Supplementary Information for

"Network-compatible unconditionally secured classical key distribution via quantum superposition-induced deterministic randomness," by

B. S. Ham
GIST, S. Korea
(bham@gist.ac.kr)

Section A: Unitary transformation

Using equation (1), the following identity and inversion matrices are obtained for the round-trip of light in Fig. 1:

$$\begin{bmatrix} E_9 \\ E_{10} \end{bmatrix} = [\mathrm{BH}] \begin{bmatrix} E_1 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -\{e^{i(\psi_2+\varphi_1)} + e^{i(\psi_1+\varphi_2)}\} & i\{e^{i(\psi_2+\varphi_1)} - e^{i(\psi_1+\varphi_2)}\} \\ i\{e^{i(\psi_1+\varphi_2)} - e^{i(\psi_2+\varphi_1)}\} & -\{e^{i(\psi_2+\varphi_1)} + e^{i(\psi_1+\varphi_2)}\} \end{bmatrix} \begin{bmatrix} E_1 \\ 0 \end{bmatrix}, \quad \text{(A1)}$$

where [BH]= $[BS]\left[\psi_{1,2}\right][BS][BS]\left[\varphi_{1,2}\right][BS]$. The matrices [BS], $\left[\psi_{1,2}\right]$, and $\left[\varphi_{1,2}\right]$ are respectively for the beam splitter, the phase controllers Ψ_i, and Φ_i in the MZI:

$$[BS] = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \quad \text{(A2)}$$

$$\left[\psi_{1,2}\right] = \begin{bmatrix} e^{i\psi_2} & 0 \\ 0 & e^{i\psi_1} \end{bmatrix}, \quad \text{(A3)}$$

$$\left[\varphi_{1,2}\right] = \begin{bmatrix} e^{i\varphi_2} & 0 \\ 0 & e^{i\varphi_1} \end{bmatrix}. \quad \text{(A4)}$$

For the round-trip MZI in Fig. 1, equation (A1) satisfies unitary transformation if $\psi_1 + \varphi_2 = \psi_2 + \varphi_1$ is satisfied:

$$\begin{bmatrix} E_9 \\ E_{10} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -\{e^{i(\psi_1+\varphi_2)} + e^{i(\psi_1+\varphi_2)}\} & i\{e^{i(\psi_1+\varphi_2)} - e^{i(\psi_1+\varphi_2)}\} \\ i\{e^{i(\psi_1+\varphi_2)} - e^{i(\psi_1+\varphi_2)}\} & -\{e^{i(\psi_1+\varphi_2)} + e^{i(\psi_1+\varphi_2)}\} \end{bmatrix} \begin{bmatrix} E_1 \\ 0 \end{bmatrix},$$

$$= -e^{i(\psi_1+\varphi_2)} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} E_1 \\ 0 \end{bmatrix}. \quad \text{(A5)}$$

Owing to the unitary transformation in equation (A1), deterministic key distribution is confirmed, where eavesdropping is random due to MZI superposition.

Section B: Determinacy of NC-USCKD

(I) Identity relation:

From equation (A5), $E_9 = \mathrm{c}E_1$ and $E_{10} = 0$ result in for the identity matrix of [BH], where c is a global phase factor. Because $\varphi_1, \psi_1 \in \{0, \pi\}$ and $\varphi_1 = \psi_1$ for the identity relation in USCKD (see ref. 21), the following relation is achieved for the address phase:

$$\psi_2 = \varphi_2. \quad \text{(B1)}$$

Unlike phase bases ψ_1 and φ_1 having two discrete orthogonal bases of 0 and π, equation (B1) has no restriction. Thus, the values of ψ_2 and φ_2 are continuous: $0 \le (\psi_2, \varphi_2) \le \pi$. With the phase-shifted controls of ψ_2 and φ_2 working for the addressable networking in NC-USCKD, the condition of $\varphi_1 = \psi_1$ is also required for the MZI directionality (see Fig. 2).

(II) Inversion relation:

To satisfy the inversion relation ($E_9 = 0$ and $E_{10} = \mathrm{c}' E_1$) in equation (A1), the exponent of each matrix element in [BH] must be $(\psi_2 + \varphi_1) = (\psi_1 + \varphi_2) \pm \pi$:

$$\begin{bmatrix} E_9 \\ E_{10} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} -\{e^{i(\psi_1+\varphi_2)} - e^{i(\psi_1+\varphi_2)}\} & i\{e^{i(\psi_1+\varphi_2)} + e^{i(\psi_1+\varphi_2)}\} \\ i\{e^{i(\psi_1+\varphi_2)} + e^{i(\psi_1+\varphi_2)}\} & -\{e^{i(\psi_1+\varphi_2)} - e^{i(\psi_1+\varphi_2)}\} \end{bmatrix}\begin{bmatrix} E_1 \\ 0 \end{bmatrix},$$

$$= \pm i e^{i(\psi_1+\varphi_2)} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} E_1 \\ 0 \end{bmatrix}. \quad \text{(B2)}$$

Because $\varphi_1, \psi_1 \in \{0, \pi\}$ and $\varphi_1 = \psi_1 \pm \pi$ are for the condition of inversion matrix in USCKD (see Fig. 3), the following relation is required:

$$\psi_2 = \varphi_2. \quad \text{(B4)}$$

Therefore, the same address phase relation obtained in equations (B1) and (B4) is universal for NC-USCC whether it is for the identity or inversion matrix in the unitary transformation. For the key distribution process as shown in Table 2 for Fig. 1 in the main text, Alice randomly selects her phase basis ψ_1 to be either identical or opposite to the Bob's choice. If Alice's phase choice is for identical (opposite), $\psi_1 = \varphi_1$ ($\psi_1 = \varphi_1 \pm \pi$), it results in the identity (inversion) relation of equation (A5) regardless of the address set if $\psi_2 = \varphi_2$ is satisfied. As a result, any value of the address set (φ_2, ψ_2) fulfills the unitary transformation in Fig. 1 satisfying NC-USCKD for the unconditional security due to deterministic randomness, resulting in infinite number of addresses. This confirms that the addressable networking of NC-USCKD with continuous phase basis or addressing.

Section C:

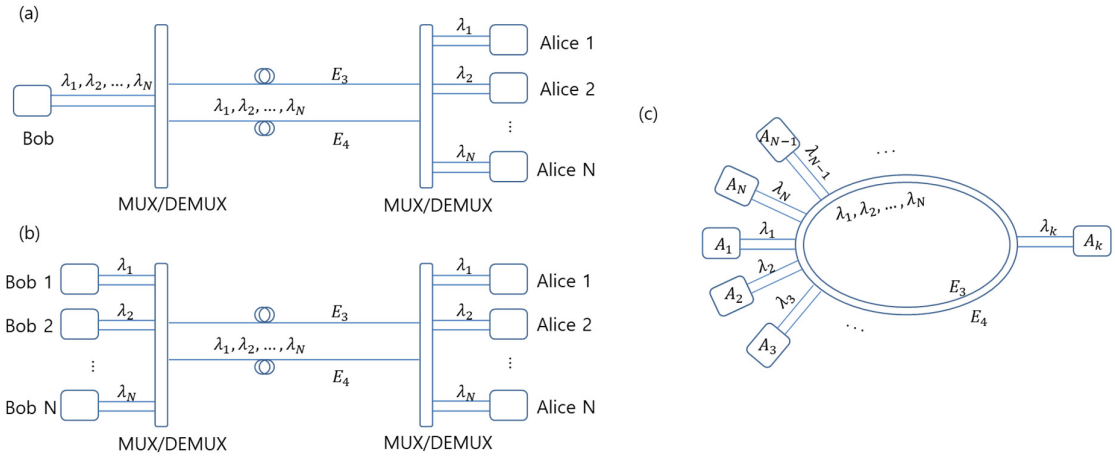

FIG. C1. Schematics of (a) 1xN, (b) NxN, and (c) ring configuration for NA-USCKD. The λ_i corresponds to φ_2^i and ψ_2^i. IN (c), each party is attached by ADD/DROP multiplexer.

Figure C1 shows potential network configurations of the addressable NC-USCKD, where the control phase φ_2 in Fig. 3 is assigned to the wavelength λ in the DWDM networks.

Section D: Channel measurement randomness

The matrix representation for the ψ_1 −controlled return light by Alice is denoted by (see equation (5) in the main text):

$$\begin{bmatrix} E_7 \\ E_8 \end{bmatrix} = \frac{1}{2\sqrt{2}}[\psi_{1,2}][BS][BS][\varphi_{1,2}][BS]\begin{bmatrix} E_1 \\ 0 \end{bmatrix}$$

$$= \frac{1}{2\sqrt{2}}\begin{bmatrix} e^{i\psi_2} & 0 \\ 0 & e^{i\psi_1} \end{bmatrix}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}\begin{bmatrix} e^{i\varphi_2} & 0 \\ 0 & e^{i\varphi_1} \end{bmatrix}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}\begin{bmatrix} E_1 \\ 0 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix} -e^{i(\psi_2+\varphi_1)} & ie^{i(\psi_2+\varphi_1)} \\ ie^{i(\psi_1+\varphi_2)} & -e^{i(\psi_1+\varphi_2)} \end{bmatrix}\begin{bmatrix} E_1 \\ 0 \end{bmatrix}. \quad \text{(D1)}$$

According to identity conditions in Appendices A and B, equation (D1) results in $|E_7| = |E_8|$, representing measurement indistinguishability in the channels by Eve (see Fig. 4). The background of this complete randomness is in the MZI path superposition corresponding to the no-cloning theorem in QKD.

Section E: Unconditional security of NC-USCKD

Table E1 shows a key distribution procedure using identity relation only for the present NC-USCKD. The technical difference between Table 2 and Table E1 is in the key distribution strategy whether bit-by-bit network initialization is used or bit-by-bit sifting is used, resulting in only different bit rate for the key generation. As discussed with identity relation in USCKD [21], any inverted key is discarded but used for network monitoring: see the bold X in Table E1. In the present NC-USCKD using two phase bases, the key generation rate is less than 50%. Before the key distribution in Table E1, a network initialization step is necessary for authentication between two addressees assigned by φ_2 and ψ_2. The key distribution procedure is as follows:

1. Bob randomly selects his phase basis $\varphi_1 \in \{0, \pi\}$ to prepare a key and sends it to Alice.
2. Bob converts the chosen basis φ_1 into a key record: x∈ {0,1}; if $\varphi_1 = 0$, x=0; if $\varphi_1 = \pi$, x=1.
3. Alice measures her visibility V_A and keeps the record.
4. Alice copies the Bob's key for her record y: if V_A=1, y=0; if V_A=−1, y=1; if $V_A \neq \pm 1$, y=V_A (error).
5. Alice randomly selects her phase basis $\psi_1 \in \{0, \pi\}$, encode the return light, and sends it back to Bob.
6. Alice converts the chosen basis ψ_1 into the key record z: z ∈ {0,1}; if $\psi_1 = 0$, z=0; if $\psi_1 = \pi$, z=1.
7. Alice compares y and z for the raw key m_A: $m_A = (y + z)$ at modulus 2. If $m_A \neq 0$, discard it, otherwise $m_A = z$.
8. Bob measure his visibility V_B.
9. Bob converts V_B into his raw key m_B. If $V_B = -1$, $m_B = x$, otherwise discard it.
10. Alice and Bob publically announce their error bits and discard them from their raw key list to set a final key, m.

Table E1. A key distribution procedure for unconditional security. The phase φ_1 is denoted without addition of φ_2. The mark 'X' indicates a discarded bit due to unsatisfied identity relation. The red 'X' indicates error corrections. Privacy amplification is not shown.

Party	Order / Sequence		1	2	3	4	5	6	7	8	9	10	set
Bob	1	φ_1	0	0	π	0	π	π	0	π	0	0	
	2	Prepared key: $x(\varphi_1)$	0	0	1	0	1	1	0	1	0	0	$\{x\}$
	8	V_B	1	−1	0.9	1	−1	−1	−1	1	1	−1	
	9	raw key	**X**	**0**	**X**	**X**	**1**	**1**	**0**	**X**	**X**	**0**	$\{m_B\}$
	10	Final key	**X**	**0**	**X**	**X**	**1**	**X**	**0**	**X**	**X**	**0**	$\{m\}$
Alice	3	V_A	1	1	−1	1	−1	−0.8	1	−1	1	−1	
	4	Copy x: y	0	0	1	0	1	−0.8	0	1	0	0	$\{y\}$
	5	ψ_1	π	0	0	π	π	π	0	0	π	0	
	6	$z(\psi_1)$	1	0	0	1	1	1	0	0	1	0	$\{z\}$
	7	raw key	**X**	**0**	**X**	**X**	**1**	**X**	**0**	**X**	**X**	**0**	$\{m_A\}$
	10	Final key	**X**	**0**	**X**	**X**	**1**	**X**	**0**	**X**	**X**	**0**	$\{m\}$

Section F:

For a given n-bit long key whose basis is binary, the maximum number of representation is 2^n. For n=128, the total number of representation is $2^{128} = 3.4\text{x}10^{38}$. Recalling the universe age is 1.38×10^{10} years or 4.35×10^{17} seconds, the eavesdropping chance for the 128-bit long key by using the most powerful supercomputer (IBM Summit) whose performance is 1.43×10^{17} flops/s is as follows:

$$\eta = \frac{6.2\times10^{34}}{3.4\times10^{38}} = 1.8 \times 10^{-4}, \qquad \text{(F1)}$$

where 6.2×10^{34} is from the universe age $(1.43 \times 10^{17})(4.35 \times 10^{17})$. The eavesdropping rate in equation (F1) results in unconditional security based on perfect randomness of MZI path superposition. Even with a personal computer whose operating system is 64-bit based, the brute force attack for the randomness in USCC takes more than 100 seconds: $2^{64} = 1.8 \times 10^{19}$. This means that the proposed NC-USCC is effective even with personal computers for the applications of the one-time-pad cryptography, where the key never be reused and the key distribution speed can be close to the optoelectronics speed or CPU speed at ~GHz. The flight time Δt of a light pulse for a 10 km optical fiber is as follows:

$$\Delta t = \text{n}\frac{1\times10^4}{3\times10^8} = 5 \times 10^{-5} \text{ (s)},$$

where n is the refractive index of the optical fiber, n~1.5. In the round-trip MZI scheme of Fig. 1 may limit its operational bandwidth if the bit-by-bit network initialization is used at less than MHz for each channel. Needless to say, this channel-bandwidth bottleneck can also be solved by multi-channel configuration such as in current fiber-optic communications networks.