SCIENCE CHINA
Information Sciences

• Supplementary File •

# Supplementary Information for "Scalable and highly fault-tolerant circular quantum Byzantine agreement"

Chen-Xun WENG[1,2†], Ming-Yang LI[1,2†], Shi-Gen LI[1,2], Mengya ZHU[3], Xiao-Ran SUN[1,2], Hua-Lei YIN[2,1*] & Zeng-Bing CHEN[1,3*]

[1]*National Laboratory of Solid State Microstructures and School of Physics, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China*
[2]*School of Physics and Key Laboratory of Quantum State Construction and Manipulation (Ministry of Education), Renmin University of China, Beijing 100872, China*
[3]*MatricTime Digital Technology Co. Ltd., Nanjing 211899, China*

## Appendix A Key generation protocol

The KGP employed in our QBA protocol can be derived from any QKD protocol with two participants. We illustrate the steps of the discrete-modulated continuous-variable (DM-CV) KGP, adapted from the DM-CV QKD with homodyne detection [1] and heterodyne detection [2], and the asymmetric coding BB84 KGP, adapted from the asymmetric coding BB84 QKD protocol in Refs. [3, 4]. In addition, we give the calculation details of both KGPs in Section Appendix D. To complete a round of OTUH-QDS, three participants need to form correlated keys. The KGP involves the signer-forwarder and signer-verifier independently sharing an identical quantum key, and the verifier (CA in our QBA protocol) calculating the bit-wise XOR of the two keys. In the description below, we describe how two participants share the identical quantum keys, and the two participants are denoted as Alice (always CA) and Bob.

### Appendix A.1 DM-CV KGP

Here, we introduce the detailed steps of two DM-CV QKD protocols with homodyne detection and heterodyne detection, respectively.

**(a) Homodyne.**

*1. Preparation*: In each round, Alice prepares a coherent state $|\alpha e^{i\phi}\rangle$, where $\phi$ is uniformly randomly chosen from $\left\{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\right\}$. She then sends the state to the receiver, Bob.

*2. Measurement*: Upon receiving the state, Bob uniformly randomly chooses a quadrature from $\{\hat{p}, \hat{q}\}$ to measure and records the measurement outcome.

*3. Parameter estimation*: After $N$ rounds, they announce the measurement quadratures through the authenticated public channel, and Bob announces a subset of the measurement results in order to evaluate the security, i.e., to compute the secret key rate. If the rate is below zero, the protocol is aborted.

*4. Key generation*: If the protocol is not aborted, suppose Bob obtains $M$ outcomes labeled as $\boldsymbol{Z} = (z_1, \ldots, z_k, \ldots, z_M)$. Alice labels the four choices as $\{00, 10, 11, 01\}$. If the quadrature that Bob measures in a given round is $\hat{q}$, Alice sets her key bit $a_k$ as the first bit of the corresponding label. Otherwise, $a_k$ is set as the second bit. As for Bob, if the measurement outcome $z_k \in (-\infty, -\Delta)$, his key bit $b_k$ is set to 1, where $\Delta$ is a non-negative sifting parameter. If $z_k \in (\Delta, \infty)$, $b_k$ is set to 0. Otherwise, $b_k$ is assigned the value $\perp$. They then obtain their key strings $\boldsymbol{A} = (a_1, \ldots, a_M)$ and $\boldsymbol{B} = (b_1, \ldots, b_M)$.

*5. Error correction and privacy amplification*: After performing error correction and privacy amplification, they obtain the final key strings.

**(b) Heterodyne.**

*1. Preparation*: The preparation process is similar. In each round, Alice prepares a coherent state with random phases and sends the state to the receiver Bob.

*2. Measurement*: Instead of measuring a quadrature, Bob directly performs a POVM described by $\{E_\gamma = (1/\pi)\,|\gamma\rangle\langle\gamma| : \gamma \in \mathcal{C}\}$.

*3. Parameter estimation*: After $N$ rounds, they use a small subset of the data to compute the secret key rate and decide whether to abort the protocol.

*4. Key generation*: Suppose they obtain $M$ measurement outcomes recorded as $\boldsymbol{Z} = (z_1, \ldots, z_k, \ldots, z_M)$, where each $z_k$ has the form $|z_k|e^{i\theta_k}$. Alice records her bits directly as $\{0, 1, 2, 3\}$ according to her choices. Bob uses two sifting parameters, $\Delta_a$ and $\Delta_p$, separately for the amplitude and phase. The mapping rule from the measurement outcomes $\boldsymbol{Z}$ to his key string $\boldsymbol{B}$ is as follows:

* Corresponding author (email: hlyin@ruc.edu.cn, zbchen@nju.edu.cn)
† These authors contributed equally to this work.

$$b_k = \begin{cases} 0 & \text{if } \theta_k \in \left[\Delta_p, \frac{\pi}{2} - \Delta_p\right) \text{ and } |z_k| \geqslant \Delta_a, \\ 1 & \text{if } \theta_k \in \left[\frac{\pi}{2} + \Delta_p, \pi - \Delta_p\right) \text{ and } |z_k| \geqslant \Delta_a, \\ 2 & \text{if } \theta_k \in \left[\pi + \Delta_p, \frac{3\pi}{2} - \Delta_p\right) \text{ and } |z_k| \geqslant \Delta_a, \\ 3 & \text{if } \theta_k \in \left[\frac{3\pi}{2} + \Delta_p, 2\pi - \Delta_p\right) \text{ and } |z_k| \geqslant \Delta_a, \\ \perp & \text{if } \theta_k \text{ and } |z_k| \text{ do not satisfy any of the above conditions.} \end{cases}$$

*5. Error correction and privacy amplification*: After the process of error correction and privacy amplification, they obtain the final key strings.

## Appendix A.2 BB84 KGP

Alice and Bob select the $\mathsf{X}$ and $\mathsf{Z}$ bases with probabilities $q_x$ and $1 - q_x$, respectively. Key generation employs only those instances where both parties select the $\mathsf{X}$ basis. Phase-randomized laser pulses are transmitted, incorporating a two-decoy setting. Each pulse intensity is randomly chosen from the set $\mathcal{K} = \{\mu_1, \mu_2, \mu_3\}$, with probabilities $p_{\mu_1}$, $p_{\mu_2}$, and $p_{\mu_3} = 1 - p_{\mu_1} - p_{\mu_2}$, subject to the constraints $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geqslant 0$. The protocol proceeds in five phases described below.

*1. Preparation.* Alice randomly selects a bit value ($y_i$), a basis ($a_i \in \{\mathsf{X}, \mathsf{Z}\}$), and an intensity ($k_i \in \mathcal{K}$). A corresponding laser pulse is then prepared and sent to Bob.

*2. Measurement.* Bob independently selects a basis ($b_i \in \{\mathsf{X}, \mathsf{Z}\}$) and measures the received pulse. The four possible outcomes are $\{0, 1, \emptyset, \perp\}$, where 0 and 1 represent bit values, $\emptyset$ denotes no detection, and $\perp$ indicates a double-click event. Bob records the outcome as $y_i'$, assigning a random bit to $y_i'$ in the case of a double-click event.

*3. Basis reconciliation.* Alice and Bob exchange their basis and intensity choices through an authenticated public channel, identifying the sets $X_k$ and $\mathcal{Z}_k$ for each intensity $k \in \mathcal{K}$. The protocol continues only if $|X_k| \geqslant n_{X,k}$ and $|\mathcal{Z}_k| \geqslant n_{\mathcal{Z},k}$ for all $k$. Otherwise, they repeat steps 1 and 2. The total number of pulses sent by Alice is denoted as $N$.

*4. Generation of raw key and error estimation.* A raw key pair $(\mathbf{X}_A, \mathbf{X}_B)$ is generated by sampling $n_X = \sum_{k\in\mathcal{K}} n_{X,k}$ elements from $X = \cup_{k\in\mathcal{K}} X_k$. The number of bit errors ($m_{\mathcal{Z},k}$) in the $\mathcal{Z}_k$ sets are then determined, along with the number of vacuum ($s_{X,0}$) and single-photon ($s_{X,1}$) events in $(\mathbf{X}_A, \mathbf{X}_B)$, and the number of phase errors ($c_{X,1}$) in the single-photon events is also calculated. The protocol proceeds only if the phase error rate $\phi_X = c_{X,1}/s_{X,1}$ is below the threshold $\phi_{tol}$.

*5. Post-processing.* This phase involves error correction (revealing $\lambda_{EC}$ bits), error verification using two-universal hash functions, and final privacy amplification to generate the secret key pair.

## Appendix B OTUH-QDS

Achieving information-theoretic security in long message signing, the OTUH-QDS framework [5] utilizes one-time pads for encryption and LFSR-based Toeplitz hashing for signature generation. Here, we first present the construction of LFSR-based Toeplitz hashing, then we detail the two phases of OTUH-QDS and present its security subsequently.

## Appendix B.1 LFSR-based Toeplitz hashing

A hash function acts like a digital fingerprint for a document or message. Even a minor change in the input results in a significantly different hash value. Moreover, it is computationally infeasible to recover the original message from its hash value, meaning there are no known efficient algorithms to do so. This makes hash functions crucial for verifying data integrity and authenticity. LFSR-based Toeplitz hashing [6] offers a compelling combination of efficiency and security, which is employed in the OTUH-QDS protocol. We will now explain how to construct an LFSR-based Toeplitz hash function and demonstrate its application in calculating a hash value with length $\mathcal{N}$ for a given message with length $\mathcal{M}$.

The construction of this hash function begins by generating a random irreducible polynomial of order $\mathcal{N}$ in the Galois field GF(2): $p(x) = x^{\mathcal{N}} + p_{\mathcal{N}-1}x^{\mathcal{N}-1} + \cdots + p_1 x + p_0$ (see Ref. [7] for an efficient method). The polynomial's coefficients, excluding the term of order $\mathcal{N}$, are represented as an $\mathcal{N}$-bit vector $p = (p_{\mathcal{N}-1}, p_{\mathcal{N}-2}, \cdots, p_1, p_0)^T$, where $T$ means the transpose of vectors. Next, a binary $\mathcal{N}$-bit string obtained from a quantum information process with unconditional security is expressed as an $N$-dimensional vector $s = (s_{\mathcal{N}-1}, s_{\mathcal{N}-2}, \cdots, s_1, s_0)^T$ with each element is either 0 or 1. In the OTUH-QDS we employed here, this bit-string is the quantum key obtained through a KGP. These two vectors determine an LFSR-based Toeplitz hashing function $H_{s,p}$. We define the following $\mathcal{M}$ vectors:

$$\begin{aligned} H_1 &= s = (s_{\mathcal{N}-1}, s_{\mathcal{N}-2}, \cdots, s_1, s_0)^T, \\ H_2 &= (p * H_1, s_{\mathcal{N}-1}, \cdots, s_2, s_1)^T, \\ H_3 &= (p * H_2, p * H_1, \cdots, s_3, s_2)^T, \\ &\cdots \\ H_{\mathcal{M}} &= (p * H_{\mathcal{M}-1}, p * H_{\mathcal{M}-2}, \cdots, p * H_{\mathcal{M}-\mathcal{N}})^T, \end{aligned} \tag{B1}$$

where $*$ denotes the dot product between two vectors. Then, the LFSR-based Toeplitz hashing function $H_{s,p}$ is expressed as a $\mathcal{N} \times \mathcal{M}$ Toeplitz matrix $H_{\mathcal{N}\mathcal{M}} = (H_1, H_2, \cdots, H_{\mathcal{M}})$.

To calculate the hash value of a message, the message $m$ is first represented as an $\mathcal{M}$-bit vector. This vector is then multiplied by the Toeplitz matrix $H_{\mathcal{N}\mathcal{M}}$, yielding an $\mathcal{N}$-bit vector. Finally, a modulo-2 operation is applied to each element of the resulting vector. The final $\mathcal{N}$-bit vector obtained represents the hash value of the input message, ensuring data integrity and facilitating secure authentication protocols.

## Appendix B.2 Detailed steps and signature rate of OTUH-QDS

*1. Distribution phase.* The initial step involves the establishment of shared secret keys among the signer ($\mathbb{S}$), forwarder ($\mathbb{F}$), and verifier ($\mathbb{V}$) through a KGP. This is achieved through a QKD or quantum secret sharing protocol, resulting in correlated bit strings where the signer's key is the bitwise XOR of the forwarder's and verifier's keys. Specifically, each party possesses three key bit strings, denoted as $\{X_{\mathbb{S}}, X_{\mathbb{F}}, X_{\mathbb{V}}\}$, $\{Y_{\mathbb{S}}, Y_{\mathbb{F}}, Y_{\mathbb{V}}\}$, and $\{Z_{\mathbb{S}}, Z_{\mathbb{F}}, Z_{\mathbb{V}}\}$. Each string, comprised of $\mathcal{N}$ bits, fulfills the relations $X_{\mathbb{S}} = X_{\mathbb{F}} \oplus X_{\mathbb{V}}$, $Y_{\mathbb{S}} = Y_{\mathbb{F}} \oplus Y_{\mathbb{V}}$, and $Z_{\mathbb{S}} = Z_{\mathbb{F}} \oplus Z_{\mathbb{V}}$.

*2. Messaging phase.* This process begins with the signer generating an LFSR-based Toeplitz hash function [6] $H_{X_{\mathbb{S}},p_{\mathbb{S}}}$, which is determined by the secret key $X_{\mathbb{S}}$ and a local random string $p_{\mathbb{S}}$ which corresponds to the coefficients of a irreducible polynomial. The message to be signed is denoted as Mes with length $\mathcal{M}$. The signer calculates the $\mathcal{N}$-bit digest value $\mathrm{Dig} = H_{X_{\mathbb{S}},p_{\mathbb{S}}}(\mathrm{Mes})$ and encrypts it with $Y_{\mathbb{S}}$ to the signature for this message $\mathrm{Sig} = \mathrm{Dig} \oplus Y_{\mathbb{S}}$. The signer also encrypts $p_{\mathbb{S}}$ with $Z_{\mathbb{S}}$ to $p = p_{\mathbb{S}} \oplus Z_{\mathbb{S}}$ and subsequently transmits $\{\mathrm{Mes}, \mathrm{Sig}, p\}$ through an authenticated channel to the forwarder.

After receiving $\{\mathrm{Mes}, \mathrm{Sig}, p\}$, the forwarder transmits this data, along with key bit strings $\{X_{\mathbb{F}}, Y_{\mathbb{F}}, Z_{\mathbb{F}}\}$, to the verifier through an authenticated channel. Subsequently, the verifier forwards key bit strings $\{X_{\mathbb{V}}, Y_{\mathbb{V}}, Z_{\mathbb{V}}\}$ to the forwarder via the same channel. The forwarder then computes three new key bit strings: $K_{X_{\mathbb{F}}} = X_{\mathbb{F}} \oplus X_{\mathbb{V}}$, $K_{Y_{\mathbb{F}}} = Y_{\mathbb{F}} \oplus Y_{\mathbb{V}}$, and $K_{Z_{\mathbb{F}}} = Z_{\mathbb{F}} \oplus Z_{\mathbb{V}}$. Using $K_{Y_{\mathbb{F}}}$, the forwarder decrypts the signature to obtain the expected digest value, $\mathrm{Dig}_{\mathrm{f1}} = \mathrm{Sig} \oplus K_{Y_{\mathbb{F}}}$. Similarly, $K_{Z_{\mathbb{F}}}$ is used to decrypt $p$, revealing the string $p_{\mathbb{F}} = p \oplus K_{Z_{\mathbb{F}}}$. Next, the forwarder employs $K_{X_{\mathbb{F}}}$ and $p_{\mathbb{F}}$ to construct an LFSR-based Toeplitz hash function, which is then applied to the message Mes. This operation yields the actual digest value, $\mathrm{Dig}_{\mathrm{f2}}$. Finally, the forwarder compares the expected and actual digest values. If $\mathrm{Dig}_{\mathrm{f1}}$ and $\mathrm{Dig}_{\mathrm{f2}}$ are identical, the signature is deemed valid; otherwise, it is considered invalid. The forwarder then announces the result.

The verifier also performs an authentication process after receiving $\{\mathrm{Mes}, \mathrm{Sig}, p\}$ and the forwarder's keys $\{X_{\mathbb{F}}, Y_{\mathbb{F}}, Z_{\mathbb{F}}\}$ if the forwarder declares acceptance. The verifier calculates keys $K_{X_{\mathbb{V}}} = X_{\mathbb{V}} \oplus X_{\mathbb{F}}$, $K_{Y_{\mathbb{V}}} = Y_{\mathbb{V}} \oplus Y_{\mathbb{F}}$, and $K_{Z_{\mathbb{V}}} = Z_{\mathbb{V}} \oplus Z_{\mathbb{F}}$. Similar to the forwarder's actions, the verifier utilizes the $Y_{\mathbb{V}}$ and $Z_{\mathbb{V}}$ to decrypt Sig and $p$ respectively, and obtains the expected digest value and a string $p_{\mathbb{V}}$. With $K_{X_{\mathbb{V}}}$ and $p_{\mathbb{V}}$, the verifier constructs an LFSR-based Toeplitz hash function and computes the actual digest value of the message. Finally, the verifier compares the expected and actual digest values to determine the validity of the signature, authenticating the signature if they match and rejecting it otherwise. We note that in our QBA protocol, the verifier is referred to as the assistant CA. CA needs to inform the forwarder, i.e., a lieutenant, of the result of verification, thereby ensuring an independent verification of the message's authenticity and integrity.

The signature rate (SR) defined as the number of secure signatures that can be generated and checked per second, is determined by [5]

$$SR = KR/3n, \tag{B2}$$

where $KR$ is the quantum key rate between two participants and $n$ is the length of the signature, reflecting that signing an $n$-bit signature using OTUH-QDS with LFSR-based Toeplitz hashing requires $3n$ bits of quantum keys.

## Appendix B.3 Security of OTUH-QDS

The security of QDS relies on two essential properties: unforgeability and non-repudiation. This Section examines the security foundations of the OTUH-QDS protocol, demonstrating its security against both classical and quantum attacks.

In a KGP process, successful privacy amplification eliminates information leakage during key generation. Consequently, an attacker's strategy for guessing the $\mathcal{N}$-bit key is reduced to randomly generating an $\mathcal{N}$-bit string and comparing it to the true key. This trivial method yields a success probability of $2^{-\mathcal{N}}$. With this relation, we can proceed to investigate potential attack strategies against almost XOR universal$_2$ (AXU) hashing, specifically focusing on the LFSR-based Toeplitz hashing method described previously. A naive approach for an attacker involves randomly generating two bit strings, $t$ of length $\mathcal{M}$ and $h$ of length $\mathcal{N}$. If, by chance, $h$ coincides with the hash value of $t$ under the employed hash function, the attacker can intercept the transmitted message Mes and signature Sig and manipulate them to $\mathrm{Mes}' = \mathrm{Mes} \oplus t$ and $\mathrm{Sig}' = \mathrm{Sig} \oplus h$. Due to the properties of the hash function, the recipient would unknowingly accept the tampered message and signature pair as valid. The success probability of this approach is only $2^{-\mathcal{N}}$. However, the inherent information leakage during key generation presents the attacker with two potential avenues for compromising the system: attempting to guess the key $Key$ that defines the hashing function based on the information leakage, or endeavouring to derive this key from the intercepted signature. As demonstrated in Ref. [8], a specific property of the LFSR-based Toeplitz hash function restricts the number of viable guesses for $Key$ to be within the range of $\mathcal{M}/\mathcal{N}$. Furthermore, considering the attacker's awareness of the chosen polynomial's irreducible nature, the success probability of this guessing strategy can be expressed as:

$$p_{\mathrm{att}} = \frac{\mathcal{M}}{\mathcal{N}} P[\text{guess } Key \mid p_g \text{ is irreducible}], \tag{B3}$$

where $P[\cdot]$ denotes the probability of an event and $p_g$ represents the attacker's chosen irreducible polynomial. According to the characteristics of GF(2), there more than $2^{\mathcal{N}-1}/\mathcal{N}$ irreducible polynomials of order $\mathcal{N}$. Thus, we have $P[\text{is irreducible}] \geqslant \frac{2^{\mathcal{N}-1}/\mathcal{N}}{2^{\mathcal{N}}} = 1/2\mathcal{N}$. Leveraging Bayes' theorem, we can establish an upper bound for $p_{\mathrm{att}}$:

$$\begin{aligned} p_{\mathrm{att}} &= \frac{\mathcal{M}}{\mathcal{N}} \cdot \frac{P[\text{guess } Key]}{P[p_g \text{ is irreducible}]} \\ &= \frac{\mathcal{M}}{\mathcal{N}} \cdot \frac{P(Key|\mathcal{B})}{P[p_g \text{ is irreducible}]} \\ &\leqslant \frac{\mathcal{M}}{\mathcal{N}} \cdot \frac{2^{-\mathcal{N}}}{1/2\mathcal{N}} = \mathcal{M} \cdot 2^{1-\mathcal{N}} = \varepsilon_{\mathrm{U}}(\mathcal{M}, \mathcal{N}). \end{aligned} \tag{B4}$$

This upper bound is a function of the message and signature lengths, as $\mathcal{N}$ is dependent on $\mathcal{N}$. It is obvious that the probability of the attacker successfully guessing the other two keys, $Y$ and $Z$, which are employed for encryption, is also constrained by $\varepsilon_{\mathrm{U}}(\mathcal{M},\mathcal{N})$. Furthermore, the alternative strategy of deriving the key $X$ from the intercepted signature also necessitates correctly guessing the key responsible for encrypting the coefficients of the irreducible polynomial. Consequently, the success probability associated with this approach remains confined by the same upper bound, $\varepsilon_{\mathrm{U}}(\mathcal{M},\mathcal{N})$. Overall, the optimal attack strategy against LFSR-based Toeplitz hashing focuses on guessing the key string that either determines the hashing function or encrypts the polynomial used within it. Consequently, regardless of the specific approach employed by the attacker, the upper bound of the failure probability for authentication schemes remains $\varepsilon_{\mathrm{U}}(\mathcal{M},\mathcal{N}) = \mathcal{M}\cdot 2^{1-\mathcal{N}}$.

Unforgeability ensures that an attacker cannot create a valid signature for a tampered message. A successful forgery would occur if the attacker could find a tampered message that, after one-time pad decryption and one-time AXU hashing, yields the same hash value as the original message, thereby leading to its acceptance. However, as previously analyzed, even considering potential information leakage during key generation, the probability of a successful forgery remains negligible. Specifically, the probability of successful forgery $\varepsilon_{\mathrm{for}}$ is directly equivalent to the failure probability of the hashing function, leading to the expression:

$$\varepsilon_{\mathrm{for}}(\mathcal{M},\mathcal{N}) = \varepsilon_{\mathrm{U}}(\mathcal{M},\mathcal{N}) = \mathcal{M}\cdot 2^{1-\mathcal{N}}. \tag{B5}$$

Non-repudiation guarantees that the signer cannot deny having signed a message or claim forgery. This QDS protocol is inherently secure against repudiation as the forwarder and verifier can recover the keys used by the signer through the authenticated classical channel, which is impervious to the signer's influence. The forwarder and verifier can then independently obtain the same actual and expected hash results, leading to the same decision. Therefore, neglecting negligible errors inherent in classical communication channels, the probability of successful repudiation is effectively zero.

## Appendix C Security analysis of circular QBA

A Byzantine agreement is capable of reaching a consensus when and only when it satisfies the two **IC** Byzantine conditions. Our security analysis demonstrates that every lieutenant receives an identical set of input messages ($\mathbf{IC}_1$). Furthermore, if the commanding general is loyal, the output will correspond to the commanding general's order ($\mathbf{IC}_2$). Unforgeability of QDS ensures that no one can tamper with the message, and non-repudiation ensures that the signer cannot deny the fact that he signs the message. These properties ensure the security of our QBA protocol.

We assume that each message $m_j$ has a length of $m$ bits, while each signature $\sigma_j$ or $\sigma^i_{j\to j+1}$ ($j\in\mathbb{Z}^+_{N-1}$) has a length of $n$ bits. Assuming a total of $N$ players, with $f$ of them being dishonest, we let $\tau_h$ and $\tau_d$ represent the set of indices corresponding to the honest and dishonest lieutenants respectively:

$$\begin{aligned}\tau_h &= \{j_h\in\mathbb{Z}^+_{N-1} \mid R_{j_h} \text{ is honest}\},\\ \tau_d &= \{j_d\in\mathbb{Z}^+_{N-1} \mid R_{j_d} \text{ is dishonest}\}.\end{aligned} \tag{C1}$$

The number of honest and dishonest lieutenants, denoted as $|\tau_h| = N_h$ and $|\tau_d| = N_d$ respectively, are dependent on whether the commanding general is loyal or disloyal. Thus, we will consider two scenarios based on the loyalty of the commanding general.

The security analysis is constructed as follows. In Sec. Appendix C.1, we analyze the security of circular gathering phase which is the building block of our circular QBA. In Sec. Appendix C.2 and Appendix C.3 we then prove the security of our protocol in scenarios where the commanding general is loyal and disloyal respectively. Finally, we analyze the overall security and the fault-tolerance ability of our circualr QBA in Sec. Appendix C.4.

### Appendix C.1 Security of circular gathering phase with malicious lieutenants

The rounds of circular gathering started by disloyal lieutenant need not to be considered since what disloyal lieutenants obtain and how they generate the output is irrelevant to two **IC** conditions. Assuming $R_1$ is loyal, the security analysis of $R_1$'s circular gathering serves as a representative example, as the analysis readily generalizes to the circular gathering initiated by other lieutenants due to their symmetrical roles. Figure C1(a) highlights a single step where lieutenant $R_j$ transmits messages and signatures to $R_{j+1}$ ($j\in\mathbb{Z}^+_{N-1}$) in the circular gathering of $R_1$.

Within a round initiated by an honest lieutenant, each disloyal lieutenant has one opportunity to sign and one to forward information. When signing, a disloyal lieutenant $R_{j_d}$ could attempt one of two forgery strategies when transmitting messages to an honest lieutenant $R_{j_h}$: (1) substituting the message-signature pair $\{m_k;\sigma_k\}$ with a forged pair $\{m^*_k;\sigma^*_k\}$ ($k\leqslant j$), where $\sigma^*_k$ is a forged signature corresponding to $m^*_k$, or (2) substituting only the original message $m_k$ with a forged message $m^*_k$. These two strategies are illustrated in Fig. C1(b). The assistant CA, by preserving the original signatures and quantum keys recorded during the order distribution phase, effectively obstructs both strategies. CA prevents the first by comparing all signatures against the original records. The second is prevented by verifying the consistency between $m^*_k$ and $\sigma_k$ using one-time universal hashing via quantum keys recorded during order distribution. While the messages themselves appear unchanged, it's important to note that the process $R_{j_d}$ may change some of the signatures generated during the circular gathering phase, specifically those within the set $\{\sigma^1_{1\to 2},\ldots,\sigma^1_{j_d-1\to j_d}\}$. This way of cheating is also prevented since CA will compare them with the record of the previous OTUH-QDS in this circular gathering.

Therefore, the key challenge lies in analyzing the potential for forgery when a disloyal lieutenant acts as a forwarder. We first analyze an information delivery step. As shown in Fig. C1(a), $R_j$ signs the total information, which are $j$ pieces of messages ($\{m_1,m_2,\cdots,m_j\}$) and $2j-1$ pieces of signatures ($\{\sigma_1,\sigma_2,\cdots,\sigma_j\}$ and $\{\sigma^1_{1\to 2},\sigma^1_{2\to 3},\cdots,\sigma^1_{j-1\to j}\}$), with the signature $\sigma^1_{j\to j+1}$, and then sends all of them to $R_{j+1}$. The length of total transmitted information from $R_j$ to $R_{j+1}$ is $L_j = jm+(2j-1)n$, and the length of signature $\sigma^1_{j\to j+1}$ is $n$. So the probability of successful forgery in this QDS process is then expressed as:

$$\varepsilon^{\mathrm{D}}_j = \varepsilon_{\mathrm{for}}(L_j,n). \tag{C2}$$

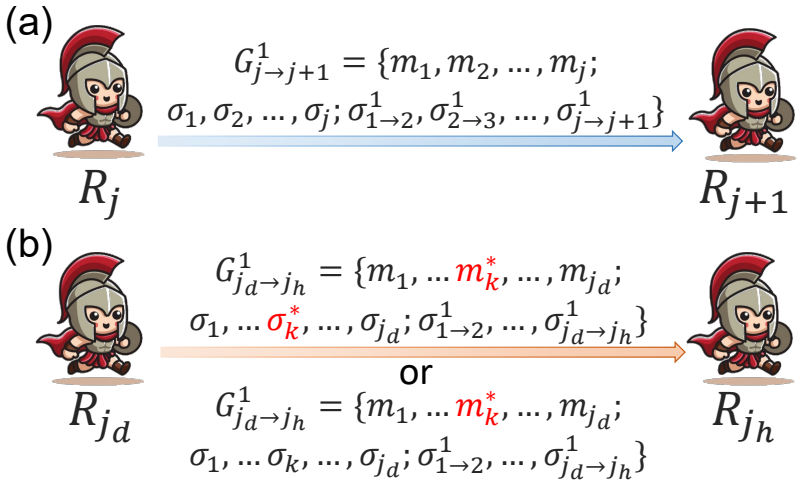


**Figure C1** (a) The information delivery step between $R_j$ and $R_{j+1}$ within $R_1$'s circular gathering. The information conveyed from $R_i$ to $R_{j+1}$ comprises $j$ message segments ($\{m_1, m_2, \cdots, m_i\}$) along with $2j-1$ signature elements ($\{\sigma_1, \sigma_2, \cdots, \sigma_j\}$ and $\{\sigma^1_{1\to 2}, \sigma^1_{2\to 3}, \cdots, \sigma^1_{j-1\to j}\}$), resulting in an overall length expressed as $L_j = jm + (2j-1)n$. (b) A disloyal lieutenant $R_{j_d}$, acting as a signer, may attempt to substitute either the original message $m_k$ with a forged message $m^*_k$, or the message-signature pair $\{m_k, \sigma_k\}$ with a forged pair $\{m^*_k, \sigma^*_k\}$, where $k \leqslant j$, and sends to a loyal lieutenant $R_{j_h}$. Both are prevented by CA, who retains a record of the original signatures and corresponding quantum keys in the order distribution phase. Malicious signers may also change the signatures $\{\sigma^1_{1\to 1}, \cdots, \sigma^1_{j_d-1\to j_d}\}$, however, CA also compares them with previous records, preventing this way of cheating. Icons Copyright 2026 Vecteezy.

According to Section Appendix B.3, as $L_j$ increases, the probability of successfully forging increases since the signature's length is fixed to $n$. This will be used to provide an upper bound for the failure probability of a circular gathering round.

A complete round of circular gathering involves $N-1$ information delivery steps and includes $N-1$ lieutenants. Since only malicious lieutenants would attempt forgery, and to guarantee that $R_1$ receives the correct messages, no QDS forgery should occur in any of the information delivery steps. Therefore, the probability of a successful circular gathering initiated by $R_1$ is calculated as follows

$$P_{\mathrm{c}}^{R_1}(\tau_d) = \prod_{j_d\in\tau_d} (1-\varepsilon^{\mathrm{D}}_{j_d}) = \prod_{j_d\in\tau_d} \left[1-\varepsilon_{\mathrm{for}}(L_{j_d}, n)\right]. \tag{C3}$$

Our goal is to guarantee that all loyal lieutenants receive the same set of messages. Therefore, we focus on the circular gatherings initiated by loyal lieutenants, denoted by $R_{j_h}$ ($j_h \in \tau_h$). All such gatherings must be successful. Moreover, $P_{\mathrm{c}}^{R_1}(\tau_d)$ is influenced by the permutations of the dishonest lieutenants within the gathering circle. Specifically, because longer messages are easier to forge, a dishonest lieutenant positioned later in the sequence poses a greater security risk. To establish a rigorous upper bound on the probability of failure, we consider the worst-case scenario for $R_1$, where $P_{\mathrm{c}}^{R_1}(\tau_d)$ is minimized. We then use this minimized value as the probability for the success of circular gatherings initiated by all loyal lieutenants. This approach is conservative, as the worst-case scenario for $R_1$ might not be the worst case for other loyal lieutenants. This simplification, however, allows for a stricter security analysis. Consequently, the probability of all circular gatherings to be successful is:

$$\begin{aligned} P_{\mathrm{c}}(\tau_d) = \prod_{j_h\in\tau_h} P_{\mathrm{c}}^{R_{j_h}}(\tau_d) &\geqslant \left[\inf_{\substack{\tau_d\subset\mathbb{Z}^+_{N-1}\\|\tau_d|=N_d}} P_{\mathrm{c}}^{R_1}(\tau_d)\right]^{N_h} = \left\{\inf_{\substack{\tau_d\subset\mathbb{Z}^+_{N-1}\\|\tau_d|=N_d}} \prod_{j_d\in\tau_d}\left[1-\varepsilon_{\mathrm{for}}(L_{j_d}, n)\right]\right\}^{N_h} \\ &\geqslant \left\{\inf_{\substack{\tau_d\subset\mathbb{Z}^+_{N-1}\\|\tau_d|=N_d}} \left[1-\sum_{j_d\in\tau_d}\varepsilon_{\mathrm{for}}(L_{j_d}, n)\right]\right\}^{N_h} = \left[1-\sup_{\substack{\tau_d\subset\mathbb{Z}^+_{N-1}\\|\tau_d|=N_d}} \sum_{j_d\in\tau_d}\varepsilon_{\mathrm{for}}(L_{j_d}, n)\right]^{N_h}, \end{aligned} \tag{C4}$$

where the infimum (inf) and supremum (sup) are taken over all possible sets $\tau_d$ (a subset of $\mathbb{Z}^+_{N-1}$ with $N_d$ elements), representing all possible sequences dishonest lieutenants. The second scaling holds because $\varepsilon_{\mathrm{for}}(L_j, n)$ is exceedingly small for all $j$. Therefore, we can disregard terms involving the product of two or more of these small probabilities, as their contribution to the succeeding probability is negligible.

For the convenience of numerical simulations and the setting of experimental parameters, we can introduce further scaling. The longest message to be signed in a circular gathering has a length of $L_{N-1} = (N-1)m + (2N-3)n$, resulting in the largest probability of forgery $\varepsilon_{\mathrm{for}}(L_{N-1}, n)$. So we have $\varepsilon_{\mathrm{for}}(L_{j_d}, n) \leqslant \varepsilon_{\mathrm{for}}(L_{N-1}, n)$ ($\forall j_d \in \tau_d$). We introduce the scaling as follows:

$$\sup_{\substack{\tau_d\subset\mathbb{Z}^+_{N-1}\\|\tau_d|=N_d}} \sum_{j_d\in\tau_d} \varepsilon_{\mathrm{for}}(L_{j_d}, n) < N_d \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n), \tag{C5}$$

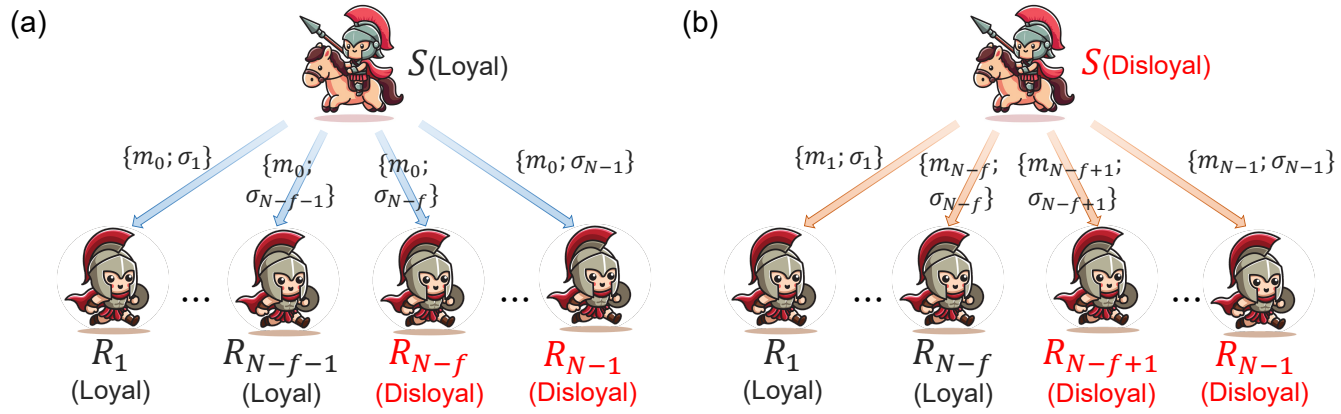


**Figure C2** The order distribution phases of two cases. (a) Case I: Loyal commanding general. In this case, the same message is distributed. The disloyal lieutenants will try to forge the correct messages. Loyal $S$ broadcasts the same message $m_0$, signed with individual signatures $\sigma_j$ ($j \in \mathbb{Z}^+_{N-1}$), to each lieutenant. (b) Case II: Disloyal commanding general. With a disloyal commanding general and $f-1$ disloyal lieutenants, the order distribution phase involves the broadcast of $N-1$ distinct messages. The goal of malicious players is to maximize uncertainty, which is achieved by the distribution of these distinct messages. Icons Copyright 2026 Vecteezy.

and the probability of all circular gathering to be successful is then (Note that $N_h + N_d = N - 1$):

$$\begin{aligned} P_{\mathrm{c}}(\tau_d) &\geqslant [1 - N_d \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n)]^{N_h} \\ &\geqslant 1 - N_d N_h \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n) \\ &= 1 - N_d \left(N - N_d - 1\right) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n) \\ &= P_{\mathrm{c}}^{\mathrm{inf}}(N_d) = 1 - \varepsilon_{\mathrm{c}}^{\mathrm{sup}}(N_d). \end{aligned} \tag{C6}$$

The second scaling also holds since $\varepsilon_{\mathrm{for}}(L_{N-1}, n) \ll 1$. Here, $P_{\mathrm{c}}^{\mathrm{inf}}(N_d)$ represents the lower bound on the probability of successful circular gatherings, while $\varepsilon_{\mathrm{c}}^{\mathrm{sup}}(N_d) = N_d(N - N_d - 1) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n)$ represents the upper bound on the probability of failure in any circular gathering. Both are functions of $N_d$, the number of disloyal lieutenants.

## Appendix C.2 Case I: Loyal commanding general

We first analyze the scenario where the commanding general $S$ is loyal and the number of disloyal lieutenants is $f$. In this case, we have $N_d = f$ and $N_h = N - f - 1$. During the order distribution phase shown in Fig. C2(a), the loyal $S$ signs the same message $m_0$ with signature $\sigma_i$ ($i \in \mathbb{Z}^+_{N-1}$) and transmits them to lieutenants, with CA acting as the verifier in OTUH-QDS. If the QDS between $S$, $R_i$, and CA is successful, the probability of successful forgery is bounded by $\varepsilon_{\mathrm{o}}^{S \to R_i} = \varepsilon_{\mathrm{for}}(m, n)$. In the order distribution phase, forgery can only occur with a very low probability in any QDS with a disloyal lieutenant since $S$ and CA are honest. Therefore, the probability of a successful order distribution phase is:

$$\begin{aligned} P_{\mathrm{Io}} &= \prod_{j_d \in \tau_d} (1 - \varepsilon_{\mathrm{o}}^{S \to R_{j_d}}) = [1 - \varepsilon_{\mathrm{for}}(m, n)]^{N_d} \\ &\geqslant 1 - N_d \cdot \varepsilon_{\mathrm{for}}(m, n) = 1 - f \cdot \varepsilon_{\mathrm{for}}(m, n) \\ &= 1 - \varepsilon_{\mathrm{Io}}. \end{aligned} \tag{C7}$$

Here, $\varepsilon_{\mathrm{Io}} = f \cdot \varepsilon_{\mathrm{for}}(m, n)$ means the probability of failure in the order distribution phase in case I.

In the circular gathering phase, the protocol must ensure that all $N - f - 1$ loyal lieutenants receive the same set of messages, even if the $f$ disloyal lieutenants attempt to disrupt the process. In Case I, the number of disloyal lieutenants is $N_d = f$. As analysed in Sec. Appendix C.1, the probability of a successful circular gathering phase is expressed by:

$$\begin{aligned} P_{\mathrm{Ic}} \geqslant P_{\mathrm{c}}^{\mathrm{inf}}(f) &= 1 - f\left(N - f - 1\right) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n) \\ &= 1 - \varepsilon_{\mathrm{Ic}}, \end{aligned} \tag{C8}$$

where $\varepsilon_{\mathrm{Ic}} = f\left(N - f - 1\right) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n)$ is the probability of failure in the circular gathering phase in case I.

As a result, in case I where the commanding general is honest, the probability of a successful operation of the whole protocol is:

$$P_{\mathrm{I}} = P_{\mathrm{Io}} \cdot P_{\mathrm{Ic}} = (1 - \varepsilon_{\mathrm{Io}})(1 - \varepsilon_{\mathrm{Ic}}) \geqslant 1 - (\varepsilon_{\mathrm{Io}} + \varepsilon_{\mathrm{Ic}}), \tag{C9}$$

since the failure probabilities $\varepsilon_{\mathrm{Io}}$ and $\varepsilon_{\mathrm{Ic}}$ are both small. Therefore, the security parameter, which stands for the failure probability of case I is then:

$$\begin{aligned} \varepsilon_{\mathrm{I}} &= \varepsilon_{\mathrm{Io}} + \varepsilon_{\mathrm{Ic}} \\ &= f \cdot \varepsilon_{\mathrm{for}}(m, n) + f\left(N - f - 1\right) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n) \\ &= f\left[\varepsilon_{\mathrm{for}}(m, n) + (N - f - 1) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n)\right]. \end{aligned} \tag{C10}$$

## Appendix C.3 Case II: Disloyal commanding general

In this scenario, there are $N_d = f - 1$ disloyal lieutenants and $N_h = N - f$ honest lieutenants. The order distribution phase is depicted in Fig. C2(b). A disloyal commanding general aims to disrupt the protocol and mislead the honest lieutenants, sending $N - 1$ different messages during the order distribution phase. In this context, forging QDS is irrelevant, as the malicious actors' objective is simply to create maximal confusion. Forging a distributed message by substituting it with another is functionally equivalent to the disloyal commanding general having initially transmitted the substituted message.

The analysis of the circular gathering phase is similar to the previous case. Given $N_d = f - 1$, as per the analysis in Sec. Appendix C.1, the probability of a successful circular gathering phase of case II $P_{\mathrm{IIc}}$, and therefore the QBA protocol's success probability in this scenario $P_{\mathrm{II}}$, is:

$$\begin{aligned} P_{\mathrm{II}} = P_{\mathrm{IIc}} &\geqslant P_{\mathrm{c}}^{\mathrm{inf}}(f-1) \\ &= 1 - (f-1)(N-f) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n) \\ &= 1 - \varepsilon_{\mathrm{II}}, \end{aligned} \tag{C11}$$

where

$$\varepsilon_{\mathrm{II}} = (f-1)(N-f) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n), \tag{C12}$$

representing the failure probability of case II.

## Appendix C.4 Overall security

Obviously, the two scenarios where the commanding general is loyal and disloyal are complementary. To provide a stricter bound, the security parameter of our QBA scheme, denoting the failure probability of protocol, is expressed as follows:

$$\begin{aligned} \varepsilon_{\mathrm{QBA}} &= \max\{\varepsilon_{\mathrm{I}}, \varepsilon_{\mathrm{II}}\} \\ &= \max\{f\left[\varepsilon_{\mathrm{for}}(m,n) + (N-f-1) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n)\right], (f-1)(N-f) \cdot \varepsilon_{\mathrm{for}}(L_{N-1}, n)\}. \end{aligned} \tag{C13}$$

## Appendix D Simulation details

In this part, we give the simulation details of circular QBA networks using different QKG protocols for the OTUH-QDS process.

## Appendix D.1 Satellite-to-Ground Channel

Here, we first present the numerical analysis for the satellite-to-ground link, focusing on the factors affecting laser signal transmission, namely attenuation, beam distortion, and deflection. This model is also employed in Ref. [9]. Within this framework, the receiver detects incoming photons, considering both the channel's transparency and environmental mode. The influence of the environmental modes, which cause variations in measurement outcomes, is quantified by the excess noise parameter

$$\xi = \frac{(\Delta q_{\mathrm{obs}})^2}{(\Delta q_{\mathrm{vac}})^2} - 1, \tag{D1}$$

where $(\Delta q_{\mathrm{obs}})^2$ and $(\Delta q_{\mathrm{vac}})^2$ stand for the variances of the $q$ quadrature for the observed states and the vacuum states, respectively.

Considering the signal loss due to photon absorption within the atmosphere, this effect is characterized by the atmospheric transmittance due to extinction, which is denoted by the Beer-Lambert equation [10]

$$\eta_{\mathrm{ext}}(h, \theta) = \exp\left\{-\int_0^z \alpha[h(y, \theta)]\, dy\right\}. \tag{D2}$$

Here, $\alpha(h) = \alpha_0 e^{-h/\tilde{h}}$ denotes the altitude-dependent extinction coefficient, where $h$ is the satellite's altitude and $\tilde{h} = 6600$ m is a scale parameter. Considering both aerosol and molecular scattering, the extinction coefficient at sea level, $\alpha_0$, is $4 \times 10^{-7}$ m$^{-1}$ for laser with 1550 nm-wavelength, and $5 \times 10^{-6}$ m$^{-1}$ for laser with 800 nm-wavelength.

Beyond simple absorption, the non-uniform structure of the atmosphere in both spatial and temporal dimensions leads to phenomena such as beam broadening and wandering [10, 11]. For short exposure times, spatial turbulence distorts the beam, causing a broadened beam waist ($W_{\mathrm{ST}}$) and a shifted beam center [12]. A common approximation for the beam waist under turbulence is denoted by [13]:

$$W_{\mathrm{ST}}^2(z) = W_0^2\left(1 + \frac{z^2}{Z_0^2}\right) + \frac{35.28 z^2}{k^2 r_s^2}\left[1 - 0.26\left(\frac{r_s}{W_0}\right)^{1/3}\right]^2, \tag{D3}$$

where $W_0$ is the initial beam waist, $z$ is the propagation distance, $Z_0 = kW_0^2/2$ is the Rayleigh distance, $k$ is the wavenumber, and $r_s$ is a measure of turbulence intensity. The turbulence intensity factor $r_s$ is determined by the refractive index structure parameter $C_n^2(h)$

$$r_s = \left[0.42k^2 \int_0^L C_n^2(h(z, \theta_z))\left(\frac{L-z}{L}\right)^{5/3} dz\right]^{-3/5}, \tag{D4}$$

where $L$ is the total path length and $C_n^2(h)$ follows the Hufnagel-Valley model [14]

$$C_n^2(h) = 8.1481 \times 10^{-56} v^2 h^{10} e^{-h/1000} + 2.7 \times 10^{-16} e^{-h/1500} + C_0 e^{-h/100}. \tag{D5}$$

Here, $v$ means the wind speed (21 m/s in our simulation), $h$ is altitude, and $C_0 = 9.6 \times 10^{-14}\mathrm{m}^{-2/3}$ is a constant [15].

Over longer periods, the deviation $r = \sqrt{x^2 + y^2}$ of the beam center from the intended path is described by a random distribution

$$P(x, y) = \frac{1}{2\pi\sigma_r^2} \exp\left(-\frac{x^2 + y^2}{2\sigma_r^2}\right), \tag{D6}$$

The variance $\sigma_r^2$ accounts for both atmospheric effects and pointing errors, defined as $\sigma_r^2 = (L\theta_p)^2 + \sigma_{\mathrm{TB}}^2$. Here, $\theta_p$ is the pointing error angle, and $\sigma_{\mathrm{TB}}^2$ is the variance due to atmospheric effects. The coupling efficiency $\eta(r)$ for a beam displaced by $r$ is described by [16]:

$$\eta(r) = \frac{2}{\pi W^2} \exp\left(-2\frac{r^2}{W^2}\right) \cdot \int_0^a \rho \exp\left(-2\frac{\rho^2}{W^2}\right) I_0\left(\frac{4r\rho}{W^2}\right) d\rho, \tag{D7}$$

where $W = W_{ST}(z = L)$ is the beam waist, $a$ is the receiver aperture radius, and $I_n(x)$ is the n-th order modified Bessel function. Additionally, we use a more efficient approximate analytical expression of $\eta(r)$, which is

$$\eta(r) = \eta_0 \exp\left[-\left(\frac{r}{R}\right)^{\lambda}\right]. \tag{D8}$$

In the expression, we have

$$\begin{aligned}
&\eta_0 = 1 - \exp\left[-2\frac{a^2}{W^2}\right], \\
&\lambda = \left[\ln\left(\frac{2T_0^2}{1 - \exp[-4\frac{a^2}{W^2}] I_0\left(4\frac{a^2}{W^2}\right)}\right)\right]^{-1} \times 8\frac{a^2}{W^2} \frac{\exp\left[-4\frac{a^2}{W^2}\right] I_1\left(4\frac{a^2}{W^2}\right)}{1 - \exp[-4\frac{a^2}{W^2}] I_0\left(4\frac{a^2}{W^2}\right)}, \\
&R = a\left[\ln\left(\frac{2T_0^2}{1 - \exp[-4\frac{a^2}{W^2}] I_0\left(4\frac{a^2}{W^2}\right)}\right)\right]^{-\frac{1}{\lambda}}.
\end{aligned} \tag{D9}$$

## Appendix D.2 DM-CV KGP

Additionally, excess noise in DM-CV type KGP is due to channel noise (scintillation, ambient light) and detection noise (device imperfections, electronic noise). Channel noise fluctuates based on environmental conditions and can be approximated by stray light power. Detection noise arises from inherent device flaws. Total excess noise is given by $\xi = \xi_{\mathrm{ch}} + \xi_{\mathrm{det}}/\eta$ [17]. Notably, heterodyne detection noise is twice that of homodyne detection [9].

### Appendix D.2.1 *Key Rate Estimation for Heterodyne Detection*

The key rate estimation in this section refers to the numerical method presented in [18, 19]. The entire system consists of three parties: Alice, Bob and Eve. The environment Eve ensures that the combined system forms a global pure state. We divide Alice's system into two parts: a measurement result register $Z$ and a remaining quantum state $A$. For the secure key rate, which is mainly given by the conditional von Neumann entropy $H(Z|E)$, we have:

$$H(Z|E) = H(ZE) - H(E),$$

Since the global state $ZABE$ is pure, the von Neumann entropy of a subsystem is equal to the entropy of its complement. Thus, we can write

$$H(Z|E) = H(ZE) - H(E) = H(AB) - H(ZAB),$$

Based on [19], the conditional entropy can be expressed as a quantum relative entropy

$$H(Z|E) = D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB}))),$$

where $D(\rho||\sigma) = \mathrm{Tr}(\rho\log\rho) - \mathrm{Tr}(\rho\log\sigma)$ is the quantum relative entropy. $\mathcal{G}$ represents the measurement operation and $\mathcal{Z}$ named the pinching channel. For heterodyne detection, the measurement $\mathcal{G}(\rho) = K\rho K^\dagger$ performed by Bob in the protocol can be described by Kraus operators

$$K = \sum_{z=0}^{3} |z\rangle_Z \otimes \mathbb{1}_A \otimes (\sqrt{R_z})_B,$$

where $|z\rangle_R$ represents the measurement outcome in a classical register, $\mathbb{1}_A$ is the identity operator on Alice's system, and $(\sqrt{R_z})_B$ acts on Bob's system. The projection operator $R_z$ is given by:

$$R_z = \frac{1}{\pi} \int_{\Delta_a}^{\infty} d\gamma \int_{z\pi/2+\Delta_p}^{(z+1)\pi/2-\Delta_p} \gamma |\gamma e^{i\theta}\rangle \langle\gamma e^{i\theta}| \, d\theta.$$

Here, $|\gamma e^{i\theta}\rangle$ denotes a coherent state. The parameters $\Delta_a$ and $\Delta_p$ define the integration range for amplitude and phase, respectively. The corresponding pinching channel $\mathcal{Z}(\rho)$ can be represented using projection operators $Z_j = |j\rangle\langle j| \otimes \mathbb{1}_{AB}$ as:

$$\mathcal{Z}(\rho) = \sum_{j=0}^{3} Z_j \rho Z_j.$$

To determine the lower bound of the key rate, we need to find the minimum relative entropy over all possible states $\rho_{AB}$ that satisfy certain constraints. Considering error correction, the asymptotic key rate can be expressed as:

$$R^{\infty} = \min_{\rho_{AB}\in S} D(\mathcal{G}(\rho_{AB})||\mathcal{Z}[\mathcal{G}(\rho_{AB})]) - p_{\text{pass}}\delta_{EC}.$$

The set $S$ of allowed states $\rho_{AB}$ must satisfy the following constraint conditions, derived from randomly sampled and publicly announced measurement data [1, 2]

$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{q})] = p_x \langle\hat{q}\rangle_x, \tag{D10}$$
$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{p})] = p_x \langle\hat{p}\rangle_x, \tag{D11}$$
$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{n})] = p_x \langle\hat{n}\rangle_x, \tag{D12}$$
$$\text{Tr}[\rho_{AB}(|x\rangle\langle x|_A \otimes \hat{d})] = p_x \langle\hat{d}\rangle_x. \tag{D13}$$

Here, $p_x$ is the probability of Alice sending the corresponding quantum state $|x\rangle$, which is set to $p_x = 0.25$. The expectation values are given by:

$$\langle\hat{q}\rangle_x = \sqrt{2\eta}\text{Re}(\alpha_x), \tag{D14}$$
$$\langle\hat{p}\rangle_x = \sqrt{2\eta}\text{Im}(\alpha_x), \tag{D15}$$
$$\langle\hat{n}\rangle_x = \eta|\alpha_x|^2 + \frac{\eta\xi}{2}, \tag{D16}$$
$$\langle\hat{d}\rangle_x = \eta[\alpha_x^2 + (\alpha_x^*)^2]. \tag{D17}$$

In these equations, $\eta$ represents the detection efficiency, $\xi$ is the electronic noise, and $\alpha_x$ is the complex amplitude of the coherent state prepared by Alice. Operators $\hat{q}$ and $\hat{p}$ are the quadrature operators, $\hat{n}$ is the photon number operator, and $\hat{d}$ is related to the second moment of the quadratures. Additionally, since Alice prepares the quantum states for Bob, Alice's reduced density matrix should have a fixed distribution:

$$\text{Tr}_B[\rho_{AB}] = \sum_{i,j=0}^{3} \sqrt{p_i p_j}\langle\phi_j|\phi_i\rangle|i\rangle\langle j|_A.$$

Here, $|\phi_i\rangle$ are the coherent states prepared by Alice. Finally, as a valid density matrix, $\rho_{AB}$ must satisfy the following conditions:

$$\text{Tr}[\rho_{AB}] = 1, \tag{D18}$$
$$\rho_{AB} \geqslant 0. \tag{D19}$$

The condition $\rho_{AB} \geqslant 0$ means that $\rho_{AB}$ must be a positive semi-definite operator. The error rate needs to be considered. For given parameters, the probability of Bob obtaining measurement outcome $z = j$ given Alice sent state $x = k$ can be predicted by [2]

$$P(z = j|x = k) = \text{Tr}(R_j \rho_B^k) \tag{D20}$$
$$= \int_{\Delta_a}^{\infty} d\gamma \int_{j\pi/2+\Delta_p}^{(j+1)\pi/2-\Delta_p} \frac{\exp\left(-\frac{|\gamma e^{i\theta} - \sqrt{\eta}\alpha_k|^2}{1+\eta\xi/2}\right)}{\pi(1+\eta\xi/2)}\gamma d\theta. \tag{D21}$$

The parameters for the error correction term can then be calculated as [1]

$$p_{\text{pass}} = \sum_x p_x[P(0|x) + P(1|x)], \tag{D22}$$
$$\delta_{EC} = (1-\beta)H(Z) + \beta H(Z|X), \tag{D23}$$
$$H(Z|X) = \sum_x p_x h\left(\frac{P(0|x)}{P(0|x)+P(1|x)}\right). \tag{D24}$$

In these equations, $\beta$ is the error correction efficiency, set to 0.95. $H(Z)$ is the Shannon entropy of Bob's outcomes, and $I(X;Z)$ is the mutual information between Alice's inputs and Bob's outcomes. $h(x)$ is the binary entropy function, defined as $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$.

### Appendix D.2.2 *Key Rate Estimation for Homodyne Detection*

Similarly, for homodyne detection, a similar key rate estimation approach is used. The main distinction is that homodyne detection can measure two quadratures, $q$ and $p$. In our protocol, these two measurement types occur with equal probability, so we average their contributions:

$$R^{\infty}=\frac{1}{2}\left\{\min_{\rho_{AB}\in S}\sum_{y\in\{q,p\}}D(\mathcal{G}_y(\rho_{AB})||\mathcal{Z}[\mathcal{G}_y(\rho_{AB})])-\sum_{y\in\{q,p\}}p^y_{\text{pass}}\delta^y_{\text{EC}}\right\}. \tag{D25}$$

For each quadrature measurement $y\in\{q,p\}$, the post-processing mapping $\mathcal{G}_y(\rho)=K_y\rho K_y^{\dagger}$ is defined by the Kraus operators:

$$K_y=\sum_{b=0}^{1}|b\rangle_Z\otimes\mathbb{1}_A\otimes(\sqrt{I_y^b})_B. \tag{D26}$$

In this expression, $\{I_y^b\}$ denotes a set of projective operators:

$$I_y^0=\int_{\Delta_c}^{\infty}dt\,|t\rangle\langle t|\,,\quad I_y^1=\int_{-\infty}^{-\Delta_c}dt\,|t\rangle\langle t|\,. \tag{D27}$$

Here, $|t\rangle$ represents an eigenstate of the quadrature operator $\hat{y}$, and $\Delta_c$ is a threshold value for the measurement outcome. Similarly, the error rate can be calculated. The probability distributions for the quadrature outcomes $q$ and $p$ given Alice's input $\alpha_x$ are:

$$\begin{aligned}P(q|x)&=\frac{1}{\sqrt{\pi(\eta\xi+1)}}\exp\left(-\frac{(q-\sqrt{2\eta}\text{Re}(\alpha_x))^2}{\eta\xi+1}\right),\\P(p|x)&=\frac{1}{\sqrt{\pi(\eta\xi+1)}}\exp\left(-\frac{(p-\sqrt{2\eta}\text{Im}(\alpha_x))^2}{\eta\xi+1}\right).\end{aligned} \tag{D28}$$

The probability distribution of Bob's bits for each quadrature $y\in\{q,p\}$ is expressed as:

$$P_y(0|x)=\int_{\Delta_c}^{\infty}P(y|x)dy,\quad P_y(1|x)=\int_{-\infty}^{-\Delta_c}P(y|x)dy,\quad P_y(\perp|x)=\int_{-\Delta_c}^{\Delta_c}P(y|x)dy. \tag{D29}$$

Here, $P_y(0|x)$ is the probability of Bob obtaining outcome '0' for quadrature $y$ given Alice sent state $x$, $P_y(1|x)$ is the probability of obtaining '1', and $P_y(\perp|x)$ is the probability of a discarded result.

## Appendix D.3 BB84 KGP

Following [4], the number of vacuum and single-photon events in the $X$-basis are estimated as:

$$s_{X,0}\geqslant\tau_0\frac{\mu_2 n^-_{X,\mu_3}-\mu_3 n^+_{X,\mu_2}}{\mu_2-\mu_3}, \tag{D30}$$

$$s_{X,1}\geqslant\frac{\tau_1\mu_1\left[n^-_{X,\mu_2}-n^+_{X,\mu_3}-\frac{\mu_2^2-\mu_3^2}{\mu_1^2}(n^+_{X,\mu_1}-\frac{s_{X,0}}{\tau_0})\right]}{\mu_1(\mu_2-\mu_3)-\mu_2^2+\mu_3^2}. \tag{D31}$$

where $\tau_n:=\sum_{k\in\mathcal{K}}e^{-k}k^n p_k/n!$ ($\mathcal{K}=\{\mu_1,\mu_2,\mu_3\}$) is the probability of transmitting an $n$-photon state, and

$$n^{\pm}_{X,k}:=\frac{e^k}{p_k}\left(n_{X,k}\pm\sqrt{\frac{n_X}{2}\log\frac{21}{\varepsilon_{\text{sec}}}}\right),\ \forall\ k\in\mathcal{K}.$$

Here, $\mu_1$, $\mu_2$ and $\mu_3$ represent the signal and two decoy intensities in decoy-state BB84 type KGP.

Equations analogous to these are used to calculate the number of vacuum events ($s_{Z,0}$) and single-photon events ($s_{Z,1}$) for $\mathcal{Z}=\cup_{k\in\mathcal{K}}\mathcal{Z}_k$ using $Z$-basis statistics. The $X$-basis single-photon phase error rate is:

$$\phi_{X,1}:=\frac{c_{X,1}}{s_{X,1}}\leqslant\frac{v_{Z,1}}{s_{Z,1}}+\gamma^U\left(s_{Z,1},s_{X,1},\frac{v_{Z,1}}{s_{Z,1}},\varepsilon_{\text{sec}}\right), \tag{D32}$$

where

$$\begin{aligned}v_{Z,1}&\leqslant\tau_1\frac{m^+_{Z,\mu_2}-m^-_{Z,\mu_3}}{\mu_2-\mu_3},\\m^{\pm}_{Z,k}&:=\frac{e^k}{p_k}\left(m_{Z,k}\pm\sqrt{\frac{m_Z}{2}\log\frac{21}{\varepsilon_{\text{sec}}}}\right),\ \forall\ k\in\mathcal{K}.\end{aligned}$$

The total number of $X$-basis events is $n_X=\sum_{k\in\mathcal{K}}n_{X,k}$ and the number of errors is $m_X=\sum_{k\in\mathcal{K}}m_{X,k}$. Finally, the key rate is calculated by

$$l_{\text{key}}=\underline{s}_{X,0}+\underline{s}_{X,1}\left[1-H(\bar{\phi}^n_{X,1})\right]-\lambda_{EC}-\log_2(\frac{2}{\varepsilon_{\text{cor}}})-6\log_2\frac{22}{\epsilon_{PA}}. \tag{D33}$$

where $\lambda_{EC}$ is the number of bits revealed during the error correction step, $\varepsilon_{\text{cor}}$ is the failure probability of error correction, and $\epsilon_{PA}$ is the failure probability of privacy amplification.

## Appendix E Algorithmic protocol description

To make our circular QBA protocol easy to follow and understand, we provide a detailed step-by-step description of its main phases in an algorithmic format as shown in Algorithm E1.

**Algorithm E1** Circular Quantum Byzantine Agreement Protocol

**Input:** $N$ players, security parameter $\lambda$.

**Initialization:** $S \leftarrow$ commanding general; $R_i (i \in \mathbb{Z}_{N-1}^{+}) \leftarrow$ lieutenants; $CA \leftarrow$ assistant.
**Phase 1: Order Distribution**
**for** $i = 1$ **to** $N - 1$ **do**
  **repeat**
    $S$ sends $\{m_i; \sigma_i\}$ to $R_i$
    CA verifies the validity of $\sigma_i$
    **if** verification fails **then**
      Restart this distribution step
    **else**
      $R_i$: $O^i \leftarrow \{m_i; \sigma_i\}$
      CA records $\sigma_i$ and related quantum keys
    **end if**
  **until** $R_i$ receives valid order
**end for**
**Phase 2: Circular Gathering**
**for all** $i \in \mathbb{Z}_{N-1}^{+}$ **do**
  $j \leftarrow i$, stipulating $(N-1)+1 \equiv 1$
  **repeat**
    **if** $j = i$ **then**
      $R_i$: $G_{i\to i+1}^{i} \leftarrow O^i = \{m_i; \sigma_i; \sigma_{i\to i+1}^{i}\}$
    **else**
      $R_j$: $G_{j\to j+1}^{i} \leftarrow G_{j-1\to j}^{i} \cup O^j \cup \sigma_{j\to j+1}^{i}$
    **end if**
    $R_j$ sends $G_{j\to j+1}^{i}$ to $R_{j+1}$
    CA performs verification: (a) $\sigma_{j\to j+1}^{i}$ is valid; (b) signatures in $G_{j\to j+1}^{i}$ are unchanged; (c) signatures match $\{m_k\}$.
    **if** any verification fails **then**
      Restart current step
    **else**
      CA records $\sigma_{j\to j+1}^{i}$
      $j \leftarrow j + 1$
    **end if**
  **until** $R_{i-1}$ sends $G_{i-1\to i}^{i}$ to $R_i$
  $R_i$ extracts $F^i \leftarrow \{m_1, m_2, \ldots, m_{N-1}\}$ from $G_{i-1\to i}^{i}$
**end for**
**Phase 3: Consensus Output**
**for all** $i \in \mathbb{Z}_{N-1}^{+}$ **do**
  $R_i$: $m^{R_i} \leftarrow D(F^i) = D(m_1, m_2, \ldots, m_{N-1})$
**end for**

**Output:** $(\forall i \in \mathbb{Z}_{N-1}^{+})$ Honest $R_i$ outputs $m^{R_i}$.


**References**

1 Liu W B, Li C L, Xie Y M, et al. Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance. PRX Quantum, 2021, 2: 040334
2 Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. Phys. Rev. X, 2019, 9: 041064
3 Lo H K, Chau H F, Ardehali M. Efficient quantum key distribution scheme and a proof of its unconditional security. J. Cryptology, 2005, 18: 133–165
4 Lim C C W, Curty M, Walenta N, et al. Concise security bounds for practical decoy-state quantum key distribution. Phys. Rev. A, 2014, 89: 022307
5 Yin H L, Fu Y, Li C L, et al. Experimental quantum secure network with digital signatures and encryption. Natl. Sci. Rev., 2023, 10: nwac228

6 Krawczyk H. LFSR-based hashing and authentication. In: Proceedings of Annual International Cryptology Conference. Springer, 1994. 129–139
7 Shoup V. On fast and provably secure message authentication based on universal hashing. In: Proceedings of Koblitz N, editor, Advances in Cryptology — CRYPTO '96, Berlin, Heidelberg: Springer Berlin Heidelberg, 1996. 313–328
8 Li B H, Xie Y M, Cao X Y, et al. One-time universal hashing quantum digital signatures without perfect keys. Phys. Rev. Appl., 2023, 20: 044011
9 Li S G, Li C L, Liu W B, et al. Discrete-modulated continuous-variable quantum key distribution in satellite-to-ground communication. Adv Quantum Technol., 2024, 7: 2400140
10 Vasylyev D, Vogel W, Moll F. Satellite-mediated quantum atmospheric links. Phys. Rev. A, 2019, 99: 053830
11 Günthner K, Khan I, Elser D, et al. Quantum-limited measurements of optical signals from a satellite in geostationary earth orbit. In: Proceedings of European Quantum Electronics Conference. Optica Publishing Group, 2017. EB_4_2
12 Dios F, Rubio J A, Rodríguez A, et al. Scintillation and beam-wander analysis in an optical ground station-satellite uplink. Appl. Opt., 2004, 43: 3866–3873
13 Yura H T. Short-term average optical-beam spread in a turbulent medium. JOSA, 1973, 63: 567–572
14 Andrews L C, Phillips R L. Laser beam propagation through random media. Laser Beam Propagation Through Random Media: Second Edition, 2005
15 Qing C, Wu X, Li X, et al. Use of weather research and forecasting model outputs to obtain near-surface refractive index structure constant over the ocean. Opt. Express, 2016, 24: 13303–13315
16 Vasylyev D Y, Semenov A, Vogel W. Toward global quantum communication: beam wandering preserves nonclassicality. Phys. Rev. Lett., 2012, 108: 220501
17 Laudenbach F, Pacher C, Fung C H F, et al. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. Adv. Quantum Technol., 2018, 1: 1800011
18 Tan E Y Z, Schwonnek R, Goh K T, et al. Computing secure key rates for quantum cryptography with untrusted devices. Npj Quantum Inf., 2021, 7: 158
19 Coles P J. Unification of different views of decoherence and discord. Phys. Rev. A, 2012, 85: 042103