Controlled Quantum Anonymous Publication

Awais Khan, Jason William Setiawan, Saw Nang Paing, Trung Q. Duong, *Fellow, IEEE*,
Moe Z. Win, *Fellow, IEEE*, and Hyundong Shin, *Fellow, IEEE*

***Abstract*—In the shift toward the quantum computing era, the foundational principles of classical cybersecurity, particularly in the realm of cryptographic algorithms, are facing unprecedented challenges. This demands comprehensive reevaluation and redesign of cryptographic infrastructures to withstand quantum adversarial attacks. With the emergence of the quantum Internet, a new approach to secure communication is possible, utilizing quantum properties that have no counterpart in classical systems. As the quantum Internet facilitates the exchange of quantum information, data publication protocols become essential in anonymizing and protecting privacy-sensitive data in quantum communication networks. This paper proposes two controlled quantum anonymous communication (QAC) protocols for publishing classical and quantum information on an Internet server (IS) with the assistance of a communication service provider. The first protocol allows for the controlled publication of classical information without revealing the publisher's identity such that an adversary, even with access to all network resources, cannot trace the publication source—i.e., achieving *perfect untraceability*. The second protocol enables anonymous publication of quantum information on an IS in a controlled and untraceable manner. These protocols serve as essential building blocks for advancing the quantum Internet, which has the potential to transform communication and information exchange methods. We provide a detailed anonymity analysis of these QAC protocols for data publication, ensuring that the published symbol or qudit information remains untraceable to its publisher. Moreover, the performance analysis in terms of publication error probability, fidelity, and degree of anonymity in noisy environments demonstrates the robustness of the protocols against noise and adversarial attacks.**

***Index Terms*—Anonymity, data publication, privacy, quantum anonymous communication, quantum Internet.**

I. Introduction

DATA PUBLISHING has expanded exponentially with the proliferation of the Internet. This digital revolution empowers individuals, businesses, and organizations to share and distribute data globally with ease. The Internet's widespread adoption and accessibility democratizes the publication process, enabling seamless dissemination of information, fostering collaboration, and facilitating the exchange of ideas like never before. As Isaac Newton once said, *"If I have seen further, it is by standing on the shoulders of Giants."* This quote highlights the critical importance of data publishing. However, it is equally crucial to prioritize security and privacy in communication networks [1].

Indeed, as data flows continue to grow, the need to balance accessible data for scientific advancement and individual privacy becomes more critical. This emphasizes the importance of developing robust data publication strategies and privacy-preserving technologies. Data published by an individual often encompasses privacy-sensitive information, which, if accessed or misused without consent, can pose severe privacy threats. Therefore, ensuring privacy while publishing data has become paramount in our data-driven society. This privacy constraint is particularly significant in Internet of Things (IoT) applications, such as intelligent healthcare, smart banking systems, smart energy and grid systems, and smart cities [2]–[4], where individual data is integral to daily life. Thus, privacy-preserving publication protocols are of utmost importance to prevent unauthorized access and potential misuse of data while ensuring the freedom and benefits of data sharing are retained. These protocols enable secure and privacy-preserving data publishing from publishers to servers. Information is encrypted, transmitted, and stored securely until recipients access it on demand [5]. Operating on a pull or subscription model, these protocols support persistent and asynchronous communication, akin to accessing websites or really simple syndication feeds, and facilitate applications beyond real-time messaging. Although classical privacy-preserving publication protocols exist [6], [7], they are still vulnerable to adversarial attacks compromising the user's identity [8], [9]. The security provided by these protocols can also be limited for IoT networks [10].

Quantum technology is poised to transform the way information is accessed and exchanged through the current internet, introducing advancements such as quantum key distribution (QKD) for unbreakable encryption, secure access to quantum computing resources, and highly accurate clock synchronization [11]–[14]. These features go beyond the limitations of the classical Internet. The quantum Internet integrates these innovations to facilitate the secure transmission of both classical and quantum information using quantum communication [15]–[18]. Over the years, numerous quantum protocols have been proposed for secure data transmission and computational tasks [19]–[23]. These experiments offer substantial enhancements to the security of data publishing processes. However, individual published data is also considered sensitive, posing privacy concerns that are a significant barrier to making such

The fundamental research described in this paper was supported, in part, by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2025-2021-0-02046) and the Convergence security core talent training business support program (IITP-2025-RS-2023-00266615) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation), by the Canada Excellence Research Chair (CERC) Program CERC-2022-00109, by the National Science Foundation under Grant CCF-2153230, and by the Robert R. Taylor Professorship. *(Corresponding author: Hyundong Shin.)*

A. Khan, J. W. Setiawan, S. N. Paing, 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, 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 with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, BT7 1NN Belfast, U.K. (e-mail: tduong@mun.ca).

M. Z. Win is with the Laboratory for Information and Decision Systems (LIDS), Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA (e-mail: moewin@mit.edu).

data widely accessible [24], [25]. Hence, privacy-preserving techniques are necessary while publishing individual data.

Anonymity in communication networks refers to the state or condition where the identity of users engaging in communication networks is concealed or kept confidential [26]. It protects user privacy in communication and computational quantum networks, aiming to ensure anonymity regardless of the adversary's computational power [27]. Many quantum anonymity applications in communication, computing, and sensing networks have been proposed to address diverse security and privacy concerns [28]–[37]. The foundational work on quantum anonymous transmission, introduced in [38], proposed two protocols: quantum anonymous broadcast and bipartite anonymous entanglement distribution. This work relied on the assumption that network participants have access to perfectly shared Greenberger–Horne–Zeilinger (GHZ), followed by subsequent anonymous protocols such as relay-based anonymous communication [39], anonymous entanglement generation using W-states [40], and anonymous GHZ state verification [41], [42]. Furthermore, anonymous versions of the quantum conference key agreement protocol for multipartite communication were proposed [43], [44]. The integration of QKD within the onion router network for developing anonymous communication protocols was also explored in [45]. More recently, the fundamental protocols for achieving anonymity in quantum networks were presented in [26]. Despite their contributions, these protocols lack incorporated control mechanisms to effectively manage and regulate anonymous communication, and are built on frameworks that diverge from the requirements of publication-oriented protocols. Moreover, these protocols often assume idealized conditions, such as perfect resources and absolute anonymity, without providing a comprehensive performance or anonymity analysis under noisy environments, highlighting critical gaps in their functionality and applicability.

These gaps in existing quantum anonymity protocols become especially critical when considering that anonymity preservation is often more important than protecting the data itself in many real-life scenarios. For instance, virtual digital twin networks (VDTNs) involves sharing detailed information about digital twins, including vehicle information, driving habits, and traffic environments [46]. While this data can enhance traffic management, optimize network performance, improve decision-making, and identify safety issues, it also poses significant privacy challenges, such as risks of identity and location exposure, unauthorized profiling, and data misuse for malicious purposes. In another scenario, patients share their data for medical research, fostering collaboration and advancements in healthcare. This patient-centric approach promotes personalized medicine and informed decision-making, driving improvements in patient health. However, if the VDTN or patient data is misused or accessed without authorization, it can lead to severe consequences, compromising individual privacy. In such cases, preserving anonymity during data sharing ensures that the benefits of this shared information can be harnessed without compromising personal privacy and security.

In this paper, we propose quantum anonymous publication (QAP) protocols for classical and quantum information. These protocols utilize local operations and classical communication (LOCC) and introduce controlled anonymous communication in the quantum network. Specifically, the communication service provider (CSP) controls the implementation of mechanisms that manage and regulate the conditions of anonymous communication. This control ensures that anonymity is maintained securely and systematically by enforcing communication rules to prevent any inconsistencies or irregularities. The key contributions of this paper are summarized as follows.

- *Controlled QAP for Classical Information:* This protocol allows a publisher to anonymously publish classical information on an Internet server (IS) with the help of a CSP in a controlled manner (see Protocol 1). It ensures untraceability, meaning the published information becomes untraceable to its publisher, even if all network resources are accessible. The protocol initially utilizes a network-wide multipartite maximally entangled state as a resource to encode the classical symbol information with the quantum Fourier transform (QFT) operation and LOCC for anonymous publication. Then, the CSP collects all quantum measurement outcomes from network users and publishes classical symbol information on the IS in a controlled and untraceable manner.
- *Controlled QAP for Quantum Information:* This protocol consists of two subprotocols for anonymously publishing quantum information on the IS in a controlled and untraceable manner (see Protocol 2). The protocol contains two integrant stages. Initially, it establishes an anonymous QAP channel between the publisher, the IS, and the CSP from the preshared network-wide maximal entanglement. This QAP channel (i.e., tripartite maximally entangled state) can be used as a resource to create an anonymous version of the quantum entanglement with diverse applications [47]–[50]. Subsequently, anonymous publication of qudit information on the IS is controlled by the CSP, facilitated through the QAP protocol for classical information (Protocol 1).
- *QAP Error Probability, Fidelity, and Perfect Anonymity:* To analyze the effect of noise on the QAP protocols, we evaluate the QAP error probability, fidelity, and degree of anonymity in noisy quantum networks. For Protocol 1, we derive publication error probability (PEP) and analyze its asymptotic behavior in the low-noise regime. The analysis reveals that Protocol 1 is *error-free* under shift-type noise and exhibits a linear PEP asymptote with the noise level and network size in low-noise regimes of depolarizing and phase-type noise. For Protocol 2, we derive the QAP channel fidelity and simulate the QAP fidelity under depolarizing, shift-type, and phase-type noise. Moreover, the anonymity analysis demonstrates the noise robustness of QAP protocols in terms of the degree of anonymity, highlighting their ability to achieve perfect anonymity for both symbol and qudit publication, even in noisy network environments.

The paper is organized as follows. Section II presents definitions, network and threat models, and system properties.

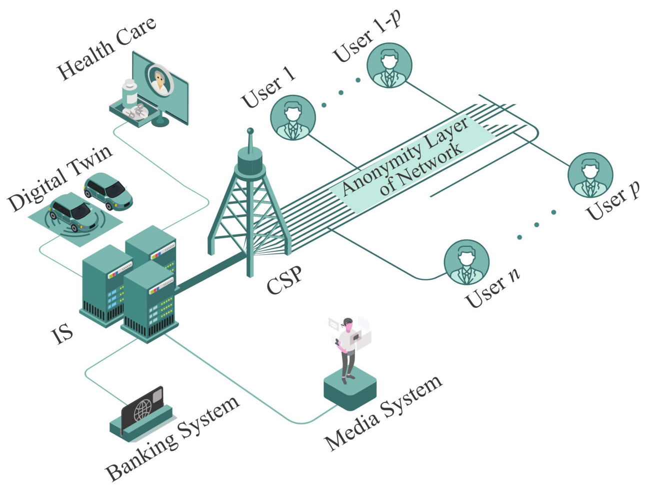


Fig. 1. A controlled QAP network: a group of n users (edge servers), the CSP, and the IS. An incorporated anonymity layer in the publication network enables any user to publish classical or quantum information without revealing its identity while the IS stores the published data in its server.

In Sections III and IV, we propose the QAP protocols to publish classical and quantum information, along with their untraceability analysis. The QAP protocols in noisy scenarios are discussed in Section V. Finally, we conclude the paper in Section VI.

Notation: Quantum states are denoted in Dirac notation by lowercase letters for single-partite systems (e.g., $|\psi\rangle$) and bold lowercase letters for multi-partite systems (e.g., $|\boldsymbol{\psi}\rangle$), respectively. Quantum density operators are represented by bold uppercase letters (e.g., $\boldsymbol{\Xi}$). The set of non-negative integers $\{0, 1, \ldots, d-1\}$ is denoted by $\mathbb{Z}_d$. Random variables are displayed in sans serif, upright fonts; their realizations in serif, italic fonts. For example, a random variable and its realization are denoted by x and x, respectively. Random vectors or sequences and its realization are represented by $\mathbf{\mathsf{X}}$ and $\boldsymbol{X}$, respectively. The probability of the event is denoted by $\mathbb{P}\{\cdot\}$.

II. Models and Definitions

In this section, we delineate quantum states, system models, and properties involved in the design of publication protocols.

A. Quantum States

A quantum digit or qudit is a d-level quantum system in the d-dimensional Hilbert space $\mathcal{H}_d$ and can be written as a linear combination (superposition) of its basis states as follows [51]

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

where the states $|j\rangle$ form the d-dimensional computational basis $\mathcal{B}_{\mathrm{c}}(d)$, the amplitudes α_j are the complex coefficients such that the probabilities of measuring the system in the basis states $|j\rangle$ are given by $|\alpha_j|^2$, and $\sum_{j\in\mathbb{Z}_d} |\alpha_j|^2 = 1$. In addition to the computational basis, the quantum state can be measured using other basis, such as the Fourier basis. Let $\mathfrak{F}_d$ be the QFT operator defined on the d-dimensional computational basis states:

$$\mathfrak{F}_d : |j\rangle \mapsto \frac{1}{\sqrt{d}} \sum_{k\in\mathbb{Z}_d} \exp\left(\frac{\iota 2\pi jk}{d}\right)|k\rangle \tag{2}$$

where $\iota = \sqrt{-1}$. Specifically, the QFT maps the computational basis state $|j\rangle$ into the superposition of computational basis states with coefficients equal to the complex roots of unity. The d-dimensional quantum state $|\psi\rangle$ in (1) can be written in the Fourier basis as follows:

$$|\psi\rangle = \sum_{k\in\mathbb{Z}_d} c_k \mathfrak{F}_d |k\rangle \tag{3}$$

where the basis states $\mathfrak{F}_d |k\rangle$ form the d-dimensional Fourier basis $\mathcal{B}_{\mathcal{F}}(d)$ and the amplitude set $c_0, c_1, \ldots c_{d-1}$ expands the discrete Fourier transform of the amplitudes α_j for the computational basis such that $\alpha_j = \sum_{k\in\mathbb{Z}_d} \exp(\iota 2\pi jk/d)\, c_k/\sqrt{d}$.

A composite quantum state is separable if it can be written as a tensor product of the individual subsystem states. In contrast, a composite quantum state is said to be entangled if it cannot be written as a tensor product of the individual subsystem states. The entangled states are essential in quantum information processing as the states exhibit nonclassical correlations that can be exploited for quantum communication and computation. The Bell state is one of the most widely encountered bipartite maximally entangled states. For multipartite systems, the n-partite d-dimensional GHZ state is known as the maximally entangled state [52] and can be written as:

$$|\mathsf{ghz}\rangle = \frac{1}{\sqrt{d}} \sum_{j\in\mathbb{Z}_d} |j\rangle^{\otimes n} \tag{4}$$

where $\otimes$ denotes the tensor product. Measuring any one of the qudits in the GHZ state collapses the entire composite state to one of the d qudit states. This GHZ state is a vital resource in quantum information processing, particularly in quantum anonymous communication (QAC).

B. Network and Threat Models

A network consists of n users (edge servers), a CSP, and an IS—denoted by $\mathcal{QN}(n+2)$, as shown in Fig. 1. All of these parties can perform LOCC. This network is divided into the following three main entities: i) an anonymous publisher (Alice) $p \in \mathcal{A} = \{1, 2, \ldots, n\}$ that can publish classical or quantum data on the IS; ii) the CSP (Bob) that controls the communication and manages the resources; and iii) the IS (Charlie) that stores the publishing data. Connecting with all users and the IS by a classical authenticated channel, the CSP establishes quantum communication links over the network using the $(n+2)$-partite d-dimensional GHZ state. There exist no direct classical links between n users and the IS.

A communication scenario is classified as *anonymous* if no identifiable information about communicating users is revealed before, during, or after communication tasks. In other words, the level of uncertainty regarding the user identity remains constant throughout the communication process. The main aim of adversaries in this communication scenario is to undermine the anonymity of publishers. The adversaries are classified

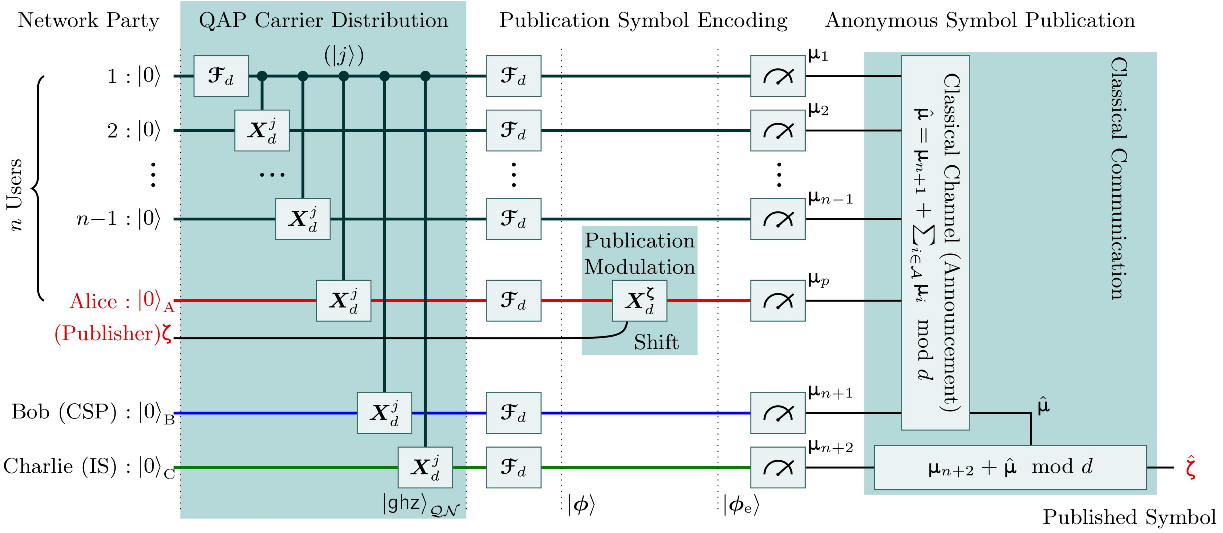


Fig. 2. A controlled QAP protocol for symbol information $\zeta \in \mathbb{Z}_d$ with GHZ preparation, QFT operations, publication encoding (shift operation), computational basis measurements, and classical communications. Bob (CSP) controls the publication process with his d-ary sum information $\hat{\mu}$. For simplicity, we set $p = n$ in the figure.

as single or colluding, each capable of conducting active and passive attacks. The adversary attempts to achieve attack objectives include identifying a target (publisher).

C. Properties

Our primary objective in designing quantum protocols over the network $\mathcal{QN}\,(n+2)$ is to develop an *untraceable* and *correct* publishing system that enables the user (Alice) $p \in \mathcal{A}$ to anonymously publish classical or quantum information on the IS (Charlie) in a controlled manner of the CSP (Bob) without disclosing its identity. To achieve this goal, we use the notion of anonymity as the condition of being unidentifiable within an anonymity set, which is a group of all conceivable subjects who could potentially initiate an action [53]. Therefore, in our problem, the anonymity set is defined as the group of all honest network users, including the anonymous publisher. We now formally define the features of quantum publication protocols, assuming that the GHZ state is preshared.

Definition 1 (Anonymity): A quantum publication protocol is said to be *anonymous* if the probability of the event $I_{\mathcal{A}}$ that the adversary (Eve) correctly identifies the publisher (Alice) in the network $\mathcal{QN}\,(n+2)$ is equal to

$$P_{\text{A}} = \mathbb{P}\{I_{\mathcal{A}}\} = \frac{1}{n}. \tag{5}$$

Remark 1 (Untraceability): Let Eve have unrestricted access to all network resources, including quantum resources of all the $(n+2)$ network parties. Then, the protocol is said to be *untraceable* if the publisher's identity remains hidden with the probability $1/n$ of correctly identifying the publisher, that is, $P_{\text{A}} = 1/n$. This untraceability property ensures the anonymity of the protocol, even if the adversary manages to gain access to all the network resources. Such a property is infeasible in classical anonymous networks.

Definition 2 (Correctness): Let an anonymous user (publisher) be able to publish quantum information $|\psi\rangle \in \mathcal{H}^d$ or classical information $\zeta \in \mathbb{Z}_d$ on the IS. A quantum publication protocol is said to be *correct* if $|\hat{\psi}\rangle = |\psi\rangle$ or $\hat{\zeta} = \zeta$ with probability one, where $|\hat{\psi}\rangle$ or $\hat{\zeta}$ is the published quantum or classical message.

III. Controlled QAP for Classical Information

We present a quantum protocol for the controlled anonymous publication of classical information, assuming only one publisher at a time. Using the anonymous collision detection protocol [28], QAP protocols can generally be designed for multiple publishers.

A. The Protocol

We design a QAP protocol for classical information in the network $\mathcal{QN}\,(n+2)$. This protocol allows any user to publish its classical information $\zeta \in \mathbb{Z}_d$ anonymously on the IS with the control of the CSP. To encode the information ζ on its qudit, an anonymous publisher p permutes the computational basis states by applying $\boldsymbol{X}_d^{\zeta}$ where the d-dimensional Pauli-X, i.e., X-qudit (or shift) operator $\boldsymbol{X}_d$ keeps the essential property of the Pauli-X gate $|0\rangle\langle 1| + |1\rangle\langle 0|$ as follows:

$$\begin{aligned}\boldsymbol{X}_d = \sum_{j\in\mathbb{Z}_d} |j+1 \mod d\rangle\langle j| :\\ |j\rangle \to |j+1 \mod d\rangle\,.\end{aligned} \tag{6}$$

Specifically, the publication protocol takes a series of steps as follows (see Protocol 1 and Fig. 2).

1) Preparation: All the parties in the network $\mathcal{QN}\,(n+2)$ including the publisher (Alice$_p$), CSP (Bob), and IS (Charlie) share the $(n+2)$-partite d-dimensional GHZ state—called the *QAP carrier*:

$$|\text{ghz}\rangle_{\mathcal{QN}} = \frac{1}{\sqrt{d}} \sum_{j\in\mathbb{Z}_d} |j\rangle^{\otimes n-1} |j\rangle_{\text{A}} |j\rangle_{\text{B}} |j\rangle_{\text{C}} \tag{7}$$

where the subscripts A, B, and C denote Alice$_p$, Bob, and Charlie, respectively.

2) QFT Operations: All $(n+2)$ network participants start the protocol by applying the QFT operation on their respective qudit states. These unitary operations transform the QAP carrier $|\mathsf{ghz}\rangle_{\mathcal{QN}}$ to the entangled GHZ-like state as follows [35]:

$$\begin{aligned} |\boldsymbol{\phi}\rangle &= \mathfrak{F}_d^{\otimes n+2} |\mathsf{ghz}\rangle_{\mathcal{QN}} \\ &= \frac{1}{\sqrt{d^{n+3}}} \sum_{j\in\mathbb{Z}_d} \sum_{\boldsymbol{k}\in\mathbb{Z}_d^{n+2}} \exp\left(\frac{\iota 2\pi j \omega(\boldsymbol{k})}{d}\right) |\boldsymbol{k}\rangle \\ &= \frac{1}{\sqrt{d^{n+1}}} \sum_{\substack{\boldsymbol{k}\in\mathbb{Z}_d^{n+2} \\ \omega(\boldsymbol{k})=0}} |\boldsymbol{k}\rangle \end{aligned} \tag{8}$$

where the last equality follows from the fact that

$$\sum_{j\in\mathbb{Z}_d} \exp\left(\frac{\iota 2\pi j \omega(\boldsymbol{k})}{d}\right) = 0 \tag{9}$$

for any nonzero integer $\omega(\boldsymbol{k}) \in \mathbb{Z}_d$ and

$$\omega(\boldsymbol{k}) = \sum_{j=1}^{n+2} k_j \mod d \tag{10}$$

denotes the modulo d addition of all the elements in the d-ary sequence (or vector) $\boldsymbol{k} = (k_1, k_2, \ldots, k_{n+2}) \in \mathbb{Z}_d^{n+2}$, called the *$d$-ary sum* of $\boldsymbol{k}$.

3) Publication Modulation: (Publisher)

Alice$_p$ performs the X-qudit operator $\boldsymbol{X}_d^{\boldsymbol{\zeta}}$ on her qudit to encode the publication information $\boldsymbol{\zeta} \in \mathbb{Z}_d$, while other network parties apply the d-dimensional identity operator $\boldsymbol{I}_d$ on their qudits, i.e., leave the qudit states as they are. The $(n+2)$-partite entangled state $|\boldsymbol{\phi}\rangle$ transforms then to

$$\begin{aligned} |\boldsymbol{\phi}_{\mathrm{e}}\rangle &= \boldsymbol{I}_d^{\otimes n-1} \otimes \boldsymbol{X}_d^{\boldsymbol{\zeta}} \otimes \boldsymbol{I}_d \otimes \boldsymbol{I}_d |\boldsymbol{\phi}\rangle \\ &= \frac{1}{\sqrt{d^{n+1}}} \sum_{\substack{\boldsymbol{k}\in\mathbb{Z}_d^{n+2} \\ \omega(\boldsymbol{k})=\boldsymbol{\zeta}}} |\boldsymbol{k}\rangle, \end{aligned} \tag{11}$$

where the encoded state $|\boldsymbol{\phi}_{\mathrm{e}}\rangle$ are in the superposition of all $|\boldsymbol{k}\rangle = |k_1 k_2 \cdots k_{n+2}\rangle$ with the d-ary sum equal to $\omega(\boldsymbol{k}) = \boldsymbol{\zeta}$.

4) Computational Basis Measurement: All $(n+2)$ parties measure their qudits in the computational basis $\mathcal{B}_{\mathrm{c}}(d)$. The measurement outcome of Alice$_i$, $i \in \mathcal{A}$, is denoted by $\mu_i \in \mathbb{Z}_d$, whereas μ_{n+1} and μ_{n+2} denote the measurement outcomes of Bob and Charlie, respectively. Note that the measurement outcome sequence $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_{n+2})$ has the d-ary sum $\omega(\boldsymbol{\mu}) = \boldsymbol{\zeta}$—equal to the value of publication information $\boldsymbol{\zeta}$—due to Alice's shift operation encoding. These $(n+2)$-tuple d-ary outcomes appear randomly with the equal probability of $1/d^{n+1}$ due to the basis change from the QFT operations even for the entangled state between the $(n+2)$ parties, which conceals the fact that Alice$_p$ has published the classical information $\boldsymbol{\zeta} \in \mathbb{Z}_d$ by shifting her qudit state.

5) Classical Communication (Users → CSP): All n users Alice$_{i\in\mathcal{A}}$ send their measurement outcomes $\mu_1, \mu_2, \ldots, \mu_n$ to Bob using the classical channel.

Protocol 1 Controlled QAP for classical information

Input: One preshared $(n+2)$-partite d-dimensional GHZ state and classical publication information $\boldsymbol{\zeta} \in \mathbb{Z}_d$

Output: Classical published information $\hat{\boldsymbol{\zeta}} \in \mathbb{Z}_d$

Protocol Participants:

- n users (Alice), CSP (Bob), IS (Charlie)
- Publisher (Alice$_p$) is the user party $p \in \mathcal{A}$

The Protocol:

1) All parties share the entangled state $|\mathsf{ghz}\rangle_{\mathcal{QN}}$.
2) All parties apply the QFT operation on their qudit states.
3) Alice$_p$ performs the X-qudit operator $\boldsymbol{X}_d^{\boldsymbol{\zeta}}$ on her qudit to anonymously publish her classical information $\boldsymbol{\zeta} \in \mathbb{Z}_d$.
4) All parties measure their qudit states on the computational basis $\mathcal{B}_{\mathrm{c}}(d)$.
5) Each Alice$_{i\in\mathcal{A}}$ sends its measurement outcome $\mu_i \in \mathbb{Z}_d$ to Bob using the classical authenticated channel.
6) Bob calculates
$$\hat{\mu} = \left(\mu_{n+1} + \sum_{i\in\mathcal{A}} \mu_i\right) \mod d$$
and sends this information $\hat{\mu} \in \mathbb{Z}_d$ to Charlie where μ_{n+1} denotes Bob's measurement outcome.
7) Charlie decodes and publishes the classical information
$$\hat{\boldsymbol{\zeta}} = \mu_{n+2} + \hat{\mu} \mod d$$
where μ_{n+2} denotes Charlie's measurement outcome.

6) Classical Communication (CSP → IS): Bob then calculates the d-ary sum

$$\hat{\mu} = \left(\mu_{n+1} + \sum_{i\in\mathcal{A}} \mu_i\right) \mod d \tag{12}$$

of n users' and his own measurement outcomes and sends this information $\hat{\mu} \in \mathbb{Z}_d$ to Bob using the classical channel. Note that Bob holds $\hat{\mu}$ and controls the publication process. Without this d-ary sum, Charlie cannot recover the classical information to publish. Bob can abort the protocol if inconsistencies, errors, or discrepancies are detected during protocol execution, such as when the user deviates from the protocol execution, fails measurements or performs invalid operations, or delays the announcement of the measurement outcomes.

7) Anonymous Publication: Finally, Charlie calculates the sum of his measurement outcome and the information received from Bob to recover the publication information $\boldsymbol{\zeta}$ of Alice$_p$ (i.e., the d-ary sum of all network measurement outcomes) as follows:

$$\hat{\boldsymbol{\zeta}} = \mu_{n+2} + \hat{\mu} \mod d, \tag{13}$$

which is the published classical information on Charlie without revealing the publisher's identity, i.e., Alice$_p$.

B. Untraceability

The encoded state $|\boldsymbol{\phi}_{\mathrm{e}}\rangle$ in (11) does not depend on the publisher's identity (index) $p \in \mathcal{A}$, implying the anonymity of

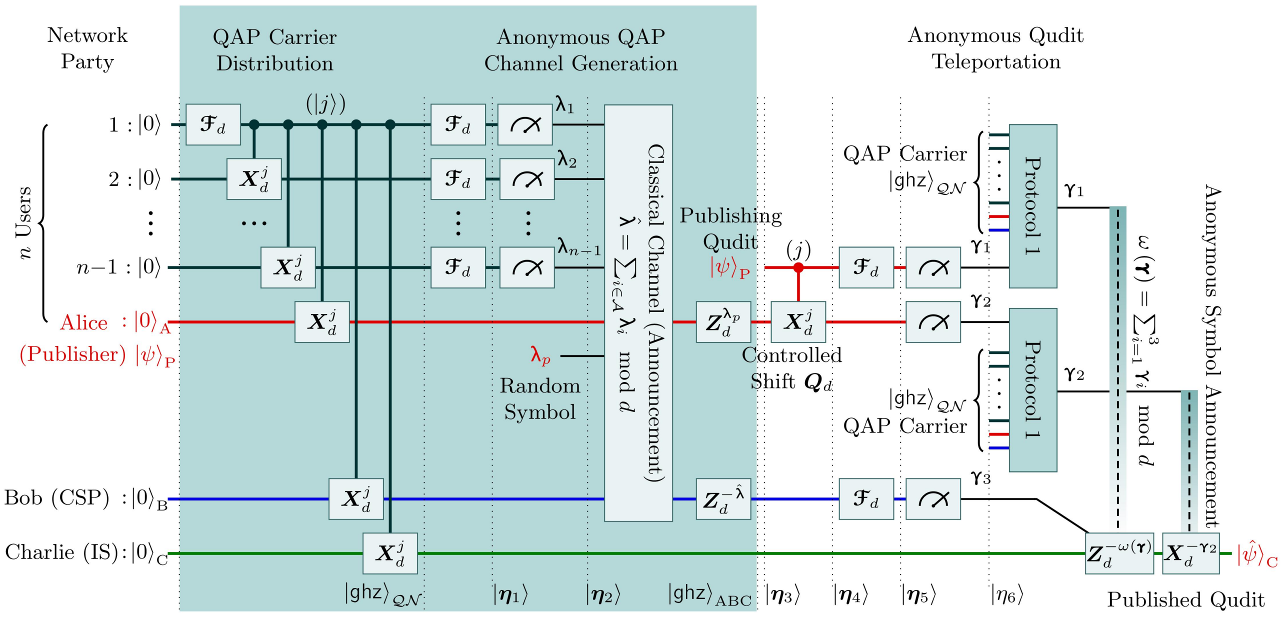

Network Party
QAP Carrier Distribution
Anonymous QAP Channel Generation
Anonymous Qudit Teleportation
n Users
$1 : |0\rangle$
$2 : |0\rangle$
$n{-}1 : |0\rangle$
Alice : $|0\rangle_{\mathrm{A}}$
(Publisher) $|\psi\rangle_{\mathrm{P}}$
Bob (CSP) : $|0\rangle_{\mathrm{B}}$
Charlie (IS): $|0\rangle_{\mathrm{C}}$
$(|j\rangle)$
$\mathfrak{F}_d$
$\boldsymbol{X}_d^j$
λ_1
λ_2
λ_{n-1}
λ_p
Random Symbol
Classical Channel (Announcement)
$\hat{\lambda} = \sum_{i\in\mathcal{A}} \lambda_i \mod d$
Publishing Qudit $|\psi\rangle_{\mathrm{P}}$
(j)
$\boldsymbol{Z}_d^{\lambda_p}$
$\boldsymbol{Z}_d^{-\hat{\lambda}}$
Controlled Shift $\boldsymbol{Q}_d$
QAP Carrier $|\mathsf{ghz}\rangle_{\mathcal{QN}}$
$|\mathsf{ghz}\rangle_{\mathcal{QN}}$ QAP Carrier
Protocol 1
Protocol 1
γ_1
γ_2
γ_3
$\omega(\boldsymbol{\gamma}) = \sum_{i=1}^{3} \gamma_i \mod d$
Anonymous Symbol Announcement
$\boldsymbol{Z}_d^{-\omega(\boldsymbol{\gamma})}$
$\boldsymbol{X}_d^{-\gamma_2}$
$|\hat{\psi}\rangle_{\mathrm{C}}$
Published Qudit
$|\mathsf{ghz}\rangle_{\mathcal{QN}}$
$|\boldsymbol{\eta}_1\rangle$
$|\boldsymbol{\eta}_2\rangle$
$|\mathsf{ghz}\rangle_{\mathrm{ABC}}$
$|\boldsymbol{\eta}_3\rangle$
$|\boldsymbol{\eta}_4\rangle$
$|\boldsymbol{\eta}_5\rangle$
$|\eta_6\rangle$

Fig. 3. A controlled QAP protocol for qudit information with anonymous QAP channel generation and anonymous qudit teleportation. Bob (CSP) controls the publication process with his d-ary sum information $\hat{\lambda}$ and Fourier basis outcome γ_3 in the QAP channel generation and qudit teleportation phases, respectively. For simplicity, we set $p = n$ in the figure.

Protocol 1. We now present the formal proof of its untraceability. Suppose that the QAP protocol for classical information (Protocol 1) is experiencing intrusion from the adversary (Eve) in the network $\mathcal{QN}\,(n+2)$. In the most adversarial scenario, we consider that Eve possesses access to all quantum resources of the network parties. In this *worst adversarial scenario*—i.e., Eve can access the encoded entire joint quantum state $|\boldsymbol{\phi}_{\mathrm{e}}\rangle$, including n honest users with an equal chance of being a publisher. Let $|\boldsymbol{\phi}_{\mathrm{e}}\rangle_p$ be the $(n+2)$-partite encoded state corresponding to the publisher $p \in \mathcal{A}$. To guess the publisher's identity, Eve needs to distinguish between the n encoded states $|\boldsymbol{\phi}_{\mathrm{e}}\rangle_{p\in\mathcal{A}}$ by measuring with the set of positive operator-valued measure (POVM) operators $\boldsymbol{\Pi}_i$, $i \in \mathcal{A}$. Then, the probability that Eve correctly identifies the publisher (i.e., the event $I_{\mathcal{A}}$ in Definition 1) is given by

$$\begin{aligned} P_{\mathrm{A}} &= \sum_{i\in\mathcal{A}} \mathbb{P}\{I_{\mathcal{A}} \mid \mathsf{p} = i\}\, \mathbb{P}\{\mathsf{p} = i\} \\ &= \frac{1}{n} \sum_{i\in\mathcal{A}} \operatorname{tr}\left\{\boldsymbol{\Pi}_i\, |\boldsymbol{\phi}_{\mathrm{e}}\rangle_i \langle\boldsymbol{\phi}_{\mathrm{e}}|\right\} \\ &= \frac{1}{n} \operatorname{tr}\left\{\sum_{i\in\mathcal{A}} \boldsymbol{\Pi}_i\, |\boldsymbol{\phi}_{\mathrm{e}}\rangle\langle\boldsymbol{\phi}_{\mathrm{e}}|\right\} \\ &= \frac{1}{n} \operatorname{tr}\left\{|\boldsymbol{\phi}_{\mathrm{e}}\rangle\langle\boldsymbol{\phi}_{\mathrm{e}}|\right\} = \frac{1}{n} \end{aligned} \tag{14}$$

where $\operatorname{tr}\{\cdot\}$ is the trace operator; the first equality is due to the law of total probability; the second equality follows from the uniform *a priori* probability for publication among the honest users; the third equality follows from the fact that $|\boldsymbol{\phi}_{\mathrm{e}}\rangle_i = |\boldsymbol{\phi}_{\mathrm{e}}\rangle$ for all $i \in \mathcal{A}$; the fourth equality is due to the completeness relation of POVM operators; and the last equality follows from the state normalization. Note from (14) that even under the most adversarial condition—i.e., complete possession of the encoded state—for Eve, the publisher remains *untraceable* in Protocol 1. This property is not feasible in classical anonymous counterparts, underscoring the distinctive advantage of QAC.

IV. Controlled QAP for Quantum Information

This section proposes a quantum protocol for the controlled QAP of quantum information by utilizing LOCC.

A. The Protocol

We now design a QAC protocol for quantum information in the network $\mathcal{QN}\,(n+2)$, which allows a publisher $p \in \mathcal{A}$ to share its quantum information $|\psi\rangle \in \mathcal{H}^d$ anonymously on the IS with the control of the CSP. This protocol first generates an anonymous entanglement link—called the *anonymous QAP channel*—between the publisher, CSP, and IS without revealing the publisher's identity. Then, using this tripartite anonymous entangled quantum resource, the publisher—controlled by the CSP—teleports its quantum publication state to the IS. To remove a phase $\theta \in \mathbb{Z}_d$ depending on the measurement outcomes during the QAP channel generation, the anonymous publisher p shifts the phase of the computational basis states by applying $\boldsymbol{Z}_d^{-\theta}$ where the d-dimensional Pauli-Z, i.e., Z-qudit (or phase) operator $\boldsymbol{Z}_d$ has the essential property of the Pauli-Z gate $|0\rangle\langle 0| - |1\rangle\langle 1|$ as follows:

$$\begin{aligned} \boldsymbol{Z}_d = \sum_{j\in\mathbb{Z}_d} \exp\left(\frac{\iota 2\pi j}{d}\right) |j\rangle\langle j| : \\ |j\rangle \rightarrow \exp\left(\iota 2\pi j/d\right) |j\rangle\,. \end{aligned} \tag{15}$$

In addition, the publisher uses the controlled X-qudit (or shift) operator

$$\boldsymbol{Q}_d = \sum_{j\in\mathbb{Z}_d} |j\rangle\langle j| \otimes \boldsymbol{X}_d^j : \\ |ij\rangle \to |i\rangle\,|i+j \mod d\rangle \tag{16}$$

to perform the d-dimensional maximally-entangled (Bell) basis measurement for anonymous qudit teleportation. Specifically, the publication protocol takes a series of steps as follows (see Protocol 2 and Fig. 3).

1) Preparation: All the parties in the network $\mathcal{QN}\,(n+2)$ including the publisher (Alice$_p$), CSP (Bob), and IS (Charlie) share three copies (QAP carriers) of the $(n+2)$-partite d-dimensional GHZ state in (7): one GHZ state is for anonymous QAP channel generation, while two GHZ states are for anonymous teleportation of quantum information

$$|\psi\rangle_{\mathrm{P}} = \sum_{j\in\mathbb{Z}_d} \alpha_j\,|j\rangle_{\mathrm{P}} \tag{17}$$

to publish.

2) Anonymous QAP Channel Generation: The first step involves anonymously generating a tripartite entanglement link between Alice$_p$, Bob, and Charlie. All the $(n-1)$ network participants except the communicating parties (Alice$_p$, Bob, and Charlie) over this anonymous QAP channel measure their qudits on the Fourier basis $\mathcal{B}_{\mathcal{F}}\,(d)$ and Alice$_i$, $i \in \mathcal{A}\setminus\{p\}$, announce their measurement outcomes to Bob, whereas Alice$_p$ announces a uniformly random classical symbol from $\mathbb{Z}_d$. These Fourier basis measurements preserve the entangled state between Alice$_p$, Bob, and Charlie as well as anonymize Alice$_p$ by converting the measurement outcomes of other $(n-1)$ entangled network parties to the *independent* d-ary uniform variables.

a) *QFT Operations*: All the $(n-1)$ network parties except Alice$_p$, Bob, and Charlie apply the QFT operation on their qudits and the preshared entangled state $|\mathsf{ghz}\rangle_{\mathcal{QN}}$ then transforms to

$$\begin{aligned} |\boldsymbol{\eta}_1\rangle &= \boldsymbol{\mathfrak{F}}_d^{\otimes n-1} \otimes \boldsymbol{I}_d \otimes \boldsymbol{I}_d \otimes \boldsymbol{I}_d\,|\mathsf{ghz}\rangle_{\mathcal{QN}} \\ &= \frac{1}{\sqrt{d}} \sum_{j\in\mathbb{Z}_d} \left(\boldsymbol{\mathfrak{F}}_d\,|j\rangle\right)^{\otimes n-1} |jjj\rangle_{\mathrm{ABC}} \\ &= \frac{1}{\sqrt{d^n}} \sum_{(\boldsymbol{k},j)\in\mathbb{Z}_d^n} \exp\left(\frac{\iota 2\pi j\omega(\boldsymbol{k})}{d}\right) |\boldsymbol{k}\rangle\,|jjj\rangle_{\mathrm{ABC}}\,. \end{aligned} \tag{18}$$

b) *Computational Basis Measurement*: Now, all the $(n-1)$ network parties except Alice$_p$, Bob, and Charlie measure their qudits on the computational basis $\mathcal{B}_{\mathrm{c}}\,(d)$. The measurement outcomes of Alice$_i$, $i \in \mathcal{A}\setminus\{p\}$, are denoted by $\lambda_i \in \mathbb{Z}_d$, while Alice$_p$ generates a random symbol $\lambda_p \in \mathbb{Z}_d$. Note that each of the $(n-1)$-tuple d-ary sequences appears at random as the measurement outcome sequence $\boldsymbol{\lambda} \in \mathbb{Z}_d^{n-1}$ of $\lambda_{i\in\mathcal{A}\setminus\{p\}}$ with the probability of $1/d^{n-1}$ due to the QFT operation. This complete randomness hides the fact that Alice$_p$ has generated the random symbol without measuring her qudit to prepare the QAP channel with preserving the entangled state between Alice$_p$, Bob, and Charlie. Then, the $(n+2)$-partite entangled state $|\boldsymbol{\eta}_1\rangle$ collapses to

$$|\boldsymbol{\eta}_2\rangle = \frac{1}{\sqrt{d}} \sum_{j\in\mathbb{Z}_d} \exp\left(\frac{\iota 2\pi j\omega(\boldsymbol{\lambda})}{d}\right) |jjj\rangle_{\mathrm{ABC}}\,. \tag{19}$$

c) *Classical Communication (Users → CSP)*: All the n network users Alice$_{i\in\mathcal{A}}$ send their measurement or random symbol (Alice$_p$) outcomes $\lambda_1, \lambda_2, \ldots, \lambda_n$ to Bob using

Protocol 2 Controlled QAP for quantum information

Input: Three preshared $(n+2)$-partite d-dimensional GHZ states and quantum publication information $|\psi\rangle \in \mathcal{H}^d$
Output: Quantum published information $|\hat{\psi}\rangle \in \mathcal{H}^d$
Protocol Participants:

- n users (Alice), CSP (Bob), IS (Charlie)
- Publisher (Alice$_p$) is the user party $p \in \mathcal{A}$

The Protocol:

1) All parties share three copies of the entangled $|\mathsf{ghz}\rangle_{\mathcal{QN}}$.
2) All parties generate a tripartite anonymous entanglement link (QAP channel) between Alice$_p$, Bob, and Charlie.
   a) All the $(n-1)$ parties except Alice$_p$, Bob, and Charlie apply the QFT operation on their qudit states.
   b) All the $(n-1)$ Alice$_{i\in\mathcal{A}\setminus\{p\}}$ except Alice$_p$ measure their qudit states on the computational basis $\mathcal{B}_{\mathrm{c}}\,(d)$, while Alice$_p$ generates a random symbol $\lambda_p \in \mathbb{Z}_d$.
   c) Each Alice$_{i\in\mathcal{A}}$ sends its outcome $\lambda_i \in \mathbb{Z}_d$ to Bob using the classical authenticated channel.
   d) Alice$_p$ and Bob perform the Z-qudit operators $\boldsymbol{Z}_d^{\lambda_p}$ and $\boldsymbol{Z}_d^{-\hat{\lambda}}$ on their respective qudits to anonymously generate a tripartite d-dimensional GHZ state for the publication of quantum information where
$$\hat{\lambda} = \sum_{i\in\mathcal{A}} \lambda_i \mod d.$$
3) Alice$_p$ teleports her qudit $|\psi\rangle$ anonymously to Charlie for publication. This is done under Bob's control, without revealing her identity, using the tripartite anonymous d-dimensional GHZ state shared by Step 2).
   a) Alice$_p$ performs the controlled X-qudit operator $\boldsymbol{Q}_d$ on her two qudits: the publication qudit (as a control) and her member qudit (as a target) of the GHZ state.
   b) Alice$_p$ and Bob apply the QFT operation on her publication qudit and his qudit, respectively.
   c) Alice$_p$ and Bob measure both her qudits and his single qudit in the computational basis $\mathcal{B}_{\mathrm{c}}\,(d)$, respectively.
   d) Alice$_p$ anonymously announces the measurement outcomes $\gamma_1, \gamma_2 \in \mathbb{Z}_d$ for her publication qudit and GHZ member qudit to Charlie using Protocol 1.
   e) Bob announces his measurement outcome $\gamma_3 \in \mathbb{Z}_d$ to Charlie using the classical authenticated channel. Then, Charlie calculates the d-ary sum $\omega(\boldsymbol{\gamma})$ for the measurement outcome sequence $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \gamma_3) \in \mathbb{Z}_d^3$.
   f) Charlie applies the Z-qudit operator $\boldsymbol{Z}_d^{-\omega(\boldsymbol{\gamma})}$ and the X-qudit operator $\boldsymbol{X}_d^{-\gamma_2}$ on his qudit to correct the teleported state and publishes this quantum information.

the classical authenticated channel.

d) *Phase-Removal Operation (Publisher and CSP)*: Now, Bob calculates the d-ary sum

$$\hat{\boldsymbol{\lambda}} = \sum_{i \in \mathcal{A}} \boldsymbol{\lambda}_i \mod d. \tag{20}$$

Alice$_p$ and Bob perform $\boldsymbol{Z}_d^{\boldsymbol{\lambda}_p}$ and $\boldsymbol{Z}_d^{-\hat{\boldsymbol{\lambda}}}$ on their respective qudits to remove the phase $\omega(\boldsymbol{\lambda}) \in \mathbb{Z}_d$ depending on the measurement sequence $\boldsymbol{\lambda}$ of the $(n-1)$ network users Alice$_{i \in \mathcal{A} \setminus \{p\}}$. Then, the (maximally entangled) tripartite GHZ state, i.e., the QAP channel is generated (preserved) anonymously between Alice$_p$, Bob, and Charlie with concealing the identity of Alice$_p$ as follows:

$$\begin{aligned} |\mathsf{ghz}\rangle_{\mathrm{ABC}} &= \boldsymbol{Z}_d^{\boldsymbol{\lambda}_p} \otimes \boldsymbol{Z}_d^{-\hat{\boldsymbol{\lambda}}} \otimes \boldsymbol{I}_d \, |\boldsymbol{\eta}_2\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{j \in \mathbb{Z}_d} |jjj\rangle_{\mathrm{ABC}} , \end{aligned} \tag{21}$$

which is anonymous entanglement between Alice$_p$, Bob, and Charlie for the publication of quantum information. Note that Bob's qudit retains maximally entangled in (21) to control the publication of Alice$_p$ on Charlie.

3) Anonymous Qudit Teleportation (Publisher → IS): The state of the entire anonymous teleportation system is a product state of the publication state (17) and the tripartite anonymous GHZ state (21) as follows:

$$\begin{aligned} |\boldsymbol{\eta}_3\rangle &= |\psi\rangle_{\mathrm{P}} \otimes |\mathsf{ghz}\rangle_{\mathrm{ABC}} \\ &= \frac{1}{\sqrt{d}} \sum_{i,j \in \mathbb{Z}_d} \alpha_i \, |ijjj\rangle_{\mathrm{PABC}} . \end{aligned} \tag{22}$$

a) *Publication Modulation (Publisher)*: Alice$_p$ begins interacting her publication state (control)—the first qudit in (22)—with her member (target) of the GHZ triplet—the second qudit in (22)—by applying the controlled X-qudit operator $\boldsymbol{Q}_d$. This controlled operation transforms $|\boldsymbol{\eta}_3\rangle$ to

$$\begin{aligned} |\boldsymbol{\eta}_4\rangle &= \boldsymbol{Q}_d \otimes \boldsymbol{I}_d \otimes \boldsymbol{I}_d \, |\boldsymbol{\eta}_3\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{i,j \in \mathbb{Z}_d} \alpha_i \, |i\rangle_{\mathrm{P}} \, |i+j \mod d\rangle_{\mathrm{A}} \, |jj\rangle_{\mathrm{BC}} . \end{aligned} \tag{23}$$

b) *QFT Operations (Publisher and CSP)*: Alice$_p$ performs QFT on her publication qudit. Bob also applies the QFT operator on his qudit for the Fourier basis measurement to control the publication. Then, the entangled state $|\boldsymbol{\eta}_4\rangle$ transforms to

$$\begin{aligned} |\boldsymbol{\eta}_5\rangle &= \mathfrak{F}_d \otimes \boldsymbol{I}_d \otimes \mathfrak{F}_d \otimes \boldsymbol{I}_d \, |\boldsymbol{\eta}_4\rangle \\ &= \frac{1}{\sqrt{d^3}} \sum_{\substack{(\boldsymbol{k},j) \in \mathbb{Z}_d^4 \\ \boldsymbol{k}=(k_1,k_2,k_3)}} \Bigg[\alpha_j \exp\left(\frac{\iota 2\pi j \omega(\boldsymbol{k})}{d} \right) \\ &\qquad \times \boldsymbol{I}_d^{\otimes 3} \otimes \boldsymbol{X}_d^{k_2} \, |\boldsymbol{k}j\rangle_{\mathrm{PABC}} \Bigg] . \end{aligned} \tag{24}$$

c) *Computational Basis Measurement (Publisher and CSP)*: Now, Alice$_p$ makes the computational basis measurement on both qudits in her possession. Bob also measures his qudit on the computational basis $\mathcal{B}_{\mathrm{c}}(d)$. Let $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \gamma_3) \in \mathbb{Z}_d^3$ be the measurement outcome sequence where γ_1, γ_2, and γ_3 denote the measurement outcomes of qudits P, A, and B in the state (24), respectively. Then, the state $|\boldsymbol{\eta}_5\rangle$ collapses to

$$|\eta_6\rangle = \sum_{j \in \mathbb{Z}_d} \alpha_j \exp\left(\frac{\iota 2\pi j \omega(\boldsymbol{\gamma})}{d} \right) \boldsymbol{X}_d^{\gamma_2} \, |j\rangle_{\mathrm{C}} . \tag{25}$$

Note that Bob controls the publication process with his measurement outcome γ_3 in the qudit teleportation phase.

d) *Anonymous Announcement (Publisher → IS)*: Alice$_p$ announces her measurement outcomes γ_1 and γ_2 anonymously to Charlie with two runs of Protocol 1 using two preshared $(n+2)$-partite d-dimensional GHZ states.

e) *Classical Communication (CSP → IS)*: Bob announces his measurement outcome γ_3 to Charlie using the classical authenticated channel.

f) *Anonymous Publication*: Charlie finally corrects the phase $\omega(\boldsymbol{\gamma})$ and the shift γ_2 in his state $|\eta_6\rangle$ to reconstruct the original teleported qudit state $|\psi\rangle_{\mathrm{P}}$ using the measurement outcomes announced from Alice$_p$ and Bob as follows:

$$\begin{aligned} |\hat{\psi}\rangle_{\mathrm{C}} &= \boldsymbol{Z}_d^{-\omega(\boldsymbol{\gamma})} \boldsymbol{X}_d^{-\gamma_2} \, |\eta_6\rangle \\ &= \sum_{j \in \mathbb{Z}_d} \alpha_j \, |j\rangle_{\mathrm{C}} , \end{aligned} \tag{26}$$

which is the published quantum information on Charlie without revealing the publisher's identity, i.e., Alice$_p$.

The controlled QAP protocol for quantum information utilizes three GHZ states, each serving a distinct role in ensuring secure and anonymous data publication. The first GHZ state establishes a tripartite anonymous entanglement channel among Alice$_p$ Bob, and Charlie, i.e., Step 2), enabling Alice$_p$ to encode her publication qudit using controlled X-qudit and QFT operations, i.e., Step 3)-a) and Step 3)-b), before measurement, i.e., Step 3)-c). The remaining two GHZ states enable the anonymous announcement of her measurement outcomes, ensuring that the entire process remains untraceable, i.e., Step 3)-d).

B. Untraceability

Protocol 2 combines two main ingredients: i) anonymous QAP channel generation and ii) anonymous qudit teleportation. We now show its untraceable property in both phases using the same argument in verifying the untraceability of Protocol 1. In the worst adversarial scenario, we assume again Eve can access the entire joint quantum states $|\boldsymbol{\eta}_1\rangle$ and $|\boldsymbol{\eta}_5\rangle$ in the two protocol phases. Note that these two quantum states do not rely on the publisher's identity $p \in \mathcal{A}$, implying the anonymity of Protocol 2, i.e., holding the anonymity of both the QAP channel generation and the qudit teleportation in the protocol. Let $|\boldsymbol{\eta}_1\rangle_p$ and $|\boldsymbol{\eta}_5\rangle_p$ be the $(n+2)$-partite state and the tripartite four-qudit state corresponding to the publisher

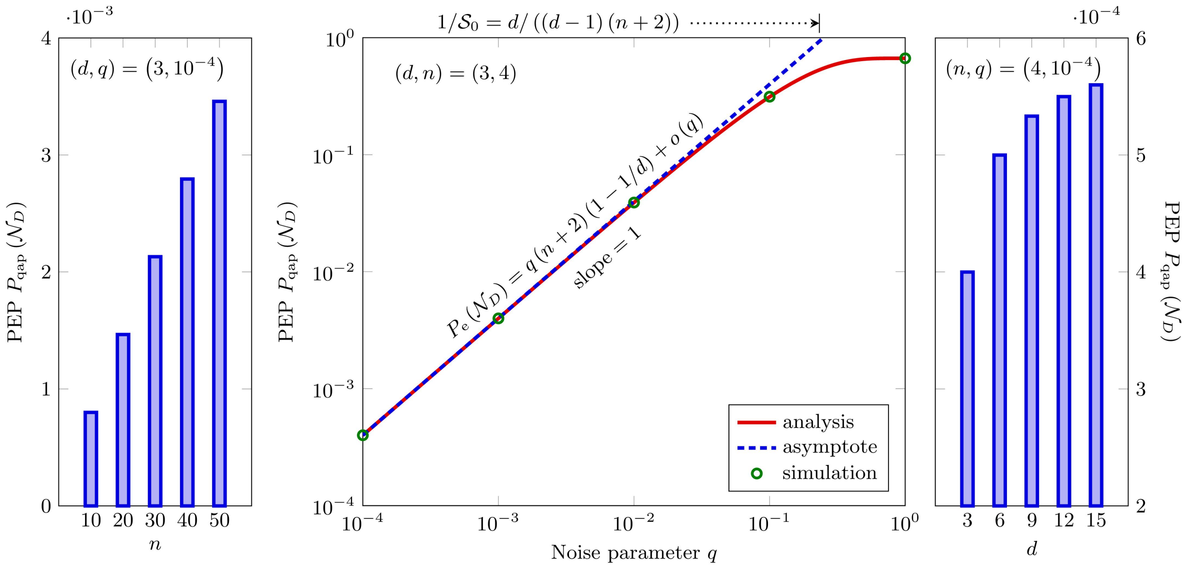


Fig. 4. PEP $P_{\text{qap}}(\mathcal{N}_D)$ for the QAP Protocol 1 as a function of the noise parameter q when $n=4$ and $d=3$ under depolarizing noise $\mathcal{N}_D$ (center). The PEP $P_{\text{qap}}(\mathcal{N}_D)$ is also plotted as a function of the number n of users when $(d,q) = (3, 10^{-4})$ (left) and the qudit dimension d when $(n,q) = (4, 10^{-4})$ (right), respectively.

$p \in \mathcal{A}$, respectively. Then, the probability that Eve correctly identifies the publisher in Protocol 2 is given by

$$\begin{aligned} P_{\text{A}} &= \frac{1}{n} \sum_{i \in \mathcal{A}} \mathbb{P}\Big\{ I_{\mathcal{A}} \mid |\boldsymbol{\eta}_1 \boldsymbol{\eta}_5\rangle_{\mathsf{p}} = |\boldsymbol{\eta}_1 \boldsymbol{\eta}_5\rangle_i \Big\} \\ &= \frac{1}{n} \sum_{i \in \mathcal{A}} \text{tr}\left\{ \boldsymbol{\Pi}_{1i} \otimes \boldsymbol{\Pi}_{5i} \, |\boldsymbol{\eta}_1 \boldsymbol{\eta}_5\rangle_i \langle \boldsymbol{\eta}_1 \boldsymbol{\eta}_5| \right\} \\ &= \frac{1}{n} \text{tr}\left\{ \sum_{i \in \mathcal{A}} \boldsymbol{\Pi}_{1i} \, |\boldsymbol{\eta}_1\rangle\langle \boldsymbol{\eta}_1| \right\} \text{tr}\left\{ \sum_{i \in \mathcal{A}} \boldsymbol{\Pi}_{5i} \, |\boldsymbol{\eta}_5\rangle\langle \boldsymbol{\eta}_5| \right\} \\ &= \frac{1}{n} \text{tr}\left\{ |\boldsymbol{\eta}_1\rangle\langle \boldsymbol{\eta}_1| \right\} \text{tr}\left\{ |\boldsymbol{\eta}_5\rangle\langle \boldsymbol{\eta}_5| \right\} = \frac{1}{n} \end{aligned} \tag{27}$$

where the sets of POVM operators $\boldsymbol{\Pi}_{1i}$ and $\boldsymbol{\Pi}_{5i}$, $i \in \mathcal{A}$, are to perform the measurement on $|\boldsymbol{\eta}_1\rangle_p$ and $|\boldsymbol{\eta}_5\rangle_p$, respectively.

V. QAP Protocols with Noisy Carriers

In this section, we analyze the QAP performance in a noisy quantum network.

A. Noisy QAP Carriers

A quantum depolarizing channel is a completely positive trace-preserving (CPTP) map that transforms a quantum state into a linear combination of itself and a completely mixed state. We consider that each qudit of the d-dimensional GHZ state is subject to the local depolarizing noise as follows:

$$\mathcal{N}_D(\boldsymbol{\varXi}) = (1-q)\,\boldsymbol{\varXi} + \frac{q}{d} \boldsymbol{I}_d \tag{28}$$

where $\boldsymbol{\varXi}$ is a density matrix for the d-dimensional qudit state and $q \in [0,1]$ denotes a noise parameter such that the quantum state $\boldsymbol{\varXi}$ is *depolarized*, i.e., completely lost and evolves into the completely mixed qudit state $\boldsymbol{I}_d/d$ with probability q while left untouched (no error) with probability $1-q$. Let $\boldsymbol{U}_{ij}$, $i,j \in \mathbb{Z}_d$, be the Heisenberg–Weyl basis defined by [54]

$$\boldsymbol{U}_{ij} = \boldsymbol{X}_d^i \boldsymbol{Z}_d^j. \tag{29}$$

Then, we can describe the isotropic depolarizing noise $\mathcal{N}_D(\boldsymbol{\varXi})$ in the Kraus operator-sum representation:

$$\mathcal{N}_D(\boldsymbol{\varXi}) = (1-q)\,\boldsymbol{\varXi} + \frac{q}{d^2} \sum_{i,j \in \mathbb{Z}_d} \boldsymbol{U}_{ij} \boldsymbol{\varXi} \boldsymbol{U}_{ij}^{\dagger} \tag{30}$$

where † denotes the conjugate transpose; the trace-preserving property follows from the fact that $\sum_{i,j \in \mathbb{Z}_d} \boldsymbol{U}_{ij}^{\dagger} \boldsymbol{U}_{ij} = d^2 \boldsymbol{I}_d$; and combining all d^2 anisotropic depolarizing noise maps $\boldsymbol{U}_{ij} \boldsymbol{\varXi} \boldsymbol{U}_{ij}^{\dagger}$ each with probability q/d^2 transforms the quantum system to the completely mixed state $\boldsymbol{I}_d/d$ with depolarizing probability q. We also consider noisy interactions that generalize bit-flip (Pauli-X) and phase-flip (Pauli-Z) qubit noises to a d-dimensional qudit system. The *symbol-shift* (or X-qudit) quantum noise is described as

$$\mathcal{N}_X(\boldsymbol{\varXi}) = (1-q)\,\boldsymbol{\varXi} + \frac{q}{d-1} \sum_{j=1}^{d-1} \boldsymbol{X}_d^j \boldsymbol{\varXi} \boldsymbol{X}_d^{-j} \tag{31}$$

where the qudit is left untouched with probability $1-q$, while there is a symbol-shift error with probability q. Similarly, the *phase-shift* (or Z-qudit) quantum noise is defined as

$$\mathcal{N}_Z(\boldsymbol{\varXi}) = (1-q)\,\boldsymbol{\varXi} + \frac{q}{d-1} \sum_{j=1}^{d-1} \boldsymbol{Z}_d^j \boldsymbol{\varXi} \boldsymbol{Z}_d^{-j}. \tag{32}$$

Suppose that the $(n+2)$-partite d-dimensional QAP carrier (GHZ state) is under the noisy environment as follows:

$$\begin{aligned} \boldsymbol{\varXi}_{\text{ghz}}(\mathcal{N}) &= \mathcal{N}^{\otimes n+2}\left(|\mathsf{ghz}\rangle_{\mathcal{QN}} \langle \mathsf{ghz}| \right) \\ &= \frac{1}{d} \sum_{i,j \in \mathbb{Z}_d} \mathcal{N}\left(|i\rangle\langle j| \right)^{\otimes n+2} \end{aligned} \tag{33}$$

where $\mathcal{N} \in \{\mathcal{N}_D, \mathcal{N}_X, \mathcal{N}_Z\}$. For the noiseless case (i.e., $q=0$), we denote it simply as $\boldsymbol{\varXi}_{\text{ghz}} = |\mathsf{ghz}\rangle_{\mathcal{QN}} \langle \mathsf{ghz}|$.

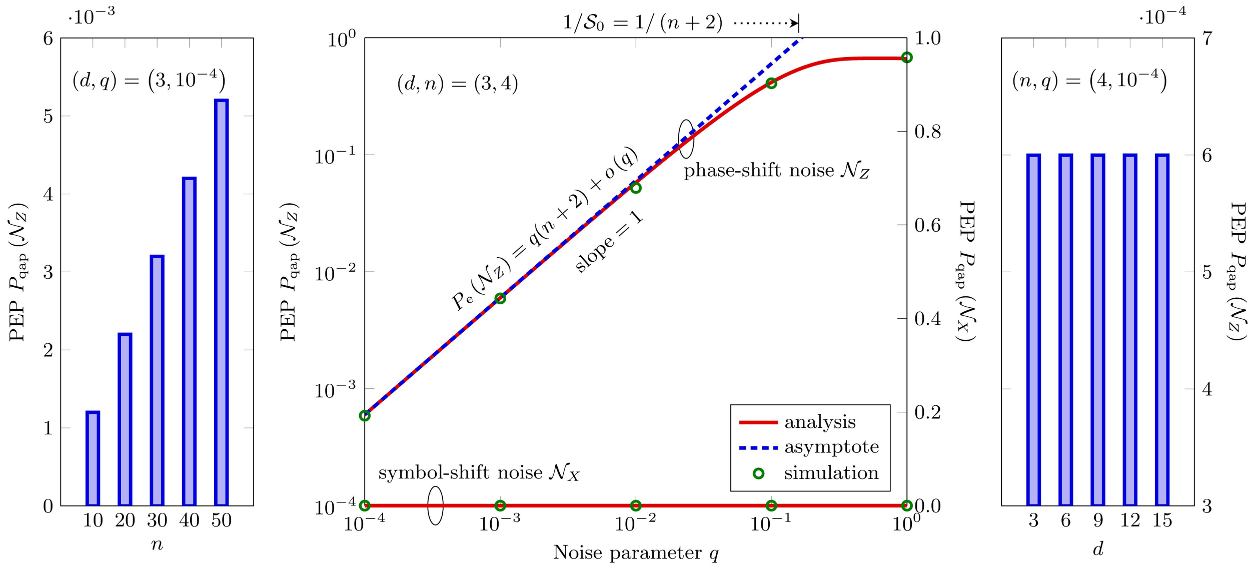


Fig. 5. PEP $P_{\text{qap}}(\mathcal{N})$ for the QAP Protocol 1 as a function of the noise parameter q when $n = 4$ and $d = 3$ under symbol-shift noise $\mathcal{N}_X$ and phase-shift noise $\mathcal{N}_Z$ (center). The PEP $P_{\text{qap}}(\mathcal{N}_Z)$ is also plotted as a function of the number n of users when $(d,q) = (3, 10^{-4})$ (left) and the qudit dimension d when $(n,q) = (4, 10^{-4})$ (right) under phase-shift noise $\mathcal{N}_Z$, respectively.

B. QAP Error Probability

Now, we analyze the PEP $P_{\text{qap}}(\mathcal{N})$ for Protocol 1 with the noisy QAP carrier $\boldsymbol{\mathit{\Xi}}_{\text{ghz}}(\mathcal{N})$:

$$P_{\text{qap}}(\mathcal{N}) = \sum_{m \in \mathbb{Z}_d} \mathbb{P}\left\{\hat{\boldsymbol{\zeta}} \neq \boldsymbol{\zeta} | \boldsymbol{\zeta} = m, \boldsymbol{\mathit{\Xi}}_{\text{ghz}}(\mathcal{N})\right\} \mathbb{P}\{\boldsymbol{\zeta} = m\} \tag{34}$$

where $\mathbb{P}\{\boldsymbol{\zeta} = m\} = 1/d$ for equiprobable *a priori* publication information. Due to the symmetry of error events, we can consider $\boldsymbol{\zeta} = 0$ to calculate the PEP. The decoding of the publication information is equivalent to measuring the $(n+2)$ qudits of the noisy state (33) locally in the Fourier basis and calculating the d-ary sum $\omega(\boldsymbol{\mu})$ of these measurement outcomes $\boldsymbol{\mu} \in \mathbb{Z}_d^{n+2}$—i.e., the decoded publication information is equal to $\hat{\boldsymbol{\zeta}} = \omega(\boldsymbol{\mu})$.

The Fourier-basis projection of $|i\rangle\langle j|$ for $i, j, k \in \mathbb{Z}_d$ is given by

$$\langle k|_{\mathcal{F}} \, |i\rangle\langle j| k\rangle_{\mathcal{F}} = \frac{1}{d} \exp\left(\frac{\iota 2\pi k (i-j)}{d}\right) \tag{35}$$

where $|k\rangle_{\mathcal{F}} = \mathfrak{F}_d |k\rangle \in \mathcal{B}_{\mathcal{F}}(d)$ is the kth Fourier-basis state. Hence, we obtain these projections of the quantum noise map $\mathcal{N}$ on the diagonal $|i\rangle\langle i|$ and non-diagonal $|i\rangle\langle j|$ states for $i \neq j \in \mathbb{Z}_d$ as follows:

$$\langle k|_{\mathcal{F}} \mathcal{N}(|i\rangle\langle i|) \, |k\rangle_{\mathcal{F}} = 1/d \tag{36}$$

$$\langle k|_{\mathcal{F}} \mathcal{N}(|i\rangle\langle j|) \, |k\rangle_{\mathcal{F}} = \frac{G_{\mathcal{N}}}{d} \exp\left(\frac{\iota 2\pi k (i-j)}{d}\right) \tag{37}$$

where $L_d = (d-1)/d$ and

$$G_{\mathcal{N}} = \begin{cases} 1-q, & \mathcal{N} = \mathcal{N}_D \\ 1, & \mathcal{N} = \mathcal{N}_X \\ 1 - q/L_d, & \mathcal{N} = \mathcal{N}_Z. \end{cases} \tag{38}$$

Using (33) and (36)–(38), the probability that the measurement outcome sequence $\boldsymbol{\mu}$ belongs to the set $\mathbb{Z}_d^{n+2}(0)$ of $(n+2)$-tuple d-ary sequences (or vectors) with the zero d-ary sum for the noisy QAP carrier $\boldsymbol{\mathit{\Xi}}_{\text{ghz}}(\mathcal{N})$ is given by

$$\mathbb{P}\left\{\boldsymbol{\mu} \in \mathbb{Z}_d^{n+2}(0) \, | \boldsymbol{\mathit{\Xi}}_{\text{ghz}}(\mathcal{N})\right\} = \frac{1 + (d-1)\, G_{\mathcal{N}}^{n+2}}{d^{n+2}}. \tag{39}$$

Since $\left|\mathbb{Z}_d^{n+2}(0)\right| = d^{n+1}$, we obtain the QAP error probability under quantum noise $\mathcal{N}$ as follows:

$$\begin{aligned} P_{\text{qap}}(\mathcal{N}) &= 1 - \mathbb{P}\{\omega(\boldsymbol{\mu}) = 0 | \boldsymbol{\zeta} = 0, \boldsymbol{\mathit{\Xi}}_{\text{ghz}}(\mathcal{N})\} \\ &= L_d \left(1 - G_{\mathcal{N}}^{n+2}\right). \end{aligned} \tag{40}$$

Note that the error-free robustness—namely, $P_{\text{qap}}(\mathcal{N}_X) = 0$—of the QAP protocol under X-qudit noise $\mathcal{N}_X$ is due to the fact that projecting $|i\rangle\langle j|$ in the Fourier basis is equivalent to projecting its symbol-shift version in the Fourier basis, i.e.,

$$\langle k|_{\mathcal{F}} \, \boldsymbol{X}_d \, |i\rangle\langle j| \, \boldsymbol{X}_d^{-1} \, |k\rangle_{\mathcal{F}} = \langle k|_{\mathcal{F}} \, |i\rangle\langle j| k\rangle_{\mathcal{F}}. \tag{41}$$

In the low-noise regime ($q \ll 1$), the QAP error probability $P_{\text{qap}}(\mathcal{N})$ behaves as

$$P_{\text{qap}}(\mathcal{N}) = q\mathcal{S}_0 + o(q) \qquad (q \to 0) \tag{42}$$

where

$$\begin{aligned} \mathcal{S}_0 &= \lim_{q \to 0} \frac{P_{\text{qap}}(\mathcal{N})}{q} \\ &= \begin{cases} L_d (n+2), & \mathcal{N} = \mathcal{N}_D \\ n+2, & \mathcal{N} = \mathcal{N}_Z. \end{cases} \end{aligned} \tag{43}$$

The asymptotic PEP (42) reveals that in a log-log plot, the low-noise slope of $P_{\text{qap}}(\mathcal{N})$ as a function of q is equal to one. The quantity $1/\mathcal{S}_0$ represents the low-noise offset in the PEP asymptote as $q \to 0$. Specifically, $P_{\text{qap}}(\mathcal{N})$ scales linearly with the phase-shift and depolarizing probability q and the network size $(n+2)$ in the low-noise regime. Figs. 4 and 5

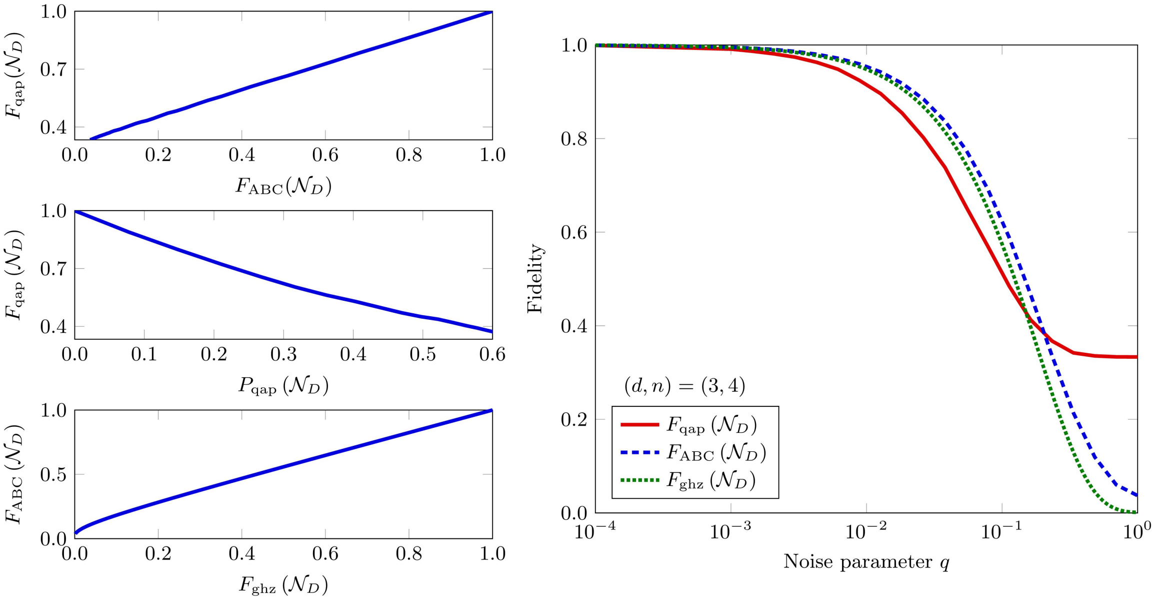


Fig. 6. QAP fidelity $F_{\rm qap}(\mathcal{N}_D)$ for Protocol 2 along with the subprotocol QAP channel fidelity $F_{\rm ABC}(\mathcal{N}_D)$ and QAP carrier fidelity $F_{\rm ghz}(\mathcal{N}_D)$ as a function of the noise parameter q when $n=4$ and $d=3$ under depolarizing noise $\mathcal{N}_D$ (right). The QAP fidelity $F_{\rm qap}(\mathcal{N}_D)$ is also plotted as a function of the subprotocol fidelity and PEP performance: $F_{\rm ABC}(\mathcal{N}_D)$ (upper left) and $P_{\rm qap}(\mathcal{N}_D)$ of Protocol 1 (anonymous symbol announcement) for $\boldsymbol{\gamma}_1$ or $\boldsymbol{\gamma}_2$ (center left). In addition, we plot the QAP channel fidelity $F_{\rm ABC}(\mathcal{N}_D)$ as a function of the QAP carrier fidelity $F_{\rm ghz}(\mathcal{N}_D)$ (lower left).

show the QAP error probability $P_{\rm qap}(\mathcal{N})$ for Protocol 1 as a function of the noise parameter q when $n=4$ and $d=3$ under depolarizing noise $\mathcal{N}_D$, symbol-shift noise $\mathcal{N}_X$, and phase-shift noise $\mathcal{N}_Z$ (center). We also depict the PEP $P_{\rm qap}(\mathcal{N})$ at the noise parameter $q=10^{-4}$ as a function of the number n of users when $d=3$ (left) and the qudit dimension d when $n=4$ (right) under depolarizing noise $\mathcal{N}_D$ (Fig. 4) and phase-shift noise $\mathcal{N}_Z$ (Fig. 5), respectively. From these figures, we ascertain the error-free $P_{\rm qap}(\mathcal{N}_X)$ under symbol-shift noise $\mathcal{N}_X$ and the asymptotic PEP linearity in (42) including the d-independent $P_{\rm qap}(\mathcal{N}_Z)$ under phase-shift noise $\mathcal{N}_Z$ in the low-noise regime.

C. QAP Fidelity

Under noise $\mathcal{N}$, the QAP carrier $\boldsymbol{\Xi}_{\rm ghz}(\mathcal{N})$ has the fidelity

$$\begin{aligned} F_{\rm ghz}(\mathcal{N}) &= \varrho\left(\boldsymbol{\Xi}_{\rm ghz}(\mathcal{N}), |\mathsf{ghz}\rangle_{\mathcal{QN}}\right) \\ &= \langle \mathsf{ghz}|_{\mathcal{QN}}\, \boldsymbol{\Xi}_{\rm ghz}(\mathcal{N})\, |\mathsf{ghz}\rangle_{\mathcal{QN}} \end{aligned} \tag{44}$$

where the fidelity $\varrho(\boldsymbol{\Xi}, \boldsymbol{\Upsilon})$ between two density matrices $\boldsymbol{\Xi}$ and $\boldsymbol{\Upsilon}$ in general is defined by

$$\varrho(\boldsymbol{\Xi}, \boldsymbol{\Upsilon}) = \left[\operatorname{tr}\left\{\sqrt{\sqrt{\boldsymbol{\Xi}}\boldsymbol{\Upsilon}\sqrt{\boldsymbol{\Xi}}}\right\}\right]^2. \tag{45}$$

After some algebra, we obtain

$$F_{\rm ghz}(\mathcal{N}) = \begin{cases} \frac{1}{d}(1-qL_d)^{n+2} + L_d G_{\mathcal{N}}^{n+2} & \\ \quad + L_d (q/d)^{n+2}, & \mathcal{N}=\mathcal{N}_D \\ (1-q)^{n+2} + (d-1)\left(\frac{q}{d-1}\right)^{n+2}, & \mathcal{N}=\mathcal{N}_X \\ \frac{1}{d} + L_d G_{\mathcal{N}}^{n+2}, & \mathcal{N}=\mathcal{N}_Z. \end{cases} \tag{46}$$

As illustrated in Figs. 6 and 7, we simulate the QAP fidelity $F_{\rm qap}(\mathcal{N})$ between the publishing qudit $|\psi\rangle_{\rm P}$ and the noisy published state $\boldsymbol{\Xi}_{\rm C}(\mathcal{N})$ for Protocol 2 with the noisy QAP carrier $\boldsymbol{\Xi}_{\rm ghz}(\mathcal{N})$:

$$\begin{aligned} F_{\rm qap}(\mathcal{N}) &= \varrho\left(\boldsymbol{\Xi}_{\rm C}(\mathcal{N}), |\psi\rangle_{\rm P}\right) \\ &= \langle\psi|_{\rm P}\, \boldsymbol{\Xi}_{\rm C}(\mathcal{N})\, |\psi\rangle_{\rm P}\,. \end{aligned} \tag{47}$$

For the subprotocol, the QAP channel fidelity is also given by

$$\begin{aligned} F_{\rm ABC}(\mathcal{N}) &= \varrho\left(\boldsymbol{\Xi}_{\rm ABC}(\mathcal{N}), |\mathsf{ghz}\rangle_{\rm ABC}\right) \\ &= \langle\mathsf{ghz}|_{\rm ABC}\, \boldsymbol{\Xi}_{\rm ABC}(\mathcal{N})\, |\mathsf{ghz}\rangle_{\rm ABC} \end{aligned} \tag{48}$$

where $\boldsymbol{\Xi}_{\rm ABC}(\mathcal{N})$ denotes the noisy QAP channel generated by the noisy QAP carrier $\boldsymbol{\Xi}_{\rm ghz}(\mathcal{N})$. With Fourier-basis $|0\rangle_{\mathcal{F}}\langle 0|$ measurements of all parties except Alice$_p$, Bob, and Charlie on their respective qudits, after some algebra, we obtain

$$F_{\rm ABC}(\mathcal{N}) = \begin{cases} \frac{1}{d} + L_d G_{\mathcal{N}}^{n+2} - L_d\left(\frac{d-2}{d^2}\right)q^3 & \\ \quad + \frac{3}{d}L_d q\,(qL_d - 1), & \mathcal{N}=\mathcal{N}_D \\ 1 - q^3 L_{d-1}/L_d + 3q\,(q-1), & \mathcal{N}=\mathcal{N}_X \\ F_{\rm ghz}(\mathcal{N}), & \mathcal{N}=\mathcal{N}_Z. \end{cases} \tag{49}$$

Figs. 6 and 7 show the QAP fidelity $F_{\rm qap}(\mathcal{N})$ for Protocol 2 as a function of the noise parameter q when $n=4$ and $d=3$ under depolarizing noise $\mathcal{N}_D$, symbol-shift noise $\mathcal{N}_X$, and phase-shift noise $\mathcal{N}_Z$ (right). In Fig. 6, the subprotocol QAP channel fidelity $F_{\rm ABC}(\mathcal{N})$ and QAP carrier fidelity $F_{\rm ghz}(\mathcal{N})$ are also depicted to illustrate the effect of depolarizing noise. In addition, to ascertain the effects of noisy subprotocols, the QAP $F_{\rm qap}(\mathcal{N})$ is plotted as a function of $F_{\rm ABC}(\mathcal{N})$ (upper left) and $F_{\rm ghz}(\mathcal{N})$ (lower left) under depolarizing noise $\mathcal{N}_D$ (Fig. 6), symbol-shift noise $\mathcal{N}_X$, and phase-shift noise $\mathcal{N}_Z$ (Fig. 7), respectively. In Fig. 6, we also plot the $F_{\rm qap}(\mathcal{N}_D)$ as a function of $P_{\rm qap}(\mathcal{N}_D)$ of Protocol 1 (anonymous symbol

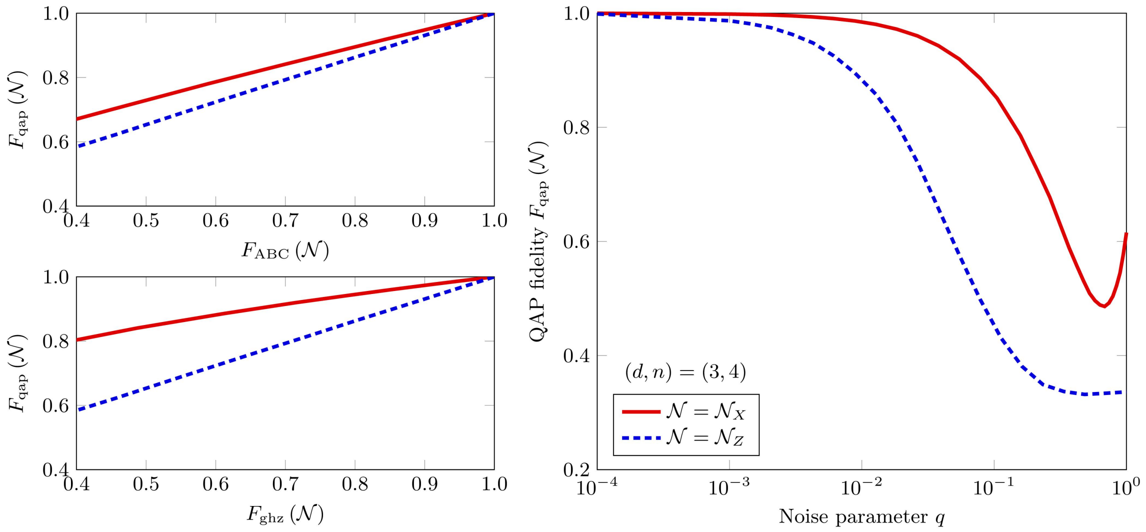


Fig. 7. QAP fidelity $F_{\mathrm{qap}}(\mathcal{N})$ for Protocol 2 as a function of the noise parameter q when $n = 4$ and $d = 3$ under symbol-shift noise $\mathcal{N}_X$ and phase-shift noise $\mathcal{N}_Z$ (right). The QAP fidelity $F_{\mathrm{qap}}(\mathcal{N})$ is also plotted as a function of the QAP channel fidelity $F_{\mathrm{ABC}}(\mathcal{N})$ (upper left) and the QAP carrier fidelity $F_{\mathrm{ghz}}(\mathcal{N})$ (lower left), respectively.

announcement) for anonymous γ_1 or γ_2 announcement (center left). We can see that the QAP fidelity $F_{\mathrm{qap}}(\mathcal{N})$ for Protocol 2 remains robust against the noise until approximately $q = 10^{-3}$. However, it starts decreasing significantly from around 10^{-2}, showing a sharp decline. Note that the symbol-shift noise $\mathcal{N}_X$ gives the minimum fidelity at $q = (d-1)/d = 2/3$ due to the application of the symbol-shift error with uniform probability.

Note that the core of controlled QAP protocols relies on the generation and distribution of multipartite high-dimensional GHZ states. From the analysis above, we can determine the tolerable noise levels required to maintain robust fidelity, establishing a benchmark for the minimum fidelity needed in the preparation and distribution of GHZ states to ensure the successful implementation of these protocols. The experimental implementation of these states can be realized using various quantum system modalities. Photon-based implementations are particularly relevant since we aim to distribute these states to remote parties. To realize multipartite entanglement, several degrees of freedom have been utilized, such as the path degree of freedom [55], transverse spatial modes like orbital angular momentum (OAM) [56], time and frequency modes [57], and their simultaneous use of multiple degrees [58]. Specifically, OAM modes have been shown to generate a qutrit GHZ state for tripartite systems with a fidelity of approximately 0.752 and a count rate of 1.2 millihertz (mHz) [56]. While this experiment is limited in scale, our protocols can also be adapted to qubit ($d = 2$) GHZ states, which are more salable. Notably, 18-qubit GHZ entanglement has been achieved with a fidelity of 0.708 and a count rate of 55 mHz using multiple degrees of freedom [58].

D. Degree of Anonymity

Let $P_{\mathrm{A}}(\mathcal{N})$ be the probability of correctly identifying the publisher in Definition 1 with the noisy QAP carrier $\boldsymbol{\Xi}_{\mathrm{ghz}}(\mathcal{N})$:

$$P_{\mathrm{A}}(\mathcal{N}) = \mathbb{P}\{I_{\mathcal{A}} | \boldsymbol{\Xi}_{\mathrm{ghz}}(\mathcal{N})\}, \tag{50}$$

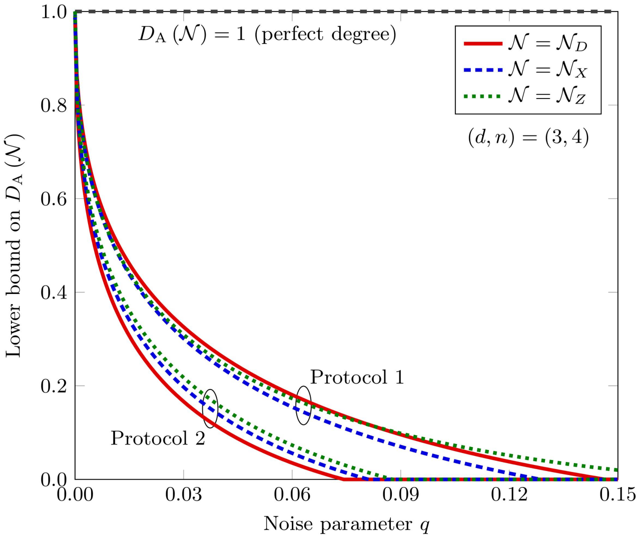


Fig. 8. Lower bounds on the degree of anonymity $D_{\mathrm{A}}(\mathcal{N})$ for Protocol 1 and Protocol 2 as a function of the noise parameter q when $n = 4$ and $d = 3$ under depolarizing $\mathcal{N}_D$, symbol-shift $\mathcal{N}_X$, and phase-shift $\mathcal{N}_Z$ noise.

which is now used to measure a degree of anonymity achieved by the QAP protocols. Similar to entropy-based measures [59], [60], this probabilistic measure specifically quantifies the uncertainty an adversary (Eve) has in identifying the publisher in the network $\mathcal{QN}(n+2)$, evaluating the effectiveness of QAP protocols. Eve assigns probabilities to honest users based on their observed network activities, with smaller groups more likely to be suspected as the source of publication. To achieve the highest degree of anonymity in communication, it is essential that each user is equally probable to be the publisher. However, Eve can reduce the level of anonymity by gathering user information and executing attacks to narrow down the group of potential publishers. The entropy-based measures utilize the overall uncertainty in this probability distribution.

To reflect the uncertainty faced by Eve in correctly identifying the publisher, we transform the probability $P_{\mathrm{A}}(\mathcal{N})$ of correct identification into the degree of anonymity, defined as:

$$D_{\mathrm{A}}(\mathcal{N}) = -\log_n P_{\mathrm{A}}(\mathcal{N}). \tag{51}$$

For the noiseless case ($q = 0$), we denote it simply as $D_{\mathrm{A}} = -\log_n P_{\mathrm{A}}$. Note that by preserving anonymity ($P_{\mathrm{A}} = 1/n$) as proved in (14) and (27), Protocols 1 and 2 for both classical and quantum information attain the maximum degree $D_{\mathrm{A}} = 1$ in a noiseless network. If Eve narrows down a potential publisher with certainty $P_{\mathrm{A}}(\mathcal{N}) = 1$, the anonymity degree vanishes—i.e., $D_{\mathrm{A}}(\mathcal{N}) = 0$. To analyze the degree $D_{\mathrm{A}}(\mathcal{N})$ of anonymity, we use the following inequality [51]:

$$\operatorname{tr}\{\boldsymbol{\Pi}(\boldsymbol{\Xi} - \boldsymbol{\Upsilon})\} \leqslant \sqrt{1 - \varrho\big(\boldsymbol{V}\boldsymbol{\Xi}\boldsymbol{V}^{\dagger}, \boldsymbol{V}\boldsymbol{\Upsilon}\boldsymbol{V}^{\dagger}\big)} \tag{52}$$

that holds for any POVM $\boldsymbol{\Pi}$, isometry operation $\boldsymbol{V}$, and two density matrices $\boldsymbol{\Xi}$ and $\boldsymbol{\Upsilon}$.

1) Controlled QAP for Classical Information (Protocol 1): Let $\boldsymbol{\Xi}_{\mathrm{e}}(\mathcal{N})$ be the noisy state of the $(n+2)$-partite encoded state $|\boldsymbol{\phi}_{\mathrm{e}}\rangle$ in Protocol 1 with the noisy QAP carrier $\boldsymbol{\Xi}_{\mathrm{ghz}}(\mathcal{N})$. Then, using (14) and (50), we have

$$\begin{aligned} P_{\mathrm{A}}(\mathcal{N}) &= \frac{1}{n}\sum_{i\in\mathcal{A}} \operatorname{tr}\{\boldsymbol{\Pi}_i \boldsymbol{\Xi}_{\mathrm{e}}(\mathcal{N})\} \\ &= \frac{1}{n}\operatorname{tr}\{\boldsymbol{\Xi}_{\mathrm{e}}(\mathcal{N})\} = \frac{1}{n} \qquad (53)\\ &\leqslant \left[\frac{1}{n}\sum_{i\in\mathcal{A}}\left(\operatorname{tr}\{\boldsymbol{\Pi}_i |\boldsymbol{\phi}_{\mathrm{e}}\rangle\langle\boldsymbol{\phi}_{\mathrm{e}}|\} + \sqrt{1 - F_{\mathrm{ghz}}(\mathcal{N})}\right)\right]^{-} \\ &= \left[\frac{1}{n} + \sqrt{1 - F_{\mathrm{ghz}}(\mathcal{N})}\right]^{-} \qquad (54) \end{aligned}$$

where $[x]^{-} = \min\{1, x\}$ is the unit cap of x; the perfect anonymity (53) follows from the completeness of POVM operators and the trace-preserving property of noisy maps; the QAP carrier fidelity $F_{\mathrm{ghz}}(\mathcal{N})$ is given in (46); and the inequality follows from (52) and the fact that the QFT $\boldsymbol{\mathfrak{F}}_d$ and X-qudit $\boldsymbol{X}_d$ are unitary (and hence, isometry). Note that (53) reveals that the noisy carrier does not deteriorate the perfect anonymity of Protocol 1, preserving the perfect degree $D_{\mathrm{A}}(\mathcal{N}) = 1$ with noise robustness. The degree of anonymity for Protocol 1 is then given by

$$D_{\mathrm{A}}(\mathcal{N}) = 1 \geqslant \left[-\log_n\left(\frac{1}{n} + \sqrt{1 - F_{\mathrm{ghz}}(\mathcal{N})}\right)\right]^{+} \tag{55}$$

where $[x]^{+} = \max\{0, x\}$ is the positive part of x and the lower bound corresponds to the minimum degree of anonymity preserved by Protocol 1, even against any privacy attacks.

2) Controlled QAP for Quantum Information (Protocol 2): Let $\boldsymbol{\Xi}_1(\mathcal{N})$ and $\boldsymbol{\Xi}_5(\mathcal{N})$ be the noisy states of $|\boldsymbol{\eta}_1\rangle$ and $|\boldsymbol{\eta}_5\rangle$ in Protocol 2 with the noisy QAP carrier $\boldsymbol{\Xi}_{\mathrm{ghz}}(\mathcal{N})$, respectively. Using (27) and similar arguments for Protocol 1, the probability of correctly identifying the publisher in Protocol 2 under noise $\mathcal{N}$ is given by

$$\begin{aligned} P_{\mathrm{A}}(\mathcal{N}) &= \frac{1}{n}\sum_{i\in\mathcal{A}} \operatorname{tr}\{(\boldsymbol{\Pi}_{1i}\otimes\boldsymbol{\Pi}_{5i})(\boldsymbol{\Xi}_1(\mathcal{N})\otimes\boldsymbol{\Xi}_5(\mathcal{N}))\} \\ &= \frac{1}{n}\operatorname{tr}\{\boldsymbol{\Xi}_1(\mathcal{N})\}\operatorname{tr}\{\boldsymbol{\Xi}_5(\mathcal{N})\} = \frac{1}{n} \qquad (56)\\ &\leqslant \left[\frac{1}{n} + \sqrt{1 - \varrho(\boldsymbol{\Xi}_1(\mathcal{N})\otimes\boldsymbol{\Xi}_5(\mathcal{N}), |\boldsymbol{\eta}_1\boldsymbol{\eta}_5\rangle)}\right]^{-} \\ &= \left[\frac{1}{n} + \sqrt{1 - F_{\mathrm{ghz}}(\mathcal{N})F_{\mathrm{ABC}}(\mathcal{N})}\right]^{-} \qquad (57) \end{aligned}$$

leading to the degree of anonymity for Protocol 2 as follows:

$$D_{\mathrm{A}}(\mathcal{N}) = 1 \geqslant \left[-\log_n\left(\frac{1}{n} + \sqrt{1 - F_{\mathrm{ghz}}(\mathcal{N})F_{\mathrm{ABC}}(\mathcal{N})}\right)\right]^{+} \tag{58}$$

where the QAP channel fidelity $F_{\mathrm{ABC}}(\mathcal{N})$ is given in (49). Again, even under noise $\mathcal{N}$, Protocol 2 achieves the perfect anonymity with $D_{\mathrm{A}}(\mathcal{N}) = 1$, while its minimum degree against Eve's attacks is characterized by the lower bound (58).

Fig. 8 illustrates the lower bounds (minimum degrees) on the degree of anonymity $D_{\mathrm{A}}(\mathcal{N})$ for Protocol 1 and Protocol 2 as a function of the noise parameter q when $n = 4$ and $d = 3$ under depolarizing noise $\mathcal{N}_D$, symbol-shift noise $\mathcal{N}_X$, and phase-shift noise $\mathcal{N}_Z$. The noise effect on the minimum degree of anonymity is similar across all three types, highlighting the importance of maintaining low noise levels to ensure perfect anonymity against adversarial attacks. As expected, the QAP protocol for quantum information (Protocol 2) exhibits more significant noise vulnerability than Protocol 1 for classical information in terms of its minimum degree.

VI. Conclusion

This paper has introduced the controlled QAC protocols for publishing both classical and quantum information. By utilizing high-dimensional multipartite entanglement, the QAP protocols ensure the anonymity of the publisher and provide untraceability even in scenarios where adversaries have access to all network resources, thereby distinguishing these protocols from classical anonymous networks. We have evaluated the robustness of the protocols against noise and adversarial attacks in terms of QAP error probability, fidelity, and degree of anonymity. This work provides privacy-preserving quantum protocols to ensure the anonymous publication of classical and quantum information in the quantum era, significantly advancing the protection of communication privacy against the emerging threats of the quantum computing age. There is considerable potential for advancing QAP protocols. One promising direction is to optimize these protocols to improve efficiency and simplify their implementation while maintaining a significant level of security by leveraging diverse quantum resources, such as mixed quantum states [61]. Furthermore, exploring these protocols in device-independent scenarios can enhance their robustness against imperfections in experimental setups, ensuring secure and reliable performance.

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, Jul. 2015.

[2] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10 474–10 498, Mar. 2021.

[3] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2820–2835, Jun. 2017.

[4] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, Aug. 2017.

[5] B. C. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," *ACM Comput. Surv.*, vol. 42, no. 4, pp. 1–53, Jun. 2010.

[6] S. Cui, S. Belguith, P. D. Alwis, M. R. Asghar, and G. Russello, "Collusion defender: Preserving subscribers' privacy in publish and subscribe systems," *IEEE Trans. Depend. Sec. Comput.*, vol. 18, no. 3, pp. 1051–1064, May 2021.

[7] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. S. Shen, "Privacy-preserving attribute-keyword based data publish-subscribe service on cloud platforms," *Inf. Sci.*, vol. 387, pp. 116–131, May 2017.

[8] S. A. Gaballah, C. Coijanovic, T. Strufe, and M. Mühlhäuser, "2PPS-publish/subscribe with provable privacy," in *Proc. IEEE Int. Symp. Reliable Distrib. Syst. (SRDS)*, Chicago, IL, USA, Sep. 2021, pp. 198–209.

[9] F. Chen, Y. Huo, J. Zhu, and D. Fan, "A review on the study on MQTT security challenge," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Washington, DC, USA, Nov. 2020, pp. 128–133.

[10] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, Firstquarter 2020.

[11] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, p. 1023–1030, Jun. 2008.

[12] U. Khalid, M. S. Ulum, A. Farooq, T. Q. Duong, O. A. Dobre, and H. Shin, "Quantum semantic communications for Metaverse: Principles and challenges," *IEEE Wireless Commun.*, vol. 30, no. 4, pp. 26–36, Aug. 2023.

[13] D. Castelvecchi, "The quantum internet has arrived (and it hasn't)," *Nature*, vol. 554, no. 7692, Feb. 2018.

[14] 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.

[15] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, p. eaam9288, Oct. 2018.

[16] 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.

[17] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum internet: Networking challenges in distributed quantum computing," *IEEE Netw.*, vol. 34, no. 1, pp. 137–143, Feb. 2020.

[18] 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.

[19] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozof, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 830-km fibre," *Nat. Photon.*, vol. 16, no. 2, pp. 154–161, Feb. 2022.

[20] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. R. N. Sangouard, and J.-D. Bancal, "Experimental quantum key distribution certified by Bell's theorem," *Nature*, vol. 607, no. 7920, pp. 682–686, Jul. 2022.

[21] F. Zaman, U. Khalid, T. Q. Duong, H. Shin, and M. Z. Win, "Quantum full-duplex communication," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 9, pp. 2966–2980, Sep. 2023.

[22] X. Yu, Y. Liu, X. Zou, Y. Cao, Y. Zhao, A. Nag, and J. Zhang, "Secret-key provisioning with collaborative routing in partially-trusted-relay-based quantum-key-distribution-secured optical networks," *J. Lightw. Technol.*, vol. 40, no. 12, pp. 3530–3545, Feb. 2022.

[23] S. N. Paing, J. W. Setiawan, M. A. Ullah, F. Zaman, T. Q. Duong, O. A. Dobre, and H. Shin, "Counterfactual quantum Byzantine consensus for human-centric Metaverse," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 4, pp. 905–918, Apr. 2024.

[24] B. Goldacre, "Are clinical trial data shared sufficiently today? Yes," *BMJ*, vol. 347, 2013.

[25] A. S. Downey and S. Olson, *Sharing Clinical Research Data: Workshop Summary*. Washington, DC: National Academies Press, 2013.

[26] 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.

[27] 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.

[28] 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, 2021.

[29] 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.

[30] L. Jiang, G. He, D. Nie, J. Xiong, and G. Zeng, "Quantum anonymous voting for continuous variables," *Phys. Rev. A*, vol. 85, p. 042309, Apr. 2012.

[31] N. Bao and N. Y. Halpern, "Quantum voting and violation of Arrow's impossibility theorem," *Phys. Rev. A*, vol. 95, p. 062306, Jun. 2017.

[32] 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, Apr. 2022.

[33] 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.

[34] F. Hahn, J. de Jong, and A. Pappa, "Anonymous quantum conference key agreement," *Phys. Rev. X*, vol. 1, p. 020325, Dec. 2020.

[35] 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.

[36] 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.

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

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] M. S. Rahman, S. DiAdamo, M. Mehic, and C. Fleming, "Quantum secure anonymous communication networks," in *Proc. Int. Conf. Quantum Commun., Netw., and Comput. (QCNC)*, Kanazawa, Japan, May 2024, pp. 346–351.

[46] Y. Wang, Z. Su, S. Guo, M. Dai, T. H. Luan, and Y. Liu, "A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 14 965–14 987, Sep. 2023.

[47] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, Feb. 1981.

[48] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for web transactions," *ACM Trans. Inf. Syst. Secur.*, vol. 1, no. 1, pp. 66–92, Nov. 1998.

[49] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 482–494, May 1998.

[50] F. Stajano and R. Anderson, "The cocaine auction protocol: On the power of anonymous broadcast," in *Proc. Inf. Hiding: 3rd Int. Workshop*, Dresden, Germany, Oct. 1999, pp. 434–447.

[51] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[52] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's theorem," in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*. Dordrecht, Netherlands: Springer, Oct. 1989, pp. 69–72.

[53] 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.

[54] C. K. Burrell, "Geometry of generalized depolarizing channels," *Phys. Rev. A*, vol. 80, no. 4, p. 042330, Sep. 2009.

[55] J. C. Adcock, C. Vigliar, R. Santagati, J. W. Silverstone, and M. G. Thompson, "Programmable four-photon graph states on a silicon chip," *Nat. Commun.*, vol. 10, p. 3528, Aug. 2019.

[56] M. Erhard, M. Malik, M. Krenn, and A. Zeilinger, "Experimental Greenberger–Horne–Zeilinger entanglement beyond qubits," *Nat. Photon.*, vol. 12, no. 12, pp. 759–764, Dec. 2018.

[57] B. Fang, M. Menotti, M. Liscidini, J. E. Sipe, and V. O. Lorenz, "Three-photon discrete-energy-entangled W state in an optical fiber," *Phys. Rev. Lett.*, vol. 123, p. 070508, Aug. 2019.

[58] X.-L. Wang *et al.*, "18-qubit entanglement with six photons' three degrees of freedom," *Phys. Rev. Lett.*, vol. 120, p. 260502, Jun. 2018.

[59] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Proc. Int. Workshop on Privacy Enhanc. Technol.*, Berlin, Heidelberg, Germany, Jun. 2002, pp. 54–68.

[60] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proc. Int. Workshop on Privacy Enhanc. Technol.*, Berlin, Heidelberg, Germany, Jun. 2002, pp. 41–53.

[61] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, no. 3, p. 648, Jul. 1999.

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 Postdoctoral 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.

Jason William Setiawan received the B.S. degree in electrical engineering from 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.

Saw Nang Paing received the B.E. degree in computer engineering and information technology from Mandalay Technology University, Myanmar, in 2019. She is working towards 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.

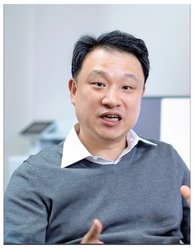
Trung Q. Duong (Fellow, IEEE) is a Canada Excellence Research Chair (CERC) and a Full Professor at Memorial University, Canada. He is also an adjunct professor at Queen's University Belfast, UK and Kyung Hee University, South Korea. He was a Distinguished Advisory Professor at Inje University, South Korea (2017-2019). His current research interests include wireless communications, quantum machine learning, and quantum optimisation.

Dr. Duong has served as an Editor/Guest Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE COMMUNICATIONS LETTERS, IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE WIRELESS COMMUNICATIONS, IEEE COMMUNICATIONS MAGAZINES, and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He received the Best Paper Award at the IEEE VTC-Spring 2013, IEEE ICC 2014, IEEE GLOBECOM 2016, 2019, 2022, IEEE DSP 2017, IWCMC 2019, 2023, 2024 and IEEE CAMAD 2023, 2024. He is the Editor in Chief of IEEE Communications Surveys & Tutorials He has received the two prestigious awards from the Royal Academy of Engineering (RAEng): RAEng Research Chair and the RAEng Research Fellow. He is the recipient of the prestigious Newton Prize 2017. He is the recipient of the prestigious Newton Prize 2017. He is a Fellow of the Engineering Institute of Canada (EIC) and Asia-Pacific Artificial Intelligence Association (AAIA).

Moe Z. Win (Fellow, IEEE) is a Professor at the Massachusetts Institute of Technology (MIT) and the founding director of the Wireless Information and Network Sciences Laboratory. Prior to joining MIT, he was with AT&T Research Laboratories and with NASA Jet Propulsion Laboratory.

His research encompasses fundamental theories, algorithm design, and network 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 has served the IEEE Communications Society as an elected Member-at-Large on the Board of Governors, as elected Chair of the Radio Communications Committee, and as an IEEE Distinguished Lecturer. Over the last two decades, he held various editorial positions for IEEE journals and organized numerous international conferences. Recently, he has served on the SIAM Diversity Advisory Committee.

Dr. Win is an elected Fellow of the AAAS, the EURASIP, the IEEE, and the IET. He was honored with two IEEE Technical Field Awards: the IEEE Kiyo Tomiyasu Award (2011) and the IEEE Eric E. Sumner Award (2006, jointly with R. A. Scholtz). His publications, co-authored with students and colleagues, have received several awards. Other recognitions include the MIT Frank E. Perkins Award (2024), the MIT Everett Moore Baker Award (2022), the IEEE Vehicular Technology Society James Evans Avant Garde Award (2022), the IEEE Communications Society Edwin H. Armstrong Achievement Award (2016), the Cristoforo Colombo International Prize for Communications (2013), the Copernicus Fellowship (2011) and the *Laurea Honoris Causa* from the Università degli Studi di Ferrara (2008), and the U.S. Presidential Early Career Award for Scientists and Engineers (2004). He is an ISI Highly Cited Researcher.



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 post-doctoral 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.