

Side-channel free quantum digital signature with source monitoring

Luo-Jia Ma(马洛嘉), Ming-Shuo Sun(孙铭烁), Chun-Hui Zhang(张春辉), Hua-Jian Ding(丁华建), Xing-Yu Zhou(周星宇), Jian Li(李剑), and Qin Wang(王琴)

Citation: Chin. Phys. B, 2025, 34 (**1**): 010301. DOI: 10.1088/1674-1056/ad8871
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Effects of quantum noise on teleportation of arbitrary two-qubit state via five-particle Brown state

Ao Wang(汪澳), Yu-Zhen Wei(魏玉震), Min Jiang(姜敏), Yong-Cheng Li(李泳成), Hong Chen(陈虹), and Xu Huang(黄旭)

Chin. Phys. B, 2024, 33 (**8**): 080307. DOI: 10.1088/1674-1056/ad3dc8

Improvement and security analysis of multi-ring discrete modulation continuous variable quantum secret sharing scheme

Huan-Yao Jiang(姜欢窈), Min Nie(聂敏), Guang Yang(杨光), Ai-Jing Sun(孙爱晶), Mei-Ling Zhang(张美玲), and Chang-Xing Pei(裴昌幸)

Chin. Phys. B, 2024, 33 (**7**): 070303. DOI: 10.1088/1674-1056/ad3b81

A quantum blind signature scheme based on dense coding for non-entangled states

Ke Xing(邢柯), Ai-Han Yin(殷爱菡), and Yong-Qi Xue(薛勇奇)

Chin. Phys. B, 2024, 33 (**6**): 060309. DOI: 10.1088/1674-1056/ad2bed

Passive round-robin differential-quadrature-phase-shift quantum key distribution scheme with untrusted detectors

Hongwei Liu(刘宏伟), Wenxiu Qu(屈文秀), Tianqi Dou(窦天琦), Jipeng Wang(王吉鹏), Yong Zhang(张勇), Haiqiang Ma(马海强)

Chin. Phys. B, 2018, 27 (**10**): 100309. DOI: 10.1088/1674-1056/27/10/100309

Hong-Ou-Mandel interference with two independent weak coherent states

Hua Chen(陈华), Xue-Bi An(安雪碧), Juan Wu(伍娟), Zhen-Qiang Yin(银振强), Shuang Wang(王双), Wei Chen(陈巍), Zhen-Fu Han(韩正甫)

Chin. Phys. B, 2016, 25 (**2**): 020305. DOI: 10.1088/1674-1056/25/2/020305

SPECIAL TOPIC — Quantum communication and quantum network

Side-channel free quantum digital signature with source monitoring

Luo-Jia Ma(马洛嘉)[1,2], Ming-Shuo Sun(孙铭烁)[1,2], Chun-Hui Zhang(张春辉)[1,2], Hua-Jian Ding(丁华建)[1,2], Xing-Yu Zhou(周星宇)[1,2], Jian Li(李剑)[1,2], and Qin Wang(王琴)[1,2,†]

[1] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[2] *Broadband Wireless Communication and Sensor Network Technology, Key Laboratory of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

(Received 30 July 2024; revised manuscript received 6 October 2024; accepted manuscript online 18 October 2024)

Quantum digital signature (QDS) can guarantee the information-theoretical security of a signature with the fundamental laws of quantum physics. However, most current QDS protocols do not take source security into account, leading to an overestimation of the signature rate. In this paper, we propose to utilize Hong–Ou–Mandel interference to characterize the upper bound of the source imperfections, and further to quantify information leakage from potential side-channels. Additionally, we combine decoy-state methods and finite-size analysis in analyzing the signature rate. Simulation results demonstrate the performance and feasibility of our approach. Our current work can improve the practical security of QDS systems, thereby promoting their further networked applications.

Keywords: Hong–Ou–Mandel interference, side-channel free, quantum digital signature

PACS: 03.67.Dd, 03.67.HK, 42.79.Sz

DOI: 10.1088/1674-1056/ad8871 **CSTR:** 32038.14.CPB.ad8871

1. Introduction

The digital signature,[1] as an important cornerstone to ensure the security of the current internet, can ensure the unforgeability, transference and non-repudiation of messages, and is widely used in financial transactions and e-commerce. Generally, the security of classical digital signatures is based on the computational complexity of mathematical problems. However, with the development of quantum computers,[2] its security is under threat.

Compared with classical digital signatures, quantum digital signature (QDS) based on the basic principles of quantum mechanics can offer a higher level of security. Since the first QDS protocol, known as the GC-01 protocol, proposed by Gottesman and Chuang in 2001,[3] experiment-friendly protocols have been proposed and validated.[4–6] Subsequently, researchers have successively implemented measurement-device-independent QDS,[7,8] passive decoy-state QDS,[9] long-distance transmission of QDS,[10] and efficient QDS based on a one-time universal hashing.[11] And at present, it is developing towards practical applications.

QDS is a multi-user encryption system that includes a distribution stage and a messaging stage. In the three-party scenario, assume Alice is the signer of the message, Bob and Charlie are the verifiers of the signed message. In the distribution stage, the pairs Alice–Bob and Alice–Charlie individually adopt key generation protocol (KGP) to generate correlated bit strings. In the message stage, Alice signs the message and transmits it to a desired recipient, say Bob. After verifying the received signed message, Bob forwards it to Charlie for verification. The KGP process is actually the quantum part of quantum key distribution, that is, two pairs independently implement the decoy-state QKD protocol but without error correction or privacy amplification.

Although QDS is guaranteed to be unconditionally secure by quantum mechanics, it is necessary to assume that the eavesdropper will not gain any desired information in the KGP process.[12–16] However, active and passive side-channel attacks on the sender can easily undermine this assumption. For example, an active attack, called Trojan horse attack,[17] where the eavesdropper sends a strong light to the sender and obtains information about the devices by analyzing the reflected light. In passive attacks, the idea is to utilize the deviations of the actual quantum signal from the desired one, which exist in higher dimensions and are influenced by factors such as spectrum bandwidth,[18] frequency,[19] time jitter,[20] and so on. Unlike the problem of state preparation flaws at the source,[21] which can be addressed by loss-tolerant method because it only exists in two dimensions,[22] the differences between actual signals are influenced by multidimensional factors. These influences are difficult to characterize accurately through measurements in a single dimension. Fortunately, Hong–Ou–Mandel (HOM) interference visibility can be applied to characterize the distinguishability in all dimensions of the signal, and Ref. [23] provides a method of using the maximum HOM interference visibility between different emitted signals to characterize the

†Corresponding author. E-mail: qinw@njupt.edu.cn

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

distinguishability with the same intensity at different bases. Besides, a fundamental implicit assumption in the decoy-state protocol is that the yield of an n-photon state is independent of the intensity, it will also be broken as different intensities are likely to exhibit distinguishability in source.[24] Here we present a more practical QDS protocol and consider its finite size effect.

The paper is organized as follows. In Section 2, we present the scheme of QDS with source monitoring. In Section 3, the signature rates of QDS with distinguishable decoy-state and bases are re-estimated. Then, in Section 4 we carry out corresponding numerical calculations and simulations. Finally, conclusions are given in Section 5.

2. QDS protocol with source monitoring

The process of the two-decoy QDS protocol with source monitoring will be introduced below. Figure 1(a) shows the schematic of our present scheme, i.e., the QDS with source monitoring modules. Suppose the total number of pulses used for key transmission in each round is N_{tot}, and then one selects the L-length block from the key pool for signing a message m ($m = 0$ and 1).

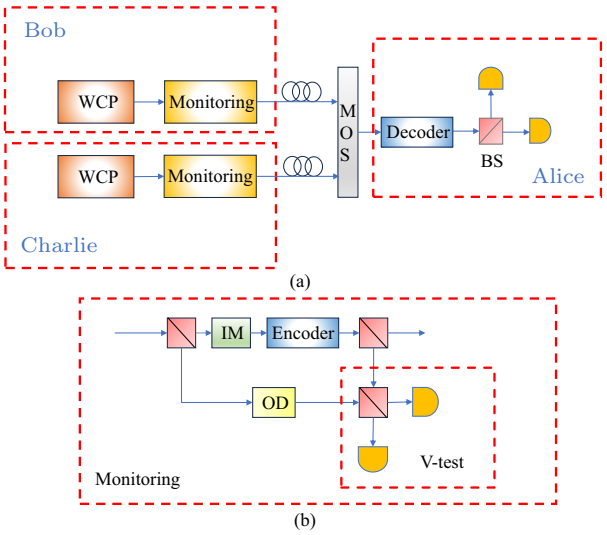


Fig. 1. (a) The schematic of QDS scheme with source monitoring modules. WCP, weak coherent pulses; MOS, mechanical optical switch; BS, beam-splitter. (b) Monitoring module. IM, intensity modulator; OD, optical delay.

Distribution stage Bob (Charlie) prepares N_{tot} photon pulses. After the pulses enter the monitoring module in Fig. 1(b), they are divided into two portions by BS. The pulses of the upper path are modulated by intensity modulator (IM) and encoder, and each of them is randomly modulated into intensity $\omega \in \{\mu, \nu, 0\}$ (signal, decoy1, decoy2) with probability P_ω and basis $\varsigma \in \{X, Z\}$ with probability P_ς. Then there are a total of eight modulated states: $|0\rangle_\mu, |1\rangle_\mu, |+\rangle_\mu, |-\rangle_\mu, |0\rangle_\nu, |1\rangle_\nu, |+\rangle_\nu, |-\rangle_\nu$, where $|0\rangle_\omega$ and $|1\rangle_\omega$ are the encoded states of Z basis, $|+\rangle_\omega$ and $|-\rangle_\omega$ are the encoded states of X basis. Then the light of the upper path is defined as ρ_ω^φ, $\varphi \in \{|0\rangle_\omega, |1\rangle_\omega, |+\rangle_\omega, |-\rangle_\omega\}$. The lower path serves as a reference light and is defined as $\rho_{\omega'}^{\varphi'}$, where its polarization is different from that of the upper path, written as φ', and for simplicity $\omega' = \nu$. To characterize the defects of the modulator including IM and encoder, two paths of light interfere at the V-test, monitoring the source in real time. We call this module as V-test as we use HOM interference visibility to test the IM and encoder. It is worth noting that the optical delay (OD) in the lower path is used to achieve the synchronous arrival time of the two optical paths and ensure phase randomization of the pulses. Subsequently, rest pulses are transmitted to Alice through the quantum channel.

Alice randomly chooses ς basis to measure the pulses she received. Later, Alice–Bob (Alice–Charlie) publicly announce their basis options through the authenticated classical channel and keep the matched results. When they all choose Z basis, the corresponding bits are used to extract sifted keys, say N_Z, but in the case that Alice chooses the X basis, the corresponding bits are used for parameter estimation. Furthermore, they randomly select a portion of keys of Z basis, say n_{test}, to estimate the error rate e_{AB} (e_{AC}). The rest keys of Z basis are kept as the key pool n_{pool} for the signature. To sign for a future possible message m, Alice and Bob (Charlie) opt for a L-length block from n_{pool} to generate signature sequences K_m^{B} and B_m^{A} (K_m^{C} and C_m^{A}), where K_m^{B} and K_m^{C} are held by Alice, B_m^{A} (C_m^{A}) are held by Bob (Charlie). Finally, Bob (Charlie) randomly selects half of his keys and transmits them with their corresponding positions to Charlie (Bob) through a secret channel. The half of the keys that Bob (Charlie) keeps is denoted as $B_{m,\text{keep}}^{\text{A}}$ ($C_{m,\text{keep}}^{\text{A}}$), and the other half as $B_{m,\text{forward}}^{\text{A}}$ ($C_{m,\text{forward}}^{\text{A}}$). At this point, the symmetric keys held by Bob and Charlie are $S_m^{\text{B}} = (B_{m,\text{keep}}^{\text{A}}, C_{m,\text{forward}}^{\text{A}})$ and $S_m^{\text{C}} = (C_{m,\text{keep}}^{\text{A}}, B_{m,\text{forward}}^{\text{A}})$, respectively.

According to the error rate e_{AB}, the upper bound of the observed error rate e_{AB}^{U} can be estimated using the Serfling inequality[25]

$$e_{\text{AB}}^{\text{U}} = e_{\text{AB}} + \frac{2}{L}\sqrt{\frac{\ln(1/\varepsilon_{\text{PE}})}{2n_{\text{test}}}(L/2+1)(L/2+n_{\text{test}})}, \quad (1)$$

where ε_{PE} is the failure probability of Eq. (1). Likely, the upper bound of observed error rate e_{AC}^{U} can also be calculated, and $e^{\text{U}} = \max(e_{\text{AB}}^{\text{U}}, e_{\text{AC}}^{\text{U}})$. Next, consider the minimum rate at which eavesdropper Eve can make errors p_{E}, which satisfies

$$H_2(p_{\text{E}}) = 2s_{Z,1}^{\text{L}}\left[1 - H_2(\phi_{Z,1}^{\text{U}})\right]/N_Z, \quad (2)$$

where $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function; $s_{Z,1}^{\text{L}}$ and $\phi_{Z,1}^{\text{U}}$ are the lower bound of single-photon counts and the upper bound of the single-photon error rate in Z basis.

Messaging stage Alice sends (m, Sig_m) to a recipient (such as Bob), where $Sig_m = \left(K_m^{\mathrm{B}}, K_m^{\mathrm{C}}\right)$. Bob records the mismatching number between S_m^{B} and Sig_m. If the number in both parts of S_m^{B} is less than $s_\alpha L/2$, then Bob accepts the signature message and forwards it to Charlie, where s_α denotes the authentication threshold required for the security level of the QDS protocol. Otherwise, Bob rejects the message and announces termination of protocol, Charlie tests the signature message forwarded by Bob by the same method with another threshold s_v $(0 < s_\alpha < s_v < 0.5)$. Finally, Charlie accepts the message if the numbers of mismatches in both halves of his keys are still less than $s_v L/2$.

Next, consider the three major security analyses of QDS protocol: robustness P_{rob}, non-repudiation P_{rep} and non-forging P_{for}. To ensure the security of QDS system, the security level P_{sec} satisfies[6]

$$\max\left\{P_{\mathrm{rob}}, P_{\mathrm{rep}}, P_{\mathrm{for}}\right\} \leq P_{\mathrm{sec}}. \tag{3}$$

3. Method with distinguishable decoy states and bases imbalance

Considering that each pulse pair entering the V-test measurement has different polarization and intensity, it is necessary to normalize the HOM interference visibility of each pair. The measured and corresponding ideal visibility under each pair is defined as V_ω^φ and $\langle V_\omega^\varphi \rangle$, respectively. After normalizing, we define the visibility for each pair as follows:

$$\tilde{V}_\omega^\varphi = \frac{\langle V_\omega^\varphi \rangle - \left| V_\omega^\varphi - \langle V_\omega^\varphi \rangle \right|}{2\langle V_\omega^\varphi \rangle}. \tag{4}$$

To characterize the imperfection of the source, the fidelity between two states can be calculated by[23,26]

$$F\left(\hat{\rho}_\omega^\varphi, \hat{\rho}_{\omega'}^{\varphi'}\right) = \sum_{n=0}^{\infty} \sqrt{P_n^\omega P_n^{\omega'}} \tilde{\gamma}_\omega^{\varphi\,\frac{n}{2}}, \tag{5}$$

where P_n^ω represents the Poisson distribution at n-photon and ω intensity, $\tilde{\gamma}_\omega^\varphi = 2\tilde{V}_\omega^\varphi$ is applied to define the similarity between states, $\hat{\rho}_\omega^\varphi$ and $\hat{\rho}_{\omega'}^{\varphi'}$ represent the density matrices of the single-photon states[23]

$$\begin{aligned}\hat{\rho}_\omega^\varphi = & \sum_{n=0}^{\infty} P_n^\omega \left(\sqrt{\tilde{\gamma}_\omega^\varphi}\hat{a}_1^\dagger + \sqrt{1-\tilde{\gamma}_\omega^\varphi}\hat{a}_{\perp 1}^\dagger\right)^n |0\rangle\langle 0| \\ & \times \left(\sqrt{\tilde{\gamma}_\omega^\varphi}\hat{a}_1 + \sqrt{1-\tilde{\gamma}_\omega^\varphi}\hat{a}_{\perp 1}\right)^n, \end{aligned} \tag{6}$$

$$\hat{\rho}_{\omega'}^{\varphi'} = \sum_{n=0}^{\infty} P_n^{\omega'} \left(\hat{a}_1^\dagger\right)^n |0\rangle\langle 0| \left(\hat{a}_1\right)^n, \tag{7}$$

where $\hat{a}_1^\dagger$ and $\hat{a}_1$ represent the creation and annihilation operators, $\hat{a}_{\perp 1}^\dagger$ and $\hat{a}_{\perp 1}$ represent all modes orthogonal to $\hat{a}_1^\dagger$ and $\hat{a}_1$, respectively.

A fundamental assumption in the decoy-state analysis is that the yield is independent of the intensity. However, the imperfection of the source can cause differences between signal states and decoy states in high-dimension freedom. According to Refs. [24,27], the imperfection can be characterized by

$$D_\omega^\varphi = \frac{1}{2}\mathrm{Tr}\left|\hat{\rho}_\omega^\varphi - \hat{\rho}_{\omega'}^{\varphi'}\right| \leq \sqrt{1 - F\left(\hat{\rho}_\omega^\varphi, \hat{\rho}_{\omega'}^{\varphi'}\right)^2}, \tag{8}$$

and for simplicity, we assume every pair shares the same and worst imperfection $D_{\mu\nu} = \max_{\omega=\mu} \tilde{D}_\omega^\varphi$. It is convenient to acquire $\left|s_{Z,n}^\mu - s_{Z,n}^\nu\right| \leq N_{\mathrm{tot}} P_{\mathrm{ZA}} P_{\mathrm{ZB}} \tau_n D_{\mu\nu}$ from Eq. (8), where $s_{Z,n}^\omega$ expresses the counts of n-photon states with intensity ω, P_{ZA} represents the probability of Alice using Z basis for detection, P_{ZB} represents the probability of Bob using Z basis for preparation and τ_n is the probability that sender prepares an n-photon state. Actually, in a QDS system based on prepare-and-measure protocol, according to the optical transmittance of receiver η_{d}, we can obtain[28]

$$\left|s_{Z,n}^\mu - s_{Z,n}^\nu\right| \leq N_{\mathrm{tot}} P_{\mathrm{ZA}} P_{\mathrm{ZB}} \tau_n D_{\mu\nu}\left[1 - (1-\eta_{\mathrm{d}})^n\right], \tag{9}$$

then we can obtain the lower bound of single-photon counts in Z basis

$$\begin{aligned} s_{Z,1}^{\mathrm{L}} = & \frac{\tau_1 \mu}{\mu\nu - \nu^2}\left\{\frac{\mathrm{e}^\nu \underline{N}_{Z,\nu}}{P_\nu} - \frac{\nu^2}{\mu^2}\frac{\mathrm{e}^\mu \overline{N}_{Z,\mu}}{P_\mu}\right. \\ & - \frac{\left(\mu^2 - \nu^2\right)}{\mu^2}\frac{\overline{N}_0 P_{\mathrm{ZA}} P_{\mathrm{ZB}}}{P_0} \\ & \left. - P_{\mathrm{ZA}} P_{\mathrm{ZB}} N_{\mathrm{tot}} D_{\mu\nu}\left[\mathrm{e}^\nu - \mathrm{e}^{\nu(1-\eta_{\mathrm{d}})}\right]\right\}, \end{aligned} \tag{10}$$

where $\tilde{N}_{\varsigma,\omega}$ is the observed counts of intensity ω on ς basis with statistical fluctuations. We use the Hoeffding inequalities[29] to give lower bound and upper bound: $\underline{N}_{\varsigma,\omega} = \tilde{N}_{\varsigma,\omega} - \delta\left(N_\varsigma, \varepsilon_{\mathrm{SF}}\right)$ and $\overline{N}_{\varsigma,\omega} = \tilde{N}_{\varsigma,\omega} + \delta\left(N_\varsigma, \varepsilon_{\mathrm{SF}}\right)$, where $\delta(m,n) = \sqrt{m \ln\left(\frac{1}{n}\right)/2}$. $\overline{N}_0$ is the upper bound on counts of vacuum state.

Next, we consider the estimation of phase error rate for the Z basis when there are differences between signal states and decoy states in high-dimension freedom. The upper bound of single-photon bit error rate $\phi_{X,1}^{\mathrm{U}}$ can be estimated by

$$\phi_{X,1}^{\mathrm{U}} = \frac{\nu_{X,1}^{\mathrm{U}}}{s_{X,1}^{\mathrm{L}}}, \tag{11}$$

where $s_{X,1}^{\mathrm{L}}$ is the lower bound of single-photon counts in X basis

$$\begin{aligned} s_{X,1}^{\mathrm{L}} = & \frac{\tau_1 \mu}{\mu\nu - \nu^2}\left\{\frac{\mathrm{e}^\nu \underline{N}_{X,\nu}}{P_\nu} - \frac{\nu^2}{\mu^2}\frac{\mathrm{e}^\mu \overline{N}_{X,\mu}}{P_\mu}\right. \\ & - \frac{\left(\mu^2 - \nu^2\right)}{\mu^2}\frac{\overline{N}_0 P_{\mathrm{XA}} P_{\mathrm{XB}}}{P_0} \\ & \left. - P_{\mathrm{XA}} P_{\mathrm{XB}} N_{\mathrm{tot}} D_{\mu\nu}\left[\mathrm{e}^\nu - \mathrm{e}^{\nu(1-\eta_{\mathrm{d}})}\right]\right\}, \end{aligned} \tag{12}$$

and $\nu_{X,1}^{\mathrm{U}}$ denotes the upper bound on the number of bit errors, and it can be estimated by[30]

$$\nu_{X,1}^{\mathrm{U}} \leq \min\left\{K^\mu, K^\nu, K^{\mu\nu}\right\}, \tag{13}$$

where K^{μ}, K^{ν} and $K^{\mu\nu}$ can be calculated by

$$K^{\mu} = \frac{\tau_1}{\mu}\left(\frac{e^{\mu}}{P_{\mu}}\overline{M}^{\mathrm{U}}_{X,\mu} - P_{\mathrm{XA}}P_{\mathrm{XB}}N_{\mathrm{tot}}e_0Y_0\right), \tag{14}$$

$$K^{\nu} = \frac{\tau_1}{\nu}\left\{\frac{e^{\nu}}{P_{\nu}}\overline{M}^{\mathrm{U}}_{X,\nu} - P_{\mathrm{XA}}P_{\mathrm{XB}}N_{\mathrm{tot}} \times \left[e_0Y_0 - \nu D_{\mu\nu}\left(e^{\nu} - e^{\nu-\nu\eta_{\mathrm{d}}}\right)\right]\right\}, \tag{15}$$

$$K^{\mu\nu} = \frac{\tau_1}{\mu-\nu}\left[\frac{e^{\mu}}{P_{\mu}}\overline{M}^{\mathrm{U}}_{X,\mu} - \frac{e^{\nu}}{P_{\nu}}\underline{M}^{\mathrm{U}}_{X,\nu} + P_{\mathrm{XA}}P_{\mathrm{XB}}N_{\mathrm{tot}}D_{\mu\nu}\left(e^{\nu} - e^{\nu-\nu\eta_{\mathrm{d}}}\right)\right], \tag{16}$$

where $\tilde{M}_{\varsigma,\omega}$ is the observed error counts of intensity ω in ς basis with statistical fluctuations, and the equations above can be calculated from

$$\left|v^{\mu}_{X,n} - v^{\nu}_{X,n}\right| \leq N_{\mathrm{tot}}P_{\mathrm{ZA}}P_{\mathrm{ZB}}\tau_n D_{\mu\nu}\left(1-(1-\eta_{\mathrm{d}})^n\right),$$

where $v^{\omega}_{X,n}$ expresses the bit error of n-photon states with intensity ω.

In an ideal scenario, an eavesdropper cannot distinguish between different bases. However, considering the imperfection at the source side, differences may arise in the density matrices of different bases. According to Ref. [31], the value called bases imbalance can be applied to quantify the differences between density matrices of the X and Z bases

$$\Delta = \frac{1-\sqrt{F\left(\hat{\rho}_X,\hat{\rho}_Z\right)}}{2}, \tag{17}$$

where $F\left(\hat{\rho}_X,\hat{\rho}_Z\right)$ is the fidelity between X and Z bases. Although it is hard to obtain the bases imbalance directly, we use the distance and triangle inequality to construct a lower bound on fidelity between X and Z bases depending on the fidelity between the initial and auxiliary states[27]

$$\begin{aligned}&\arccos\sqrt{F\left(\hat{\rho}_X,\hat{\rho}_Z\right)}\\ \leq\ &\arccos\max_{i,j\in 0,1}\sqrt{F\left(\hat{\rho}_{X,i},\hat{\rho}_{Z,j}\right)}\\ &+\sum_{b\in\{X,Z\}}\arccos\frac{1+\sqrt{F\left(\hat{\rho}_{b,0},\hat{\rho}_{b,1}\right)}}{2},\end{aligned} \tag{18}$$

where $\hat{\rho}_{X,i}$ and $\hat{\rho}_{Z,i}$ respectively denote the auxiliary for each basis, and b represents for the X and Z bases. To simplify the final result, we assume every pair of bits share the same fidelity and represent them as F. After substituting Eq. (17) into Eq. (18), we can obtain

$$\Delta \leq \frac{1}{2} - \frac{1}{2}\cos\left(2\arccos\frac{1+\sqrt{F}}{2} + \arccos\sqrt{F}\right). \tag{19}$$

In consideration of the ability of Eve to access a lossless channel, we use a method mentioned in Ref. [31] to quantify the impacts of the differences between different bases: $\Delta' = \frac{\Delta}{s^{\mathrm{L}}_{Z,1}}P_{\mathrm{ZA}}P_{\mathrm{ZB}}N_{\mathrm{tot}}\tau_1$. Then the upper bound of single-photon phase error rate in Z basis is obtained as follows:

$$\begin{aligned}\phi^{\mathrm{U}}_{Z,1}{}' &= \phi^{\mathrm{U}}_{X,1} + 4\left(1-\Delta'\right)\Delta'\left(1-2\phi^{\mathrm{U}}_{X,1}\right)\\ &\quad + 4\left(1-2\Delta'\right)\sqrt{\Delta'\left(1-\Delta'\right)\phi^{\mathrm{U}}_{X,1}\left(1-\phi^{\mathrm{U}}_{X,1}\right)},\end{aligned} \tag{20}$$

after this, we replace $\phi^{\mathrm{U}}_{Z,1}$ in Eq. (2) with $\phi^{\mathrm{U}}_{Z,1}{}'$ in Eq. (20) for subsequent signature rate estimation.

4. Simulation results

Based on the formulas presented above, we perform numerical simulations of signature rates with the two-decoy method. The system parameters we used are listed in Table 1. Here, P_{sec} is the security level of the protocol. P_{d} and η_{d} are the dark rate and detection efficiency of receiver's detectors; α represents the channel attenuation; e_{d} is the optical misalignment error; N_{tot} is the total number of pulses sent by sender; $\varepsilon_{\mathrm{PE}}$ and $\varepsilon_{\mathrm{SF}}$ are the probability of failure for the error test and statistical fluctuation. To estimate the worst case, we assume $V = \min_{\varphi,\omega}\tilde{V}^{\varphi}_{\omega}$. Our simulation considers the finite size effect and global optimization to achieve more practical results.

Table 1. List of system parameters used in numerical simulations.[32]

P_{sec}	P_{d}	η	α (dB/km)	e_{d}	N_{tot}	$\varepsilon_{\mathrm{PE}}$	$\varepsilon_{\mathrm{SF}}$
10^{-5}	10^{-8}	0.85	0.2	0.015	10^{12}	10^{-5}	10^{-10}

To ensure the security of the QDS protocol, it is necessary to ensure that the minimum rate p_{E} is larger than the error rate caused by normal communication between the communicating parties e^{U}, i.e., $p_{\mathrm{E}} > e^{\mathrm{U}}$. After calculating e^{U} and p_{E}, we construct the relationship between the number of pulses emitted by the sender and the security level of the protocol to calculate the signature rate, which is defined as $R = 1/N$, and N refers to the minimum number of pulses needed to sign a bit of message given a certain security level.

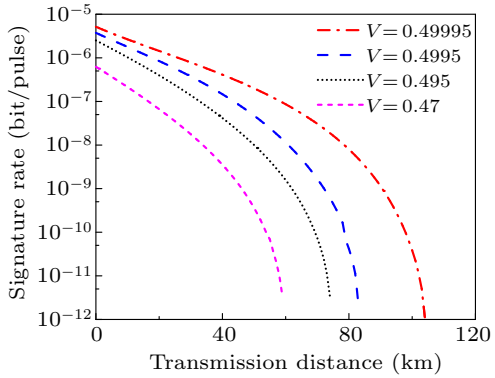


Fig. 2. The variation of the signature rate with transmission distance considering side-channel leakage. Each color corresponds to a different HOM interference visibility.

Figure 2 shows the signature rate versus HOM interference visibility, where each line corresponds to a different HOM interference visibility (V), ranging from 0.49995 to 0.47.[33] We can see from Fig. 2 that the performance

of the present scheme is quite sensitive to the value of V. For example, the transmission distance quickly declines from 105 km to 60 km, with the value of V decreasing from 0.49995 to 0.47. Second, with current experimental conditions, i.e., $V = 0.495$,[20] the transmission distance can exceed 75 km.

Figure 3 illustrates the variation of the signature rate versus visibilities at fixed transmission distances of 0 km, 20 km, 40 km, and 60 km respectively. It is evident that the signature rate exhibits a rapid decline as the visibility gradually decreases at each fixed transmission distance. For instance, at 40 km, the signature rate experiences a significant decrease of two orders of magnitude when the visibility changes from 0.5 to 0.45. Moreover, the signature rate at 60 km exhibits an even steeper decline compared to those at transmission distances of 0 km, 20 km, and 40 km, and it becomes almost unfeasible to achieve an effective signature process when the visibility falls below 0.47.

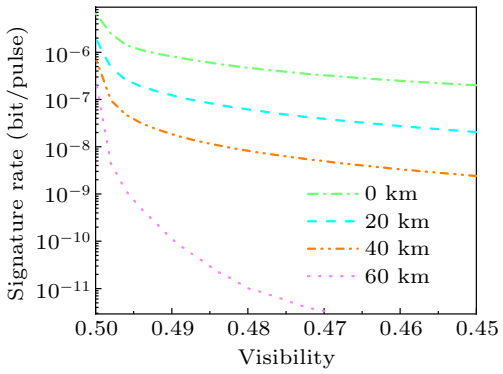


Fig. 3. The signature rate versus HOM interference visibility. Here the transmission distance is fixed at 0 km, 20 km, 40 km and 60 km respectively.

Figure 4 provides the variation of single-photon phase error rate $\phi_{Z,1}^{U\,\prime}$ versus the transmission distance under different HOM interference visibilities. As we can see, when the value of V is close to the idea visibility (0.5), i.e., $V = 0.49995$, the value of $\phi_{Z,1}^{U\,\prime}$ gradually increases its value with the increasing transmission distance; while when the value of V is relatively lower, i.e., $V = 0.47$, $\phi_{Z,1}^{U\,\prime}$ rapidly rises its value with the increasing transmission distance. This is consistent with the results in Figs. 3 and 4.

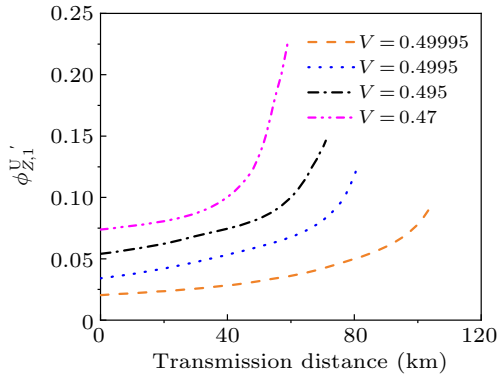


Fig. 4. The single-photon phase error rate $\phi_{Z,1}^{U\,\prime}$ versus transmission distance with different HOM interference visibilities.

5. Conclusion and perspectives

In this paper, we propose a scheme to improve the practical security of QDS system by monitoring the HOM interference visibility of the source. Considering source imperfections might cause information leakage from side channels,[34] we give a more general model by taking the distinguishabilitiy between the signal state and the decoy state into account. It only needs one parameter to characterize the source security, which simplifies the system complexity compared with other existing methods using individual parameters for each device.[35] But, we should admit that additional devices are incorporated in the V-test module and a high HOM interference visibility is required to maintain good system performance in the present scheme. Then better analytical methods are needed to make the parameter estimation more precise and enhance the robustness of the scheme. Besides, the monitoring module can be constructed as a plug-and-play module in practical applications to reduce its system complexity. Moreover, some advanced technologies, such as the advantage distillation technology[36–38] can also be implemented to further improve its performance, which will be our future research work. We hope our present work can provide a valuable reference for practical applications of QDS.

Acknowledgements

We gratefully acknowledge the financial support from the Natural Science Foundation of Jiangsu Province (Grant Nos. BE2022071 and BK20192001), the National Natural Science Foundation of China (Grant Nos. 12074194, 62471248, 12104240, and 62101285), and the Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX22_0954).

References

[1] Diffie W and Helman M E 1976 *IEEE Trans. Inf. Theory* **22** 644
[2] Ladd T D, Jelezko F, Laflamme M, Nakamura Y, Monroe C and O'Brien J L 2010 *Nature* **464** 45
[3] Gottesman D and Chuang I 2001 arXiv: 0105.032v2 [quant-ph]
[4] Clarke P J, Collins R J, Dunjko V, Andersson E, Jeffers J and Buller G S 2012 *Nat. Commun.* **3** 1174
[5] Dunjko V, Wallden P and Andersson E 2014 *Phys. Rev. Lett.* **112** 040502
[6] Amiri R, Wallden P, Kent A and Andersson E 2016 *Phys. Rev. A* **93** 032325
[7] Yin H L, Wang W L, Tang Y L, Zhao Q, Liu H, Sun X X, Zhang W J, Li H, Puthoor I V, You L X, Andersson E, Wang Z, Liu Y, Jiang X, Ma X F, Zhang Q, Curty M, Chen T Y and Pan J W 2017 *Phys. Rev. A* **95** 042338
[8] Roberts G L, Lucamarini M, Yuan Z L, Dynes J F, Comandar L C, Sharpe A W, Shields A J, Curty M, Puthoor I V and Andersson E 2017 *Nat. Commun.* **8** 1098
[9] Zhang C H, Zhou X Y, Ding H J, Zhang C M, Guo G C and Wang Q 2018 *Phys. Rev. Appl.* **10** 034033
[10] Ding H J, Chen J J, Li J, Zhou X Y, Zhang C H, Zhang C M and Wang Q 2020 *Opt. Lett.* **45** 1711

[11] Yin H L, Fu Y, Li L C, Weng C X, Li B H, Gu J, Lu Y S, Huang S and Chen B Z 2023 *Natl. Sci. Rev.* **10** 1093

[12] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photonics* **4** 686

[13] Lu F Y, Ye P, Wang Z H, Wang S, Yin Z Q, Wang R, Huang X J, Chen W, He D Y, Fan Yuan G J, Guo G C and Han Z F 2023 *Optica* **4** 520

[14] Zhou Y, Li H W, Zhou C, Wang Y, Lu Y F, Jiang M S, Zhang X X and Bao W S 2023 *Chin. Phys. B* **32** 050305

[15] Sun M S, Wang W L, Zhou X Y, Zhang C H and Wang Q 2023 *Phys. Rev. Res.* **5** 043179

[16] Ma L J, Ding H J, Chen Z Q, Zhan C H and Wang Q 2024 *Acta Phys. Sin.* **73** 020301 (in Chinese)

[17] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320

[18] Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H and Weinfurter H 2009 *New J. Phys.* **11** 065001

[19] Pereira M, Curty M and Tamaki K 2019 *npj. Quantum. Inf.* **5** 62

[20] Comandar L, Lucamarini M, Fröhlich B, Dynes J F, Yuan Z L and Shields A J 2016 *Opt. Express* **24** 17849

[21] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Phys. Rev. A* **85** 042307

[22] Tamaki K, Curty M, Kato G, Lo H K and Azuma K 2014 *Phys. Rev. A* **90** 052314

[23] Duplinskiy A and Sych D 2021 *Phys. Rev. A* **104** 012601

[24] Tamaki K, Curty M and Lucamarini M 2016 *New J. Phys.* **18** 065008

[25] Serfling R J 1974 *Ann. Statist.* **2** 39

[26] Jozsa R 1994 *J. Mod. Opt.* **41** 2315

[27] Ma Z, Zhang F L and Chen J L 2009 *Phys. Lett. A* **373** 3407

[28] Marøy Ø, Lydersen L and Skaar J 2017 *Quantum Sci. Technol.* **2** 044013

[29] Hoeffding W 1963 *J. Am. Stat. Assoc.* **58** 13

[30] Huang A Q, Sun S H, Liu Z H and Makarov V 2018 *Phys. Rev. A* **98** 012330

[31] Koashi M 2009 *New J. Phys.* **11** 045018

[32] Wang W L, Zhou X Y, Sun M S, Zhang C H and Wang Q 2023 *IEEE Photonics J.* **15** 1

[33] Rubenok A, Slater J A, Chan P, Lucio M I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501

[34] Lu F Y, Lin X, Wang S, Fan Yuan G J, Ye P, Wang R, Yin Z Q, He D Y, Chen W, Guo G C and Han Z F 2021 *npj Quantum Inf.* **7** 75

[35] Jie G, Cao X Y, Yao F, He Z W, Yin Z J, Hua H L and Chen Z B 2022 *Sci. Bull.* **67** 2167

[36] Wang R Q, Zhang C M, Yin Z Q, Li H W, Wang S, Chen W, Guo G C and Han Z F 2022 *New J. Phys.* **24** 073049

[37] Li H W, Zhang C M, Jiang M S and Cai Q Y 2022 *Commun. Phys.* **5** 53

[38] Li H W, Hao C P, Chen Z J, Gong L, Lu Y F, Wang Y, Li J J, Zhang C M, Wang R, Yin Z Q and Cai Q Y 2024 *Sci. China Phys., Mech. Astron.* **67** 270313