key distribution system for distant users," *Nature*, vol. 607, no. 7920, pp. 687–691, Jul. 2022.

[14] H. Yu, S. Sciara, M. Chemnitz, N. Montaut, B. Crockett, B. Fischer, R. Helsten, B. Wetzel, T. A. Goebel, R. G. Krämer *et al.*, "Quantum key distribution implemented with d-level time-bin entangled photons," *Nat. Commun.*, vol. 16, no. 1, p. 171, Jan. 2025.

[15] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A*, vol. 69, no. 5, p. 052319, May 2004.

[16] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum secure direct communication with quantum memory," *Phys. Rev. Lett.*, vol. 118, no. 22, p. 220501, May 2017.

[17] L. Zhou, B.-W. Xu, W. Zhong, and Y.-B. Sheng, "Device-independent quantum secure direct communication with single-photon sources," *Phys. Rev. Appl.*, vol. 19, no. 1, p. 014036, Jan. 2023.

[18] D. Pan, G.-L. Long, L. Yin, Y.-B. Sheng, D. Ruan, S. X. Ng, J. Lu, and L. Hanzo, "The evolution of quantum secure direct communication: On the road to the qinternet," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1898–1949, Feb. 2024.

[19] H. Dai, Q. Shen, C.-Z. Wang, S.-L. Li, W.-Y. Liu, W.-Q. Cai, S.-K. Liao, J.-G. Ren, J. Yin, Y.-A. Chen *et al.*, "Towards satellite-based quantum-secure time transfer," *Nat. Phys.*, vol. 16, no. 8, pp. 848–852, May 2020.

[20] M. T. Rahim, A. Khan, U. Khalid, J. ur Rehman, H. Jung, and H. Shin, "Quantum secure metrology for network sensing-based applications," *Sci. Rep.*, vol. 13, no. 1, p. 11630, Jul. 2023.

[21] S. M. A. Rizvi, U. Khalid, S. Chatzinotas, T. Q. Duong, and H. Shin, "Controlled quantum semantic communication for industrial CPS networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 13, pp. 996–1009, 2026.

[22] S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of blind quantum computing," *Science*, vol. 335, no. 6066, pp. 303–308, Jan. 2012.

[23] C. Greganti, M.-C. Roehsner, S. Barz, T. Morimae, and P. Walther, "Demonstration of measurement-only blind quantum computing," *New J. Phys.*, vol. 18, no. 1, p. 013020, Jan. 2016.

[24] B. Polacchi, D. Leichtle, G. Carvacho, G. Milani, N. Spagnolo, M. Kaplan, E. Kashefi, and F. Sciarrino, "Experimental verifiable multiclient blind quantum computing on a Qline architecture," *Phys. Rev. Lett.*, vol. 134, no. 20, p. 200603, May 2025.

[25] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, pp. 1829–1834, Mar. 1999.

[26] B. A. Bell, D. Markham, D. Herrera-Martí, A. Marin, W. Wadsworth, J. Rarity, and M. Tame, "Experimental demonstration of graph-state quantum secret sharing," *Nat. Commun.*, vol. 5, no. 1, pp. 1–12, Nov. 2014.

[27] Z.-F. Liu, W.-M. Shang, J.-M. Xu, Z.-M. Cheng, W.-Z. Zhu, H. Li, P. Wan, S.-T. Xue, Y.-C. Lou, C. Chen *et al.*, "Experimental demonstration of complete quantum information masking and generalization of quantum secret sharing," *Commun. Phys.*, vol. 8, no. 1, p. 30, Jan. 2025.

[28] R. V. Meter, K. Nemoto, and W. J. Munro, "Communication links for distributed quantum computation," *IEEE Trans. Comput.*, vol. 56, no. 12, pp. 1643–1653, Dec. 2007.

[29] V. Lipinska, J. Ribeiro, and S. Wehner, "Secure multiparty quantum computation with few qubits," *Phys. Rev. A*, vol. 102, no. 2, p. 022405, Aug. 2024.

[30] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudonymity: A proposal for terminology," in *Proc. Designing Privacy Enhanc. Technol.: Int. Workshop on Des. Issues in Anonymity and Unobservability*, Berkeley, CA, USA, Jan. 2001, pp. 1–9.

[31] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865–942, Jun. 2009.

[32] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[33] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Phys. Rev. A*, vol. 54, no. 3, p. 1844, Sep. 1996.

[34] S. N. Paing, J. W. Setiawan, T. Q. Duong, D. Niyato, M. Z. Win, and H. Shin, "Quantum anonymous networking: A quantum leap in privacy," *IEEE Netw.*, vol. 38, no. 5, pp. 131–145, Sep. 2024.

[35] A. Khan, T. T. Bui, J. ur Rehman, S. Chatzinotas, S. L. Cotton, O. A. Dobre, T. Q. Duong, and H. Shin, "Integrated non-terrestrial and terrestrial quantum anonymous networks," *IEEE Netw.*, vol. 39, no. 3, pp. 196–206, May 2025.

[36] Z. Huang, S. K. Joshi, D. Aktas, C. Lupo, A. O. Quintavalle, N. Venkatachalam, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu *et al.*, "Experimental implementation of secure anonymous protocols on an eight-user quantum key distribution network," *npj Quantum Inform.*, vol. 8, no. 1, p. 25, Mar. 2022.

[37] M. S. Ulum, U. Khalid, J. W. Setiawan, T. Q. Duong, M. Z. Win, and H. Shin, "Variational anonymous quantum sensing," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 9, pp. 2275–2291, Sep. 2024.

[38] S. Tariq, U. Khalid, B. E. Arfeto, T. Q. Duong, and H. Shin, "Integrating sustainable big AI: Quantum anonymous semantic broadcast," *IEEE Wireless Commun.*, vol. 31, no. 3, pp. 86–99, Jun. 2024.

[39] M. Christandl and S. Wehner, "Quantum anonymous transmissions," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Chennai, India, Dec. 2005, pp. 217–235.

[40] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, "Anonymous quantum communication," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Kuching, Sarawak, Malaysia, Dec. 2007, pp. 460–473.

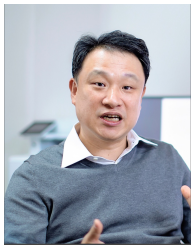
[41] J. Bouda and J. Šprojcar, "Quantum communication between anonymous sender and anonymous receiver in the presence of strong adversary," *Int. J. Quantum Inf.*, vol. 9, no. 02, pp. 651–663, Mar. 2011.
[42] T.-Y. Wang, Q.-Y. Wen, and F.-C. Zhu, "Economical quantum anonymous transmissions," *J. Phys. B*, vol. 43, no. 24, p. 245501, Nov. 2010.
[43] X.-Q. Cai and H.-F. Niu, "Quantum private communication with an anonymous sender," *Int. J. Theor. Phys.*, vol. 52, no. 2, pp. 411–419, Sep. 2013.
[44] W. Yang, L. Huang, and F. Song, "Privacy preserving quantum anonymous transmission via entanglement relay," *Sci. Rep.*, vol. 6, no. 1, p. 26762, Jun. 2016.
[45] S. N. Paing, J. W. Setiawan, S. Tariq, M. T. Rahim, K. Lee, and H. Shin, "Counterfactual anonymous quantum teleportation in the presence of adversarial attacks and channel noise," *Sensors*, vol. 22, no. 19, p. 7587, Oct. 2022.
[46] J. Bouda and J. Sprojcar, "Anonymous transmission of quantum information," in *Proc. Int. Conf. Quantum, Nano Micro Technol.*, Guadeloupe, French Caribbean, Jan. 2007, pp. 12–12.
[47] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, "Anonymity for practical quantum networks," *Phys. Rev. Lett.*, vol. 122, no. 24, p. 240501, Jun. 2019.
[48] Y.-G. Yang, Y.-L. Yang, X.-L. Lv, Y.-H. Zhou, and W.-M. Shi, "Examining the correctness of anonymity for practical quantum networks," *Phys. Rev. A*, vol. 101, no. 6, p. 062311, Jun. 2020.
[49] V. Lipinska, G. Murta, and S. Wehner, "Anonymous transmission in a noisy quantum network using the W state," *Phys. Rev. A*, vol. 98, no. 5, p. 052320, Nov. 2018.
[50] Y. Wang, X. Li, Y. Han, and K. Zhang, "Practical anonymous entanglement with noisy measurement," *Quantum Inf. Process.*, vol. 21, no. 2, p. 49, Jan. 2022.
[51] Y.-G. Yang, X.-X. Liu, S. Gao, Y.-H. Zhou, W.-M. Shi, J. Li, and D. Li, "Towards practical anonymous quantum communication: A measurement-device-independent approach," *Phys. Rev. A*, vol. 104, no. 5, p. 052415, Nov. 2021.
[52] J. A. Vaccaro, J. Spring, and A. Chefles, "Quantum protocols for anonymous voting and surveying," *Phys. Rev. A*, vol. 75, no. 1, p. 012333, Jan. 2007.
[53] L. Jiang, G. He, D. Nie, J. Xiong, and G. Zeng, "Quantum anonymous voting for continuous variables," *Phys. Rev. A*, vol. 85, no. 4, p. 042309, Apr. 2012.
[54] N. Bao and N. Y. Halpern, "Quantum voting and violation of Arrow's impossibility theorem," *Phys. Rev. A*, vol. 95, no. 6, p. 062306, Jun. 2017.
[55] S. Mishra, K. Thapliyal, A. Parakh, and A. Pathak, "Quantum anonymous veto: a set of new protocols," *EPJ Quantum Technol.*, vol. 9, no. 1, p. 14, May 2022.
[56] A. Khan, J. ur Rehman, and H. Shin, "Quantum anonymous notification for network-based applications," *Quantum Inf. Process.*, vol. 20, no. 12, p. 397, Nov. 2021.
[57] B. Gong, F. Gao, and W. Cui, "Anonymous communication protocol over quantum networks," *Quantum Inf. Process.*, vol. 21, no. 3, p. 99, Feb. 2022.
[58] F. Hahn, J. de Jong, and A. Pappa, "Anonymous quantum conference key agreement," *PRX Quantum*, vol. 1, no. 2, p. 020325, Dec. 2020.
[59] F. Grasselli, G. Murta, J. de Jong, F. Hahn, D. Bruß, H. Kampermann, and A. Pappa, "Secure anonymous conferencing in quantum networks," *PRX Quantum*, vol. 3, no. 4, p. 040306, Oct. 2022.
[60] J. W. Webb, J. Ho, F. Grasselli, G. Murta, A. Pickston, A. Ulibarrena, and A. Fedrizzi, "Experimental anonymous quantum conferencing," *Optica*, vol. 11, no. 6, pp. 872–875, Jun. 2024.
[61] A. Khan, U. Khalid, J. ur Rehman, K. Lee, and H. Shin, "Quantum anonymous collision detection for quantum networks," *EPJ Quantum Technol.*, vol. 8, no. 1, p. 27, Dec. 2021.
[62] W. Zheng and B. Gong, "Anonymous collision detection for practical quantum networks," *Phys. Lett. A*, vol. 525, p. 129854, Nov. 2024.
[63] W. Huang, Q.-Y. Wen, B. Liu, Q. Su, S.-J. Qin, and F. Gao, "Quantum anonymous ranking," *Phys. Rev. A*, vol. 89, no. 3, p. 032325, Mar. 2014.
[64] S. Lin, G.-D. Guo, F. Huang, and X.-F. Liu, "Quantum anonymous ranking based on the chinese remainder theorem," *Phys. Rev. A*, vol. 93, no. 1, p. 012318, Jan. 2016.
[65] Q. Wang, Y. Li, C. Yu, H. He, and K. Zhang, "Quantum anonymous ranking and selection with verifiability." *Quantum Inf. Process.*, vol. 19, no. 5, p. 166, May 2020.
[66] A. Khan, U. Khalid, Y. H. Kim, T. Q. Duong, and H. Shin, "Anonymous quantum group communication in quantum linear networks," in *Proc. Int. Conf. Industrial Netw. Intell. Syst.*, Da Nang, Vietnam, Feb. 2025, pp. 94–106.
[67] Q.-l. Wang, Y.-y. Wang, Y.-c. Li, G.-d. Li, Y.-g. Han, and L. Cheng, "A secure dynamic quantum anonymous secret sharing protocol utilizing GHZ states," *Phys. Scr.*, vol. 99, no. 10, p. 105115, Sep. 2024.
[68] A. Khan, U. Khalid, J. ur Rehman, and H. Shin, "Quantum anonymous private information retrieval for distributed networks," *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4026–4037, Jun. 2022.
[69] Y.-G. Yang, B.-X. Liu, G.-B. Xu, Y.-H. Zhou, and W.-M. Shi, "Practical quantum anonymous private information retrieval based on quantum key distribution," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 4034–4045, Jun. 2023.
[70] X. Song, Y. Liu, H. Deng, and Y. Xiao, "High-dimensional quantum threshold anonymous identity authentication scheme," *Quantum Inf. Process.*, vol. 17, no. 9, p. 214, Jul. 2018.
[71] A. Khan, J. W. Setiawan, S. N. Paing, T. Q. Duong, M. Z. Win, and H. Shin, "Controlled quantum anonymous publication," *IEEE J. Sel. Areas Commun.*, vol. 43, no. 8, pp. 2875–2889, Aug. 2025.
[72] B. A. Nguyen, "Quantum dialogue," *Physics Lett. A*, vol. 328, no. 1, pp. 6–10, Jul. 2004.
[73] S. N. Paing, F. Zaman, J. ur Rehman, K. M. Byun, J. Cho, T. Q. Duong, and H. Shin, "Counterfactual quantum protocols for dialogue, teleportation, and comparison," *IEEE Trans. Commun.*, vol. 73, no. 2, pp. 874–888, Feb. 2025.
[74] R.-h. Shi and X.-q. Fang, "Anonymous classical message transmission through various quantum networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 3, pp. 2901–2913, May 2024.
[75] G. Cariolaro, *Quantum Communications*. Cham, Switzerland.: Springer, 2015.
[76] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2017.
[77] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, Mar. 1993.
[78] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, pp. 2881–2884, Nov. 1992.
[79] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Physics*, vol. 1, no. 3, pp. 195–200, Nov. 1964.
[80] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's theorem," *Am. J. Phys.*, vol. 58, no. 12, pp. 1131–1143, Dec. 1990.
[81] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Phys. Rev. Lett.*, vol. 96, no. 7, p. 070502, Feb. 2006.
[82] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, p. 441, Jul. 2000.
[83] X.-L. Wang *et al.*, "18-qubit entanglement with six photons' three degrees of freedom," *Phys. Rev. Lett.*, vol. 120, p. 260502, Jun. 2018.

Awais Khan received his B.S. degree in Electronics Engineering from the Ghulam Ishaq Khan (GIK) Institute, Topi, Pakistan, in 2015, and his Ph.D. degree in Electronics Engineering from Kyung Hee University (KHU), South Korea, in February 2023. Since March 2023, he has been serving as a Post-doctoral Research Fellow in the Department of Electronics and Information Convergence Engineering at KHU. His research interests include quantum information science, quantum-secure communication and computation, and quantum networks.

Syed Muhammad Abuzar Rizvi received his B.S. degree in Electrical Engineering from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2018. He is currently pursuing the Ph.D. degree with the Department of Electronics and Information Convergence Engineering, Kyung Hee University, South Korea. His research interests include quantum computing, quantum machine learning, quantum communication, and quantum information science.

Trung Q. Duong (Fellow, IEEE) is currently a Canada Excellence Research Chair (CERC) and a Full Professor with Memorial University, St. John's, NL, Canada. He is also an Adjunct Professor with Queen's University Belfast, Belfast, U.K., and Kyung Hee University, Yongin-si, South Korea. From 2017 to 2019, he was a Distinguished Advisory Professor with Inje University, Gimhae, South Korea. His research interests include wireless communications, quantum machine learning, and quantum optimization. Dr. Duong was an Editor/Guest Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE COMMUNICATIONS LETTERS, IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE WIRELESS COMMUNICATIONS, IEEE COMMUNICATIONS MAGAZINES, IEEE NETWORK, and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is the Editor-in-Chief of IEEE COMMUNICATIONS SURVEYS & TUTORIALS and an IEEE ComSoc Distinguished Lecturer. He was the recipient of the Best Paper Award at the IEEE VTC-SPRING 2013, IEEE ICC 2014, IEEE GLOBECOM 2016, 2019, 2022, IEEE DSP 2017, IWCMC 2019, 2023, and 2024, and IEEE CAMAD 2023, 2024. He received two prestigious awards from the Royal Academy of Engineering (RAEng): RAEng Research Chair and the RAEng Research Fellow, and the prestigious Newton Prize 2017. He is also a fellow of the Engineering Institute of Canada (EIC), Canadian Academy of Engineering (CAE), Institution of Engineering and Technology (IET), and Asia-Pacific Artificial Intelligence Association (AAIA).

Een-Kee Hong (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Yonsei University, in 1989, 1991, and 1995, respectively. He was a Senior Research Engineer at SK Telecom, from September 1995 to February 1999, and a Visiting Senior Engineer at NTT DoCoMo, from October 1997 to December 1998. From 2006 to 2007, he was a Visiting Professor at Oregon State University. Since 1999, he has been a Professor and the Vice Dean of the College of Electronics and Information Engineering, Kyung Hee University, South Korea. His research interests include physical layer in wireless communication, radio resource management, and spectrum engineering. He received the Best Paper Award, the Institute of Information Technology Assessment, and the Haedong Best Paper Award, KICS; and the Order of Merit of the Republic of Korea for his contribution to information and communication.



Hyundong Shin (Fellow, IEEE) received the B.S. degree in Electronics Engineering from Kyung Hee University (KHU), Yongin-si, Korea, in 1999, and the M.S. and Ph.D. degrees in Electrical Engineering from Seoul National University, Seoul, Korea, in 2001 and 2004, respectively. During his postdoctoral research at the Massachusetts Institute of Technology (MIT) from 2004 to 2006, he was with the Laboratory for Information Decision Systems (LIDS). In 2006, he joined the KHU, where he is currently a Professor in the Department of Electronic Engineering. His research interests include quantum information science, wireless communication, and machine intelligence. Dr. Shin received the IEEE Communications Society's Guglielmo Marconi Prize Paper Award and William R. Bennett Prize Paper Award. He served as the Publicity Co-Chair for the IEEE PIMRC and the Technical Program Co-Chair for the IEEE WCNC and the IEEE GLOBECOM. He was an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS LETTERS.