Detection loophole-free photon key distribution using coherent light

Byoung S. Ham
Center for Photon Information Processing, School of Electrical Engineering and Computer Science, Gwangju
Institute of Science and Technology
123 Chumdangwagi-ro, Buk-gu, Gwangju 61005, S. Korea
(Submitted on August 3, 2018; Resubmitted on Oct. 25, 2018; bham@gist.ac.kr)

Over the last three decades quantum key distribution (QKD) has been intensively studied for the unconditionally secured cryptography based on quantum mechanics. Due to the quantum loopholes of imperfect detectors, however, QKD has been fragile to quantum hacking. In addition, the lack of deterministic single photon and entangled photon pair generations may prevent current QKD from commercial applications such as online banking. Here, by using bright coherent light as a photon key carrier in paired channels of a Mach-Zehnder interferometer (MZI), detection loophole-free photon key distribution (PKD) is proposed for the unconditionally secured cryptography, where PKD is compatible with current fiber-optic communications networks. The unconditional security of PKD is owing to the complete randomness of eavesdropping in the paired channels of MZI. The proposed PKD is distance unlimited owing to the compatibility with coherence optics and robust to channel noise and intensity/phase fluctuations of the carrier lights owing to the MZI characteristics.

INTRODUCTION

The unconditional security in quantum key distribution (QKD) is provided by quantum mechanics of no-cloning theorem and/or Bell’s inequality. However, the unconditional security is not fully guaranteed in practice due to mainly the detection loophole by imperfect detectors. This detection loophole affects all QKD protocols of single photon-based, entangled photon-based, and coherent light-based (cv) protocols. Thus, the quantum hacking is always open to eavesdroppers, and QKD becomes a practical issue unless the detection loophole is completely closed. For example, in a standard optical fiber whose loss is 10^{-2} per 100 km, the actual quantum bit rate (QBR) drops down to 10^{-4}, resulting in only ~kilo-bits per second (bps) at most. Besides, other practical issues such as nondeterministic single photon and entangled photon-pair generations make current QKD extremely inefficient compared with the classical counterpart. Most of all, current QKD is not compatible with conventional fiber-optic communications networks mainly due to nonlinear optics devices such as optical amplifiers violating the no-cloning theorem. Thus, the transmission distance in QKD has been limited. For multiparty QKD in the future quantum networks, multipartite entangled photon pairs are prerequisite but their generation is extremely unrealistic.

The one-time-pad cryptography has been a long-lasting goal in human history for a perfect communication security. Here, a completely different concept of unconditionally secured photon key distribution (PKD) is presented by using classical (coherence) optics in paired channels of Mach-Zehnder interferometer (MZI). Owing to coherence optics, PKD does not rely on nonclassical light and thus free from the no-cloning theorem in QKD. In other words, PKD has no limit in transmission distance and QBR is compatible with that in current fiber-optic communications. The unconditional security in PKD is based on quantum superposition between the paired channels of MZI, where absolute phase information cannot be extracted unless the input phase information is known. Any measurement trial in the MZI channels reveals the eavesdropper due to the fringe shift in the output. This fringe shift is compatible with the measurement-caused destruction of a quantum state in QKD, resulting in the foundation of the unconditional security in a classical version. Although an eavesdropper can technically measure relative phase information between the paired channels of MZI without shifting the output fringe, the measured information has no meaning due to complete randomness as in BB84 E91 using double polarization/phase bases. Thus, the proposed PKD offers a detection loophole-free unconditionally secured cryptography keeping all benefits of coherence optics such as cloning, switching, and storing. Owing to the compatibility with current optical systems of fiber-optic communications networks, the long-lasting goal of one-time-pad can be implemented by the proposed
PKD due to ultralow error rate at ultrahigh speed. Here, it should be noted that the paired channels of MZI in PKD are not for the encoding (by a sender) or decoding (by a receiver) as in current (B91-related) QKD protocols, but for the communication channel itself. Unlike all other QKDs relying on no-cloning theorem in a single communication channel, the proposed PKD relies on quantum superposition of double communications channels in MZI. Therefore, the unconditional security of PKD is not provided by the no-cloning theorem, but by the measurement indistinguishability in the double channels of MZI.

The rate-distance relation of an optical carrier roots in the optical loss in a channel. In a standard optical fiber, the polarization and phase of traveling light degrade as it propagates, which is the main bottleneck of the current QKDs for long-haul transmission. A typical detection efficiency of commercial photodiodes at telecommunication wavelengths is about 30%, so the success rate of measurement is roughly one out of three events, resulting in a serious chance of eavesdropping. The first QKD protocol, BB84, is based on Heisenberg’s uncertainty principle of two nonorthogonal polarization bases for single photons. Practically, however, BB84-based QKD uses weak coherent light with decoy states, but even the decoy states does not guarantee the unconditional security. E91-based QKD such as MDI- and DDI-QKD based on entangled photon pairs has also been failed in the unconditional security due to the detection loophole as well as the Bell’s inequality violation loophole. Although the optical loss in an optical fiber results in exponential decay in the QBR as a function of distance, quantum bit error rate (QBER) actually sets the practical upper bound of the QBR due to mainly the detection loophole. Unless the detection loophole is completely closed, current QKD protocols cannot guarantee unconditional security, and their QBR is unrealistically low to be commercialized for such as online banking. Most of all, current QKDs are not compatible with current optical systems because of the use of nonclassical lights violating cloning.

Owing to strong demand in both wired and wireless communications, the information traffic in an optical fiber has increased three fold every two years over the last thirty years. In commercial applications of optical communications, a traffic speed of 100 Gbps per (wavelength) channel has been deployed for 80 channels in a dense wavelength division multiplexing system, resulting in a total capacity of 8 Tbps in a single-core optical fiber. Thus, the capacity per fiber will reach its theoretical upper bound of 100 Tbps in a decade. Eventually a multicore fiber will replace the single-core fiber in the near future to overcome the capacity saturation. In the multi-core fiber, the environmental noise such as vibrations and temperature causing a relative path-length drift in the MZI is frozen due to spatial proximity between cores in a micron scale. Thus, the basic infrastructure of the double channels satisfying the MZI system for the present PKD is provided with the multicore fiber in the near future fiber-optic communications networks.

To understand the basic physics of the present PKD, we review the beam splitter matrix and the double MZI unitary transformation. Then, the PKD protocol is presented in a phase controlled double MZI (PhD-MZI) system, where the phase (key) selection by one party is supposed to be automatically confirmed by the other party. For PKD, we use two phase bases to provide a random eavesdropping chance given by MZI physics. The phase shifter \( \Phi \) in Fig. 1 is used for random phase selection and directional determinacy in the outputs. This directional determinacy prohibits the typical intercept and resend technique from eavesdropping (discussed later). Universal quantum gate operations such as Hadamard gates have been presented in a phase shifter-coupled MZI. The present PhD-MZI scheme also satisfies the unitary operation for PKD (analyzed in Figs. 2 and 3). Like the nonorthogonal polarization bases in BB84, the phase bases play the same role of indistinguishability-induced randomness in measurement due to quantum superposition of the double MZI channels, resulting in prefect randomness for eavesdropping. The unconditional security of the present PKD is also achieved by the phase-dependent directionality resulting in a distinct visibility. Here, it should be noted that the beam splitter (BS) matrix is sustained for both coherence and incoherence optics. For coherence optics, the split lights are perfectly coherent regardless of the bandwidth, intensity fluctuation, and phase noise. For incoherence optics, intensity correlation (or 4th order interference) has been proved for a bunching phenomenon with the particle nature of light. The present PKD belongs to coherence optics but is not limited whether it is a wave (coherent light) or a particle (a single photon).

The BS matrix was firstly discussed in 1979 by Degiorgio and generalized in 1980 by Zeilinger, where there exists a \( \pi/2 \) phase difference between the split lights, the transmitted \( (E_t) \) and reflected \( (E_r) \) ones as shown in Fig. 1. Thus, the BS matrix \([BS]\) is represented by:
resulting in $E_3 = \frac{E_i}{\sqrt{2}}$ and $E_4 = \frac{iE_i}{\sqrt{2}}$. There is no way to measure the absolute phase of light in each path, unless the input light ($E_i$) is given as a reference. More importantly, the measurement itself destroys the key idea of indistinguishability in the quantum superposition between two paths in MZI. In other words, any trial of measurement destroys the interference fringe in the outputs, offering the basic physics of unconditional security. Thus, the superposition of two paths in the MZI represents both Heisenberg’s uncertainty principle and no-cloning theorem even to the bright coherent light. This is the fundamental physics of PKD for the measurement independent or detection loophole-free cryptography. Owing to coherence optics of MZI, the compatibility with classical optics systems is the intrinsic property of PKD without losing the unconditional security in key distribution process.

RESULTS

Quantum superposition of MZI for detection loophole-free measurement

Figure 1 shows a typical MZI scheme composed of two BSs, and the quantum superposition of paths is analyzed for the detection loophole-free key distribution. Mirrors are redundant due to the same phase creation in both paths. The input light $E_i$ impinges on the first BS (BS1), is separated into two parts ($E_3$ and $E_4$), and is merged on the second BS (BS2). Here, the light $E_3$ and $E_4$ are perfectly coherent regardless of the bandwidth, intensity, or phase fluctuations of $E_i$. In other words, MZI works even for a single photon whose phase is random as an upper bound. In Fig. 1a, the MZI matrix representation with a phase shifter $\Phi$ is denoted by:

$$[MZ]_\phi = \frac{1}{2} \begin{bmatrix} 1 - e^{i\phi} & i(1 + e^{i\phi}) \\ i(1 + e^{i\phi}) & -(1 - e^{i\phi}) \end{bmatrix},$$

(2)

where $[\Phi] = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$ and $[MZ]_\phi = [BS][\Phi][BS]$. Thus, the double-pass MZI, $[MZ]^2$ results in an identity matrix:

$$[MZ]^2 = (-e^{i\phi}) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

(3)

where, the matrix $[MZ]_\phi$ satisfies the unitary operation. The physical meaning of the unitary transformation by MZI is a reversible process, which is the key concept of not only quantum optics but also coherence optics such as photon storage. Here, the global phase has nothing to do with measurements, so is neglected for the unitary operation.

If there is no relative phase difference ($\phi = 0$) between two paths of MZI, the outputs light become unidirectional: $E_5 = 0$; $E_6 = iE_i$. The factor “$i$” represents a phase induced by the MZI with respect to the input light $E_i$. This phase factor has nothing to do with measurement, either. If a $\pi$–phase shift ($\phi = \pi$) is given in the MZI path, then the output light direction is switched: $E_5 = E_i$; $E_6 = 0$. Thus, the output directionality of MZI is controllable by adjusting the phase $\phi$, resulting in distinctive visibility as shown in Fig. 1b (see the green and red dots in the solid curve). These two $\phi$–values of 0 and $\pi$ are used for potential bases (keys) in the present PKD (discussed below).

Allowing ideal and independent measurements in the paths of MZI without altering the output interference fringe, the analysis in both visibility and interference between $E_3$ and $E_4$ gives the basic physics of randomness for eavesdropping. The two $\phi$–values used for distinct visibility in Fig. 1b show complete indistinguishability in Fig. 1c due to the fundamental physics of quantum superposition between two paths in MZI: a definite knowledge for one light results in complete randomness in the other. The $\phi$–independent uniform visibility in Fig. 1c is obvious due to phase independency in measurements: $|E_3|^2 = |E_4|^2$.

If eavesdropper Eve intrudes into the MZI system to extract the absolute phase information of the light, such a trial always accompanies measurement and induces a phase shift to the outputs according to coherence/quantum...
optics. Thus, such a measurement-induced phase shift results in the visibility change of the outputs, witnessing Eve’s existence (see Fig. 1b for \( \varphi \not\in \{0, \pi\} \)). Even if Eve’s measurements induce the same phase shift in both paths, she never know whether it is for \( \varphi = 0 \) or \( \varphi = \pi \). This is because there is no way to measure the absolute path lengths from the BS1 to the measurement positions. Compared with nonorthogonal polarization bases in BB84, quantum superposition between two pathways in MZI gives the same mechanism of randomness for eavesdropping. Thus, the quantum superposition of MZI paths results in the closure of the detection loophole in current QKDs.

Figure 1. Detection loophole-free MZI. (a) MZI with a phase shifter \( \Phi(\varphi) \): M, Mirror; BS, beam splitter. \( E_i \) indicates light field in each region \( i \). (b and c) Visibility \( V_{ij} \) (solid curve): \( V_{ij} = \frac{I_j - I_i}{I_j + I_i} \); \( I_i \) is the intensity of \( E_i \). \( I_{N_{ij}} \) is the interference between \( E_i \) and \( E_j \) in the unit of \( I_0 \). The green and red dots refer to the basis \( \varphi = \{0, \pi\} \).

Figure 2 shows a schematic of the present PKD based on PhD-MZI satisfying identity and inversion matrices. The sensitivity of interference and visibility of the output lights \( E_5 \) and \( E_6 \), however, is affected by the bandwidth \( (\delta f) \) of \( E_1 \) in terms of coherence length \( l_c \), where \( l_c = \frac{c}{nf} \) and \( n \) is the refractive index. In practice, the physical path lengths of MZI vary due to environmental noise related to air fluctuations, mechanical/acoustic vibrations, and temperature. Locking such noisy environments, however, is just a technical issue as proved in, e.g., gravitational wave detections. In particular, for a multi-core fiber, the relative path length variation between cores is frozen, resulting in noise-free MZI for the present PKD. The noise-free MZI is an essential condition for PKD implementation.

In Fig. 2, the phase shifter \( \Psi(\Phi) \) is invisible to the outbound (inbound) lights \( E_5 \) and \( E_6 \) (\( E_9 \) and \( E_{10} \)). Bob randomly selects a phase \( \varphi \in [0, \pi] \) for a coherent input light pulse to prepare a key, either for ‘0’ or ‘1,’ and sends it to Alice. According to the MZI theory discussed in equation (2) and in Fig. 1, Alice at the output port of the MZI surely knows about Bob’s choice by her measurement for visibility \( V_A (= V_{5,6}) \) by observing \( A_1 \) and \( A_2 \). For example, if Alice detects only \( A_2 \) click for \( E_5 \) (\( V_{5,6} = -1 \)) as shown in Fig. 1b, she definitely knows that Bob prepared it for the key ‘1’ with \( \varphi = \pi \), unless there is no error: see Table 1a. For the reflected light by the mirror, Alice randomly selects her phase basis \( \psi \in \{0, \pi\} \) to control her phase shifter \( \Psi(\psi) \) and send it back to Bob. The \( \psi \)-set output light \( E_8 \) together with \( E_7 \) is now going back through the same MZI, resulting in the final output lights, \( E_9 \) and \( E_{10} \) at Bob’s side. Here, only the same basis selections \( (\varphi = \psi) \) result in the identity relation and used for key distribution, otherwise discarded (see Tables 1b and 1c). The discarded ones are used for network monitoring of eavesdropping (discussed in Fig. 3).
The matrix \([BH]\) for the outputs \(E_9\) and \(E_{10}\) in the PhD-MZI PKD of Fig. 2 is represented by:

\[
[BH]_{\psi/\varphi} = [MZ]_{\psi}[MZ]_{\varphi} = \frac{1}{2} \begin{bmatrix}
-\left(e^{i\varphi} + e^{i\psi}\right) & e^{i(\psi - \varphi)} \\
-i\left(e^{i\psi} - e^{i\psi}\right) & -\left(e^{i\varphi} + e^{i\psi}\right)
\end{bmatrix}.
\] (4)

where \(\begin{bmatrix} E_9 \\ E_{10} \end{bmatrix} = [BH]_{\psi/\varphi} \begin{bmatrix} E_1 \\ 0 \end{bmatrix}\). From equation (4), the four possible \([BH]\) matrices are obtained:

\[
[BH]_{0/0} = (-1) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad (5-1)
\]

\[
[BH]_{\pi/\pi} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad (5-2)
\]

\[
[BH]_{0/\pi} = -i \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad (5-3)
\]

\[
[BH]_{\pi/0} = i \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad (5-4)
\]

where each of them satisfies either identity \((E_9)\) or inversion \((E_{10})\) relation: see Table 1b. Thus, Bob also surely knows which phase basis is set by Alice by simply observing his detectors \(B_3\) and \(B_4\) for visibility, \(V_{9,10} (=V_B)\).

As shown in Table 1b, the identity matrix of equations (5-1) and (5-2) is achieved if Alice chooses the same basis as Bob does \((\varphi = \psi)\), and it is maximally distinguished from the inversion case of \(\varphi \neq \psi\). Even though the same bases of \(\varphi = \psi\) result in the same value of \(V_B = -1\), Bob surely knows about Alice’s basis selection because he has prepared \(\varphi\); see Table 1c. Table 1c summarizes the key distribution determinacy in the present PKD. Unlike QKDs, the sifting process is not mandatory in PKD, where the randomness is provided by two superposed paths of MZI. In addition to the randomness, path superposition of MZI also offers a great benefit of deterministic
information sharing between two parties without leakage or public announcement. This is the unique property of PKD, where the upper bound of QBR is 100% of the prepared keys if Alice’s basis selection is deterministic (see DISCUSSION).

Table 1. PKD in PhD-MZI. $V_A = V_{5,6}$, $V_B = V_{9,10}$.

| a | Alice | $A_1$ | $A_2$ | Visibility ($V$) | Key (Preparation) |
|---|---|---|---|---|---|
| 0 | On | Off | 1 | 0 |
| $\pi$ | Off | On | $-1$ | 1 |

| b | $\Phi(\psi)$ | $\Psi(\psi)$ | 0 (key=0) | $\pi$ (key=1) |
|---|---|---|---|---|
| 0 (key=0) | $B_3$ ($V_B=-1$) | $B_4$ ($V_B=+1$) |
| $\pi$ (key=1) | $B_3$ ($V_B=-1$) |

Bob's choice ($\phi$) key prepared Alice's choice ($\psi$) $V_A$ $V_B$ key final

| 0 | 0 | 0 | 1 | $-1$ | 0 |
|---|---|---|---|---|---|
| 0 | $\pi$ | 1 | 1 | NA |
| $\pi$ | 1 | 0 | $-1$ | 1 | NA |
| 1 | $\pi$ | $-1$ | $-1$ | 1 |

Photon key distribution and a QBER map

Figure 3 shows numerical calculations for Fig. 2 using equation (4). For the identity matrix of equations (5-1) and (5-2) with $\phi = \psi$, the visibility of $V_{9,10}(V_B) = -1$ is confirmed for key distribution in Figs. 3a and 3b (see the green and red dots). For the inversion matrix in equations (5-3) and (5-4) with $\phi \neq \psi$, the visibility of $V_{9,10} = +1$ is also confirmed for network monitoring (see the open circles).

As discussed in Fig. 1c for eavesdropping randomness in MZI, the same analysis is performed for the return lights, $E_7$ and $E_8$ for indistinguishability of equation (6), where both fields have the same amplitude but different phase determined by $\phi$ and $\psi$:

$$\begin{bmatrix} E_7 \\ E_8 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} -e^{i\phi} & i e^{i\psi} \\ i e^{-i\psi} & -e^{-i\phi} \end{bmatrix} \begin{bmatrix} E_1 \\ 0 \end{bmatrix}. \tag{6}$$

As shown in Figs. 3c and 3d, the path analysis of indistinguishability in equation (6) is numerically proved in both interference (IN$_{7,8}$) and visibility (V$_{7,8}$). Remembering the indistinguishability in the MZI path measurements as discussed in Fig. 1c, Eve’s measurement for the return lights ($E_7$ and $E_8$) reveals the same randomness in both visibility and interference. Eve never know what basis is chosen by Alice as well as Bob in any case even in the case of using the same measurement tool as Alice’s, because the absolute path-length measurement to the tapping position is impossible (see Fig. 2). Thus, there is no way for Eve to extract the phase information in the channels of the PhD-MZI between Bob and Alice. This is the essence of the detection loophole-free PKD, whose key distribution process is entirely automatic owing to the MZI directional determinacy. This automatic key distribution process in PKD allows implementations of the one-time-pad cryptography owing to the ultrahigh speed deterministic photon key distribution in current optical systems of the fiber-optic communications networks.

Except for the keys denoted in green and red dots in Fig. 3a, all other points in the $\phi$ and $\psi$ coordinates imply visibility shifts caused by network errors such as eavesdropping trials (measurement), resulting in a QBER map. In the QBER map, such a measurement-caused visibility shift must be random to the Eve’s eavesdropping trial. Once Eve is successful for a safe tapping in both channels, the potential phase shift is fixed at one point in the QBER map. Assuming no influence on the Bob’s visibility, Eve can measure relative phase difference and trace the change dependent upon Bob’s choice of $\phi$. Even in this case, Eve’s extraction probability is random at 50% at each trial.
because she cannot distinguish between \( \varphi = 0 \) and \( \varphi = \pi \). Here, the random chance of eavesdropping for the perfect overlap with each dot at \( \varphi = \psi = \{0,1\} \) is fairly low. This overlapping probability is determined by the sensitivity of detectors (~\(10^4\) in commercially available avalanche photodiodes), where the visibility at each point is ultrastable regardless of the intensity or phase fluctuations of the light owing to the benefit of MZI.

**Figure 3.** Numerical proofs for PKD in Fig. 2. (a and b) Visibility \( V_{9,10} \) for key distribution between Alice and Bob. The dashed and dotted curves are interference \( I_{9,10} \) for \( \varphi = 0 \) and \( \pi \), respectively. (c and d) Interference \( I_{7,8} \) is for eavesdropping randomness. Green and Red dots indicate random keys set by Alice with \( \psi \in \{0,\pi\} \) for \( \varphi = \psi \). The open circles in (a) and (c) represent for discarded keys by Alice (see also open circles in (b)).

Visibility \( V_{ij} = \frac{I_j - I_i}{I_j + I_i} \); \( I_i \) is the intensity of \( E_i \).

PKD procedure
The key distribution procedure of the present PKD is as follows (see Table 2):
1. Bob randomly selects his phase \( \varphi \in \{0,\pi\} \) to create a \( \varphi \)-controlled coherent light pulse via the phase shifter \( \Phi \) and sends it to Alice. Here, the \( \varphi \)-controlled light can be an N-bit chain.
2. Bob converts his chosen \( \varphi \) into a key in \( \{x\} \) for a record: \( x = 0 \) if \( \varphi = 0 \) and \( x = 1 \) if \( \varphi = \pi \).
3. Alice measures her detectors \( A_1 \) and \( A_2 \) for visibility \( V_A \) to copy Bob’s key \( \{x\} \) in \( \{y\} \) (see Table 1a): \( y = 0 \) if \( V_A = 1 \); \( y = 1 \) if \( V_A = -1 \); \( y = V_A \) if \( V_A \neq \pm 1 \); \( \{y\} = \{x\} \), except for \( V_A \neq \pm 1 \). Here, \( V_A \neq \pm 1 \) stands for an error due to eavesdropping or network problem: see the red number in Table 2.
4. Alice randomly selects her phase \( \psi \in \{0,\pi\} \) to create a \( \psi \)-controlled light pulse via the phase shifter \( \Psi \) and sends it back to Bob. Here, the \( \psi \)-phase control is performed on the reflected \( \varphi \)-controlled light pulse(s).
5. Alice converts her chosen \( \psi \) into a key in \( \{z\} \) for a record: \( z = 0 \) if \( \psi = 0 \) and \( z = 1 \) if \( \psi = \pi \).
6. Alice herself sifts her prepared key in \( \{z\} \) into \( \{a\} \): \( a = y \) if \( y - z = 0 \); \( a = D \) if \( y - z \neq 0 \). Here, \( D \) stands for discarded.
7. Bob measures his detectors \( B_3 \) and \( B_4 \) for visibility \( V_B \): \( w = x \) if \( V_B = -1 \); \( w = D \) if \( V_B = 1 \); \( w = V_B \) if \( V_B \neq \pm 1 \). This step results in the copy of \( \{a\} \) into \( \{w\} \) (see Table 1c). Here, \( V_B \neq \pm 1 \) stands for an error due to eavesdropping or network problem.
8. Bob sifts the copied key in \( \{w\} \) into \( \{b\} \): \( b = w \) if \( w - x = 0 \); \( b = D \) if \( w - x \neq 0 \); \( \{w\} = \{a\} \), except for \( V_B \neq \pm 1 \).
9. Alice and Bob announce their error bits only for $V_A \neq \pm 1$ or $V_B \neq \pm 1$, and discard the corresponding bits in their keys $\{a\}$ and $\{b\}$, respectively. Alice and Bob now share the same key $\{m\}$. They never announce their selected bases or visibilities.

According to the detection loophole-free PKD analyzed in Figs. 1–3, however, Alice does not need to randomly select her phase basis $\psi$. In this case, the column numbers 1, 3, 5, 6, and 8 are effective, where 6 and 8 are due to network errors or eavesdropping trials.

Table 2. Sequence for PKD in Fig. 2.

| Party | Order | Sequence | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | set |
|-------|-------|----------|---|---|---|---|---|---|---|---|---|----|-----|
| Alice | 3     | $V_A$    | 1 | -1| -1| 1 | -1| 1 | 1 | -0.5* | 1 | -1 |     |
|       |       | Copy x: y| 0 | 1 | 1 | 0 | 1 | 0 | 0 | -0.5 | 0 | 1   |  \{y\} |
|       | 4     | $\psi$  | 0 | 0 | $\pi$| $\pi$| $\pi$| 0 | $\pi$| $\pi$| $\pi$| 0    |
|       | 5     | z(\psi) | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0   |  \{z\} |
|       | 6     | Sifting y: a | 0 | D | 1 | D | 1 | 0 | D | D | D | D  |  \{a\} |
|       | 9     | Final key | 0 | D | 1 | D | 1 | D** | D | D | D | D  |  \{m\} |
| Bob   | 1     | $\varphi$ | 0 | $\pi$| $\pi$| 0 | $\pi$| 0 | $\pi$| 0 | $\pi$|     |
|       | 2     | Prepared key: $x(\varphi)$ | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1   |  \{x\} |
|       | 7     | $V_B$    | -1| 1 | -1| 1 | -1| -0.8* | 1 | -1 | 1 | 1    |
|       |       | Copy A: w | 0 | D | 1 | D | 1 | -0.8 | D | 1 | D | D   |  \{w\} |
|       | 8     | Sifting w: b | 0 | D | 1 | D | 1 | D | D | 1 | D | D  |  \{b\} |
|       | 9     | Final key | 0 | D | 1 | D | 1 | D | D | D** | D | D  |  \{m\} |

The numbers in red refer to network errors or eavesdropping.

**Only error bits are announced publically to discard the corresponding bit from the final key set \{m\}. Here, D represents an error bit and can be set to any number, e.g., D=9 for a computing algorithm.

$V_A = V_{5,6}$; $V_B = V_{9,10}$.

DISCUSSION

Deterministic key distribution in PKD

The deterministic key distribution is possible due to detection loophole-free PKD in the MZI path superposition of Fig. 2. As will be discussed below in the Initialization procedure for PKD, Eve cannot extract the Bob’s chosen phase. Compared with BB84 based on post-measurement sifting process with the random basis selection, the randomness in PKD comes from the path superposition of MZI, so that deterministic basis selection is possible. In this case, the upper bound of QBR in PKD is 100%. As shown in Fig. 2, the deterministic basis selection is technically obtained by the A3/A4 detector-triggered control for the phase shifter $\Psi$. The reason of random basis selection by Alice in Table 2 is not necessary.

Multicore fiber-optic networks

In the fiber-optic communications networks, the PhD-MZI configuration of Fig. 2 is satisfied by a multicore fiber (see Fig. 4). Although the intrinsic characteristics induced by material itself are slightly different among cores in a multicore fiber, the relative refractive index change by nosey environments is nearly zero due to the micron scale proximity between cores enclosed by a cladding. Thus, the MZI configuration of a multicore fiber should be robust to the environmental noise for the present PhD-MZI system. For the applications of PKD, current ~100 km spaced
EDFA fiber optic networks are perfectly fit, where the MZI length becomes unlimited due to the coherence nature of light via coherent amplifications at EDFA and modulations. This unlimited transmission distance is the 2nd novelty of the present PKD, where photon cloning by EDFA is basically phase-locked process, resulting in a fixed phase shift. The fixed phase shift in the cloning process can be technically adjusted for visibility of outputs.

![Figure 4. A schematic of optical fiber-based PKD. L, Laser; OM, optical modulator; OD, optical delay; A1, detector at Alice side; B1, detectors at Bob’s side; M, mirror; Φ, phase controller at Bob’s side; Ψ, phase controller at Alice’s side. Ei, coherent light pulse. C, 50/50 fiber coupler.]

Initialization procedure for PKD

Regarding the phase-dependent visibility $V_A$ in Figs. 1b and 3b, Alice does not know what phase basis is set by Bob unless the network (MZI) configuration is known. To solve this problem, Alice may scan her phase shifter $Ψ(δ)$ and fix it with a correct $δ$ for a maximum visibility $V_A$. The value of $V_A$, however, is random until Alice knows Bob’s choice of $φ$. This situation applies to Eve exactly in the same way. To solve this dilemma, i.e., to let Alice know secretly the $φ$ value set by Bob, the following initialization stage is needed before starting the PKD procedure.

**Table 3. Initialization for PKD.**

| Party | Order (N) | Sequence | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|-------|-----------|----------|---|---|---|---|---|---|---|---|---|----|
| Alice | 1         | $Ψ$      | $δ$ | $δ$ | $δ+π$ | $δ$ | $δ+π$ | $δ$ | $δ+π$ | $δ$ | $δ+π$ |    |
|       | 3         | $V_A$    | 1  | $−1$ | 1  | 1  | 1  | 1  | $−1$ | $−1$ | $−1$ |    |
| Bob   | 2         | $φ$      | 0  | $π$ | $π$ | 0  | $π$ | 0  | $π$ | 0  |     |    |
|       | 4         | Correctness | √ | √ | √ | √ | √ | √ |     |     |     |    |

$V_A = V_{5,6}$.

The preparation stage for PKD in Table 3:
1. Alice randomly selects additional phase $α ∈ \{0, π\}$ to add the fixed $δ$ for $Ψ$.
2. Bob randomly selects $φ ∈ \{0, π\}$, and sends the $φ$-encoded light to Alice.
3. Alice measures $V_A$ and publically announces the results.
4. Bob publically announces the correctness with respect to the Alice’s results.

Table 3 shows the initialization procedure how the $φ$-dependent directionality in Fig. 1 is effective. First, Alice randomly sets her phase controller $Ψ$ with either the $δ$ obtained in the scanning stage or $δ+π$. Second, Bob randomly selects $φ ∈ \{0, π\}$ for the light pulse $E_4$ and sends it to Alice along with $E_3$. Third, Alice publically announces her measurement results of $V_A$. She never announces her phase choices for $Ψ$. Lastly, Bob publically
announces the correct ones with respect to Alice’s $V_A$ results. Then Alice knows secretly whether the $\delta$ is correct or $\pi$–phase shifted: Table 3 is for the correct $\delta$. Here, Eve can know the tendency of the $\varphi$–dependent $V_A$ even without the correct $\delta$ by doing the same measurement as Alice does and by tracing the public announcements, if there is no random selection in the phase choice by Bob and Alice. To surprise, the unconditional security in PKD is done by classical (coherent) light pulses.

In conclusion, a novel coherence optics-based PKD protocol is proposed, analyzed, and discussed to overcome the low QBR, rate-distance dependency, transmission limitations, and conditional security in conventional QKD protocols limited by detection loophole as well as by the inconvenience of nonclassical lights. The physics of the proposed PKD is in the quantum superposition of paired channels in MZI, where no-cloning theorem and randomness in current QKD are replaced by the path superposition of coherent lights. The unconditional security in the proposed PKD is rooted in the coherence nature of the MZI system, where the detection loophole is closed perfectly regardless of detector efficiency. Eventually, all-optical computers can be directly combined with the present PhD-MZI system for all-in-one secured information processing and communications. The present PhD-MZI scheme is also applicable for wireless or satellite PKD via MIMO technologies with coherent light (discussed elsewhere).

METHODS

The numerical calculations in Figs. 1 and 3 were performed by Matlab using equations appeared in the text. The data that support the findings of this study are available from the corresponding author upon reasonable request.

ACKNOWLEDGEMENTS

The author acknowledges that the present work was supported by the ICT R&D program of MSIT/ITP (1711042435: Reliable crypto-system standards and core technology development for secure quantum key distribution network).

CONTRIBUTION

B.S.H. solely wrote the manuscript text and prepared all figures.

COMPETING INTERESTS

The author declares no conflict of interest.

REFERENCES

1. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. Nature 299, 802 (1982).
2. Gisin, N., Ribordy, G., Tittle, W. & Zbinden, H. Quantum key distribution. Rev. Mod. Phys. 74, 145 (2002).
3. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. Quantum Info. 2, 1 (2016).
4. Lydersen L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. & Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photon. 4, 686 (2010).
5. Huang, A., Sun, S.-H., Liu, Z. & Makarov, V. Quantum key distribution with distinguishable decoy states. Phys. Rev. A 98, 012330 (2018).
6. Gerhardt, I. et al. Experimental faking the violation of Bell’s inequalities. Phys. Rev. Lett. 107, 170404 (2011).
7. Sajee, S, Huang, A., Suon, S. Xu, F., Makarov, V. & Curty, M. Insecurity of detector-device-independent quantum key distribution. Phys. Rev. Lett. 117, 250505 (2016).
8. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400 (2018).
9. Qin, H., Kumar, R., Makarov, V. & Alleaume, R. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Phys. Rev. A* **98**, 012312 (2018).
10. Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nature Photon.* **7**, 210 (2013).
11. Zhu, C., Xu, F. & Pei, C. W-state analyzer and multi-party measurement-device-independent quantum key distribution. *Sci. Rep.* **5**, 17449 (2015).
12. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8. New York, 1984
13. Ekert, A. Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
14. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121 (1992).
15. Sasaki, M. *et al.*, Field test of quantum key distribution in the Tokyo QKD network. *Opt. Exp.* **19**, 10387 (2011).
16. Sibson, P. *et al.* Chip-based quantum key distribution. *Nature Communi.* **10**, 1038 (2016).
17. Christensen, B. G. *et al.* Detection-loophole-free test of quantum nonlocality and applications. *Phys. Rev. Lett.* **111**, 130406 (2013).
18. Matsuoka, S. Ultrahigh-speed ultrahigh-capacity transport network technology for cost-effective core and metro networks. *NTT Tech. Rev.* **9** (No. 8) 1 (2011).
19. Essiambre, R.-J. & Tkach, R. W. Capacity trends and limit of optical communication networks. *Proceeding of IEEE* **5**, 1035 (2012).
20. SK Telecommunications, S. Korea. Private conversation.
21. Saitoh, K. Multicore fiber technology. *J. Lightwave Tech.* **34**, 55 (2016).
22. Honjo, T., Inoue, K. & Takahashi, H. Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer. *Opt. Lett.* **29**, 2797 (2004).
23. Cerf, N. J., Adami, C. & Kwiat, P. G. Optical simulation of quantum logic. *Phys. Rev. A* **57**, R1477 (1998).
24. Degiorgio, V. Phase shift between the transmitted and the reflected optical fields of a semireflecting lossless mirror is $\pi/2$. *Am. J. Phys.* **48**, 81 (1980).
25. Zeilinger, A. General properties of lossless beam splitters in interferometry. *Am. J. Phys.* **49**, 882 (1981).
26. Mandel, L. Photon interference and correlation effects produced by independent quantum sources. *Phys. Rev. A* **28**, 929 (1983).
27. Hong, C. K., Ou, Z. Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044 (1987).
28. Haider, G. B. & von der Weid, J. P. Stable single-photon interference in a 1 km fiber-optic Mach-Zehnder interferometer with continuous space adjustment. *Opt. Lett.* **36**, 1764 (2011).
29. Carolan, J. *et al.* Universal linear optics. *Science* **349**, 711 (2015).
30. Capbell, G. T., Pinel, O., Hosseini, M., Ralph, T. C., Buchler, B. C. & Lam, P. K. Configurable unitary transformations and linear logic gates using quantum memories. *Phys. Rev. Lett.* **113**, 063601 (2014).
31. Ham, B. S. Wavelength convertible quantum memory: controlled echo. *Sci. Rep.* **8**, 10675 (2018).
32. Kikforman, J.-P., Joffre, M., & Thierry-Mieg, V. Measurement of photon echoes by use of femtosecond Fourier-transform spectral interferometry. *Opt. Lett.* **22**, 1104 (1997).
33. Ham, B. S., Shahriari, M. S., Kim, M. K. & Hamer, P. R. Spin coherence excitation and rephrasing with optically shelved atoms. *Phys. Rev. B* **58**, R11825 (1998).
34. Abbott, B. P. *et al.* Observation of gravitational waves from binary black hole merger *Phys. Rev. Lett.* **116**, 061102 (2016).
35. Ham, B. S. Observations of ultraslow light-based photon logic gates: NAND/OR. *Appl. Phys. Lett.* **94**, 101110 (2009).
36. Nauerth, S., Moll, F., Rau, M., Fuchs, C., Horwath, J., Frick, S. & Weinfurter, H. Air-to-ground quantum communication. *Nature Photon.* **7**, 382 (2013).
37. Liao, S.-K. *et al.* Satellite-to-ground quantum key distribution. *Nature* **549**, 43 (2017).
38. Larsson, E. G., Edfors, O., Tufvesson, F. & Marzetta, T. L. Massive MIMO for next generation wireless systems. *IEEE Communi. Mag.* **186** (Feb. 2014).