SCIENTIFIC REPORTS
nature research

Check for updates

OPEN

Unconditionally secured classical cryptography using quantum superposition and unitary transformation

Byoung S. Ham

Over decades quantum cryptography has been intensively studied for unconditionally secured key distribution in a quantum regime. Due to the quantum loopholes caused by imperfect single photon detectors and/or lossy quantum channels, however, the quantum cryptography is practically inefficient and even vulnerable to eavesdropping. Here, a method of unconditionally secured key distribution potentially compatible with current fiber-optic communications networks is proposed in a classical regime for high-speed optical backbone networks. The unconditional security is due to the quantum superposition-caused measurement indistinguishability between paired transmission channels and its unitary transformation resulting in deterministic randomness corresponding to the no-cloning theorem in a quantum key distribution protocol.

In (classical) cryptographic technologies, there are two major versions: One is symmetric key-based private cryptography, and another is asymmetric key-based public one[1]. The public cryptography is called RSA and has become prevalent now, where its security relies on non-polynomial computational complexity of prime number factorization. Thus, the classical cryptography has been focused on the developments of efficient encrypting algorithms requiring more computing recourses in crypto-analysis. This is why the RSA key size has been continuously increased over decades, and now it is as long as 2048 bits[1]. As Internet traffic rapidly increases recently, information security has gained much more attention to protect the data from potential eavesdropping. Although the security of classical (public) cryptography looks good to some extent, it is basically conditional (or breakable) and even vulnerable to a quantum computer[2].

Quantum key distribution (QKD) belongs to the symmetric key-based private cryptography, and its security relies on how to distribute the keys rather than how to generate them. QKD has gained its importance due to theoretically confirmed unconditional security by Heisenberg's uncertainty principle in quantum mechanics[3]. Specifically the unconditional security of QKD is based on no-cloning theorem[4], resulting from quantum superposition between paired conjugate (non-orthogonal) variables used for bases of a quantum key[5]. The unconditional security of QKD, however, is not guaranteed in practice due to the quantum loopholes based on imperfectness of a single photon detector[6–12] and/or a quantum channel[12]. The detection loophole with the channel loss affects all QKD protocols based on single photons[5–7], entangled photon pairs[8–11], and coherent continuous variables[12]. As a result, QKD is practically fragile to eavesdropping unless the quantum loophole is completely closed[13]. Thus, the unconditional security of QKD has become a practical matter, resulting in the unrealistically low key rate. 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 kilo–Mega-bits per second (bps) depending on the single/entangled photon generation rate[10]. Besides, technical difficulties in single-photon or entangled photon-pair generations make current QKD highly impractical. Most of all, current QKD is not compatible with conventional (classical) networks mainly due to nonlinear effects violating the no-cloning theorem. As a result, the transmission distance in QKD through an optical fiber is severely limited unless quantum repeaters are implemented[14].

Historically one-time-pad (OTP) has been proposed for an ideal communication system satisfying unconditional security, where the key is equivalent or longer than the data in length and must be used only one time[15]. Any existing cryptographic technologies, thus, do not support OTP simply due to either the low key rate or

Center for Photon Information Processing, School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea. email: bham@gist.ac.kr

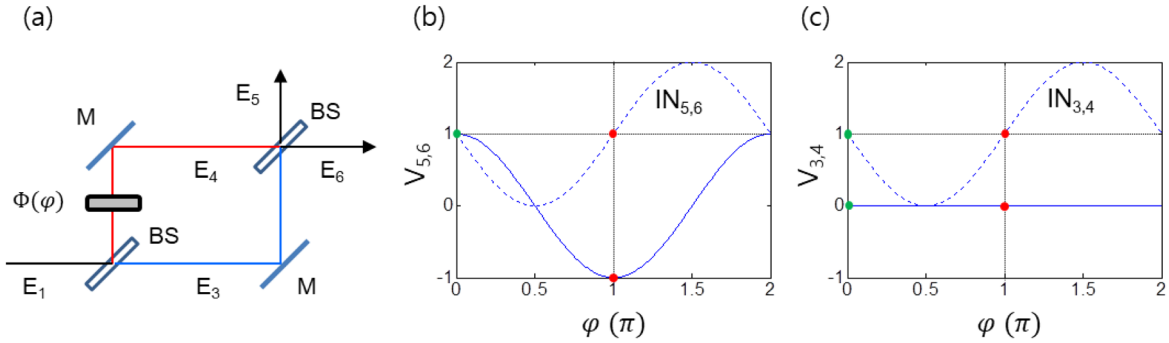

Figure 1. Deterministic randomness in MZI. (**a**) MZI with a phase shifter $\Phi(\varphi)$: M, Mirror; BS, beam splitter. E_i indicates light field in each region *i*. (**b**, **c**) Visibility $V_{i,j}$ (solid curve): $V_{i,j} = \frac{I_j - I_i}{I_j + I_i}$. E_i, coherent light pulse; I_i is the intensity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

conditional security, while the classical data traffic rate in current fiber-optic communications backbone networks is more than 10 Gbps per channel, and its transmission distance is unlimited. Here, a completely different concept of unconditionally secured cryptography is proposed in a classical regime to overcome the limitations in both classical and quantum cryptographies and to support OTP. The proposed cryptography is safe from all kind attacks and quantum computers because its security is based on perfect randomness and measurement immunity.

Unlike QKD, the unconditional security in the proposed cryptography is provided by quantum-superposed transmission channels such as in a typical Young's double-slit experiment. As is well known, the Young's double-slit experiment is satisfied by both coherence (wave nature)[16,17] and incoherence (particle nature) optics[18]. Moreover, the double slit can be replaced by a beam splitter (BS) in a Mach–Zehnder interferometer (MZI). In this paper, we focus on the classical nature of light (coherence optics) rather than the quantum nature to satisfy its classicality in both fundamental physics and potential applications. Compared with non-orthogonal basis set of a single photon in QKD, the orthogonal basis set of bright coherent light in the proposed cryptography has technical advantages to fit coming information era in terms of speed and compatibility. The key concept of the Young's double-slit experiments is in the measurement indistinguishability satisfied by both coherence (classical) and incoherence (quantum) physics. In other words, the state of a light such as a phase and a polarization cannot be measured definitely in MZI channels due to quantum superposition, resulting in prefect randomness in a binary system. According to the Shannon's information theory, the prefect randomness is equivalent to no eavesdropping or unconditional security[19]. To prove the unconditional security of the proposed cryptography, we present, analyze and discuss the fundamental physics of how to generate and distribute a perfect randomness-based key in a measurement-immune condition. Reminding of that QKD is the only method satisfying the unconditional security in key distribution using quantum mechanics, it is counterintuitive to perform the same function in a classical manner. This is the quintessence of the present paper.

As a physical infrastructure of the proposed unconditionally secured classical cryptography, an MZI scheme is used for the real transmission lines to realize both randomness-based key generation and unconditionally safe distribution via quantum superposition and unitary transformation (discussed in Figs. 1, 2 and 3). It should be noted that MZI itself has already been used for some QKD protocols for encoding (for a sender) and decoding (for a receiver) through single transmission line[20–22], but it has nothing to do with the proposed one relied on double transmission lines with classical light. In the case of single-core fibers comprising the MZI scheme, the phase stability between them has already been proved for a km distance range by using a common locking technique[23]. Locking delicate noisy environments caused by temperatures, vibrations, and air fluctuations has also been proved in a free space for a 4-km distance range[24]. Technically the MZI stability issue is now closed and can be applied for a much longer traveling distance.

In the middle of 1990s, a MZI-channel-based QKD protocol was introduced for orthogonal bases, where the security relies on MZI physics of path superposition[25]. The eavesdropping randomness of the orthogonal bases could be obtained by random timing of key generation. For such unknown information distribution between remote parties QKD is necessary, in which another quantum channel is required to support the orthogonal MZI protocol. The basic physics of MZI channels for QKD with orthogonal bases were analytically discussed using a simple projection-based measurement for a quantum state. In that sense, the MZI physics of randomness is clarified for the secured key distribution. However, unconditional security cannot be fulfilled in such a one-way process in a single MZI scheme, unless the unknown timing information distribution is solved. Here, we present a complete protocol for orthogonal basis in a double MZI scheme, whose secured key distribution is achieved by time-reversal process of unitary transformation without an additional quantum channel relied on QKD itself.

To understand the fundamental physics of the proposed cryptography, firstly, we present eavesdropping randomness and transmission directionality in an ideal MZI scheme. Then, round-trip MZI physics is analyzed for unitary transformation for eigenvalue controllability. The unitary transformation in the proposed protocol is fulfilled with non-canonical (orthogonal) phase bases to satisfy a classical regime. The round-trip MZI-physics is then discussed for deterministic randomness, in which the key generation is random to eavesdroppers but deterministic to both sender and receiver. The deterministic randomness equivalent to the no-cloning theorem in QKD in a technical point of view is achieved classically via random shuffling of the eigenvalues in the MZI

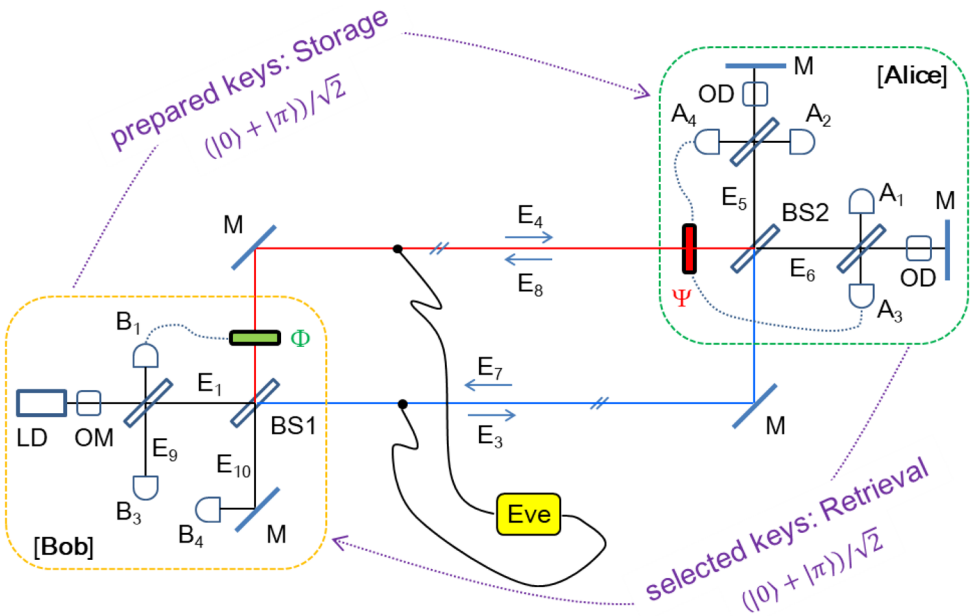

Figure 2. A schematic of PCD-MZI for OKD. LD, Laser; OM, optical modulator; A_i, detector at Alice side; B_i, detectors at Bob's side; BS, 50/50 unpolarized beam splitter; M, mirror; Φ, Bob's phase controller; Ψ, Alice's phase controller; OD, optical delay; Eve, eavesdropper.

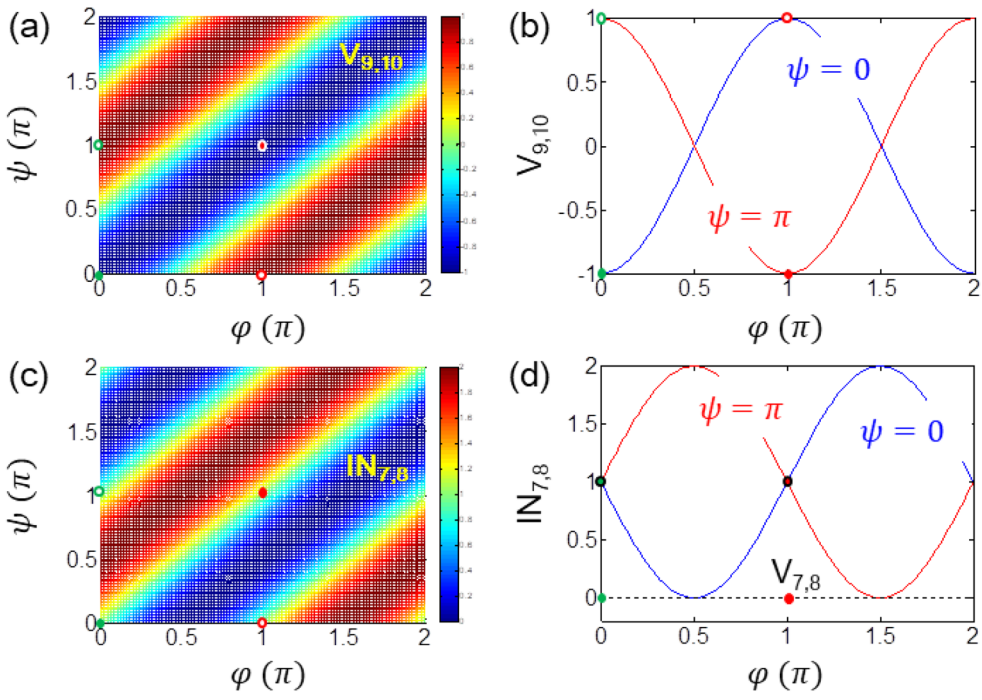

Figure 3. Numerical proofs for OKD in Fig. 2. (**a**, **b**) Visibility $V_{9,10}$ for key distribution between Alice and Bob. The dashed and dotted curves are interference $I_{9,10}$ for , respectively. (**c**, **d**) The same value of interference $IN_{7,8}$ shows eavesdropping randomness. Green and Red dots indicate random keys set by Alice with for . The open circles in (**a**) and (**c**) represent for discarded keys by Alice [see also open circles in (**b**)]. Visibility : I_i is the intensity of E_i.

unitary transformation. Finally, the classically unconditional key distribution protocol is presented and discussed for potential attacks and future fiber-optic applications. This classically achieved unconditional security with perfect randomness in eavesdropping surpasses QKD and RSA and has never been discussed before.

Results

The phase shifter Φ in an MZI scheme of Fig. 1a is for a random basis selection between two orthogonal phase bases 0 and π. For the MZI unitary transformation, universal quantum gate operations have already been presented in a phase shifter-coupled MZI in a quantum regime[26]. Compared with nonorthogonal bases in QKD resulting in randomness according to the Heisenberg's uncertainty principle, the orthogonal bases in the proposed classical cryptography play the same role of the randomness in a classical regime (discussed in Figs. 2 and 3). For coherence optics with bright light fields, the split lights E_3 and E_4 on the first BS are perfectly coherent regardless of the bandwidth, intensity fluctuation, and phase noise of E_1. For incoherence optics with single photons, intensity correlation (or 4th order interference) has been proved for photon anti-bunching of the particle nature in a quantum regime[27]. These two different roles of BS have been intensively discussed for complementarity in quantum mechanics, where both phenomena cannot be dealt with simultaneously. The present protocol is for coherence optics but not excludes the particle nature of incoherence optics, either.

The BS matrix, [BS], was firstly discussed in 1979 by Degiorgio[16] and generalized in 1980 by Zeilinger[17], where there exists a π/2 phase shift between the split lights, the transmitted (E_3) and the reflected (E_4) for $\varphi = 0$ (see Fig. 1):

$$[BS] = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \tag{1}$$

where, $E_3 = \frac{E_1}{\sqrt{2}}$ and $E_4 = \frac{iE_1}{\sqrt{2}}$. There is no way to measure the absolute phase of traveling lights in the MZI channels unless E_1 is known. In other words, the measurement randomness in MZI channels is self-sustained by physics[25]. Here, any measurement in the MZI channels also violates the indistinguishability in quantum superposition regardless of coherence or incoherence optics. This means that the channel measurement itself causes a fringe shift in the output interference pattern between E_5 and E_6. The relative phase measurement without fringe shift may be technically possible in an ideal system[28], but useless in crypto-analysis without knowing the input light (E_1) due to 50% chance in success (randomness). This randomness in eavesdropping represents no information withdrawal[19]. The path superposition of MZI channels, thus, becomes the origin of the unconditional security of the proposed protocol for a classical regime.

In a typical MZI scheme of Fig. 1a, each mirror generates the same phase shift in each path, resulting in perfect phase cancellation. The original light pulse E_1 generated by a commercial laser system hits on the first BS and split into two, E_3 and E_4. The split lights E_3 and E_4 are perfectly coherent each other in principle. This robust coherence of MZI even works for a single photon whose phase is random as an upper bound[23,28]. The random φ -phase control for E_3 is provided by Bob using his phase shifter Φ, where the phase basis is binary and orthogonal: $\varphi = \{0, \pi\}$. In Fig. 1a, the MZI matrix representation with a phase shifter Φ is denoted by:

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

where $[\Phi] = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$ and $[MZ]_\varphi = [\mathrm{BS}][\Phi][\mathrm{BS}]$. For $\varphi = 0$, the output lights at the second BS become unidirectional into E_6: $E_6 = iE_1$; $E_5 = 0$. The phase factor "i" in E_6 indicates a phase gain via MZI with respect to the input light E_1. For $\varphi = \pi$, the output light direction is switched into E_5 according to Eq. (2): $E_5 = E_1$; $E_6 = 0$. As shown in Fig. 1b (see the green and red dots in the solid curve), the output directionality in MZI is predetermined depending on the phase basis.

Allowing Eve to copy the traveling lights through MZI channels without altering the output interference fringe, the eavesdropping analysis in both visibility and interference between E_3 and E_4 proves the basic physics of measurement randomness: see Fig. 1c. The orthogonal φ-values used for distinct visibility in Fig. 1b, however, represent complete indistinguishability in the eavesdropping measurement. This φ-independent visibility in Fig. 1c is somewhat obvious owing to phase independency in measurements: $|E_3|^2 = |E_4|^2$. The measurement randomness is due to the fundamental physics of quantum superposition between two paths (phases) of MZI and corresponds to the no-cloning theorem in QKD. Even if Eve is highly sophisticated in eavesdropping with the same measurement tool of MZI as Alice's, Eve's success rate is 50% in average, resulting in perfect randomness like ideal coin tossing. This is because the path length-caused phase change cannot be controlled for two independent MZI systems (Bob-Alice and Bob-Eve; see Fig. 2) simultaneously: Further discussions are given in Discussion section.

Figure 2 shows a schematic of the proposed protocol based on a round-trip MZI scheme, where the result of $[MZ]_\varphi^2$ is the identity matrix for $\varphi = \psi$ (see Section S1 of the Supplementary Information):

$$[MZ]_\varphi^2 = \left(-e^{i\varphi}\right)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{3}$$

From Eq. (3), it is clear that a typical MZI system satisfies unitary transformation regardless of φ if $\varphi = \psi$. The physical meaning of the identity matrix in Eq. (3) for the double-MZI scheme implies a time-reversible process as in an optical quantum memory, where the quantum memory has been discussed for both quantum

(a)

Alice / $\Phi(\varphi)$	A_1	A_2	Visibility (V_A)	Key (Preparation)
0	On	Off	1	0
π	Off	On	−1	1

(b)

$\Phi(\varphi)$ / $\Psi(\psi)$	0 (key=0)	π (key=1)
0 (key=0)	B_3 (V_B=−1)	B_4 (V_B=+1)
π (key=1)	B_4 (V_B=+1)	B_3 (V_B=−1)

(c)

Bob's choice (φ)	key prepared	Alice's choice (ψ)	V_A	V_B	key final
0	0	0	1	−1	0
	0	π	1	1	NA
π	1	0	−1	1	NA
	1	π	−1	−1	1

Table 1. Visibility measurement-based key distribution in PCD-MZI. (a) Alice's visibility V_A, (b) Bob's visibility V_B, (c) key sharing via deterministic randomness: $V_A = V_{5,6}$; $V_B = V_{9,10}$; $V_{ij} = \frac{I_j - I_i}{I_j + I_i}$.

optics[29,30] and classical optics[31,32]. Here, the global phase in Eq. (3) has nothing to do with a measurement value or unitary transformation.

In the round-trip MZI configuration of Fig. 2, the phase shifter $\Psi(\Phi)$ is supposed to be invisible to the outbound (inbound) lights E_5 and E_6 (E_9 and E_{10}). For the key distribution, firstly, Bob prepares a key for Alice via random choosing of the phase basis $\varphi \in \{0, \pi\}$ and sends it to Alice via MZI channels. According to the MZI theory discussed in Eq. (2) and Fig. 1, Alice at the output port surely knows what Bob's random choice was by measuring her visibility V_A (= $V_{5,6}$): MZI directional determinacy. For example, if Alice detects A_2 click for E_5 ($V_{5,6} = -1$) as shown in Fig. 1b (see the red dot), she definitely knows what Bob prepared is $\varphi = \pi$ representing the key '1', unless network error occurs: see Table 1a in details.

For the reflected light of E_5 and E_6, Alice randomly selects her phase basis $\psi \in \{0, \pi\}$ for her phase shifter Ψ and sends it back to Bob via the same MZI channels. The ψ-set inbound light E_8 together with E_7 is now going back to Bob, resulting in the final output lights, E_9 and E_{10} at Bob's side. The matrix [BH] for the return light of E_9 and E_{10} in Fig. 2 is represented by:

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

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

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

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

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

$$[BH]_{\pi/0} = i\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{5-4}$$

Each of them satisfies either identity (E_9) or inversion (E_{10}) relation: see Table 1b in details. Thus, Bob also surely knows which phase basis was set by Alice by observing his detectors B_3 and B_4 for visibility $V_{9,10}$ (= V_B). Then, the key is set deterministically if and only if the identity matrix is satisfied ($\varphi = \psi$), otherwise discarded: see Table 1c in details. Unlike mandatory sifting in QKD, Bob and Alice do not need to communicate each other with their measurement results. Although the key setting is inner shared with 100% sureness in the double MZI system, it is perfectly random to an eavesdropper Eve due to the measurement randomness as discussed in Fig. 1: deterministic randomness. Here, the deterministic randomness of the double-MZI presented in Figs. 1 and 2 as well as Table 1 is of course good enough for QKD but not sufficient for classical cryptography due to the *memory-based attack* (see Discussion section). To protect it from this classical attack an additional action such as QKD-like sifting or *network initialization* must be given (discussed later). The deterministic randomness in Fig. 2 offers a significant feature of unconditional security to a classical regime. The discarded keys ($\varphi \neq \psi$) are of course used for network monitoring of eavesdropping (discussed in Fig. 3).

Party	Sequence		Order										
			1	2	3	4	5	6	7	8	9	10	Set
Alice	3	V_A	1	−1	−1	1	−1	1	1	−0.5[a]	1	−1	
		Copy x: y	0	1	1	0	1	0	0	−0.5	0	1	$\{y\}$
	4	ψ	0	0	π	0	π	0	π	π	π	π	
	5	z (ψ)	0	0	1	0	1	0	1	1	1	1	{z}
	6	Sifting y: a	0	D[b]	1	0	1	0	D[b]	D	D[b]	1	$\{a\}$
	9	Final key	**0**	**D**	**1**	**0**	**1**	**D**	**D**	**D**	**D**	**1**	$\{m\}$
Bob	1	φ	0	π	π	0	π	0	0	π	0	π	
	2	Prepared key: x (φ)	0	1	1	0	1	0	0	1	0	1	{x}
	7	V_B	−1	1	−1	−1	−1	−0.8[a]	1	−1	1	−1	
		Copy a: w	0	D	1	0	1	−0.8	D	1	D	1	{w}
	8	Sifting w: b	0	D[b]	1	0	1	D	D[b]	1	D[b]	1	{b}
	9	Final key	**0**	**D**	**1**	**0**	**1**	**D**	**D**	**D**	**D**	**1**	{m}

Table 2. A key distribution procedure for Fig. 2. The discarded bit D can be represented by any big number, e.g., D = 9 for a computing algorithm: $V_A = V_{5,6}$; $V_B = V_{9,10}$; $V_{ij} = \frac{I_j - I_i}{I_j + I_i}$. [a]The numbers in red refer to network errors by disturbance or eavesdropping. [b]By the sifting process the discarded bit D is shared between Alice and Bob automatically even without public announcement owing to the MZI determinacy. Only error bits denoted by red numbers are announced publically to discard the corresponding bit from the final key set $\{m\}$: see the red D.

As shown in Table 1b, the identity matrix of Eqs. (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 identical basis ($\varphi = \psi$) results in the same value of $V_B = -1$ (see the diagonal values), Bob surely knows Alice's choice because he has prepared the key with φ: see also Table 1c. Table 1c summarizes the key distribution determinacy in the proposed cryptography.

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

As analyzed in Fig. 1c for eavesdropping randomness in MZI, the same analysis is performed for the return lights, E_7 and E_8 for indistinguishability, where the lights in both MZI paths have the same amplitude but different phase determined by φ and ψ:

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

As shown in Fig. 3c, d, the matrix analysis of Eq. (6) for indistinguishability is numerically proved in both interference ($IN_{7,8}$) and visibility ($V_{7,8}$) (see the same value for different bases). Recalling the indistinguishability in the MZI path measurements in Fig. 1c, Eve's measurement for the return lights (E_7 and E_8) reveals the same randomness: Eve never knows what basis is chosen by Alice as well as Bob due to the random basis selections as well as measurement indistinguishability in the superposed paths of MZI. This is the essence of the proposed cryptography using quantum superposition of MZI paths. The deterministic random key distribution process analyzed in Figs. 2 and 3 shows potential OTP applications owing to the compatibility with classical physics including duplication and amplification (see Discussion section).

Except for the keys marked by green and red dots in Fig. 3a along the off-diagonal direction, all others are considered as network errors caused by such as environmental noises and eavesdropping trials. Thus, Fig. 3a can be used as a bit error rate (BER) map. If Eve is successful for a safe measurement in both channels of MZI without the fringe shift, she can brutely scan her interferometer until a distinctive fringe patterns are observed. This brute force trial appears as a single curve in the BER map such as in Fig. 3b. Even in this case, the probability of exact matching with the original one of Fig. 3b is 50% in average because there is no way to know exact MZI configuration due to independency of both systems. Thus, Eve's eavesdropping chance is random as in coin tossing. Here it should be noted that the random eavesdropping chance by Eve is, however, consistent to all copied bits, resulting in a room for a *memory-based attack* in classical crypto-analysis: see the *memory-based attack* in Discussion section. By the way, the phase selection by both parties may be performed using a random number generator[33].

Key distribution procedure. The order (1–10) in Table 2 can be performed either individually or in a packet. The sifting process is necessary to avoid the *memory-based attack* (see Discussion section). Assuming no network error or perfect tapping by Eve without affecting fringe shift, each bit rate in the key distribution procedure is as high as 50% with respect to Bob's key provision rate, which is more than Gbps according to current optoelectronic device in fiber optic communications. As mentioned above, the outbound (inbound) light

is invisible to the phase shifter Ψ (Φ). The key distribution procedure of the present cryptography is as follows (see Table 2):

[Sequence].

1. Bob randomly selects his phase basis $\varphi \in \{0, \pi\}$ to provide a φ-controlled coherent light pulse via the phase shifter Φ and sends it to Alice. Here, the φ-controlled light can be either individual or an N-bit chain for a batch job.
2. Bob converts his chosen φ into a key set $\{x\}$ for a record: $x \in \{0, 1\}$, where $x = 0$ 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 $\{y\}$ according to MZI physics of directionality (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 problems: see the red number in Table 2.
4. Alice randomly selects her phase $\psi \in \{0, \pi\}$ to create a ψ-controlled light pulse via the phase shifter Ψ and sends it back to Bob. Here, the ψ-phase control is performed on the reflected φ- controlled light pulse(s). This process is for the key setting, resulting in eavesdropping randomness as the inner-shared sifting process in addition to the MZI indistinguishability.
5. Alice converts her chosen ψ into a key set $\{z\}$ for a record: $z \in \{0, 1\}$, where $z = 0$ if $\psi = 0$ and $z = 1$ if $\psi = \pi$.
6. Alice sifts her prepared key in $\{z\}$ into $\{a\}$ by herself: $a = y$ if $y - z = 0$; $a = D$ if $y - z \neq 0$. Here, D stands for a discarded bit. This process is to avoid the *memory-based attack*.
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) except for error D (red). Here, $V_B \neq \pm 1$ stands for an error due to eavesdropping or network problems.
8. Bob sifts the copied key in $\{w\}$ into $\{b\}$ by himself: $b = w$ 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 (red) only for $V_A \neq \pm 1$ or $V_B \neq \pm 1$, and discard all corresponding bits in their key sets $\{a\}$ and $\{b\}$, respectively. They never announce their selected bases or visibilities. Alice and Bob finally share the same key $\{m\}$. In Table 2, the occurrence of network error (red D) is exaggerated for demonstration purpose, where the key rate of {m} is close to the half of the prepared one {x}.

Discussion

Unconditional security. The basic physics of unconditional security in the proposed classical cryptography lies in the quantum superposition between noncanonical (orthogonal) variables in MZI, corresponding to the no-cloning theorem in QKD, where the no-cloning theorem originates in Schrodinger's uncertainty principle with canonical (nonorthogonal) variables. Compared with the Heisenberg's uncertainty principle-caused no-cloning theorem in QKD, the unconditional security of the present cryptography belongs to classical physics of indistinguishability in MZI channel measurement. The measurement (eavesdropping)-caused fringe shift in MZI corresponds to the measurement-caused demolition of a quantum state in QKD.

When Alice's random phase choice is activated for the prepared keys by Bob, the unconditional security is fulfilled via round-trip MZI unitary transformation in a classical regime, where the random choice corresponds to post-measurement sifting in QKD. In other words, the eigenvalue (a chosen raw basis) provided by Bob is randomly selected (a basis for a final key) by Alice for key setting, resulting in deterministic randomness as analyzed in Fig. 2 (see also Fig. S1 in the Supplementary Information). The deterministic randomness means that the eigenvalue is deterministically inner shared between both parties but perfectly random to an eavesdropper owing to the double unitary transformations in a double MZI scheme. Thus, the phase controlled round-trip MZI becomes the physical bedrock of the present unconditionally secured classical cryptography. The novelty of the present cryptography protocol is in the potential application of the unconditional security to the classical regime with orthogonal (non-canonical) bases of bright light. As a result, the proposed cryptography is compatible with current fiber-optic communications networks, and thus, can support OTP with a high-speed (high-bit rate) optical key distribution at an extremely low error rate.

Memory-based attack. The *memory-based attack* is one of the major attacks in classical crypto-analysis. All classically encoded data can be intercepted and stored in a permanent memory device until a new technology such as a powerful computer or an efficient algorithm emerges. This is why there are several different encryption levels depending on the confidential level, e.g., in government documents. In the present cryptography, the *memory-based attack* can also be a powerful tool to a sophisticated eavesdropper, where the 50% chance in eavesdropping applies to all bits synchronously. Thus, Eve just unanimously flips all bits in the same key block $\{m'\}$ for correction if her guess is wrong. This is why the random basis selection is needed for sifting as shown in Table 2, resulting in bit-by-bit randomness.

Another way to protect the key from the *memory-based attack* is to use *network initialization* (discussed in Table 3) for each bit of the key. By either sifting or *network initialization*, the eavesdropping randomness in Fig. 2 is achieved. Thus, the eavesdropping chance exponentially decreases as the key length increases: For an n-bit-long key block, the eavesdropping chance η is $\eta = 2^{-n}$. If the key length is as short as 128-bit long ($n = 128$), it takes thousand times longer than the universe age to decipher the key with even the most powerful supercomputer in the world (see Section S3 of the Supplementary information). Because there is no efficient algorithm for perfect random variables and the 128-bit long key can be easily and repeatedly (to some extent) generated by an even pseudo-random generator, it proves that the present protocol is unconditionally secured in a classical regime. By using personal computers and optoelectronic devices operating at GHz speed, the key distribution rate is

Party	Sequence		Order (N)									
			1	2	3	4	5	6	7	8	9	10
Alice	2	V_A[a]	1	−1	−1	1	−1	1	1	1	−1	1
	3	ψ	δ	δ	δ + π	δ	δ + π	δ + π	δ	δ + π	δ	δ + π
	5	Correctness	O	X	O	O	O	X	O	X	X	X
Bob	1	φ	0	π	π	0	π	0	0	0	π	0
	4	V_B[a]	−1	1	−1	−1	−1	1	−1	1	1	1

Table 3. Network initialization for Table 2. Table 3 is for non-π-added δ. For π-added δ, see Section S4 of the Supplementary Information. "O" ("X") represents a correct (wrong) one. [a]$V_A = V_{5,6}; V_B = V_{9,10}$.

independent of the transmission distance if a batch job is performed as shown in Table 2. Thus, the proposed protocol can be potentially applicable to a real-time key distribution system opening the door to OTP.

Network Initialization. For the deterministic randomness analyzed in Figs. 1, 2 and 3, the *network initialization* between Alice and Bob is prerequisite to avoid the *memory-based attack* if there is no sifting. As a preparation step, Alice resets the MZI network with intentional phase turbulence to break the synchronized randomness in Eve's eavesdropping strategy. To do this, Alice scans her phase shifter $\Psi(\delta)$ until she has maxima in visibility V_A for the same test bits provided by Bob. The value of V_A, however, is not determined by the φ phase basis because of $\varphi \neq \delta$. This fact also applies to Eve (δ') in the same analogy: $\delta \neq \delta'$. Thus, the key sharing between Bob and Alice is not deterministic anymore. To solve this dilemma, i.e., to let only Alice know secretly and deterministically the φ-value set by Bob, the following *network initialization* procedure must be performed before the key procedure of Table 2.

Table 3 is for *network initialization* preceded the key distribution procedure in Table 2: sequence 2–5. For this, firstly, Alice randomly resets the MZI system by arbitrarily adjusting a path length with an additional phase variable δ and scans it for her phase controller $\Psi(\delta)$ until she gets maxima in V_A for the Bob prepared test bit. Then, Alice sends a cue to Bob. For this, Bob sends the same test bits encoded by $\varphi \in \{0, \pi\}$. Now, first, Bob randomly selects $\varphi \in \{0, \pi\}$ for the light pulse E_4 and sends it to Alice along with E_3 (see Fig. 2). Second, Alice randomly sets her phase controller Ψ with either δ or $\delta + \pi$ measures V_A. Third, Allice publically announces her measurement result. Alice never announces her phase choice either for ψ or δ. Fourth, Bob measures his V_B and publically announces whether Alice's measurement is correct or not. Then, Alice knows secretly and deterministically whether the δ is correct or wrong: Table 3 is for the case of non-π-phase shifted δ. For the wrong case, Alice simply added a π phase to δ to fix it. The sequence 2–5 may be repeated until successful or to have a batch code for *network initialization*. As mentioned in Table 2, each *network initialization* must be performed for each bit if there is no sifting.

[Sequence].

0. Initially Alice resets the MZI network by disturbing the MZI with her phase controller $\Psi(\delta)$ and scans δ until she gets $V_A = \pm 1$ for the test bits provided by Bob. The δ is a phase variable added to her phase basis $\psi \in \{0, \pi\}$. Then, Alice gives a cue to Bob.
1. Bob randomly selects his phase basis $\varphi \in \{0, \pi\}$, encodes his light with φ, and sends it to Alice.
2. Alice measures V_A and publically announces the result.
3. Alice resend the φ-set light after encoding it with $\delta + \psi$.
4. Bob measures V_B and publically announces whether Alice's result is correct (O) or not (X).
5. Alice resets her phase basis $\psi \in \{0, \pi\}$ to either $\psi \in \{\delta, \pi + \delta\}$ or $\psi \in \{-\delta, \pi - \delta\}$ depending on the Bob's announcement: end of network initialization: correctness
6. The sequence 2–5 may be repeated if not successful or to have a batch code with different δ values: order (N = 2–10).

Eve can also do the same job as Alice does with an arbitrary value of δ'. In the same analogy Eve may get the same but unsynchronized fringe pattern due to $\delta \neq \delta'$. The chance of $\delta = \delta'$ is extremely low as shown in the BER map in Fig. 3a. Here, the BER map resolution is determined by the detector's sensitivity which is very high ($> 10^4$ V/W at GHz) for commercially available photodiodes. Thus, the eavesdropping-immune MZI security can be obtained by *network initialization*. To surprise, this MZI security is achieved by all classical means to satisfy the present unconditionally secured cryptography. One might repute that Eve's intervention may cause a V_A shift so that the initialization sequence could results an error. It could be true, but a consistent V_A shift does not affect the unconditional security at all, otherwise, reveals Eve's existence. Thus, the *network initialization* can be used as authentication.

With the sifting in Table 2, the *network initialization* does not have to be repeated. The expected overall key distribution rate in Table 2, therefore, would be half of the usual data traffic rate. Without sifting, however, the *network initialization* must be performed for each bit to avoid the *memory-based attack*: see Section S4 of the

Supplementary Information. With the *network initialization* for each bit without sifting the key distribution speed for Table 2 (without sifting) may be slowed down.

The man-in-the-middle attack. The *man-in-the-middle attack* represents for 'intercept and resend,' where Eve behaves as Alice to Bob. As discussed in the *network initialization*, however, this attack cannot be successful to break the inner-shard determinacy of MZI. The inner-shard determinacy is the intrinsic property of the MZI coherence as explained in Figs. 1, 2 and 3. In other words, the MZI channel configuration between Bob and Alice cannot be exactly duplicated for Eve due to the system independency in coherence. Either single tapping or double tapping in Fig. 2, the phase synchronization between Alice and Eve cannot be achieved by any means. Thus, the *man-in-the-middle attack* should be failed for the proposed scheme.

Bit error rate: BER. In QKD, QBER strongly depends on Eve's strategy for sifting rate, the transmission distance, and detector's noise such as dark count rate and efficiency[34]. As a result, QBER can reach at a few percent[3,34]. On the contrary, the present protocol belonging to a classical cryptography is independent of detector's dark count noise and efficiency as well as sifting rate because Eve's intrusion is openly allowed and bright coherent light is used as a key carrier. The upper bound of BER of the present protocol is determined by both network errors and computational complexity as mentioned in the section of *memory-based attack*. The BER for long-haul fiber-optic communications networks has already been widely accepted to be less than one part per ten billions[35]. Thus, the cryptographic BER of the present protocol may be combined with computational complexity, $BER = BER_{net} + BER_{comp}$, where BER_{net} is related with current fiber-optic-based network BER, and BER_{comp} is related with a key length as mentioned in the section of *memory-based attack*. A key length as short as 128 bit long results in $BER_{comp} = \left(\frac{1}{2}\right)^{126} \sim 10^{-38}$, where no algorithm exists to decode random numbers. Although the upper bound of BER of the present protocol determined by BER_{net} may be increased by Eve's intrusion, a smart Eve may not deteriorate it. Due to the *Initialization* process, however, Eve's gain should be limited by the lower bound of BER_{comp}. More detailed analysis is beyond the present scope.

Applications. Owing to strong demand in both wired and wireless communications, the information traffic in an optical fiber has increased three folds every two years over the last thirty years[35,36]. In optical fiber backbone networks, a traffic speed of 100 Gbps per (wavelength) channel has already 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[37]. Thus, the capacity per fiber will reach its theoretical upper bound of 100 Tbps in a decade. Eventually a multicore fiber may replace current single-core fibers in the near future to overcome the channel capacity saturation[38]. In the multi-core fiber, a relative path-length drift caused by environmental noises such as vibrations and temperatures should be frozen due to spatial proximity between them in a few micron scale. Thus, the basic infrastructure of the double channels satisfying the MZI scheme for the present cryptography can be easily provided (see Fig. S3 of the Supplementary Information).

For the applications, current 10–100 km spaced EDFA fiber-optic networks may be fit, where the MZI length becomes unlimited due to the coherence nature of light even with coherent amplifications of EDFA. This unlimited transmission distance is the 2nd novelty of the present cryptography, where photon cloning by EDFA is basically phase-locked coherence process, resulting in only a fixed phase shift. The fixed phase shift in the cloning process can be dynamically adjusted in real time via visibility monitoring with laser locking techniques[23,24].

In conclusion, a coherence optics-based classical key distribution protocol was proposed, analyzed, and discussed to overcome the limitations in both classical and quantum cryptographies. The unconditional security of the proposed cryptography was obtained in a classical regime by using quantum superposition of MZI transmission channels and unitary transformation of MZI matrix. To prevent the system from typical cryptoanalysis such as memory-based attack and man-in-the-middle attack, sifting and network initialization protocols were presented and discussed for the unconditionally secured key distribution. In addition, the network initialization can also be adapted for authentication. By definition of coherence optics, the presented cryptography should be compatible with current fiber-optic communications networks at ~Gbps key rate. Thus, the proposed protocol has potential for one-time-pad cryptography which is the long lasting goal in human history for coming information era. Eventually, all-optical computers[39] may be combined with the present scheme for all-in-one secured information networks. The proposed cryptography is also applicable for wireless[40] or satellite[41] communications via MIMO[42] technologies (discussed elsewhere). Therefore, the round-trip unitary transformation based on MZI path superposition with non-canonical variables opens a door to new physics beyond QKD limited to a quantum regime.

Received: 7 September 2019; Accepted: 15 June 2020
Published online: 15 July 2020

References

1. Mao, W. *Modern Cryptography: Theory and Practice* (Prentice Hall, Inc, Upper Saddle River, 2004).
2. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Issnformation* (Cambridge University Press, Cambridge, 2000).
3. Gisin, N., Ribordy, G., Tittle, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
4. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).

5. 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*, Vol. 1, 175–179 (New York, 1984); *ibid*, *Theor. Comput. Sci.* **560**, 7–11 (2014).
6. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *Quantum Inf.* **2**, 16025 (2016).
7. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686–689 (2010).
8. Huang, A., Sun, S.-H., Liu, Z. & Makarov, V. Quantum key distribution with distinguishable decoy states. *Phys. Rev. A* **98**, 012330 (2018).
9. Gerhardt, I. *et al.* Experimental faking the violation of Bell's inequalities. *Phys. Rev. Lett.* **107**, 170404 (2011).
10. Sajeed, S. *et al.* Insecurity of detector-device-independent quantum key distribution. *Phys. Rev. Lett.* **117**, 250505 (2016).
11. 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**, 400–403 (2018).
12. Qin, H., Kumar, R., Makarov, V. & Alleaume, R. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Phys. Rev. A* **98**, 012312 (2018).
13. Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nat. Photon.* **7**, 210–214 (2013).
14. Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33–80 (2011).
15. Vernam, G. S. *Secrete signaling system*. US patent 1,310,719 (1919).
16. Degiorgio, V. Phase shift between the transmitted and the reflected optical fields of a semireflecting lossless mirror is π/2. *Am. J. Phys.* **48**, 81–82 (1980).
17. Zeilinger, A. General properties of lossless beam splitters in interferometry. *Am. J. Phys.* **49**, 882–883 (1981).
18. Mandel, L. Photon interference and correlation effects produced by independent quantum sources. *Phys. Rev. A* **28**, 929–943 (1983).
19. Shannon, C. A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 379–423 (1948).
20. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121–3124 (1992).
21. 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**, 2797–2799 (2004).
22. Sibson, P. *et al.* Chip-based quantum key distribution. *Nat. Commun.* **8**, 13984 (2016).
23. Xaiver, 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**, 1764–1766 (2011).
24. Abbott, B. P. *et al.* Observation of gravitational waves from binary black hole merger . *Phys. Rev. Lett.* **116**, 061102 (2016).
25. Goldenberg, L. & Vaidman, L. Quantum cryptography based on orthogonal states. *Phys. Rev. Lett.* **75**, 1239–1243 (1995).
26. Cerf, N. J., Adami, C. & Kwiat, P. G. Optical simulation of quantum logic. *Phys. Rev. A* **57**, R1477–R1480 (1998).
27. Hong, C. K., Ou, Z. Y. & Mandel, L. Measurement of subpicosend time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044–2046 (1987).
28. Carolan, J. *et al.* Universal linear optics. *Science* **349**, 711–716 (2015).
29. Capbell, G. T. *et al.* Configurable unitary transformations and linear logic gates using quantum memories. *Phys. Rev. Lett.* **113**, 063601 (2014).
30. Ham, B. S. Wavelength convertible quantum memory: controlled echo. *Sci. Rep.* **8**, 10675 (2018).
31. Kikforman, J.-P., Joffre, M. & Thierry-Mieg, V. Measurement of photon echoes by use of femtosecond Fourier-transform spectral interferometry. *Opt. Lett.* **22**, 1104–1106 (1997).
32. Ham, B. S., Shahriar, M. S., Kim, M. K. & Hemmer, P. R. Spin coherence excitation and rephrasing with optically shelved atoms. *Phys. Rev. B* **58**, R11825–R11828 (1998).
33. Gentle, J. E. *Random Number Generation and Monte Carlo Methods* 2nd edn. (Springer, New York, 2004).
34. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic device. *Rev. Mod. Phys.* **92**, 025002 (2020).
35. Winzer, P. J., Neilson, D. T. & Chraplyvy, A. R. Fiber-optic transmission and networking: the previous 20 and the next 20 years [invited]. *Opt. Exp.* **26**, 24190–24239 (2018).
36. Matsuoka, S. Ultrahigh-speed ultrahigh-capacity transport network technology for cost-effective core and metro networks. *NTT Tech. Rev.* **9**, 1–7 (2011).
37. Essiambre, R.-J. & Tkach, R. W. Capacity trends and limit of optical communication networks. *Proc. IEEE* **5**, 1035–1055 (2012).
38. Saitoh, K. Multicore fiber technology. *J. Lightwave Technol.* **34**, 55–66 (2016).
39. Ham, B. S. & Hahn, J. Observations of ultraslow light-based photon logic gates: NAND/OR. *Appl. Phys. Lett.* **94**, 101110 (2009).
40. Nauerth, S. *et al.* Air-to-ground quantum communication. *Nat. Photon.* **7**, 382–386 (2013).
41. Liao, S.-K. *et al.* Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
42. Larsson, E. G., Edfors, O., Tufvesson, F. & Marzetta, T. L. Massive MIMO for next generation wireless systems. *IEEE Commun. Mag.* **52**, 186–195 (2014).

Acknowledgements

The author acknowledges that the present work was supported by the ICT R&D program of MSIT/IITP (1711042435: Reliable crypto-system standards and core technology development for secure quantum key distribution network) and GRI grant funded by GIST in 2020.

Author contributions

B.S.H. wrote the manuscript and prepared all figures sssand tables. Correspondence and request of materials should be addressed to BSH (email: bham@gist.ac.kr).

Competing interests

The author declares no competing interests.

Additional information

Supplementary information is available for this paper at https://doi.org/10.1038/s41598-020-68038-7.

Correspondence and requests for materials should be addressed to B.S.H.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.