Counterfactual Quantum Communication: Information Exchange in Quantum Shadows

Saw Nang Paing, Fakhar Zaman, Uman Khalid, Trung Q. Duong, *Fellow, IEEE*, Moe Z. Win, *Fellow, IEEE*, and Hyundong Shin, *Fellow, IEEE*

***Abstract*—Counterfactual quantum communication (CQC) is an intriguing paradigm originating from quantum mechanics, enabling spatially separated parties to achieve communication tasks without the need to transmit any physical particles across the channel. Conventional quantum communication typically relies on particle transmission or utilizes entanglement-assisted protocols with local operations and classical communication, such as quantum teleportation and superdense coding, to transfer information. As the research area of quantum communication is being rapidly developed, significant progress has been made in the development of CQC. In this paper, we present a comprehensive tutorial on CQC for transmitting both classical and quantum information, noting that no physical particles are found in the channel during successful information transmission. We begin by studying the origin of CQC, followed by a detailed examination of counterfactual protocols for classical and quantum information transmission. This paper highlights the applications of CQC and outlines future research directions.**

***Index Terms*—Counterfactual communication, interaction-free measurement, quantum communication, quantum cryptography, quantum Zeno effect.**

I. Introduction

COMMUNICATION systems are crucial for the advancement of society and serve as the backbone of human interaction [1]. These systems enable the transmission of information between remote parties and facilitate the exchange of ideas within a network. Throughout the history of communication networks, these systems have evolved to improve data security, increase data rates, achieve high throughput efficiency, and enhance accessibility [2]–[4]. In the 19th century, the invention of the telephone and the telegraph significantly advanced communication systems by enabling the transmission of information in the form of electrical signals over long distances [5]. These inventions not only increased the transmission rate compared to ancient communication methods but also laid the foundation for the modern-day communication infrastructure [6]–[15] (see Fig. 1).

Modern-day communication systems with enhanced data rates and accessibility play a vital role in connecting individuals and businesses all over the world. For instance, it is expected that the 6G era of wireless communication will enable numerous services and applications, including the Internet-of-Everything, unhackable Internet, smart health care, autonomous transportation systems, and smart banking [15]–[19]. These applications and services require transmitting secret information over public channels. However, the communication security of classical cryptographic systems relies on the assumed hardness of computational problems such as prime factorization, and their security is threatened by quantum computers [20]–[22]. The development of quantum technologies can allow eavesdroppers to break access controls over the open Internet (trust), steal private data (security), or user credentials to access unauthorized resources (privacy), which can compromise user safety and can even lead to national security concerns. Furthermore, the possibility of delayed attacks on recorded data makes these concerns even more crucial. Hence, ensuring the confidentiality, integrity, and authenticity of transmitted data is paramount to maintaining trust and reliability in communication networks.

Quantum technologies provide unique ways to transmit secret information with unconditional security and the capability to detect the presence of an eavesdropper in the channel. Quantum cryptography—a subfield of quantum communication—provides state-of-the-art protocols such as quantum key distribution (QKD)—*to distribute a secret key in a network with information-theoretic security* [23]; anonymous quantum algorithms—*to enable legitimate parties to perform network operations privately and securely without revealing their identities*; and quantum secure direct communication (QSDC)—*to enable secure communication without establishing a secret key* [24]–[34]. On the other hand, quantum superdense coding (QSC)—*enables a sender to transmit two-bit classical information in one qubit using preshared entanglement*—and quantum teleportation (QT)—*allows a sender to convey a single qubit of quantum information by utilizing two classical bits and one preshared entangled qubit pair*—allowing to transmit classical and quantum information in quantum net-

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) under RS-2025-00556064 and by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2025-RS-2021-II212046) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation). The work of T. Q. Duong was supported in part by the Canada Excellence Research Chair (CERC) Program CERC-2022-00109, in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant Program RGPIN-2025-04941, and in part by the NSERC CREATE program (Grant number 596205-2025). The work of M. Z. Win was supported in part by the National Science Foundation under Grant CCF-2153230. *(Corresponding author: Hyundong Shin.)*

S. N. Paing, F. Zaman, U. Khalid, 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). S. N. Paing and F. Zaman contributed equally to this paper.

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, 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).

works, respectively [11], [35]–[37]. However, these protocols demand a common phase reference between distant parties in a quantum network [38], [39].

In quantum networks, a major limitation for quantum computation and communication protocols includes an implicit assumption regarding prior shared phase reference among remote parties—*the existence of common definitions of quantum superposition states and non-diagonal Hamiltonian evolution* [40], [41]. Consider that Alice prepares a qubit in $|\psi\rangle_{\mathrm{A}} = |+\rangle$ state and transmits the prepared state to Bob via a quantum channel, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. In the absence of the shared phase reference, Bob reads the state as $|\psi\rangle_{\mathrm{B}} = (|0\rangle + e^{-\imath\varphi}|1\rangle)/\sqrt{2}$ even if Bob knows the basis of the initial state, where $\imath = \sqrt{-1}$ and φ is the relative phase. Hence, it is evident that the lack of a shared phase reference leads to undesired errors, even in perfect channel conditions. In counterfactual quantum communication (CQC), qubits always undergo local quantum operations since no particles carrying information are transmitted across the channel. Therefore, independent local definitions regarding a phase reference are attainable in a counterfactual scenario [42]. In the era of information theory, one of the most significant advantages of quantum communication over classical communication includes theoretical unconditional security enabled by the principles of quantum mechanics, including quantum superposition, quantum non-locality, and quantum entanglement. However, there can still be vulnerabilities under practical deployment due to device imperfections. Recently, it has been shown that if an eavesdropper (Eve) utilizes a CQC setup, she can break the security of the conventional quantum cryptography protocols [43]. In addition, it has also been shown that counterfactual quantum cryptography can detect the presence of an eavesdropper even if it launches counterfactual attacks [43].

Counterfactuality is a surprising phenomenon in quantum mechanics, which has no counterpart in classical physics [49]. The fundamental concept of counterfactuality is that the result of an event may be learned, even if the event does not occur. The idea of counterfactuality was initiated in counterfactual quantum computation, which enables determining the outcome of a computation without running the computer [50]. In communication systems, counterfactuality allows transmission of information without transmitting any physical particle over the channel, categorized as partially and fully counterfactual [51]–[57]. For instance, counterfactual communication to convey a single bit of classical information has two possible bit values—*either 0 or 1* [58]. In this scenario, communication protocols counterfactual for both bit values are categorized as fully counterfactual protocols. Otherwise, the protocols are categorized as partially counterfactual. Counterfactuality was first introduced in communication systems as a cryptographic algorithm—called the Noh protocol—to distribute a secret key in a quantum network, but no information-carrying particle is transmitted over the channel. The basic concept of the Noh algorithm is derived from interaction-free measurement (IFM), allowing for the detection of the absence or presence of an absorptive object (AO) in an interferometer without direct physical interaction [59]. The IFM was initially introduced

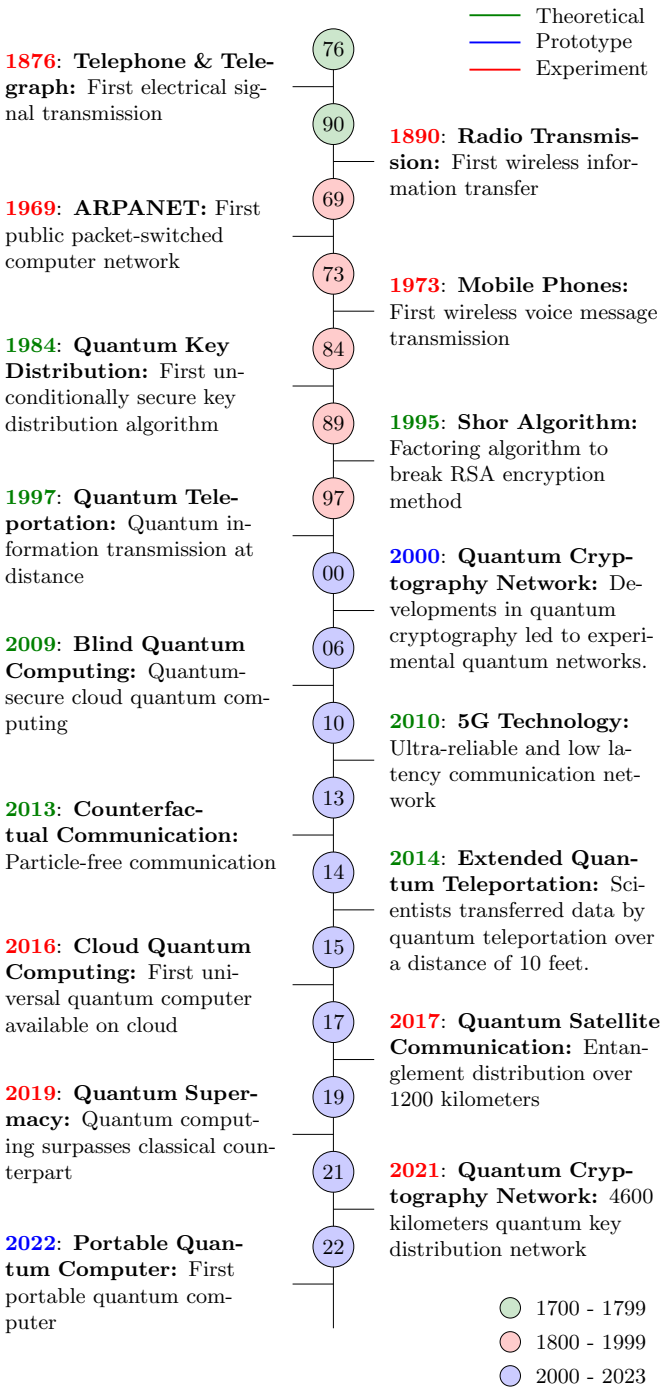


Fig. 1. Evolution of communication systems and networks [10]–[12], [21], [24], [44]–[48].

using the Mach-Zenhander interferometer (MZI), where the presence of an AO in one of the interferometer's arms disrupts the photon's interference pattern without absorbing it [60], [61]. However, it limits the key distribution rate to $1/8$ in ideal channel conditions.

The direct CQC leverages the chained quantum Zeno (CQZ) effect, encoding a classical bit as the absence or presence of the AO within the interferometer. When an AO is present, the communication protocol is signified as counterfactual. However,

it has been argued that in the absence of an AO, the photon leaves a weak trace in the transmission channel, compromising the protocol's counterfactual nature [12]. Recently, this direct CQC protocol has been adjusted to achieve counterfactuality by removing the weak trace [62]. Notably, to counterfactually transfer classical information, the AO in the interferometer is classically controlled by the sender. Conversely, transferring quantum information necessitates using a quantum AO (QAO) in a superposition of absence and presence states. This concept was first showcased in [63] for counterfactual quantum information transfer, requiring a single-bit classical announcement. It was further expanded in [64] to enable quantum information transfer without any physical particles passing through either a quantum or classical channel by employing controlled disentanglement. Later on, a relatively efficient version of the aforementioned counterfactual communication protocol was introduced in [65] that utilizes the dual CQZ effect.

Note that the concept of CQC fundamentally differs from quantum teleportation in its mechanism of information transfer. CQC enables the transmission of classical information without any physical propagation of an information-carrying particle through the communication channel. Instead, the measurement frequency—the rate at which weak, interaction-free measurements are performed within CQZ gate—carries the information to the receiver [66]. Notably, CQC does not require pre-shared entanglement or classical communication for its operation. In contrast, quantum teleportation relies on both pre-shared entanglement and classical communication to transmit a quantum state. Although no qubit physically travels through the channel, the process involves performing a Bell state measurement (BSM) on the sender's side, which destroys both the original quantum state and one qubit from the entangled pair. The receiver then reconstructs the quantum state by applying quantum operations based on the classical information received. Furthermore, the success probability of CQC is inherently probabilistic due to its reliance on IFM and the probability of photon survival. However, the increase in the success probability comes at the cost of increased channel usage and time consumption. Quantum teleportation is theoretically deterministic under ideal conditions, but may exhibit probabilistic failures in practical implementations due to entanglement imperfections and decoherence. These fundamental differences illustrate two distinct quantum communication paradigms: CQC achieves information transfer by eliminating particle transmission entirely, whereas quantum teleportation transfers quantum states by leveraging entanglement and classical communication.

From the above discussion, it is clear that CQC has gained a lot of attention in the last decade due to its applications and unique properties, such as enhanced security and no shared phase requirement. This paper presents a comprehensive survey of counterfactual communication and compares the performance of the different protocols. The rest of the paper is organized as follows. Section II overviews the basics of quantum information, such as quantum states, quantum measurements, quantum entanglement, and quantum operations. Section III describes the fundamentals of counterfactual communication, including interferometers and the quantum Zeno (QZ) effect, followed by IFM. Section IV presents the fundamental gates to achieve communication and cryptography in counterfactual manners. In Section V, we describe simplex and full-duplex communication protocols to transfer classical as well as quantum information between remote parties in a quantum network. Section VI presents counterfactual QKD and QSDC algorithms. Section VII describes the experimental implementation of counterfactual QKD and direct CQC protocols. Section VIII discusses open challenges and future research directions. Finally, Section IX concludes this tutorial.

TABLE I
OUTLINE OF THE PAPER

Notation: Quantum states and quantum density operators are denoted Dirac notation (e.g., $|\psi\rangle$) and uppercase letters (e.g., $\boldsymbol{\Xi}$), respectively. The identity, Pauli-x, Pauli-y, Pauli-z, and Hadamard matrices are denoted by $\boldsymbol{I}$, $\boldsymbol{P}_{\mathrm{x}}$, $\boldsymbol{P}_{\mathrm{y}}$, $\boldsymbol{P}_{\mathrm{z}}$, and $\boldsymbol{P}_{\mathrm{h}}$, respectively. The Hamiltonian of a quantum system is denoted $\boldsymbol{H}$. The tensor product is denoted by $\otimes$ and the mth tensor power of $\boldsymbol{X}$ is denoted by $\boldsymbol{X}^{\otimes m}$.

II. Preliminaries

In this section, we provide the fundamentals of quantum mechanics relevant to our work, including quantum states, multiqubit states, quantum measurement, and quantum gates.

A. Quantum States

A classical bit, or simply a bit, is the fundamental unit of information in classical information processing, represented by either 0 or 1. A quantum bit, or qubit, is the quantum analogue of the classical bit and is characterized by a superposition of orthonormal basis states $|\mu_0\rangle$ and $|\mu_1\rangle$ for a two-dimensional complex Hilbert space [67]:

$$|\psi\rangle = a_0|\mu_0\rangle + a_1|\mu_1\rangle \tag{1}$$

where a_0 and a_1 are complex coefficients with $|a_0|^2+|a_1|^2 = 1$. In quantum information processing, the orthonormal basis states $|0\rangle$ and $|1\rangle$, known as the *computational basis states*, correspond to the classical bits 0 and 1. However, unlike classical bits, a qubit is a two-dimensional state vector that can be expressed as a linear combination of these orthonormal basis states. For example, if $|\mu_0\rangle = |0\rangle$ and $|\mu_1\rangle = |1\rangle$, the state of a qubit can be represented as a vector as follows

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}. \tag{2}$$

In general, a quantum state is described as a d-dimensional state vector, referred to as *a qudit*, and can be expressed as a linear combination of d-dimensional basis states [68], as shown below:

$$|\psi\rangle = \sum_{i=0}^{d-1} a_i|\mu_i\rangle \tag{3}$$

where $\sum_{i=0}^{d-1}|a_i|^2 = 1$, $\langle\mu_i|\mu_j\rangle = \delta_{ij}$, and δ_{ij} denotes the Kronecker delta function. A quantum system can exist as either a pure state or a mixed state. Equations (1) and (3) represent pure qubit and qudit states, respectively. Conversely, a mixed quantum state is an ensemble of pure states $\{p_j, |\psi_j\rangle\}$ and is described by a density matrix $\boldsymbol{\Xi}$ as follows:

$$\boldsymbol{\Xi} = \sum_j p_j|\psi_j\rangle\langle\psi_j| \tag{4}$$

where $\sum_j p_j = 1$, $|\psi_j\rangle = \sum_{i=0}^{d-1} a_{ij}|\mu_i\rangle$ and $\sum_{i=0}^{d-1}|a_{ij}|^2 = 1$ for all j. To visualize the quantum state, Fig. 2 shows the graphical representation of a qubit. The Bloch sphere with radius one denotes the state space of a single-qubit system where the computational basis vectors are at the north and south poles of the sphere. Specifically, the points on the surface of the sphere denote the pure qubit states, while the points inside the sphere correspond to the mixed qubit states.

B. Multiqubit States

A single bit can have two possible states, and the number of such states grows exponentially with the increasing number of bits. For instance, a 2-bit classical system can exist in one of the four possible states 00, 01, 10, and 11. Similarly, a two-qubit quantum system can exist in a superposition of four

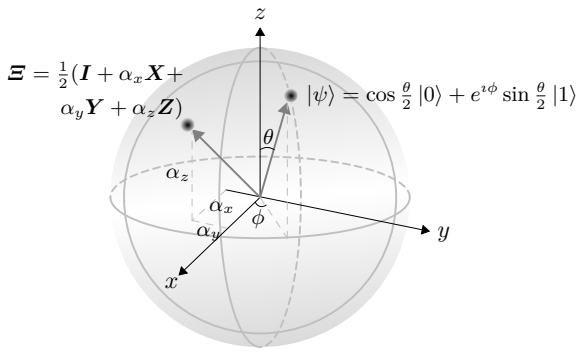


Fig. 2. Graphical representation of a single qubit system. Here, $0 \leq \theta \leq \pi$ and $0 \leq \varphi \leq 2\pi$ are the real numbers; and α_x, α_y, and α_z are the cartesian coordinates of a single-qubit mixed state, respectively (see Table II for operator definitions and their matrix representations [67]).

orthonormal basis states. Assuming that the first qubit is in the state $|\psi_0\rangle = a_{00}|0\rangle + a_{10}|1\rangle$ and the second qubit is in the state $|\psi_1\rangle = a_{01}|0\rangle + a_{11}|1\rangle$, the composite state of the system is given as

$$\begin{aligned} |\psi\rangle &= |\psi_0\rangle \otimes |\psi_1\rangle = |\psi_0\psi_1\rangle \\ &= \begin{bmatrix} a_{00} \\ a_{10} \end{bmatrix} \otimes \begin{bmatrix} a_{01} \\ a_{11} \end{bmatrix} = \begin{bmatrix} a_{00}a_{01} \\ a_{00}a_{11} \\ a_{10}a_{01} \\ a_{10}a_{11} \end{bmatrix} \\ &= a_{00}a_{01}|00\rangle + a_{00}a_{11}|01\rangle + a_{10}a_{01}|10\rangle \\ &\quad + a_{10}a_{11}|11\rangle. \end{aligned} \tag{5}$$

As the states of two qubits are independent of each other, called the separable states, the measurement on one qubit has no effect on the state of the other qubit. In quantum mechanics, it is not necessary that the state of a multiple-qubit system can be represented only as the tensor product of its components. For example, widely used Bell pairs are defined as follows:

$$|\psi_{xy}\rangle = \frac{1}{\sqrt{2}}\left(|0y\rangle + (-1)^x|1\bar{y}\rangle\right) \tag{6}$$

where $x, y \in \{0, 1\}$.[1] For the Bell states $|\psi_{xy}\rangle$, there exist no a_{00}, a_{10}, a_{01} and a_{11}, which satisfy

$$|\psi_{xy}\rangle = \left(a_{00}|0\rangle + a_{10}|1\rangle\right) \otimes \left(a_{01}|0\rangle + a_{11}|1\rangle\right). \tag{7}$$

Such states are called the entangled states—*quantum entanglement* [69]. In general, an n-qubit quantum state can be characterized as a linear combination of 2^n orthonormal basis states as follows [67], [70]:

$$|\psi\rangle = a_0|00\ldots0\rangle + a_1|00\ldots1\rangle + \cdots + a_{2^n-1}|11\ldots1\rangle \tag{8}$$

where each basis state is a 2^n-dimensional vector and $\sum_{i=0}^{2^n-1}|a_i|^2 = 1$. If $|\psi\rangle$ in (8) can be decomposed into the tensor product of n single-qubit states as follows

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle, \tag{9}$$

the state of each qubit can be represented separately from one another. In case the composite state $|\psi\rangle$ does not satisfy (9),

[1]For binary variables x and y, we denote the bitwise OR, AND, XOR, and NOT operations by $x + y$, $x \cdot y$, $x \oplus y$, and $\bar{x}$, respectively.

the quantum system is entangled. Commonly used entangled n-qubit states are W states [71], [72] and Greenberger–Horne–Zeilinger (GHZ) states [73]:

$$|\psi_{\mathrm{w}}^{n}\rangle = \frac{1}{\sqrt{n}}\left(|0\rangle^{\otimes(n-1)}|1\rangle + \sqrt{n-1}|\psi_{\mathrm{w}}^{n-1}\rangle|0\rangle\right) \tag{10}$$

$$|\psi_{\mathrm{g}}^{n}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right) \tag{11}$$

for $n > 2$. In quantum cryptography, these entangled states play an important role in detecting the presence of an eavesdropper in the quantum channel. For example, consider that a maximally entangled Bell pair is distributed between two legitimate parties. The remote parties quantify the amount of entanglement shared between them. If it is less than a threshold, the legitimate parties identify the eavesdropping activity in the channel and discard the protocol.

C. Quantum Measurements

Measurements are conducted to determine the properties of the system being observed [74]. In classical systems, performing measurements on a classical variable does not alter the state of the system. Contrastingly, in quantum systems, the state collapses to one of the post-measurement states upon measurement associated with its measurement operator [67]. Suppose that a single-qubit state $|\psi\rangle$ defined in (2) is measured in the computational basis. Then, the state of the system corresponding to the respective measurement outcome collapses as follows:

$$\begin{aligned} 0: &\quad |\psi\rangle \to |0\rangle \quad \text{with probability } |a_0|^2 \\ 1: &\quad |\psi\rangle \to |1\rangle \quad \text{with probability } |a_1|^2. \end{aligned} \tag{12}$$

Therefore, the quantum measurement irreversibly transforms the original state of the quantum system. If one performs repeated measurements of a quantum state in the computational basis, the measurement outcome does not change. In general, a qubit can be measured in a basis different from the basis used to prepare the qubit. For example, $|\psi\rangle$ defined in (2) can be measured in Hadamard basis $|\pm\rangle$ and the post-measurement states are $|\pm\rangle$ with probability $|a_0 \pm a_1|^2/2$ where

$$|\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right). \tag{13}$$

For an n-qubit system, quantum measurements can be performed either on a part of the system or on the complete system. For instance, the measurement on a 2-qubit state can be performed in the Bell basis $|\psi_{xy}\rangle$ or by measuring the first qubit only in the computational basis. For a separable state, measuring one qubit does not impact the state of the other qubit [75]. Conversely, in a maximally entangled system, measuring one qubit directly affects the state of the other qubit, rendering the state of the entire system immediately and certainly known. For example, assume that the initial composite state of a 2-qubit system is $|\psi_{00}\rangle$, if the post-measurement state of the first qubit is $|0\rangle$, then the state of the second qubit collapses to $|0\rangle$ with certainty and vice versa (see Fig. 3). This distinctive phenomenon of quantum mechanics is essential in detecting eavesdroppers in the quantum channel.

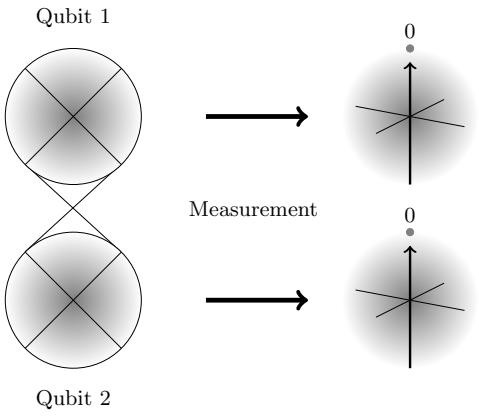


Fig. 3. Graphical representation of a quantum measurement on the two-qubit maximally entangled state $|\psi_{00}\rangle$. It illustrates that if two qubits are maximally entangled, the post-measurement states of these qubits are perfectly correlated [67].

D. Quantum Gates

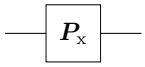
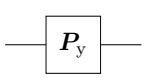
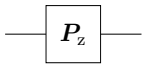
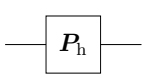
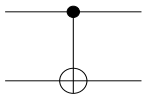
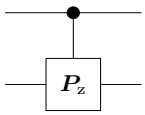
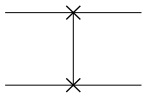
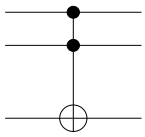
Logic gates serve as the building blocks of digital circuits in classical computing, and most of these logic gates are irreversible. Conversely, quantum gates are reversible and enable the execution of classical computing tasks using reversible quantum gates [67]. For example, the Pauli gates $\boldsymbol{P}_{\mathrm{x}}$, $\boldsymbol{P}_{\mathrm{y}}$, and $\boldsymbol{P}_{\mathrm{z}}$, along with the Hadamard gate $\boldsymbol{P}_{\mathrm{h}}$, are fundamental single-qubit gates. The Pauli-x gate $\boldsymbol{P}_{\mathrm{x}}$ performs a bit flip, mapping $|\psi\rangle$ defined in (2) to $a_1|0\rangle + a_0|1\rangle$. The Pauli-$z$ gate $\boldsymbol{P}_{\mathrm{z}}$ flips the phase of $|1\rangle$, yielding $a_0|0\rangle - a_1|1\rangle$, while the Pauli-$y$ gate $\boldsymbol{P}_{\mathrm{y}}$ applies both a bit and phase flip, resulting in $-\imath a_1|0\rangle + \imath a_0|1\rangle$. The Hadamard gate $\boldsymbol{P}_{\mathrm{h}}$ creates equal superpositions of basis states; e.g., $\boldsymbol{P}_{\mathrm{h}}$ maps $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ to $|0\rangle$. Alongside the single-qubit gates, multi-qubit gates extend operations across multiple qubits. For instance, the CNOT, Controlled-$\boldsymbol{P}_{\mathrm{z}}$, and SWAP gates are key two-qubit unitaries. The CNOT gate applies a $\boldsymbol{P}_{\mathrm{x}}$ operation to the target qubit conditioned on the control qubit being $|1\rangle$, implementing $|1a\rangle \to |1\bar{a}\rangle$ where $a \in \{0, 1\}$. The Controlled-$\boldsymbol{P}_{\mathrm{z}}$ gate applies a phase flip only to the $|11\rangle$ state, while the SWAP gate exchanges qubit states via $|a\rangle|b\rangle \to |b\rangle|a\rangle$. These gates are essential for entanglement, conditional operations, and qubit routing within quantum circuits. Extending this, the reversible Toffoli gate is a three-qubit gate that can be used to realize any Boolean function, but at the cost of requiring an extra ancilla qubit, mapping $|11a\rangle \to |11\bar{a}\rangle$. Table II presents the extensively employed quantum gates along with their notations, matrix forms (used for analytical computations) and equation forms (used for conceptual action of each gate on quantum states).

In general, a unitary operator $\boldsymbol{U} = \exp\{-\imath \boldsymbol{H} t/\hbar\}$ for a time-independent Hamiltonian is used to represent a quantum gate. This operator transforms a closed-quantum system as (governed by the Schrödinger equation) [76]

$$\imath\hbar \frac{\partial|\psi\rangle}{\partial t} = \boldsymbol{H}|\psi\rangle \tag{14}$$

where $\boldsymbol{H}$ denotes the Hamiltonian of the quantum system and $\hbar$ is the reduced Planck constant. In single-qubit systems,

TABLE II
ELEMENTARY QUANTUM GATES [67]

Operator	Gate	Matrix	Equation
Pauli-x $\boldsymbol{P}_{\mathrm{x}}$		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\|0\rangle\langle 1\| + \|1\rangle\langle 0\|$
Pauli-y $\boldsymbol{P}_{\mathrm{y}}$		$\begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}$	$-\imath\|0\rangle\langle 1\| + \imath\|1\rangle\langle 0\|$
Pauli-z $\boldsymbol{P}_{\mathrm{z}}$		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$
Hadamard $\boldsymbol{P}_{\mathrm{h}}$		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$\|+\rangle\langle -\| + \|-\rangle\langle +\|$
Contolled NOT (CNOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	$\|00\rangle\langle 00\| + \|01\rangle\langle 01\| + \|10\rangle\langle 11\| + \|11\rangle\langle 10\|$
Contolled-$\boldsymbol{P}_{\mathrm{z}}$		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	$\|00\rangle\langle 00\| + \|01\rangle\langle 01\| + \|10\rangle\langle 10\| - \|11\rangle\langle 11\|$
Swap		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	$\|00\rangle\langle 00\| + \|01\rangle\langle 10\| + \|10\rangle\langle 01\| + \|11\rangle\langle 11\|$
Toffoli		$\begin{bmatrix} \boldsymbol{I}_{6\times 6} & \boldsymbol{0}_{6\times 2} \\ \boldsymbol{0}_{2\times 6} & \boldsymbol{P}_{\mathrm{x}} \end{bmatrix}$	$\sum_{\substack{i,j,k \\ ijk\neq 110,111}} \|ijk\rangle\langle ijk\| + \|110\rangle\langle 111\| + \|111\rangle\langle 110\|$

unitary operators are represented by 2×2 matrices that can be factored into three rotation matrices as [77]

$$\boldsymbol{U} = \boldsymbol{R}_{\mathrm{z}}(\vartheta)\, \boldsymbol{R}_{\mathrm{y}}(\theta)\, \boldsymbol{R}_{\mathrm{z}}(\varphi) \tag{15}$$

where ϑ, θ, and φ are Euler angles and rotation matrices are given by

$$\boldsymbol{R}_{\mathrm{y}}(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \tag{16}$$

$$\boldsymbol{R}_{\mathrm{z}}(\varphi) = \begin{bmatrix} e^{-\imath\varphi/2} & 0 \\ 0 & e^{\imath\varphi/2} \end{bmatrix}. \tag{17}$$

In an n-qubit system, $\boldsymbol{U}$ is a $2^n \times 2^n$ matrix, which transforms the n-qubit input state $|\psi_{\text{in}}\rangle$ to the n-qubit output state $|\psi_{\text{out}}\rangle = \boldsymbol{U}|\psi_{\text{in}}\rangle$. Similar to quantum states, if $\boldsymbol{U}$ can be decomposed into

$$\boldsymbol{U} = \boldsymbol{U}_1 \otimes \boldsymbol{U}_2 \otimes \cdots \otimes \boldsymbol{U}_n, \tag{18}$$

the quantum operations on each qubit are independent of each other. Here, $\boldsymbol{U}_i$ is an arbitrary single-qubit unitary operation performed on the ith qubit. For instance, the Hadamard gate can be performed on each qubit of a 2-qubit system as $(\boldsymbol{P}_{\mathrm{h}} \otimes \boldsymbol{I})\,(\boldsymbol{I} \otimes \boldsymbol{P}_{\mathrm{h}}) = (\boldsymbol{I} \otimes \boldsymbol{P}_{\mathrm{h}})\,(\boldsymbol{P}_{\mathrm{h}} \otimes \boldsymbol{I}) = \boldsymbol{P}_{\mathrm{h}} \otimes \boldsymbol{P}_{\mathrm{h}}$. In contrast if a controlled-NOT (CNOT) gate is applied on a 2-qubit system, it cannot be decomposed into a tensor product as in (18). The CNOT gate is a special case of the 2-qubit controlled-unitary operator $\boldsymbol{U}_{\mathrm{c}}$ where

$$\boldsymbol{U}_{\mathrm{c}} = |0\rangle\langle 0| \otimes \boldsymbol{I} + |1\rangle\langle 1| \otimes \boldsymbol{U} \tag{19}$$

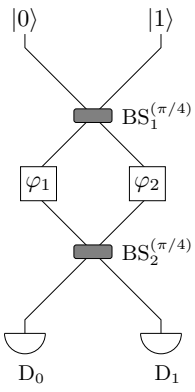
and $\boldsymbol{U}$ is an arbitrary single-qubit unitary operation. Here, it is important to note that the first qubit acts as a control qubit and the second qubit acts as a target qubit. If $\boldsymbol{U} = \boldsymbol{P}_{\mathrm{x}}$, $\boldsymbol{U}_{\mathrm{c}}$ is the unitary operator of the CNOT gate.

III. FUNDAMENTALS OF COUNTERFACTUALITY

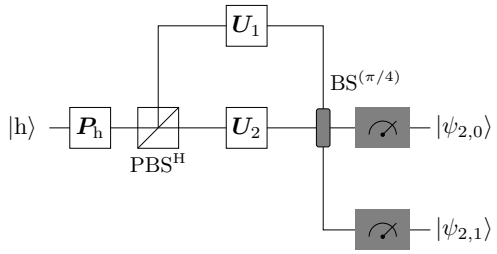
This section presents the fundamental concepts of counterfactual quantum communication, encompassing interferometers, QZ effect, and IFM.

A. Interferometers

Interferometry, a phenomenon based on the interference of waves, plays an important role in a wide range of fundamental laws of physics such as gravitational waves detection [78]–[80], fiber optics, metrology [81], [82], and sensing [83]–[85].



(a) MZI with BSs



(b) MZI with a PBS and a BS

Fig. 4. Mach-Zenhander interferometer. (a) Standard MZI with balanced BSs using a single degree of freedom of the photon. (b) Standard MZI with a PBS and a balanced BS using multiple degrees of freedom of the photon. Here, PBS stands for a polarizing beam splitter, $0 \leq \varphi_1 \leq 2\pi$ and $0 \leq \varphi_2 \leq 2\pi$ are Euler angles, $\boldsymbol{U}_1 = \boldsymbol{P}(\varphi_1, 0)$, and $\boldsymbol{U}_2 = \boldsymbol{P}(0, \varphi_2)$ [60], [86].

In general, interferometers consist of two types of components: i) passive components that split or recombine the light and ii) active components that manipulate the phase of light. This section briefly overviews two widely used interferometers in quantum mechanics, namely MZIs [60], [61], [86], [87] and Michelson interferometers (MIs) [88]–[91]. Table III compares their basic structures, interference mechanisms, and light path behaviors, providing a clear explanation of their operational distinctions.

1) Mach-Zehnder Interferometer: The MZI is a two-path interferometer that consists of one phase-changing unitary operation in each path and two BSs as illustrated in Fig. 4 [87]. It was first introduced by Mach and Zehnder in 1890 and the first quantum description was demonstrated in 1986 [86]. The aim of MZI is to measure the relative phase shift between the two paths by observing the interference pattern obtained after the second BS. The unitary operation of a BS is commonly represented by the matrix

$$\boldsymbol{U}_\mathrm{bs} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \tag{20}$$

which resembles a rotation around the y-axis in a two-dimensional Hilbert space, denoted by $\boldsymbol{R}_\mathrm{y}(\phi)$. By setting $\phi = 2\theta$, the BS transformation is mathematically equivalent to a qubit rotation, i.e., $\boldsymbol{U}_\mathrm{bs} = \boldsymbol{R}_\mathrm{y}(2\theta)$ [92]. When light passes through the first BS, it is split into two paths, each of which undergoes a phase shift. These phase shifts are modeled by a diagonal unitary matrix

$$\boldsymbol{P}(\varphi_1, \varphi_2) = \begin{bmatrix} e^{-\imath\varphi_1} & 0 \\ 0 & e^{-\imath\varphi_2} \end{bmatrix} \tag{21}$$

where $\varphi_1, \varphi_2 \in [0, 2\pi]$ are Euler angles. The relative phase shift $\varphi_1 - \varphi_2$ determines the interference outcome at the second BS. Hence, variations in these parameters directly control the constructive or destructive interference at the MZI output, allowing dynamic tuning of the output state [93]. The overall action of the MZI can be represented as a single-qubit unitary operation $\boldsymbol{U}(\theta_2, \varphi_2, \varphi_1, \theta_1)$ where

$$\boldsymbol{U}(\theta_2, \varphi_2, \varphi_1, \theta_1) = \boldsymbol{R}_\mathrm{y}(2\theta_2)\, \boldsymbol{P}(\varphi_1, \varphi_2)\, \boldsymbol{R}_\mathrm{y}(2\theta_1)\,. \tag{22}$$

A standard MZI uses balanced BSs with $\theta_1 = \theta_2 = \pi/4$ and the spatial degree of freedom of the photon (see Fig. 4(a)). In later years, the MZI has been demonstrated by using the multiple degrees of freedom of the photon, such as the polarization degree and spatial mode. In this MZI, the first $\mathrm{BS}^{(\pi/4)}$ is replaced by a combination of Hadamard $\boldsymbol{P}_\mathrm{h}$ gate followed by a polarizing beam splitter $\mathrm{PBS}_1^\mathrm{H}$ as they functionally mimic each other. Assume a single photon source produces a horizontally (H) polarized photon in a specific spatial mode, and a qubit is encoded in its polarization. The $\boldsymbol{P}_\mathrm{h}$ gate transforms this polarization into a superposition, and then the $\mathrm{PBS}_1^\mathrm{H}$ gate separates the $|\mathrm{h}\rangle$ and $|\mathrm{v}\rangle$ components into different paths. The state of the photon after PBS is given as

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|\mathrm{h}\rangle|0\rangle + |\mathrm{v}\rangle|1\rangle\right) \tag{23}$$

where $|0\rangle$ and $|1\rangle$ denote the spatial degree of freedom of the photon. Note that polarization and spatial degrees of freedom of the photon are entangled. The photon components in each path undergo phase changing unitary operations—$\boldsymbol{U}_2 = \boldsymbol{P}(\varphi_1, 0)$ in path $|0\rangle$ and $\boldsymbol{U}_1 = \boldsymbol{P}(0, \varphi_2)$ in path $|1\rangle$—before recombined at the $\mathrm{BS}^{(\pi/4)}$ (as illustrated in Fig. 4(b)). The state of the photon then transforms as

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\big[\big(\boldsymbol{P}(\varphi_1, 0) \otimes \boldsymbol{I}\big)|\mathrm{h}\rangle|0\rangle + \big(\boldsymbol{P}(0, \varphi_2) \otimes \boldsymbol{I}\big)|\mathrm{v}\rangle|1\rangle\big]. \tag{24}$$

After $\mathrm{BS}^{(\pi/4)}$, $|\psi_1\rangle$ transforms to

$$\begin{aligned} |\psi_1\rangle = \frac{1}{2}\big[&\big(e^{-\imath\varphi_1}|\mathrm{h}\rangle + e^{-\imath\varphi_2}|\mathrm{v}\rangle\big)|0\rangle \\ &+ \big(e^{-\imath\varphi_1}|\mathrm{h}\rangle - e^{-\imath\varphi_2}|\mathrm{v}\rangle\big)|1\rangle\big] \end{aligned} \tag{25}$$

leading to destructive or constructive interference at the output detectors, D_0 and D_1, upon measurement, depending on the relative phase $\varphi_1 - \varphi_2$.

2) Michelson Interferometer: The MI is another two-path interferometer that consists of one phase-changing unitary operation in each path and one BS, as illustrated in Fig. 5. It was first devised by Albert Michelson in 1881 and was used to detect the motion of the Earth through a hypothetical medium known as the ether [94]. This MI produces interference fringes by splitting the incoming light source into two paths and recombines them after performing phase shift unitary operations in each path. Similar to the MZI, a standard MI also uses the balanced beam splitter $\mathrm{BS}^{(\pi/4)}$ and the spatial

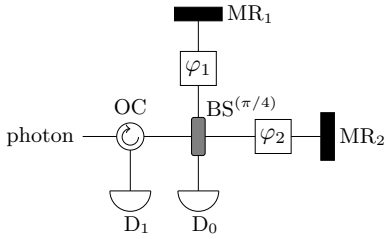


Fig. 5. Michelson interferometer. Standard MI with a balanced BS using a single degree of freedom of the photon [88].

TABLE III
DIFFERENCE BETWEEN MZI AND MI

Feature	MZI	MI
Basic Structure	Two phase-changing unitary operators and two BSs in linear configuration.	Two phase-changing unitary operators, two mirrors (MRs), and one BS in perpendicular configuration.
Interference Mechanism	Light is split at first BS and recombined at another BS.	Light is split, reflected by MRs, and recombined at BS.
Light Path Behavior	Two distinct, well-separated paths, each traversed only once.	Same path traversed twice (forward and backward), then recombined.

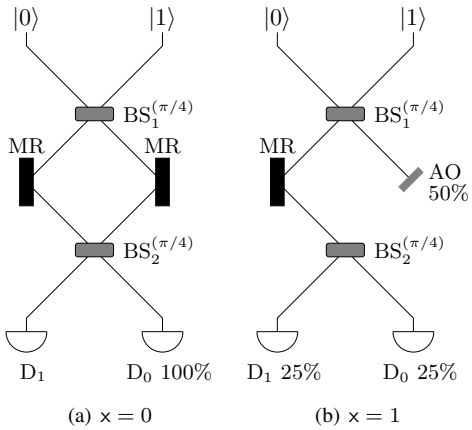
degree of freedom of the photon. The MI works similarly to the MZI for multiple degrees of freedom of the photon and undergoes a similar state transformation as in (23)–(25) [95]. The only difference is that it uses only one $\mathrm{BS}^{(\pi/4)}$ as shown in Fig. 5 and thus the light that propagates into two paths is reflected back by the mirrors (MRs) to recombine. Based on the interference pattern determined by the relative phase $\varphi_1 - \varphi_2$, the photon is detected at one of the detectors, where the path to detector D_1 is directed by the optical circulator (OC). Note that the two path lengths should be identical in both the MZI and MI.

B. QZ Effect

The QZ effect is a phenomenon that arises in the realm of quantum mechanics and is named after the ancient Greek philosopher Zeno of Elea [96]. It seemingly defies our intuition about the nature of the time evolution of a quantum system and how the measurements can affect this evolution. For instance, in a closed quantum system, the pure state $|\psi(t)\rangle$ of the given system evolves under the unitary evolution, which is governed by the Schrödinger equation in (14), where the Hamiltonian $\boldsymbol{H}$ can be decomposed as

$$\boldsymbol{H} = \boldsymbol{H}_0 + \sum_{k=1}^{K} u_k(t)\boldsymbol{H}_k. \tag{26}$$

Here, $\boldsymbol{H}_0$ denotes the internal Hamiltonian, $u_k(t)$ symbolizes the kth control parameter, and $\boldsymbol{H}_k$ are control Hamiltonians [97], [98]. It is already well known that the Schrödinger equation is linear, and its solution is given by the unitary operator $\boldsymbol{U}(t, t_0)$ and the state of the system is given as $|\psi(t)\rangle = \boldsymbol{U}(t, t_0)\,|\psi(t_0)\rangle$, where $\boldsymbol{U}(t, t) = \boldsymbol{I}$.



(a) $\mathsf{x} = 0$ (b) $\mathsf{x} = 1$

Fig. 6. EV-IFM. (a) For $\mathsf{x} = 0$, it causes destructive interference and detector D_0 clicks with probability one. (b) For $\mathsf{x} = 1$, the photon interacts with AO with probability $1/2$ and the photon is absorbed by AO. If the photon is not absorbed by AO, detectors D_0 and D_1 click with equal probability. Here, MR stands for a mirror [99].

In the conventional picture of quantum dynamics, the evolution of the quantum systems governed by the Schrödinger equation can be breakdown into a sequence of states by assuming that the control parameters remain constant for time duration $\Delta t = t_i - t_{i-1}$ where t_i denotes the ith time instant and $t_i > t_{i-1} > t_0$ for all i [100]. The Hamiltonian $\boldsymbol{H}^{(i)}$ and the state $|\psi(t_i)\rangle$ of the system at the ith time instant are given as

$$\boldsymbol{H}^{(i)} = \boldsymbol{H}_0 + \sum_{k=1}^{K} u_k^{(i)}\boldsymbol{H}_k \tag{27}$$

$$|\psi(t_i)\rangle = \prod_{m=1}^{i} \boldsymbol{U}(t_m, t_{m-1})\,|\psi(t_0)\rangle \tag{28}$$

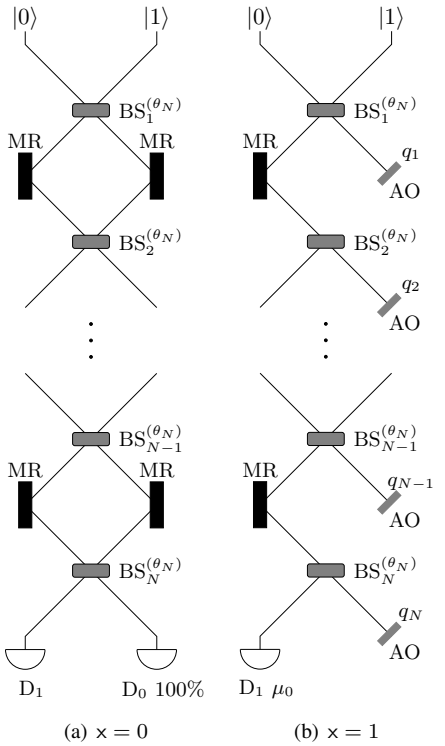
where $|\psi(t_0)\rangle$ denotes the initial state and

$$\boldsymbol{U}(t_m, t_{m-1}) = \exp\{-\imath\Delta t\boldsymbol{H}^{(m)}\} \tag{29}$$

is the mth unitary propagator for $m = 1, 2, \ldots, i$. However, the QZ effect introduces an intriguing phenomenon that the frequent measurements can "freeze" the Hamiltonian evolution of a quantum system in its initial state [101]. Assume that the given quantum system is initialized in the eigenstate of an observable, and the system is measured at each time instant. Then, the probability that the system retains its initial state approaches one as Δt goes to zero.

C. IFM

IFM demonstrates non-locality by allowing the detection of an object's presence in a region without direct interaction. This concept was first proposed by Dicke in 1981 [103] and further developed by the EV-IFM method in 1993 [99], though its efficiency was limited to 0.5. In 1995, KW-IFM combined IFM with the QZ effect, significantly increasing IFM efficiency to nearly 1 [102].



(a) $\mathsf{x} = 0$ (b) $\mathsf{x} = 1$

Fig. 7. KW-IFM. (a) For $\mathsf{x} = 0$, N unbalanced BSs transform the state of the photon under unitary operation $\boldsymbol{U}_N^N$ and detector D_0 clicks with certainty. (b) For $\mathsf{x} = 1$, the photon interacts with AO with probability ϵ_N in each cycle. If the photon is not absorbed by AO, detectors D_1 click with certainty. Here, $\boldsymbol{U}_N = \boldsymbol{R}_{\mathrm{y}}(2\theta_N)$, $\epsilon_N = \sin^2\theta_N$, $q_i = \epsilon_N \cos^{2(i-1)}\theta_N$, $\mu_0 = \cos^{2N}\theta_N$, and $\theta_N = \pi/(2N)$ [102].

1) EV-IFM: This IFM utilizes the MZI with a balanced beam splitter $\mathrm{BS}^{(\pi/4)}$ and two detectors, D_0 and D_1, as shown in Fig. 6 [99], [104]. Consider that $|0\rangle$ and $|1\rangle$ indicate the presence of a photon in path a and path b, respectively. The EV-IFM protocol begins with the photon initialized in the state $|\psi_0\rangle = |0\rangle$. Then, $\mathrm{BS}_1^{(\pi/4)}$ produces an equal superposition of the photon:

$$|\psi_0\rangle \to |\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \tag{30}$$

To certify the presence of an AO in the interferometer, it is assumed that a photon would be lost to AO upon interaction. Consider that a random variable $\mathsf{x} \in \{0, 1\}$ denotes the state of AO in path b, where $\mathsf{x} = 0$ and $\mathsf{x} = 1$ denote the absence and presence of AO, respectively. The possible transformations of the photon's state are given as follows.

- $\mathsf{x} = 0$: When the AO is absent, the split photon components in path state $|0\rangle$ and $|1\rangle$ recombine at $\mathrm{BS}_2^{(\pi/4)}$ and transforms $|\psi_1\rangle$ to $|\psi_2\rangle$ where

$$|\psi_2\rangle = \frac{1}{2}\big(|0\rangle + |1\rangle - |0\rangle + |1\rangle\big) = |1\rangle. \tag{31}$$

  This leads to destructive interference and D_0 clicks with certainty (see Fig. 6(a)).
- $\mathsf{x} = 1$: When the AO is present, there are two possible scenarios. (i) The photon interacts with the AO and no detector clicks. As $\mathrm{BS}_2^{(\pi/4)}$ creates a balanced superposition of the photon in paths a and b, the probability that the photon is absorbed by the AO is $1/2$. (ii) Unless the photon is absorbed by AO, constructive interference is formed after $\mathrm{BS}_2^{(\pi/4)}$, and D_0 and D_1 have an equal probability of clicking. Since D_0 can register a click in both scenarios ($\mathsf{x} = 0$ and $\mathsf{x} = 1$), it does not provide definitive information about the presence of the AO. However, if D_1 clicks, it indicates that the AO exists in the interferometer, despite the photon not interacting with the AO (see Fig. 6(b)). It is important to note that the photon was never in the path state $|1\rangle$ during any stage of the protocol if it is not absorbed by the AO, which is fundamental to CQC.

Note that, in the presence of the AO, i) the system behaves similarly to a measurement in the computational basis, and ii) the photon exists in an unstable quantum state, meaning it either arrives at $\mathrm{BS}_2^{(\pi/4)}$ or is absorbed by the AO. EV-IFM efficiency is limited to a maximum of 50% due to the strong interaction between the AO and the unstable quantum state of the photon, and the low frequency of the measurement [99].

2) KW-IFM: In Section III-C1, it has been shown that the non-locality of quantum mechanics enables one to estimate the existence of an object, more specifically an AO, without interacting with it. However, as the measurement is conducted only a single time in EV-IFM, the photon decays at a rate of $1/2$ [99]. To minimize this decay rate close to 0, the QZ-assisted IFM is employed to repeatedly measure the state of the photon [102]. Fig. 7 depicts this KW-IFM with the decay rate approaching to zero under the asymptotic limits where $\mathrm{BS}^{(\theta_N)}$ denotes an unbalanced BS with transmission $\sin^2\theta_N$ and reflection $\cos^2\theta_N$, N denotes the number of BSs, and $\theta_N = \pi/(2N)$. The $\mathrm{BS}_i^{(\theta_N)}$ transforms the state of the photon under the unitary operation $\boldsymbol{U}_N = \boldsymbol{R}_{\mathrm{y}}(2\theta_N)$ for all $i = 1, 2, \ldots, N$. The protocol begins with the photon initialized in the state $|\psi_0\rangle = |0\rangle$. Then, according to the unitary operation $\boldsymbol{U}_N$, $\mathrm{BS}_1^{(\theta_N)}$ creates an unbalanced spatial superposition as outlined below:

$$\begin{aligned}|\psi_1\rangle &= \boldsymbol{U}_N|\psi_0\rangle \\ &= \cos(\theta_N)|0\rangle + \sin(\theta_N)|1\rangle.\end{aligned} \tag{32}$$

- $\mathsf{x} = 0$: When the AO is absent, $\mathrm{BS}_i^{(\theta_N)}$ rotates the photon component by an angle θ_N for each i. After passing through the nth ($\leq N$) beam splitter $\mathrm{BS}_n^{(\theta_N)}$, the photon state becomes:

$$|\psi_n\rangle = \cos(n\theta_N)|0\rangle + \sin(n\theta_N)|1\rangle. \tag{33}$$

  Upon completion of the protocol, the photon state evolves to $|\psi_N\rangle = \boldsymbol{U}_N^N|\psi_0\rangle = |1\rangle$, ensuring that detector D_0 definitely registers a click (see Fig. 7(a)).
- $\mathsf{x} = 1$: When the AO is present, the probability of the photon being absorbed by AO in the first cycle is nonzero, which is ϵ_N. Consequently, the photon state decoheres to the mixed state

$$\boldsymbol{\Upsilon}_1 = (1 - \epsilon_N)|\psi_0\rangle\langle\psi_0| + \epsilon_N|\epsilon\rangle\langle\epsilon| \tag{34}$$

  where $|\epsilon\rangle$ denotes the erasure state of the photon and $\boldsymbol{U}_N|\epsilon\rangle = |\epsilon\rangle$. As only the photon component in path $|1\rangle$ interacts with the AO, we have $\epsilon_N = \sin^2\theta_N$. In general,

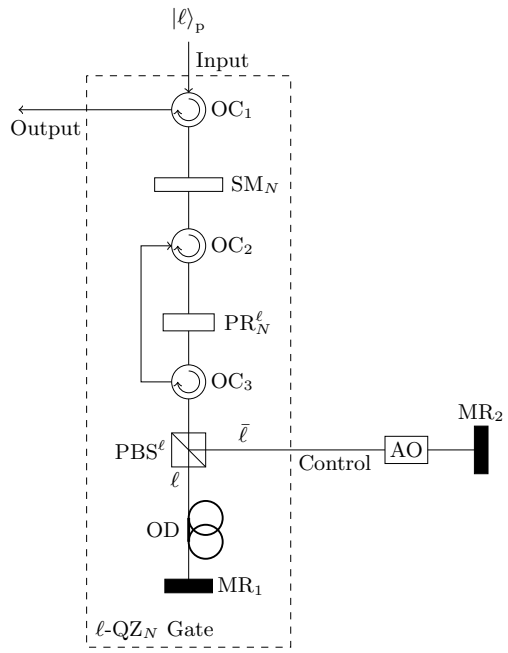


Fig. 8. ℓ-$\rm QZ_N$ gate where $\ell = 0$ denotes H and $\ell = 1$ denotes a V polarized photon. Here, PR stands for a polarization rotator and OD denotes an optical delay to match the path length of two optical paths $\rm SM_N$ to $\rm MR_1$ and $\rm SM_N$ to $\rm MR_2$ [12], [65].

the photon state after $\rm BS_n^{(\theta_N)}$ and AO in the nth cycle are given as $\boldsymbol{\Xi}_n$ and $\boldsymbol{\Upsilon}_n$, respectively:

$$\boldsymbol{\Xi}_n = \boldsymbol{V}\boldsymbol{\Upsilon}_{n-1}\boldsymbol{V}^{\dagger} \tag{35}$$

$$\boldsymbol{\Upsilon}_n = (1-\varepsilon)^n |\psi_0\rangle\langle\psi_0| + \sum_{i=1}^{n} \varepsilon\,(1-\varepsilon)^{i-1} |\epsilon\rangle\langle\epsilon| \tag{36}$$

where $\boldsymbol{V} = \boldsymbol{U}_N$, $\varepsilon = \epsilon_N$, and the superscript $\dagger$ denotes the conjugate transpose. Upon completion of the protocol, the photon state transforms to its initial state with probability $\mu_0 = (1-\epsilon_N)^N = \cos^{2N}\theta_N$. If the photon is not lost to the AO, detector $\rm D_1$ registers a click with certainty (see Fig. 7(b)).

From the above discussion, it can be concluded that unless the photon is discarded in frequent measurements, the presence of AO in the interferometer can be determined with certainty (only $\rm D_x$ clicks for each value of x). As $N \to \infty$, the trace distance between the initial state $|\psi_0\rangle$ and $\boldsymbol{\Xi}_n$ approaches zero, which indicates that the decay rate $\epsilon_N \to 0$. In later years, the idea of IFM has been demonstrated experimentally [105], [106] and extended to many applications such as interaction-free quantum gates [107], interaction-free computing [108], and interaction-free imaging [109].

IV. Counterfactual Quantum Gates

This section overviews the fundamental gates, such as the QZ and CQZ gates, followed by the modified QZ (MQZ) and distributed controlled flipping (DCF) gates, which form the basis of CQC and cryptography, where each gate has three terminals (input, output, and control). In order to perform communication and cryptography tasks in counterfactual manners, only the control terminal of the counterfactual quantum gates interacts with AO.

A. QZ Gates

The QZ gates signify the Michelson equivalent of the KW-IFM that utilizes the polarization and spatial properties of photons to detect the presence of an AO in the interferometer. Fig. 8 shows the schematic of QZ gates where $\ell = 0$ denotes H and $\ell = 1$ denotes V; and H-$\rm QZ_N$ and V-$\rm QZ_N$ are two types of QZ gates. Note that the H-$\rm QZ_N$ gate uses the combination of $\rm PR_N^H$ and $\rm PBS^H$ whereas the V-$\rm QZ_N$ gate uses the combination of $\rm PR_N^V$ and $\rm PBS^V$, where PR stands for a polarization rotator and PBS denotes a polarizing beam splitter.

To demonstrate the operating principle of QZ gates, assume that the ℓ-$\rm QZ_N$ gate takes an $|\ell\rangle_{\rm p}$ polarized photon as an input, where the subscript p denotes the polarization degree of freedom. The protocol starts by directing the photon towards a switchable mirror (SM), which is initially turned off to allow the photon to pass and is turned on for N cycles. In each cycle, the $\rm PR_N^{\ell}$ gives the rotation of an angle θ_N in the polarization degree of freedom of the photon under the unitary operation $\boldsymbol{U}_{N,\ell}$ where

$$\boldsymbol{U}_{N,\ell} = \boldsymbol{R}_{\rm y}\big((-1)^{\ell}\, 2\theta_N\big), \tag{37}$$

and PBS separates or reunites the H and V components of the photon in two or one optical path(s). For instance, the state of the photon after $\rm PBS^{\ell}$ in the first cycle of the ℓ-$\rm QZ_N$ gate is

$$\begin{aligned} |\psi_1\rangle &= \big(|\ell\rangle_{\rm p}\langle\ell| \otimes \boldsymbol{I} + |\bar{\ell}\rangle_{\rm p}\langle\bar{\ell}| \otimes \boldsymbol{P}_{\rm x}\big)\big(\boldsymbol{U}_{N,\ell} \otimes \boldsymbol{I}\big)|\psi_0\rangle \\ &= \cos(\theta_N)\,|\ell\rangle_{\rm p}|0\rangle_{\rm s} + \sin(\theta_N)\,|\bar{\ell}\rangle_{\rm p}|1\rangle_{\rm s} \end{aligned} \tag{38}$$

where $|\psi_0\rangle = |\ell\rangle_{\rm p}|0\rangle_{\rm s}$. Here, $|0\rangle_{\rm s}$ and $|1\rangle_{\rm s}$ denote the presence of photon in optical paths from $\rm SM_N$ to $\rm MR_1$ and $\rm SM_N$ to $\rm MR_2$, respectively, and the subscript s denotes the spatial degree of freedom of the photon. Note that the combined action of $\rm PR_N^{\ell}$ and $\rm PBS^{\ell}$ acts as an unbalanced beam splitter $\rm BS^{(\theta_N)}$.

- $\mathsf{x} = 0$: In the absence of an AO, the component of the photon in path state $|1\rangle_{\rm s}$ reflected back to the $\rm PBS^{\ell}$ by $\rm MR_2$ and reunites with the component of the photon in path state $|0\rangle_{\rm s}$. As $\rm SM_N$ is turned on for N cycles, it reflects the photon to $\rm PR_N^{\ell}$ and the same process repeats for the remaining $N-1$ cycles. The state of the photon after $\rm PBS^{\ell}$ in the nth cycle is

$$\begin{aligned} |\psi_n\rangle &= \big(|\ell\rangle_{\rm p}\langle\ell| \otimes \boldsymbol{I} + |\bar{\ell}\rangle_{\rm p}\langle\bar{\ell}| \otimes \boldsymbol{P}_{\rm x}\big)\big(\boldsymbol{U}_{N,\ell} \otimes \boldsymbol{I}\big)^n|\psi_0\rangle \\ &= \cos(n\theta_N)\,|\ell\rangle_{\rm p}|0\rangle_{\rm s} + \sin(n\theta_N)\,|\bar{\ell}\rangle_{\rm p}|1\rangle_{\rm s}. \end{aligned} \tag{39}$$

  After N cycles, the photon state transforms to $|\bar{\ell}\rangle_{\rm p}$ with certainty.[2]
- $\mathsf{x} = 1$: In the presence of an AO, only the component of the photon in path state $|1\rangle_{\rm s}$ interacts with AO and the photon undergoes the same state transformation as in (35) and (36) where $\boldsymbol{V} = \boldsymbol{U}_{N,\ell} \otimes \boldsymbol{I}$ and $\varepsilon = \epsilon_N$ for the ℓ-$\rm QZ_N$ gate. After N cycles, the photon state collapses back to

[2]Note that since there is only one optical path at the output of the ℓ-$\rm QZ_N$, the path information of the photon at the output is ignored.

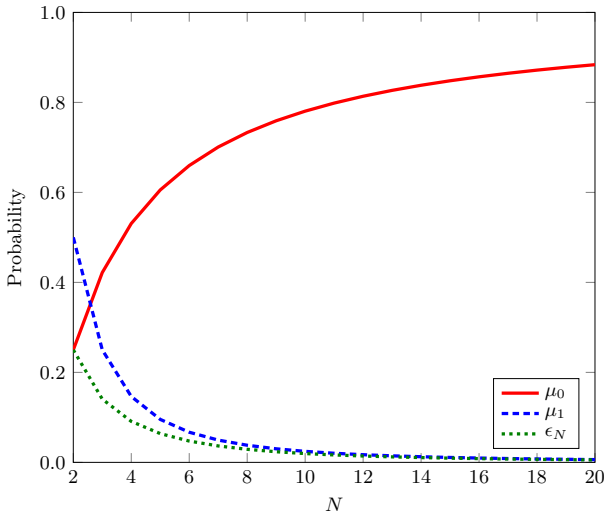
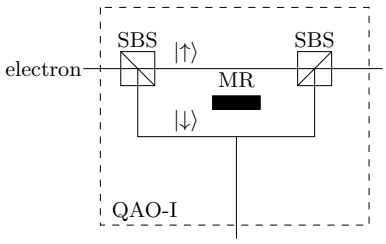
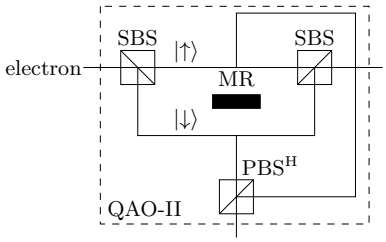


Fig. 9. Probabilities μ_0 and μ_1, and ϵ_N as a function of N. As $N \to \infty$, μ_0 approaches one, whereas μ_1 and ϵ_N go to zero.



(a) Type-I



(b) Type-II

Fig. 10. Types of QAO. (a) In type I, the electron component in state $|\downarrow\rangle$ acts as blocking the photon's path. (b) In type II, the electron component in state $|\downarrow\rangle$ acts as $\mathsf{x} = \ell$ for the ℓ-QZ$_N$ gate and vice versa. Here, SBS stands for a spin beam splitter [65].

the initial state $|\ell\rangle_{\mathrm{p}}$ with probability μ_0. As $N \to \infty$, this probability approaches one (see Fig. 9).

Following the same procedure, the ℓ-QZ$_N$ gate transforms the input state $|\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}$ as follows:

$$\ell\text{-QZ}_N : \begin{cases} |\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}} \to (-1)^{\mathsf{b}\oplus\ell}\,|\mathsf{a}\rangle_{\mathrm{o}}|\big(\bar{\mathsf{a}}\cdot\bar{\mathsf{b}} + \mathsf{a}\cdot\ell\big)\rangle_{\mathrm{p}} \\ \text{with the probability } \mu^{\mathsf{a}}_{\mathsf{b}\oplus\ell} \end{cases} \tag{40}$$

where $|\mathsf{a}\rangle_{\mathrm{o}}$ denotes the state of an AO, $\mathsf{a}, \mathsf{b} \in \{0, 1\}$, and

$$\mu_1 = \sin^2\theta_N \left(1 - \sin^2\theta_N\right)^{N-1}. \tag{41}$$

Henceforth, only the classical behavior of the AO and the photon are considered for ℓ-QZ$_N$ gates. In general, the QAO

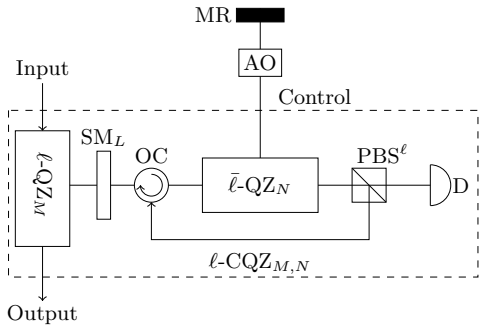


Fig. 11. ℓ-CQZ$_{M,N}$ gate with M outer and N inner cycles [65]. Here, the ℓ-CQZ$_{M,N}$ gate uses the combination of ℓ-QZ$_M$ and ℓ-QZ$_N$ gates [12], [65].

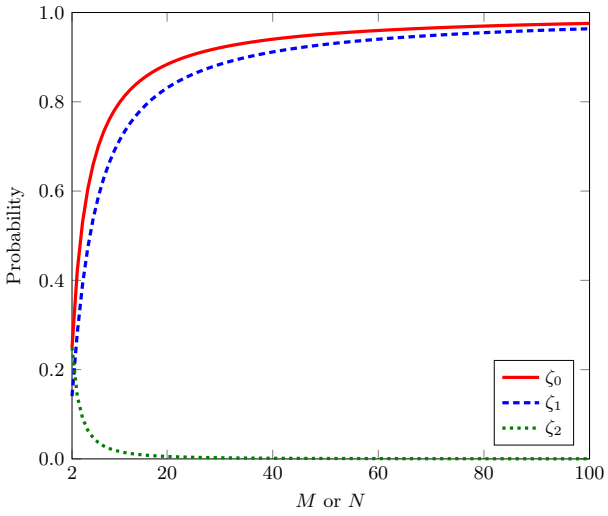


Fig. 12. Probabilities ζ_0 and ζ_2 as a function of M, whereas ζ_1 as a function of N when $L = 1$ and $M^\star = \arg\max_M \zeta_1 = 2$. Note that ζ_0 and ζ_2 go to respectively one and zero as $M \to \infty$, while ζ_1 approaches one as $N \to \infty$.

can exist in the superposition of absence and presence of AO, as illustrated in Fig. 10, where the spin beam splitter (SBS) separates or reunites the up spin $|\uparrow\rangle = |0\rangle_{\mathrm{o}}$ and down spin $|\downarrow\rangle = |1\rangle_{\mathrm{o}}$ of the electron. Since μ_1 approaches to zero as $N \to \infty$, a general composite state of QAO-I and photon for the ℓ-QZ$_N$ gate is approximated as:

$$|\mathrm{qz}_\ell\rangle_{\mathrm{op}} = \alpha_0|00\rangle_{\mathrm{op}} + \alpha_1|01\rangle_{\mathrm{op}} + \alpha_2|1\ell\rangle_{\mathrm{op}} \tag{42}$$

where $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 = 1$. Here, $|0\rangle_{\mathrm{o}}$ and $|1\rangle_{\mathrm{o}}$ denote the presence and absence of an AO for QAO-I, respectively. From (40), the input state $|\mathrm{qz}_\ell\rangle_{\mathrm{op}}$ is transformed by the ℓ-QZ$_N$ gate to:

$$\begin{aligned}\ell\text{-QZ}_N\big(|\mathrm{qz}_\ell\rangle_{\mathrm{op}}\big) = (-1)^{\ell}\,\alpha_0|01\rangle_{\mathrm{op}} + (-1)^{\bar{\ell}}\,\alpha_1|00\rangle_{\mathrm{op}} \\ + \alpha_2|1\ell\rangle_{\mathrm{op}}\end{aligned} \tag{43}$$

with the probability

$$\lambda_1 = \left(1 - |\alpha_2|^2\epsilon_N\right)^N \tag{44}$$

tending to one as $N \to \infty$.

B. CQZ Gates

CQZ gates are the chained version of the QZ gates to counterfactually determine the presence of an AO in the interferometer for all x. Fig. 11 shows the schematic of CQZ gates where H-CQZ$_{M,N}$ and V-CQZ$_{M,N}$ are two types of CQZ gates [12], [110]. Note that the ℓ-CQZ$_{M,N}$ gate uses the combination of ℓ-QZ$_M$ and $\bar{\ell}$-QZ$_N$ gates, where QZ$_M$ denotes the outer gate with M cycles and QZ$_N$ denotes the inner gate with N cycles [12], [110].

To demonstrate the operating principle of CQZ gates, assume that the ℓ-CQZ$_{M,N}$ gate takes an $|\ell\rangle_{\rm p}$ polarized photon. The protocol starts by directing the photon towards the ℓ-QZ$_M$ gate. In each outer cycle, PR$_M^{\ell}$ in the ℓ-QZ$_M$ gate gives the rotation of an angle $\theta_M = \pi/(2M)$ in the polarization degree of freedom under the unitary operation $\boldsymbol{U}_{M,\ell}$. Similarly, in each inner cycle, PR$_N^{\bar{\ell}}$ in the $\bar{\ell}$-QZ$_N$ gate gives the rotation of an angle θ_N in the polarization degree of freedom of the photon under the unitary operation $\boldsymbol{U}_{N,\bar{\ell}}$. The SM$_L$ is initially switched off during each outer cycle to enable the transmission of the $\bar{\ell}$ component of the photon towards the $\bar{\ell}$-QZ$_N$ gate. Once the photon has successfully passed through, the SM$_L$ is switched on for L rounds of the inner QZ gate. After completing L rounds, SM$_L$ is switched on again, enabling the photon to proceed towards the ℓ-QZ$_M$ gate.

- $\mathsf{x} = 0$: In the absence of an AO, the $\bar{\ell}$-QZ$_N$ gate transforms the $|\bar{\ell}\rangle_{\rm p}$ photon component to $|\ell\rangle_{\rm p}$. Unless the photon is discarded at the detector D, the photon state transitions back to the initial state. The switchable mirror SM$_L$ gives L repeated actions of the $\bar{\ell}$-QZ$_N$ gate to remove the weak trace of the photon in the control terminal. In M outer cycles, the photon undergoes the same state transformation as in (35) and (36) where $|\psi_0\rangle = |\ell\rangle_{\rm p}|0\rangle_{\rm s}$, $\boldsymbol{V} = \boldsymbol{U}_{M,\ell} \otimes \boldsymbol{I}$ and $\varepsilon = \epsilon_M = \sin^2\theta_M$ for the ℓ-CQZ$_{M,N}$ gate. After M cycles, the photon state transitions back to the initial state $|\ell\rangle_{\rm p}$ with the probability
$$\zeta_0 = (1-\epsilon_M)^M = \cos^{2M}\theta_M. \tag{45}$$
As $M \to \infty$, this probability goes to one.
- $\mathsf{x} = 1$: In the presence of AO, the state of $|\bar{\ell}\rangle$ photon component is unchanged by $\bar{\ell}$-QZ$_N$ gate transformation. Unless the photon is absorbed by QAO, the component of the photon in path state $|1\rangle_{\rm s}$ reunites with the component of the photon in path state $|0\rangle_{\rm s}$ in the ℓ-QZ$_M$ gate. After $m\,(\leq M)$ cycles, the state of the photon transforms to
$$\begin{aligned}|\psi_m\rangle &= \left(|\ell\rangle_{\rm p}\langle\ell| \otimes \boldsymbol{I} + |\bar{\ell}\rangle_{\rm p}\langle\bar{\ell}| \otimes \boldsymbol{P}_{\rm x}\right)\left(\boldsymbol{U}_{M,\ell} \otimes \boldsymbol{I}\right)^m |\psi_0\rangle \\ &= \cos(m\theta_M)\,|\ell\rangle_{\rm p}|0\rangle_{\rm s} + \sin(m\theta_M)\,|\bar{\ell}\rangle_{\rm p}|1\rangle_{\rm s}.\end{aligned} \tag{46}$$
Upon completion of the protocol, the photon state transforms to $|\bar{\ell}\rangle$ with probability
$$\zeta_1 = \prod_{m=1}^{M}\left(1-\epsilon_{m,N}\right)^{LN} \tag{47}$$
where $\epsilon_{m,N} = \sin^2(m\theta_M)\sin^2(\theta_N)$. As $N \to \infty$, this probability approaches to one (see Fig. 12).[3]

[3]For simplicity, we set $L = 1$ for all numerical examples in this paper.

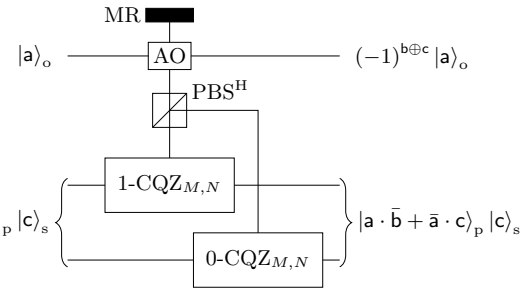


Fig. 13. D-CQZ$_{M,N}$ gate with M outer and N inner cycles [65].

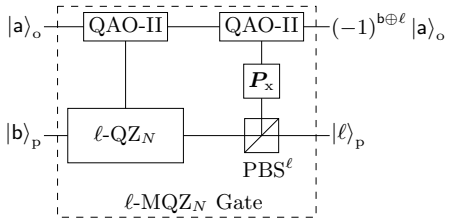


Fig. 14. ℓ-MQZ$_N$ gate with N cycles. Here ℓ-MQZ$_N$ gate uses the ℓ-QZ$_N$ gate [65].

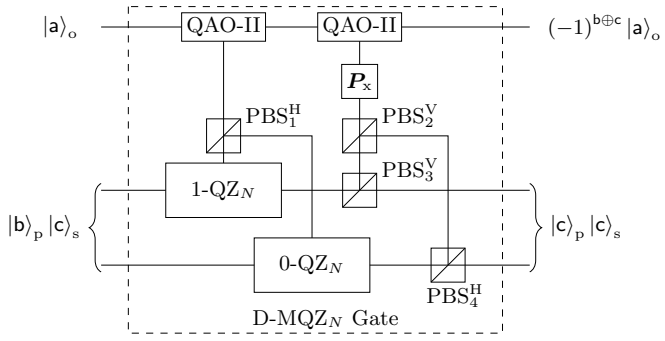


Fig. 15. D-MQZ$_N$ gate with N cycles [18].

Following the same procedure, the input state $|\mathsf{a}\rangle_{\rm o}|\mathsf{b}\rangle_{\rm p}$ is transformed by the ℓ-CQZ$_{M,N}$ gate to:

$$\ell\text{-CQZ}_{M,N}: \begin{cases} |\mathsf{a}\rangle_{\rm o}|\mathsf{b}\rangle_{\rm p} \to (-1)^{\mathsf{b}\oplus\ell}|\mathsf{a}\rangle_{\rm o}\left|\mathsf{x}\cdot\bar{\mathsf{b}}+\bar{\mathsf{a}}\cdot\ell\right\rangle_{\rm p} \\ \text{with the probability } \zeta_0^{\mathsf{b}\bar{\oplus}\ell}\zeta_1^{\mathsf{a}}\zeta_2^{\mathsf{b}\oplus\ell}\end{cases} \tag{48}$$

where

$$\zeta_2 = \epsilon_M\left(1-\epsilon_M\right)^{M-1}. \tag{49}$$

Since ζ_2 approaches to zero as $M \to \infty$, a general composite state of QAO-I and photon for the ℓ-CQZ$_{M,N}$ gate is approximated as

$$|\mathrm{cqz}_\ell\rangle_{\rm op} = \alpha_0|0\ell\rangle_{\rm op} + \alpha_1|10\rangle_{\rm op} + \alpha_2|11\rangle_{\rm op}. \tag{50}$$

From (48), the input state $|\mathrm{cqz}_\ell\rangle_{\rm op}$ is transformed by the ℓ-CQZ$_{M,N}$ gate to

$$\begin{aligned}\ell\text{-CQZ}_{M,N}\left(|\mathrm{cqz}_\ell\rangle_{\rm op}\right) = \alpha_0|0\ell\rangle_{\rm op} &+ (-1)^{\ell}\alpha_1|11\rangle_{\rm op} \\ &+ (-1)^{\bar{\ell}}\alpha_2|10\rangle_{\rm op}\end{aligned} \tag{51}$$

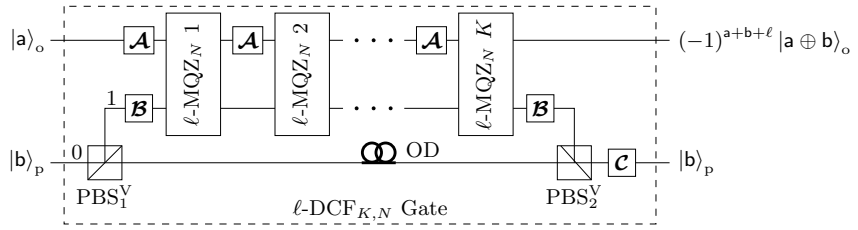


Fig. 16. ℓ-DCF$_{K,N}$ gate with K MQZ gates where each MQZ gate has N cycles. The ℓ-DCF$_{K,N}$ gate uses the ℓ-MQZ$_N$ gate. Here, $\boldsymbol{\mathcal{A}} = \boldsymbol{R}_y\,(2\theta_K)$ and $\boldsymbol{\mathcal{B}} = \boldsymbol{P}_{\mathrm{x}}^{\ell}$ [18].

with probability $\lambda_2 = f_1\left(|\alpha_0|^2, |\alpha_1|^2 + |\alpha_2|^2\right)$ tending to one as $M, N \to \infty$, where

$$f_1\,(u,v) = (1-u\epsilon_M)^M \prod_{m=1}^{M} (1-v\epsilon_{m,N})^{LN}\,. \tag{52}$$

C. Dual CQZ Gates

The dual CQZ (D-CQZ) gate is the dual form of CQZ gates (see Fig. 13). The D-CQZ$_{M,N}$ gate with M outer and N inner cycles takes a $|\mathsf{b}\rangle_{\mathrm{p}}$ polarized photon in path state $|\mathsf{c}\rangle_{\mathrm{s}}$ and an AO in state $|\mathsf{a}\rangle_{\mathrm{o}}$ as an input. The protocol starts by directing the photon component in path state $|\ell\rangle_{\mathrm{s}}$ to the ℓ-CQZ$_{M,N}$ gate. Note that PBS$^{\mathrm{V}}$ combines the photon components in the control terminals of 0-CQZ$_{M,N}$ and 1-CQZ$_{M,N}$ gates. From (48), the input state $|\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}|\mathsf{c}\rangle_{\mathrm{s}}$ is transformed by the D-CQZ$_{M,N}$ gate as follows:

$$\text{D-CQZ}_{M,N}: \begin{cases} |\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}|\mathsf{c}\rangle_{\mathrm{s}} \to (-1)^{\mathsf{b}\oplus\mathsf{c}}\,|\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{a}\cdot\bar{\mathsf{b}}+\bar{\mathsf{a}}\cdot\mathsf{c}\rangle_{\mathrm{p}}|\mathsf{c}\rangle_{\mathrm{s}} \\ \text{with the probability } \zeta_0^{\mathsf{b}\bar{\oplus}\mathsf{c}}\zeta_1^{\mathsf{a}}\zeta_2^{\mathsf{b}\oplus\mathsf{c}}\,. \end{cases} \tag{53}$$

Since ζ_2 approaches to zero as $M \to \infty$, a general composite state of QAO-I and photon for the D-CQZ$_{M,N}$ gate is approximated as

$$|\mathrm{dcqz}\rangle_{\mathrm{ops}} = \gamma|\mathrm{cqz}_0\rangle_{\mathrm{op}}|0\rangle_{\mathrm{s}} + \delta|\mathrm{cqz}_1\rangle_{\mathrm{op}}|1\rangle_{\mathrm{s}}. \tag{54}$$

From (53), the input state $|\mathrm{dcqz}\rangle_{\mathrm{ops}}$ is transformed by the D-CQZ$_{M,N}$ gate to

$$\begin{aligned} &\text{D-CQZ}_{M,N}\left(|\mathrm{dcqz}\rangle_{\mathrm{ops}}\right) \\ &\quad = \gamma\alpha_0|000\rangle_{\mathrm{ops}} + \gamma\alpha_1|110\rangle_{\mathrm{ops}} - \gamma\alpha_2|100\rangle_{\mathrm{ops}} \\ &\qquad + \delta\alpha_0|011\rangle_{\mathrm{ops}} - \delta\alpha_1|111\rangle_{\mathrm{ops}} + \delta\alpha_2|101\rangle_{\mathrm{ops}} \end{aligned} \tag{55}$$

with the probability λ_2.

D. MQZ Gates

The modified version of QZ gates has been presented in [18]—namely, the *MQZ gate* as illustrated in Fig. 14. The main advantage of MQZ gates is associated with type-II QAO where PBS separates the H and V components of the photon such that $|0\rangle_{\mathrm{o}}$ and $|1\rangle_{\mathrm{o}}$ act as $\mathsf{x} = \bar{\ell}$ and $\mathsf{x} = \ell$, respectively, for the ℓ-QZ$_N$ gate, as shown in Fig. 10(b). To demonstrate the operating principle of MQZ gates, assume that the ℓ-MQZ$_N$ gate takes $|\psi_0\rangle = |\mathsf{a}\rangle_{\mathrm{o}}|\ell\rangle_{\mathrm{p}}$ as an input. From (40), the ℓ-QZ$_N$ gate transforms the composite state of an AO and photon to $|\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{a}\cdot\ell\rangle_{\mathrm{p}}$ with the probability $\mu_0^{\bar{\mathsf{a}}\oplus\ell}$. The PBS$^{\ell}$ redirects the $|\bar{\ell}\rangle_{\mathrm{p}}$ component of the photon towards the AO to discard the component of the photon found in the control terminal. Unless the photon is absorbed by the AO, the composite state collapses to the initial state. Following the same procedure, the input state $|\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}$ is transformed by the ℓ-MQZ$_N$ gate as follows:

$$\ell\text{-MQZ}_N: \begin{cases} |\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}} \to (-1)^{\mathsf{b}\oplus\ell}\,|\mathsf{a}\rangle_{\mathrm{o}}|\ell\rangle_{\mathrm{p}} \\ \text{with probability } \mu_{\mathsf{b}\oplus\ell}^{\bar{\mathsf{a}}\oplus\ell}\Delta_{\mathsf{a},\mathsf{b},\ell} \end{cases} \tag{56}$$

where $\Delta_{\mathsf{a},\mathsf{b},\ell} = 0$ if $\mathsf{a} \neq \mathsf{b} = \ell$, otherwise $\Delta_{\mathsf{a},\mathsf{b},\ell} = 1$.

Since $\Delta_{\mathsf{a},\mathsf{b},\ell} = 0$ for $\mathsf{a} \neq \mathsf{b} = \ell$, the ℓ-MQZ$_N$ gate takes the Bell-type composite state $|\mathrm{mqz}_\ell\rangle_{\mathrm{op}}$ of QAO-II and photon as an input

$$|\mathrm{mqz}_\ell\rangle_{\mathrm{op}} = \left(\alpha_0|00\rangle_{\mathrm{op}} + \alpha_1|11\rangle_{\mathrm{op}}\right) \tag{57}$$

where $|\alpha_0|^2 + |\alpha_1|^2 = 1$. From (56), the input state $|\mathrm{mqz}_\ell\rangle_{\mathrm{op}}$ is transformed by the ℓ-MQZ$_N$ gate to

$$\ell\text{-MQZ}_N\left(|\mathrm{mqz}_\ell\rangle_{\mathrm{op}}\right) = \left(\alpha_0|0\rangle_{\mathrm{o}} - \alpha_1|1\rangle_{\mathrm{o}}\right)|\ell\rangle_{\mathrm{p}} \tag{58}$$

with probability $\lambda_3 = f_2\left(|\alpha_\ell|^2\right)$ where

$$f_2\,(x) = x\left(1 - x\sin^2\theta_N\right)^N. \tag{59}$$

E. Dual MQZ Gates

The dual MQZ (D-MQZ) gate represents the dual form of MQZ gates (see Fig. 15). Similar to MQZ gates, the main advantage of D-MQZ gates is associated with type-II QAO (see Fig. 10(b)). The D-MQZ$_N$ gate with N cycles takes a $|\mathsf{b}\rangle_{\mathrm{p}}$ polarized photon in path state $|\mathsf{c}\rangle_{\mathrm{s}}$ and type-II QAO in state $|\mathsf{a}\rangle_{\mathrm{o}}$ as input. Similar to D-CQZ gates, Bob inputs the component of the photon in path state $|\ell\rangle_{\mathrm{s}}$ to the ℓ-QZ$_N$ gate. Here, it is important to note that PBS$^{\mathrm{H}}$ combines the components of the photon in the control terminals of 0-QZ$_N$ and 1-QZ$_N$ gates. From (56), the input state $|\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}|\mathsf{c}\rangle_{\mathrm{s}}$ is transformed by the D-MQZ$_N$ gate as follows:

$$\text{D-MQZ}_N: \begin{cases} |\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}|\mathsf{c}\rangle_{\mathrm{s}} \to (-1)^{\mathsf{b}\oplus\mathsf{c}}\,|\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{c}\rangle_{\mathrm{p}}|\mathsf{c}\rangle_{\mathrm{s}} \\ \text{with the probability } \mu_{\mathsf{b}\oplus\mathsf{c}}^{\bar{\mathsf{a}}\oplus\mathsf{c}}\Delta_{\mathsf{a},\mathsf{b},\mathsf{c}}. \end{cases} \tag{60}$$

Since $\Delta_{\mathsf{a},\mathsf{b},\mathsf{c}} = 0$ for $\mathsf{a} \neq \mathsf{b} = \mathsf{c}$, a general composite state of QAO-II and photon for the D-MQZ$_N$ gate is approximated as

$$|\mathrm{dmqz}\rangle_{\mathrm{ops}} = \gamma|\mathrm{mqz}_0\rangle_{\mathrm{op}}|0\rangle_{\mathrm{s}} + \delta|\mathrm{mqz}_1\rangle_{\mathrm{op}}|1\rangle_{\mathrm{s}}. \tag{61}$$

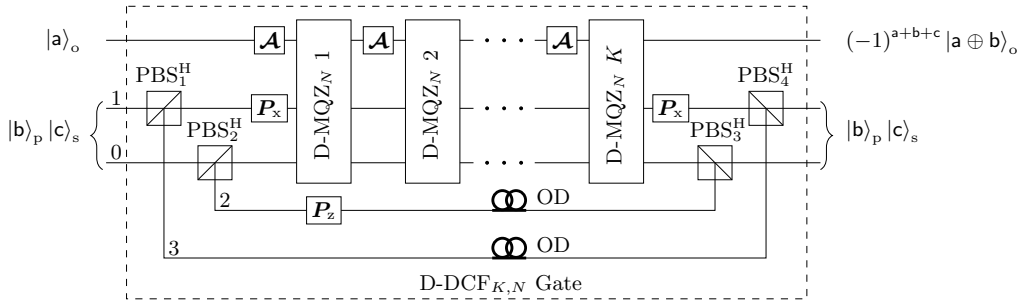


Fig. 17. D-DCF$_{K,N}$ gate with K D-MQZ gates where each D-MQZ gate has N cycles [18].

From (60), the input state $|\mathrm{dmqz}\rangle_{\mathrm{ABC}}$ is transformed by the D-MQZ$_N$ gate to

$$\text{D-MQZ}_N\big(|\mathrm{dmqz}\rangle_{\mathrm{ops}}\big) = \gamma|000\rangle_{\mathrm{ops}} + \delta|111\rangle_{\mathrm{ops}} \tag{62}$$

with probability $\lambda_4 = f_2\big(|\gamma\alpha_0|^2 + |\delta\alpha_1|^2\big)$.

F. DCF Gates

The DCF gates represent the concatenated version of the MQZ gates. Fig. 16 shows the schematic of the DCF gate where 0-DCF$_{K,N}$ and 1-DCF$_{K,N}$ are two types of the DCF gates. Note that the ℓ-DCF$_{K,N}$ gate uses K ℓ-MQZ$_N$ gates concatenated in series. To demonstrate the operating principle of DCF gates, assume that the ℓ-DCF$_{K,N}$ gate takes $|\psi_0\rangle = |\mathsf{x}\rangle_{\mathrm{o}}|0\rangle_{\mathrm{p}}$ as an input where $|\mathsf{x}\rangle_{\mathrm{o}}$ denotes the initial state of QAO-II encoded in an electron. The protocol starts by directing the photon towards $\mathrm{PBS}_1^{\mathrm{V}}$, which allows the V component of the photon to pass and redirects the H component of the photon towards ℓ-MQZ$_N$ gates. We perform local operations $\boldsymbol{\mathcal{A}} = \boldsymbol{R}_y\,(2\theta_K)$ and $\boldsymbol{\mathcal{B}} = \boldsymbol{P}_{\mathsf{x}}^{\ell}$ on the electron and photon, respectively, and the composite state of electron and photon transforms to $|\psi_1\rangle$ where

$$|\psi_1\rangle = \big(\cos(\theta_K)\,|\mathsf{x}\rangle_{\mathrm{o}} + (-1)^{\mathsf{x}}\sin(\theta_K)\,|\bar{\mathsf{x}}\rangle_{\mathrm{o}}\big)|\ell\rangle_{\mathrm{p}}|1\rangle_{\mathrm{s}}. \tag{63}$$

Now, we input the electron and the component of the photon in path state $|1\rangle_{\mathrm{s}}$ to the ℓ-MQZ$_N$ gate, where $|0\rangle_{\mathrm{s}}$ and $|1\rangle_{\mathrm{s}}$ denote the optical path from $\mathrm{PBS}_1^{\mathrm{V}}$ to $\mathrm{PBS}_2^{\mathrm{V}}$ and $\mathrm{PBS}_1^{\mathrm{V}}$ to the ℓ-MQZ$_N$ gate, respectively.

- $\mathsf{x} = \ell$: From (56), the first ℓ-MQZ$_N$ gate transforms the composite state of the electron and photon $|\psi_1\rangle$ to $|\psi_2\rangle = |\ell\rangle_{\mathrm{o}}|\ell\rangle_{\mathrm{p}}|1\rangle_{\mathrm{s}}$ with probability

$$\zeta_2 = \big(1-\sin^2\theta_K\big)\big(1-\cos^2\theta_K\sin^2\theta_N\big)^N. \tag{64}$$

  After $K-1$ subsequent ℓ-MQZ$_N$ gates, the composite state of the electron and photon collapses to $|\psi_2\rangle$ with probability $\zeta_3 = f_3\,(1)$ where

$$\begin{aligned} f_3\,(u) = &\big(1-u\sin^2\theta_K\big)^K \\ &\times\big(1-u\cos^2\theta_K\sin^2\theta_N\big)^{KN} \end{aligned} \tag{65}$$

  tending to one as K and N approaches to infinity. In case the photon interacts with the electron, it is absorbed by the electron and causes an erasure of the information.

- $\mathsf{x} = \bar{\ell}$: Similar to $\mathsf{x} = \ell$ case, the first ℓ-MQZ$_N$ gate transforms the composite state of the electron and photon $|\psi_1\rangle$ to $|\psi_2\rangle$ with probability

$$\zeta_4 = \big(1-\cos^2\theta_K\big)\big(1-\sin^2\theta_K\sin^2\theta_N\big)^N \tag{66}$$

  approaching to zero as K and N go to infinity. After $K-1$ subsequent ℓ-MQZ$_N$ gates, the composite state of the electron and photon remains unchanged with probability

$$\zeta_5 = \frac{\zeta_4 f_3\,(1)}{\zeta_2}. \tag{67}$$

Upon completion of the protocol, we again perform local operation $\mathcal{B}$ on the photon and direct the photon towards $\mathrm{PBS}_2^{\mathrm{V}}$ to discard the path information of the photon. Here, it is important to note that if the input state is $|\mathsf{x}\rangle_{\mathrm{o}}|1\rangle_{\mathrm{p}}$, there is no electron-photon interaction, and the composite state of the photon transforms to $|\bar{\mathsf{x}}\rangle_{\mathrm{o}}|1\rangle_{\mathrm{p}}$ with probability one. Following the same procedure, the input state $|\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}$ is transformed by the ℓ-DCF$_{K,N}$ gate as follows:

$$\ell\text{-DCF}_{K,N}: \begin{cases} |\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}} \to (-1)^{\mathsf{a}+\mathsf{b}+\ell}\,|\mathsf{a}\oplus\mathsf{b}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}} \\ \text{with probability } \zeta_3^{\bar{\mathsf{b}}}\Delta_{\mathsf{a},\mathsf{b}\oplus\ell,\ell}. \end{cases} \tag{68}$$

Since ζ_5 approaches zero as K and N go to infinity, a general composite state of QAO-II and photon for the ℓ-DCF$_{K,N}$ gate is approximated as

$$|\mathrm{dcf}_\ell\rangle_{\mathrm{op}} = \alpha_0|\ell 0\rangle_{\mathrm{op}} + \alpha_1|01\rangle_{\mathrm{op}} + \alpha_2|11\rangle_{\mathrm{op}}. \tag{69}$$

From (68), the input state $|\mathrm{dcf}_\ell\rangle_{\mathrm{op}}$ is transformed by the ℓ-DCF$_{K,N}$ gate to

$$|\mathrm{dcf}_{\ell 1}\rangle_{\mathrm{op}} = \alpha_0|\ell 0\rangle_{\mathrm{op}} + (-1)^{\bar{\ell}}\,\alpha_1|01\rangle_{\mathrm{op}} + (-1)^{\ell}\,\alpha_2|11\rangle_{\mathrm{op}}. \tag{70}$$

with probability $\lambda_5 = f_3\,\big(|\alpha_0|^2\big)$.

G. Dual DCF Gates

The dual DCF (D-DCF) gates represent the dual form of the DCF gates and the concatenated version of the D-MQZ gate. Fig. 17 shows the schematic of the D-DCF gate where K D-MQZ gates are concatenated in series. The D-DCF gate takes $|\mathsf{b}\rangle_{\mathrm{p}}$ in path state $|\mathsf{c}\rangle_{\mathrm{s}}$ and an AO encoded in type-II QAO in state $|\mathsf{a}\rangle_{\mathrm{o}}$ as an input. The protocol starts by directing the photon towards $\mathrm{PBS}_1^{\mathrm{H}}$ and $\mathrm{PBS}_2^{\mathrm{H}}$, which separate the H and V components of the photon in each path. The PBSs direct the

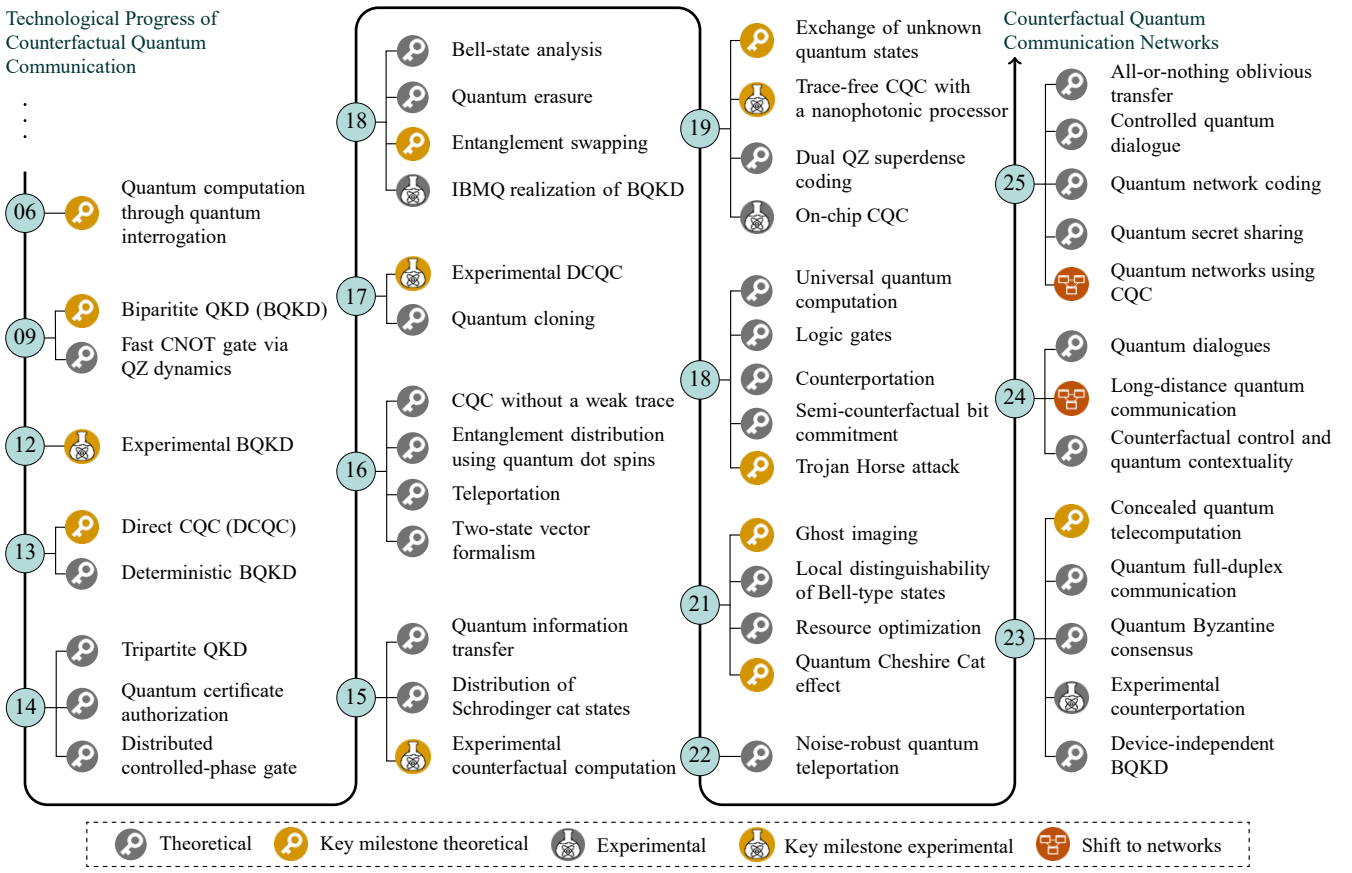


Fig. 18. Technological progress in CQC, starting from quantum computation through quantum interrogation and evolving to diverse CQC protocols. Distinct icons are used to distinguish theoretical developments, experimental demonstrations, and a shift to networks, with milestone years highlighted in yellow to mark key advances in CQC.

$|\mathsf{h}\rangle_{\mathrm{p}}$ component of the photon in path state $|\ell\rangle_{\mathrm{s}}$ to the ℓ-MQZ$_N$ gate (in the D-MQZ gate). The D-DCF gate operates similar as DCF gates and transforms the input state $|\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}|\mathsf{c}\rangle_{\mathrm{s}}$ as follows:

$$\text{D-DCF}_{K,N}: \begin{cases} |\mathsf{a}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}|\mathsf{c}\rangle_{\mathrm{s}} \rightarrow (-1)^{\mathsf{a}+\mathsf{b}+\mathsf{c}}\,|\mathsf{a}\oplus\mathsf{b}\rangle_{\mathrm{o}}|\mathsf{b}\rangle_{\mathrm{p}}|\mathsf{c}\rangle_{\mathrm{s}} \\ \text{with the probability } \zeta_3^{\bar{\mathsf{b}}}\Delta_{\mathsf{a},\mathsf{b}\oplus\mathsf{c},\mathsf{c}}. \end{cases} \tag{71}$$

A general composite state of QAO-II and photon for the D-DCF$_{K,N}$ gate is approximated as

$$|\mathrm{ddcf}_0\rangle_{\mathrm{ops}} = \gamma|\mathrm{dcf}_0\rangle_{\mathrm{op}}|0\rangle_{\mathrm{s}} + \delta|\mathrm{dcf}_1\rangle_{\mathrm{op}}|1\rangle_{\mathrm{s}}. \tag{72}$$

From (71), the input state $|\mathrm{ddcf}\rangle_{\mathrm{ops}}$ is transformed by the D-DCF$_{K,N}$ gate to

$$\begin{aligned} \text{D-DCF}_{K,N}\left(|\mathrm{ddcf}\rangle_{\mathrm{ops}}\right) = \gamma|\mathrm{dcf}_{01}\rangle_{\mathrm{op}}|0\rangle_{\mathrm{s}} \\ + \delta|\mathrm{dcf}_{11}\rangle_{\mathrm{op}}|1\rangle_{\mathrm{s}} \end{aligned} \tag{73}$$

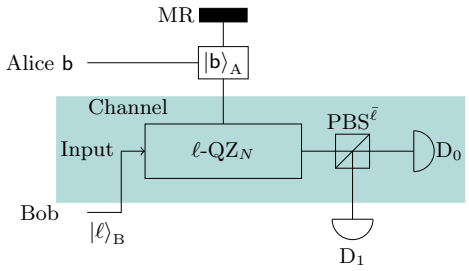
with probability λ_5. Overall, the QZ, CQZ, and MQZ gates constitute the foundational gates for CQC protocols. Developed upon these foundational gates, D-CQZ, D-MQZ, DCF, and D-DCF represent advanced gates, facilitating the implementation of specialized and application-specific CQC communication frameworks.

V. CQC Protocols

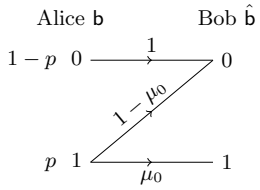
The CQC protocols can be designed to transmit classical as well as quantum information by using QZ, CQZ, MQZ, and DCF gates. Fig. 18 illustrates the technological evolution in CQC, beginning with foundational developments in counterfactual quantum computation [50], [111], [112] and cryptography [59], [113]–[119], and extending to advanced CQC protocols [42], [43], [50], [52], [57], [62]–[66], [110], [120]–[154]. This timeline highlights the key theoretical milestones, the progression toward experimental maturity, and the prospective integration into quantum networks. This section focuses on CQC protocols that facilitate information exchange, emphasizing simplex and full-duplex communication protocols to transmit classical and quantum information in a counterfactual manner.

A. Simplex CQC for Classical Information

To transmit classical information in one direction, we consider that Alice acts as a sender who controls the existence of an AO in a classical manner, whereas Bob receives one bit of classical information in each round of communication. Assume that Alice encodes one bit of classical information b as $|\mathsf{b}\rangle_{\mathrm{A}} = |\mathsf{b}\rangle_{\mathrm{o}}$ where the subscript A denotes a qubit possessed by Alice.



(a) QZ communication



(b) Binary Z-channel

Fig. 19. Simplex QZ communication for classical information [65]. (a) Alice encodes one-bit information in the classical behavior of AO and Bob inputs $|\ell\rangle_{\mathrm{B}}$ polarized photon in the ℓ-QZ$_N$ gate. Bob decodes one-bit classical information as $\hat{\mathsf{b}}=1$ if the detector D$_1$ clicks. Otherwise, Bob decodes one-bit classical information as $\hat{\mathsf{b}}=0$. (b) The simplex QZ communication forms a binary Z-channel.

1) Simplex QZ Communication: As illustrated in Fig. 19(a), Bob equips a single-photon source and detector D$_1$ for simplex QZ communication. The QZ gate forms part of the transmission channel and is connected to the single-photon source at the input terminal [128]. Bob initiates the protocol by generating his $|\ell\rangle_{\mathrm{B}}$ polarized single photon and directing it towards the ℓ-QZ$_N$ gate. Bob decides $\hat{\mathsf{b}}=1$ if D$_1$ clicks, where $\hat{\mathsf{b}}\in\{0,1\}$. Otherwise, Bob decides $\hat{\mathsf{b}}=0$. It is noteworthy that Bob decodes the classical information as $\hat{\mathsf{b}}=0$ in case the photon is discarded in the QZ gate for $\mathsf{b}=1$, resulting in a classical binary Z-channel (see Fig. 19(b)). Let $p=\mathbb{P}\{\mathsf{b}=1\}$. Then, the mutual information $\mathcal{I}_1\big(\mathsf{b};\hat{\mathsf{b}}\big)$ is

$$\mathcal{I}_1\big(\mathsf{b};\hat{\mathsf{b}}\big)=h\left(p\right)-q_1 h\left(\frac{p\left(1-\mu_0\right)}{q_1}\right) \tag{74}$$

where $h\left(p\right)=-p\log_2\left(p\right)-\left(1-p\right)\log_2\left(1-p\right)$ is the binary entropy function and

$$\begin{aligned} q_1&=\mathbb{P}\Big\{\hat{\mathsf{b}}=0\Big\}\\ &=\left(1-p\right)+p\left(1-\mu_0\right). \end{aligned} \tag{75}$$

According to Shannon's channel coding theorem [155], [156], the capacity is defined as the maximum mutual information achieved over all possible input distributions. Hence, the capacity C_1 in [bits/photon] can be determined by optimizing the mutual information $\mathcal{I}_1\big(\mathsf{b};\hat{\mathsf{b}}\big)$ with respect to the input distribution p, which simplifies to [65]:

$$C_1=\log_2\Big(1+2^{g(\mu_0)}\Big) \tag{76}$$

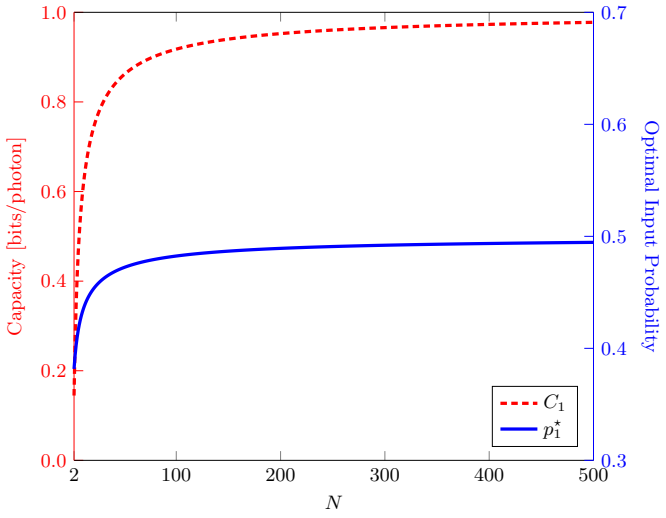


Fig. 20. Capacity C_1 [bits/photon] and capacity-achieving probability $p_1^\star$ as a function of N for simplex QZ communication.

where $g\left(\mu_0\right)=\mu_0/h\left(\mu_0\right)$ and the optimal probability distribution is

$$p_1^\star=\frac{1}{\mu_0\big(1+2^{-g(\mu_0)}\big)}. \tag{77}$$

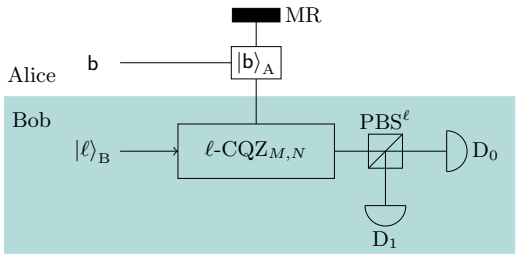
Fig. 20 shows the capacity C_1 and the optimal (i.e., capacity-achieving) probability $p_1^\star$ as a function of N. It can be seen that the capacity tends to 1 bit/photon with $p_1^\star$ approaching $1/2$ as $N\to\infty$. Note that the photon is transmitted in the opposite direction of the information flow. In case Bob equips the QZ gate, detectors D$_0$, and D$_1$ for simplex communication, the QZ gate enables particle-free communication for $\mathsf{b}=1$ only—called the *semi-counterfactual* communication [12]. The photon is found in the transmission channel with certainty for $\mathsf{b}=0$ [65].

2) Simplex CQZ Communication: For simplex CQZ communication, Bob is equipped with the CQZ gate where the control terminal is connected with Alice's AO via a quantum channel, as illustrated in Fig. 21(a) [12], [62], [125]. The protocol starts by directing the $|\ell\rangle_{\mathrm{B}}$ polarized photon to the ℓ-CQZ$_{M,N}$ gate and Bob decodes the message $\hat{\mathsf{b}}$ as the detector D$_{\hat{\mathsf{b}}}$ clicks. If the photon is found in the quantum channel, it is either discarded at the detector D inside the CQZ gate (when $\mathsf{b}=0$ with the probability $1-\zeta_0$) or absorbed by AO (when $\mathsf{b}=1$ with the probability $1-\zeta_1$). This simplex communication forms an asymmetric binary erasure channel (BEC) (see Fig. 21(b)) and the mutual information $\mathcal{I}_2\big(\mathsf{b};\hat{\mathsf{b}}\big)$ is

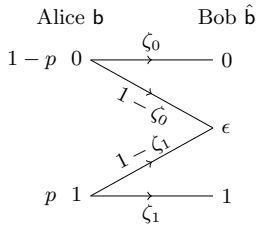
$$\mathcal{I}_2\big(\mathsf{b};\hat{\mathsf{b}}\big)=h\left(p\right)-q_2 h\left(\frac{p\left(1-\zeta_1\right)}{q_2}\right) \tag{78}$$

where

$$\begin{aligned} q_2&=\mathbb{P}\{\mathsf{b}\text{ is erasured}\}\\ &=\left(1-p\right)\left(1-\zeta_0\right)+p\left(1-\zeta_1\right). \end{aligned} \tag{79}$$



(a) CQZ communication



(b) Asymmetric BEC

Fig. 21. Simplex CQZ communication for classical information [65]. (a) Alice encodes one-bit information in the classical behavior of AO and Bob inputs $|\ell\rangle_{\mathrm{B}}$ polarized photon in the ℓ-CQZ$_{M,N}$ gate. Bob decodes one-bit classical information as $\hat{\mathsf{b}}$ if the detector D$_{\hat{\mathsf{b}}}$ clicks. (b) The simplex CQZ communication forms an asymmetric BEC.

In general, the capacity C_2 in [bits/photon] can be determined by optimizing the mutual information $\mathcal{I}_2(\mathsf{b};\hat{\mathsf{b}})$ with respect to the input distribution p which simplifies to:

$$\frac{\left[(1-p)(1-\zeta_0)+p(1-\zeta_1)\right]^{\zeta_0+\zeta_1}}{p^{\zeta_1}(1-p)^{\zeta_0}} = \zeta_1^{\zeta_1}\zeta_0^{\zeta_0}2^{h(\zeta_0)-h(\zeta_1)} \tag{80}$$

leading to the optimal probability $p_2^\star$, which can be obtained numerically. Fig. 22 shows the capacity C_2 and the capacity-achieving probability $p_2^\star$ as a function of N when $M=2$ and $L=1$. It can be seen that the capacity tends to 1 bit/photon with $p_2^\star$ approaching $1/2$ as $N\to\infty$ [65].

B. Full-Duplex CQC for Classical Information

1) Quantum Duplex Coding: Fig. 23(a) illustrates the full-duplex CQC protocol—called *quantum duplex coding*—which enables Alice and Bob to simultaneously exchange a single bit of classical information in each direction using preshared entanglement. The basic idea of full-duplex CQC originates from the quantum superdense coding, which allows a sender to transmit two bits of classical information using one qubit [123], [157], [158]. Similar to the quantum superdense coding, assume that Alice and Bob possess a preshared entangled state $|\psi_{00}\rangle_{\mathrm{AB}}$ where

$$|\psi_{\mathsf{ab}}\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}\big(|\mathsf{a}0\rangle_{\mathrm{AB}} + (-1)^{\mathsf{b}}\,|\bar{\mathsf{a}}1\rangle_{\mathrm{AB}}\big). \tag{81}$$

Alice and Bob each encode one bit of classical information as follows:

$$|\psi_0\rangle = \big(\boldsymbol{P}_{\mathrm{z}}^{\mathsf{b}_1}\otimes\boldsymbol{P}_{\mathrm{x}}^{\mathsf{b}_2}\big)|\psi_{00}\rangle_{\mathrm{AB}} \tag{82}$$

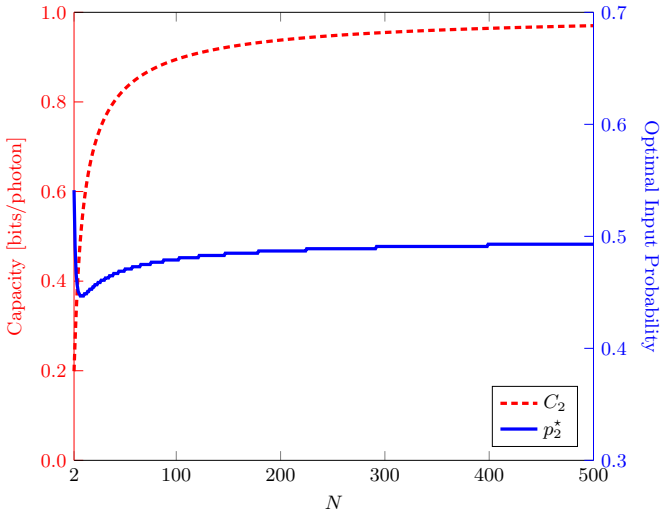


Fig. 22. Capacity C_2 [bits/photon] and capacity-achieving probability $p_2^\star$ as a function of N for simplex CQZ communication when $M=2$.

where $\mathsf{b}_1,\mathsf{b}_2\in\{0,1\}$ denote the classical information Alice and Bob want to transmit, respectively. As the full-duplex CQC uses preshared entanglement, the communication task is achieved by using the QAO-II and DCF gates. Note that qubits A and B are encoded in QAO-II and a photon, respectively. After encoding the information, Alice and Bob apply the ℓ-DCF$_{K,N}$ gates for $\mathsf{b}_2=\ell$ (see Fig 16). The overall action of the DCF gates for Bell states is the same as the CNOT gate, where qubits A and B act as target and control qubits, respectively, and disentangles the Bell state as follows:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}|\mathsf{b}_2\rangle_{\mathrm{A}}\big(|0\rangle_{\mathrm{B}} + (-1)^{\mathsf{b}_1}\,|1\rangle_{\mathrm{B}}\big) \tag{83}$$

with probability $\zeta_{\mathrm{c}} = f_3(1/2)$.

To decode the classical information, Alice directly measures her qubit in the computational basis and decides the classical information $\hat{\mathsf{b}}_2$ corresponding to the post-measurement state $|\hat{\mathsf{b}}_2\rangle_{\mathrm{A}}$ whereas Bob applies a Hadamard gate on his qubit before measuring his qubit in the computational basis and decides the classical information $\hat{\mathsf{b}}_1$ corresponding to the post-measurement state $|\hat{\mathsf{b}}_1\rangle_{\mathrm{B}}$. In case any physical particle appears in the transmission channel, it is absorbed by the QAO-II. It causes the erasure of b_1 and b_2 and forms the full-duplex BEC as shown in Fig. 23(b). Let $p_i=\mathbb{P}\{\mathsf{b}_i=1\}$, $i=1,2$. Then, the mutual information $\mathcal{I}(\mathsf{b}_i;\hat{\mathsf{b}}_i)$ is

$$\mathcal{I}_3(\mathsf{b}_i;\hat{\mathsf{b}}_i) = h(p_i) - (1-\zeta_{\mathrm{c}}). \tag{84}$$

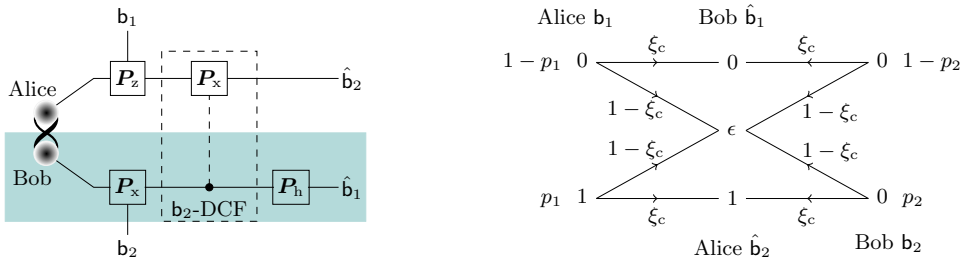
The total capacity C_3 [bits/Bell-pair] for capacity-achieving $p_i^\star = \arg\max_{p_i}\mathcal{I}_3(\mathsf{b}_i;\hat{\mathsf{b}}_i) = 1/2$ is

$$C_3 = 2\zeta_{\mathrm{c}} \tag{85}$$

tending to 2 bits/Bell-pair as $K,N\to\infty$ (see Fig. 24).

C. Simplex CQC for Quantum Information

To transmit quantum information in a single direction [63], [121], [159], [160], Alice controls the existence of an AO in



(a) Quantum duplex coding communication

(b) Full-duplex BEC

Fig. 23. Quantum duplex coding: full-duplex CQC for classical information [65]. (a) Alice and Bob exchange one bit of classical information in each direction simultaneously and counterfactually using a preshared Bell pair. (b) Quantum duplex coding forms a full-duplex BEC.

a quantum manner, and Bob receives one qubit of quantum information in each round of the communication. Assume that Alice encodes one qubit of quantum information into a QAO as $|\phi\rangle_{\rm A}$ where

$$|\phi\rangle_{\rm A} = \alpha_0|0\rangle_{\rm A} + \alpha_1|1\rangle_{\rm A}. \tag{86}$$

1) Simplex CQZ Communication: Fig. 25 shows the simplest model to transfer quantum information in a counterfactual manner. Bob commences the protocol by directing an H polarized photon towards a 0-CQZ$_{M,N}$ gate, which transforms the initial composite state $|\psi_1\rangle = |\phi\rangle_{\rm A}|0\rangle_{\rm B}$ to $|\psi_2\rangle$ with probability $\xi_1 = f_1\left(|\alpha_0|^2, |\alpha_1|^2\right)$ where

$$|\psi_2\rangle = \alpha_0|00\rangle_{\rm AB} + \alpha_1|11\rangle_{\rm AB}. \tag{87}$$

To disentangle Alice's qubit with Bob's qubit, Alice locally applies the Hadamard gate $\boldsymbol{P}_{\rm h}$ and measures her qubit in the computational basis, which collapses the state of Bob's qubit to

$$\boldsymbol{\Xi}_{\rm B} = \frac{1}{2}\left(|\phi\rangle_{\rm B}\langle\phi| + \boldsymbol{P}_{\rm z}|\phi\rangle_{\rm B}\langle\phi|\boldsymbol{P}_{\rm z}^{\dagger}\right) \tag{88}$$

where $|\phi\rangle_{\rm B} = \alpha_0|0\rangle_{\rm B} + \alpha_1|1\rangle_{\rm B}$. Alice publicly announces her measurement result m via classical communication, and Bob applies the $\boldsymbol{P}_{\rm z}^{\mathsf{m}}$ on his qubit to fully recover the transmitted quantum information. If the photon appears in the quantum channel, it is absorbed by the electron and forms a simplex quantum erasure channel. Note that this CQZ simplex communication protocol requires one-bit classical communication to transmit one-qubit quantum information. The quantum capacity Q_1 in [qubits/electron-photon] for CQZ communication is

$$Q_1 = \max\{0, 2\xi_1 - 1\} \tag{89}$$

tending to 1 qubit/electron-photon as $M, N \to \infty$. Fig. 26 illustrates the quantum capacity Q_1 and the optimal $M_1^{\star} = \arg\max_M \xi_1$ as a function of N when $|\alpha_0|^2 = |\alpha_1|^2 = 1/2$.

2) Simplex D-CQZ Communication: Fig. 27 shows the D-CQZ model to transfer quantum information counterfactually without requiring any classical communication. Initially, the composite state of Alice and Bob is given as $|\psi_1\rangle = |\phi\rangle_{\rm A}|0\rangle_{\rm B}$ and the 0-CQZ$_{M,N}$ gate transforms $|\psi_1\rangle$ to $|\psi_2\rangle$ in (87). Alice and Bob locally apply the Hadamard gate $\boldsymbol{P}_{\rm h}$ on their qubits, followed by the D-CQZ$_{M,N}$ gate as shown in Fig. 28. After the D-CQZ$_{M,N}$ gate, Bob applies BS$^{(\pi/4)}$ to create the equal

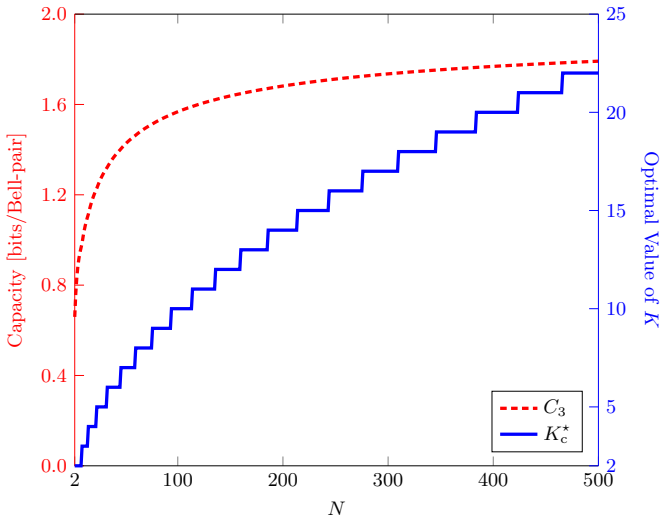


Fig. 24. Capacity C_3 [bits/Bell-pair] and optimal $K_{\rm c}^{\star} = \arg\max_K \zeta_{\rm c}$ as a function of N for quantum duplex coding.

superposition of the photon in two paths and the composite state of Alice and Bob is transformed to $|\psi_3\rangle$ with probability $\xi_2 = \xi_1 f_1\left(1/2, 1/2\right)$ where

$$\begin{aligned}|\psi_3\rangle = &\frac{\alpha_0}{2\sqrt{2}}\left(|00\rangle_{\rm AB} + |01\rangle_{\rm AB} + |10\rangle_{\rm AB} + |11\rangle_{\rm AB}\right)|0\rangle_{\rm C}\\ &+ \frac{\alpha_1}{2\sqrt{2}}\left(|00\rangle_{\rm AB} - |01\rangle_{\rm AB} + |10\rangle_{\rm AB} - |11\rangle_{\rm AB}\right)|0\rangle_{\rm C}\\ &+ \frac{\alpha_0}{2\sqrt{2}}\left(|00\rangle_{\rm AB} - |01\rangle_{\rm AB} - |10\rangle_{\rm AB} + |11\rangle_{\rm AB}\right)|1\rangle_{\rm C}\\ &+ \frac{\alpha_1}{2\sqrt{2}}\left(|00\rangle_{\rm AB} + |01\rangle_{\rm AB} - |10\rangle_{\rm AB} - |11\rangle_{\rm AB}\right)|1\rangle_{\rm C}\end{aligned} \tag{90}$$

and the qubit C denotes path information of the photon. Bob performs the non-demolition measurement to determine the photon path without significantly disturbing his quantum state. Now, Alice and Bob locally apply a $\boldsymbol{P}_{\rm h}$ gate on their respective qubits, followed by Bob applying $\boldsymbol{P}_{\rm x}^{\mathsf{m}}$ on his qubit to fully recover the quantum information, where m denotes the outcome of the non-demolition measurement. We obtain the quantum capacity $Q_2 = \max\{0, 2\xi_2 - 1\}$ in [qubits/electron-photon] for D-CQZ communication, tending to 1 qubit/electron-photon as $M, N \to \infty$. Fig. 28 illustrates the quantum capacity Q_2

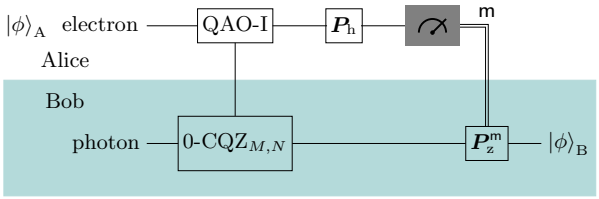


Fig. 25. Simplex CQZ communication for quantum information [65]. Alice encodes her one-qubit information in the quantum behavior of AO and Bob inputs his photon $|0\rangle_{\mathrm{B}}$ to the 0-CQZ$_{M,N}$ gate. Upon completion of the protocol, Alice measures her qubit in the computational basis and announces the measurement outcome for Bob to fully recover the quantum information.

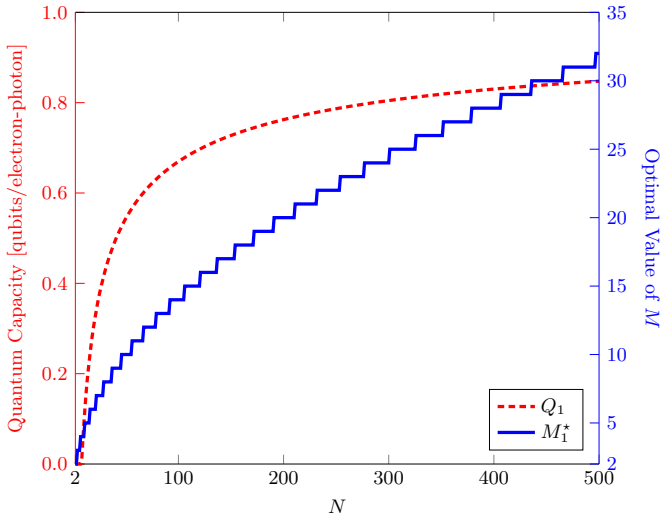


Fig. 26. Quantum capacity Q_1 [qubits/electron-photon] and optimal $M_1^\star = \arg\max_M \xi_1$ as a function of N for simplex CQZ communication when $|\alpha_0|^2 = |\alpha_1|^2 = 1/2$.

and optimal $M_2^\star = \arg\max_M \xi_2$ as a function of N when $|\alpha_0|^2 = |\alpha_1|^2 = 1/2$.

D. Full-duplex CQC for Quantum Information

Quantum state exchange is a full-duplex form of quantum communication, enabling Alice and Bob to exchange quantum information through preshared entanglement [161], [162]. Recently, counterfactual quantum state exchange protocols have been proposed without using preshared entanglement [64], [65], [163]. Alice and Bob encode their one-qubit quantum information as $|\phi_1\rangle_{\mathrm{A}} = |\phi\rangle_{\mathrm{A}}$ and $|\phi_2\rangle_{\mathrm{B}}$, respectively, where

$$|\phi_2\rangle_{\mathrm{B}} = \beta_0|0\rangle_{\mathrm{B}} + \beta_1|1\rangle_{\mathrm{B}} \tag{91}$$

with $|\beta_0|^2 + |\beta_1|^2 = 1$.

1) Quantum Telexchanging: Consider the initial composite state of Alice and Bob is given as $|\psi_1\rangle = |\phi_1\rangle_{\mathrm{A}}|\phi_2\rangle_{\mathrm{B}}$. To achieve full-duplex communication for quantum information, Bob entangles his qubit B with an ancillary qubit C initialized as $|0\rangle_{\mathrm{C}}$ where the qubit C denotes the photon path information (see Fig. 29). This can be done by directing his photon towards PBS$^{\mathrm{H}}$, as shown in Fig. 30. Alice and Bob apply the nonlocal CNOT operation on their qubits, where the qubit A acts as a control and the qubit B acts as a target qubit, respectively. To

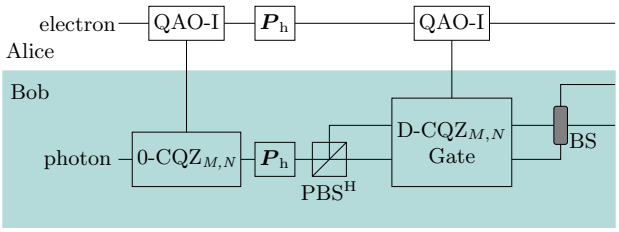


Fig. 27. Simplex D-CQZ communication for quantum information without requiring classical communication [65]. Upon completion of the protocol, Bob performs the non-demolition measurement to determine his photon path. Alice and Bob locally perform $\boldsymbol{P}_{\mathrm{h}}$ on their respective qubits, and Bob finally performs $\boldsymbol{P}_{\mathrm{x}}^{\mathsf{m}}$ on his qubit to fully recover the quantum information with the outcome m of the non-demolition measurement.

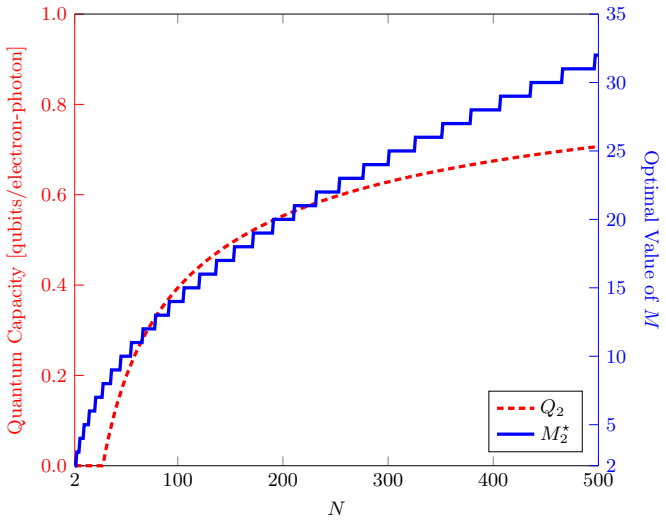


Fig. 28. Quantum capacity Q_2 [qubits/electron-photon] and optimal $M_2^\star = \arg\max_M \xi_2$ as a function of N for simplex D-CQZ communication when $|\alpha_0|^2 = |\alpha_1|^2 = 1/2$.

ensure the counterfactuality of the protocol, Alice and Bob apply a nonlocal CNOT operation using the D-CQZ gate, which evolves the initial state $|\psi_1\rangle$ to $|\psi_2\rangle$ with the probability ξ_1 where

$$\begin{aligned}|\psi_2\rangle = {} & (\alpha_0\beta_0|00\rangle_{\mathrm{AB}} + \alpha_1\beta_0|11\rangle_{\mathrm{AB}})\,|0\rangle_{\mathrm{C}} \\ & + (\alpha_0\beta_1|01\rangle_{\mathrm{AB}} + \alpha_1\beta_1|10\rangle_{\mathrm{AB}})\,|1\rangle_{\mathrm{C}}.\end{aligned} \tag{92}$$

Now, Alice and Bob apply a second CNOT operation. However, in this second nonlocal CNOT operation, the qubits A and B act as target and control qubits, respectively. Again, to ensure the counterfactuality of the protocol, Alice and Bob implement the second CNOT operation using the D-DCF gate, which transforms the state $|\psi_2\rangle$ to $|\psi_3\rangle$ with the probability $\xi_3 = f_3\left(|\alpha_0\beta_0|^2 + |\alpha_1\beta_1|^2\right)$ where

$$\begin{aligned}|\psi_3\rangle &= (\alpha_0\beta_0|00\rangle_{\mathrm{AB}} + \alpha_1\beta_0|01\rangle_{\mathrm{AB}})\,|0\rangle_{\mathrm{C}} \\ &\quad + (\alpha_0\beta_1|11\rangle_{\mathrm{AB}} + \alpha_1\beta_1|10\rangle_{\mathrm{AB}})\,|1\rangle_{\mathrm{C}} \\ &= \beta_0|00\rangle_{\mathrm{AC}}\,(\alpha_0|0\rangle_{\mathrm{B}} + \alpha_1|1\rangle_{\mathrm{B}}) \\ &\quad + \beta_1|11\rangle_{\mathrm{AC}}\,(\alpha_0|1\rangle_{\mathrm{B}} + \alpha_1|0\rangle_{\mathrm{B}})\,.\end{aligned} \tag{93}$$

To disentangle the qubit B from the qubits A and C, Bob locally performs a CNOT operation where the qubit B acts as a

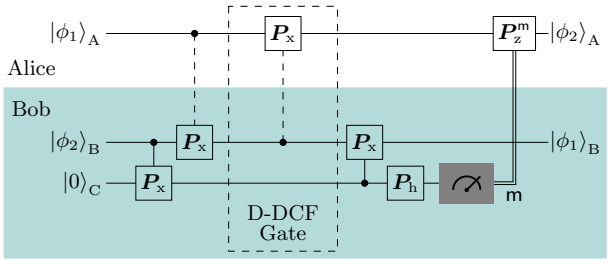


Fig. 29. Quantum telexchanging: full-duplex CQC for quantum information [65].

target and the qubit C acts as a control qubit. Upon completion of the protocol, Bob applies a Hadamard gate on the qubit C, followed by measuring his auxiliary qubit in the computational basis. As the qubit A and C have been entangled, the state of the qubit A collapses to:

$$\boldsymbol{\Xi}_{\mathrm{A}} = \frac{1}{2}\left(|\phi_2\rangle_{\mathrm{A}}\langle\phi_2| + \boldsymbol{P}_{\mathrm{z}}|\phi_2\rangle_{\mathrm{A}}\langle\phi_2|\boldsymbol{P}_{\mathrm{z}}^{\dagger}\right). \tag{94}$$

Finally, Alice performs $\boldsymbol{P}_{\mathrm{z}}^{\mathsf{m}}$ on her qubit, where m denotes the measurement outcome of Bob's auxiliary qubit C. The quantum capacity Q_3 in [qubits/electron-photon] for quantum telexchanging is

$$Q_3 = 2\max\left\{0, 2\xi_1\xi_3 - 1\right\} \tag{95}$$

tending to 2 qubits/electron-photon as $K, M, N \to \infty$. Fig. 31 illustrates the quantum capacity Q_3, $M_3^\star$, and $K_{\mathrm{q}}^\star$ as a function of N when $|\alpha_0|^2 = |\beta_0|^2 = 1/3$ where $M_3^\star$ and $K_{\mathrm{q}}^\star$ are the optimal values of M and K that maximize the capacity Q_3 or equivalently $M_3^\star = \arg\max_M \xi_1$ and $K_{\mathrm{q}}^\star = \arg\max_K \xi_3$. Note that the dependency of Q_3 on Bob's quantum information $|\phi_2\rangle_{\mathrm{B}}$ (i.e., the probability $|\beta_0|^2$) vanishes when $|\alpha_0|^2 = |\alpha_1|^2$.

2) Quantum State Exchange: Assume the initial composite state of Alice and Bob is given as $|\psi_1\rangle = |\phi_1\rangle_{\mathrm{A}}|\phi_2\rangle_{\mathrm{B}}$. To achieve full-duplex communication for quantum information, Alice and Bob perform the following steps (see Fig. 32).

1. Bob initiates the protocol by directing his photon toward the time-bin device (TBD), which generates a time-bin quantum state by encoding information into different time intervals within the photon's wave function. It transforms $|\psi_1\rangle$ to $|\psi_2\rangle$ where

$$|\psi_2\rangle = |\phi_1\rangle_{\mathrm{A}}\left(\beta_0|0\rangle_{\mathrm{B}} + \beta_1|2\rangle_{\mathrm{B}}\right) \tag{96}$$

and $|2\rangle_{\mathrm{B}} = |\mathrm{h}'\rangle$ denotes the delayed H component of the photon. Bob inputs the time-bin quantum state into the 0-CQZ$_{M,N}$ gate, which transforms $|\psi_2\rangle$ to $|\psi_3\rangle$ with the probability ξ_1 where

$$\begin{aligned}|\psi_3\rangle = {}& \alpha_0\beta_0|00\rangle_{\mathrm{AB}} + \alpha_1\beta_0|11\rangle_{\mathrm{AB}} \\ & + \alpha_0\beta_1|02\rangle_{\mathrm{AB}} + \alpha_1\beta_1|13\rangle_{\mathrm{AB}}\end{aligned} \tag{97}$$

and $|3\rangle_{\mathrm{B}} = |\mathrm{v}'\rangle$ denotes the delayed V component of the photon.

2. Alice and Bob apply their respective local operations $\boldsymbol{\mathcal{A}}_1$ and $\boldsymbol{\mathcal{B}}_1$ where

$$\boldsymbol{\mathcal{A}}_1 = |+\rangle_{\mathrm{A}}\langle 0| - |-\rangle_{\mathrm{A}}\langle 0| \tag{98}$$

$$\boldsymbol{\mathcal{B}}_1 = |0\rangle_{\mathrm{B}}\langle 0| + |1\rangle_{\mathrm{B}}\langle 1| + |2\rangle_{\mathrm{B}}\langle 3| + |3\rangle_{\mathrm{B}}\langle 2| \tag{99}$$

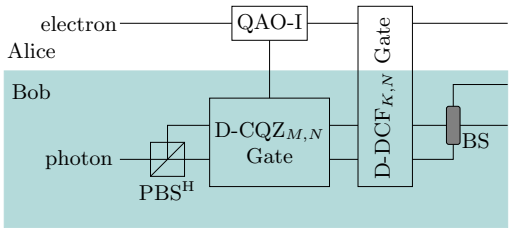


Fig. 30. CQZ-DCF quantum telexchaning for arbitrary unknown quantum states [18]. Initially, Alice and Bob possess an untangled pair $|\phi_1\rangle_{\mathrm{A}}|\phi_2\rangle_{\mathrm{B}}$ of the electron and photon. The D-CQZ$_{M,N}$ gate entangles this message pair, and the D-DCF$_{K,N}$ gate disentangles the message pair in a counterfactual manner. Finally, Bob applies the $\boldsymbol{P}_{\mathrm{x}}$ gate on the photon component in the path state $|1\rangle_{\mathrm{C}}$ and performs the non-demolition measurement on the spatial degree of freedom of the photon to complete the CQZ-DCF quantum telexchaning.

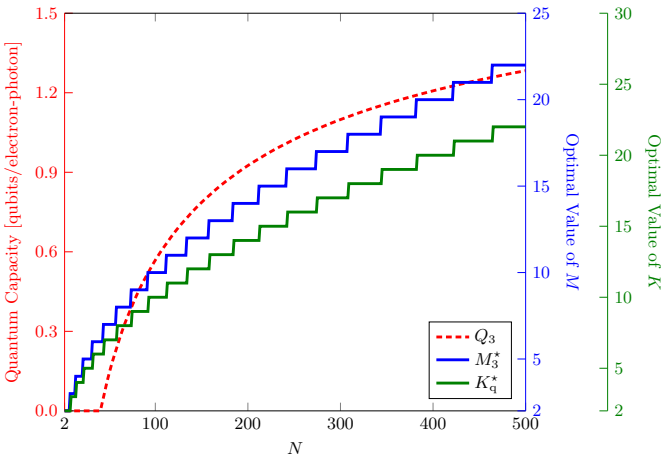


Fig. 31. Quantum capacity Q_3 , $M_3^\star$, and $K_{\mathrm{q}}^\star$ as a function of N for quantum telexchanging when $|\alpha_0|^2 = |\beta_0|^2 = 1/3$ where $M_3^\star$ and $K_{\mathrm{q}}^\star$ are the optimal values of M and K that maximize the capacity Q_3 or equivalently $M_3^\star = \arg\max_M \xi_1$ and $K_{\mathrm{q}}^\star = \arg\max_K \xi_3$.

and $|\pm\rangle_{\mathrm{A}} = \left(|0\rangle_{\mathrm{A}} \pm |1\rangle_{\mathrm{A}}\right)/\sqrt{2}$.

3. Bob applies the PBS$_1^{\mathrm{H}}$ to septate the H and V components of the photon and inputs the H polarized component of the photon to the 0-CQZ$_{2M,N}$ gate. After the CQZ gate, Bob recombines the H and V components of the photon. Due to the non-zero erasure probability of the photon in the CQZ gate, the overall action of the CQZ gate and PBSs transform $|\psi_3\rangle$ to $|\psi_4\rangle$ with the probability

$$\xi_4 = f_1^2\left(|\alpha_0\beta_0|^2 + |\alpha_1\beta_1|^2, |\alpha_0\beta_0|^2 + |\alpha_1\beta_1|^2\right) \tag{100}$$

where

$$\begin{aligned}|\psi_4\rangle = {}& |-\rangle_{\mathrm{A}}\left(\alpha_0\beta_0|0\rangle_{\mathrm{B}} - \alpha_1\beta_0|1\rangle_{\mathrm{B}}\right) \\ & + |+\rangle_{\mathrm{A}}\left(\alpha_0\beta_1|3\rangle_{\mathrm{B}} - \alpha_1\beta_1|2\rangle_{\mathrm{B}}\right).\end{aligned} \tag{101}$$

4. Alice and Bob apply their respective local operations $\boldsymbol{\mathcal{A}}_2$ and $\boldsymbol{\mathcal{B}}_2$ where

$$\boldsymbol{\mathcal{A}}_2 = |1\rangle_{\mathrm{A}}\langle +| - |0\rangle_{\mathrm{A}}\langle -| \tag{102}$$

$$\begin{aligned}\boldsymbol{\mathcal{B}}_2 = {}& \left(|+\rangle_{\mathrm{B}}\langle 0| - |-\rangle_{\mathrm{B}}\langle 1| + |+'\rangle_{\mathrm{B}}\langle 2| - |-'\rangle_{\mathrm{B}}\langle 3|\right) \\ & \left(|0\rangle_{\mathrm{B}}\langle 0| + |1\rangle_{\mathrm{B}}\langle 3| + |2\rangle_{\mathrm{B}}\langle 2| + |3\rangle_{\mathrm{B}}\langle 1|\right)\end{aligned} \tag{103}$$

and $|\pm'\rangle_{\mathrm{B}} = \left(|2\rangle_{\mathrm{B}} \pm |3\rangle_{\mathrm{B}}\right)/\sqrt{2}$.

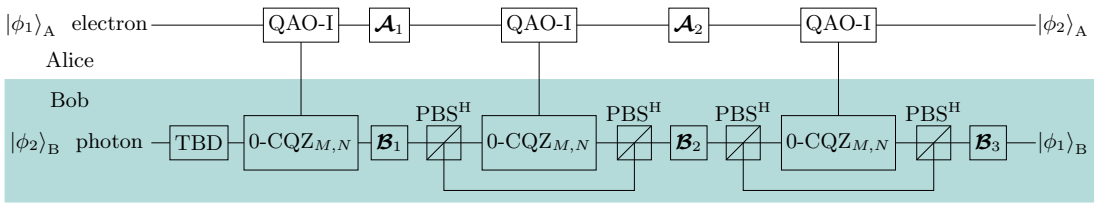


Fig. 32. Quantum state exchange: full-duplex CQC for quantum information without requiring classical communication [65].

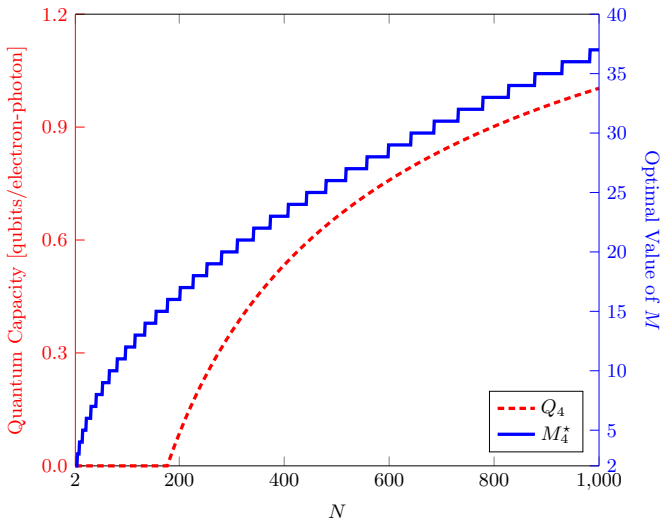


Fig. 33. Quantum capacity Q_4 and optimal $M_4^\star = \arg\max_M \xi_1\xi_4\xi_5$ as a function of N for quantum state exchange when $|\alpha_0|^2 = |\beta_0|^2 = 1/3$.

5. Alice and Bob repeat Step 3, which transforms $|\psi_4\rangle$ to $|\psi_5\rangle$ with probability

$$\xi_5 = f_1^2\left(|\beta_0|^2, |\beta_1|^2\right) \tag{104}$$

where

$$\begin{aligned}|\psi_5\rangle = |0\rangle_A\left(\alpha_0\beta_0|+\rangle_B + \alpha_1\beta_0|-'\rangle_B\right)\\ + |1\rangle_A\left(\alpha_0\beta_1|+\rangle_B + \alpha_1\beta_1|-'\rangle_B\right).\end{aligned} \tag{105}$$

In case the photon is found in the transmission channel, it causes an erasure of $|\phi_1\rangle_A$ and $|\phi_2\rangle_B$.

6. Upon completion of the protocol, Bob performs the local operation $\mathcal{B}_3$ to transform $|\psi_5\rangle$ to $|\psi_6\rangle = |\phi_2\rangle_A|\phi_1\rangle_B$ where

$$\begin{aligned}\mathcal{B}_3 = &\left(|0\rangle_B\langle 0| - |1\rangle_B\langle 3| + |2\rangle_B\langle 2| - |3\rangle_B\langle 1|\right)\\ &\left(|-\rangle_B\langle 0| + |+\rangle_B\langle 1| + |-'\rangle_B\langle 2| + |+'\rangle_B\langle 3|\right).\end{aligned} \tag{106}$$

Note that $\mathcal{B}_1, \mathcal{B}_2$, and $\mathcal{B}_3$ can be implemented using the TBD and switchable polarization rotators.

The quantum capacity Q_4 in [qubits/electron-photon] for quantum state exchange is given by

$$Q_4 = 2\max\left\{0, 2\xi_1\xi_4\xi_5 - 1\right\} \tag{107}$$

tending to 2 qubits/electron-photon as $M, N \to \infty$. Fig. 33 depicts the quantum capacity Q_4 and the optimal $M_4^\star = \arg\max_M \xi_1\xi_4\xi_5$ as a function of N when $|\alpha_0|^2 = |\beta_0|^2 = 1/3$. Note that the quantum state exchange of quantum information requires no classical announcement for full-duplex CQC with a sacrifice of the quantum capacity of the protocol in comparison with the quantum telexchanging protocol (see Fig. 31).

Table IV summarizes the functionalities, characteristics, and trade-offs of the CQC protocols discussed in this section, providing a systematic evaluation of their feasibility in practical applications. While there is a trade-off between ultra-security and execution time, these protocols collectively establish a framework for ultra-secure quantum communication, marking a significant step toward future quantum networks where communication security is guaranteed by particle-free communication.

VI. Counterfactual Quantum Cryptography

In this section, counterfactual quantum cryptography is explored to achieve secure communication without the transmission of physical particles. We will explore the foundational protocols such as counterfactual QKD variants, including bipartite QKD (BQKD), extended tripartite QKD (TQKD), and device-independent BQKD. Furthermore, we examine QSDC and quantum secure dialogue (QSD) protocols, which enable secure information exchange based on counterfactual entanglement. A comparative overview of conventional and counterfactual quantum cryptography protocols is provided in Table V, highlighting their tradeoffs in terms of functionalities, strengths, and weaknesses. Finally, we discuss potential security threats and countermeasures to ensure the robustness of CQC.

A. Counterfactual QKD

QKD protocols enable the distribution of a secret key between two or more parties [27], [28], [164]–[166]. In contrast to public key distributions, the QKD protocols achieve unconditional security using principles from quantum mechanics, including the no-cloning theorem and entanglement [69], [167]. Counterfactual quantum cryptography was first introduced in BQKD [59]. The basic idea of the BQKD originated from the EV-IFM, and later, the counterfactual QKD has been extended to TQKD by integrating the EV-IFM and the 0-CQZ$_{M,N}$ gate [168].

1) Counterfactual BQKD: The BQKD protocol is widely known as the Noh 2009 (N09) protocol, which was proposed in [59]. In the N09 protocol, Bob equips a single-photon source that randomly generates either an H- or V-polarized photon and a BS$^{(\pi/4)}$ that generates the equal superposition of the

TABLE IV
CQC PROTOCOLS: FUNCTIONALITY, CHARACTERISTICS, AND TRADE-OFFS

Protocol	Information	Functionality	Characteristics	Strength	Weakness
Simplex QZ Communication	Classical	Particle-free communication in one direction using QZ gate where Alice holds an AO and Bob prepares a photon.	Binary Z-channel	Shorter execution time as it depends only on N inner cycles.	Semi-counterfactual
	Quantum	Particle-free quantum information transfer in one direction using CQZ gate where Alice holds a QAO and Bob prepares a photon.	Simplex quantum erasure channel	No pre-shared entanglement is required.	Requires one-bit classical announcement to fully recover counterfactually transmitted quantum state.
Simplex CQZ Communication	Classical	Particle-free communication in one direction using CQZ gate where Alice holds an AO and Bob prepares a photon.	Assymetric binary erasure channel	Full-counterfactual	Longer execution time as it depends on both N inner and M outer cycles.
	Quantum	Particle-free quantum information transfer in one direction using CQZ and D-CQZ gates where Alice holds a QAO and Bob prepares a photon.	N/A	No classical announcement is required.	Longer execution time as it utilizes two counterfactual gates.
Quantum Duplex Coding	Classical	Particle-free simultaneous exchange of information using DCF gate where Alice's QAO and Bob's photon are entangled.	Full-duplex binary erasure channel	Maximizes channel capacity via entanglement-enhanced qubit efficiency.	Requires preshared entanglement and longer execution time as it depends on N inner cycles and K MQZ gates.
Quantum Telexchanging	Quantum	Particle-free simultaneous exchange of information using D-CQZ and D-DCF gates where Alice holds a QAO and Bob prepares a photon in superposition.	N/A	Maximizes quantum capacity without pre-shared entanglement.	Requires one-bit classical announcement and longer execution time as it utilizes two counterfactual gates.
Quantum State Exchange	Quantum	Particle-free simultaneous exchange of information using 3 CQZ gates and local operations where Alice holds a QAO and Bob prepares a photon in superposition.	N/A	No classical announcement is required.	Less quantum capacity compared to quantum telexchanging.

photon in two paths $|0\rangle$ and $|1\rangle$. The path component $|1\rangle$ of the photon enters the quantum channel that connects Bob with Alice where PBS^{H} gives the delay of time Δt to the V-polarized photon by using an optical loop (OL) such that H- and V-polarized photons reach at a switch (SW) at time t_0 and t_1, respectively, as illustrated in Fig. 34. Alice uses the different switching times t_0 and t_1 to direct the H- and V-polarized photons in the path state $|1\rangle$ either to the detector D_4 to block the path of the photon ($\mathsf{x} = 1$) or to the MR_2 to allow the photon to pass ($\mathsf{x} = 0$). Suppose that Alice and Bob prepare random bit sequences $\mathbf{a} = \{\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_T\}$ and $\mathbf{b} = \{\mathsf{b}_1, \mathsf{b}_2, \ldots, \mathsf{b}_T\}$, respectively. Alice and Bob encode these bits as switching time t_{a_k} and polarization of the photon $|\mathsf{b}_k\rangle_{\text{B}}$, respectively, where $k = \{1, 2, \ldots, T\}$. In each round of the N09 protocol, say, the kth round, there are two possibilities.

- $\mathsf{a}_k \neq \mathsf{b}_k$: In this case, Alice allows the photon to pass, and the reflected component of the photon in the path state $|1\rangle$ recombines with the photon component in the path state $|0\rangle$ at the BS. The N09 protocol works similarly as $\mathsf{x} = 0$ for the EV-IFM and the detector D_{b_k} clicks with certainty. Bob publicly announces the measurement result and the initially prepared polarization of the photon to detect the presence of an eavesdropper (Eve) in the quantum channel.
- $\mathsf{a}_k = \mathsf{b}_k$: In this case, Alice blocks the path of the photon, and the interference of the photon is destroyed due to the blockage of Alice. The N09 protocol works similarly as $\mathsf{x} = 1$ for the EV-IFM and the detectors D_4, D_{b_k}, and $\text{D}_{\mathsf{b}_k+2}$ click with probabilities $1/2$, $1/4$, and $1/4$, respectively. The secret key is generated only if the detector $\text{D}_{\mathsf{b}_k+2}$ clicks. The rest of the cases are to detect the presence of an eavesdropper (Eve) in the quantum channel. Note that the detector $\text{D}_{\mathsf{b}_k+2}$ clicks only if no physical particle is found in the quantum channel.

As no physical particle is found in the transmission channel at the time of successful key generation and Eve has access to a subsystem only (the photon component in the path state $|1\rangle$), it enhances the security of the protocol against conventional quantum attacks such as the photon-number splitting attack. Note that $\mathsf{a}_k \neq \mathsf{b}_k$ and $\mathsf{a}_k = \mathsf{b}_k$ are equiprobable events, which lead to $\gamma \to 1/8$ as $T \to \infty$, where γ denotes a key generation rate. Later, the key generation rate has been improved to $1/2$ under the asymptotic limits by using a series of N unbalanced BSs in the path state $|1\rangle$ [115]. The idea of counterfactual BQKD has been experimentally demonstrated by using the

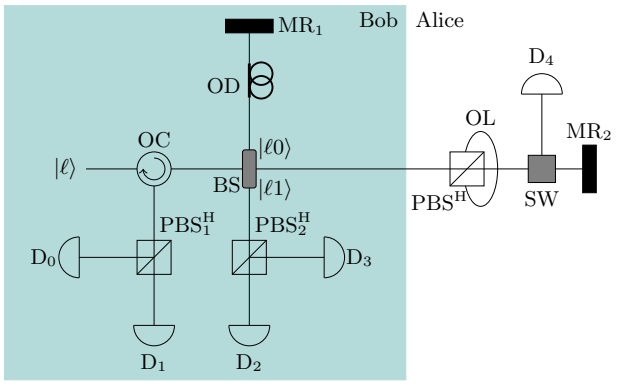


Fig. 34. Counterfactual BQKD based on EV-IFM. Here, SW and OL stand for a switch and an optical loop, respectively [59].

weak coherent states [114], [116], [127] and extended to the private database queries [169].

2) Counterfactual TQKD: After the invention of CQZ gates to transfer classical information in uni-direction with certainty under the asymptotic limits, the N09 setup has been extended to the counterfactual TQKD protocol by using the CQZ gates in the path states $|0\rangle$ and $|1\rangle$ to generate secret keys [168]. Suppose that Alice and Charlie prepare random bit sequences $\mathbf{a} = \{\mathsf{a}_1, \mathsf{a}_2, \ldots, \mathsf{a}_T\}$ and $\mathbf{c} = \{\mathsf{c}_1, \mathsf{c}_2, \ldots, \mathsf{c}_T\}$, respectively. Alice and Charlie encode these bits as $|\mathsf{a}_k\rangle_{\rm AO}$ and $|\bar{\mathsf{c}}_k\rangle_{\rm AO}$, respectively. In each round of the protocol, Bob prepares the H-polarized photon and directs it towards $\mathrm{BS}^{(\pi/4)}$ to create the equal superposition of the photon in each path. Bob applies the H-CQZ$_{M,N}$ gates in each path of the photon, which leads to the two possibilities in each round of the protocol, say, the kth round.

- $\mathsf{a}_k \neq \mathsf{c}_k$: In this case, the components of the photon in both arms of the $\mathrm{BS}^{\pi/4}$ are identically polarized and D_0 clicks with certainty unless the photon is discarded in the H-CQZ$_{M,N}$ gates with the probability.
- $\mathsf{a}_k = \mathsf{c}_k$: In this case, the components of the photon in both arms of the $\mathrm{BS}^{\pi/4}$ are oppositely polarized and the detectors D_0 and D_1 click with the probability $1/2$ unless the photon is discarded in the H-CQZ$_{M,N}$ gates with the probability $\xi_6 = (\zeta_0 + \zeta_1)/4$.

At the end of each round of the protocol, Bob publicly announces the measurement results. As D_1 clicks if $\mathsf{a}_k = \mathsf{c}_k$, this click results in a secret key generation. In case D_0 clicks, Alice and Charlie can use this outcome to detect the presence of an eavesdropper in the channel. Note that $\mathsf{a}_k \neq \mathsf{c}_k$ and $\mathsf{a}_k = \mathsf{c}_k$ are equiprobable events, the key generation rate approaches $\gamma \to 1/4$ under the asymptotic limits of M and N.

3) Device-Independent Counterfactual BQKD: Counterfactual BQKD requires Alice and Bob to announce "which detector clicked" during the key generation process, introducing a critical security loophole. An eavesdropper (Eve) can exploit this by performing a side-channel attack, where a malicious detector encodes Bob's bit information into the timing intervals between detection events. When Bob announces the detection results, Eve decodes the key by analyzing these timing patterns, effectively extracting secret information without being detected. To address this, a device-independent counterfactual BQKD protocol was proposed, where only Bob's state preparation and BS are trusted, while detectors on both sides may be untrusted [170]. In this modified counterfactual BQKD, a phase modulator (PM) is added at path $|0\rangle$ after the $\mathrm{BS}^{(\pi/4)}$, allowing Bob to apply either a π-phase shift or no phase on the photon component. The device-independent counterfactual BQKD protocol follows the same procedure as the original counterfactual BQKD protocol. Specifically, for each round $k \in \{1, 2, \ldots, T\}$ of the protocol:

- $\mathsf{a}_k \neq \mathsf{b}_k$: The photon component in path $|1\rangle$ is reflected from Bob's MR_2 and interferes with phase-controlled component in path $|0\rangle$. If π-phase is applied, detector $\mathrm{D}_{\mathsf{b}_{k+2}}$ clicks with certainty; other wise, $\mathrm{D}_{\mathsf{b}_k}$ clicks.
- $\mathsf{a}_k = \mathsf{b}_k$: The photon component in path $|1\rangle$ is absorbed by D_4, and no interference occurs. The photon component in path $|0\rangle$ passes through $\mathrm{BS}^{(\pi/4)}$ again, triggering either $\mathrm{D}_{\mathsf{b}_k}$ or $\mathrm{D}_{\mathsf{b}_{k+2}}$ with equal probability. A conclusive key bit is obtained only when Bob's phase choice aligns with the detector that clicks: π for $\mathrm{D}_{\mathsf{b}_k}$, or 0 for $\mathrm{D}_{\mathsf{b}_{k+2}}$.

As a result, detector click disclosure is no longer necessary for secure key extraction, mitigating a major side-channel vulnerability.

B. Counterfactual Quantum Dialogues

The only classical way to ensure information-theoretic security is to encrypt a secret message by using a private key before transmission of the message. In a classical cryptographic system, its security relies on the assumed hardness of computational problems such as factoring. In contrast to classical cryptography, quantum mechanics provides physical ways of secure communication such as QKD, which enable legitimate parties to establish private keys securely, QSDC and QSD, which allow two legitimate parties to transfer a secret classical message with guaranteed information-theoretic security without establishing a private key [29], [31], [171]–[174]. QSDC protocols enable a sender, say, Bob, to transfer a secret classical message to a receiver, say, Alice, securely—i.e., *simplex secure communication*—whereas the QSD protocols allow each legitimate party to send and receive secret classical messages securely and simultaneously—i.e., *full-duplex secure communication*. The unconditional security of the QSDC and QSD protocols relies on the fundamental laws of quantum mechanics, such as entanglement, the no-cloning theorem, and non-locality. Recently, the idea of CQC has been extended to the QSDC and QSD protocols, where the unconditional security relies on the secure counterfactual entanglement swapping by using the counterfactual swap (C-Swap) gate [175]. As the counterfactual QSDC and QSD tasks are achieved without the transmission of any physical particle over the channel, the protocols give the security advantage against conventional eavesdropping attacks, e.g., the man-in-the-middle (MITM) attack [139].

1) Counterfactual QSDC: The goal of the counterfactual QSDC protocols is to achieve information-theoretic security without establishing a secret key and without the transmission of any physical particle over the channel. The basic idea of

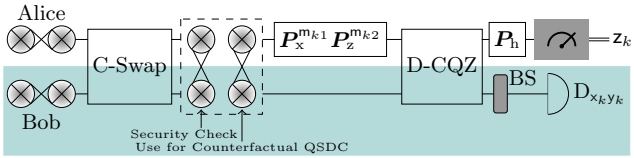


Fig. 35. Counterfactual QSDC. The protocol starts by directing one qubit of each locally entangled pair to the C-Swap gate, which transforms the initial state to two maximally entangled pairs between Alice and Bob. Alice and Bob use one entangled pair for a security check and the remaining entangled pair to transfer two-bit classical information under unconditional security [139].

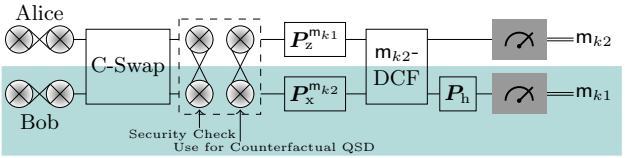


Fig. 36. Counterfactual QSD. Similar to counterfactual QSDC, the protocol starts by directing one qubit of each locally entangled pair to the C-Swap gate, which transforms the initial state to two maximally entangled pairs between Alice and Bob. Alice and Bob use one entangled pair for a security check and the remaining entangled pair to simultaneously transfer one-bit classical information in each direction under unconditional security [139].

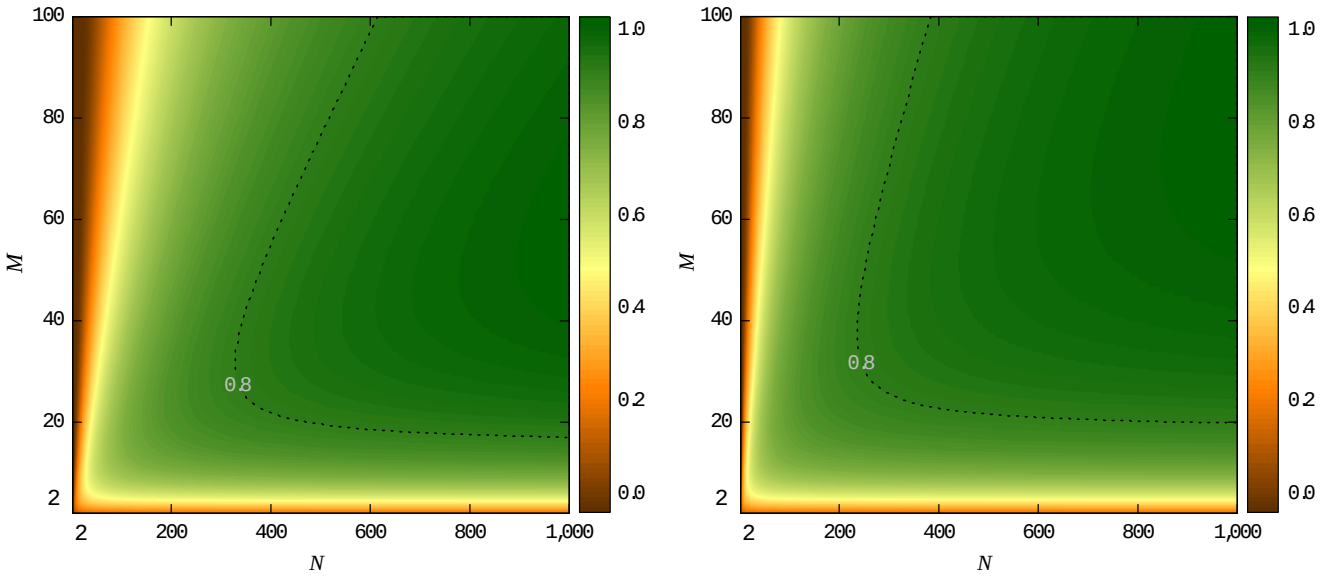
the counterfactual QSDC originated from the two-step QSDC protocol [30]. In counterfactual QSDC protocols, Alice and Bob take the following steps to ascertain the unconditional security of the transmitted secret messages (see Fig. 35).

1. Alice and Bob locally prepare T entangled pairs $|\psi_{00}\rangle_{\mathrm{A}_{k1}\mathrm{A}_{k2}}$ and $|\psi_{00}\rangle_{\mathrm{B}_{k1}\mathrm{B}_{k2}}$, respectively, where $k = \{1, 2, \ldots, T\}$. Alice and Bob perform T rounds of the C-Swap gate. In the kth round of the C-Swap gate, Alice and Bob input A_{k2} and B_{k1} to the C-Swap gate, respectively, and generate two entangled pairs $|\psi_{00}\rangle_{\mathrm{A}_{k\ell}\mathrm{B}_{k\ell}}$ in each round of the counterfactual entanglement swapping where $\ell = 1, 2$.
2. From each round of the C-Swap gate, Alice randomly chooses ℓ_k and measures her qubit $\mathrm{A}_{k\ell_k}$ in a randomly chosen basis $\boldsymbol{M}_k \in \{\boldsymbol{P}_{\mathrm{x}}, \boldsymbol{P}_{\mathrm{z}}\}$. For T uses of the C-Swap gate, Alice prepares a selected entangled-pair position sequence $\boldsymbol{\ell} = \{\ell_1, \ell_2, \ldots, \ell_T\}$, a randomly chosen measurement basis sequence $\boldsymbol{\mathcal{M}} = \{\boldsymbol{M}_1, \boldsymbol{M}_2, \ldots, \boldsymbol{M}_T\}$, and a measurement outcome sequence $\mathbf{b} = \{\mathsf{b}_1, \mathsf{b}_2, \ldots, \mathsf{b}_T\}$, where $\mathsf{b}_k \in \{0, 1\}$. Alice publicly announces these sequences. Bob measures his qubits $\mathrm{B}_{k\ell_k}$ and compares his results with Alice's measurement outcomes b_k.
3. After ensuring the security of the generated entangled pairs, Alice uses the remaining entangled pairs to encode a two-bit secret message $\mathsf{m}_{k1}\mathsf{m}_{k2}$ in each entangled pair as follows:
$$|\psi_0\rangle = (\boldsymbol{P}_{\mathrm{x}}^{\mathsf{m}_{k1}} \boldsymbol{P}_{\mathrm{z}}^{\mathsf{m}_{k2}} \otimes \boldsymbol{I}) |\psi_{00}\rangle_{\mathrm{A}_k\mathrm{B}_k}. \tag{108}$$
Note that, for simplicity, we denote the remaining entangled pairs as $|\psi_{00}\rangle_{\mathrm{A}_k\mathrm{B}_k}$.
4. To transfer the secret message without the transmission of any physical particle through the channel, Alice and Bob apply the D-CQZ$_{M,N}$ gate, as illustrated in Fig. 35, and the encoded state $|\psi_0\rangle$ transforms to $|\psi_1\rangle$ where
$$|\psi_1\rangle = \begin{cases} |\psi_{x0}\rangle \to \dfrac{1}{\sqrt{2}} \left(|00\rangle_{\mathrm{A}_k\mathrm{C}_k} \right. \\ \qquad \left. + (-1)^x |11\rangle_{\mathrm{A}_k\mathrm{C}_k}\right) |0\rangle_{\mathrm{B}_k}, \\ |\psi_{x1}\rangle \to \dfrac{1}{\sqrt{2}} \left(|10\rangle_{\mathrm{A}_k\mathrm{C}_k} \right. \\ \qquad \left. + (-1)^x |01\rangle_{\mathrm{A}_k\mathrm{C}_k}\right) |1\rangle_{\mathrm{B}_k} \end{cases} \tag{109}$$
where C_k denotes the path information of the photon.
5. For each Bell-pair, Bob applies BS$^{(\pi/4)}$ on his photon and measures the path and polarization degrees of freedom of the photon by detecting it at the detector $\mathrm{D}_{\mathsf{x}_k\mathsf{y}_k}$, where $\mathsf{x}_k, \mathsf{y}_k \in \{0, 1\}$. Alice applies a Hadamard gate $\boldsymbol{P}_{\mathrm{h}}$ to her qubit and measures in the computational basis. Now, Alice publicly announces her measurement result $\mathsf{z}_k \in \{0, 1\}$, enabling Bob to fully recover the secret bit string. Bob decodes the two-bit classical message $\hat{\mathsf{m}}_{k1}\hat{\mathsf{m}}_{k2}$, where $\hat{\mathsf{m}}_{k1} = \mathsf{x}_k$ and $\hat{\mathsf{m}}_{k2} = \mathsf{y}_k + \mathsf{z}_k$. As z_k is uniformly distributed for each Bell pair, an eavesdropper is unable to decode the secret message even if they listen to the classical announcement z_k [129], [176], [177].

To ascertain the security of the transmitted message and measure the bit error rate, Alice encodes random bits (not the secret message) in randomly chosen pairs at Step 3 and reveals the position of the selected pairs and encoded random bits. Under ideal conditions, the success probability of counterfactual QSDC is $\xi_7 = f_1\left(1/2, 1/2\right)^2 f_3\left(1/2\right)$. In Fig. 37(a), we analyze the asymptotic behavior of ξ_7 as a function of M, N. The results indicate that ξ_7 approaches unity as $M, N \to \infty$, signifying that the counterfactual success probability converges to 1. This ensures near-perfect secure transmission, achieved without the direct physical transmission of particles through the communication channel.

2) Counterfactual QSD: Similar to QSDC, the goal of QSD is to exchange secret messages simultaneously with unconditional security and without establishing a secret key. Recently, the idea of QSD has been implemented using CQC. To explain the counterfactual QSD protocol, suppose that Alice and Bob have K_{A} and K_{B} bits of secret messages that Alice and Bob want to send each other, respectively. They take the following steps to transmit the secret information without establishing a secret key (see Fig. 36).

1. Alice and Bob locally prepare T entangled pairs and take Steps 1 and 2 of the counterfactual QSDC protocol to securely distribute the entangled pairs where
$$T = \min\left\{T_{\mathrm{A}}, T_{\mathrm{B}}\right\} + \left\lceil \frac{|T_{\mathrm{A}} - T_{\mathrm{B}}|}{2} \right\rceil + \tilde{T}. \tag{110}$$
Here, $\lceil x \rceil$ represents the smallest integer greater than or equal to a real number x; T_{A} and T_{B} denote the lengths of the bit strings Alice and Bob want to transmit to Bob and Alice, respectively; and $\tilde{T}$ denotes the number of entangled pairs to measure the bit error rate in the counterfactual QSD protocol.
2. After ensuring the security of the generated entangled pairs, Alice and Bob undergo the steps in quantum duplex



(a) Counterfactual QSDC (b) Counterfactual QSD

Fig. 37. The success probabilities, ξ_7 and ξ_8, for counterfactual QSDC and counterfactual QSD protocols, respectively, are evaluated at $N = 1000$ and $M = K = 100$. It is observed that for both protocols, the success probabilities increase as N and $M(K)$ increase.

coding for $\min\{T_{\rm A}, T_{\rm B}\}$ entangled pairs to exchange classical information. To ensure the security of the transmitted messages, Alice and Bob encode random bits (not secret messages) in randomly chosen $\tilde{T}$ pairs and reveal the position of the selected pairs and encoded random bits to detect the presence of an eavesdropper in the quantum channel and measure the bit error rate.

3. Alice and Bob take Steps 3–5 of the counterfactual QSDC protocol for the remaining entangled pairs if $T_{\rm A} > T_{\rm B}$. In case $T_{\rm A} \leq T_{\rm B}$, Bob acts as a sender and encodes two bits of classical information in each remaining entangled pair. In this case, Alice equips the D-CQZ$_{M,N}$ gate and Bob encodes his qubit in a QAO.

In this protocol, the success probability is by $\xi_8 = f_1\left(1/2, 1/2\right) f_3\left(1/2\right)^2$. Fig. 37(b) illustrates the asymptotic behavior of ξ_8 as a function of M, N. To simplify the analysis, we assume that the number of MQZ gates used in m$_{k_2}$-DCF gate matches the number of outer cycles, i.e $M = K$. The results demonstrate that as $M, N \to \infty$, the success probability ξ_8 asymptotically approaches unity, ensuring ultra secure dialogues, with the non-transmission of physical information-carrying particles.

C. Counterfactual Attacks

1) Counterfactual Trojan Horse Attacks: Traditional Trojan Horse (TH) attacks, such as invisible-photon TH attacks and delay-photon TH attacks, involve sending an auxiliary photon to the apparatus of a communicating party (say, Alice) and extracting valuable information from the reflected auxiliary photon. When it comes to the CQC setting, this auxiliary photon can cause abnormal detector clicks or be discarded when it appears in the communication channel, thereby exposing the presence of an eavesdropper (say, Eve). To tackle this situation, a counterfactual TH (CTH) attack was proposed in [43]. In the CTH attack, a CQZ gate is implemented at Eve's site, reducing the probability of the auxiliary photon appearing in the channel to almost zero, effectively making it invisible. This counterfactual setting can take either a single-cycle or double-cycle form. Here, the rotation angle of PR$_M$ used in Eve's CQZ gate is denoted by $\theta_M = \frac{\pi}{4M}$.

- *Single-Cycle CTH Attacks:* Eve implements a QZ gate with M' cycles and sends her auxiliary photon to Alice through the QZ gate. In the case of no blocking, the photon component is reflected back to Eve, triggering a detector click with probability one. On the other hand, if Alice blocks the incoming photon component, it gets absorbed by Alice's apparatus. However, if no photon is lost to Alice, even if she measures it, the probability that Eve's photon remains at his site is $\lambda_1 = 1 - \cos^{2M'} \frac{\pi}{2M'}$, indicated by another detector click. As $M' \to \infty$, the probability that Alice detects Eve's photon approaches zero.
- *Double-Cycle CTH Attacks:* In this case, Eve uses the CQZ gate with N' inner and M' outer cycles. Following the execution of the CQZ operation, the probabilities of Alice detecting Eve's photon in the blocking or unblocking cases are $1 - \zeta_0$ and $1 - \zeta_1$, respectively. As N' and M' increase, the chance that Alice discovers Eve's photon diminishes significantly. Compared to the single-cycle CTH attack, the double-cycle CTH attack requires more cycles, making it more time-intensive. Nevertheless, it has a smaller chance of being detected by Alice.

However, specific conditions are required for a CTH attack to succeed. Firstly, Eve needs to execute her attack within the time frame before the access window of Alice's detector expires. Secondly, Eve's photon must undergo multiple manipulations to obtain information about Bob's apparatus

TABLE V
COMPARISON OF CONVENTIONAL AND COUNTERFACTUAL CRYPTOGRAPHY

Protocol	Type	Functionality	Strength	Weakness
QKD	Conventional	Distribution of a secret key between two or more parties	Higher key generation rate	Vulnerable to side-channel and counterfactual attacks
	Counterfactual	Particle-free distribution of a secret key between two or more parties	Potentially higher resistance to eavesdropping	Sensitive to channel noise and error due to interference-based setup
QSDC	Conventional	Simplex secure communication without establishing a private key	Direct and fast communication	Vulnerable to undetected leakage via side-channel or counterfactual attacks
	Counterfactual	Particle-free simplex secure communication without establishing a private key	More robust against security threats as well as dephasing noise	Low efficiency (due to probabilistic success and photon discards) and high hardware complexity
QSD	Conventional	Duplex secure communication without establishing a private key	High-speed secure dialogue with moderate security	Vulnerable to undetected leakage via side-channel or counterfactual attacks
	Counterfactual	Particle-free duplex secure communication without establishing a private key	Ultra-secure dialogue where message interception is off-limits	Low efficiency (due to probabilistic success and photon discards) and high hardware complexity

and estimate Alice's manipulation. Thirdly, Alice's setup must remain constant throughout these manipulations. Thus, Alice can improve the probability of detecting Eve's photon by adopting infrequent measurements (i.e., random blocking or unblocking of the transmission channel), as opposed to a constant approach, or varying the frequency or time window of the detector.

2) Detector Blinding Attacks: The most commonly used photon detectors in quantum communication are avalanche photodiodes (APDs), which are operated in the Geiger mode when a single-photon detection occurs. After a detection event, it needs some time to recover before detecting another photon. This detector blinding attack makes use of this transition time by sending a bright light to the detector and changes the APD mode from the Geiger mode to a linear mode, where the single-photon detection events are not registered. Then, Eve can manipulate the actions of Alice's QAO through her blinded quantum states without raising any alarm from Alice's detector. This attack can be counteracted through active monitoring of Alice's detector [178].

3) Intercept-and-Resend Attacks: The intercept-and-resend attack involves intercepting the photon component in the channel, measuring it in a random basis, and transmitting the resulting state to Alice. In counterfactual communication, it is obvious that the photon that passes through the communication channel is an ℓ-polarized photon for the ℓ-CQZ gate. This channel state information does not carry any meaningful information, and hence, Eve cannot extract any useful information from the interception. Since the wave function of the incoming photon has already been measured by Eve during the attack, it will lead to false detector clicks at Alice's side [118]. By employing proper detection techniques, Alice and Bob can reveal the presence of Eve in the channel.

4) Man-in-the-Middle Attacks: In this attack, Eve deceives by taking on the roles of both Alice and Bob. In the forward path, Eve impersonates Alice and manipulates the incoming photons of Bob using her own QAO [179]. Meanwhile, she transmits her photon to Alice to steal useful information about the communication in the return path. In the case of classical or quantum information transmission through the CQZ gate, Eve remains undetectable to Alice and Bob. Nevertheless, Bob can utilize decoy photons, or Alice can randomly change the frequency or time window of her detector to unveil Eve's existence within the channel.

5) Entangle-and-Measure Attacks: Using the CNOT gate, Eve can entangle her qubit with Bob's qubit and measure it to observe Alice's manipulation of her QAO. When Bob receives the final quantum state sent by Alice, the density matrix of that state will differ from that of the actual quantum state sent by Alice. Due to the presence of Eve, when Eve's system is traced out from the system, the resulting density matrix for the remaining subsystem may not represent a pure state. Additionally, the measurement by Eve can also alter the state being transmitted. Thus, Alice and Bob can identify the presence of Eve if they check the security of the channel through the use of decoy photons [57].

D. Security Analysis

1) Security of Counterfactual QKD: The security of counterfactual BQKD is demonstrated against a general intercept-and-resend attack in [118]. If one or more detectors trigger clicks at the end of the key distribution, it is certain that an eavesdropper is launching an attack in the channel. As described in Section VI-A, there are two possible scenarios for counterfactual QKD—Alice and Bob's chosen random bits (i.e., polarization) are the same ($\mathsf{a}_k = \mathsf{b}_k$) and they are different ($\mathsf{a}_k \neq \mathsf{b}_k$). The subsequent lists explain which detector triggers a click for those scenarios when Eve launches the intercept-and-resend attack.

- $\mathsf{a}_k \neq \mathsf{b}_k$: In this case, the detector $\mathrm{D}_{\mathsf{b}_k}$ is supposed to click in the absence of Eve. When Eve launches the attack, two or more detectors, including the detector $\mathrm{D}_{\mathsf{b}_k}$, may trigger clicks, but no information is lost to Eve.

- $\mathsf{a}_k = \mathsf{b}_k$: In the absence of Eve, there are three events that each detector triggers a click: (E1) D_4 is supposed to click with the probability $1/4$; (E2) $\mathrm{D}_{\mathsf{b}_k}$ is supposed to click with the probability $1/2$; and (E3) $\mathrm{D}_{\mathsf{b}_k+2}$ is supposed to click with the probability $1/4$. However, Eve's attack leads to the simultaneous clicks of the detectors—D_4 and other detector trigger clicks for (E1); all three detectors may trigger clicks for (E2) and $\mathrm{D}_{\mathsf{b}_k+2}$ and other detector trigger clicks for (E3). For (E1) and (E3), it is not possible for Eve to get any information about the key, but it is possible for (E2). In (E2), Eve can take advantage of the non-vacuum state in path 1 to probe Alice's polarization choices. The key rate of counterfactual QKD is bounded by the probabilities of the events (E1), (E2), and (E3), and the error rates in the events (E1) and (E3). Hence, a positive key rate can be achieved as long as the error rates in the events (E1) and (E3) remain sufficiently low [118], [179], [180]. Through the use of 2 polarization rotators (PRs), Eve has to make sure to reproduce the statistics at Alice an Bob if no light is coming back.

In 2016, two variants of Trojan Horse (TH) attack were investigated against counterfactual BQKD by adding either a delayed photon or an invisible photon [136]. In the delayed-photon-based TH attack, Eve injects a probe photon into the system with a delay time, making it invisible to Alice's detection system. Depending on whether the photon is reflected (indicating different bit values) or blocked (indicating equal bit values), Eve can infer the key bit without introducing detectable disturbances. Since Alice and Bob announce detector click information, Eve extracts the secret key upon observation of detector $\mathrm{D}_{\mathsf{b}_k+2}$ clicks. In a similar manner, the invisible photon-based TH attack uses photon wavelengths outside Alice's detector sensitivity. These attacks exploit practical imperfections like timing and spectral vulnerabilities, bypassing the theoretical security of N09. To mitigate such threats, Alice can employ switchable polarization rotator (SPR) to randomly flip the polarization state before the polarization switch, with key bits postselected for $\mathrm{D}_{\mathsf{b}_k+2}$ detection event. Additionally, proper designation of the system with spatial, temporal, and spectral filters is required to suppress side-channel leakage.

Later, another attack, known as the detector blinding attack described in Section VI-C2, was launched in 2021 [178], by exploiting the vulnerabilities, namely, APDs, which can be forced into a non-sensitive linear mode using bright light, effectively blinding them. Practical implementation of counterfactual BQKD often relies on assumptions such as weak coherent states, binary imperfect detectors, lossy channels, and malicious detectors. Two strategies—blind-and-reduce-loss attacks and blinding-measurement-and-faked-state attacks—were introduced to perform a detector blinding attack.

- *Blind-and-Reduce-Loss Attacks:* In this attack, Eve randomly selects a polarization and injects a bright blinding pulse into a PBS, which transmits the blinding pulse toward Alice and diverts Bob's orthogonal polarization component into a delay line. If the pulse is reflected back, Eve infers a polarization mismatch with Bob; if not, a match is assumed, and she suppresses Alice's stored photon via high attenuation to emulate expected protocol behavior. To maintain the expected detection statistics and remain undetected, she replaces the original channel with a lower-loss link and adds attenuation to compensate for the resulting 6 dB round-trip reduction. The approach, though theoretically effective, is technologically intensive due to its stringent requirements on polarization control, loss engineering, and precise timing synchronization.
- *Blinding-Measurement-and-Faked-State Attacks:* This attack targets counterfactual BQKD systems that utilize weak coherent states. In this scenario, Eve exploits the multi-photon nature of coherent states to extract Bob's polarization by measuring one or more photons along path $|1\rangle$. Based on the outcome, she transmits a bright pulse to manipulate or blind Alice's detector. After monitoring Alice's detector response, she injects fake quantum states into the channel that statistically mimic a legitimate, attack-free protocol. If her measurement yields a vacuum state, she still transmits a fake state to Alice with a certain probability to infer Alice's bit choice. To avoid detection, Eve finely tunes both the amplitude of the fake states and compensates for channel losses to replicate expected detection statistics, thus gaining full or partial information about the key bits. Mitigating these attacks requires active countermeasures: watchdog detectors to detect anomalously bright pulses, dynamically varying the BS's transmitivity (instead of a fixed 50:50 ratio), and introducing randomness via intensity modulation or variable detector efficiencies. Further protection can be achieved through advanced receiver configurations and by incorporating hardware imperfections into the formal security proofs. Overall, while counterfactual BQKD has inherent security advantages, these attacks reveal that active countermeasures are essential to ensure its robustness in practical implementations.

2) Security of Counterfactual Communication: In contrast to counterfactual QKD, direct counterfactual communication lacks security against potential eavesdropping. In direct communication, Alice determines the bit that Bob transmits by assessing the final polarization of her output photon. It is undeniable that counterfactual communication offers enhanced security compared to conventional quantum communication due to the absence of information-carrying particles in the communication channel. As a result, attacks that rely on signals within the transmission channel become ineffective in the context of CQC. Nevertheless, if the devices owned by Alice and Bob are imperfect and Eve exploits these imperfections, vulnerabilities arise. For instance, Eve might replace Bob's channel with a mechanism to tap into Alice's imperfect detector, thereby gaining access to Alice's transmitted information. Additionally, Eve could intercept and detect the particle reflected back from Alice when she transmits a bit 0. This interception by Eve disrupts the interference pattern of the photon's wave function, causing Bob to detect a bit 1 instead of the intended bit 0. Consequently, direct CQC is susceptible to active counterfactual attacks. To counteract these vulnerabilities, strategies such as employing decoy photons

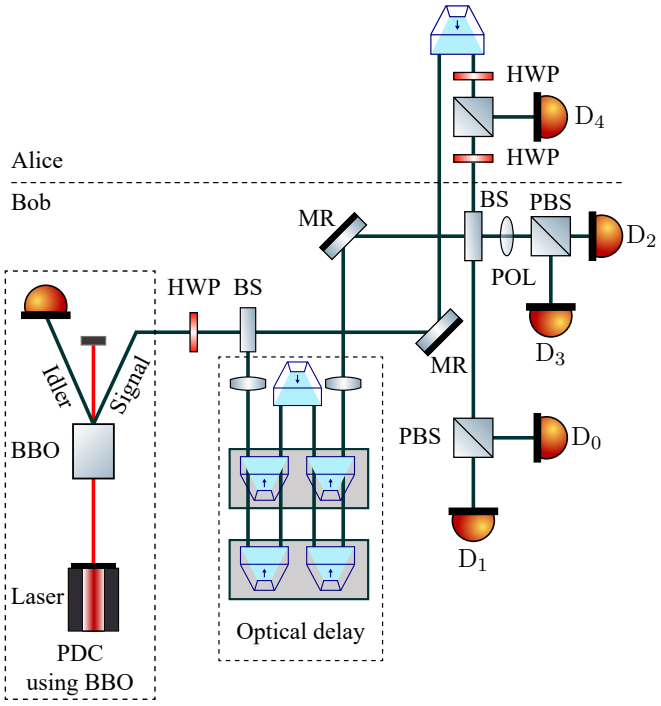


Fig. 38. Experimental setup of counterfactual QKD. A signal photon generated through parametric down-conversion (PDC) in a β-BaB_2O_4 (BBO) crystal is injected into MZI. The interferometric setup comprises BSs, half-wave plates (HWPs), a polarizer (POL), PBS, and single-photon detectors (D). An optical delay, implemented with a closed-loop piezoelectric movement system, is used to balance the path length difference between the two arms of the MZI.

and introducing randomization of the wavelength or time window for Bob's detectors can be implemented. For instance, in counterfactual QSDC and QSD protocols, a portion of the counterfactually distributed entangled resources is allocated to detect the presence of an eavesdropper in the quantum channel, particularly under MITM and TH attacks [139]. This security check, executed prior to message encoding, leverages entanglement correlations to flag any anomaly introduced by an adversary. These countermeasures are essential for practical deployments to reliably detect the presence of Eve within the communication channel.

The discussed counterfactual cryptographic protocols—QKD and quantum dialogues—enable ultra-secure quantum communication, with or without pre-shared keys. While advancements in CQC may open avenues for sophisticated interception attempts, robustness against counterfactual attacks can be ensured through rigorous security checks, precise device calibration, and strategic randomization of wavelengths and timing.

VII. Experimental Implementation

In this section, we provide an overview of the experimental implementations of counterfactual QKD and direct CQC.

A. Realization of Counterfactual QKD

To validate counterfactual QKD described in Section VI-A, a group of researchers implemented this protocol using an optical interferometer, as illustrated in Fig. 38 [181]. A heralded single-photon source, generated via parametric down conversion (PDC) in a β-BaB_2O_4 crystal pumped at 406 nm, was filtered and coupled into MZI. One arm of MZI is connected to Bob's side, where the other arm is connected to the quantum channel. Alice's side, connecting at the other side of the quantum channel, is composed of PBS, two half-wave plates, and detector D_4. A closed-loop piezo-electric movement system was used to balance the path length difference between the two arms of the interferometer. The single-photon avalanche detectors with an approximate detection efficiency of 60% at 812 nm were used to register photon detection. The detection events were analyzed using a PicoQuant HydraHarp 400 multichannel event timer. The setup ensured that when key-establishing events occurred at D_{b_k+2}, the photon never left Alice's domain, thereby confirming counterfactual key exchange.

The setup was implemented at a laboratory scale, operating over a free-space path of a few meters between Alice and Bob. The experimental results demonstrated high interference visibility, with maximum values of $92\% \pm 4\%$ at detector D_{b_k} and $96\% \pm 4\%$ at D_{b_k+2}. The mean quantum bit error rate (QBER) was measured at $12\% \pm 1\%$ and improved to $7\% \pm 1\%$ when accounting for background noise and detector inefficiencies. However, the secret key transmission rate was extremely low, yielding only about nine useful counts per second. With the implementation of high-stability fiber-based MZIs, this experiment could, in principle, be extended to distances of several kilometers, enabling feasibility in practical scenarios. To assess security vulnerabilities in practical implementations, the setup was tested against a photon-number-splitting attack. The measured second-order correlation function at zero time delay, $g^{(2)}(0) = (7 \pm 5) \times 10^{-9}$, confirmed the near-ideal single-photon nature of the source with negligible multi-photon emission. Further security analysis against time-shift attacks yielded positive mutual information differences, validating the feasibility of secure key distribution. These findings provide strong experimental evidence supporting the viability of counterfactual QKD. However, several challenges remain in this experimental setup. First, generating single photons using the PDC requires precise filtering and alignment. Low coupling efficiency and stringent spectral and spatial filtering contribute to significant photon loss. Additionally, detector inefficiencies—such as high dark count rates—can adversely affect the QBER rate. Second, inferometer instability and channel noise can induce decoherence. Third, the bulky implementation of optical components in the interferometer setup limits system scalability. Finally, although the robustness of the protocol against general attacks has been discussed, potential security concerns remain—particularly due to unheralded photon leakage and vulnerabilities to detector-based attacks.

B. Direct CQC via QZ Effect

The experimental realization of counterfactual direct quantum communication, as proposed in [12], was achieved in 2017 [124]. In their experimental setup, single photons were generated via spontaneous PDC, producing entangled photon

TABLE VI
COMPARISON BETWEEN CQC AND DIFFERENT QUANTUM TECHNOLOGIES

Attribute	CQC	QKD	QSDC	QSC	QT
Application scenarios	Direct communication without particle transmission	Key generation for encryption	Direct secure message transfer	High-capacity classical information transfer	Transfer of quantum states
Achievable distance	Limited (tens of km), dependent on interferometric stability [127]	Long (up to 1000+ km with satellites) [182]	Moderate (up to 100 km in practice) [183]	Short (due to entanglement fidelity and decoherence) [184]	Limited by entanglement generation and fidelity (ranging from 500 km to 1400 km) [185]
Scability	Low; due to complex interferometric setup	High; demonstrated at global scale	Moderate; more complex than QKD	Low to Moderate; entanglement resource-intensive	Moderate; entanglement and classical channel requirements
Applicability	Very specialized; not general-purpose	Widely used	Potential for high-security direct message transfer	Useful in capacity-limited networks	Useful in quantum networks and computation requirements
Security	Ultra secure due to counterfactual ghost photons	Proven unconditional security	High due to no requirement of pre-shared key	Depend on quantum channel quality	Require secure classical channels
Maturity	Early stage	Wide; commercial products exist	Early to mid-stage	Experimental; not yet in practical use	Mid-stage
Field trial	Very limited, mostly proof-of-concept demos	Yes; satellite-based QKD	Limited field tests	Mostly experiments	Demonstrated in labs and space

pairs. One photon from each pair was directed to a heralded detection arm, while the other, designated as the signal photon, was routed into an interferometric system implementing the ℓ-CQZ$_{M,N}$ gate. This interferometer comprised nested interferometric loops, controlled through a sequence of BSs, MRs, and wave plates, designed to leverage the CQZ effect. At Alice's side, liquid-crystal phase modulator (LCPM) and PBS were utilized to block or unblock the incoming photon. For the transmission of the classical bit 0, a π-phase shift was applied using the LCPM, altering the interference conditions within the system. Conversely, no phase modulation was introduced for the transmission of the classical bit 1. To account for the experimental constraints associated with finite values of M and N within ℓ-CQZ$_{M,N}$ gate, an additional detector, D$_f$ was implemented to register inconclusive results. Specifically, in the case of classical bit '0' transmission, the photon could traverse the channel with a nonzero probability, leading to detection at D$_f$. To maintain phase coherence and minimize system errors, an active phase stabilization system incorporating piezoelectric translation stages was utilized, enabling long-term stable interference with a visibility of 98% over several hours.

In the experiment, a 100×100-pixel monochrome bitmap, depicting a Chinese knot, was transmitted bit by bit over a duration of five hours. The 50-cm communication channel exhibited a total loss of 52 dB, requiring multiple photon attempts per bit to achieve successful transmission. The experiment employed $M = 4$ outer and $N = 2$ inner cycles, which would yield success probabilities of 85.4% and 100% for bit 0 and 1 transmission, respectively, under ideal conditions. However, in the practical implementation, these probabilities were reduced to $83.4\%\pm2.2\%$ and $91.2\%\pm1.1\%$ respectively. These deviations indicate performance degradation due to imperfections in interference stability and cumulative errors in the interferometric system. Despite these limitations, 98.6% of detected photons did not enter the channel, confirming that the communication was counterfactual and the Chinese knot was transmitted with high visibility. Additionally, the maximum theoretical data rate from leaked photons was 0.014 bits per detection, while the actual transmission achieved 0.83 bits per detection, further proving that photons were not traveling through the channel. The primary sources of error included beam splitter imperfections, phase fluctuations, and accumulated loss in the interferometers, particularly for bit 1 transmission, where visibility degradation was more pronounced. These findings validate the feasibility of direct counterfactual quantum communication, wherein Alice was able to infer Bob's binary decisions without any physical photon traveling the transmission medium. Although this experiment demonstrates a strong proof of principle, the current setup is not yet practical for scalable or high-rate communication. The requirement for nanosecond-speed mirror switching is technically challenging, and the use of a half-mirror introduces significant loss. The nested interferometer demands subwavelength stability, maintained via active phase stabilization, and precise control of parameters M and N. Additionally, transmitting a 10-kilobit bitmap took over five hours due to high channel loss (~ 52 dB) and the need for repeated postselected detections, leading to long acquisition time and limiting system efficiency.

As the development of CQC is still in its nascent stage, only a limited number of experimental demonstrations have been reported [111], [124], [127], [181]. To date, the distance of all testbeds is limited to short range. The experimental demonstrations of counterfactual QKD using free-space interferometer setups have confirmed its feasibility, albeit with low key rates.

Meanwhile, bulk-optics implementations of direct CQC over centimeter scales have verified counterfactual transfer at the cost of high loss and low throughput. Overall, current testbeds emphasize validating the principle, improving stability, and reducing errors. However, the realization of practical long-distance, high-rate counterfactual communication networks remains a future goal. Table VI provides a comprehensive comparison between CQC and various established quantum communication protocols, delineating their application scenarios, achievable distances, scalability, applicability, security, maturity, and field-trial status.

VIII. Open Challenges and Future Research Directions

We outline key open challenges and potential future research directions for CQC protocols.

A. Open Challenges

While CQC offers intriguing security benefits, it is still a developing field with many technical hurdles, as outlined below, to overcome before it can be widely implemented in practical communication systems.

1) Efficiency and Scalability: Most CQC protocols necessitate a large number of inner (N) and outer (M) cycles per CQZ gate, along with intricate interferometric configurations, to attain a meaningful success probability. This results in significantly increased execution times relative to conventional protocols. The use of such nested cycles also leads to exponential growth in complexity, making real-time operation and dynamic switching between communication nodes highly inefficient. In addition, scaling to multi-node networks is hindered by the requirement that each node must implement at least one CQZ gate, leading to increased susceptibility to cumulative phase errors and losses. Furthermore, the protocol is aborted if a photon is detected in the communication channel, which not only reduces throughput but also introduces a fundamental trade-off between security and efficiency. This conditional discard mechanism inherently limits the achievable data rate and makes high-speed or continuous communication infeasible in current implementations. Collectively, these factors present substantial challenges for the practical deployment of CQC protocols in large-scale or high-performance quantum communication networks.

2) Loss and Noise Sensitivity: In H(V)-CQZ gates, only the H(V) polarization component propagates through the channel, rendering the channel effectively entropy-free and inherently resilient to dephasing noise due to the fixed input basis. However, CQC protocols remain highly susceptible to other forms of quantum channel noise—such as bit-flip, depolarizing, amplitude damping, and phase damping—which can significantly degrade communication fidelity. The inherent reliance on precise interferometric stability makes CQC setups particularly vulnerable to misalignment and phase mismatch. Photon loss, both in the optical components and the channel, directly impacts protocol success probability as the counterfactual condition is violated upon detection of any photon in transit. Moreover, detector dark counts, timing jitter, and inefficiencies further reduce overall performance. These challenges are exacerbated in long-distance implementations, where loss scales with distance and optical coherence is harder to maintain. As a result, despite their theoretical robustness against certain noise models, current CQC protocols lack resilience under general noise conditions, limiting their practicality in real-world deployments.

3) Network-Level Deployment: Extending end-to-end CQC protocols to network-level architectures presents several challenges. Generalizing point-to-point counterfactual QKD to multi-user settings requires proper management of interferometric arms—specifically, determining which arms are associated with which users, when and how to block particular paths for measurement, and how to precisely synchronize photon emission and detection across distributed nodes. Furthermore, the inherently low key-generation efficiency and susceptibility to loss in CQC are further exacerbated in large-scale networks. In conventional quantum networks, long-distance communication between spatially separated nodes is typically enabled by quantum repeaters. However, entanglement swapping in CQC diverges fundamentally from standard protocols, as it is inherently probabilistic and governed by system parameters such as M, N, and the number of D-MQZ gates [140]. Moreover, the architecture imposes a strict alternation in the type of entangled resources across repeater nodes: repeaters at even indices must be initialized with photon-photon entangled pairs, while those at odd indices require QAO-QAO entangled pairs [140]. Finally, the deployment of scalable CQC networks demands the development of stable quantum memories and error-correction techniques specifically designed for the unique characteristics of CQC protocols, posing both engineering and theoretical challenges.

B. Future Research Directions

The existing counterfactual protocols, including simplex and full-duplex CQC, counterfactual QKD, and counterfactual quantum dialogues, hold significant promise in laying the groundwork for the future implementation of counterfactual communication systems. We present potential directions for future research.

1) Resource Optimization: The performance of CQC protocols heavily relies on the number of N inner and M outer cycles within each CQZ gate. In [66], a specific optimization technique aimed at minimizing the number of channel usages $\eta \propto MN$ and the total communication time $T \propto MNT_c$, while maintaining a desired success probability. Despite this specific optimization framework, more general and adaptable optimization strategies are still required. Future work should investigate dynamic optimization algorithms that adjust M and N based on real-time channel conditions, multi-objective optimizations that balance trade-offs among counterfactuality, fidelity, latency, and loss tolerance, and application-specific optimization, where N and M are tailored for different use cases.

2) Error Correction and Mitigation Schemes for CQC: Unlike conventional quantum communication, where the entire

photon traverses the channel, CQC involves only a vanishingly small photon component in the channel as N and M increase. Consequently, standard error correction and mitigation techniques are not directly applicable. CQC requires specialized error correction and mitigation strategies tailored to its unique operational model. One promising approach is error-aware protocol design, where N and M are dynamically optimized to balance noise resilience and counterfactuality. Detection-side techniques—such as dark count suppression, bias correction, and timing calibration—are also essential for improving robustness. Error correction schemes must be designed to preserve the core principle of counterfactuality while mitigating the effects of environmental noise, device imperfections, and optical instability [186]. Developing such schemes is critical to improving reliability, enabling long-distance communication, and facilitating integration into scalable quantum networks.

3) Multi-Node Architecture: Current CQC protocols are primarily designed for end-to-end communication. Scaling to multi-node networks introduces substantial challenges, including increased hardware complexity, cumulative phase instability, and optical losses. To enable practical deployment, future research should focus on modular, reconfigurable architectures supporting dynamic routing, node addressing, and scalable communication under counterfactual constraints. One potential direction is the development of hub-based or hierarchical topologies, where trusted central nodes coordinate counterfactual links among distributed clients using time-multiplexing or wavelength-division techniques. Addressing these challenges is essential for realizing practical and scalable counterfactual quantum networks capable of secure communication across multiple parties.

IX. Conclusion

Counterfactual communication is a unique concept in quantum communication that distinguishes itself from classical and other quantum communication methods by leveraging a fundamentally different approach to transfer information. By primarily emphasizing the wave-particle duality of quantum mechanics, quantum interference, and the CQZ effect, CQC achieves information transmission with no physical particle being found in the channel. This fact not only enhances the security of communication systems but also opens the door to the potential of performing counterfactual attacks on other quantum systems without being detected. While counterfactual communication offers intriguing security benefits, it is still a largely experimental field with many technical hurdles to overcome before achieving practical deployment. Nonetheless, the existing counterfactual protocols, including simplex and full-duplex CQC, counterfactual QKD, and counterfactual quantum dialogues, hold significant promise in laying the groundwork for the future implementation of practical counterfactual communication systems.

Acknowledgment

The authors wish to thank M. Clouâtré for his helpful suggestions and careful reading of the paper.

References

[1] L. Leydesdorff, "The evolution of communication systems," *Int. J. Syst. Res. Inf. Sci.*, vol. 6, pp. 219–230, Mar. 1994.
[2] A. Ephremides and B. Hajek, "Information theory and communication networks: An unconsummated union," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2416–2434, Oct. 1998.
[3] P. Baran, "On distributed communications networks," *IEEE Trans. Commun.*, vol. 12, no. 1, pp. 1–9, Mar. 1964.
[4] L. Kleinrock, "An early history of the internet," *IEEE Commun. Mag.*, vol. 48, no. 8, pp. 26–36, Aug. 2010.
[5] H. Nyquist, "Certain topics in telegraph transmission theory," *IEEE Trans. Amer. Inst. Elec. Eng.*, vol. 47, no. 2, pp. 617–644, Apr. 1928.
[6] H. Harada, K. Sato, and M. Fujise, "A radio-on-fiber based millimeter-wave road-vehicle communication system by a code division multiplexing radio transmission scheme," *IEEE Trans. Intell. Transp.*, vol. 2, no. 4, pp. 165–179, Dec. 2001.
[7] J. McQuillan, I. Richer, and E. Rosen, "The new routing algorithm for the ARPANET," *IEEE Trans. Commun.*, vol. 28, no. 5, pp. 711–719, May 1980.
[8] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, Jul. 2020.
[9] L. Bacsardi, "On the way to quantum-based satellite communication," *IEEE Wireless Commun.*, vol. 51, no. 8, pp. 50–55, Aug. 2013.
[10] T. Taleb, A. Ksentini, and R. Jantti, "Anything as a service for 5G mobile systems," *IEEE Netw.*, vol. 30, no. 6, pp. 84–91, Dec. 2016.
[11] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," *Nat. Photonics*, vol. 9, no. 10, pp. 641–652, Sep. 2015.
[12] H. Salih, Z.-H. Li, M. Al-Amri, and M. S. Zubairy, "Protocol for direct counterfactual quantum communication," *Phys. Rev. Lett.*, vol. 110, no. 17, p. 170502, Apr. 2013.
[13] R. Kaewpuang, M. Xu, D. Niyato, H. Yu, Z. Xiong, and J. Kang, "Stochastic qubit resource allocation for quantum cloud computing," in *Proc. International Symposium on Network Operations and Management (NOMS)*, Miami, FL, USA, May 2023.
[14] 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.
[15] 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.
[16] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, Jul. 2020.
[17] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5416–5441, Apr. 2021.
[18] 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.
[19] Y. Lu, S. Maharjan, and Y. Zhang, "Adaptive edge association for wireless digital twin networks in 6G," *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16 219–16 230, Nov. 2021.
[20] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, May 2022.
[21] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, p. 145, Mar. 2002.
[22] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Optica*, vol. 12, no. 14, pp. 1012–1236, Dec. 2020.
[23] G. Brassard and C. H. Bennett, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. International Conference on Computers, Systems and Signal Processing (ICCSSP)*, Bangalore, India, Dec. 1984.
[24] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground entanglement-based quantum key distribution," *Phys. Rev. Lett.*, vol. 119, no. 20, p. 200501, Nov. 2017.

[25] X. Wang, J. Liu, X. Li, and Y. Li, "Generation of stable and high extinction ratio light pulses for continuous variable quantum key distribution," *IEEE Trans. Quantum Eng.*, vol. 51, no. 6, pp. 1–6, Jun. 2015.

[26] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, no. 7501, pp. 475–478, May 2014.

[27] M. C. Hoi-Kwong Lo and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, 2012.

[28] X. M. Hoi-Kwong Lo and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, 2005.

[29] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum secure direct communication with quantum memory," *Phys. Rev. Lett.*, vol. 118, p. 220501, May 2017.

[30] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys. Rev. A*, vol. 68, p. 042317, Oct. 2003.

[31] H. Wang, Y. Q. Zhang, X. F. Liu, and Y. P. Hu, "Efficient quantum dialogue using entangled states and entanglement swapping without information leakage," *Quantum Inf. Process*, vol. 15, no. 6, pp. 2593–2603, Mar. 2016.

[32] A. Khan, U. Khalid, J. ur Rehman, K. Lee, and H. Shin, "Quantum anonymous collision detection for quantum networks," *EPJ Quantum Technol.*, vol. 8, no. 1, p. 27, Dec. 2021.

[33] A. Khan, J. ur Rehman, and H. Shin, "Quantum anonymous notification for network-based applications," *Quantum Inf. Process*, vol. 20, no. 12, p. 397, Nov. 2021.

[34] A. Khan, U. Khalid, J. ur Rehman, and H. Shin, "Quantum anonymous private information retrieval for distributed networks," *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4026–4037, Jun. 2022.

[35] A. Harrow, P. Hayden, and D. Leung, "Superdense coding of quantum states," *Phys. Rev. Lett.*, vol. 92, no. 18, p. 187901, May 2004.

[36] X. S. Liu, G. L. Long, D. M. Tong, and F. Li, "General scheme for superdense coding between multiparties," *Phys. Rev. A*, vol. 65, no. 2, p. 022304, Jan. 2002.

[37] X.-M. Jin, J.-G. Ren, B. Yang, Z.-H. Yi, F. Zhou, X.-F. Xu, S.-K. Wang, D. Yang, Y.-F. Hu, S. Jiang, T. Yang, H. Yin, K. Chen, C.-Z. Peng, and J.-W. Pan, "Experimental free-space quantum teleportation," *Nat. Photonics*, vol. 4, no. 6, pp. 376–381, May 2010.

[38] A. Marie and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 95, no. 1, p. 012316, Jan. 2017.

[39] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, "Quantum clock synchronization based on shared prior entanglement," *Phys. Rev. Lett.*, vol. 85, no. 9, p. 2010, Aug. 2000.

[40] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, "Reference frames, superselection rules, and quantum information," *Rev. Mod. Phys.*, vol. 79, pp. 555–609, Apr. 2007.

[41] E. O. Ilo-Okeke, L. Tessler, J. P. Dowling, and T. Byrnes, "Remote quantum clock synchronization without synchronized clocks," *npj Quantum Inf.*, vol. 4, no. 1, pp. 1–5, Aug. 2018.

[42] M. A. Ullah, S. N. Paing, and H. Shin, "Noise-robust quantum teleportation with counterfactual communication," *IEEE Access*, vol. 10, pp. 61 484–61 493, Mar. 2022.

[43] Z.-H. Li, L. Wang, J. Xu, Y. Yang, M. Al-Amri, and M. S. Zubairy, "Counterfactual Trojan horse attack," *Phys. Rev. A*, vol. 101, p. 022336, Feb. 2020.

[44] R. J. Tosiello, *The birth and early years of the Bell Telephone System, 1876-1880*. Boston University Graduate School, 1971.

[45] M. Rikitianskaia, G. Balbi, and K. Lobinger, "The mediatization of the air: Wireless telegraphy and the origins of a transnational space of communication, 1900–1910s," *J. Commun.*, vol. 68, no. 4, pp. 758–779, Jun. 2018.

[46] J. McQuillan, G. Falk, and I. Richer, "A review of the development and performance of the ARPANET routing algorithm," *IEEE Trans. Commun.*, vol. 26, no. 12, pp. 1802–1811, Dec. 1978.

[47] J. F. Fitzsimons, "Private quantum computation: An introduction to blind quantum computing and related protocols," *npj Quantum Inf.*, vol. 3, no. 1, pp. 1–11, May 2017.

[48] A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," *Rev. Mod. Phys.*, vol. 68, no. 3, pp. 733–753, Jul. 1996.

[49] M. A. Ullah, J. ur Rehman, and H. Shin, "Photon dynamics in counterfactual quantum communication," in *Proc. Korea Information and Communication Society (KICS) Winter Conference*, Pyeongchang, Korea, Feb. 2021.

[50] O. Hosten, M. T. Rakher, J. T. Barreiro, N. A. Peters, and P. G. Kwiat, "Counterfactual quantum computation through quantum interrogation," *Nature*, vol. 439, no. 7079, pp. 949–952, Feb. 2006.

[51] F. Zaman, Y. Jeong, and H. Shin, "Counterfactual quantum superdense coding," in *Bulletin of the American Physical Society (BAPS)*, Boston, MA, Mar. 2019, (Volume 64, Number 2, Session R28.00005).

[52] S. N. Paing, F. Zaman, J. ur Rehman, and H. Shin, "Counterfactual universal logic gates," in *Proc. Korea Information and Communication Society (KICS) Summer Conference*, Pyeongchang, Korea, Aug. 2020.

[53] S. N. Paing, F. Zaman, and H. Shin, "Counterfactual controlled quantum teleportation," in *Proc. Korea Information and Communication Society (KICS) Winter Conference*, Pyeongchang, Korea, Feb. 2021.

[54] ——, "Counterfactual quantum private comparison," in *Proc. Korea Information and Communication Society (KICS) Winter Conference*, Pyeongchang, Korea, Feb. 2022.

[55] M. A. Ullah, S. N. Paing, and H. Shin, "Noise-robust quantum teleportation with counterfactual communication," *IEEE Access*, vol. 10, pp. 61 484–61 493, Jun. 2022.

[56] S. N. Paing, J. W. Setiawan, S. Tariq, M. T. Rahim, K. Lee, and H. Shin, "Counterfactual anonymous quantum teleportation in the presence of adversarial attacks and channel noise," *Sensors*, vol. 22, no. 19, p. 7587, Oct. 2022.

[57] 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.

[58] F. Zaman, Y. Jeong, and H. Shin, "Superdense coding via semi-counterfactual Bell measurements," in *Proc. Asian Quantum Information Science (AQIS) Conference*, Nagoya, Japan, Sep. 2018.

[59] T.-G. Noh, "Counterfactual quantum cryptography," *Phys. Rev. Lett.*, vol. 103, no. 23, p. 230501, Dec. 2009.

[60] J. G. Rarity, P. R. Tapster, E. Jakeman, T. Larchuk, R. A. Campos, M. C. Teich, and B. E. A. Saleh, "Two-photon interference in a Mach-Zehnder interferometer," *Phys. Rev. Lett.*, vol. 65, no. 11, pp. 1348–1351, Sep. 1990.

[61] Y. Ji, Y. Chung, D. Sprinzak, M. Heiblum, D. Mahalu, and H. Shtrikman, "An electronic Mach-Zehnder interferometer," *Nature*, vol. 422, no. 6930, pp. 415–418, Mar. 2003.

[62] Y. Aharonov and L. Vaidman, "Modification of counterfactual communication protocols that eliminates weak particle traces," *Phys. Rev. A*, vol. 99, no. 1, p. 010103, Jan. 2019.

[63] Q. Guo, L.-Y. Cheng, L. Chen, H.-F. Wang, and S. Zhang, "Counterfactual quantum-information transfer without transmitting any physical particles," *Sci. Rep.*, vol. 5, no. 1, pp. 1–6, Feb. 2015.

[64] Z.-H. Li, M. Al-Amri, X.-H. Yang, and M. S. Zubairy, "Counterfactual exchange of unknown quantum states," *Phys. Rev. A*, vol. 100, no. 2, p. 022110, Aug. 2019.

[65] 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.

[66] F. Zaman, K. Lee, and H. Shin, "Information carrier and resource optimization of counterfactual quantum communication," *Quantum Inf. Process*, vol. 20, no. 5, pp. 1–10, May 2021.

[67] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge university press, 2010.

[68] P. Kaye, R. Laflamme, and M. Mosca, *An introduction to quantum computing*. OUP Oxford, 2006.

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

[70] T. M. Graham, Y. Song, J. Scott, C. Poole, L. Phuttitarn, K. Jooya, P. Eichler, A. M. X. Jiang, B. Grinkemeyer, M. Kwon, M. Ebert, J. Cherek, M. T. Lichtman, M. Gillette, J. Gilbert, D. Bowman, T. Ballance, C. Campbell, E. D. Dahl, O. Crawford, N. S. Blunt, B. Rogers, T. Noel, and M. Saffman, "Multi-qubit entanglement and algorithms on a neutral-atom quantum computer," *Nature*, vol. 604, no. 7906, pp. 457–462, Apr. 2022.

[71] P. Agrawal and A. Pati, "Perfect teleportation and superdense coding with W states," *Phys. Rev. A*, vol. 74, no. 6, p. 062320, Dec. 2006.

[72] J. McQuillan, G. Falk, and I. Richer, "Detection of genuine N-qubit W state, GHZ state and Twin-Fock state via Quantum Fisher information," *Phys. Rev. A*, vol. 384, no. 20, p. 126413, Mar. 2020.

[73] D. M. Greenberger, "GHZ (Greenberger—Horne—Zeilinger) theorem and GHZ states," in *Compendium of Quantum Physics*. Springer, Jul. 2009, pp. 258–263.

[74] E. Davies, "Information and quantum measurement," *IEEE Trans. Inf. Theory*, vol. 24, no. 5, pp. 596–599, Sep. 1978.

[75] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "Distinguishing separable and entangled states," *Phys. Rev. Lett.*, vol. 88, no. 18, p. 187904, Apr. 2002.

[76] F. A. Berezin and M. Shubin, *The Schrödinger Equation*. Springer Science & Business Media, 2012, vol. 66.

[77] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Phys. Rev. A*, vol. 52, no. 5, pp. 3457–3467, Nov. 1995.

[78] Y. Aharonov, E. Cohen, and S. Popescu, "Gravity-wave interferometers as quantum-gravity detectors," *Nature*, vol. 398, no. 6724, pp. 216–218, Mar. 1999.

[79] J. G. Baker, J. Centrella, D.-I. Choi, M. Koppitz, and J. van Meter, "Gravitational-wave extraction from an inspiraling configuration of merging black holes," *Phys. Rev. Lett.*, vol. 96, no. 11, p. 111102, Mar. 2006.

[80] B. P. A. *et. al.*, "Observation of gravitational waves from a binary black hole merger," *Phys. Rev. Lett.*, vol. 116, no. 6, p. 061102, Feb. 2016.

[81] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum metrology," *Phys. Rev. Lett.*, vol. 96, no. 1, p. 010401, Jan. 2006.

[82] U. Khalid, J. ur Rehman, and H. Shin, "Metrologically resourceful multipartite entanglement under quantum many-body effects," *Quantum Sci. Technol.*, vol. 6, no. 2, p. 025007, Jan. 2021.

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

[84] J. M. Boss, K. Cujia, J. Zopes, and C. L. Degen, "Quantum sensing with arbitrary frequency resolution," *Science*, vol. 356, no. 6340, pp. 837–840, May 2017.

[85] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, "Advances in photonic quantum sensing," *Nat. Photonics*, vol. 12, no. 12, pp. 724–733, Nov. 2018.

[86] B. Yurke, S. L. McCall, and J. R. Klauder, "SU(2) and SU(1,1) interferometers," *Phys. Rev. A*, vol. 33, no. 6, pp. 4033–4054, Jun. 1986.

[87] R. Demkowicz-Dobrzanski, U. Dorner, B. J. Smith, J. S. Lundeen, W. Wasilewski, K. Banaszek, and I. A. Walmsley, "Quantum phase estimation with lossy interferometers," *Phys. Rev. A*, vol. 80, no. 1, p. 013825, Jul. 2009.

[88] P. G. Kwiat, W. A. Vareka, C. K. Hong, H. Nathel, and R. Y. Chiao, "Correlated two-photon interference in a dual-beam Michelson interferometer," *Phys. Rev. A*, vol. 41, no. 5, pp. 2910–2913, Mar. 1990.

[89] K. McKenzie, D. A. Shaddock, D. E. McClelland, B. C. Buchler, and P. K. Lam, "Experimental demonstration of a squeezing-enhanced power-recycled Michelson interferometer for gravitational wave detection," *Phys. Rev. Lett.*, vol. 88, no. 23, p. 231102, May 2002.

[90] Y.-J. Wang, D. Z. Anderson, V. M. Bright, E. A. Cornell, Q. Diot, T. Kishimoto, M. Prentiss, R. A. Saravanan, S. R. Segal, and S. Wu, "Atom Michelson interferometer on a chip using a Bose-Einstein condensate," *Phys. Rev. Lett.*, vol. 94, no. 9, p. 090405, Mar. 2005.

[91] H. Vahlbruch, S. Chelkowski, B. Hage, A. Franzen, K. Danzmann, and R. Schnabel, "Demonstration of a squeezed-light-enhanced power- and signal-recycled Michelson interferometer," *Phys. Rev. Lett.*, vol. 95, no. 21, p. 211102, Nov. 2005.

[92] R. A. Campos, B. E. A. Saleh, and M. C. Teich, "Quantum-mechanical lossless beam splitter: SU(2) symmetry and photon statistics," *Phys. Rev. A*, vol. 40, no. 3, p. 1371, Aug. 1989.

[93] K. P. Zetie, S. F. Adams, and R. M. Tocknell, "How does a Mach-Zehnder interferometer work?" *Phys. Educ.*, vol. 35, no. 1, p. 46, Jan. 2000.

[94] A. A. Michelson, "The relative motion of the earth and the luminiferous ether," *Am. J. Sci.*, vol. 22, no. 128, p. 120, Nov. 1881.

[95] A. Canagasabey, A. Michie, J. Canning, J. Holdsworth, S. Fleming, H.-C. Wang, and M. L. Åslund, "A comparison of Michelson and Mach-Zehnder interferometers for laser linewidth measurements," in *Proc. Conference on Lasers and Electro-Optics/Pacific Rim*. Optical Society of America, 2011, p. C428.

[96] W. M. Itano, D. J. Heinzen, J. J. Bollinger, and D. J. Wineland, "Quantum Zeno effect," *Phys. Rev. Lett.*, vol. 41, no. 5, p. 2295, Mar. 1990.

[97] M. Clouâtré, M. J. Khojasteh, and M. Z. Win, "Model-predictive quantum control via Hamiltonian learning," *IEEE Trans. Quantum Eng.*, vol. 3, pp. 1–23, Oct. 2022, Art no. 4100623.

[98] M. Clouâtré, S. Marano, P. L. Falb, and M. Z. Win, "Admissible optimal control for parameter estimation in quantum systems," *IEEE Control Syst. Lett.*, vol. 8, pp. 2283–2288, Sep. 2024.

[99] A. Elitzur and L. Vaidman, "Quantum mechanical interaction-free measurement," *Found. Phys.*, vol. 23, no. 76, pp. 987–997, Jul. 1993.

[100] N. Benedikter, M. Porta, and B. Schlein, *Effective evolution equations from quantum dynamics*. Springer, 2016, vol. 7.

[101] T. Petrosky, S. Tasaki, and I. Prigogine, "Quantum Zeno effect," *Physics Lett. A*, vol. 151, no. 3-4, pp. 109–113, Dec. 1990.

[102] P. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. A. Kasevich, "Interaction-free measurement," *Phys. Rev. Lett.*, vol. 74, no. 24, p. 4763, Nov. 1995.

[103] R. H. Dicke, "Interaction-free quantum measurements: A paradox," *Am. J. Phys.*, vol. 49, no. 10, pp. 925–930, Jun. 1981.

[104] E. du Marchie Van Voorthuysen, "Realization of an interaction-free measurement of the presence of an object in a light beam," *Am. J. Phys.*, vol. 64, no. 12, pp. 1504–1507, Apr. 1996.

[105] P. G. Kwiat, A. G. White, J. R. Mitchell, O. Nairz, G. Weihs, H. Weinfurter, and A. Zeilinger, "High-efficiency quantum interrogation measurements via the quantum Zeno effect," *Phys. Rev. Lett.*, vol. 83, no. 23, pp. 4725–4728, Dec. 1999.

[106] A. J. DeWeerd, "Interaction-free measurement," *Am. J. Phys.*, vol. 70, no. 3, pp. 272–275, Nov. 2001.

[107] Y. P. Huang and M. G. Moore, "Interaction- and measurement-free quantum Zeno gates for universal computation with single-atom and single-photon qubits," *Phys. Rev. A*, vol. 77, no. 6, p. 062332, Jun. 2008.

[108] H. Azuma, "Interaction-free quantum computation," *Phys. Rev. A*, vol. 70, no. 1, p. 012318, Jul. 2004.

[109] A. G. White, J. R. Mitchell, O. Nairz, and P. G. Kwiat, "Interaction-free imaging," *Phys. Rev. A*, vol. 58, no. 1, pp. 605–613, Jul. 1998.

[110] F. Zaman, Y. Jeong, and H. Shin, "Counterfactual Bell-state analysis," *Sci. Rep.*, vol. 8, no. 1, p. 14641, Oct. 2018.

[111] F. Kong, C. Ju, P. Huang, P. Wang, X. Kong, F. Shi, L. Jiang, and J. Du, "Experimental realization of high-efficiency counterfactual computation," *Phys. Rev. Lett.*, vol. 115, no. 8, p. 080501, Aug. 2015.

[112] H. Salih, J. R. Hance, W. McCutcheon, T. Rudolph, and J. Rarity, "Exchange-free computation on an unknown qubit at a distance," *New J. Phys.*, vol. 23, no. 1, p. 013004, Jan. 2021.

[113] H. Salih, "Tripartite counterfactual quantum cryptography," *Phys. Rev. A*, vol. 90, no. 1, p. 012333, Jul. 2014.

[114] Z.-Q. Yin, H.-W. Li, Y. Yao, C.-M. Zhang, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, "Counterfactual quantum cryptography based on weak coherent states," *Phys. Rev. A*, vol. 86, no. 2, p. 022313, Aug. 2012.

[115] Y. Sun and Q.-Y. Wen, "Counterfactual quantum key distribution with high efficiency," *Phys. Rev. A*, vol. 82, no. 5, p. 052318, Nov. 2010.

[116] M. Ren, G. Wu, E. Wu, and H. Zeng, "Experimental demonstration of counterfactual quantum key distribution," *Laser Phys.*, vol. 21, no. 4, pp. 755–760, Mar. 2011.

[117] S. Zhang, J. Wnang, and C. J. Tang, "Counterfactual attack on counterfactual quantum key distribution," *Europhys. Lett.*, vol. 98, no. 3, p. 30012, May 2012.

[118] Z. Sheng, W. Jian, and T. Chao-Jing, "Security proof of counterfactual quantum cryptography against general intercept-resend attacks and its vulnerability," *Chinese Phys. B*, vol. 21, no. 6, p. 060303, Jun. 2012.

[119] Y.-B. Li, "Analysis of counterfactual quantum key distribution using error-correcting theory," *Quantum Inf. Process*, vol. 13, no. 10, pp. 2325–2342, Jul. 2014.

[120] Y. Chen, D. Jian, X. Gu, L. Xie, and L. Chen, "Counterfactual entanglement distribution using quantum dot spins," *J. Opt. Soc. Am. B-Opt. Phys.*, vol. 33, no. 4, pp. 663–669, Jan. 2016.

[121] Z.-H. Li, M. Al-Amri, and M. S. Zubairy, "Direct counterfactual transmission of a quantum state," *Phys. Rev. A*, vol. 92, no. 5, p. 052315, Nov. 2015.

[122] Q. Guo, S. Zhai, L.-Y. Cheng, H.-F. Wang, and S. Zhang, "Counterfactual quantum cloning without transmitting any physical particles," *Phys. Rev. A*, vol. 96, no. 5, p. 052335, Nov. 2017.

[123] F. Zaman, Y. Jeong, and H. Shin, "Dual quantum Zeno superdense coding," *Sci. Rep.*, vol. 9, no. 1, p. 11193, Aug. 2019.

[124] Y. Cao, Y.-H. Li, Z. Cao, J. Yin, Y.-A. Chen, H.-L. Yin, T.-Y. Chen, X. Ma, C.-Z. Peng, and J.-W. Pan, "Direct counterfactual communication via quantum Zeno effect," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 114, no. 19, pp. 4920–4924, May 2017.

[125] Z.-H. Li, M. Al-Amri, and M. S. Zubairy, "Direct quantum communication with almost invisible photons," *Phys. Rev. A*, vol. 89, no. 5, p. 052334, May 2014.

[126] Z. Cao, "Counterfactual universal quantum computation," *Phys. Rev. A*, vol. 102, no. 5, p. 052413, Nov. 2020.

[127] Y. Liu, L. Ju, X.-L. Liang, S.-B. Tang, G.-L. S. Tu, L. Zhou, C.-Z. Peng, K. Chen, T.-Y. Chen, Z.-B. Chen, and J.-W. Pan, "Experimental demonstration of counterfactual quantum communication," *Phys. Rev. Lett.*, vol. 109, no. 3, p. 030501, Jul. 2012.

[128] I. A. Calafell, T. Strömberg, D. Arvidsson-Shukur, L. Rozema, V. Saggio, C. Greganti, N. Harris, M. Prabhu, J. Carolan, M. Hochberg *et al.*, "Trace-free counterfactual communication with a nanophotonic processor," *npj Quantum Inf.*, vol. 5, no. 1, pp. 1–5, Jul. 2019.

[129] F. Zaman, E.-K. Hong, and H. Shin, "Local distinguishability of Bell-type states," *Quantum Inf. Process*, vol. 20, no. 5, pp. 1–12, May 2021.

[130] Y. Aharonov, E. Cohen, and S. Popescu, "A dynamical quantum Cheshire Cat effect and implications for counterfactual communication," *Nat. Commun.*, vol. 12, no. 1, pp. 1–8, Aug. 2021.

[131] Q. Guo, L.-Y. Cheng, L. Chen, H.-F. Wang, and S. Zhang, "Counterfactual entanglement distribution without transmitting any particles," *Opt. Express*, vol. 22, no. 8, pp. 8970–8984, Apr. 2014.

[132] Y. Chen, X. Gu, D. Jiang, L. Xie, and L. Chen, "Tripartite counterfactual entanglement distribution," *Opt. Express*, vol. 23, no. 16, pp. 21 193–21 203, Aug. 2015.

[133] H. Salih, "Protocol for counterfactually transporting an unknown qubit," *Front. Phys.*, vol. 3, p. 94, Jan. 2016.

[134] Q. Guo, L.-Y. Cheng, L. Chen, H.-F. Wang, and S. Zhang, "Counterfactual quantum-information transfer without transmitting any physical particles," *Sci. Rep.*, vol. 5, p. 8416, Feb. 2015.

[135] D. R. M. Arvidsson-Shukur and C. H. W. Barnes, "Quantum counterfactual communication without a weak trace," *Phys. Rev. A*, vol. 94, no. 6, p. 062303, Dec. 2016.

[136] X. Yang, K. Wei, H. Ma, S. Sun, Y. Du, and L. Wu, "Trojan horse attacks on counterfactual quantum key distribution," *Physics Lett. A*, vol. 380, no. 18-19, pp. 1589–1592, Apr. 2016.

[137] A. Shenoy-Hejamadi and R. Srikanth, "Counterfactual distribution of Schrödinger cat states," *Phys. Rev. A*, vol. 92, no. 6, p. 062308, Dec. 2015.

[138] H. A. Shenoy, R. Srikanth, and T. Srinivas, "Counterfactual quantum certificate authorization," *Phys. Rev. A*, vol. 89, no. 5, p. 052307, May 2014.

[139] S. N. Paing, F. Zaman, J. ur Rehman, K. M. Byun, J. Cho, T. Q. Duong, and H. Shin, "Counterfactual quantum protocols for dialogue, teleportation, and comparison," *IEEE Trans. Commun.*, vol. 73, no. 2, pp. 874–888, Feb. 2025.

[140] S. N. Paing, T. Q. Duong, and H. Shin, "Counterfactual long-distance quantum communication," in *Proc. International Conference on Quantum Communications, Networking, and Computing (QCNC)*, Kanazawa, Japan, Jul. 2024.

[141] H. Salih, "From counterportation to local wormholes," *Quantum Sci. Technol.*, vol. 8, no. 2, p. 025016, Mar. 2023.

[142] J. R. Hance and J. Rarity, "Counterfactual ghost imaging," *npj Quantum Inf.*, vol. 7, no. 1, p. 88, Jun. 2021.

[143] H. F. Hofmann, J. R. Hance, T. Matsushita, M. Ji, and M. Iinuma, "Counterfactual control and quantum contextuality in multi-mode interferometers," in *Proc. SPIE, Quantum Communications and Quantum Imaging XXII*, San Francisco, CA, USA, Feb. 2024.

[144] X.-Q. Cai, Y.-G. Yang, T.-Y. Wang, G.-B. Xu, and D.-H. Jiang, "Counterfactual all-or-nothing oblivious transfer for quantum messages," *Adv. Quantum Technol.*, p. 2400454, Jan. 2025.

[145] Z.-H. Li, X.-F. Ji, S. Asiri, L. Wang, and M. Al-Amri, "Counterfactual logic gates," *Phys. Rev. A*, vol. 102, no. 2, p. 022606, Aug. 2020.

[146] Q. Guo, L.-Y. Cheng, L. Chen, H.-F. Wang, and S. Zhang, "Counterfactual distributed controlled-phase gate for quantum-dot spin qubits in double-sided optical microcavities," *Phys. Rev. A*, vol. 90, no. 4, p. 042327, Oct. 2014.

[147] Z. Cao, "Counterfactual universal quantum computation," *Phys. Rev. A*, vol. 102, no. 5, p. 052413, Nov. 2020.

[148] X.-Q. Shao, L. Chen, S. Zhang, and K.-H. Yeon, "Fast CNOT gate via quantum Zeno dynamics," *J. Phys. B*, vol. 42, no. 16, p. 165507, Jul. 2009.

[149] S. Zhang, J. Wang, and C.-J. Tang, "Counterfactual quantum deterministic key distribution," *Commun. Theor. Phys.*, vol. 59, no. 1, p. 27, Jan. 2013.

[150] H. Salih, "Counterfactual quantum erasure: Spooky action without entanglement," *R. Soc. Open Sci.*, vol. 5, no. 2, p. 171250, Feb. 2018.

[151] Y. Song and L. Yang, "Semi-counterfactual quantum bit commitment protocol," *Sci. Rep.*, vol. 10, no. 1, p. 6531, Apr. 2020.

[152] F. A. Hashmi, F. Li, S.-Y. Zhu, and M. S. Zubairy, "Two-state vector formalism and quantum interference," *J. Phys. A: Math. Theor.*, vol. 49, no. 34, p. 345302, Jul. 2016.

[153] S. Biswas, S. Razdan, B. K. Behera, and P. K. Panigrahi, "Realization of counterfactual quantum cryptography using IBM's quantum computer," Nov 2018.

[154] J. Hance, W. McCutcheon, P. Yard, and J. Rarity, "Modal, truly counterfactual communication with on-chip demonstration proposal," in *Quantum Information and Measurement (QIM) V: Quantum Technologies*, Rome, Italy, Apr. 2019.

[155] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[156] R. F. Nalewajski, "Elements of information theory," in *Perspectives in Electronic Structure Theory*, 2011, pp. 371–395.

[157] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, pp. 2881–2884, Nov. 1992.

[158] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense coding in experimental quantum communication," *Phys. Rev. Lett.*, vol. 76, no. 25, pp. 4656–4659, Jun. 1996.

[159] H. Salih, J. R. Hance, W. McCutcheon, T. Rudolph, and J. Rarity, "Deterministic teleportation and universal computation without particle exchange," *arXiv:2009.05564*, 2020.

[160] H. Salih, "Protocol for counterfactually transporting an unknown qubit," *Front. Phys.*, vol. 3, p. 94, Jan. 2016.

[161] Y. Lee, R. Takagi, H. Yamasaki, G. Adesso, and S. Lee, "State exchange with quantum side information," *Phys. Rev. Lett.*, vol. 122, p. 010502, Jan. 2019.

[162] Y. Lee, H. Yamasaki, G. Adesso, and S. Lee, "One-shot quantum state exchange," *Phys. Rev. A*, vol. 100, p. 042306, Oct. 2019.

[163] S. Yun, K. Kwon, J. ur Rehamn, F. Zaman, and H. Shin, "Quantum duplex coding for classical information on IBM quantum devices," in *Proc. Korea Information and Communication Society (KICS) Fall Conference*, Seoul, Korea, Nov. 2019, (Best Paper Award).

[164] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek *et al.*, "Entanglement-based quantum communication over 144 km," *Nat. Phys.*, vol. 3, no. 7, pp. 481–486, Jun. 2007.

[165] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, no. 7501, pp. 475–478, May 2014.

[166] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring," *Nat. Phys.*, vol. 9, no. 12, pp. 832–836, Nov. 2015.

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

[168] H. Salih, "Tripartite counterfactual quantum cryptography," *Phys. Rev. A*, vol. 90, p. 012333, Jul. 2014.

[169] J.-L. Zhang, F.-Z. Guo, F. Gao, B. Liu, and Q.-Y. Wen, "Private database queries based on counterfactual quantum key distribution," *Phys. Rev. A*, vol. 88, no. 2, p. 022334, Aug. 2013.

[170] Y.-Q. Lin, M. Wang, X.-Q. Yang, and H.-W. Liu, "Counterfactual quantum key distribution with untrusted detectors," *Heliyon*, vol. 9, no. 2, Feb. 2023.

[171] J.-Y. Hu, B. Yu, M.-Y. Jing, L.-T. Xiao, S.-T. Jia, G.-Q. Qin, and G.-L. Long, "Experimental quantum secure direct communication with single photons," *Light Sci. Appl.*, vol. 5, no. 9, pp. e16 144–e16 144, Apr. 2016.

[172] J.-M. Qi, G. Xu, X.-B. Chen, T.-Y. Wang, X.-Q. Cai, and Y.-X. Yang, "Two authenticated quantum dialogue protocols based on three-particle entangled states," *Quantum Inf. Process*, vol. 17, no. 9, pp. 1–19, Jul. 2018.

[173] F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, "Experimental long-distance quantum secure direct communication," *Sci. Bull.*, vol. 62, no. 22, pp. 1519–1524, Nov. 2017.

[174] L. Zhou, Y.-B. Sheng, and G.-L. Long, "Device-independent quantum secure direct communication against collective attacks," *Sci. Bull.*, vol. 65, no. 1, pp. 12–20, Jan. 2020.

[175] F. Zaman and H. Shin, "Counterfactual swap gates," in *Proc. Korea Information and Communication Society (KICS) Winter Conference*, Pyeongchang, Korea, Feb. 2021.

[176] F. Zaman, Y. Jeong, and H. Shin, "Counterfactual Bell basis measurement," in *Proc. Korea Information and Communication Society (KICS) Fall Conference*, Daegu, Korea, Nov. 2017.

[177] ——, "Noise analysis of semi-counterfactual Bell measurements," in *Proc. Joint Conference on Communications and Information (JCCI)*, Gangneung, Korea, May 2019.

[178] C. Navas-Merlo and J. C. Garcia-Escartin, "Detector blinding attacks on counterfactual quantum key distribution," *Quantum Inf. Process*, vol. 20, no. 6, p. 196, Jun. 2021.

[179] F. Zaman, Y. Jeong, and H. Shin, "Man in the middle attack in counterfactual quantum key distribution," in *Proc. Korea Information and Communication Society (KICS) Fall Conference*, Seoul, Korea, Nov. 2018.
[180] Z.-Q. Yin, H.-W. Li, W. Chen, Z.-F. Han, and G.-C. Guo, "Security of counterfactual quantum cryptography," *Phys. Rev. A*, vol. 82, no. 4, p. 042335, Oct. 2010.
[181] G. Brida, A. Cavanna, I. P. Degiovanni, M. Genovese, and P. Traina, "Experimental realization of counterfactual quantum cryptography," *Laser Phys. Lett.*, vol. 9, no. 3, p. 247, Jan. 2012.
[182] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, N.-L. Liu, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Satellite-based entanglement distribution over 1200 kilometers," *Nature*, vol. 549, no. 7670, pp. 43–47, Jun. 2017.
[183] H. Zhang, Z. Sun, R. Qi, L. Yin, G.-L. Long, and J. Lu, "Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states," *Photon. Res.*, vol. 11, no. 1, p. 83, Apr. 2022.
[184] B. P. Williams, R. J. Sadlier, and T. S. Humble, "Superdense coding over optical fiber links with complete Bell-state measurements," *Phys. Rev. Lett.*, vol. 118, no. 5, p. 050501, Feb. 2017.
[185] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-H. Liao, J. Yin, W.-Y. Li, Y. Cao, S.-K. Li, W.-Q. Liu, and et al., "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, Aug. 2017.
[186] M. Clouâtré, B. Kartal, S. Marano, P. L. Falb, and M. Z. Win, "Finite-time quantum reservoir engineering," in *Proc. IEEE International Conference on Communications (ICC)*, Montreal, Canada, Jun. 2025, pp. 1–6.

Saw Nang Paing received the B.E. degree in Computer Engineering and Information Technology from Mandalay Technology University (MTU), Myanmar, in 2019, and her Ph.D. in Electronics and Information Convergence Engineering from Kyung Hee University, South Korea, in Aug. 2025. Since Sep. 2025, she has been a Post-Doctoral Fellow with the Department of Electronics and Information Convergence Engineering, Kyung Hee University. Her research interests include distributed quantum networks, quantum communication, and quantum security.

Dr. Paing received the Best Paper award at KICS-Fall Conference on Communications in 2024. She served as a reviewer for IEEE TRANSACTIONS ON COMMUNICATIONS and several international conferences.

Fakhar Zaman received B.E. degree in Electrical Engineering from the National University of Sciences and Technology (NUST), Pakistan, in 2015 and Ph.D. degree in Electronics and Information Convergence Engineering from the Kyung Hee University (KHU), S. Korea, in 2023. During his Ph.D., he spent a year at the Massachusetts Institute of Technology (MIT) as an exchange visiting student. At MIT, he was with the Laboratory for Information and Decision Systems from September 2022 to August 2023.

Currently, he is a Senior Quantum Solutions Engineer at Q-CTRL, Australia. Before joining Q-CTRL, he served as a CSIRO Early Research Career (CERC) Fellow at Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia. His research interests include quantum-enhanced optimization, variational quantum algorithms, and hybrid quantum-classical machine learning.

Dr. Zaman received the Best Paper award at KICS-Fall Conference on Communications in 2019. He served as a reviewer for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS and several international conferences.

Uman Khalid received his B.S. degree in Electronics Engineering from the Ghulam Ishaq Khan (GIK) Institute, Topi, Pakistan, in 2015, and his Ph.D. in Electronics Engineering from Kyung Hee University, South Korea, in Feb. 2023. Since Mar. 2023, he has been a Post-Doctoral Fellow with the Department of Electronics and Information Convergence Engineering, Kyung Hee University. His research interests include quantum information science, quantum semantic communications, and quantum networks.

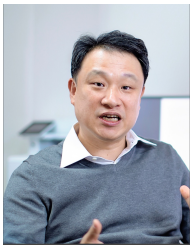
Trung Q. Duong (Fellow, IEEE) is a Canada Excellence Research Chair (CERC) and a Full Professor at Memorial University, Canada. He is also an adjunct professor at Queen's University Belfast, UK, a visiting professor at Kyung Hee University, South Korea, and an adjunct professor at Duy Tan University, Vietnam. His current research interests include wireless communications, quantum machine learning, and quantum optimization.

He is the Editor-in-Chief of IEEE Communications Surveys & Tutorials and an IEEE ComSoc Distinguished Lecturer. 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 a Fellow of the Engineering Institute of Canada (EIC), the Canadian Academy of Engineering (CAE), the Institution of Engineering and Technology (IET), 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 postdoctoral research at the Massachusetts Institute of Technology (MIT) from 2004 to 2006, he was with the Laboratory for Information Decision Systems (LIDS). In 2006, he joined the KHU, where he is currently a Professor in the Department of Electronic Engineering. His research interests include quantum information science, wireless communication, and machine intelligence. Dr. Shin received the IEEE Communications Society's Guglielmo Marconi Prize Paper Award and William R. Bennett Prize Paper Award. He served as the Publicity Co-Chair for the IEEE PIMRC and the Technical Program Co-Chair for the IEEE WCNC and the IEEE GLOBECOM. He was an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS LETTERS.