論文内容の要旨

Development of a heralded photon source with the advantage of multiphoton reduction for improved quantum key distribution

(量子鍵配布改良のための複数光子低減された伝令光子源)

堀切　智之

Quantum key distribution has drawn considerable attention as a method of achieving a shared absolutely secure private key. If a sender and a receiver of information can share the key, secure communications of information composed of bit strings become possible. However, there are imperfections in the real world which can make it difficult to guarantee security and long distance (ultimately global) communications. For instance, loss by absorption in the quantum communication channel, imperfections in the light source, or inefficiencies of detectors in the detection system. Recent progresses in the field of quantum key distribution have made it possible to utilize a weak coherent source which has a finite multiphoton probability. However, it is still desirable to obtain single photon state for a higher secure key generation rate at longer distances. Here we consider a heralded photon source (HPS) which utilizes spontaneous parametric down conversion (SPDC). Photon pairs are generated by SPDC process in a $\chi^{(2)}$ nonlinear crystal. One pump photon simultaneously splits into the photon pair (called signal and idler) where total energy and momentum are conserved. A HPS utilizes the property of the spontaneous generation which can be used in order to increase the communication distance. By getting coincidence between signal (heralded signal) and idler (heralding signal), we can substantially decrease the dark count probability and attain longer distance. Important features of the system are the availability of room-temperature operation, stability, and long-time operability guaranteed by nonlinear crystals which are nonbreakable against intense light. These are essentially required for the practical QKD. However, there is a higher multiphoton probability in the case of relatively large mean photon number close to unity. In this thesis an analysis of QKD utilizing a multiphoton reduced HPS and experimental demonstration of multiphoton reduction by a photon number resolving detector are shown.

In chapter 3, quantitative estimations of a QKD system utilizing a HPS is given. If one can use a photon number resolving detector as a trigger detector of a HPS, the commu-

nication distance and secure key generation rate can be improved. Here time-multiplexed detector (TMD) consisting of commercially available single-photon detectors and optical fibers is considered. Because it can be operated at room temperature, HPS with a TMD can easily be implemented in a practical QKD system.

The calculated secure key generation rate utilizing decoy state method is shown in Figure 1. The maximum distance of HPS ($\approx$ 171 km) becomes longer than that of weak coherent pulse ($\approx$ 140 km) even in the case of an imperfect trigger detector efficiency. Because cutoff distance is affected by a dark count probability, the decrease of dark count by coincidence detection leads to the longer distance. Though maximum secure key generation rate is lower than weak coherent pulse which is due to the imperfect detection efficiency and thermal property of the photon number distribution of a HPS, the secure key generation increases by utilizing a TMD compared with a detector which does not have an ability to resolve photon number.

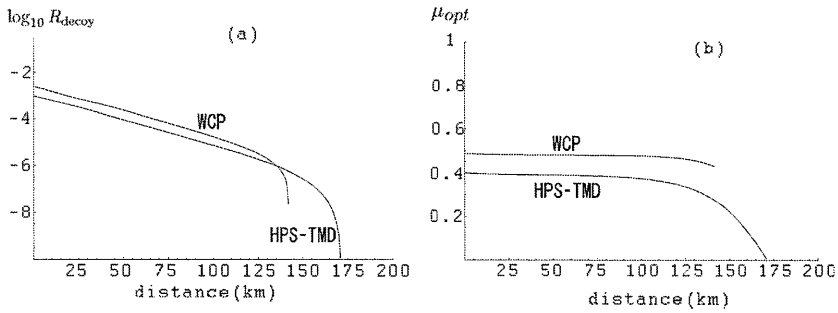

Figure 1: (a) Secure key generation rate vs distance. (b) optimal mean photon number vs distance. Detection efficiency of single photon detectors of TMD is $\eta_A = 0.6$.

In chapter 4, a second-order correlation function was measured to prove removal of multiphoton. The multiphoton reduction by a TMD was real-time processed by fast logic gates. This measurement is different from usual measurement of correlation function on the point of the triggering (Fig. 2). The intensity ratio of the main peak to neighboring peaks is given by

$$I_{\mathrm{TMD}} = \frac{p(2)\frac{1}{2}\eta^2 P(1|2)}{(p(1)\frac{\eta}{2})^2\eta_A + p(1)\frac{\eta}{2}p(2)(\frac{1}{2}\eta + \frac{1}{4}(1-(1-\eta)^2)P(1|2))},$$

while a threshold detector is given by

$$I_{\mathrm{th}} = \frac{p(2)\frac{1}{2}\eta^2(1-(1-\eta)^2)}{(p(1)\frac{\eta}{2})^2\eta_A + p(1)\frac{\eta}{2}p(2)(\frac{1}{2}\eta + \frac{1}{4}(1-(1-\eta)^2)(1-(1-\eta)^2))}.$$

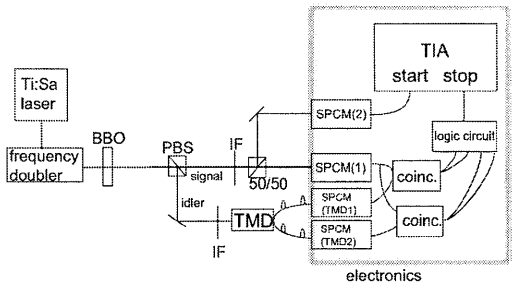

Figure 2: Experimental setup. Ti:Sa: pulsed-Ti:sa laser, doubler: frequency doubler, BBO: type II beta-barium borate crystal, PBS: polarizing beam splitter, 50/50: half beam splitter, IF: interference filter, TIA: time interval analyzer, SPCM: single photon counting module (threshold detector), coinc.: coincidence detection system.

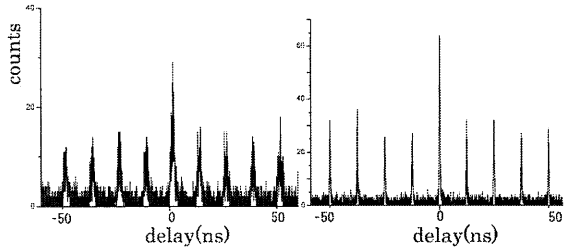

Figure 3: Triggered measurements of correlation function (left) TMD, (right) threshold detector. (band width of interference filters =1.5nm; a single mode fiber for the coupling of the signal (zoom around central peak). Noisy structure of TMD measurement is due to noise in the output voltage pulse from the logic circuit. Detailed results are in TABLE 1

Here $p(1)$ ($p(2)$) is the probability of emitting one (two) photon pair(s) in a pulse, $P(l|m)$ is TMD's detection probability of l counts for m incident photons. It is assumed that the detection efficiencies of two detectors after the 50/50 beam splitter are both equal to η. Since the 1st term in the denominators $\gg$ 2nd term ($p(1) \gg p(2)$ under the low μ condition in the present experiment), the denominators of the two ratios ($I_{\rm TMD}, I_{\rm th}$) are nearly equal to each other. By using the following approximations, $I_{\rm TMD} \approx \frac{p(2)\frac{1}{2}\eta^2 P(1|2)}{(p(1)\frac{\eta}{2})^2\eta_A} = \frac{2p(2)P(1|2)}{p(1)^2\eta_A}$, $I_{\rm th} \approx \frac{p(2)\frac{1}{2}\eta^2(1-(1-\eta_A)^2)}{(p(1)\frac{\eta}{2})^2\eta_A} = \frac{2p(2)(1-(1-\eta_A)^2)}{p(1)^2\eta_A}$, the ratio of $I_{\rm TMD}$ to $I_{\rm th}$ is shown to give the degree of removal ($I_{\rm reduction} = I_{\rm TMD}/I_{\rm th} \approx P(1|2)/(1-(1-\eta_A)^2)$). $P(1|2)$ is a probability that a TMD detects two photon as single photon and $(1-(1-\eta_A)^2)$ is a detection probability of a threshold detector. Because photon number is not resolved by a threshold detector, all signals including at least one photon are used as a key. Thus, $I_{\rm reduction}$ is a probability that a TMD detects two photon as single photon normalized by that of a threshold detector. $I_{\rm reduction}$ becomes zero in an ideal case. However, due to several imperfections such as inefficiencies, low coupling rates of detectors, and failure of mode separation in the TMD (0.25 for two photon in four mode TMD), the resulting peak is not very low (Fig. 3). Table 1 shows the ratios for four cases of setting (band width of interference filters = 1.5 nm and 10 nm, coupling fibers for the signal are singlemode and multimode fibers.) Photon number distribution changes thermal distribution to Poissonian in highly multimode cases. However, we can predict the value of ratio $I_{\rm reduction}$ is constant irrespective of the photon number distribution, as the experimental results shown in Table 1 verify. It is shown that the multiphoton probability was reduced to 0.89 compared with a threshold detector was

Table 1: $I_{\text{reduction}}$, I_{TMD}, and I_{th} for four parameter settings. All fibers on the side of trigger detectors are multi mode fibers.

coupling fibers for SPCM 1 and 2	$\Delta\lambda$	threshold detector			TMD			
		central peak	surrounding peaks	I_{th}	central peak	surrounding peaks	I_{TMD}	$I_{\text{reduction}}$
single mode fiber	1.5nm	1747	1008	1.73± 0.05	1780	1157	1.54± 0.07	0.89± 0.08
	10nm	346757	177291	1.96±0.01	333700	193671	1.72± 0.02	0.88±0.02
multimode fiber	1.5nm	476788	319559	1.49±0.01	543362	410805	1.32 ± 0.02	0.89±0.02
	10nm	1996650	1392340	1.43±0.01	3353310	2637100	1.27±0.03	0.89±0.03

utilized. If it is assumed that detection efficiencies of the two trigger detectors are equal, the triggering efficiency is calculated as $\eta_A \approx 0.28$.

The degree of improvement in the secure key generation rate by the adoption of the TMD is finally evaluated. Figure 4 shows the fractional improvement of secure key generation rate
$R_{\text{decoy HPS-TMD}}/R_{\text{decoyHPS-th}}$ ($R_{\text{decoyHPS-th}}$ ($R_{\text{decoyHPS-th}}$) is the secure key generation rate for the case of a TMD (threshold detector) is utilized as a trigger detector). In the case of

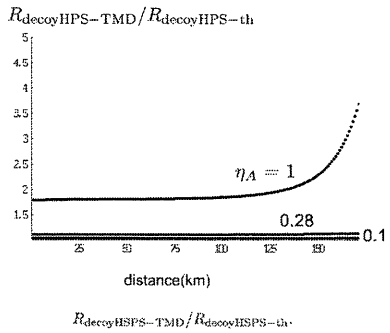

Figure 4: Dependence of Improvement in the key generation rate between HPS-TMD scheme and HPS-threshold detector scheme $R_{\text{decoyHPS-TMD}}/R_{\text{decoyHPS-th}}$ on trigger detection efficiency. $\eta_A = 1, 0.28$, and 0.1 from above. The photon number distribution is assumed to be thermal. Right edge of the figure is 171 km which is the same maximum distance realized by using an ideal single photon source.

the perfect trigger detection ($\eta_A = 1$), the degree of improvement is about 1.8 and rapidly increases from about 100km. This is due to the fact that in the case of a perfect trigger detection we can utilize just single photon signals in most of the case. However, as η_A decreases, the slope of key generation rate becomes steeper, and $R_{\text{decoyHPS-TMD}}/R_{\text{decoyHPS-th}}$ is relatively reduced. About 10% improvement of the secure key generation rate by utilizing a TMD is attained in the case of $\eta_A = 0.28$ under the present experimental condition. The rate of improvement is nearly constant in the range up to 171km.