Two-color parametric down conversion

David Castiel[a], Adam De La Zerda[a], Alex Hayat[b], Matty Katz[a], Tal Mor[a], Meir Orenstein[b], Gil Ratsaby[a] and Nadav Yoran[a]

a. Computer Science Department, Technion, Haifa 32000, Israel;

b. Electrical Engineering Department, Technion, Haifa 32000, Israel;

ABSTRACT

We propose a point to point quantum channel based on a two-color Spontaneous Parametric Down Conversion (SPDC), that may be applied for a Quantum Key Distribution (QKD) system to gain better security. We use one arm of the SPDC (770 nm - optimal for Si detection) and a Si counter at Alice's side to count the exact number of photons in each pulse. Whenever the arm contains exactly one photon, the correlated photon (1550nm - optimal for fiber transmission) in the other arm is sent via a fiber to Bob.

In the experiment we used an Ar^+ laser of 514.5nm wavelength and a BBO crystal to produce type-I photon pairs. We measured the spectrum of the SPDC and resolved specifically the 770 nm wavelength. The rate of correlated pairs (at 890-1050 nm) from our SPDC source was compared to a non-correlated source. We further developed an InGaAs single photon detector based on Geiger mode APD and achieved 10% quantum efficiency and $5 \cdot 10^{-3}$ dark counts per $20nsec$ pulse at a temperature of $-35°$C.

1. INTRODUCTION

Photon pairs of Spontaneous Parametric Down Conversion (SPDC) are widely used in Quantum Information experiments, as a source of entangled photons and a high quality source of single photons. For example these photon pairs are utilized in quantum cryptography applications,[1] teleportation[2,3] and quantum computation.[4] In the SPDC process a pump photon is split within a non linear, non centro-symmetric crystal into two photons, where one is the *signal* and the other is the *idler*. Phase matching conditions (energy and momentum conservation) are required for an efficient process. There are two SPDC types: type-I in which the *signal* and the *idler* have the same polarization, and type-II in which the *signal* and *idler* are orthogonally polarized. In this paper we report a two-color type-I SPDC quantum channel setup, that may be used for Quantum Key Distribution (QKD) applications. The purpose of QKD is to securely transfer a secret key between two honest parties called Alice and Bob, despite the presence of an eavesdropper called Eve. Many reported experimental setups use weak coherent pulse as a pseudo single photon source. Such a source emits vacuum, single photon or two and more photons with Poisson probability distribution. This approach limits the security level of the distributed key since Eve can use the Photon Number Splitting (PNS) attack to reveal the key.[5] In PNS attack on the BB84 protocol[6] Eve performs photon number non-demolition measurement on each pulse sent by Alice. In accordance with the original transmission rate, Eve blocks part or all of the pulses that contain one photon exactly. However if two or more photons are found she keeps one photon in a quantum memory and sends all the other via lossless fiber to Bob. The lossless fiber imitates the original rate so neither Alice nor Bob are able to reveal Eve due to a different rate. Having the photons in her quantum memory she waits until Bob tells Alice via a classical channel in which bases he measured his received photons. Using these bases Eve measures her photons and discloses the key between Alice and Bob without being revealed. In order to gain better security against the PNS attack a SPDC-based system may be used. The idea is to count the number of photons at the *idler* at Alice's side; whenever exactly one photon is detected, the single photon at the *signal* is allowed to be sent to Bob's lab. A two-color SPDC system can be used in order to decrease the amount of information that an eavesdropper can gain using a Photon Number Splitting (PNS) attack.[5] Here we propose a scheme which implements the two color SPDC-based method. Furthermore we report experimental demonstration of a few elements of this scheme.

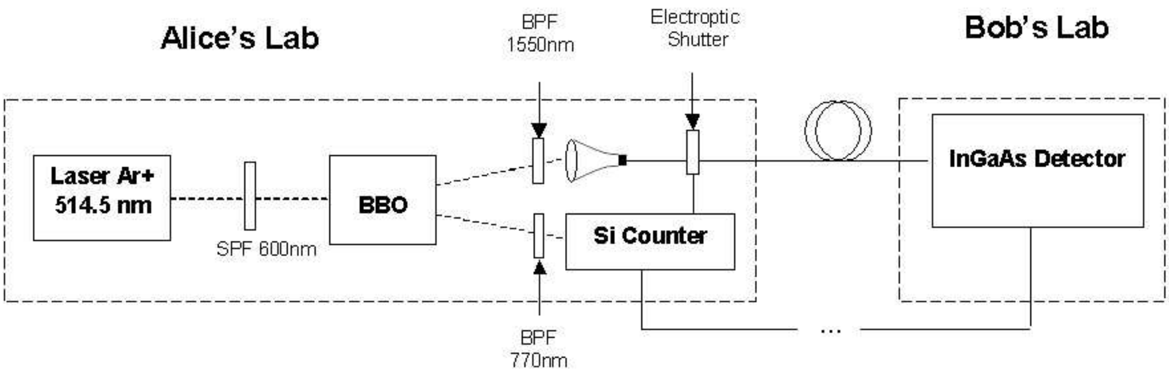


Figure 1. A proposed quantum channel setup based on two color SPDC

2. TWO COLOR SPDC PROPOSED SETUP

An optimal wavelength to detect and count single photons is 0.7 μm where Si detectors with high quantum efficiency can be used. On the other hand the optimal wavelength to distribute photons via fibers is 1.5 μm, where the losses are minimal. A technique to count the exact number of photons in a pulse is described Franson and his collaborators.[7] Therefore we planned a two color SPDC experiment using BBO crystal that produces type-I pairs where the *idler* is at 770 nm and the *signal* is at 1550 nm.

The proposed experimental setup is shown in Fig. 1. The Ar^+ laser tuned to 514.5 nm followed by short pass filters (SPF) to remove unwanted laser emission, pumps a nonlinear BBO crystal. The *idler* is fed through a bandpass filter (BPF) centered at 770 nm to a photon counter based on Si detectors. Whenever exactly one photon is counted the electrooptic shutter is opened and the correlated photon is sent through a BPF centered at 1550 nm via a long fiber to Bob's laboratory where an InGaAs detector is used to resolve single photons. There is a synchronization line between the Si counter and the InGaAs detector which is aimed to signal the InGaAs detector about the coming photon. This indication is necessary to operate the detector in Geiger mode and will be discussed in more detail in section 3.

3. EXPERIMENT AND RESULTS

Our first experimental step was to observe an image of type-I SPDC from a 3mm length BBO crystal which was cut at $\theta = 24.32°$. An Ar^+ laser was tuned to 488 nm and the image shown in Fig. 2 was taken with a CCD Si camera having a absorbtion cutoff at 1050 nm. The camera with a 3cm focal length was located at a distance of 11cm from the crystal. To eliminate the camera's saturation due to the relatively high power laser, we used room temperature long pass GaAs filter with cut-on at 890nm. The camera and the filter formed together an effective bandpass starting at 890 nm and ending at 1050 nm. SPDC process emits a whole spectrum of wavelengths. Each wavelength has its optimum output angle denoted as $\theta_s(\lambda)$ where its Phase Matching Function (PMF) gets its maximum. Similarly we denote the angular Full Width Half Maximum (FWHM) of each wavelength as $\Delta\theta_s(\lambda)$. From momentum and energy conservation, one could get analytical expressions for $\theta_s(\lambda)$ and $\Delta\theta_s(\lambda)$.

We used two methods to check that indeed finite spectrum appears in the ring shown in Fig. 2. The first method is based on a theoretical estimation. We fed our crystal parameters into a software provided by Migdall and his collaborators[8] in order to calculate the ratio $\frac{\Delta\theta_s(\lambda)}{\theta_s(\lambda)}$ within our experimental bandpass. For example, a typical ratio $\frac{\Delta\theta_s(\lambda)}{\theta_s(\lambda)} \approx \frac{0.13°}{3°} \approx 0.043$ was obtained for a single wavelength $\lambda = 976nm$. Since we expect a continuous spectrum, the expected $\frac{\Delta\theta}{\theta}$ is much larger than the calculated ratio for a single wavelength. Indeed in the experiment we measured a larger ratio of 0.2, that indicates that the image consists of a broad spectrum.

To further resolve the SPDC spectrum, we used another method based on the experimental setup shown in Fig. 3(a). The type- I SPDC output from the non-linear crystal was fed to a monochramotor, and resolved by a single photon Si detector SPCM-14 of EG&G with ≈ 100 dark counts per second, having the same cutoff as the

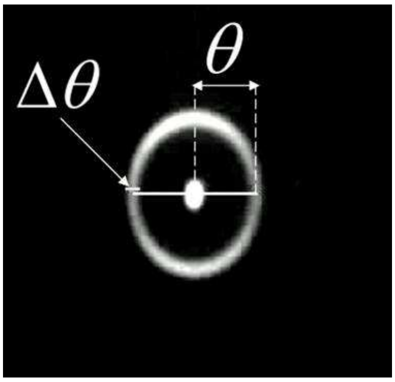


Figure 2. An image of type-I SPDC from our BBO crystal.

camera that was previously described. The electrical pulses from the detector were counted by a counter. The results, which are normalized by the quantum efficiency of the Si detector, are shown in Fig. 3(b). The finite wavelength bandwidth is due to the combination of the GaAs filter and the quantum efficiency of the Si detector as was already explained. We observe a fairly constant intensity. The lower intensity at the shorter wavelengths is due to the GaAs filter.

In order to observe the 770 nm photons the setup was slightly changed. We removed the GaAs filter and added an interference filter at $770 \pm 2nm$ (10 nm FWHM) before the detector. The filter and monochromator's rejection, eliminated off-band wavelengths. In Fig. 3(c) the spectrum around the wavelength of 770 nm is shown. The shape is a result of the filtering, and the large intensity (relative to the intensity observed at around $890 - 1050nm$) is due to the removal of the GaAs filter.

In order to quantify the correlation rate between the *idler* and the *signal* the setup in Fig. 4 is used. Counter1 and Counter2 are counting the electrical pulses of the *signal* and *idler* at the wavelength band of 890-1050 nm. The pulses are fed to a correlation device (based on a simple logical AND gate) having a response time of $35nsec$, which is connected to Counter3 that counts the number of coincidences per second. Fig. 5 compares the coincidences-level curves of the SPDC source and a non correlated source. A light bulb was chosen as a non-correlated source which was coupled directly to the objectives. For each measurement, the bulb's intensity was tuned to yield the same counts (in counters 1 and 2) as in the SPDC case. As expected, decreasing the sources' intensity, increases the correlation gap in favor of the SPDC source.

Denote the sum of the response and dead times of the detectors by τ, that divides our time scale to virtual slots of width τ. The maximal rate of output pulses from the detector is therefore $N = \frac{1}{\tau}$. We first analyze the case of coincidences resulted from the non-correlated source. Let n_1 and n_2 be the average number of counts per second produced by Counter1 and Counter2 respectively and p_1 and p_2 the average number of photons per second entering the objectives. As long as $p_i << N$, the number of counts read by each counter is proportional to the number of photons per second p_i entering the objective. Denote the fiber-objective coupling efficiency by η_i and the detector's quantum efficiency by q_i, so that $n_i = p_i q_i \eta_i$. The probability that a certain count would accommodate a certain time-slot is $\frac{n_i}{N}$. All the parameters above are approximately identical for both arms. Therefore, we define $q_i \equiv q, n_i \equiv n, \eta_i \equiv \eta, p_i \equiv p$. It follows that the probability of simultaneous detection in both Counter1 and Counter2 is $\frac{n}{N} \cdot \frac{n}{N}$, thus the number of simultaneous detections per second is:

$$C_{non-correlated} = \frac{n}{N}\frac{n}{N}N = \frac{n^2}{N} = \frac{p^2\eta^2 q^2}{N}.$$

For the SPDC, p_i, the number of photons per time slot (usually 0 or 1 due to $p_i << N$) is equal in both arms entering the objectives. Given one photon in arm 1, the probability of a photon in arm 2 is $\eta \cdot q$. The probability for a simultaneous detection for a certain time slot is $\frac{n_1}{N} q_2 \eta_2 = \frac{n_2}{N} q_1 \eta_1 = \frac{pq^2\eta^2}{N}$. It follows that the number of simultaneous detections per second is:

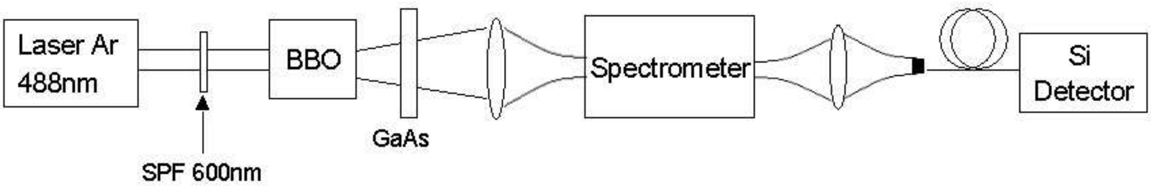
$$C_{SPDC} = pq^2\eta^2,$$

thus:

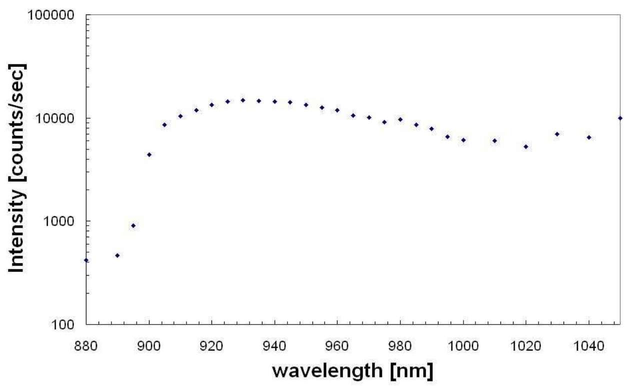
$$\frac{C_{SPDC}}{C_{non-correlated}} = \frac{N}{p}.$$

For a EGG SPCM-14 detector, $\tau \approx 66nsec$. Thus $N \approx 15,000,000$ per second, that fits well with our experimental results. We can also learn from the experimental results of Fig. 5 that for $N = p$ we obtain $n \approx 500,000$ so that $\eta q \approx 15 \pm 2dB$.

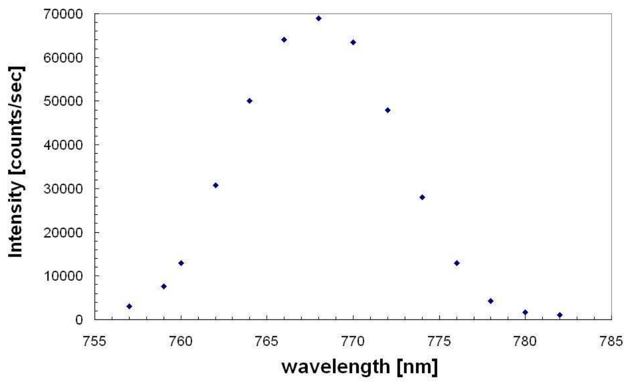
A detector that can resolve single photons at high efficiency is a key element in QKD systems in general and in ours in particular. We designed a quantum channel that transmits single photons of $1.5\mu m$ wavelength band via fibers. The best well-known solid state detector for this band is an InGaAs Avalanche Photo Diode (APD). In order to achieve the required sensitivity we activated our detectors in Geiger mode. In this mode the detector is supplied with a voltage higher than the breakdown voltage. A single photon which is absorbed, triggers an avalanche process that causes a macroscopic output current. The current is controlled, in our case, by an active quenching mechanism: a DC bias slightly lower than the breakdown voltage plus a short time voltage pulse. The sum of those voltages exceeds the breakdown voltage of the diode, enabling the avalanche process to produce a short-time current pulse. In Geiger mode, most of the false counts are due to the dark current. We used a NEC photodiode (NR8360JP) which is cooled down to $-35°C$ in order to decrease the dark counts. For the characterization of the detector we used a Continuous Wave (CW) diode laser at $1.5\mu m$. A breakdown voltage of $\approx 64V$ was measured. Therefore a DC bias of $63V$ was provided. A $20nsec$ gate pulses are set to $6V$ at $200K$ pulses per second. At this working point we achieved $20K$ readings per second for laser intensity of $-85dBm$ that corresponds to an approximately 1 photon per gate on average. The dark count level was $1K$ counts per second. Hence, we report a 10% quantum efficiency and dark count of $5 \cdot 10^{-3}$ per pulse. We believe that further cooling and a shorter time voltage gate will improve this performance.



(a) An experimental setup for resolving the SPDC spectrum.



(b) Spectrum results from the BBO crystal.



(c) Measured SPDC spectrum around 770nm.

Figure 3.

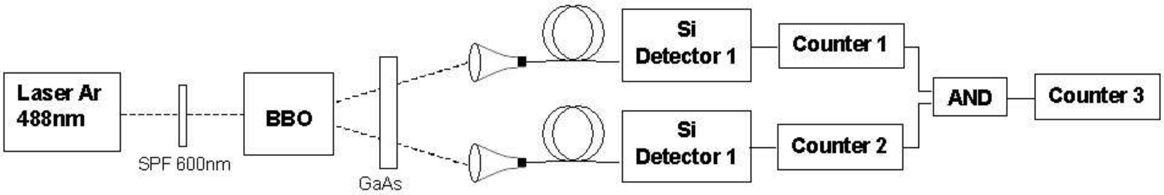


Figure 4. A schematic setup to measure the correlations between the two arms of SPDC.

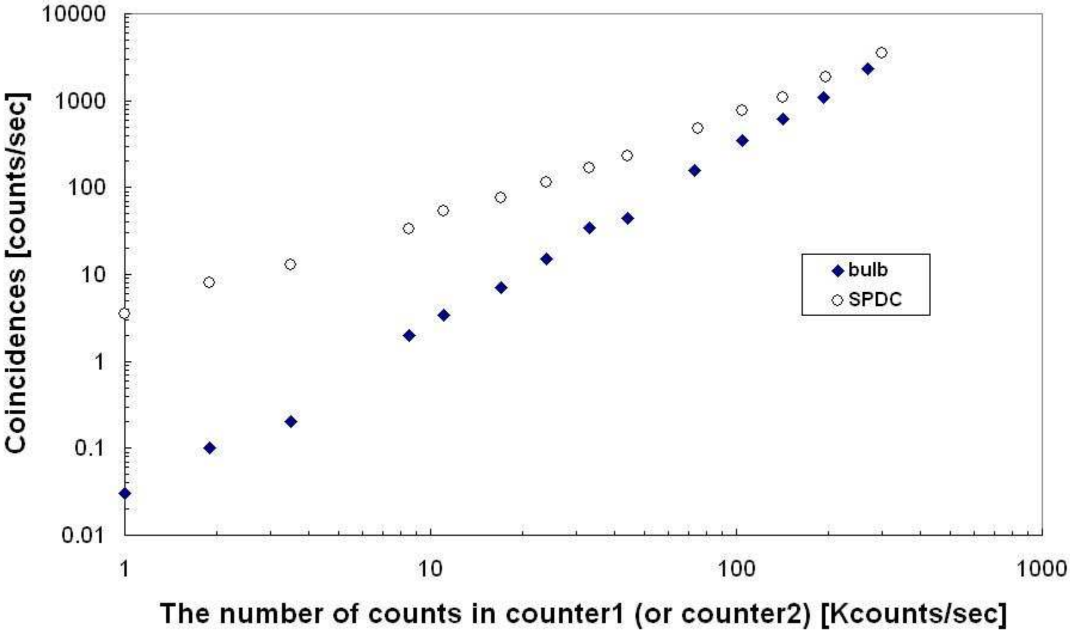


Figure 5. Coincidence levels of the SPDC source and a non correlated source.

4. SUMMARY

We propose an experimental quantum channel scheme based on a theoretical idea of a two color type-I SPDC source.[5] This setup may be used for QKD systems with improved security against PNS attack. We showed the spectrum of the BBO SPDC source, specifically its emission at 770nm. We showed the correlation rate between SPDC *signal* and *idler*, and found that the coincidences rate of the SPDC source is much greater than that of a non correlated source. Finally we report the performance of a Geiger mode InGaAs detector that may be used to detect signals at 1550nm.

ACKNOWLEDGMENTS

This work was supported in part by the Israeli MOD, by the Israel Science Foundation - FIRST (grant #4088103), and by the Technion's Barnett First Steps Program.

REFERENCES

1. A. V. Sergienko, M. Atatüre, Z. Walton, G. Jaeger, B. E. A. Saleh, and M. C. Teich, "Quantum cryptography using femtosecond-pulsed parametric down-conversion," *Phys. Rev. A.* **60**, pp. R2622–R2625, 1999.
2. D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu, "Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.* **80**, pp. 1121–1125, 1998.
3. B. Boumeester, J. W. Pan, K. Mattle, M. Eibel, H. Wienfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature* **390**, pp. 575–579, 1997.
4. Z. Zhao, A. N. Zhang, Y. A. Chan, H. Zhang, J. F. Du, T. Yang, and J. W. Pan, "Experimental demonstration of a non-destractive controlled-not quantum gate for two independent photon-qubits," *Phys. Rev. Lett.* **94**, p. 030501, 2005.
5. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.* **85**, pp. 1330–1333, 2000.
6. C. Bennent and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Computers, Systems and Signal Processing*, *Proc. IEEE* **1898**, pp. 175–179, 1984.
7. M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, "Photon number resolution using a time-multiplexed single-photon detector," *Phys. Rev. A.* **68**, p. 043814, 2003.
8. N. Boeuf, D.Branning, I. Chaperot, E. Dauler, S. Guérin, G. Jaeger, A. Muller, and A. Migdall, "Calculating characteristics of noncollinear phase matching in uniaxial and biaxial crystals," *Opt. Eng.* **39**, pp. 1016–1024, 2000.