scientific reports

Check for updates

OPEN

Experimental demonstrations of unconditional security in a purely classical regime

Byoung S. Ham

So far, unconditional security in key distribution processes has been confined to quantum key distribution (QKD) protocols based on the no-cloning theorem of nonorthogonal bases. Recently, a completely different approach, the unconditionally secured classical key distribution (USCKD), has been proposed for unconditional security in the purely classical regime. Unlike QKD, both classical channels and orthogonal bases are key ingredients in USCKD, where unconditional security is provided by deterministic randomness via path superposition-based reversible unitary transformations in a coupled Mach–Zehnder interferometer. Here, the first experimental demonstration of the USCKD protocol is presented.

Quantum key distribution (QKD) has been intensively researched for unconditionally secured key distribution over the last several decades[1–13]. Since the first QKD protocol of BB84[1], various types of QKD protocols have been successfully demonstrated using optical fibers, free space, and even satellites[10]. Regardless of QKD type, the essential requirements for unconditional security are lossless quantum channels and perfect single-photon detectors. Moreover, a deterministic nonclassical light source is required for potential applications of QKD such as online banking and quantum internet. So far, none of these requirements have been fully satisfied. As a result, the unconditional security of QKD lied in the no-cloning theorem based on Heisenberg's uncertainty principle[14] cannot be fulfilled unless quantum loopholes are completely closed[6–13]. The bedrock of no-cloning theorem for the unconditional security in QKD is the quantum superposition between binary bases, resulting in eavesdropping randomness[14]. To initiate quantum superposition-based unconditional security in QKD, the basis of keys cannot be orthogonal. This is the fundamental difference of QKD compared with classical cryptography based on orthogonal bases.

Recently, a completely different protocol for unconditionally secured classical key distribution (USCKD) has been proposed to overcome the limitations of QKD mentioned above as well as to understand the basic quantum features in a classical regime[15]. Compared with quantum superposition-caused randomness in QKD, USCKD achieves unconditional security via path superposition in a Mach–Zehnder interferometer (MZI), where a coupling method between two MZIs plays a key role[16]. Unlike QKD, USCKD is based on a purely classical system of MZIs with orthogonal bases. Thus, USCKD seems to be self-contradicting because the unconditional security of QKD is based on non-orthogonal bases. Here, secrete of unconditional security in USCKD is in the path superposition-caused measurement randomness between orthogonal bases. According to information theory, randomness represents that there is no information to eavesdrop[17]. Moreover, USCKD results in key distribution determinacy between two remote parties via the coherence physics of MZI, even without post-measurement of sifting in QKD. The key distribution determinacy in USCKD is provided by reversible unitary transformations such as in quantum optical memories[18,19]. Thus, two-way communication channels are adapted to provide eavesdropping randomness and directional determinacy to form coupled MZI channels[15].

The fundamental physics of USCKD has been studied in a coupled MZI system[15], where a specific phase relationship between the coupled MZIs results in nonclassical features of coherence de Broglie wavelength (CBW)[16,20]. CBW is a classical version of photonic de Broglie wavelength (PBW), where PBW is a typical macroscopic quantum feature studied for quantum sensing and quantum metrology over the last few decades[21–27]. Recently, experimental demonstrations of CBW have been successfully performed, where USCKD represents a special state of CBW under the same physics[28]. Thus, CBW as well as USCKD have been understood as a macroscopic feature[15,16]. In that sense, conventional understanding of the quantum nature limited to the microscopic world satisfying the uncertainty principle has been intrigued and expanded toward the macroscopic world, such as in the case of Schrodinger's cat[29,30]. Here, USCKD is experimentally demonstrated for the proof of

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, South Korea. email: bham@gist.ac.kr

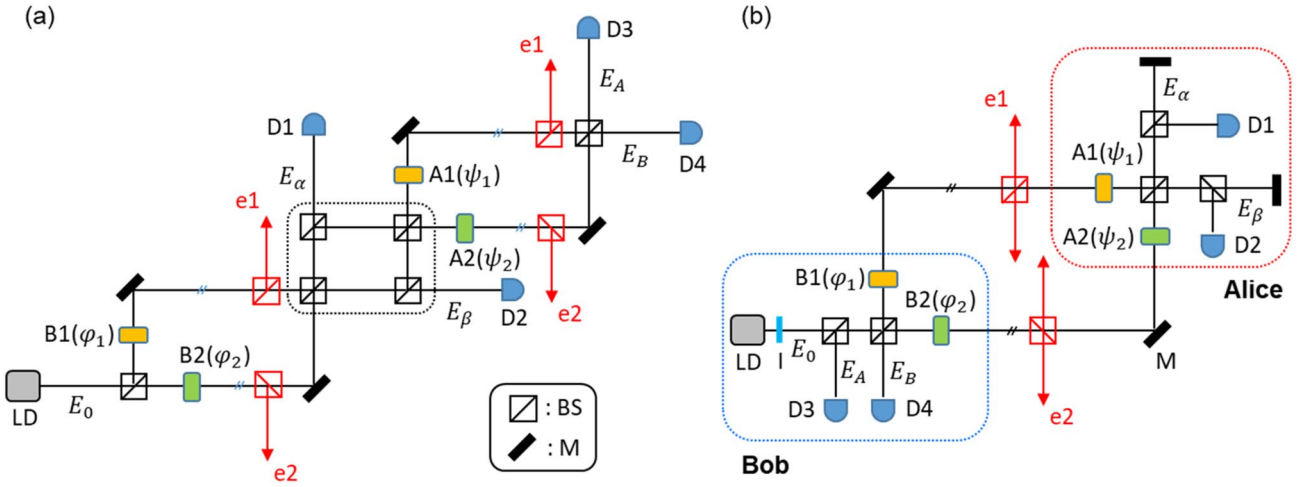

Figure 1. A schematic of unfolded USCKD for (**a**) unfolded and (**b**) folded configurations. Aj(ψ_j) and Bj(φ_j) represent an acousto-optic modulator j for Alice and Bob with phase basis $\psi \in \{0, \pi\}$ and $\varphi \in \{0, \pi\}$, respectively, where $\psi = \psi_{12}(= \psi_1 - \psi_2)$ and $\varphi = \varphi_{12}(= \varphi_1 - \varphi_2)$. The e1 and e2 in red denote eavesdropping paths by Eve. LD: Laser, I: isolator, BS: unpolarizing beam splitter, M: mirror, and Dj: detector j. All Aj's are synchronized via microwave generators at 80 MHz.

principle of unconditional security in a purely classical regime of coupled MZIs. This study may open the door to coherence quantum technology, overcoming limitations in conventional quantum technologies confined to the microscopic world[1–13,21–27].

Results

Figure 1a shows an unfolded scheme of USCKD[15] based on orthogonal bases of coherent light for classical key distribution, where two MZIs are coupled symmetrically with $\varphi_{12} = \psi_{12}$ and $\zeta_{ij} = \zeta_i - \zeta_j$. This means that the basic scheme of USCKD is composed of two identical MZIs via quantum superposition (see the dotted box) between them. Here, the coupling method for superposition plays an important role[15,16]. Unlike the symmetric coupling for USCKD in Fig. 1, CBW is based on asymmetric coupling, in which the asymmetry represents a $\pi-$phase shift to the second MZI of ψs[16]. In each MZI, two phase bases $(0, \pi)$ of each path can be controlled by an acousto-optic modulator (AOM) pair, in which each AOM driving frequency plays a key role for the phase control of the MZI (discussed in experiments). In Fig. 1a, the φ_j-based first MZI belongs to Bob for key preparation, while the ψ_j-based second MZI belongs to Alice to set the key. When Fig. 1a is folded for a round trip USCKD configuration, the right-end BS meets the left-end BS, resulting in Fig. 1b. In other words, the detectors D3 and D4 with phase shifters B1 and B2 belong to Bob, while D1 and D2 with A1 and A2 phase shifters belong to Alice. Alice and Bob have a basis set, $\psi \in \{0, \pi\}$ and $\varphi \in \{0, \pi\}$, respectively, where $\psi \equiv \psi_{12}$ and $\varphi \equiv \varphi_{12}$.

For the experiments, all AOMs are set to be in-phase, and the phase control of the MZI system relies only on the upper AOM A1 via a two-channel function generator (AFG3102, Tektronix). For this, the lower AOM driving frequencies are fixed at 80 MHz sharp. To select a phase basis for each optical key, all four AOMs are synchronized to driving frequency generators, PTS160, PTS250, and AFG3102. The lower two AOMs, B2 and A2, are controlled by PTS160 and PTS250, respectively. The upper two AOMs, B1 and A1, are controlled by AFG3102. Thus, there are four possible phase basis combinations (see "Theory").

A sophisticated eavesdropper Eve attacks the transmission lines in both MZI channels via BSs, as shown by the red lines (e1 and e2), to form the same interferometric scheme as Alice's or Bob's. Unlike QKD, such a channel attack is allowed in USCKD without revealing her existence to Bob and Alice. Due to measurement randomness or indistinguishability in MZI, however, Eve's chance to extract the correct phase information is 50% on average, resulting in unconditional security[15]. This randomness of 50% is the bedrock of unconditional security in USCKD. Here, it should be noted that Eve cannot distinguish the set basis by the MZI channel attack due to path superposition unless the set basis is known (see section A of the Supplementary Information). Regarding classical cryptographic researches, fundamental primitives for security have been developed to protect public key encryption, digital signature, or tag encoding schemes in networks from side-channel attack such as related-key attacks[31] or network pollution attacks[32]. Thus, the present research of USCKD ensures those classical security systems.

Theory. For an analytic approach, the matrix representation for the first MZI in Fig. 1a is given:

$$\begin{bmatrix} E_\alpha \\ E_\beta \end{bmatrix} = [BS][\varphi][BS]\begin{bmatrix} E_0 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 - e^{i\varphi} & i\left(1 + e^{i\varphi}\right) \\ i\left(1 + e^{i\varphi}\right) & -\left(1 - e^{i\varphi}\right) \end{bmatrix}\begin{bmatrix} E_0 \\ 0 \end{bmatrix}, \quad (1)$$

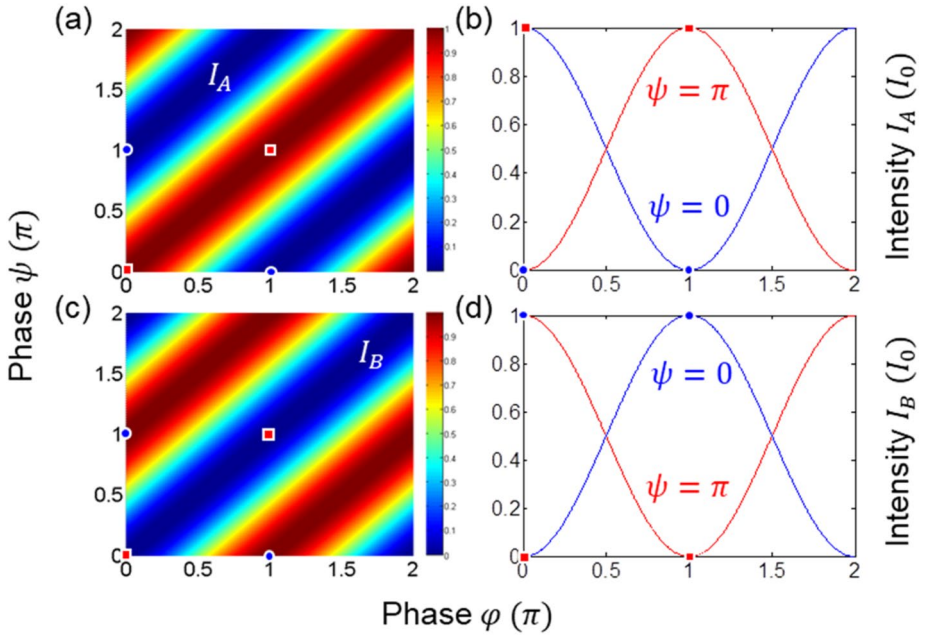

Figure 2. Numerical calculation for Eq. (4). $\varphi = \varphi_{12}$; $\psi = \psi_{12}$. (**a**)–(**d**) Red square (blue dot) indicates identity (inversion) relation between two phase bases.

where $\varphi = \varphi_{12}$ and E_0 is the input field of coherent light from LD. The BS matrix is $[BS] = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$, and the matrix of a phase shifter between two MZI paths is $[\varphi] = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$. Thus, the corresponding output intensities detected by D1 and D2 are as follows, respectively:

$$I_\alpha = \frac{1}{2}(1 - cos\varphi), \tag{2}$$

$$I_\beta = \frac{1}{2}(1 + cos\varphi), \tag{3}$$

where $I_j = E_j E_j^*$. Depending on the orthogonal phase basis of $\varphi \in \{0, \pi\}$ in MZI, the output field intensity becomes either I_α or I_β. Thus, Alice knows what basis is chosen by Bob by her visibility ($V_{\alpha\beta}$) measurements (see section B of the Supplementary Information)[15]. This represents the MZI propagation directionality. Here, it should be noted that the phase basis selection in φ (ψ) belongs to Bob (Alice) for key preparation (confirmation) according to the USCKD protocol[15]. The output field from the first MZI is inserted into the second MZI via symmetric superposition (dotted box) for Alice's control. From the second MZI, the final output fields E_A and E_B are obtained as:

$$\begin{aligned} \begin{bmatrix} E_A \\ E_B \end{bmatrix} &= [BS][\psi][BS]\begin{bmatrix} E_\alpha \\ E_\beta \end{bmatrix}, \\ &= -\frac{1}{2}\begin{bmatrix} e^{i\varphi} + e^{i\psi} & -i\left(e^{i\varphi} - e^{i\psi}\right) \\ i\left(e^{i\varphi} - e^{i\psi}\right) & e^{i\varphi} + e^{i\psi} \end{bmatrix}\begin{bmatrix} E_0 \\ 0 \end{bmatrix}. \end{aligned} \tag{4}$$

Owing to the binary phase bases of φ and ψ, there are four combinations of phase bases between Bob and Alice for the key distribution:

(i) $\varphi = 0; \psi = 0$

For the case (i), Eq. (4) becomes (see the red square in Fig. 2):

$$\begin{bmatrix} E_A \\ E_B \end{bmatrix} = -e^{i\varphi}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} E_0 \\ 0 \end{bmatrix}. \tag{5}$$

Thus, the corresponding intensities are $I_A = I_0$ and $I_B = 0$, resulting in an identity relation: $V_{AB} = 1$, where the visibility is defined as $V_{AB} = \frac{V_A - V_B}{V_A + V_B}$.

	φ	φ
φ	**0**	**π**
0	$V_{AB} = 1$	$V_{AB} = -1$
π	$V_{AB} = -1$	$V_{AB} = 1$

Table 1. Output fields in Fig. 1. $\varphi = \varphi_{12}$; $\psi = \psi_{12}$. visibility: $V_{AB} = \frac{V_A - V_B}{V_A + V_B}$

(ii) $\varphi = 0; \psi = \pi$

For the case (ii), Eq. (4) becomes (see the blue dot in Fig. 2):

$$\begin{bmatrix} E_A \\ E_B \end{bmatrix} = ie^{i\varphi} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} E_0 \\ 0 \end{bmatrix}. \tag{6}$$

Thus, the corresponding intensities are $I_A = 0$ and $I_B = I_0$, resulting in an inversion relation:$V_{AB} = -1$.

(iii) $\varphi = \pi; \psi = 0$

For the case (iii), Eq. (4) becomes (see the blue dot in Fig. 2):

$$\begin{bmatrix} E_A \\ E_B \end{bmatrix} = -ie^{i\varphi} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} E_0 \\ 0 \end{bmatrix}. \tag{7}$$

Thus, the corresponding intensities are $I_A = 0$ and $I_B = I_0$, resulting in an inversion relation:$V_{AB} = -1$.

(iv) $\varphi = \pi; \psi = \pi$

For the case (iv), Eq. (4) becomes (see the red square in Fig. 2):

$$\begin{bmatrix} E_A \\ E_B \end{bmatrix} = e^{i\varphi} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} E_0 \\ 0 \end{bmatrix}. \tag{8}$$

Thus, the corresponding intensities are $I_A = I_0$ and $I_B = 0$, resulting in an identity relation:$V_{AB} = 1$.

In a short summary, $I_A = I_0$ and $I_B = 0$ are achieved for $\varphi = \psi$, otherwise $I_A = 0$ and $I_B = I_0$. Like Alice's measurements in Eqs. (2) and (3), Bob also knows Alice's phase basis choice by measuring his visibility even without communication with her. As a basic property of coherence optics, this propagation directionality in a coupled MZI is the quintessence of USCKD with superposition-caused measurement randomness to an eavesdropper[15], where the measurement is for the channel attack by an eavesdropper (see section A of the Supplementary Information).

These four options for the key distribution process analyzed in Eqs. (5)–(8) are numerically demonstrated in Fig. 2 by solving Eq. (4). Figure 2a,b are for the output field I_A, and Fig. 2c,d are for I_B. Depending on the $\psi-$basis choice by Alice given $\varphi-$basis chosen by Bob, the visibility V_{AB} becomes either 1 or -1. As an example, for $\varphi = \pi$ (see the center red squares), Bob surely knows the basis chosen by Alice by his visibility measurements. The key distribution determinacy between Bob and Alice in USCKD is summarized in Table 1.

Experiments. Figure 3 shows experimental results corresponding to Fig. 2 and Table 1, where four different phase combinations are performed in a cw scheme of the laser light E_0. The temporal stability is determined mostly by air fluctuations in MZI paths. In Fig. 3, a rough laboratory condition is intentionally applied to the data without any system stabilization, where the MZI stability issue has already been closed[33,34]. Figure 3a shows the MZI channel stability for 20 s for the case of $\psi = \varphi$. For this, all four AOMs are set at 80 MHz and $\psi = \varphi$. Here, the experimental results of Fig. 3a are the same as in Fig. 2 (see the red squares for $\varphi = 0$). As mentioned above, the experimental data are from bare laboratory conditions, resulting in ~20% phase (path length) fluctuations in short time scales less than a minute. In a long-time scale, the output intensity varies between the minimum and maximum mostly due to air fluctuations.

Figure 3b shows a frequency-dependent phase control of AOM A1 (see Fig. 1). For this, the frequency for A1 is switched to either 1 Hz more or 1 Hz less than AOM A2 at 80 MHz sharp. The other AOMs are set at 80,000,001 Hz for B1 and 80,000,000 Hz for B2, resulting in $\varphi = 1Hz$ and $\psi = \pm 1Hz$. The asymmetric structure of the coupled MZIs with $\psi = -\varphi$ results in CBW, whose modulation frequency turns out to be doubled (2 Hz), as shown in the region left of the dashed line in Fig. 3b due to $\lambda_{CBW} = \lambda/2$[16]. This doubled frequency is a quantum feature obtained in a classical domain, where it is not the frequency beating. Here, the wavelength λ is for the input light E_0, and λ_{CBW} is due to the nonclassical properties ($V_{AB} > 0.71$) of CBW.

If the symmetric coupling condition is satisfied with $\psi = \varphi$, then the identity relation in Eqs. (5) and (8) is satisfied (see both I_A and I_B in the right region of the dashed line in Fig. 3b), where the nonclassical feature of CBW disappears. The residual 1 Hz (not 2 Hz) modulation is due to the background (leakage) from the first MZI at $\varphi_{12} = 1Hz$, which is not completely isolated in the experimental setup. Figure 3c is an extension of Fig. 3b, where the output intensities of CBWs are also opposite each other as in the conventional MZI outputs in Fig. 2. Here, the modulation depth ($V_{AB} < 0.71$) below CBW represents the classical feature of USCKD[35].

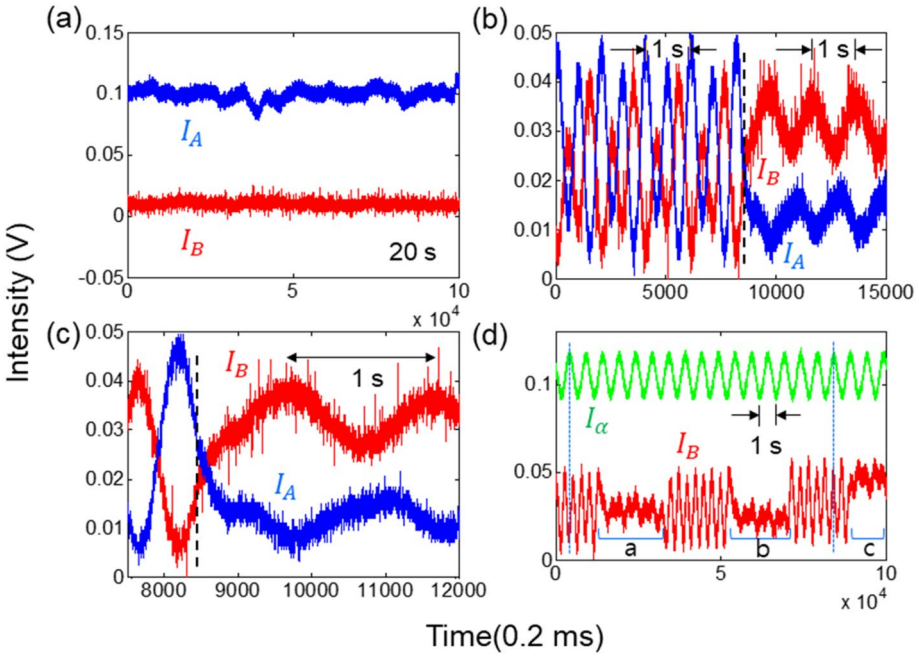

Figure 3. Experimental results for USCKD in Fig. 1. (**a**) $\psi_{12} = \varphi_{12}$. (**b**) Switching between CBW and USCKD. (c) expansion of (**b**). (**d**) Conventional MZI output (green) vs. CBW [USCKD(a/b/c)] (red). In (**b**) and (**c**), $\varphi_{12} = -\psi_{12} = 1Hz$ before the dashed line; $\varphi_{12} = \psi_{12} = 1Hz$ after the dashed line. The value of vertical axis is arbitrary.

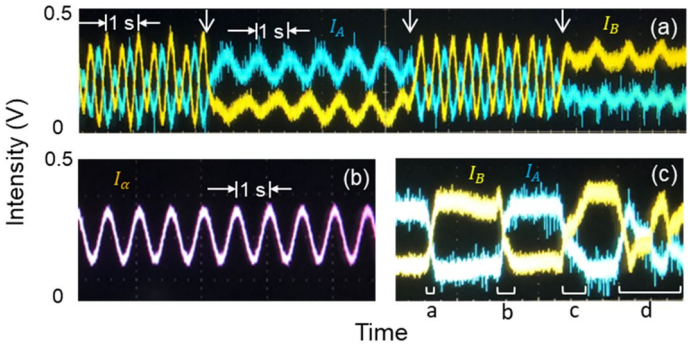

Figure 4. (**a**) CBW vs. USCKD. (**b**) Conventional MZI output I_α. (**c**) Manual phase control for ψ_1 in Fig. 1. The driving frequencies for AOM B1 and B2 are 80,000,001 Hz and 80,000,000 Hz. The brackets in (**c**) indicate manual phase (ψ) scanning. Intensities in (**a**–**c**) are arbitrary.

Figure 3d represents toggle switching between CBW and USCKD, where the green curve is for the reference of I_α from the first MZI. In the toggle switching by AOM A2 (see the red curve), the intensity value of USCKD depends on the phase of CBW at switching time as denoted in regions 'a,' 'b,' and 'c.' For potential applications of USCKD, such an arbitrary intensity value can be controlled by controlling the internal phase of an rf generator. As already known for CBW bases[35], USCKD is understood as an extreme of CBW in terms of a symmetric mode in a coupled pendulum model[36]. The alternating CBW peaks between maxima and minima for a fixed value of I_α represent the increased phase bases (see the dotted lines). In other words, the π span in a single MZI is reduced to π/2 in the doubly coupled MZI, representing a quantum feature[35]. If an n-coupled MZI is used, then the phase basis span is reduced to π/n[35]. The related movie is shown in section C of the Supplementary Information for toggle switching between CBW and USCKD.

Figure 4 shows screen captures of the output intensities from the oscilloscope for Fig. 3. Figure 4a corresponds to Fig. 3b, where both the identity and inversion relations for USCKD in Fig. 2 are shown as results of toggle switching with AOM A2 from CBW. As shown, the maxima and minima of I_A and I_B are swapped according to a proper phase at the switching time as discussed in Fig. 3(d). Figure 4b is for the I_α from the first MZI as a reference, whose modulation frequency (beating) is 1 Hz due to the preset 1 Hz driving frequency difference between AOMs B1 and B2. As mentioned in Fig. 2 as well as Eqs. (5)–(8), Fig. 4c shows ψ− dependent intensity

swapping between I_A and I_B, where the phase control is performed by manually rotating a thin glass inserted into the A1 path of Fig. 1 (see the bracket regions). Here, $\psi = \varphi = 0$ is initially set for Fig. 4c. The rotation speed is not constant, but optimistically shows the trend of phase-dependent output-intensity variations. Glass rotation starts at a normal position with respect to the beam path, and thus the phase variation speeds up as it moves from region 'a' to 'd'.

Discussion

In addition to QKD, experimental demonstration of USCKD provides the proof of principle of unconditional security. As already discussed[15,16], such unconditional security of USCKD lies in the coupled path superposition between two MZIs, which cannot be obtained conventionlly. Thus, the coupled MZI structure should be differentiated from a single MZI, where the MZI itself belongs to the classical realm. To support the nonclassical property of the coupled MZIs, phase basis-based toggle switching with $\psi - \varphi = \pm 1$ Hz was demonstrated for swapping between CBW and USCKD. Here, the phase bases are orthogonal to each other, representing two modes of the nonclassical features. All aspects of USCKD are macroscopic and coherent. Although the structure of MZIs for USCKD is definitely classical, coupled superposition results in nonclassical features of de Broglie wavelength in an asymmetric form and unitary transformations (identity relation) in a symmetric form. The unitary transformation represents deterministic randomness, where the superposition-caused randomness in MZI is the bedrock of unconditional security in USCKD[15]. Understanding that MZI is another form of BS, where orthogonal input modes are automatically provided[20], the nonclassical features of USCKD or CBW in the present demonstrations are not trivial. Here, it should be noted that the physical origin of USCKD is the coupled superposition between two MZIs[15,35].

Conclusion

Experimental demonstrations of USCKD were presented in a symmetrically coupled MZI structure along with theoretical analyses. The unconditional security of USCKD was provided by deterministic randomness with round trip unitary transformations, where randomness plays a key role for unconditional security via MZI path superposition. The quantum behavior of the coupled MZI structure was confirmed by CBW with coupling manipulations, where the coupled MZIs regenerate fundamental phase bases. For the toggle switching between CBW and USCKD, a ± 1 Hz frequency difference between the coupled MZIs was used. For the round trip MZI directionality of USCKD, a manual phase (ψ) variation with a thin glass was performed, where $0 \leq \psi \leq 2\pi$. The MZI stability was tested in bare conditions of MZIs without environmental isolations or a feedback control. Taking advantages of technologically advanced laser locking systems, an active control for MZI phase stability is not an issue anymore, and thus practical applications of USCKD are plausible for fiber-optic communications networks or free space in the future.

Methods

In Fig. 1, the input light power of E_0 is around 1 mW, and the diffraction efficiency of AOMs is ~ 70%. The wavelength of E_0 is 606 nm whose linewidth is ~ 300 kHz, and intensity fluctuation is ~ 1%. The path length of each arm of MZI is ~ 60 cm. All AOM outputs are synchronized by synchronizing rf driving frequency generators, PTS160, PTS250, and AWG3102 (Tektronix) together. Each AOM in the first MZI is without a focused lens pair whose beam diameter is ~ 1 mm. Each AOM in the second MZI, however, is focused and collimated by a 10 cm focal-length lens pair. The fringe pattern of I_α and I_β is a bar shape as usual, while the fringe pattern of I_A and I_B is an Airy disk type due to the lens-caused circular aperture (see section C of the Supplementary Information). Hamamatsu avalanche photodiodes (C12703) are used to detect the data and recorded on a Tektronix oscilloscope (DPO5204B). For the data in Fig. 3, an iris is added before each detector to pass only the zeroth-order fringe pattern. For the movie in section C of the Supplementary Information, the output light of I_B is shined on a paper screen, and the image was captured via iPhone camera. The frequency offset $\pm\delta f$ between two upper paths of the coupled MZI via AOMs is controlled by a two-channel arbitrary function generator (Tektronix AFG3102), whose frequency resolution is 0.001 Hz. All data in Figs. 3 and 4 are raw, single-shot recordings without averaging or trimming. The major error source in data is the air fluctuations in each MZI because the MZI setup of Fig. 1 is uncovered. In other words, the experimental setup is under a rough, coarse, and noisy environment intentionally to show the system's robustness for potential applications, where phase locking is technologically well matured.

Received: 14 August 2020; Accepted: 5 February 2021
Published online: 18 February 2021

References

1. 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 1, pp. 175–179, New York. (1984); *ibid*, *Theoretical Computer Sci.* **560**, 7–11 (2014).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
3. Gisin, N., Ribordy, G., Tittle, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
4. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686–689 (2010).
5. Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387–10409 (2011).
6. Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nat. Photon.* **7**, 210–214 (2013).
7. 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).

8. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *Quantum Info.* **2**, 16025 (2016).
9. Sajeed, S. *et al.* Insecurity of detector-device-independent quantum key distribution. *Phys. Rev. Lett.* **117**, 250505 (2016).
10. Qin, H., Kumar, R., Makarov, V. & Alleaume, R. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Phys. Rev. A* **98**, 012312 (2018).
11. Gerhardt, I. *et al.* Experimental faking the violation of Bell's inequalities. *Phys. Rev. Lett.* **107**, 170404 (2011).
12. Yin, J. *et al.* Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140–1144 (2017).
13. 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).
14. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
15. Ham, B. S. Unconditionally secured classical cryptography using quantum superposition and unitary transformation. *Sci. Rep.* **10**, 11687 (2020).
16. Ham, B. S. Deterministic control of photonic de Broglie waves using coherence optics. *Sci. Rep.* **10**, 12899 (2020).
17. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
18. Moiseev, S. A. & Kröll, S. Complete reconstruction of the quantum state of a single-photon wave packet absorbed by a Doppler-broadened transition. *Phys. Rev. Lett.* **87**, 173601 (2001).
19. Ham, B. S. A wavelength-convertible quantum memory: controlled echo. *Sci. Rep.* **8**, 10675 (2018).
20. Ham, B. S. The origin of anticorrelation for photon bunching on a beam splitter. *Sci. Rep.* **10**, 7309 (2020).
21. Pezze, L., Augusto, S., Oberthaler, M. K., Schmied, R. & Treutlein, P. Quantum metrology with nonclassical states of atomic ensembles. *Rev. Mod. Phys.* **90**, 035005 (2018).
22. Pirandola, S., Bardhan, B. R., Gehring, T., Weedbrook, C. & Lloyd, S. Advances in photonic quantum sensing. *Nat. Photon.* **12**, 724–733 (2018).
23. Xiao, M., Wu, L.-A. & Kimble, H. J. Precision measurement beyond the shot-noise limit. *Phys. Rev. Lett.* **59**, 278–281 (1987).
24. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photon.* **5**, 222–229 (2011).
25. Jacobson, J., Gjörk, G., Chung, I. & Yamamato, Y. Photonic de Broglie waves. *Phys. Rev. Lett.* **74**, 4835–4838 (1995).
26. Walther, P. *et al.* Broglie wavelength of a non-local four-photon state. *Nature* **429**, 158–161 (2004).
27. Wang, X.-L. *et al.* 18-qubit entanglement with six photons' three degree of freedom. *Phys. Rev. Lett.* **120**, 260502 (2018).
28. Ham, B. S. Observations of coherence de Broglie waves (2020).
29. Friedman, J. R., Patel, V., Chen, W., Tolpygo, S. K. & Lukens, J. E. Quantum superposition of distinct macroscopic states. *Nature* **406**, 43–46 (2000).
30. Wineland, D. J. Nobel lecture: superposition, entanglement, and raising Schrodinger's cat. *Rev. Mod. Phys.* **85**, 1103 (2013).
31. Chang, J., Wang, H., Wang, F., Zhang, A. & Ji, Y. RKS security for identity-based signature scheme. *IEEE Access* **8**, 17833–17841 (2020).
32. Wu, X., Xu, Y., Yuen, C. & Xiang, L. A tag encoding scheme against pollution attack to linear network coding. *IEEE Trans. Parallel Dist. Syst.* **25**, 33–42 (2014).
33. Xavier, G. B. & von der Weid, J. P. Stable single-photon interference in a 1 km fiber-optic Mach-Zehnder interferometer with continuous phase adjustment. *Opt. Lett.* **36**, 1764–1766 (2011).
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. Analysis of nonclassical features in a coupled macroscopic binary system. arXiv: 2008.02472 (2020) (To be published in New J. Phys).
36. Hemmer, P. & Prentiss, M. G. Coupled-pendulum model of the stimulated resonance Raman effect. *J. Opt. Soc. Am. B* **5**, 1613–1623 (1988).

Acknowledgements

This work was supported by a GIST research institute (GRI) grant funded by GIST in 2021.

Author contributions

B.S.H. solely wrote the manuscript text and prepared all ideas, figures, calculations, experiments, and discussions. Correspondence and request of materials should be addressed to B.S.H. (email: bham@gist.ac.kr).

Competing interests

The author declares no competing interests.

Additional information

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1038/s41598-021-83724-w.

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.