Quantum Anonymous Networking: A Quantum Leap in Privacy

Saw Nang Paing, Jason William Setiawan, Trung Q. Duong, Dusit Niyato, Moe Z. Win, and Hyundong Shin

Abstract

Preserving privacy in communication and networking is of paramount importance in the Internet-of-Everything age of escalating surveillance and data collection. Anonymous communication is a cornerstone of this endeavor, enabling individuals to interact and exchange private information without disclosing their identities. However, achieving absolute security and privacy in classical anonymous networks (CANs) is highly challenging, and in particular, the advent of quantum computing poses critical threats to securing classical communication. In this article, we explore the evolution of CANs and delve into the distinctive shift from classical to quantum anonymous networks (QANs), emphasizing a substantial leap in privacy protected by quantum anonymous communication (QAC). The fundamental motivations behind this transition are rooted in the remarkable privacy attributes—e.g., complete *anonymity* and *untraceability*—of QAC protocols, as well as the unconditional security ensured by the principles of quantum mechanics. To make these concepts more tangible in practical settings and provide a benchmark to design the QAC protocols in QANs, we usher in exemplary protocols: quantum anonymous teleportation, voting, and information retrieval. In these case studies, we assess the fidelity and error rates of the QAC protocols in noisy environments, aiming to evaluate their robustness in practical quantum entangled settings. Moreover, we discuss the primary challenges and future research directions integral to the transition towards QANs.

Introduction

Privacy vulnerabilities escalate with the rapid expansion of the Internet, necessitating an intensified demand for secure communication across networks. While considerable attention has been focused on protecting message content to ensure that the encrypted information can only be accessible to the transmitting and receiving parties, the anonymity of network parties has received comparatively less consideration. However, concealing the identities of communicating parties remains a highly desirable feature for communication networks to protect the data and metadata of communications [1]. Anonymous networks and physical layer anonymity have gained widespread popularity in addressing these issues due to their remarkable capability to facilitate privacy-preserving secure communication while maintaining the anonymity of individuals within the network [2], [3]. The anonymous networking has become indispensable in privacy-sensitive applications such as blockchain, cryptocurrency, e-health, autonomous mobility, and e-voting [4]. By enabling individuals to engage in desired communication tasks without the fear of surveillance or censorship, these networks empower network parties to enjoy their privacy, rights, and freedoms.

Classical anonymous networks (CANs), e.g., mix networks (MixNets), the onion router (Tor), dining cryptographers networks (DCNs), and Freenet, have been recognized as a means to protect privacy and preserve anonymity in the digital realm. Despite their current attempts to provide adequate privacy and anonymity, they face fundamental limitations, such as traceability, privacy vulnerability, trusted-party dependency, and scalability [1], [2]. In contrast, the laws of quantum physics offer unique benefits for information-processing tasks in computing, networking, sensing, and cryptography [4], [5], [6], [7], [8], making it possible to substantially improve security for communication and—to protect privacy. Their recent evolutions enable us to embrace the transformative potential of quantum information engineering and distinctively transition toward the innovative realm of quantum anonymous networking [9], [10], [11], [12], [13], [14], [15].

The underlying principles of quantum mechanics, such as quantum superposition and entanglement, enable communication networks to offer unprecedented security, privacy, and anonymity. Unlike CANs that rely on computational complexity for cryptographic protocols, quantum anonymous networks (QANs) capitalize on quantum entanglement, creating unbreakable cryptographic keys that offer unconditional security. Moreover, the quantum superposition allows quantum systems to exist in multiple states at the same time, enabling quantum anonymous communication (QAC) systems to utilize multiple communication paths concurrently. This capability

Saw Nang Paing, Jason William Setiawan, and Hyundong Shin (corresponding author) are with the Department of Electronics and Information Convergence Engineering, Kyung Hee University, Yongin-si, Gyeonggi-do 17104, Republic of Korea; Trung Q. Duong is with the Department of Electrical and Computer Engineering, Memorial University of Newfoundland, St. John's, NL A1B 3X5, Canada, and also with the Department of Electronics, Electrical Engineering, and Computer Science, Queen's University Belfast, BT7 1NN Belfast, U.K.; Dusit Niyato is with the College of Computing and Data Science, Nanyang Technological University, Singapore; Moe Z. Win is with the Laboratory for Information and Decision Systems (LIDS), Massachusetts Institute of Technology, Cambridge, MA 02139 USA.

Digital Object Identifier: 10.1109/MNET.2024.3408814
Date of Current Version: 16 September 2024
Date of Publication: 3 June 2024

0890-8044/24©2024IEEE

Anonymous networks allow users to exchange messages while preserving their identity confidentiality and safeguarding message content.

effectively obscures network traffic and prevents adversaries from tracing communication origins.

Quantum resources such as Bell states, Greenberger–Horne–Zeilinger (GHZ) states, and *W* states serve as foundations for devising a range of anonymous protocols to construct QANs. These QAC protocols encompass collision detection [9], private information retrieval [10], [11], conference key agreement (CKA) [12], and veto [13]. Moreover, quantum anonymity for practical quantum networks has been examined in the presence of malicious adversaries [14]. Additionally, an application of anonymous protocols has been tangibly demonstrated on the eight-user quantum key distribution (QKD) network, enhancing QKD functionalities [15]. Besides the challenge posed by malicious adversaries, the QANs face inherent challenges, such as quantum state fragility, decoherence susceptibility, and entanglement decay. Addressing these issues is vital for its practical deployment.

In this article, we delve into the distinctive transition to QANs, highlighting a substantial quantum leap in privacy. The main contributions of the paper are outlined as follows.

- We first review privacy features, developments, and limitations of CANs.
- We explore the notable transition from classical to quantum anonymous networking and highlight the QAC protocols to build QANs and their supremacy.
- We provide numerical examples of quantum anonymous qudit teleportation, dichotomous voting, and private information retrieval in noisy environments.
- Finally, we discuss challenges in deploying the QANs and conclude with future research directions.

Classical Anonymous Networks

Anonymous networks are intricate digital networks designed to conceal the user's identity and preserve its privacy. These networks play a vital role in upholding anonymity in the digital age. We now highlight their privacy features, developments, and limitations in the classical domain.

Privacy Features

Anonymous networks allow users to exchange messages while preserving their identity confidentiality and safeguarding message content. These networks involve fundamental features such as anonymity, unlinkability, untraceability, and unobservability to guarantee the utmost privacy of network parties [2]. We delve into these fundamental attributes in detail, shedding light on their crucial role in preserving privacy and anonymity.

1) Anonymity: To enable any party in the network to communicate with others while keeping their identities concealed from each other, anonymity is a crucial feature of anonymous networks. There are typically two types of anonymity: sender anonymity and receiver anonymity, which enable users to transmit and receive messages without disclosing their identities, respectively. For an *N*-party network to achieve anonymity, it is essential that the probability that an adversary correctly identifies the source of communication tends to $1/N$. However, a dishonest subset of network users can compromise this anonymity of the network, for example, by Sybil attacks and correlation attacks. When anonymous protocols provide both internal anonymity within the network as well as protect the anonymity from external adversaries, this form of anonymity is referred to as mutual anonymity.

2) Unlinkability: In anonymous networks, users may utilize resources or services more than once. Unlinkability prevents an observer from linking different communication activities of the same party by intercepting the metadata or message contents and tracing the user activities in the network. This privacy feature can be attained by privacy-preserving techniques such as message encryption, traffic mixing, randomized routing. Without unlinkability, an observer can easily trace and monitor the activities of users, which significantly compromises their security and privacy.

3) Untraceability: In anonymous communication, untraceability is an important property closely related to unlinkability. While unlinkability prevents identifying different communication activities of users, untraceability ensures that an adversary cannot trace back to the identities of communicating parties even with access to the metadata or message contents. This privacy feature is more stringent than unlinkability for preserving anonymity in the network. In CANs, it is challenging to achieve absolute untraceability due to its inherent limitations.

4) Unobservability: In communication networks, unobservability refers to the state in which an observer cannot detect any communication occurrence. This feature is achieved by generating cover traffic, dummy traffic, or message padding, thereby making the observer unable to distinguish between actual and noise messages. In addition to covertness, unobservability guarantees that the identities of communication parties are hidden from the observer as he cannot determine if any user is actively sending a message or simply in an idle state.

These four privacy features are interrelated, as illustrated in Fig 1. Unlinkability ensures that different actions or messages cannot be linked to the same user. If actions or messages are unlinkable, it becomes challenging or impossible to trace a specific action or message back to its source, thus achieving sender and receiver untraceability. A stricter condition than unlinkability and untraceability is unobservability, which hides both the source and existence of actions through message unobservability and the use of stealth addresses—random one-time addresses. When messages or actions are unlinkable or unobservable, or when the source of the message cannot be traced, it enables the anonymity of the sender or receiver, consequently facilitating identity separation.

Developments

Fig. 1 illustrates the evolution of principal anonymous networks over time. Specifically, anonymous networks can be classified into distributed networks, mix networks and peer-to-peer networks.

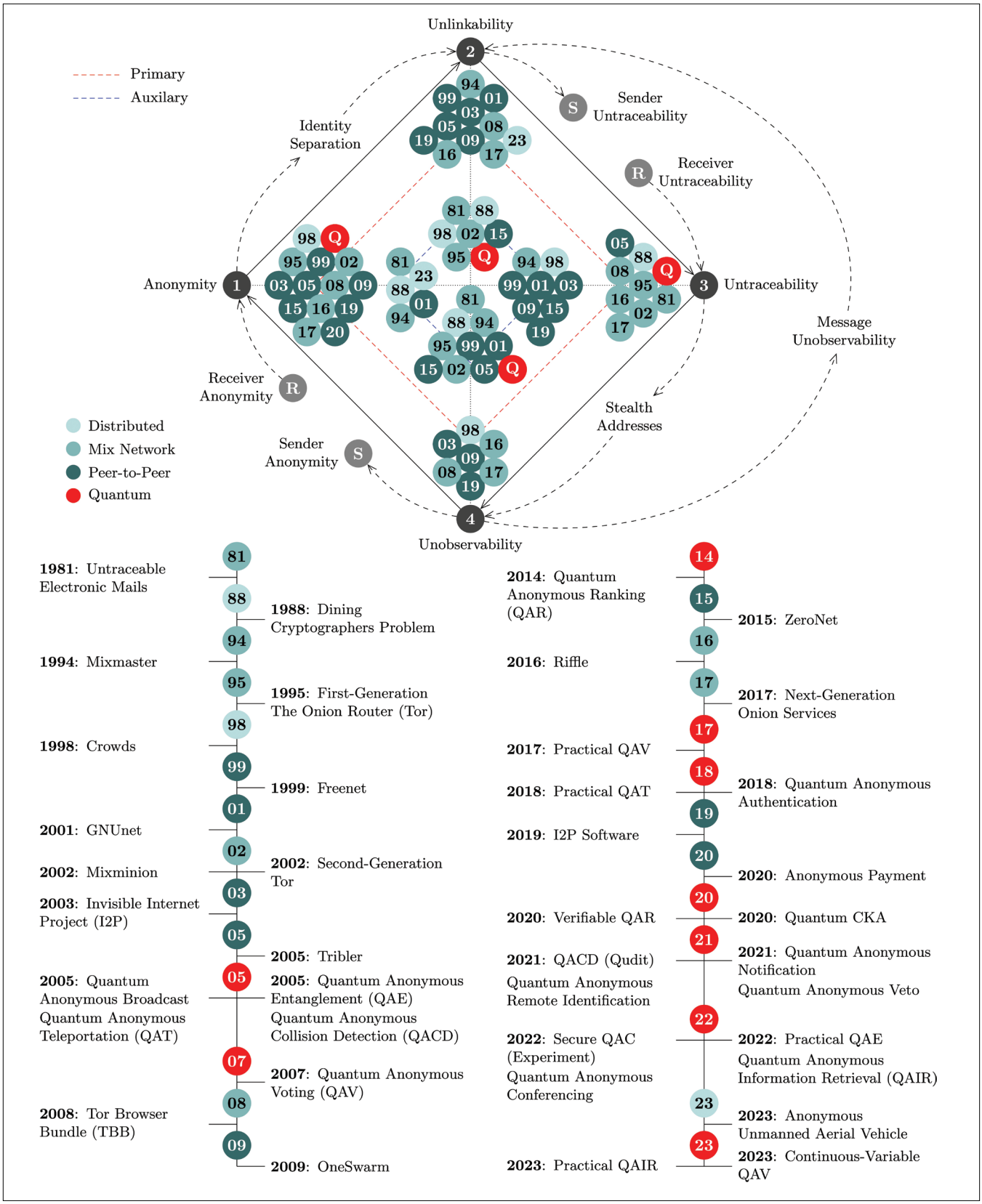

FIGURE 1. The evolution of CANs and the development of QAC protocols. The classical deployments include distributed networks, Mix networks, and peer-to-peer networks, ranging from untraceable electronic mail systems to anonymous unmanned aerial vehicles, while the QAC protocols for QANs include broadcast, entanglement, teleportation, collision detection, voting, ranking, authentication, CKA, notification, veto, remote identification, conferencing, and private information retrieval. Anonymous networks are characterized by four fundamental privacy features: anonymity, unlinkability, untraceability, and unobservability. We delineate the primary and auxiliary privacy features for each anonymous protocol, denoted by red and blue dashed lines, respectively. The interrelation of these features differs across anonymous networks based on their architectures. For instance, the QANs, marked by a red circle, prioritize anonymity and untraceability as primary features, while unlinkability and unobservability are considered auxiliary features.

In contrast to the CANs, the QANs ensure complete untraceability or tracelessness by quantum principles.

A detailed insight into notable CAN instances for these categories is described as follows.

1) Distributed Network: A distributed network utilizes decentralized architecture where the control is spread across all participants. In this network, user anonymity is achieved through cryptographic techniques, peer-to-peer communication, and distributed trust. An instance of anonymous distributed networks is described below.

- **Dining Cryptographers Networks:** The DCN protocol is designed for anonymous and untraceable communication, where network parties can send messages anonymously using broadcast or multicast communication. This protocol involves pairs of participants sharing a secret coin flip and calculating a modulo sum of their values. A network party that wants to send a message flips its value and broadcasts it. Unlike mix protocols that require trusted servers for mixing and relaying, the DCN classes operate without requiring a trusted third party (TTP). However, when a network subgroup conspires to break the communication anonymity by coordinating their coin flips or sharing information outside the protocol, it leads to a breach of anonymity. Built upon the DCN principle, Crowds is another privacy-preserving protocol especially designed for anonymous web browsing.

2) Mix Network: A mix network is designated to enhance privacy by routing data through a sequence of intermediate nodes, thereby obscuring the connection between the sender and the receiver. Below are some examples of mix networks.

- **MixNet:** Using the concept of mix nodes, which mix the received packets and hide the message input-output communication path by means of strong cryptography, the MixNets have been introduced to achieve sender anonymity. The mix nodes act as relays for the message and strip the message's identity. The first implementation is called untraceable electronic mails or Type-1 anonymous remailers. The Type-1 anonymous remailers provide unlinkability between the message and the sender-receiver pairs. The next one is Mixmaster, also known as Type-2 anonymous remailers, which introduce additional mixing to the message, such as message padding and mixing. The improved version of the Mixmaster is called Mixminion, also known as Type-3 anonymous remailers, which provide link encryption for the anonymity of forwarded messages. In addition to the forward anonymity, Type-3 also provides the ability to receive and pass messages anonymously by creating an anonymous return address. On the other hand, the MixNets rely on a large number of servers to function properly. If one of these servers is compromised, it might lead to privacy and trust violations in the network.
- **The Onion Router:** As a noteworthy alternative to the MixNets, the first-generation Tor has been introduced in the realm of circuit-based routing. This network operates with a series of servers referred to as onion routers to transmit data to a destination using fixed-size cells of the circuit network. These cells are then encrypted using multiple layers—much like the layers of an onion—and each layer is removed at the designated nodes. This innovation laid the foundation for the second-generation Tor, Tor Browser Bundle, the next-generation onion services and Riffle. The inherent design of Tor serves as a countermeasure against traffic analysis attacks by obscuring the predecessor and successor of individual data packets from potential eavesdroppers. However, the challenge of preserving anonymity arises if an adversary takes control over a significant portion of the network due to its reliance on intermediate nodes.

3) Peer-to-Peer Network: A peer-to-peer network uses a decentralized architecture, allowing participating nodes to function as both clients and servers. In this network, user anonymity can be achieved through privacy-enhancing measures such as random routing, data encryption and distributed storage. Freenet is one of the examples of peer-to-peer network.

- **Freenet:** Using a process called anonymous publication, Freenet is designed as a peer-to-peer network to enable the anonymous publishing and retrieval of information. When a party uploads data to Freenet, this information is split into small encrypted chunks and distributed across different parties in the network for storage. This makes it challenging for anyone to trace the true origin of the information. Whenever a party wants to retrieve a particular data, Freenet runs a complicated routing algorithm to locate the encrypted chunks of the requested data while keeping the party's identity concealed from the rest of the network. The party can then use its private key to decrypt the data and retrieve the information. Essentially, the structure of Freenet depends on data distributions across multiple parties to ensure privacy, anonymity, and access to shared information. However, if certain parties are compromised, it causes the risk of data loss. Other alternative network stacks for building privacy-preserving peer-to-peer networks include I2P, GNUnet, OneSwarm, Tribler, and ZeroNet.

Limitations

Although CANs offer a degree of privacy and anonymity, there are classical limitations to their effectiveness in providing stringent privacy and anonymity.

1) Lack of Complete Untraceability: The CANs, such as Tor, utilize relays to transfer information from one party to another while maintaining anonymity using encryption methods applied to the transmitted packet. Upon reaching a relay, the message is decrypted by the

relay to determine the destination party and is then encrypted again before being forwarded. To further enhance anonymity, some delay can be introduced during packet transmission. However, an adversary can use predetermined attack metrics to conduct traffic analysis attacks on the ingress and egress traffic or collude with a subset of network parties to intercept communication. By analyzing the traffic streams, the attacker can correlate them to identify the communicating parties. Hence, despite providing some level of anonymity, the CANs cannot guarantee the complete untraceability of anonymous communication [1].

2) Deanonymization: Despite anonymization techniques in anonymous networks, adversaries attempt to uncover the identities of parties using various types of attacks such as exit node attacks, traffic analysis attacks, timing attacks, and social engineering [1]. If the user identity is successfully deanonymized, the adversary can subsequently learn the identities of other users, thereby obtaining sensitive data such as login credentials and financial information. Therefore, protecting against deanonymization is crucial for upholding security and privacy of all parties in the network.

3) Quantum Cryptographic Attacks: The CANs utilize public cryptographic methods such as Rivest–Shamir–Adleman (RSA) and Diffie-Hellman algorithms, based on complex calculation problems. With the unprecedented growth of quantum computing, quantum attacks pose significant threats to security and privacy of CANs. Quantum cryptography can potentially undermine the security measures in place for decades. For instance, it would take a classical computer 13.7 billion years to break an RSA-2048 cipher, while a quantum computer using Shor's algorithm could accomplish the same task in just 42 minutes.

4) TTP Dependency: Apart from distributed networks, the CANs often rely on TTPs to ensure the proper functioning and security of the network. TTPs can take a variety of forms, including central services, certification authorities, or intermediary nodes responsible for message routing and mixing. However, the dependence on such TTPs introduces risks and potential vulnerabilities to security and privacy. A dishonest TTP can act as a single point of failure, disrupting the entire network and compromising user's identities, message integrity, and overall network security. Thus, addressing the dependence on TTPs is a crucial challenge in anonymous networks.

5) Scalability: One of the notable CAN limitations is scalability. Tor, for instance, introduces substantial communication overhead due to multiple layers of encryption and decryption to preserve anonymity. This overhead increases the size of transmitted data, leading to growing bandwidth utilization and network latency. Scalability is also influenced by the expansion of the anonymity set, which enhances anonymity and reduces the risk of correlation attacks. This expansion entails accommodating more participants in the network, thereby placing additional requirements on computational and storage resources as well as burdening the network infrastructure. Therefore, addressing scalability requires considering the network infrastructure, resource management, and communication overhead to balance security, privacy, and anonymity.

Quantum Anonymous Networks

With inspiration from classical counterparts, QANs harness the principles of quantum mechanics to revolutionize communication anonymity.

Quantum Anonymity

Quantum anonymity is a cutting-edge paradigm in information security that uses the unique properties of quantum mechanics to protect sensitive data. This breakthrough provides unparalleled privacy and anonymity, outperforming the classical solutions. In the following discussion, we explore the fundamentals and quantum protocols for QANs.

1) Fundamentals: In contrast to CANs that involve sending anonymous messages as bit strings, a new form of information carriers, known as quantum states, is used for anonymous message transmission in QANs. In these networks, quantum nodes play a fundamental role in generating, manipulating, and measuring quantum states. These nodes are interconnected by quantum communication channels to facilitate the transmission of quantum states. When communicating parties are significantly separated, quantum relays can be used as intermediaries for efficient routing between distant communicating parties. The fundamentals of quantum communication are rooted in the distinctive characteristics of quantum mechanics, including the quantum superposition, entanglement, no-cloning theorem, and uncertainty principle. These properties form the foundation for secure and unique information transmission in the QANs [14].

2) Transition from Classical to Quantum: The transition from classical to quantum anonymous networking requires incorporating quantum principles and anonymous protocols into the infrastructure of anonymous networks. It is not feasible to replace the entire network infrastructure with quantum components as quantum networks are still in their nascent development stages. Therefore, integrating quantum elements and protocols into anonymous networks becomes a crucial step in enabling this transition and enhancing security and privacy of the network.

- **Quantum-Classical Interface:** To establish a connection between classical and quantum channels, a quantum-classical interface is needed. By incorporating quantum memory for the temporary storage and retrieval of quantum states, this interface facilitates the conversion of classical bits into quantum states and vice versa. Recently, a quantum network program of a low-level instruction set architecture, known as NetQASM, enables the integration between classical communication and quantum operation. To effectively utilize the NetQASM, communicating nodes must be equipped with both classical and quantum processing units. Using the QAC protocols, quantum states converted by the interface are decoded by the quantum-capable end nodes and converted back to classical bits by the interface. As a result, the interface enables seamless integration of quantum nodes into the classical network infrastructure, making it possible to use the QAC protocols for

quantum-empowered security, privacy, and anonymity.

- **Hybrid Quantum-Classical Network:** Integrating quantum anonymous networks into existing classical infrastructure involves implementing quantum key distribution (QKD) for secure key generation and encryption, deploying quantum repeaters to extend communication range, and utilizing quantum-classical interface for seamless interaction between classical and quantum domains. The classical network stack typically encompasses the Open Systems Interconnection (OSI) layers, while the quantum network stack comprises the physical layer for qubit transmission, quantum link layer for the generation of entanglement between network nodes, and quantum network layer for routing. Recently, the integration of quantum simulation (QuNetSim) and classical network emulation (ComsNetsEmu) was demonstrated, which integrates the quantum link layer and physical layer to the existing classical network stack. In this setup, a bridge interface is used to route the network layer traffic to QuNetSim and back to ComsNetsEmu. Source node packets are disassembled into binary streams, encoded into QuNetSim's link layer states, and transmitted to the receiver. Upon reception, qubits are decoded at the receiver's QuNetSim link layer. Finally, the network-layer packet is reassembled and routed through the bridge. This setup can be extended for multiple users scenarios to perform QAC protocols, distributing GHZ states among them and executing desired QAC protocols based on these states.
- **Quantum Encryption and Hybrid Routing:** Quantum encryption techniques, such as QKD, quantum one-time pads, and quantum key encapsulation mechanisms can be integrated into CANs to secure anonymous communication channels with encryption keys. For instance, the security and privacy of DCN is threatened by the advancements of quantum computing. Its security and privacy can be enhanced by using QKD and QAC protocols. This includes discreetly broadcasting information through quantum anonymous broadcast, utilizing the quantum anonymous vetoing protocol for binary decision-making while maintaining anonymity, employing QAN to inform groups without revealing identities, implementing quantum anonymous collision detection to verify a single sender, and utilizing quantum anonymous information retrieval to exchange encrypted messages while shielding sender and receiver identities, ensuring robust security and privacy within the cryptographic context [15]. In addition, variational quantum algorithms such as quantum annealing and the quantum approximate optimization algorithm can be exploited in CANs to optimize routing decisions in a manner that minimizes the exposure of sensitive information. Classical routing algorithms alone may not fully optimize the network in anonymous scenarios. In this setup, the classical routing components can still be used for routine tasks.

QAC Protocols

The QAC protocols form the foundation for the QANs (see Fig. 1). We succinctly present anonymous broadcasting, entangling, teleporting, voting, and information-retrieving quantum protocols, highlighting their features and functionalities.

1) Anonymous Data Disseminating: QAB, often referred to as anonymous data dissemination, allows Alice (or any party) to anonymously broadcast her classical symbol to all other nodes in the N-party network without revealing her identity. This anonymous and untraceable broadcast is crucial for anonymous teleportation. Specifically, using a preshared N-partite d-dimensional maximally entangled state (i.e., *broadcast carrier*), the QAB protocol takes the Fourier-basis measurement, digit-shift operation, classical announcement, and modulo d sum calculation for the anonymous broadcast of d-ary symbol information.

- **Broadcast Carrier:** All the N parties in the network, including Alice, initially share an N-partite d-dimensional entangled GHZ state. By applying the d-dimensional quantum Fourier transform (QFT) gate $\boldsymbol{\mathcal{F}}_d$ to the first qudit and then sequentially performing controlled d-dimensional Weyl-x, i.e., digit-shift $\boldsymbol{X}_d^j$ gates with the first qudit as the control and each of the subsequent qudits as the target, the N-qudit system is prepared in the N-partite d-dimensional maximally entangled state. In this controlled digit-shift operation, if the control qudit is in the state $|j\rangle$, the target qudit is shifted by j in the computational basis applying j times the d-dimensional digit-shift Weyl gate $\boldsymbol{X}_d$. These entangled N qudits are distributed across the network participants—serving as a broadcast carrier.
- **Broadcast Modulation:** Alice (broadcast party) performs $\boldsymbol{X}_d^{\zeta}$ on her qudit to modulate the broadcast information ζ in a classical d-ary symbol, i.e., the broadcast party applies the digit-shift Weyl operator $\boldsymbol{X}_d$ ζ times to her qudit state. The other network parties apply the d-dimensional identity operator $\boldsymbol{I}_d$ on their qudits, i.e., leave the qudit states as they are. All the network parties (including Alice) then perform the QFT operation $\boldsymbol{\mathcal{F}}_d$ on their respective qudits. Due to the QFT and digit-shift operations, this modulated state is in the even superposition of all d^{N-1} N-qudit states whose modulo d sum is equal to the broadcast symbol ζ.
- **Broadcast Detection:** All the N network parties measure their qudits in the computational basis and get their d-ary outcomes $\mu_1, \mu_2, \ldots, \mu_N$. The modulo d sum of all these measurement outcomes is equal to the broadcast information ζ—due to the symmetry of the modulated state from Alice's digit-shift operation. These N-tuple d-ary outcomes appear randomly with an equal probability of $1/d^{N-1}$ due to the basis change from the QFT operations, even for the entangled state between the

N network parties. This randomness completely conceals the fact that Alice has broadcast the symbol ζ by digit-shifting her qudit state. Now, all the parties utilize classical communication to announce their measurement outcomes. Finally, any recipient party calculates the modulo d sum of all announced measurement outcomes to recover the broadcast symbol without revealing the broadcaster's identity, i.e., Alice.

In this protocol, Alice's broadcast modulation, represented by her local operation $\boldsymbol{X}_d^{\zeta}$, alters the global state's phase, which cannot be determined by anyone else in the network. At this point, each party has equal chance of being a sender as the reduced density matrix is identical for all parties. Additionally, the superposition of all d^{N-1} N-qudit states resulted from the QFT operations by each party introduces the uncertainty for each qudit. As a result, the measurement outcomes during the broadcast detection phase are inherently random, determined by the probabilistic nature of quantum mechanics. Despite the classical announcements of measurment outcomes being dependent on the global state, this inherent randomness completely obscures any traces of Alice—thus preserving anonymity and untraceability throughout the broadcast process.

2) Anonymous Multiparty Entangling: The quantum anonymous entanglement (QAE) allows Alice and Bob_i (or any K-party subgroup), $i = 1, 2, \ldots, K-1, K < N$, in the N-party network to anonymously share the K-partite d-dimensional maximally entangled GHZ state without revealing their identities. This anonymous and untraceable entanglement is also crucial for anonymous teleportation and private information retrieval. Specifically, using a preshared N-partite d-dimensional maximally entangled GHZ state (i.e., *entangling anonymizer*), the QAE protocol takes the Fourier-basis measurement, random symbol generation, classical announcement, and phase-removal operation to anonymize multipartite d-dimensional maximal entangling among Alice and Bobs.

- **GHZ Anonymization:** All $N-K$ network parties, except the anonymizing subgroup (Alice and Bobs), start the protocol by performing the QFT operation $\boldsymbol{\mathcal{F}}_d$ on their respective qudits. Then, these parties perform the computational basis measurement on their respective qudits and get their d-ary outcomes $\mu_1, \mu_2, \ldots, \mu_{N-K}$, while Bobs and Alice generate their random d-ary uniform symbols $\lambda_1, \lambda_2, \ldots, \lambda_K$. The $(N-K)$-tuple d-ary outcomes appear randomly with an equal probability of $1/d^{N-K}$ due to the QFT operations. This complete randomness hides the fact that the subgroup parties have generated the random symbols without measuring their qudits to anonymize the maximal multipartite entanglement among Alice and $K-1$ Bobs.
- **Anonymous Entanglement:** All N network parties announce their measurement outcomes $\mu_1, \mu_2, \ldots, \mu_{N-K}$ or random symbols $\lambda_1, \lambda_2, \ldots, \lambda_K$ using classical communication. Alice now calculates the modulo d sum $\hat{\mu}$ of all announced d-ary information $\mu_1, \mu_2, \ldots, \mu_{N-K}$ and $\lambda_1, \lambda_2, \ldots, \lambda_{K-1}$ received from other network parties. Finally, Alice and $K-1$ Bob_i perform the d-dimensional Weyl-z, i.e., phase-shift operators $\boldsymbol{Z}_d^{-\hat{\mu}}$ and $\boldsymbol{Z}_d^{\lambda_i}$ on their respective qudits conditionally to correct the measurement phase. Now, the K-partite d-dimensional maximally entangled GHZ state is anonymously shared among the K-party subgroup (Alice and Bobs) without revealing their identities.

The qubits of the anonymizing subgroup remain untouched during the GHZ anonymization stage while other parties are unaware of it. As the announced outcomes by all N network parties are completely random, no one can determine who is involving in the generation of anonymous entanglement, thus leaving no traces of anonymizing subgroup. The phase correction operations performed by the anonymizing group, denoted by $\boldsymbol{Z}_d^{-\hat{\mu}}$ and $\boldsymbol{Z}_d^{\lambda_i}$, are also local operations, unknown to other parties. Thus the anonymous multiparty entangling process guarantees anonymity and untraceability.

3) Anonymous Qudit Teleporting: The quantum anonymous teleportation (QAT) allows Alice (or any sending party) to anonymously teleport her arbitrary (known or unknown) d-dimensional qudit state to Bob (or any receiving party) without revealing their identities. Specifically, using three preshared N-partite d-dimensional maximally entangled GHZ states (i.e., one entangling anonymizer and two QAB carriers), the QAT protocol takes anonymous d-dimensional Bell pairing, d-dimensional Bell-basis (Weyl-basis) measurement, anonymous d-ary symbol announcement, and qudit reconstruction to anonymize qudit teleportation from Alice to Bob (see Fig. 2).

- **Anonymous *d*-Dimensional Bell Pairing (QAE):** Alice and Bob anonymously share the d-dimensional maximally entangled Bell pair by running the QAE protocol ($K = 2$) using one preshared N-partite d-dimensional GHZ state—i.e., the entangling anonymizer.
- **Weyl-Basis Measurement:** Alice applies the controlled digit-shift Weyl gate, i.e., the d-dimensional controlled-NOT (CNOT) gate between her teleporting qudit (control) $|\psi\rangle_{\text{T}}$ and her member qudit (target) of the d-dimensional entangled Bell pair for Weyl-basis measurement. Now, Alice performs the QFT operation on her teleporting qudit possession to change the basis. Subsequently, Alice measures both qudits in the computational basis and obtains the d-ary measurement outcomes μ_{T} and μ_{A} of the teleporting and Bell-pair member qudits,respectively.
- **Anonymous Symbol Announcement (QAB):** Alice announces her two measurement outcomes (d-ary symbols) μ_{T} and μ_{A} anonymously to Bob with two runs of the QAB protocol using two preshared N-partite d-dimensional GHZ states (i.e., two broadcast carriers). Bob gets $\hat{\mu}_{\text{T}}$ and $\hat{\mu}_{\text{A}}$ from these QABs. This classical symbol information is required for Bob to correct (remove) the phase and/or digit shifts in his qudit state.

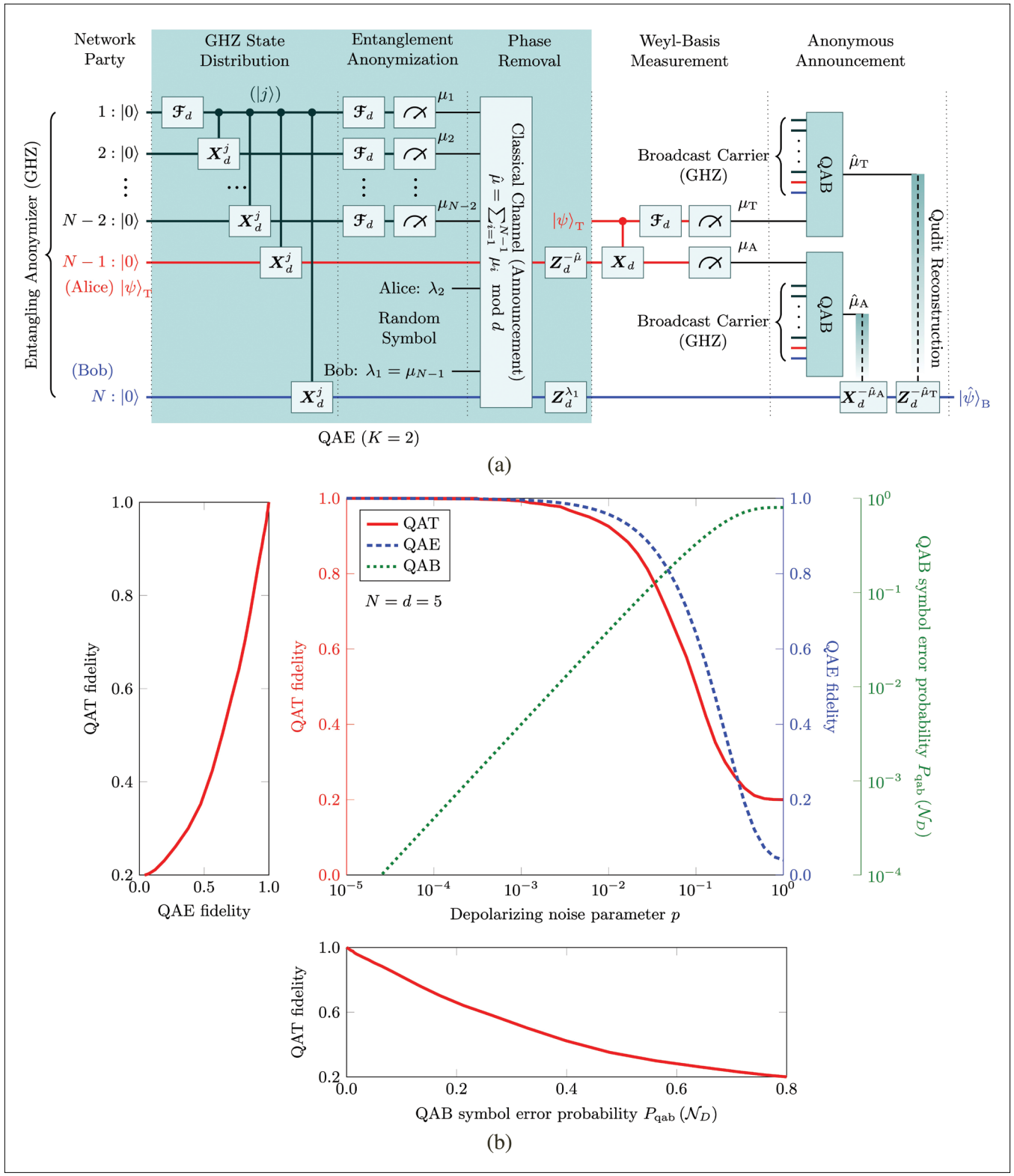

FIGURE 2. Quantum anonymous qudit teleportation in an N-party network. (a) Using three N-partite d-dimensional GHZ states, the QAT protocol successively performs the QAE (GHZ state distribution, entanglement anonymization, and phase removal), Weyl-basis measurement, and anonymous symbol announcements (two QABs) to teleport a qudit state $|\psi\rangle_T$ anonymously while concealing identities of a teleporting pair (Alice and Bob). (b) The QAT protocol is evaluated when $N = d = 5$ for noisy GHZ states (entangling anonymizer and two broadcast carriers) under the depolarizing noise $\mathcal{N}_D(\boldsymbol{\rho}) = q\boldsymbol{\rho} + p\mathbf{I}_d/d$ with the noise parameter $p \in [0, 1]$ where $q = 1 - p$. The qudit QAT fidelity between $|\psi\rangle_T$ and $|\hat{\psi}\rangle_B$ is plotted as a function of the depolarizing parameter p (upper right). The QAB symbol error probability $P_{qab}(\mathcal{N}_D)$ for the anonymous announcement of μ_T or μ_A and the QAE fidelity for qudit Bell pairing are also plotted as a function of the noise parameter p. With depolarizing probability p, we have $P_{qab}(\mathcal{N}_D)/Q_d = 1 - q^N$ and its asymptote $P_{qab}(\mathcal{N}_D)/Q_d = pN + o(p)$ as $p \to 0$, where $Q_d = 1 - 1/d$. In addition, the qudit QAT fidelity is depicted as a function of the QAE fidelity (upper left) and the QAB $P_{qab}(\mathcal{N}_D)$ (lower right) where the GHZ states are subject to the depolarizing noise for only the entangling anonymizer and two broadcast carriers, respectively.

- **Qudit Reconstruction:** Bob finally corrects the phase and digit shifts by applying d-dimensional Weyl operators $\boldsymbol{Z}_d^{-\hat{\mu}_T}$ and $\boldsymbol{Z}_d^{-\hat{\mu}_A}$ on his qudit state to reconstruct the teleporting qudit state $|\hat{\psi}\rangle_B$ using the measurement outcomes announced by Alice. This QAT protocol completely conceals the teleportation pair, i.e., both Alice and Bob.

The QAT protocol follows the steps of conventional teleportation. It replaces the initial shared entanglement between Alice and Bob with anonymous Bell pairing, facilitated by QAE, and uses QAB to communicate d-ary measurement outcomes. As no additional information is disclosed during the teleporation process, it upholds the anonymity and untraceability by inheriting these properties from the QAE and QAB protocols.

Case Study: To demonstrate the noise effect on the QAT protocol as depicted in Fig. 2(a), we assess the QAT fidelity under the depolarizing noise $\mathcal{N}_D$. This isotropic quantum noise involves introducing random phase and digit shifts to quantum states. Specifically, the depolarizing noise map $\mathcal{N}_D$, characterized by the depolarizing probability $p \in [0,1]$, evolves a quantum state into a completely mixed state with probability p and leaves it unchanged with probability $1-p$. Additionally, we consider two hyperparameters, which are the number of parties N and the dimensionality of the qudit d. In order to demonstrate high dimensionality effect as compared to previously studied qubit protocol, we choose $d = 5$. As the parameter describes N-partite d-dimensional GHZ state, its implementation can be done using photon path or orbital angular momentum, or other degree of freedom. However, due to the expensive resource required to perform Monte Carlo simulation of multiple qudit systems, we consider $N = 5$ to depict a small-scale quantum network, which aligns with the current status of experimental realization of quantum networks.

Fig. 2(b) shows the qudit QAT fidelity between $|\psi\rangle_T$ and $|\hat{\psi}\rangle_B$ along with the subprotocol performances (QAE fidelity and QAB symbol error probability) as a function of the depolarizing parameter p when $N = d = 5$ for noisy entangling anonymizer and two broadcast carriers. We also ascertain the effect of each noisy subprotocol on the QAT fidelity (upper left and lower right). Fig. 2(b) shows that the QAT protocol exhibits robustness to the depolarizing noise up to approximately $p = 10^{-3}$.

As the teleportation fidelity depends on the input quantum state, we calculate the average fidelity of the teleported state depicted by QAT fidelity. As seen from the upper left figure, the anonymous entanglement fidelity determines the quality of the QAT fidelity. Teleportation requires an shared entanglement between sender and receiver. When the shared entanglement is perfect, we can perform teleportation to transfer the input state by performing Bell basis measurement depicted as Controlled $\boldsymbol{X}_d$ gate along with Fourier transformation. However, when the shared entanglement is disturbed due to noise, the teleported state will not always be the same as the input state, which reduces the overall average QAT fidelity.

For the QAB subprotocol, the error in measurement announcements causes error in the correction performed by the receiver, which can give a teleported state orthogonal to the input state. This will give zero fidelity, which also reduces the overall average QAT fidelity.

4) Anonymous Dichotomous Voting: Quantum anonymous voting (QAV) allows $N-1$ voting parties (say, Bob_i, $i = 1, 2, \ldots N-1$) to anonymously cast their binary (yes or no) votes v_i and one central authority (say, Alice) to count yes votes without revealing their identities. Specifically, using an N-dimensional Bell pair (i.e., *voting carrier* or *quantum ballot*), the QAV protocol takes the N-dimensional digit-shift Weyl operation and the projective (von Neumann) quantum measurement in the entangled basis for voting modulation and decision (see Fig. 3).

- **Quantum Ballot:** Alice (central authority) prepares the N-dimensional entangled Bell state, holds the first qudit, and sends the second ballot qudit to the first voting party Bob_1. This entangled ballot qudit is sequentially traveled across the voting parties (Bobs) to cast their votes using quantum state transfer.
- **Voting Modulation:** The first voting party Bob_1 performs the N-dimensional digit-shift Weyl operation $\boldsymbol{X}_N^{v_1}$ on the ballot qudit conditionally to modulate his vote v_1, i.e., if Bob_1 votes yes, he applies the digit-shift Weyl operator $\boldsymbol{X}_N$ on the ballot state; otherwise, he leaves the ballot state as it is. Now, Bob_1 sends this modulated ballot qudit to the next voting party Bob_2. All $N-1$ voting parties, Bob_i, sequentially modulate their votes v_i by performing $\boldsymbol{X}_N^{v_i}$ on the traveling ballot qudit. Then, the count $v = \sum_{i=1}^{N-1} v_i$ of yes votes is modulated on the ballot qudit state.
- **Voting Decision:** The final voting party Bob_{N-1} sends the modulated ballot qudit back to Alice for the voting decision. Finally, Alice measures the qudit pair in the entangled basis to demodulate the dichotomous voting count and announces the measurement outcome $\hat{v}$ as the ballot count of yes voting without revealing the voting outcomes of any parties. Note that during the entire time that the ballot qudit is traveling, the reduced density matrix of the N-dimensional entangled state is in the maximally mixed state. This randomness completely conceals all the voting outcomes—thus preserving privacy (anonymity and untraceability) in the voting process.

In this protocol, the total number of yes votes can only be determined with collective measurement done by Alice. Each individual vote, although cast on the traveling ballot qudit, is stored within the correlations of the entangled Bell state. Thus, the traveling ballot qudit does not disclose any information about individual votes. Attempts to tamper with individual votes through attacks such as measurement and resend attack on the traveling ballot qudit is ineffective. Consequently, the voting process ensures to preserve the voting privacy (anonymity and untraceabiliy) of each party.

Case Study: Fig. 3(a) illustrates the QAV protocol and Fig. 3(b) depicts the QAV tally error probability P_{qav} ($\mathcal{N}_Z$) for the noisy quantum ballot

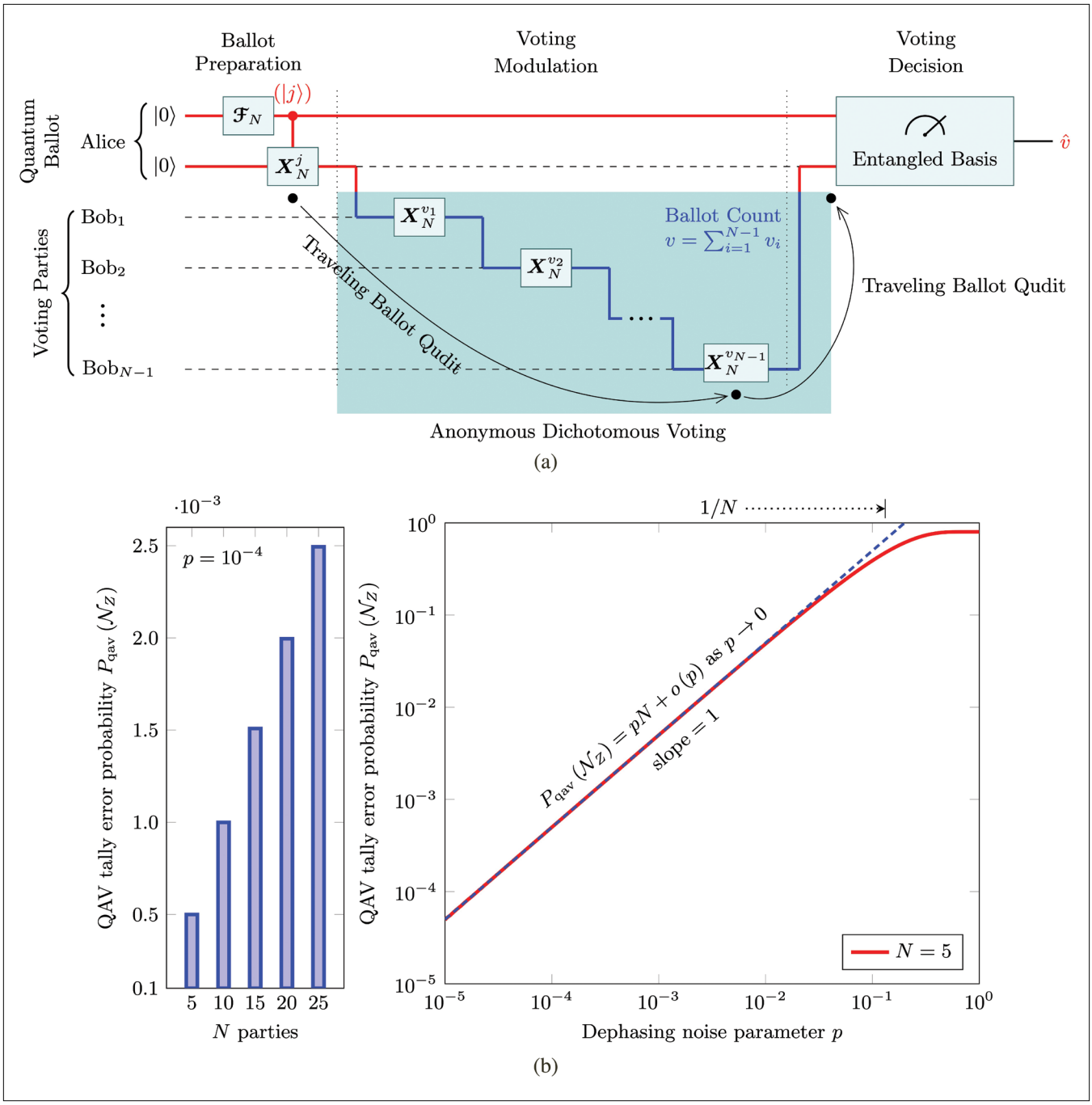

FIGURE 3. Quantum anonymous dichotomous voting in an N-party network. (a) Using an N-dimensional Bell state, the QAV protocol successively performs the ballot preparation (Alice), voting modulation (Bobs), and voting decision (Alice) to count yes votes v without revealing the vote casts of any parties (Bobs). (b) The QAV protocol is evaluated for the noisy N-dimensional Bell state (quantum ballot) under the dephasing noise $\mathcal{N}_Z(\boldsymbol{\rho}) = (1-p)\boldsymbol{\rho} + p/\left(N-1\right)\sum_{k=1}^{N-1} \boldsymbol{Z}_N^k \boldsymbol{\rho} \boldsymbol{Z}_N^{-k}$ with the noise parameter $p \in [0, 1]$. The QAV tally error probability $P_{\text{qav}}(\mathcal{N}_Z)$ is plotted as a function of the number N of network parties when $p = 10^{-4}$ (left) and the dephasing parameter p when $N = 5$ (right). With dephasing probability p, we have $P_{\text{qav}}(\mathcal{N}_Z)/Q_N = 1-(1-p/Q_N)^N$ and its asymptote $P_{\text{qav}}(\mathcal{N}_Z) = pN + o(p)$ as $p \to 0$.

under the dephasing noise $\mathcal{N}_Z$. We choose the hyperparameter to be $N = 5$, which depicts 4 voters with qudit of dimensions $d = 5$. In general we can choose the dimensionality to be at least higher than the number of voters. In our case of study, we choose d to be number of voters plus one, which is the minimum dimensions needed to run the QAV protocol. Similar with previous case study, N is chosen to depict small scale quantum network.

The dephasing noise map $\mathcal{N}_Z$ primarily erodes the coherence between the different basis states without affecting their populations, i.e., the phase information of a qudit state is degraded while the probability of measuring each basis state remains unchanced. Fig. 3(b) shows that the QAV error $P_{\text{qav}}(\mathcal{N}_Z)$ scales linearly with the dephasing probability p and the network size N in the low-noise regime.

5) Anonymous Information Retrieving: QAIR allows Alice (or any querying party) to

anonymously retrieve private binary information $\mathcal{B}(x)$ at index $x \in \{1, 2, \ldots, d-1\}$ from the database held by Bob (or any serving party) while keeping their identities concealed from the network of N parties. Specifically, using six preshared N-partite d-dimensional GHZ states, the QAIR protocol takes two sets of anonymous d-dimensional Bell pairing (i.e., *query carrier* and *response carrier*), the phase-flip Oracle operation, four runs of the QAB protocol, and the orthonormal state discrimination to anonymously teleport query and response qudit states for private information retrieval (see Fig. 4).

- **Retrieving Carrier (QAE):** Alice and Bob anonymously share two d-dimensional maximally entangled Bell pairs with two runs of the QAE protocol ($K = 2$) using two preshared N-partite d-dimensional GHZ states. These two d-dimensional anonymous Bell pairs—i.e., query and response carriers—serve as anonymous qudit teleportation links for the private information query and response, respectively.
- **Query and Response Teleportation (QAT):** Alice prepares the d-dimensional query qudit state $|\psi\rangle_A$ to modulate the d-ary query index x in a superposition state of the basis states $|0\rangle$ and $|x\rangle$, e.g., $|\psi\rangle_A = |x_0\rangle$ where $\sqrt{2}\,|x_b\rangle = |0\rangle + (-1)^b\,|x\rangle$ for b = 0, 1. Subsequently, Alice teleports this modulated state to Bob anonymously and untraceably using the QAT protocol on the first d-dimensional anonymous Bell pair (query carrier). Then, Bob performs the Oracle operation $\mathcal{O}$ on the teleported query state $|\hat{\psi}\rangle_B$ to prepare the response qudit state $|\varphi\rangle_B$. The Oracle operation $\mathcal{O}$ modulates database information $\mathcal{B}(x)$ at index x on $|\varphi\rangle_B$ by flipping the phase of the basis state $|x\rangle$ conditioned on the query information as $|\varphi\rangle_B = |x_{\mathcal{B}(x)}\rangle$. Bob teleports the response state $|\varphi\rangle_B$ back to Alice anonymously and untraceably using the QAT protocol on the second d-dimensional anonymous Bell pair (response carrier). Note that all other network parties, including Bob, are not aware of the identity of Alice as well as the index of the query information Alice wants to retrieve.
- **Response Retrieval:** Alice demodulates Bob's response message by distinguishing the phase of the basis $|x\rangle$ in the teleported response qudit $|\hat{\phi}\rangle_A$. Alice detects the database information at index x by determining if the teleported response state is equal to the original query state $|\psi\rangle_A$ or its orthonormal state $|x_1\rangle$. With the projective measurement for orthonormal state discrimination, Alice anonymously retrieves the private information of Bob's database at index x as $\hat{\mathcal{B}}(x) = b$ if $|\hat{\phi}\rangle_A = |x_b\rangle$. The QAIR protocol guarantees to hide the identities of the information retrieval pair in the network by leveraging the QAE and QAT protocols.

In this QAIR protocol, the retrieving carrier process facilitated by QAE ensures that the identities of both Alice and Bob remain hidden. In addition, the QAT protocol used for query state transmission and response state transmission gaurantees to leave no traces of anonymous communication between Alice and Bob. Furthermore, the Oracle operation performed by Bob has no affect on the anonymity and untraceabiliy of the information retrieval process. Thus, the QAIR protocol effectively maintains anonymity and untraceability [10].

Case Study: The QAIR protocol depends on the fidelity of both query QAT and response QAT subprotocols, as illustrated in Fig. 4(a). The QAIR error probability $P_{\text{qav}}(\mathcal{N}_D)$ in the presence of depolarizing noise $\mathcal{N}_D$ is depicted in Fig. 4(b) for when $N = d = 5$. Similarly with QAT protocol, we choose N and d to depict small scale quantum network, where for this case d determines database entry. Specifically, the projective measurement for orthonormal state discrimination to retrieve private information $\mathcal{B}(x)$ forms—a binary symmetric channel with erasures. Fig. 4(b) shows that the QAIR error $P_{\text{qair}}(\mathcal{N}_D)$ degrades with the noisy fidelity and error probability of the subprotocols (QAE, QAB, and QAT). Both types of QAIR errors, i.e., the bit error probability ϵ and the erasure probability α are directly proportional to the depolarizing parameter p in the low-noise regime. Hence, the QAIR error reveals a unit asymptotic slope of $P_{\text{qair}}(\mathcal{N}_D)$ versus p in a log-log plot as a degree of depolarizing noise vanishes ($p \to 0$).

Note that most of the QAC protocols rely on the initial shared GHZ states, which are then used to establish anonymous communication channels between the parties involved. Foundational QAC protocols like QAE, QAN, and QACD are utilized as subprotocols within larger QAC protocols like QAT and QAIR. In essence, these QAC protocols are synergistically used to realize certain QAN applications.

Quantum Supremacy of QANs

The term "*quantum supremacy*" refers to the capability to tackle problems that are practically impossible for classical counterparts. The following discussions emphasize the quantum supremacy exhibited by QANs.

1) Complete Untraceability: Any adversary that traces the communicating identities can compromise the privacy and anonymity of the network. In contrast to the CANs, the QANs ensure complete untraceability or tracelessness by quantum principles [14]. The QAC protocols establish a quantum channel among the network parties by utilizing a shared entangled state, ensuring that each participant is equally involved. In addition, the global state of the system after the local operation performed by any party is independent of its specific identity. At this stage, each party has an equal probability of performing a local operation. As a result, the probability that an adversary can guess the identity of the communicating party is uniformly distributed even with access to all network resources.

2) Unconditional Security: Although the primary purpose of anonymous networks is to preserve privacy, their security is also vital, as the intercepted information could potentially expose the identity of the communicating parties. In CANs, their security relies on computational assumptions, making it vulnerable

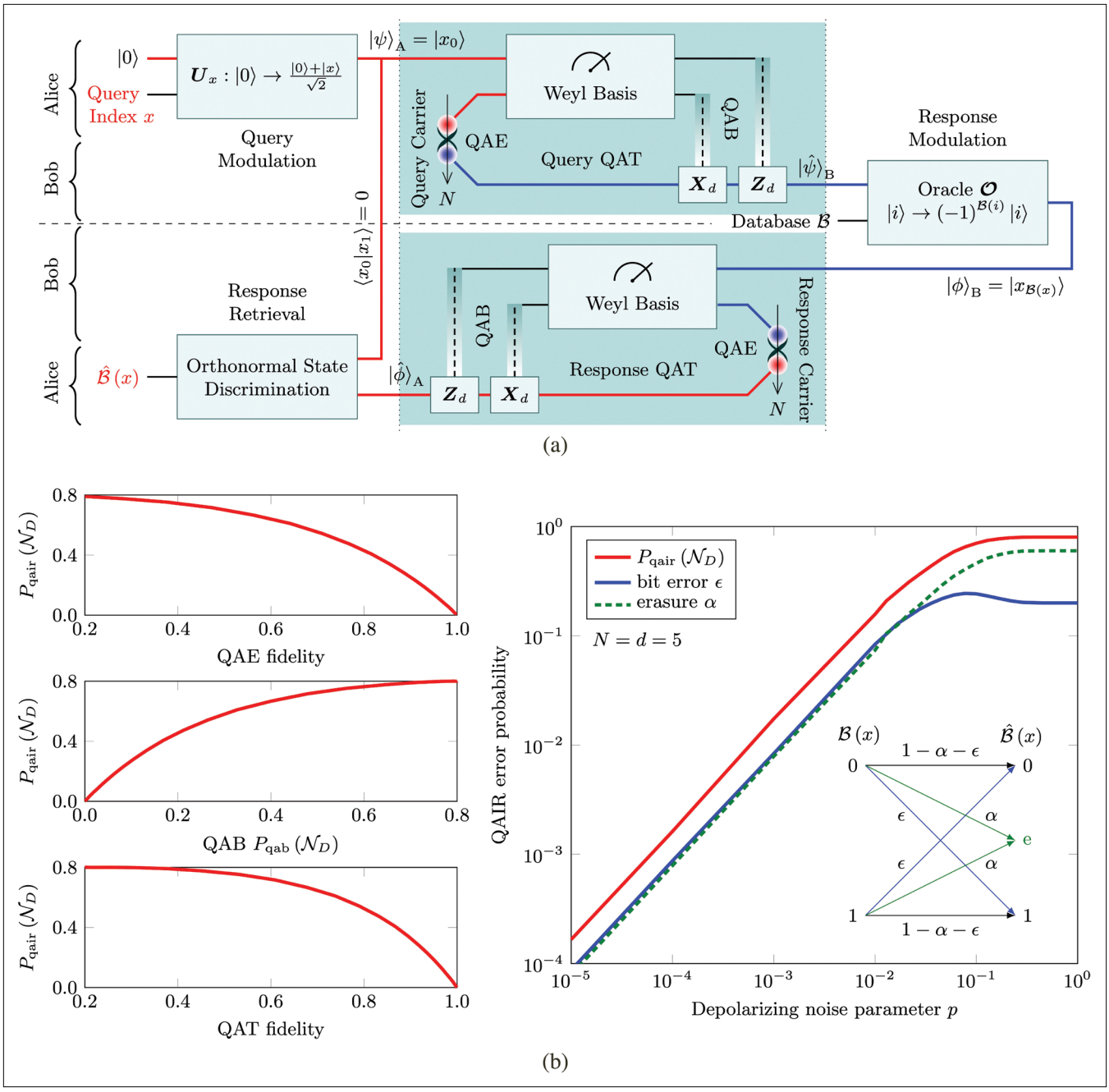

FIGURE 4. Quantum anonymous private information retrieval in an N-party network. (a) Using six N-partite d-dimensional GHZ states, the QAIR protocol successively performs the query modulation (Alice), query QAT (Alice $\rightarrow$ Bob), response modulation (Bob), response QAT (Bob $\rightarrow$ Alice), and information-retrieving orthogonal state discrimination (Alice) to retrieve Bob's private information $\mathcal{B}(x)$ at index $x \in \{1, 2, \ldots, d-1\}$ anonymously while concealing identities (Alice and Bob) as well as the query index x in the information retrieval process. To modulate the query index x and its corresponding response information $\mathcal{B}(x)$, Alice and Bob apply the d-dimensional superposition operation $\boldsymbol{U}_x = \left(|0\rangle\langle 0| + |x\rangle\langle 0|\right)/\sqrt{2}$ and the d-dimensional Oracle operation $\mathcal{O} = \sum_{i=0}^{d-1}(-1)^{\mathcal{B}(i)}|i\rangle\langle i|$ with $\mathcal{B}(0) = 0$, respectively. (b) The QAIR protocol is evaluated when $N = d = 5$ for noisy GHZ states (query carrier, response carrier, and four broadcast carriers) under the depolarizing noise $\mathcal{N}_D$. The QAIR error probability $P_{\text{qair}}(\mathcal{N}_D)$ is plotted as a function of the depolarizing parameter p (right). With depolarizing probability p, the QAIR $P_{\text{qair}}(\mathcal{N}_D)$ arises from both bit errors, i.e., $\hat{\mathcal{B}}(x) = 1 - \mathcal{B}(x)$ (blue solid line), and erasures, i.e., $\hat{\mathcal{B}}(x) = \text{e} \neq 0, 1$ (green dashed line). In addition, the QAIR $P_{\text{qair}}(\mathcal{N}_D)$ is depicted as a function of the QAE fidelity (top left), the QAB $P_{\text{qab}}(\mathcal{N}_D)$ (middle left), and the QAT fidelity (bottom left), where the GHZ states are subject to the depolarizing noise for only the query and response carriers, four broadcast carriers, and all carriers, respectively.

to powerful quantum computing. In contrast, QANs achieve unconditional security by quantum principles such as the no-cloning theorem and the quantum uncertainty principle. This means that the quantum-safe security of QANs remains impervious to the computational abilities of adversaries. This feature makes QANs highly appealing for secure and privacy-preserving communication.

3) Eavesdropping Resilience: In the QANs, quantum cryptography introduces a quantum layer of security and privacy. Quantum

entanglement plays a crucial role by linking the legitimate parties in forms of entangled states, making any attempt of interception or malicious actions by dishonest parties immediately noticeable as they disrupt the initial state of the system. The QKD and quantum CKA protocols also provide essential methods to create secure encryption keys, allowing only the intended recipients to decrypt messages and thwarting security breach attacks. Additionally, the quantum random number generators offer random and unguessable encryption keys, adding an extra layer of security by preventing adversaries from predicting or manipulating keys. Quantum state verification further bolsters network resilience, enabling nodes to verify the integrity of transmitted quantum states and safeguarding against integrity breach attempts. These quantum cryptographic properties collectively fortify the QANs against eavesdropping and ensure the security and integrity of anonymous communication.

4) Trust-Minimized Architecture: QANs operate on a trustminimized architecture, primarily driven by the concept of quantum entanglement. This entanglement underpins essential functions such as message transmission, key distribution, encryption, and multiparty computation. For instance, the QAC protocols can be applied in a multiuser QKD quantum network where the users share perfectly random and secure keys with each other. These protocols enhance the capabilities of fully-connected QKD networks without relying on trusted nodes [15]. Additionally, the quantum CKA protocol enables a group of network participants to share a secret key without requiring excessive trust in any single entity. This protocol achieves a trust-minimized architecture by leveraging anonymity, decentralization, randomness, and consensus-building mechanisms [12]. Thus, the integration of quantum cryptographic protocols into QANs reduces their dependence on TTPs, effectively minimizing the need for trust in these intermediaries.

5) Enhanced Scalability: QANs offer a potential solution to address scalability limitations present in CANs. With integrating QKD, secure keys can be shared between two end nodes, streamlining key management infrastructure and reducing communication overhead associated with key distribution. Quantum teleportation enhances communication efficiency by enabling quantum states to convey multiple bits of information, while quantum parallelism allows for simultaneous quantum operations, harnessing the computational power of quantum systems. These advantages contribute to scalability, particularly in managing large anonymity sets within QANs. Therefore, by incorporating QAC techniques, QANs can offer a practical solution to enhance scalability while ensuring efficient and privacy-preserving communication.

The QAC protocols outlined in our paper are fundamental components of QANs. By exploiting quantum mechanical properties and privacy features detailed in the section "QAC Protocols," these protocols achieve the above-mentioned quantum supremacy, providing unprecedented levels of anonymity, untraceabiliy, security and efficiency in various information processing tasks. This makes them highly desirable for privacy-preserving communication in quantum anonymous networks.

Implementation of QANs involves several key challenges for successful deployment.

Challenges and Research Directions

We identify the primary challenges in deploying QANs and investigate research directions to shape future perspectives in this domain. Additionally we also points out the fundamental differences between QAN and CAN we constitutes its weakness that may need to be addressed.

Key Challenges

Implementation of QANs involves several key challenges for successful deployment. We highlight technical hurdles in developing efficient, scalable, and reliable QANs, emphasizing the need for innovative solutions to address issues of quantum state stability, entanglement engineering, network integration, and technology heterogeneity.

1) Quantum Fragility: Quantum states are highly sensitive to environmental interactions, and even small disturbances can disrupt quantum superposition or entanglement for quantum communication. This disruption, called quantum decoherence, introduces unwanted errors and inaccuracies in quantum communication. Consequently, it poses a significant challenge in preserving the integrity and fidelity of quantum information in QANs. As an example, experimental realization of quantum communications uses single photon. Unlike classical communication where we can increase the power of the transmitter to achieve higher SNR, the same cannot be done for quantum case. Fundamentally, this introduces a new paradigm in designing high performance communication systems based on principle of quantum states.

2) Entanglement Scalability: QANs require entanglement as their primary resources, and thus, any anonymous tasks require high-fidelity and high-rate engineering of both bipartite and multipartite entanglement. While various improvements have been made to generate and distribute the entanglement, its reliability and scalability still remain necessary to be further developed for anonymous services. For example, generating a large number of entangled qubits in GHZ forms still faces limitations in hardware developments and hence, the QAN will be limited to small-scale networking in its early evolution. While quantum entanglement is a unique phenomenon that we leverage for achieving anonymous tasks, it introduces a new challenge for its generation and distribution, which is a unique characteristics of quantum anonymous network unlike classical anonymous network.

3) Quantum Memory Limits: Quantum communication typically requires shared entanglement among network nodes spatially separated across space. Quantum repeaters are located along the communication path as relays to distribute these entangled states. These repeaters store quantum states and facilitate entanglement swapping. However, the limited lifetime of quantum memory and environmental factors such as noise and

decoherence significantly impact the degree of entanglement. Consequently, maintaining and preserving entanglement distribution over long distances while ensuring anonymity poses significant technical challenges in QANs. The main motivation of developing quantum memory is for the quantum repeater which allows long distance quantum state transfer. Unlike classical communication where we can simply copy and amplify a signal to achieve long distance communication, the no-cloning theorem forbids copying of arbitrary quantum states. This also introduces new paradigm of designing repeater based quantum network.

4) Network Hybridization: Deploying a whole new infrastructure for QANs requires a huge amount of resources, and thus, a more sustainable approach is integrating quantum and classical networks. However, their distinctive natures create significant hurdles in achieving compatibility, efficient signal conversion, and interface design between these two domains. For example, the most common classical network for integration with quantum technology is optical communication networks, as photonic qubits are most suitable for communication purposes. While various attempts have been made to integrate QKD into classical optical networks, the tasks in QANs are not limited to key distribution alone, introducing new challenges specific to anonymous networks [5].

5) Quantum Heterogeneity: Quantum information processing is implemented in general using various types of qubit modalities such as superconducting, photonic, or trapped-ion qubits. Fully operational QANs need to facilitate various types of qubits and require interfacing quantum devices to convert between these multimodal qubits. Inevitably, information losses due to these conversions reduce the quality of qubits involved in QANs, and effective engineering efforts are needed to ensure quality of service.

Conclusion and Research Directions

The pivotal role of anonymous networks in ensuring security and privacy is undeniable. While the CANs have evolved over time to satisfy the anonymity requirements of contemporary privacy-preserving communication, their classical limitations have led to persistent security and privacy concerns. The incorporation of quantum principles into anonymous networks embodies a paradigm shift with the potential to address these issues. The QAC protocols provide complete untraceability and unconditional security, offering a promising path for achieving a significant quantum leap in privacy across various networking applications where privacy is paramount. The QAN research requires prioritizing physics-informed designs and controls, considerations for noisy or perfect intermediate-scale quantum (PISQ) networking, and semantic awareness.

1) Physics-Informed Anonymity: The physics-native approach is essential in designing and realizing practical quantum anonymous networking. It is crucial to analyze physics-informed design metrics, such as qubit fidelity, qubit coherence time, entanglement rate, error rates, and quantum transfer efficiency, and optimize physics-informed controls, such as quantum memory, quantum error correction, decoherence prevention, quantum routing, and quantum repeaters. These metrics and controls enable QANs to leverage state-of-the-art quantum technologies, thereby augmenting entanglement scalability for long-range QAC and facilitating network hybridization.

2) PISQ Anonymity: The noisy intermediate-scale quantum (NISQ) networks enable distributed and parallel computing through the interconnection of network nodes. PISQ networks serve as an abstraction of NISQ networks, employing perfect qubits. With fault-tolerant quantum computing techniques, these perfect devices will eventually enable the integration of developments from both NISQ and PISQ paradigms. These NISQ and PISQ networks have the potential to harness the advancement of decentralized architectures within QANs, enhancing the network scalability and efficiency.

3) Semantic-Aware Anonymity: Semantic communication brings new concepts of communication efficiency, reliability, and quality of experience in contrast to context-agnostic communication by conveying the meaning inherent in the message rather than the message itself. This computing-intensive communication empowers semantic-aware networking to overcome context-agnostic constraints on overall network scalability and complexity. To realize these advantages, integrating QANs with semantic awareness is essential for improving the privacy of semantic information.

Acknowledgment

This work was supported by the Kyung Hee University in 2023 under Grant KHU-20233691.

References

[1] E. Erdin, C. Zachor, and M. H. Gunes, "How to find hidden users: A survey of attacks on anonymity networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2296–2316, 4th Quart., 2015.
[2] C. Kuhn, "Formal foundations for anonymous communication," Ph.D. dissertation, Karlsruhe Inst. Technol., Karlsruhe, Germany, 2022.
[3] Z. Wei et al., "Physical layer anonymous precoding: The path to privacy-preserving communications," *IEEE Wireless Commun.*, vol. 29, no. 2, pp. 154–160, Apr. 2022.
[4] F. Zaman et al., "Concealed quantum telecomputation for anonymous 6G URLLC networks," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 7, pp. 2278–2296, Jul. 2023.
[5] F. Xu et al., "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, no. 2, May 2020, Art. no. 025002.
[6] F. Zaman et al., "Quantum machine intelligence for 6G URLLC," *IEEE Wireless Commun.*, vol. 30, no. 2, pp. 22–30, Apr. 2023.
[7] U. Khalid et al., "Quantum semantic communications for Metaverse: Principles and challenges," *IEEE Wireless Commun.*, vol. 30, no. 4, pp. 26–36, Aug. 2023.
[8] U. Khalid et al., "Quantum network engineering in the NISQ age: Principles, missions, and challenges," *IEEE Netw.*, vol. 38, no. 1, pp. 112–123, Jan. 2024.
[9] A. Khan et al., "Quantum anonymous collision detection for quantum networks," *EPJ Quantum Technol.*, vol. 8, no. 1, p. 27, Dec. 2021.
[10] A. Khan et al., "Quantum anonymous private information retrieval for distributed networks," *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4026–4037, Jun. 2022.
[11] Y.-G. Yang et al., "Practical quantum anonymous private information retrieval based on quantum key distribution," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 4034–4045, Jun. 2023.
[12] F. Grasselli et al., "Secure anonymous conferencing in quantum networks," *PRX Quantum*, vol. 3, no. 4, Oct. 2022, Art. no. 040306.
[13] S. Mishra et al., "Quantum anonymous veto: A set of new protocols," *EPJ Quantum Technol.*, vol. 9, no. 1, p. 14, May 2022.

[14] A. Unnikrishnan et al., "Anonymity for practical quantum networks," *Phys. Rev. Lett.*, vol. 122, no. 24, Nov. 2019, Art. no. 240501.
[15] Z. Huang 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.

Biographies

Saw Nang Paing received the B.E. degree in computer engineering and information technology from Mandalay Technology University, Myanmar, in 2019. She is currently pursuing the Ph.D. degree with the Department of Electronics and Information Convergence Engineering, Kyung Hee University, South Korea. Her research interests include quantum communications, quantum security, and quantum networks.

Jason William Setiawan received the B.S. degree in electrical engineering from the Bandung Institute of Technology, Indonesia, in 2020. He is currently pursuing the Ph.D. degree in quantum information science with the Department of Electronics and Information Convergence Engineering, Kyung Hee University (KHU), South Korea. His research interests include quantum information science, quantum communication, and quantum networks.

Trung Q. Duong (Fellow, IEEE) is currently the Canada Excellence Research Chair and a Professor with the Memorial University of Newfoundland, Canada. He is also a Research Chair with the Royal Academy of Engineering, U.K., and an Adjunct Professor with Queen's University Belfast, U.K.

Dusit Niyato (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Canada. He is currently a Professor with the College of Computing and Data Science, Nanyang Technological University, Singapore. His research interests include sustainability, edge intelligence, decentralized machine learning, and incentive mechanism design.

Moe Z. Win (Fellow, IEEE) is currently a Professor with the Massachusetts Institute of Technology. His research encompasses developing fundamental theories, designing algorithms, and conducting experimentation for a broad range of real-world problems. His current research topics include ultra-wideband systems, network localization and navigation, network interference exploitation, and quantum information science. He was honored with two IEEE Technical Field Awards: the IEEE Kiyo Tomiyasu Award (2011) and the IEEE Eric E. Sumner Award (2006).

Hyundong Shin (Fellow, IEEE) (hshin@khu.ac.kr) is currently a Professor with Kyung Hee University, Korea. He received IEEE Guglielmo Marconi Prize Paper Award and IEEE William R. Bennett Prize Paper Award. He was an Editor of IEEE Transactions on Wireless Communications and IEEE Communications Letters.