SCIENCE CHINA
Information Sciences

August 2020, Vol. 63 180504:1–180504:15
https://doi.org/10.1007/s11432-020-2886-x

• RESEARCH PAPER •
Special Focus on Quantum Information

A universal simulating framework for quantum key distribution systems

Guan-Jie FAN-YUAN[1,2,3], Wei CHEN[1,2,3*], Feng-Yu LU[1,2,3], Zhen-Qiang YIN[1,2,3], Shuang WANG[1,2,3], Guang-Can GUO[1,2,3] & Zheng-Fu HAN[1,2,3*]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei* 230026*, China;*
[2]*State Key Laboratory of Cryptography, P.O. Box* 5159*, Beijing* 100878*, China;*
[3]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026*, China*

Received 6 January 2020/Accepted 24 April 2020/Published online 15 July 2020

Abstract Quantum key distribution (QKD) provides a physical-based way to conciliate keys between remote users securely. Simulation is an essential method for designing and optimizing QKD systems. We develop a universal simulation framework based on quantum operator descriptions of photon signals and optical devices. The optical devices can be freely combined and driven by the photon excitation events, which make it appropriate for arbitrary QKD systems in principle. Our framework focuses on realistic characters of optical devices and system structures. The imperfections of the devices and the non-local properties of a quantum system are taken into account when modeling. We simulate the single-photon and Hong-Ou-Mandel (HOM) interference optical units, which are fundamental of QKD systems. The results using this event-driven framework agree well with the theoretical results, which indicate its feasibility for QKD.

Keywords quantum key distribution, quantum optics, simulation, modeling, C++

Citation Fan-Yuan G-J, Chen W, Lu F-Y, et al. A universal simulating framework for quantum key distribution systems. Sci China Inf Sci, 2020, 63(8): 180504, https://doi.org/10.1007/s11432-020-2886-x

1 Introduction

Quantum key distribution (QKD) [1, 2] can generate keys between remoter users in public channels against the threat of quantum computing [3, 4]. Since its first protocol was proposed [1] in 1984, QKD has achieved significant progress in theory [5–18] and experiment [19–34]. However, there are still some challenges for QKD on its road to real-life applications [4,35–40]. One of the essential challenges is the gap between the practical systems and the theoretical model of QKD [4,35] because the device imperfections are in multiple dimensions and hardly to theoretically evaluate, especially in a comprehended system. Fortunately, a reliable simulation model will significantly benefit the design and analysis of an optical communication system [41–43] with no exception of QKD.

In general, there are two kinds of simulation models aiming at different targets. Most of the existing QKD simulations are focusing on the theoretical part of the protocols, and always try to catch a tight bound of the secure key rate (SKR) [6,7,11,13,14,44]. The realization scheme of the protocols, as well as the imperfection of the devices, is essential in practical QKD security evaluations. Unfortunately, these vital factors have not been considered meticulously in most of the existing simulation studies. From the perspective of signals and systems, a quantum system can be regarded as the transformation of quantum

* Corresponding author (email: weich@ustc.edu.cn, zfhan@ustc.edu.cn)

signals, and the other QKD simulations are model-based design (MBD) [41–43, 45]. The components in MBD-based frameworks are modeled individually and can build complex systems by combining these devices.

Furthermore, with the help of searching and optimizing algorithms, MBD simulation frameworks will benefit from designing and evaluating quantum information processing systems [45]. Regrettably, the major flaw in existing MBD-based models for QKD is the quantum states and devices are depicted using classical electromagnetic field (EMF) theory. Therefore, it is difficult to precisely simulate some specific quantum procedures in the quantum field, for example, the sub-Poissonian photon statistics and anti-bunching of photons.

QKD is a procedure involving the preparation, propagation, transformation, and measurement of quantum states. In order to subtly evaluate the practical QKD systems, as well as their imperfections, we develop a universal framework for QKD modeling with quantum descriptions. We describe the quantum states of photons and optical components in quantum operators. The states and the devices have multiple dimensions and parameters which can be adjusted independently. Thus the practical characteristics of the optical devices and the disturbance from the eavesdropper or the environment can be simulated comprehensively. We employ C++ language and combine our self-designed packages into OMNet++ [46–48], which is widely adopted in simulations of classical optical systems and networks. The devices are built independently and can be combined to build a complex QKD system. With the software package, we successfully verify single-photon and Hong-Ou-Mandel (HOM) interference [49] optical units, which are the kernel of the BB84 [1] and measurement-device-independent [10] QKD protocols. The simulation results indicate that this quantum-described framework is available for QKD simulation. Furthermore, because OMNet++ is employed widely in simulations of classical optics communication networks, this study shows the feasibility of extending the classical simulation platform like OMNet++ into the field of quantum research with quantum descriptions.

Firstly, we show the design methods of the simulation framework in Section 2. In Section 3, we describe the models of the optical elements in QKD systems, which are the quantum light source and the photons states, the transformation of the photon states with optical devices, and the function of SPDs. Section 4 gives the simulation results of the single-photon and Hong-Ou-Mandel interference with our framework. Finally, we give a conclusion and a short discussion.

2 Design of the simulation framework

A mature QKD modeling framework should achieve equilibrium of multi-features, such as accuracy, scalability, efficiency, operability, compatibility, and cost. Our prime motivation is to design an elaborate modeling framework for the signals, elements, and the procedure in a quantum system with quantum representations. Therefore, we pay more attention to the simulation accuracy of the framework and focus on a discrete-variable-based QKD systems in this study. We design the simulation framework in three layers: the system layer, modeling layer, and implementation layer. The construction and realization of this simulation framework are shown in Figure 1.

Photons are natural carriers for quantum information. The optical units in a QKD system generally execute three steps, which are the preparation of photon states with the light source, manipulation of photon states using optical components, and measurement of photons by detectors. The system layer maps the real-life QKD systems into these three types of simulation units, handles their connections, and dispose of the interaction between the users and the abstract underlying data.

The modeling layer takes charge of the abstract units and their data structures. There are two types of data structures, which are quantum optical devices and quantum signals. The former describes the behaviors of different types of optical devices when photons arrive, and the latter contains the quantum states entering and exiting of the optical devices. Besides providing the quantum description of signals and components, we use the discrete-event driving scheme to handle the quantum processing procedure of the system. The modeling layer is the kernel of the simulation framework, and the details are described

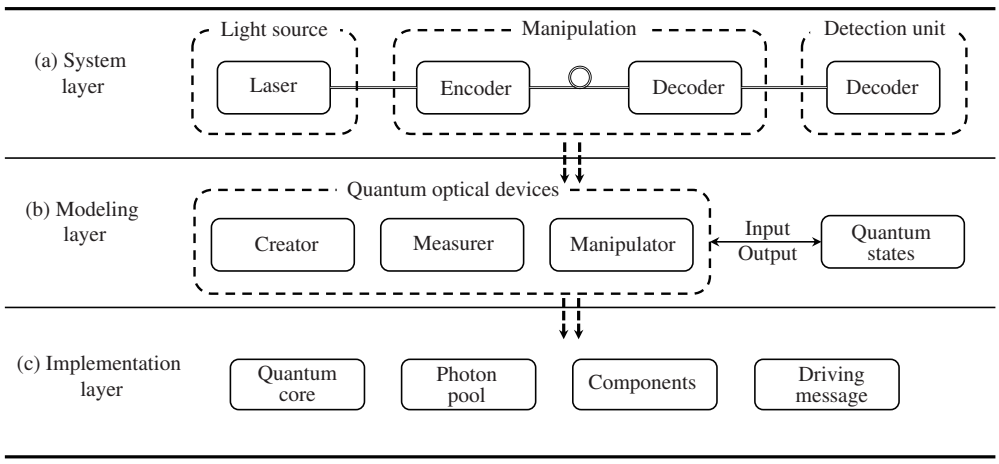

Figure 1 Model construction. (a) System layer: the tripartite optical devices of real-world QKD systems, which consist of the light source, manipulation, and detection units. The quantum states of photons are created by the light source, manipulated by the systems and the channels, and finally measured by detectors. (b) Modeling layer: devices and procedure modeling. Quantum optical devices are modeled as creator, measurer, and manipulator according to the three types of quantum operations in (a). Quantum states transfer the optical devices and are transformed. The quantum signals are passed through the devices through their input and output ports. (c) Implementation layer: realization of the models in modeling layer using C++ classes integrated with OMNet++. Specifically, each optical device is encapsulated as a component class, of which the input and output ports are driven by messages. The quantum pool is a custom-designed array to store the same kind of quantum states, and the quantum core is the processor of the quantum operations like Pauli operators and the projection measurements.

in Section 3.

The implementation layer contains three major packages to handle the evolution of quantum states (QuantumCore), to storage the homogeneous quantum states (PhotonPool), and to process the driving message of arriving photons (Components). We use C++ language to implement the data structure, handle the messages, and execute the procedures (also described in Section 3). We integrate these C++ packages into OMNet++ platform [46–48], and use its visual interface and message-driving engine to verify the simulation.

3 Modeling of quantum state and optical components

The process of QKD can be regarded as the transformations of the quantum states by optical components. Thus, the descriptions of the quantum states are foundational to make the simulation model universal and expansible. The method to descript the quantum states is shown in Subsection 3.1. Furthermore, in Subsections 3.2–3.4, we introduce the modeling of optical components in the order of sequential operations of the quantum states (preparation, manipulation, and measurement).

3.1 Modeling of quantum state

A typical light source for QKD, no matter the weak coherent-state source, sub-Poissonian source, or single-photon source, can be represented with the basis of Fock states in principle. For example, phase-randomized coherent-state light source [6, 50], which has been widely adopted in practical QKD systems, can be described as

$$\rho = \int_0^{2\pi} \frac{\mathrm{d}\theta}{2\pi} |\alpha\rangle\langle\alpha| = \sum_n \frac{\mathrm{e}^{-\mu}\mu^n}{n!} |n\rangle\langle n|, \tag{1}$$

where $\mu = |\alpha^2|$ is the average photon number, while the single-photon state can be regarded as a crucial point of Fock states.

In order to simulate practical QKD systems, the descriptions of the photon states should contain frequently-used physical degrees of freedom. At present, our framework includes five independently

Table 1 Member variables definition of photon state

Variable name	Data type	Explanation
Delay	Double	The relative time delay between the photon states which in a same multi-photon states system
RouteID	Double	The path where the photon state is propagating
SpectralMu	Double	The mean of the Gaussian frequency distribution
SpectralSigma	Double	The standard deviation of the Gaussian frequency distribution
Phase	Double	The relative phrase between the photon states which in a same multi-photon states system
Alpha	Double	The amplitude of the field in the horizontal direction
Beta	Double	The amplitude of the field in the vertical direction
DeltaPhase	Double	The difference between the phase angles of fields in horizontal and vertical directions
Coefficient	Double	The normalization coefficient

operable degrees of freedom for QKD encoding, which are time, path (momenta), phase, polarization, and frequency. The photon state created in path α is given by

$$|\psi\rangle_\alpha = C\int \mathrm{d}\omega\phi(\omega)\mathrm{e}^{-\mathrm{i}(\omega\tau-\varphi)}(\alpha\hat{a}_H^\dagger(\omega)+\beta\mathrm{e}^{-\mathrm{i}\theta}\hat{a}_V^\dagger(\omega))|0\rangle, \tag{2}$$

where C is the normalization coefficient, $\phi(\omega)$ is the frequency distribution assumed to be the Gaussian profile $\phi(\omega)=\frac{\mathrm{e}^{-(\omega-\omega_\mu)^2/4\sigma^2}}{(2\pi)^{1/4}\sqrt{\sigma}}$, $\hat{a}_H^\dagger(\omega)$ represents a creation operators acting on a single frequency mode ω and a polarization mode H, $\hat{a}_V^\dagger(\omega)$ is similar. α and $\beta\mathrm{e}^{-\mathrm{i}\theta}$ are the components of Jones vector [51]. The normalization requires that $\int \mathrm{d}\omega|\phi(\omega)|^2=1$ and $|\alpha|^2+|\beta\mathrm{e}^{-\mathrm{i}\theta}|^2=1$.

We create a photon state class with 9 independently tunable variables according to (2), as shown in Table 1. The parameters of spectrum (SpectralMu and SpectralSigma), pulse width (Delay) and polarization (Alpha, Beta, DeltaPhase) base on the characteristics of the light source user employed. RouteID depends on the connections of the optical devices. C is initialized by $(\frac{1}{\sqrt{n!}})^{\frac{1}{n}}$ to ensure the normalization of n-photon Fock state, $\frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle$.

According to the design above, we can depict the quantum states of the photons with the basis of Fock states. Furthermore, we merge the photons from an individual system with common attributes, for example, the photons from a laser source into a common data set. This data set noted as PhotonPool, which is dynamic in our modeling framework, can be created by emitting a light pulse from a laser source, merged by the correlation among individual systems, and pruned by measuring all its photon. In a PhotonPool, each photon can be described with the superposition of the photon states mentioned above, and the photon state is the fundamental element of this data structure. The data structure is shown in Figure 2 and the quantum state of a PhotonPool can be described as

$$|\psi\rangle_{\mathrm{PhotonPool}}=(|\psi\rangle_{11}+|\psi\rangle_{12}+\cdots)(|\psi\rangle_{21}+|\psi\rangle_{22}+\cdots)\times\cdots=\prod_m\sum_n|\psi\rangle_{mn}, \tag{3}$$

where $|\psi\rangle_{mn}$ denotes the nth photon state of the mth photon.

3.2 Modeling of the quantum-state preparation

In our model, the pulsed laser prepares a quantum state is equivalent to create and initialize a PhotonPool. The photon number of an initialized PhotonPool is a random number generated by a random number generator with a specific probability distribution related to the character of the laser source. For example, for a weak-coherent source, the photon number follows a Poisson distribution, as shown in (1).

In addition, each photon of the PhotonPool initially contains only one photon state without any manipulation. The initial value of the variables listed in Table 1 is assigned according to the character of a laser source. For undefined characters, the initial values can be constants or random numbers with a uniform distribution, according to the requirement of the users.

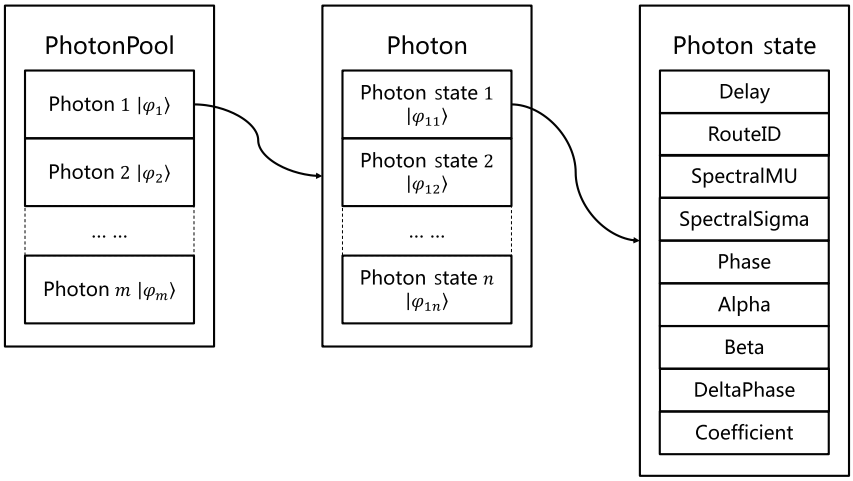

Figure 2 Data structure for the depiction of PhotonPool. The quantum state, as a constitution of photons, is stored in a PhotonPool which is an array of photons. In PhotonPool, each photon consists of the superposition of photon states, which is the basic element of the data structure and contains the information of the degrees of freedom listed in Table 1.

Therefore, the quantum state of an initialized PhotonPool can be expressed as

$$|\psi\rangle_{\text{NewPhotonPool}} = |\psi\rangle_{11}|\psi\rangle_{21}\cdots = \prod_m |\psi\rangle_{m1}, \tag{4}$$

where the $|\psi\rangle_{m1}$ is an initialized photon state of mth photon. $|\psi\rangle_{m1}$ can be derived by (2):

$$|\psi\rangle_{m1} = C_0 \int \mathrm{d}\omega\phi(\omega)\mathrm{e}^{-\mathrm{i}(\omega\tau_0-\varphi_0)}(\alpha_0\hat{a}_H^\dagger(\omega) + \beta_0\mathrm{e}^{-\mathrm{i}\theta_0}\hat{a}_V^\dagger(\omega))|0\rangle, \tag{5}$$

where the subscripts represent the initial value.

Moreover, the size of PhotonPool is finite, however, a phase-randomized coherent state has infinite components of Fock states. Therefore, a truncation is essential to the practical simulation. The users can select the starting Fock state of the truncation on demand. Also, here we provide a reference method of truncation.

Because the photon number of a phase-randomized coherent state is a random variable following the Poisson distribution and the number of the trials N_μ that preparing the weak coherent state with a mean photon number μ in a QKD task is finite, the truncation point n_t can be given by the minimal solution which satisfies the following equation:

$$\epsilon_t = 1 - \left(\sum_{n=0}^{n_t} \frac{\mathrm{e}^{-\mu}\mu^n}{n!}\right)^{N_\mu}, \tag{6}$$

where ϵ_t is a security parameter, which indicates the probability that the maximal photon number in N_μ trials is not less than n_t. So the photon numbers which are greater than n_t can be discarded with a failure probability of ϵ_t.

3.3 Modeling of the quantum-state manipulation

The photon states can be created, modified, or annihilated by optical components. The linear optical devices in QKD systems, as well as the quantum channels like fiber and free-space, are regarded as the manipulations of the photon states. These devices can be divided into two categories according to whether the device contains path-depending operation. The path-depending operation is completed by a beamsplitter (BS) or a polarization beamsplitter (PBS), and other optical elements only change the parameters of the photon states without creating or merging any optical path.

When a BS or a PBS splits the path states of the photons from one path to two paths, new photon states with different values of RouteID are created and added to the state set of the photons. The BS and

Table 2 Member variables definition of BS and PBS

Component	Variable name	Data type	Explanation
Beamsplitter	SplittingRatioR	Double	Reflectance
	SplittingRatioT	Double	Transmittance
	Loss	Double	Loss
	ExtinctionRatio	Double	ExtinctionRatio
Polarization beamsplitter	Loss	Double	Loss
	LossH	Double	The loss of the field in the horizontal direction
	LossV	Double	The loss of the field in the vertical direction

Table 3 Common modeled optical elements

Attenuator	Bandpass filter	Circulator	Polarization modulator
Phase modulator	Isolator	1×2 optical switch	Waveplate
Fiber	Faraday mirror (FM)		

PBS also can correlate the incident photons from different paths. Therefore, the merging of PhotonPools can occur if the incident photons belonging to different PhotonPool.

The path-splitting operations of BS and PBS can be described as follows:

$$\hat{a}^\dagger(\omega) \to \sqrt{T}\hat{c}^\dagger(\omega) - \sqrt{R}\hat{d}^\dagger(\omega), \tag{7}$$

$$\hat{b}^\dagger(\omega) \to \sqrt{T}\hat{c}^\dagger(\omega) + \sqrt{R}\hat{d}^\dagger(\omega), \tag{8}$$

$$\hat{a}_H^\dagger(\omega) \to \hat{c}_H^\dagger(\omega), \quad \hat{a}_V^\dagger(\omega) \to \hat{d}_V^\dagger(\omega), \tag{9}$$

$$\hat{b}_H^\dagger(\omega) \to \hat{d}_H^\dagger(\omega), \quad \hat{b}_V^\dagger(\omega) \to \hat{c}_V^\dagger(\omega), \tag{10}$$

where T and R are the transmissivity and the reflectivity of the elements, respectively. Eqs. (7) and (8) and Eqs. (9) and (10) describe the actions of a BS and a PBS, individually.

Eqs. (7)–(10) characterize the behaviors of the BS and PBS. However, the parameters like transmission loss and the extinction ratio of the optical devices should match the parameters of the off-the-shelf devices. The modified equations are

$$\hat{a}^\dagger(\omega) \to \sqrt{10^{\frac{-l}{10}}T}\hat{c}^\dagger(\omega) - \sqrt{10^{\frac{-l}{10}}R}\hat{d}^\dagger(\omega), \tag{11}$$

$$\hat{b}^\dagger(\omega) \to \sqrt{10^{\frac{-l}{10}}T}\hat{c}^\dagger(\omega) + \sqrt{10^{\frac{-l}{10}}R}\hat{d}^\dagger(\omega), \tag{12}$$

$$\hat{a}_H^\dagger(\omega) \to \sqrt{10^{\frac{-l_H}{10}}\frac{R_E}{R_E+1}}\hat{c}_H^\dagger(\omega), \quad \hat{a}_V^\dagger(\omega) \to \sqrt{10^{\frac{-l_V}{10}}\frac{R_E}{R_E+1}}\hat{d}_V^\dagger(\omega), \tag{13}$$

$$\hat{b}_H^\dagger(\omega) \to \sqrt{10^{\frac{-l_H}{10}}\frac{R_E}{R_E+1}}\hat{d}_H^\dagger(\omega), \quad \hat{b}_V^\dagger(\omega) \to \sqrt{10^{\frac{-l_V}{10}}\frac{R_E}{R_E+1}}\hat{c}_V^\dagger(\omega), \tag{14}$$

where R_E is the extinction ratio, l is the loss, l_H and l_V are the polarization dependent loss (PDL). Eqs. (11) and (12) are for a BS and Eqs. (13) and (14) are for a PBS.

According to (11)–(14), the tunable parameters of BS and PBS are shown in Table 2, which can be adjusted according to the specific components and their measurement results in practical experiments.

Optical devices without path state operation are listed in Table 3 and shown in Appendix A in detail. Each optical device is an individual component in the optical device library of the simulation framework and can be instantiated to multiple units and combined to build a simulation scheme. The final states of the incoming photons that go through the whole system can be obtained by calculating the transformations of these units.

Moreover, the channel disturbance is included in the design of the fiber component. Specifically, the random walk theory is used to simulate the normal distributed random disturbance of fiber to the parameters of photon states.

$$a_o = a_i + \delta, \tag{15}$$

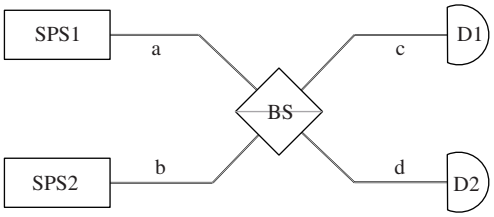

Figure 3 Hong-Ou-Mandel interference at a beam splitter. SPS: single-photon source; BS: beamsplitter; D: detector.

where $a \in \{\varphi, \alpha, \beta, \theta\}$ is one of the parameters of photon state, the subscripts o and i represent the output and input, respectively. δ is the random disturbance that follows a normal distribution:

$$\delta \sim N(\mu_a, \sigma_a), \tag{16}$$

where μ_a and σ_a are the expectation and variance of the distribution and can be estimated by practical data.

The fiber component is common for the polarization maintaining fiber and the single mode fiber by modulating the polarization-dependent μ and σ.

3.4 Modeling of the single-photon detector

In discrete-variable QKD systems, the photon state propagating in a specific path arrives in a single photon detector (SPD) module after creations and transformations. The measurement of photon states is fulfilled by the SPDs together with the optical elements for QKD decoding, and then the photon annihilates.

The simulating system processes the response of SPDs according to the information of the photons stored in PhotonPool. Firstly, the SPD module sends the necessary information to a processing unit named QuantumCore, including the ID of measuring PhotonPool, and the RouteID represents the path where the SPD is located. Secondly, QuantumCore calculates the photon number arrived at SPD and sends the reserved quantum states back to the QuantumPool according to the models of the quantum states and the optical devices mentioned above. Finally, the SPD module calculates the click probability based on its parameters and the photon number that arrives at the SPD. The detailed procedure is explained in the following subsections 3.4.1 and 3.4.2.

3.4.1 *Calculation of the photon numbers*

There are two critical calculations, which are the photon number after projection measurements and the click probability of the photons. QuantumCore firstly calculates the arriving probabilities of the different number of photons according to the final quantum states exited from the optical devices. The probability of $0 \cdots n$ photons arrives at the SPD after projection measurement is $p_0, p_1, \ldots, p_n$ $(\sum_n p_n = 1)$, where n is the photon number with the same path ID as the SPD, which is also the maximum photon number which can arrive at the SPD. Following the Monte Carlo method [52], we randomly assign the instant light pulse arriving at the SPD in a specific path as the Fock states with photon number m $(0 \leqslant m \leqslant n)$ according to the probabilities of p_0 to p_n. As a demonstration, we calculate p_n in a HOM interference with ideal single photons [49] as shown in Figure 3.

The two-photon input state is described as

$$\begin{aligned} |\psi\rangle_{\text{in}} &= C_1 \int \mathrm{d}\omega_1 \phi(\omega_1) \mathrm{e}^{-\mathrm{i}(\omega_1\tau_1 - \varphi_1)} (\alpha_1 \hat{a}_H^\dagger(\omega_1) + \beta_1 \mathrm{e}^{-\mathrm{i}\theta_1} \hat{a}_V^\dagger(\omega_1)) \\ &\quad \times C_2 \int \mathrm{d}\omega_2 \phi(\omega_2) \mathrm{e}^{-\mathrm{i}(\omega_2\tau_2 - \varphi_2)} (\alpha_2 \hat{a}_H^\dagger(\omega_2) + \beta_2 \mathrm{e}^{-\mathrm{i}\theta_2} \hat{a}_V^\dagger(\omega_2)) \\ &= \left(\hat{a}_{1H}^\dagger + \hat{a}_{1V}^\dagger\right) \left(\hat{b}_{2H}^\dagger + \hat{b}_{2V}^\dagger\right) |0\rangle, \end{aligned} \tag{17}$$

where

$$\begin{aligned}\hat{a}_H^\dagger &= C\int \mathrm{d}\omega\phi(\omega)\mathrm{e}^{-\mathrm{i}(\omega\tau-\varphi)}\alpha\hat{a}_H^\dagger(\omega),\\ \hat{a}_V^\dagger &= C\int \mathrm{d}\omega\phi(\omega)\mathrm{e}^{-\mathrm{i}(\omega\tau-\varphi)}\beta\mathrm{e}^{-\mathrm{i}\theta}\hat{a}_V^\dagger(\omega).\end{aligned} \tag{18}$$

The action of BS is given by (11)–(14), and the output state is

$$|\psi\rangle_{\mathrm{out}} = \left(\hat{c}_{1H}^\dagger - \hat{d}_{1H}^\dagger + \hat{c}_{1V}^\dagger - \hat{d}_{1V}^\dagger\right)\left(\hat{c}_{2H}^\dagger + \hat{d}_{2H}^\dagger + \hat{c}_{2V}^\dagger + \hat{d}_{2V}^\dagger\right)|0\rangle. \tag{19}$$

When the measurement occurs in path c, $|\psi\rangle_{\mathrm{out}}$ indicates three possible numbers of photon:

$$\begin{aligned}|\psi_0\rangle &= \left(-\hat{d}_{1H}^\dagger - \hat{d}_{1V}^\dagger\right)\left(\hat{d}_{2H}^\dagger + \hat{d}_{2V}^\dagger\right)|0\rangle,\\ |\psi_1\rangle &= \left(\left(\hat{c}_{1H}^\dagger + \hat{c}_{1V}^\dagger\right)\left(\hat{d}_{2H}^\dagger + \hat{d}_{2V}^\dagger\right)\left(-\hat{d}_{1H}^\dagger - \hat{d}_{1V}^\dagger\right)\left(\hat{c}_{2H}^\dagger + \hat{c}_{2V}^\dagger\right)\right)|0\rangle,\\ |\psi_2\rangle &= \left(\hat{c}_{1H}^\dagger + \hat{c}_{1V}^\dagger\right)\left(\hat{c}_{2H}^\dagger + \hat{c}_{2V}^\dagger\right)|0\rangle.\end{aligned} \tag{20}$$

Thus, the probabilities of different photon numbers are given by $p_i = \langle\psi_i|\psi_i\rangle$, where $i = 0, 1, 2$. For example, for the case of p_0,

$$\begin{aligned}p_0 &= \langle\psi_0|\psi_0\rangle\\ &= \langle 0|\left(-\hat{d}_{1H} - \hat{d}_{1V}\right)\left(\hat{d}_{2H} + \hat{d}_{2V}\right)\left(-\hat{d}_{1H}^\dagger - \hat{d}_{1V}^\dagger\right)\left(\hat{d}_{2H}^\dagger + \hat{d}_{2V}^\dagger\right)|0\rangle.\end{aligned} \tag{21}$$

By such equations, we obtain the probability distribution of the Fock states with different photon numbers. QuantumCore returnes the photon number and updates the variables of the measured PhotonPool for the next measurement. Because the detection of SPD is essentially the projection of the quantum states in a unique path where the SPD lays, and the projection measurement will collapse a photon into a specific state. Therefore, the photons projected successfully would be removed from the PhotonPool, and all states that remain photons with the identical RouteID of the SPD but do not be detected are removed simultaneously. The normalization coefficient of the remaining photon states would be recalculated and updated. The removal of projected photons completes the local measurement on a path. In addition, the update of the remaining photon correlates this measurement with other measurements of new PhotonPool and reflects the non-local properties of a quantum system.

3.4.2 *Calculating the clicking probability*

The clicking events of a SPD are generally composed of three parts, which are the photons arrived, the dark counts (dark current), and the after pulses. We build the SPD module with seven elements, including the response of the photons and their electrical parameters, to cover the realistic characters of the SPD.

The parameters and their definitions are listed in Table 4. The clicking probability p_c can be calculated using the formula:

$$p_c = 1 - ((1-\eta)^n(1-p_d\delta t)(1-p_a)), \tag{22}$$

where η is the detection efficiency, n is the photon number, p_d is the dark count probability, δt is the duration of gating time and p_a is the afterpulse probability of SPD [40].

4 Simulation results

The QKD session is the statistical result of plenty of independent photons with the procedure of preparation, manipulation, and measurement. The encoder and the decoder (codec) is the kernel to perform QKD protocols. Therefore, we simulate the Mach-Zehnder interferometer (MZI) [53, 54] and HOM interference [49], of which the former is the kernel unit in a phase-encoding QKD system and the latter is

Table 4 Member variables definition of SPD

Variable name	Data type	Explanation
DetectionEfficiency	Double	The detection efficiency of the given wavelength
ProbabilityDarkCount	Double	The dark count probability of the SPD
ProbabilityAfterpulse	Double	The afterpulse probability of the SPD
TimingJitter	Double	The jitter of click signal emission time
ResolvesPhotonNumber	Bool	The flag of photon number resolution, when it is true, the SPD return photon number, otherwise it return click signal
Enable	Bool	The flag of SPD on-off state, when it is true, the SPD responds the photon pulse, otherwise it does not work
TimeWidth	Double	The duration of open gate for gate mode

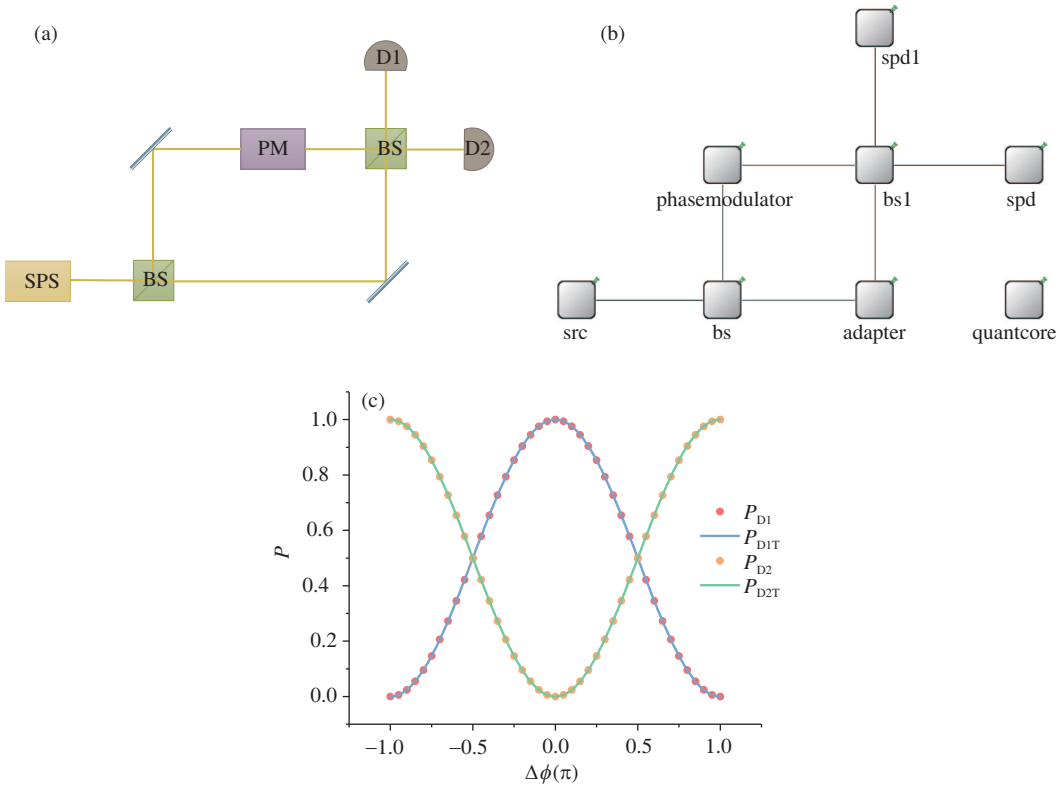

Figure 4 (Color online) Schematic and simulation network of MZI. (a) Schematic diagram of MZI. SPS: single-photon source; BS: beamsplitter; PM: phase modulator; D: detector. (b) Network description of simulation program. src: single-photon source; bs: beamsplitter; phasemodulator: phase modulator; adapter: just for aesthetics; spd: detector; quantcore: QuantumCore. (c) Comparison of simulation results and theoretical calculations. The dotted red and yellow correspond to simulation results P_{D1} and P_{D2}, respectively. The solid blue and green are theoretical curves derived from (24), respectively.

the core of measurement-device-independent (MDI) QKD. It is worth to be mentioned that we perform the simulation by connecting the fundamental elements according to the structure we exam and then importing the excitation signals. In the simulation, we care about the optical structures rather than the protocols. We compare the simulation results obtained according to the behaviors of the photons and comparing them with the theoretical results to demonstrate that the simulation method is appropriate for QKD system simulation.

For the convenience of expression in the article, we use a single-photon source as the input excitation signals of the system. The system also supports various types of light sources such as the weak coherent light source and the entanglement light source.

Figure 4 shows the schematic of an MZI, which is widely used in QKD systems, the combination of the basic units in the simulation system, and the simulation results. The evolution of a photon is described

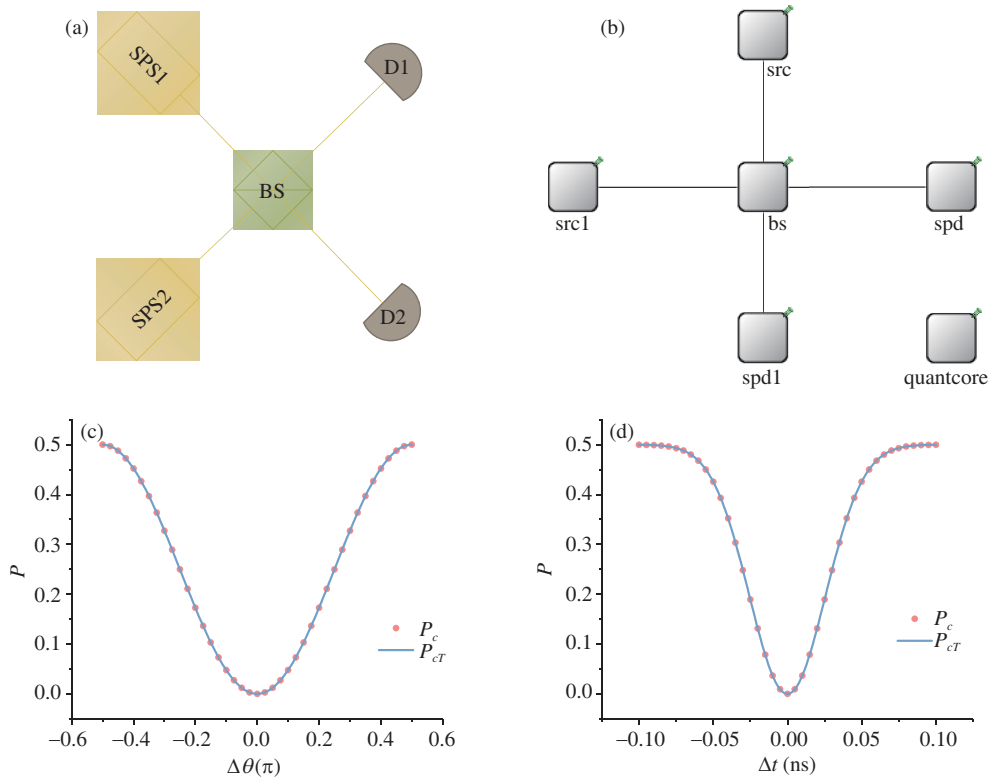

Figure 5 (Color online) Schematic and simulation network of HOM interferometry. (a) Schematic diagram of HOM interferometry. SPS: single-photon source; BS: beamsplitter; D: detector. (b) Network description of simulation program. src: single-photon source; bs: beamsplitter; spd: detector; quantcore: QuantumCore. (c) Comparison of simulation results and theoretical calculations. The dotted red and solid blue correspond to simulation coincidence probability versus $\delta\theta$ and theoretical curves derived from (26), respectively. (d) The dotted red and solid blue correspond to simulation coincidence probability as a function of δt and theoretical curves derived from (27), respectively. The σ is 65 GHz, which is a typical value for a 1550 nm laser.

as

$$|a\rangle \xrightarrow{\text{BS1}} \frac{1}{\sqrt{2}}\left(|a\rangle + |b\rangle\right) \xrightarrow{\text{PM}} \frac{1}{\sqrt{2}}\left(|a\rangle + \mathrm{e}^{\mathrm{i}\phi}|b\rangle\right) \xrightarrow{\text{BS2}} \frac{1}{2}\left(\left(\mathrm{e}^{\mathrm{i}\phi}+1\right)|c\rangle + \left(\mathrm{e}^{\mathrm{i}\phi}-1\right)|d\rangle\right). \tag{23}$$

The theoretical probabilities of detecting the photon at D1 (path c) and D2 (path d) are given by

$$P_{\mathrm{D1T}} = \frac{1+\cos(\phi)}{2}, \quad P_{\mathrm{D2T}} = \frac{1-\cos(\phi)}{2}. \tag{24}$$

From Figure 4(c), we can see that the simulation results are in agreement with the theoretical result, according to (24).

The simulation of HOM interference with polarization encoding is shown in Figure 5. The coincidence probability can be characterized by the relative differences in polarization and arriving time. Without loss of generality, we can depict the relative polarization difference $\delta\theta$ of the two input photon as $|\psi_1\rangle = \hat{a}^\dagger_{1H}|0\rangle, |\psi_2\rangle = (\alpha\hat{b}^\dagger_{2H} + \beta\hat{b}^\dagger_{2V})|0\rangle$, where $\alpha = \cos(\delta\theta)$, $\beta = \sin(\delta\theta)$, $|\alpha|^2 + |\beta|^2 = 1$. Then the output state of the BS is given by

$$|\psi_o\rangle = \frac{1}{2}\left(\hat{a}^\dagger_{1H} + \hat{b}^\dagger_{1H}\right)\left(\alpha\left(\hat{a}^\dagger_{2H} - \hat{b}^\dagger_{2H}\right) + \beta\left(\hat{a}^\dagger_{2V} - \hat{b}^\dagger_{2V}\right)\right)|0\rangle, \tag{25}$$

and the theoretical coincidence probability of getting one photon in each path is given by

$$P_{cT} = \frac{|\beta|^2}{2}. \tag{26}$$

Taking the arriving time of individual photons into account, the theoretical coincidence probability is [49]

$$P_{cT} = \frac{1}{2} - \frac{1}{2}\mathrm{e}^{-\sigma^2\delta t^2}, \tag{27}$$

where σ is the standard deviation of the Gaussian frequency distribution, as shown in (2). The relationship between σ and the full width at half maximum (FWHM) of the frequency spectrum is given by

$$\mathrm{FWHM} = 2\sqrt{2\ln(2)}\sigma. \tag{28}$$

By comparing the results shown in Figure 5, we can see that the module-based simulation results of HOM interference are finely consistent with the theoretical results according to (26) and (27). Because the polarization and the arriving time variations relate to the practical issues of the photon states, the results also indicate the availability of independent operations of the physical variables of photons and show potentials for practical QKD system analysis.

5 Conclusion and discussion

We introduced a universal framework for simulation of practical QKD systems. We treat the processing procedure of a QKD system as the cascade transformations to quantum states, which are described with the quantum operators. The processing based on quantum states reflects the non-local properties. The event-driven mechanism of the framework focuses on the detailed quantum procedure of the system, which is commonly ignored in most of the existing simulation studies. The multi-dimension descriptions of the signal and the elements make the model universal to evaluate the QKD system of variable protocols, as well as the practical non-idealities of the system.

Compared with traditional numerical simulations, although our model is at a disadvantage of time consumption, it can precisely and vividly demonstrate the imperfections of practical devices, which is nearly impossible to deduce an analytical formula. Moreover, our program can be further optimized for high running speed. The parallel computing running on a GPU is an option, which can significantly save the time. Also, replacing the Fock basis with the coherent state is convenient for the simulations based on weak coherent sources, that is, the optical elements operate the coherent state directly, although such changes can weaken the universality. Therefore, our model has a distinct advantage of simulating the imperfections of practical devices in quantum language. The time consumption is acceptable and can be reduced further.

It is worth indicating that although this simulation framework provides a possible way for QKD system evaluation, it is constrained when simulating complex systems or signals with multi-photons owing to its computational complexity. There are challenging studies to optimize the model and the computational process of the software before making it valid for designing QKD systems or evaluating their potential security issues in practice.

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2018YFA0306400), National Natural Science Foundation of China (Grant Nos. 61627820, 61675189, 61622506, 61822115), Anhui Initiative in Quantum Information Technologies (Grant No. AHY030000). We also appreciate Dr. Xuebi AN and Yuyang DING of Anhui Qasky, Co. Ltd. for helpful discussion.

References

1 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of Conference on Computers, Systems and Signal Processing, Bangalore, 175
2 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663
3 Gottesman D, Lo H K, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices. In: Proceedings of International Symposium on Information Theory, Chicago, 2004. 136
4 Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The security of practical quantum key distribution. Rev Mod Phys, 2009, 81: 1301–1350
5 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett, 2005, 94: 230503
6 Lo H K, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett, 2005, 94: 230504
7 Tomamichel M, Renner R. Uncertainty relation for smooth entropies. Phys Rev Lett, 2011, 106: 110506
8 Laing A, Scarani V, Rarity J G, et al. Reference-frame-independent quantum key distribution. Phys Rev A, 2010, 82: 012304

9 Yin Z Q, Wang S, Chen W, et al. Reference-free-independent quantum key distribution immune to detector side channel attacks. Quantum Inf Process, 2014, 13: 1237–1244
10 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503
11 Curty M, Xu F, Cui W, et al. Finite-key analysis for measurement-device-independent quantum key distribution. Nat Commun, 2014, 5: 3732
12 Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance. Nature, 2014, 509: 475–478
13 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
14 Rusca D, Boaron A, Grünenfelder F, et al. Finite-key analysis for the 1-decoy state QKD protocol. Appl Phys Lett, 2018, 112: 171104
15 Lucamarini M, Yuan Z L, Dynes J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature, 2018, 557: 400–403
16 Ma X, Zeng P, Zhou H. Phase-matching quantum key distribution. Phys Rev X, 2018, 8: 031043
17 Wang X B, Yu Z W, Hu X L. Twin-field quantum key distribution with large misalignment error. Phys Rev A, 2018, 98: 062323
18 Cui C, Yin Z Q, Wang R, et al. Twin-field quantum key distribution without phase postselection. Phys Rev Appl, 2019, 11: 034053
19 Peng C Z, Zhang J, Yang D, et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. Phys Rev Lett, 2007, 98: 010505
20 Dixon A R, Yuan Z L, Dynes J F, et al. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. Opt Express, 2008, 16: 18790
21 Wang S, Yin Z Q, Chen W, et al. Experimental demonstration of a quantum key distribution without signal disturbance monitoring. Nat Photon, 2015, 9: 832–836
22 Wang C, Song X T, Yin Z Q, et al. Phase-reference-free experiment of measurement-device-independent quantum key distribution. Phys Rev Lett, 2015, 115: 160502
23 Takesue H, Sasaki T, Tamaki K, et al. Experimental quantum key distribution without monitoring signal disturbance. Nat Photon, 2015, 9: 827–831
24 Yin H L, Chen T Y, Yu Z W, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys Rev Lett, 2016, 117: 190501
25 Comandar L C, Lucamarini M, Fröhlich B, et al. Quantum key distribution without detector vulnerabilities using optically seeded lasers. Nat Photon, 2016, 10: 312–315
26 Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground quantum key distribution. Nature, 2017, 549: 43–47
27 Fröhlich B, Lucamarini M, Dynes J F, et al. Long-distance quantum key distribution secure against coherent attacks. Optica, 2017, 4: 163–167
28 Boaron A, Boso G, Rusca D, et al. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett, 2018, 121: 190502
29 Wang S, Chen W, Yin Z Q, et al. Practical gigahertz quantum key distribution robust against channel disturbance. Opt Lett, 2018, 43: 2030
30 Wang S, He D Y, Yin Z Q, et al. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. Phys Rev X, 2019, 9: 021046
31 Minder M, Pittaluga M, Roberts G L, et al. Experimental quantum key distribution beyond the repeaterless secret key capacity. Nat Photon, 2019, 13: 334–338
32 Zhong X, Hu J, Curty M, et al. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. Phys Rev Lett, 2019, 123: 100506
33 Liu Y, Yu Z W, Zhang W, et al. Experimental twin-field quantum key distribution through sending or not sending. Phys Rev Lett, 2019, 123: 100505
34 Chen J P, Zhang C, Liu Y, et al. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. 2020, 124: 070501
35 Lo H K, Curty M, Tamaki K. Secure quantum key distribution. Nat Photon, 2014, 8: 595–604
36 Yoshino K, Fujiwara M, Nakata K, et al. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. npj Quantum Inf, 2018, 4: 8
37 Angrisani L, D'Arco M. Modeling timing jitter effects in digital-to-analog converters. IEEE Trans Instrum Meas, 2008, 58: 330–336
38 Wang F X, Chen W, Li Y P, et al. Non-Markovian property of afterpulsing effect in single-photon avalanche detector. J Lightw Technol, 2016, 34: 3610–3615
39 Zhang J, Itzler M A, Zbinden H, et al. Advances in InGaAs/InP single-photon detector systems for quantum communication. Light Sci Appl, 2015, 4: e286
40 Fan-Yuan G J, Wang C, Wang S, et al. Afterpulse analysis for quantum key distribution. Phys Rev Appl, 2018, 10: 064032
41 Buhari A, Zukarnain Z A, Subramaniam S K, et al. An efficient modeling and simulation of quantum key distribution protocols using OptiSystem^{TM}. In: Proceedings of IEEE Symposium on Industrial Electronics and Applications, 2012. 84–89
42 Mailloux L O, Morris J D, Grimaila M R, et al. A modeling framework for studying quantum key distribution system

implementation nonidealities. IEEE Access, 2015, 3: 110–130
43 Archana B, Krithika S. Implementation of bb84 quantum key distribution using optsim. In: Proceedings of the 2nd International Conference on Electronics and Communication Systems (ICECS), 2015. 457–460
44 Ma X, Qi B, Zhao Y, et al. Practical decoy state for quantum key distribution. Phys Rev A, 2005, 72: 012326
45 Krenn M, Malik M, Fickler R, et al. Automated search for new quantum experiments. Phys Rev Lett, 2016, 116: 090405
46 Varga A. Using the OMNeT++ discrete event simulation system in education. IEEE Trans Educ, 1999, 42: 11
47 Varga A. Discrete event simulation system. In: Proceedings of the European Simulation Multiconference (ESM'001), 2001. 1–7
48 Varga A, Hornig R. An overview of the OMNeT++ simulation environment. In: Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, 2008. 1–10
49 Hong C K, Ou Z Y, Mandel L. Measurement of subpicosecond time intervals between two photons by interference. Phys Rev Lett, 1987, 59: 2044
50 Glauber R J. Coherent and incoherent states of the radiation field. Phys Rev, 1963, 131: 2766–2788
51 Jones R C. A new calculus for the treatment of optical systems. I. description and discussion of the calculus. J Opt Soc Am, 1941, 31: 488–493
52 Metropolis N, Ulam S. The Monte Carlo method. J Am Stat Assoc, 1949, 44: 335–341
53 Zehnder L Z. Ein neuer interferenzrefraktor. Instrumentenkunde, 1891, 11: 275–285
54 Mach L. Ueber einen interferenzrefraktor. Zeitschrift für Instrumentenkunde, 1892, 12: 89

Appendix A

We show the details regarding the model optical elements in Table A1. All input and output parameters are denoted by subscript i and o, respectively.

Table A1 Explanation and output of optical element

Optical element	Variable name	Explanation
Attenuator	Loss	The loss of attenuator
		$C_o = C_i\sqrt{10^{\frac{-l}{10}}}$, where l is the loss.
Bandpass filter	Loss	The loss of bandpass filter
		$C_o = C_i\sqrt{10^{\frac{-l_\omega}{10}}}$, where l_ω is the loss when the photon frequency is ω.
Circulator	Loss	The insertion loss of circulator
		$C_o = C_i\sqrt{10^{\frac{-l}{10}}}$, where l is the insertion loss.
Polarization modulator	Alpha	The target value of the amplitude of the field in the horizontal
	Beta	The target value of the amplitude of the field in the vertical
	DeltaPhase	The target value of the difference between the phase angles of fields in horizontal and vertical directions
	Loss	The insertion loss of polarization modulator
		$\alpha_o = \alpha,\ \beta_o = \beta,\ \delta\theta_o = \delta\theta,\ C_o = C_i\sqrt{10^{\frac{-l}{10}}}$, where $\alpha, \beta, \delta\theta$ are the target value of the polarization parameters and l is the insertion loss.

(*To be continued on the next page*)

(*Continued*)

Optical element	Variable name	Explanation
Phase modulator	Phase	The target value of the phase
	Loss	The insertion loss of phase modulator
		$\varphi_o = \varphi, C_o = C_i\sqrt{10^{\frac{-l}{10}}},$ where φ are the target value of phase and l is the insertion loss.
Isolator	Loss	The insertion loss of isolator
	IsolationLoss	The isolation loss of isolator
		$\begin{cases} C_o = C_i\sqrt{10^{\frac{-l+l_i s}{10}}}, & \text{transmitting along the forward direction,} \\ C_o = C_i\sqrt{10^{\frac{-l}{10}}}, & \text{transmitting along the reverse direction,} \end{cases}$ where l is the insertion loss and $l_i s$ is the isolation loss.
1×2 optical switch	Loss	The insertion loss of optical switch
	IsolationLoss	The isolation loss of optical switch
		$\begin{cases} C_o = C_i\sqrt{10^{\frac{-l+l_i s}{10}}}, & \text{emitting from the desired output port,} \\ C_o = C_i\sqrt{10^{\frac{-l}{10}}}, & \text{emitting from the undesired output port,} \end{cases}$ where l is the insertion loss and $l_i s$ is the isolation loss.
Waveplate	RelativePhase	The phase shift between polarization components, π for a half-wave plate and π/2 for a quarter-wave plate
	OffsetAngle	The angle of the fast axis
	Loss	The insertion loss of the waveplate
		The Stokes vector of input photon state is given by $S_i = \left(1, \alpha_i^2 - \beta_i^2, 2\alpha_i\beta_i\cos\delta\theta_i, 2\alpha_i\beta_i\sin\delta\theta_i\right)^{\mathrm{T}},$ where α and β are the amplitudes of the field in the horizontal and vertical direction respectively, $\delta\theta$ is the difference between the phase angles of fields in horizontal and vertical directions. The Mueller matrice of the waveplate is given by $M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\theta)+\cos(\delta)\sin^2(2\theta) & \cos(2\theta)\sin(2\theta)-\cos(2\theta)\cos(\delta)\sin(2\theta) & \sin(2\theta)\sin(\delta) \\ 0 & \cos(2\theta)\sin(2\theta)-\cos(2\theta)\cos(\delta)\sin(2\theta) & \cos(\delta)\cos^2(2\theta)+\sin^2(2\theta) & -\cos(2\theta)\sin(\delta) \\ 0 & -\sin(2\theta)\sin(\delta) & \cos(2\theta)\sin(\delta) & \cos(\delta) \end{pmatrix},$ where θ is the OffsetAngle and δ is the RelativePhase. Then the Stokes vectors of output photon state is given by $S_o = S_i M = (S_0, S_1, S_2, S_3)^{\mathrm{T}}.$ So the polarization parameters of output photon state become $\alpha_o = \sqrt{1+S_1},\ \beta_o = \sqrt{1-S_1},\ \delta\theta_o = \begin{cases} 0, & \alpha_o\beta_o = 0, \\ \arccos\left(\frac{S_2}{2\alpha_o\beta_o}\right), & \alpha_o\beta_o \neq 0,\ S_2 \geqslant 0, \\ -\arccos\left(\frac{S_2}{2\alpha_o\beta_o}\right), & \alpha_o\beta_o \neq 0,\ S_2 < 0, \end{cases}$ Also, the output normalization coefficient is given by $C_o = C_i\sqrt{10^{\frac{-l}{10}}},$ where l is the insertion loss.

(*To be continued on the next page*)

(*Continued*)

Optical element	Variable name	Explanation
Single mode (SM) fiber	Alpha	The loss of SM fiber per kilometer
	Length	The length of SM fiber
	Sigma	The variance of the normal distribution for random disturbance
	Expectation	The expectation of the normal distribution for random disturbance
		$C_o = C_i\sqrt{10^{\frac{-Al}{10}}},\ a_o = a_i + \delta,\ \delta \sim N(\mu_a, \sigma_a)$, where A is the Alpha, l is the Length, μ_a and σ_a are the Expectation and Sigma, respectively, and $a \in \{\varphi, \alpha, \beta, \theta\}$. For an ideal polarization maintaining fiber, the polarization-dependent μ and σ should be 0.
Faraday mirror (FM)	Loss	The insertion loss of FM
	Theta	The faraday rotation of a single pass
		A Faraday mirror is a combination of a Faraday rotator and an ordinary mirror whose Jones matrix is given by[a)] $$\mathrm{FM} = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix},$$ therefore, $$\mathrm{FM} = \begin{pmatrix} \cos^2(\theta) - \sin^2(\theta) & -2\sin(\theta)\cos(\theta) \\ -2\sin(\theta)\cos(\theta) & \sin^2(\theta) - \cos^2(\theta) \end{pmatrix},$$ where θ is the Theta. Then the output photon state is given by $$\mathrm{e}^{\mathrm{i}\varphi} \begin{pmatrix} \alpha_o \\ \beta_o \mathrm{e}^{\mathrm{i}\theta_o} \end{pmatrix} = \mathrm{FM} \begin{pmatrix} \alpha_i \\ \beta_i \mathrm{e}^{\mathrm{i}\theta_i} \end{pmatrix},\ \varphi_o = \varphi_i + \varphi.$$ Also, the output normalization coefficient is given by $$C_o = C_i\sqrt{10^{\frac{-l}{10}}},$$ where l is the insertion loss.

a) Mo X F, Zhu B, Han Z F, et al. Faraday-Michelson system for quantum cryptography. Opt Lett, 2005, 30: 2632–2634.