2019년 동계 UST 연구인턴십 최종보고서

고전광을 이용한 유사 GHZ 상태의 생성

The Generation of Three-photon GHZ-like state with Classical Light

캠퍼스(스쿨) : 한국과학기술연구원 양자정보단

지도교수 : 김 용 수

인턴 : 신 윤 정

제출일: 2019년 2월 25일

목 차

요약(Abstract)

Quantum information built upon the concept of quantum bit (or qubit) deals with the information processing tasks based on the laws of quantum mechanics. Its specialty especially stands out in quantum communication (QC) where Quantum key distribution (QKD) protocol allows participants to generate a common string of secret bits in the presence of an eavesdropper. Although most of QKD protocols have suggested based on ideal photon sources, pseudo-single-photon sources such as weak coherent laser pulses are more favorably used in real QC for practical reason. Despite its random nature in the photon number distribution, laser pulses can act almost like photons on some conditions. The quantum-ness criteria is still so ambiguous that it needs to be clear. Defining more clear boundary will allow us to evaluate the power of classical light and use it more wisely for QC. Bell state measurement (BSM) is a projective measurement onto Bell states and plays crucial roles in many photonic quantum processing application. To resolve the dilemma of original BSM schemes, an informationally symmetric BSM scheme was proposed recently. Inspired by this research, a three-photon GHZ state generator was developed and genuine GHZ state was produced with entangled photon pairs. However, given practicality, it is worth to conduct the GHZ state generation experiment with classical lights, which is exactly what we did in this research. We generate a GHZ-like state with the use of unsynchronous AOMs and a GHZ state generator. Then we analyze an output state theoretically and experimentally. We find that experimental data from QST, that is density matrices, are compatible with theoretical ones. The generation of a GHZ-like state with classical light turns out successful. Even though they are not perfect GHZ states with additional diagonal terms in its density matrix, these imperfection can be dealt with by outstanding advantages of MDI-QKD. When applied to MDI-QKD, the GHZ-like state is expected to be used in many kind of practical multiparty quantum communication.

Ⅰ. 서론

Quantum information built upon the concept of quantum bit (or qubit) deals with the information processing tasks based on the laws of quantum mechanics. Quantum mechanical approach allows us to perform not only faster operations but also operations inaccessible to classical means.[1] Its specialty especially stands out in quantum communication where Quantum key distribution (QKD) protocol allows participants to generate a common string of secret bits in the presence of an eavesdropper.[2] Although most of QKD protocols have suggested based on ideal photon sources, pseudo-single-photon sources such as weak coherent laser pulses are more favorably used in real quantum communication for practical reason. Despite its random nature in the photon number distribution, laser pulses can act almost like photons on some conditions. The quantum-ness criteria is still so ambiguous that it needs to be clear. Defining more clear boundary between quantum and classic would allow us to evaluate the power of classical light for quantum communication and use it more wisely. Bell state measurement (BSM) is a projective measurement onto Bell states and plays crucial roles in many photonic quantum processing application. However, the original BSMs cannnot simultaneously achieve symmetric and secure distribution of information. To resolve the dilemma, an informationally symmetric BSM scheme was proposed recently. One of its strengths is that it can be generalized to N-photon cases, which allows preparation and analysis of GHZ states.[3] GHZ state refers to the maximally entangled multi-photon state considered as a promising resource to carry quantum information.[3] Inspired by this research, a three-photon GHZ state generator was developed and genuine GHZ state was produced with entangled photon pairs. However, given practicality, it is worth to conduct the GHZ state generation experiment with classical lights. Even though perfect GHZ states cannot be generated from laser pulses due to its nature, we can make GHZ-like state and any imperfections can be readily taken care of by measurement-device-independent (MDI) QKD.[4-5] The GHZ-like state is expected to be practically used in many kind of multiparty quantum communication.

In first half of this report, I try to give detailed information about motivations of this research : the ambiguous quantum-ness criteria, informationally symmetric BSM, and MDI quantum communication. Then I thoroughly describe the research procedure : how to make three phase-incoherent laser pulses with unsynchronous AOMs, theoretical calculations through which the exact output

states of a GHZ state generator can be predicted, and experimental results on HOM dips and quantum state tomography (QST).

Ⅱ. 본론

1. Motivations

1). Ambiguous Quantum-ness criteria

When two identical photons enter into a beam splitter (BS) at the same time, the coincidence counts between two detectors are completely suppressed, see Fig. 1. This phenomenon is represented as a dip shaped curve in the graph of the number of coincidence counts according to the optical path difference between two lights. A so-called Hong-Ou-Mandel (HOM) dip results from two-photon quantum interference. Interestingly, this kind of interference also happens with classical lights when they are especially phase-incoherent to each other. Visibility V, the important parameter that describes a dip, is defined as the relative depth of the dip compared to the noninterfering case. It can reach up to V = 1 for photons[Fig. 1(a)], but there's the classical limit V = 0.5 for classical light[Fig. 1(b)].[6-7]

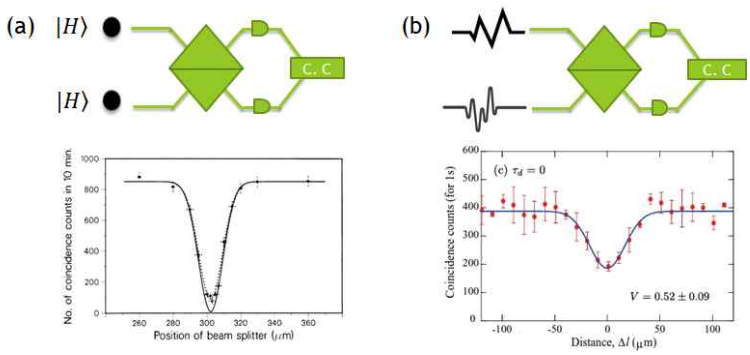

Fig. 1. Bell state measurement (BSM) scheme and a HOM dip (a) for two identical photons and (b) for phase-incoherent laser pulses

If we change the polarizations of the incoming photons orthogonal to each other, the interference will not occur anymore because they are now distinguishable. That is, the HOM dip disappears. However, in this case, we can get Bell states which are maximally entangled two-qubit states by post-selecting the case where there is one photon at each output, see Fig. 2(a). When it comes to classical light, we can classify the interference according to the existence of mutual coherence. If they're mutually coherent, the output states will not have any quantum relation, see Fig. 2(b).. In contrast, if they're incoherent, they will have a certain kind of quantum correlation that can be represented by quantum

discord as shown in Fig. 2(c). Quantum discord is a broader concept than entanglement. It allows us to describe the quantum correlation of states more specifically.[8]

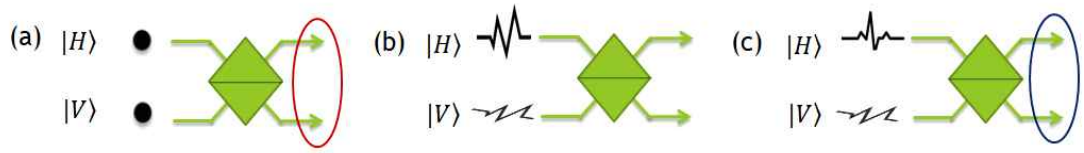

Fig. 2. BSM scheme for the light sources with orthogonal polarizations. (a) when it comes to photons, the post-selective measurement can yield Bell states, the maximally entangled two-qubit states. (b) For mutually coherent laser pulses, the output states have no quantum correlation. (c) For mutually incoherent laser pulses, the output states have a certain kind of relation which can be described by quantum discord.

Actually, the difference between photon and classical light is just in their photon number distributions. There is literally one grain of light for photon, while the number of photons in classical light follows Poissonian distribution. The probability $P(n)$ for observing n photons in classical light per pulse is given by

$$P(\mu,n)=\frac{\mu^n}{n!}e^{-\mu} \tag{1}$$

where μ is the average photon number per pulse. Classical lights can be classified according to their relative magnitudes of the standard deviation to that of Poissonian such as Super-Poissonian ($\sigma>\sqrt{n}$), Poissonian ($\sigma=\sqrt{n}$), and Sub-Poissonian ($\sigma<\sqrt{n}$). Perfectly coherent light like laser has Poissonian photon statistics.[9]

Photons and laser pulses have different nature, but they can act the almost same way on some conditions. The quantum mechanical-classical criteria is so ambiguous that it needs to be clear. In most of quantum key distribution processes, pseudo-single-photon sources such as weak coherent pulses (WCPs) are more favorably used rather than real photons for practical reason. They are laser pulses attenuated down to the extent that the mean number of photons per pulse μ is smaller than 1 (usually $\mu=0.1$).[4-5,9] Defining much more clear boundary between quantum and classic would allow us to evaluate the power of classical light for quantum communication and use them more wisely.

2). Informationally Symmetric BSM [3]

The standard linear optical bell state measurement (BSM) is a projective measurement onto Bell states and plays crucial roles in many photonic quantum

processing application processes. we can think BSM as sharing information. The standard BSM is based on HOM interference where two photons meet simultaneously and interfere with each other at a BS. However, it is proven that both classical and quantum two-photon interference are caused by the interference between probability amplitudes, rather than photons.[7.10-11] In other words, temporal overlapping between optical pulses is not required for interference. Based on the fact, a new BSM scheme without BS was proposed recently.

Let us suppose that each participant Alice (A) and Bob (B) has a single photon. Fig. 3 shows the standard linear optical BSM schemes for polarization qubits. The incoming photons from A and B meet at a BS, and HOM interference occurs. It is often to scan the optical delay of one of the photons in order to overlap two photons at a BS. Then, the photons are split by each polarization beam splitters (PBS) and detected by single-photon detectors (D1 - D4). Fig. 3(a) is a scheme for an original entanglement-based BSM. If they want to perform BSM using their own photons, A locally generates an entangled photon pair and distributes one of them to B. In this case, A has much more information than B as she has full control of generating entangled photon pairs, and this asymmetric information-sharing-process can cause conflict between participants.[9] Fig. 3(b) shows the other scheme that induces entanglement between outputs by measurement and post-selection. Unlike Fig. 3(a), it can become informationally symmetric by employing a third party C. He is going to perform BSM with the states from A and B and send the results back to them. However, here occurs another critical problem that we never know whether the third party is trustworthy or not.

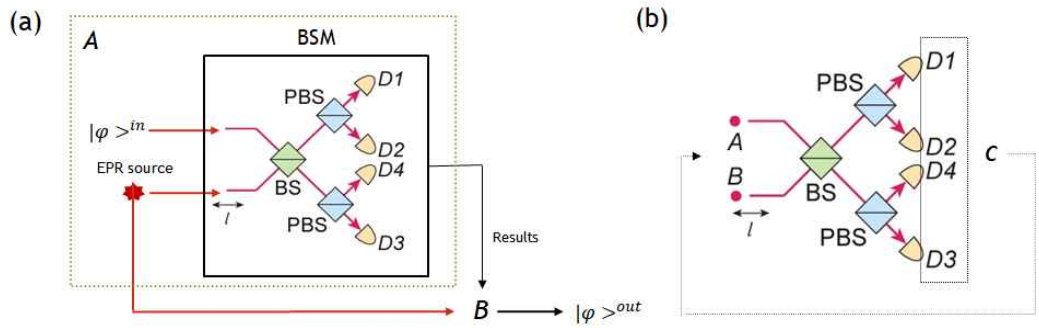

Fig. 3. Original BSM schemes. (a) Entanglement-based BSM. This informationally asymmetric scheme can cause conflict between participants. (b) Entanglement-inducing BSM. A third party is employed to make the scheme informationally symmetric, but he can cause a security problem

On the other hand, in the new BSM scheme in Fig. 4(a), participants can conduct measurement themselves in tandem without any suspicious third party. The probability amplitudes of |H> and |V> of photons A and B are divided by PBS1. While A and B keep the probability amplitudes of |H>, they exchange the probability amplitudes of |V>. After half waveplates (HWP, H1) at 45°, the probability amplitudes interfere at PBS2. Finally, the photons are detected by the four detectors after passing through HWP at 22.5°(H2) and PBS3. similar to the standard one, the optical delay l of one of the photons should be scanned in order to allow interference. By exchanging the probability amplitudes, it remarkably solves the security problem and ensures the remote communication. Given these advantages, the symmetric scheme seem to outperform the original one when applied to measurement-device-independent (MDI) quantum communication, Also, Fig. 4(b) shows that this symmetric scheme can be generalized to arbitrary number of N-photons. Just by adding it in parallel, we can prepare and analyze N-photon Greenberger-Horne-Zeilinger (GHZ) states. They are originally introduced to reveal the extreme violation of local realism aganist quantum mechanics like Bell states. In quantum communication, they draw lots of attention as promising resources carrying quantum information due to its quantum correlation. GHZ state refers to the maximally entangled multi-photon state where all the qubits are at |0> or |1>.[12]

$$|GHZ_N^{\pm} \geqq \frac{1}{\sqrt{2}}(|0>^{\otimes N} \pm |1>^{\otimes N}) \tag{2}$$

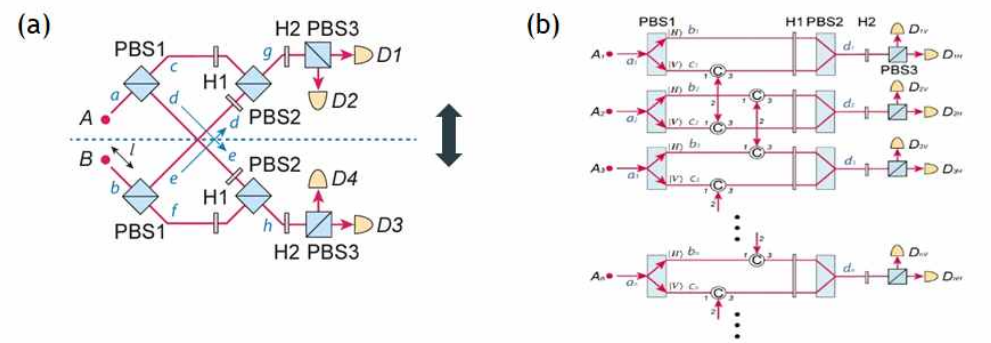

Fig. 4. (a) Informationally symmetric BSM scheme without a third party (b) It can be generalized to multiple photon GHZ states just by adding it in parallel.

3). MDI Qunatum Communication

Quantum key distribution (QKD) allows participants to generate a common string of secret bits, called a secret key, in the presence of an eavesdropper.[2] This key can be used for tasks such as secure communication. QKD protocols guarantee unconditional security based on the laws of quantum mechanics,

which outperform their classical counterparts. However, actual implementations is unfortunately not as ideal as it was thought to be. To bridge the gap between theory and practice, several solutions have been proposed so far. Among them, we consider measurement-device-independent QKD (MDI-QKD) the most promising for applying our GHZ-like states generated from classical light. As the name suggest, MDI technic does not require complete detection and knowledge of how devices work. It is also able to get more immune to side attacks when combined with the decoy state technic and entanglement purification. Decoy states refer to additionally prepared states aside from key states only for detecting eavesdropping attacks.[13] Purification is a method for distilling a certain kind of pure states (sometimes called 'cat' states) from mixed states.[14] In contrast to the standard protocol where entangled states generated by spontaneous parametric down conversion (SPDC) of nonlinear crystal are used, entanglement is induced by post-selective BSM in MDI protocol. Even with conventional laser sources, it ensures long distance key distribution that is almost comparable to the standard one with entangled photon pairs, see Fig. 5(b).[4-5]

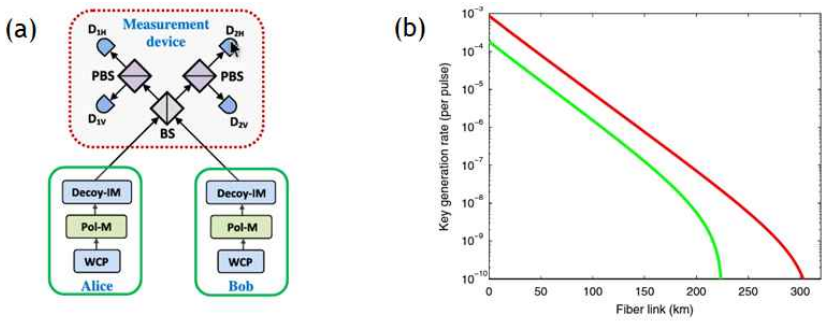

Fig. 5. (a) Basic setup for a MDI-QKD protoco. (b) Key generation rate according to communication distance(fiber link). The green curve corresponds with a standard QKD using entangled photons and red one with a MDI-QKD using lasers.

GHZ state is an important resource for Multiparty quantum communication (QC). Many practical applications such as quantum cryptographic conferencing (QCC) and quantum secret sharing (QSS) have been proposed so far. However, they are quite limited due to many constraints such as the lack of high intensity source and reliable scheme for remote distribution of the GHZ states. The primary purpose of QCC and QSS is to share almost perfect GHZ states, and MDI-QKD can be a promising foundation for them.

QCC can be employed when A would like to broadcast a message securely only to B and C, in the presence of an eavesdropper, E. One way to achieve it is that all the participants share a common conference key first, then A use the

key as a one-time-pad for encrypting her message (0404133). If three members of a GHZ state are measured along Z basis, each of them will give a random outcome, Z_A, Z_B, and Z_C in perfect correlations $Z_A=Z_B=Z_C$, which can be used for QCC.

QSS is a protocol of splitting a message into several parts among a group of participants, see Fig 6(b). Recovering the key is possible only if all the key are combined. The goal of QSS is to ensure that E cannot learn about the secrets even when he steals some, and to prevent a part of participants from occupying the whole secret and making important decision arbitrary. When three members of a GHZ state are measured along X basis, they begin to share a binary correlation $X_A \oplus X_B \oplus X_C=0$. Suppose a president A would like to divide up a secret bit a between two vice presidents B and C. Assume A has a broadcast channel and broadcasts $b=a \oplus X_A$. Note that if B and C get together, they can compute $X_B \oplus X_C$ and thus, $b \oplus X_B \oplus X_C=a \oplus X_A \oplus X_B \oplus X_C=a$. Therefore, Bob and Charles can recover the secret a, if they come together. However, neither Bob or Charles on his own has any information at all about the bit. In this way, they can achieve sharing of classical secrets.[5,15]

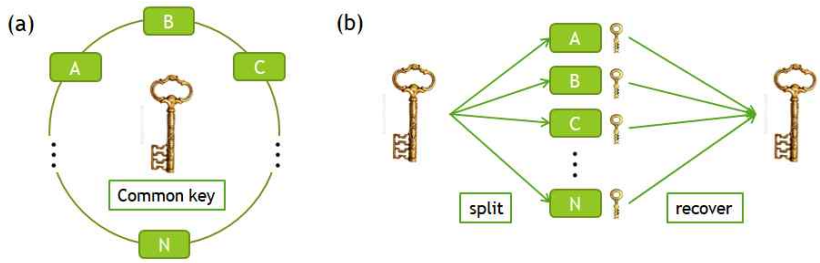

Fig. 6. (a) Quantum cryptographic conference (QCC) (b) Quantum secret sharing (QSS)

2. Research

1). Three phase-incoherent Laser Pulses

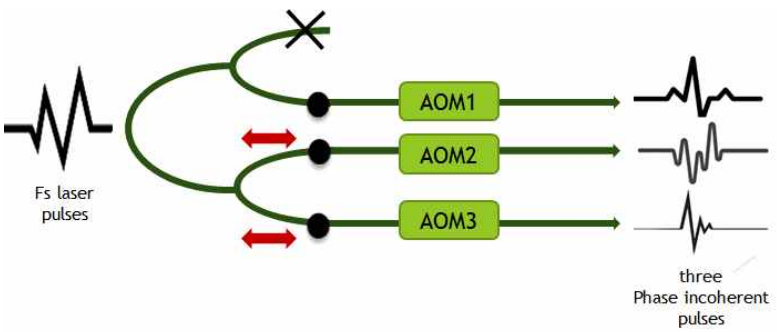

Fig. 7. Scheme for making three phase-incoherent pulses. We split fs laser pulses into the four and discard one. Each lights then go through independent AOMs, turning to be phase-incoherent to one another.

Femto-second laser pulses with the central wavelength of 780nm are used for the experiment. The intensity attenuator is introduced to reduce the average photon number per pulse and 1nm bandwidth filter to increase the visibility of HOM dips. A fiber beam splitter (FBS) splits the incoming pulses into two paths first, then following two FBSs split each pulse into another two again. In this way, we get four splitted lights, but we only use three of them to get 3-photon entangled states. This kind of light-splitting process is not actually required in real QKD where all the participants are supposed to generate their own state from independent lasers. Since some proof of principle experiment showed that a high-visibility HOM interference between two independent classical lights is feasible(130503), we divided a laser to guarantee interference between splitted lights for simplifying our experiment. Then each splitted pulse goes through asynchronous acousto-optical modulators (AOM1, AOM2, and AOM3). We block out except the 1st order diffracted pulses with irises and they are collected by corresponding single-mode optical fibers.

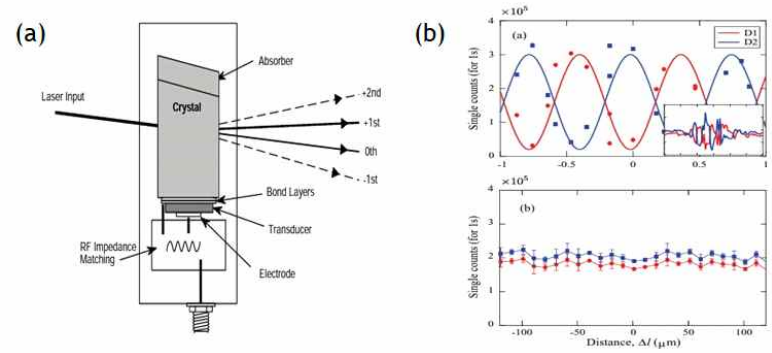

Fig. 8. (a) Schematic design for AOM and its working principle (b) unsynchronous AOMs can wash out first order interference between lights. Interference fringes disappear after employing AOMs (from above to below).

AOM is a kind of diffraction grating that uses the acousto-optic effect to diffract light and shift the frequency of light using sound waves usually at radio-frequency. Fig. 8(a) shows its working principle. A piezoelectric transducer is attached to a material such as glass. An external oscillating electric signal drives the transducer to vibrate, which creates sound waves in the material. These can be thought of as moving periodic planes with expansion and compression that change the index of refraction. Incoming light scatters off the resulting periodic index modulation and interference occurs like kind of Bragg diffraction. A diffracted beam emerges at an angle θ which depends on the wavelength of the light λ relative to the wavelength of the sound Λ and the

order of diffraction $m = 0, \ \pm 1 \ \pm 2 \ \ldots$.

$$2\Lambda \sin\theta = m\lambda \tag{3}$$

AOM can change many properties of the light such as intensity, frequency, phase, etc. In this experiments, they are especially employed to wash out the 1st order coherence. The phase of the diffracted light is shifted by the amount of the phase of the sound wave. That is, the lights become phase-incoherent to one another after getting out of unsynchronous AOMs. The operating RF frequencies of all the AOM drivers are set to be slightly different to one another like 49, 50, and 51MHz.[7,16-17]

2). GHZ State Generator

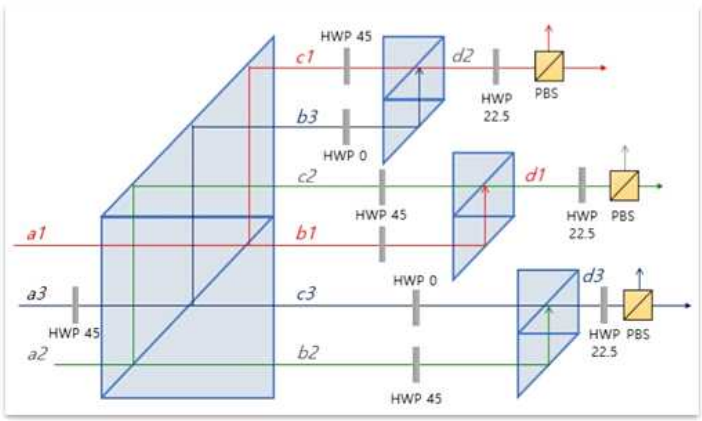

Fig. 9. Scheme for a GHZ state generator. The output state would be GHZ-like state due to third order interference in the interferometer.

The phase-randomized lights now go into a GHZ state generator. The output states would be kind of GHZ state due to the 3rd order interference in the interferometer. The exact output states can be predicted by theoretical calculations. When the lights coming in input modes of the interferometer are mutually incoherent to one another, we can deal with the input states separately according to the incident photon numbers at each input mode. We'll post-select only the case where one photon emerges at each output mode so that entanglement can be induced by measurement. Thus we should consider only seven cases: $|\Psi>_{(111)}$, $|\Psi>_{(210)}$, $|\Psi>_{(201)}$, $|\Psi>_{(120)}$, $|\Psi>_{(021)}$, $|\Psi>_{(102)}$, and $|\Psi>_{(012)}$ except that all the three photons come to the same input mode. The output state will be the statistical mixture of the output states from the seven input states and we set all the polarization states of them |DDD>.

First, we need to calculate the density matrix $\rho^{(ijk)}$ of the post-selected output

for each case. For example, for the calculation of the input state where one photon comes in each input mode $|\Psi>_{(111)}^{i.n} = a_{D1}^{\dagger}a_{D2}^{\dagger}a_{D3}^{\dagger}|0>|0>|0>$, we should consider the action of PBS and the unitary transformation of the BS that can be written as

$$\begin{pmatrix} a^{\dagger} \\ b^{\dagger} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} c^{\dagger} \\ d^{\dagger} \end{pmatrix} \tag{4}$$

where $a^{\dagger}$ and $b^{\dagger}$ denote creation operators at the input modes of BS, $c^{\dagger}$ and $d^{\dagger}$ are those for the output modes of BS. After considering post selection, we can get the output state written as

$$|\Psi>_{111} = -\frac{|HHH> + |VVV>}{2\sqrt{2}} \tag{5}$$

and its density matrix can be obtained by its own outer product as

$$\rho^{111} = |\Psi>_{111\ \ 111}<\Psi| = \begin{pmatrix} 1/8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/8 \end{pmatrix} \tag{6}$$

The expectation value on the number of counted photons after post-selection is

$$p_{111} = Tr(\rho^{111} n) = \frac{1}{4} \tag{7}$$

After normalization, the output state (5) and its density matrix (6) become

$$|\Psi>_{(111)} = -\frac{|HHH> + |VVV>}{\sqrt{2}} \tag{8}$$

$$\rho^{111} = |\Psi>_{(111)\ \ (111)}<\Psi| = \begin{pmatrix} 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 \end{pmatrix} \tag{9}$$

Density matrices of the other input states and expectation values considering post selection can be calculated the same way. All the expectation values are calculated as same as $\frac{1}{4}$ regardless of the configuration of the number of photons in input states. Finally, the overall state ρ is given as the statistical

mixture of seven density matrices.

$$\rho = \frac{p(111)\rho^{(111)} + p(210)\rho^{(210)} + p(201)\rho^{(201)} + p(120)\rho^{(120)} + p(021)\rho^{(021)} + p(102)\rho^{(102)} + p(012)\rho^{(012)}}{Tr[p(111)\rho^{(111)} + p(210)\rho^{(210)} + p(201)\rho^{(201)} + p(120)\rho^{(120)} + p(021)\rho^{(021)} + p(102)\rho^{(102)} + p(012)\rho^{(012)}]}$$

$$= \begin{pmatrix} 1/8 & 0 & 0 & 0 & 0 & 0 & 0 & 1/8 \\ 0 & 1/8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/8 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1/8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1/8 & 0 \\ 1/8 & 0 & 0 & 0 & 0 & 0 & 0 & 1/8 \end{pmatrix} \quad (10)$$

where $p(111) = P(\mu,1)^3/4$ and $p(210) = \cdots = p(012) = P(\mu,2)P(\mu,1)P(\mu,0)/4$ are the conditional probabilities that correspond to $\rho^{(111)}$, $\rho^{(210)}$, $\cdots$,and $\rho^{(012)}$respectively. The conditional probability $p(ijk)$ is the probability of occurring coincidence event when i, j, and k photons are incident on each input, given that $P(\mu,n)$ is the Poissonian distribution of the photon numbers (1) and the factor $\frac{1}{4}$ (7) comes from the expectation value on the number of counted photons after post selection.[8] Due to its nature, what we can get from classical light is just GHZ-like state, not actual GHZ state. However, this imperfection can be readily dealt with when the GHZ-like states are applied to MDI-QKD.

3). HOM Dips

Now that 1st order interferences are removed, we can see HOM dips from coincidence counts between three sets of the outputs. if we make their optical paths the same. To find out the exact positions where the 2nd order interferences take place, we fix the light source *a3* and scan the optical delays of the other sources a*1* and a*2* by using translation stages (Z825B, Thorlabs) and motor controllers (KST 101, Thorlabs), see Fig. 9. They can move backwards and forwards about one inch relative to the central position. Then avalanche-photodiode-based photon detectors (SPCM-AQRH-12-FC, Digi-key electronics) measure coincidence counts between any one of three sets of the outputs. We make the polarization of the incident state |DDA> with the use of PBS and HWP (not shown in the figure), and rotate all the HWPs in front of PBSs 22.5 degrees relative to its offset angle.

First, after blocking *a1*, we scan the optical delay of *a2* and find the dip due to the 2nd order interference between *a2* and *a3*. we use Mathematica, the technical computing software, to plot the data and find out the position where the extreme value of coincidence counts appears and the visibility of the dip. The

interference maximally takes place when *a2* is located at 4.690 um, and we fixed it there, see Fig. 10(a). The visibility of the dip is 46.8 % which is pretty close to the classical limit V = 0.5. Next, under the condition that all the lights that are shown in the Fig. 9 exist, we scan the optical delay of *a1*, and simultaneously find the two dips caused by the interaction between the two pairs, (*a1, a2*) and (*a1, a3*). Fig. 10(b) and (c) show that the dip positions are at 13.553 and 13.585 um, and their visibilities are 48.5 % and 47.3 %, respectively. The red vertical line in Fig. 10(d) represents the average value of them, 13.565 um and we fixed *a1* there like we did about *a2*.

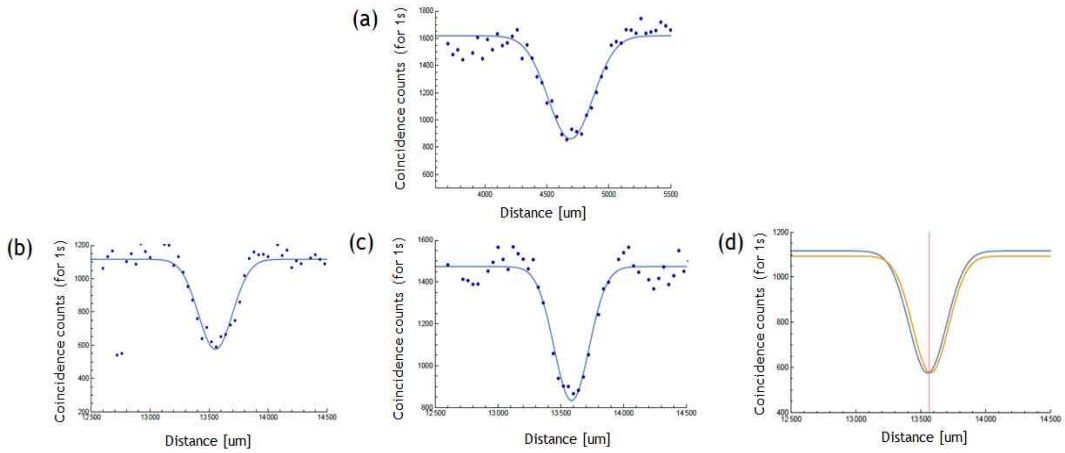

Fig. 10. HOM dips for interference between the sources (a) *a2* and *a3* (b) *a1* and *a2* (c) *a1* and *a3*. (b) and (c) were taken simultaneously by moving the position of a1. Two dip positions from (b) and (c) allow us to calculate the average location of *a1* (the red vertical line)

5) Quantum State Tomography

After adjusting the photon counts of the six output compatible to one another, we perform quantum state tomography (QST). QST is an experimental procedure for determination of the density matrix associated with a quantum system. It can be accomplished by successive measurements on repeated identical preparations of the same system, because we are not able to know the exact state of the system with few measurements.[18-19]

The density matrix has all the achievable information on a quantum system. From the density matrix obtained by QST, we can calculate Fidelity and Purity, the two basic quantities which describe a quantum state. Fidelity is a measure of the closeness of two quantum state, the theoretical and experimental states in the case of this research. It is bounded by $0 \leq F \leq 1$ and $F=0$ if ρ_1 and ρ_2 are orthogonal, while $F=1$ if they are equal. The definition of fidelity is [1]

$$F(\rho_1,\rho_2) = Tr[\sqrt{\sqrt{\rho_1}\,\rho_2\sqrt{\rho_1}}]^2 \tag{11}$$

On the other hand, purity gives the information on how much a state is mixed, bounded by $\frac{1}{d} \le P \le 1$ for a normalized quantum state where d is the dimension of the Hilbert space upon which the state is defined. The lower bound is obtain by a completely mixed state, a statistical ensemble of pure states, while the upper one by a pure state. A pure state is getting mixed, i.e. Purity decreases, when a composite quantum system gets an entangled state on it. Purity is defined as [20]

$$P = Tr(\rho^2) \tag{12}$$

We conducted QSTs as changing the position of the light sources or the polarization of input states. QSTs with input state |DDA> were conducted at about the four different positions shown in Fig. 11 to check the effect of interference between input states.

In contrast, QSTs with input state |VVH> and |HHV> were performed only at the wing position because, in these cases, the interference does not take place regardless of the position of the light source. To prevent possible confusion, note that input state |DDA>, |VVH>, and |HHV> change to DDD>, |HHH>, and |VVV> at the end of the interferometer as they go through several HWPs.

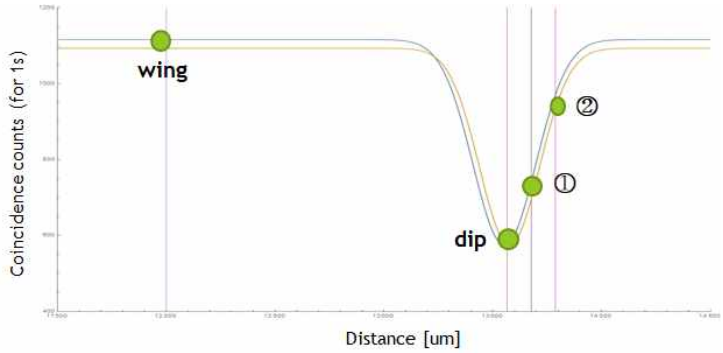

Fig 11. Positions of the source *a1* where the QSTs with input state |DDA> were taken. The source *a2* was located at its dip position 4.69 um for dip, ①, and ② of *a1* and at its wing position 4.3 um for wing of *a1*

	ρ_{dip}		$\rho_{①}$	$\rho_{②}$	ρ_{wing}	
	Theory	Experiment	Experiment	Experiment	Theory	Experiment
Fidelity	0.250	0.216	0.192	0.176	0.125	0.124
Purity	0.156	0.150	0.146	0.135	0.125	0.129
Off-diagonal		0.094	0.077	0.051		0.002

Table. 1. Characteristics of the theoretical and experimental density matrices at four different locations.

Table. 1 shows the physical quantities taken at the four sets of different positions of the sources. The experimental values of fidelity and purity are nearly similar to their corresponding theoretical ones with the error rate 13.6% for the dip and 0.8% for the wing. High fidelity and purity at the dip position verify that the output state is almost the same with the GHZ-like state as predicted. We can see the interference between input states gradually disappear as they are getting further from the dip given that the decrease of Fidelity, purity, and the magnitude of off-diagonal term. In other words, the output state is evidently generated by the interference and would have a certain of quantum correlation. This can be investigated by additional calculations of concurrence and discord from its the density matrix.

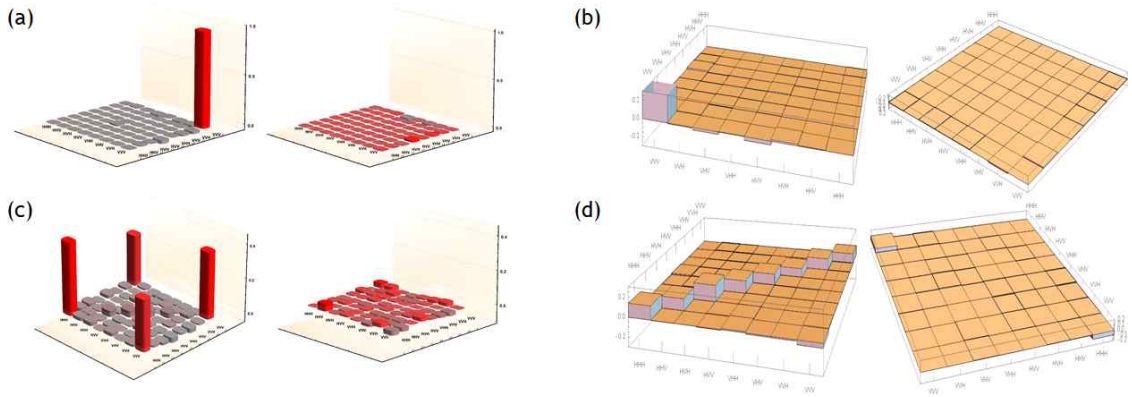

Fig. 12. Comparison on experimentally obtained density matrices for photons [(a), (c)] and laser pulses [(b), (d)]. The figures in fist row are about input states of |VVV> each for (a) photons and (b) laser pulses. The figures in second row are about input states of |DDD> each for (c) photons and (d) laser pulses. The left and right figures denote the real and imaginary parts of the density matrix, respectively.

	|VVV>		|DDD>	
	laser pulse	photon	laser pulse	photon
Fidelity	0.216	0.496	0.126	0.69
Purity	0.150	0.954	0.150	0.53

Table. 2. Characteristics of the density matrices of laser pulses and photons with two different input state |VVV> and |DDD>.

With Fig. 12 and Table. 2, we can compare three-photon entagled states from laser pulses to that from photons. The resluts with photons were obtained by the previous study inspired by a paper on new BSM scheme. In both cases, the input state |VVV> passes through the interferometer, preserving their polarization due to the lack of interference. On the other hand, when the input state is |DDD>, state with some kind of quantum correlation emerges at output.

The results with photons Fig. 11(c) shows that the output state is the superposition of |HHH> and |VVV> in similar proportion. Also, its higher fidelity than the reference value 0.5 verifies the generation of real GHZ state. In contrast, the density matrix with laser pulses have additional diagonal terms except |HHH> and |VVV> as we predicted based on the quantum theory (11). The existence of diagonal terms would be considered as a noise when applied to quantum communication. However, this imperfections in preparation process can be readily taken care of in MDI-QKD.

Ⅲ. 결론

After going through some motivations of this research, the detailed explanations on how we generate GHZ-like states are described. First, we split a fs laser into three and make them phase-incoherent to one another with the use of unsynchronous AOMs. After getting out of AOMs, the lights go through a GHZ generator which is developed under the inspiration of the informationally symmetric BSM scheme. Then they turn to some kind of three-photon entangled state due to third order interference in the interferometer. We find the HOM dips to make sure of the absence of first order interference and to find out the exact positions where second order interferences take place. The exact states at the output modes of the GHZ state generator are be predicted theoretically. We find that experimental data from QST, that is density matrices, are compatible with theoretical ones. we generate GHZ-like state with classical light, as we expected. Even though they are not perfect GHZ states with additional diagonal terms in its density matrix, these imperfection can be dealt with by MDI-QKD. It has many outstanding advantages such as high security when combined with the decoy state technic and purification, the possibility for long distance key distribution, etc. When applied to MDI-QKD, the GHZ-like state is expected to be used in many kind of practical multiparty quantum communication.

참고문헌

[1] Sansoni, L., Integrated Devices for Quantum information with Polarization Encoded Qubits, Springer, 2014.

[2] N. Gisin et al., Rev. Mod. Phys. 74, 145 (2002); M. Dus˘ek, N. Lu¨tkenhaus, and M. Hendrych, in Progress in Optics, edited by E. Wolf (Elsevier, New York, 2006), Vol. 49, p. 381.

[3] Kim, Yong-Su, et al. "Informationally symmetrical Bell state preparation and measurement." Optics express 26.22 (2018): 29539-29549.

[4] Lo, Hoi-Kwong, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution." Physical review letters 108.13 (2012): 130503.

[5] Fu, Yao, et al. "Long-distance measurement-device-independent multiparty quantum communication." Physical review letters 114.9 (2015): 090501.

[6] Hong, Chong-Ki, Zhe-Yu Ou, and Leonard Mandel. "Measurement of subpicosecond time intervals between two photons by interference." Physical review letters 59.18 (1987): 2044.

[7] Kim, Yong-Su, et al. "Conditions for two-photon interference with coherent pulses." Physical Review A 87.6 (2013): 063843.

[8] Choi, Yujun, et al. "Generation of a non-zero discord bipartite state with classical second-order interference." Optics express 25.3 (2017): 2540-2551.

[9] Mark Fox, Quantum Optics, Oxford university press, 2006.

[10] Pittman, T. B., et al. "Can two-photon interference be considered the interference of two photons?." Physical Review Letters 77.10 (1996): 1917.

[11] Kim, Yoon-Ho, et al. "Quantum interference by two temporally distinguishable pulses." Physical Review A 60.1 (1999): R37.

[12] Erven, C., et al. "Experimental three-particle quantum nonlocality under strict locality conditions." arXiv preprint arXiv:1309.1379 (2013).

[13] Lo, Hoi-Kwong, Xiongfeng Ma, and Kai Chen. "Decoy state quantum key distribution." Physical review letters 94.23 (2005): 230504.

[14] Maneva, Elitza N., and John A. Smolin. "Improved two-party and multi-party purification protocols." CONTEMPORARY MATHEMATICS 305 (2002): 203-212.

[15] Chen, Kai, and Hoi-Kwong Lo. "Multi-partite quantum cryptographic protocols with noisy GHZ states." arXiv preprint quant-ph/0404133 (2004).

[16] "Acousto-optics modulator", Wikipedia, https://en.wikipedia.org/wiki/Acousto-optic_modulator, 2019.02.25.

[17] Kim, Yong-Su, et al. "Two-photon interference with continuous-wave

multi-mode coherent light." Optics express 22.3 (2014): 3611-3620.
[18] James, Daniel FV, et al. "On the measurement of qubits." Asymptotic Theory Of Quantum Statistical Inference: Selected Papers. 2005. 509-538.
[19] Banaszek, K., et al. "Maximum-likelihood estimation of the density matrix." Physical Review A 61.1 (1999): 010304.
[20] “Purity (quantum mechanics)", Wikipedia,
https://en.wikipedia.org/wiki/Acousto-optic_modulator, 2019.02.25.