IJCSC International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 191-194

Photon Sources : Quantum Cryptography Challenge

Anand Sharma[1] **& Vibha Ojha**[2]

[1]CSE Deptt., FET, MITS, Lakshmangarh, Sikar, Rajasthan, India
[2]CSE Deptt., IITM, Gwalior, M.P., India
Email: [1]anand_glee@yahoo.co.in, [2]vibha.ojha@gmail.com

ABSTRACT

Quantum cryptography is based on the use of single photon Fock states. Unfortunately, these states are difficult to realize experimentally. Nowadays, practical implementations rely on faint laser pulses or entangled photon pairs, where both the photon as well as the photon-pair number distribution obeys Poisson statistics. Hence, both possibilities suffer from a small probability of generating more than one photon or photon pair at the same time. For large losses in the quantum channel even small fractions of these multi-photons can have important consequences on the security of the key. In this paper we briefly comment on sources based on faint pulses as well as on entangled photon-pairs, and we compare their advantages and drawbacks.

Keywords: Quantum Cryptography, Photon Polarization, Photon Source, Photon Gun

1. INTRODUCTION

Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. In fact, QC rests on two pillars of 20th century quantum mechanics – the Heisenberg Uncertainty principle and the principle of photon polarization. According the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the point when it is measured. Secondly, the photon polarization principle describes how light photons can be oriented or polarized in specific directions.

Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984 as part of a study between physics and information. Bennet and Brassad stated that an encryption key could be created depending on the amount of photons reaching a recipient and how they were received. Their belief corresponds to the fact that light can behave with the characteristics of particles in addition to light waves. These photons can be polarized at various orientations and these orientations can be used to represent bits encompassing ones and zeros. Thus, while the strength of modern digital cryptography is dependent on the computational difficulty of factoring large numbers, quantum cryptography is completely dependent on the rules of physics and is also independent of the processing power of current computing systems.

But in this paper we are considering the challenge for upcoming Quantum cryptography that is photon source. In the first section we describe Faint laser pulses solution then in next section we consider Photon pairs generated by parametric downconversion and at last we consider photon guns for photon generator for quantum cryptography.

2. FAINT LASER PULSES

There is a very simple solution to approximate single photon Fock states: coherent states with an ultra-low mean photon number m. They can easily be realized using only standard semiconductor lasers and calibrated attenuators. The probability to find n photons in such a coherent state follows the Poisson statistics:

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

Accordingly, the probability that a non-empty weak coherent pulse contains more than 1 photon, can be made arbitrarily small.

$$\begin{aligned} P(n > 1 \mid n > o, \mu) &= \frac{1 - P(0,\mu) - P(1,\mu)}{1 - P(0,\mu)} \\ &= \frac{1 - e^{-\mu}(1+\mu)}{1 - e^{-\mu}} \cong \frac{\mu}{2} \end{aligned} \tag{2}$$

Weak pulses are thus extremely practical and have indeed been used in the vast majority of experiments. However, they have one major drawback. When μ is small, most pulses are empty:

$$P(n = 0) \approx 1 - \mu.$$

In principle, the resulting decrease in bit rate could be compensated for thanks to the achievable GHz modulation rates of telecommunication lasers. But in practice the problem comes from the detectors' dark. Indeed, the detectors must be active for all pulses, including the empty ones. Hence the total dark counts increase with the laser's modulation rate and the ratio of the detected photons over the dark counts decreases with μ. The problem is especially severe for longer wavelengths where photon detectors based on Indium Gallium Arsenide semiconductors (InGaAs) are needed, since the noise of these detectors explodes if they are opened too frequently (in practice with a rate larger than a few MHz). This prevents the use of really low photon numbers, smaller than approximately 1%. Most experiments to date relied on $\mu = 0.1$, meaning that 5% of the nonempty pulses contain more than one photon. However, it is important to stress that, there is an optimal μ depending on the transmission losses[1]. After key distillation, the security is just as good with faint laser pulses as with Fock states. The price to pay for using such states lies in a reduction of the bit rate.

3. PHOTON PAIRS GENERATED BY PARAMETRIC DOWNCONVERSION

Another way to create pseudo single-photon states is the generation of photon pairs and the use of one photon as a trigger for the other one [2]. In contrast to the sources discussed before, the second detector must be activated only whenever the first one detected a photon, hence when $\mu = 1$, and not whenever a pump pulse has been emitted, therefore circumventing the problem of empty pulses. The photon pairs are generated by spontaneous parametric down conversion in a $\chi^{(2)}$ non-linear crystal. In this process, the inverse of the well-known frequency doubling, one photon spontaneously splits into two daughter photons – traditionally called signal and idler photon – conserving total energy and momentum. In this context, momentum conservation is called phase matching and can be achieved despite chromatic dispersion by exploiting the birefringence of the nonlinear crystal. The phase matching allows to choose the wavelength, and determines the bandwidth of the downconverted photons. For the non degenerate case one typically gets 5-10 nm, whereas in the degenerate case (central frequency of both photons equal) the bandwidth can be as large as 70 nm. This photon pair creation process is very inefficient, typically it needs some 10^{10} pump photons to create one pair in a given mode. The number of photon pairs per mode is thermally distributed within the coherence time of the photons, and follows a poissonian distribution for larger time windows [3]. With a pump power of 1 mW, about 10^6 pairs per second can be collected in single mode fibers. Accordingly, in a time window of roughly 1ns the conditional probability to find a second pair having detected one is $10^6 \cdot 10^{-9} \approx 0.1\%$. In case of continuous pumping, this time window is given by the detector resolution. Tolerating, e.g. 1% of these multi-pair events, one can generate 10^7 pairs per second, using a realistic 10 mW pump. Detecting for example 10 % of the trigger photons, the second detector has to be activated 10^6 times per second. In comparison, the example of 1% of multi-photon events corresponds in the case of faint laser pulses to a mean photon number of $\mu = 0.02$. In order to get the same number 10^6 of non-empty pulses per second, a pulse rate of 50 MHz is needed. For a given photon statistics, photon pairs allow thus to work with lower pulse rates (e.g. 50 times lower) and hence reduced detector-induced errors. However, due to limited coupling efficiency into optical fibers, the probability to find the sister photon after detection of the trigger photon in the respective fiber is in practice lower than 1. This means that the effective photon number is not one, but rather $\mu \approx 2/3$, still well above $\mu = 0.02$ [4].

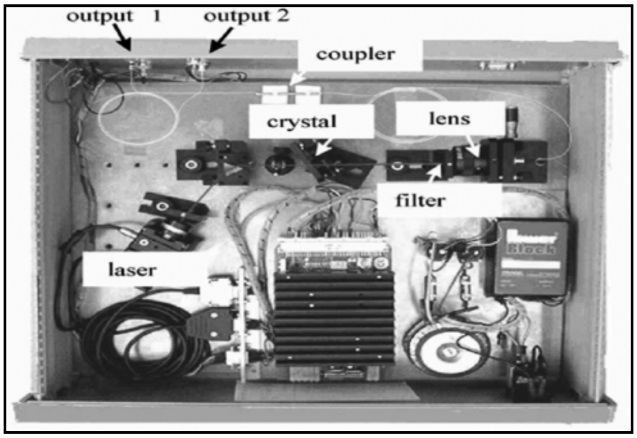

Fig. 1: Entangled Photon Pair Source as Used in the First Long-distance Test of Bell Inequalities (Whole Source Fits in a Box of Only 40*45* 15 cm^3 Size and Neither Special Power Supply Nor Water Cooling is Necessary)

Photon pairs generated by parametric down conversion offer a further major advantage if they are not merely used as pseudo single-photon source, but if their entanglement is exploited. Entanglement leads to quantum correlations which can be used for key generation. In this case, if two photon pairs are emitted within the same time window but their measurement basis is chosen independently, they produce completely uncorrelated results. Hence, depending on the realization, the problem of multiple photon can be avoided. Figure 1 shows one of our sources creating entangled photon pairs at 1310 nm wavelength as used in tests of Bell inequalities over 10 kilometers [6]. Although not as simple as faint laser sources, diode pumped photon pair sources emitting in the near infrared can be made compact, robust and rather handy.

4. PHOTON GUN

The ideal single photon source is a device that when one pulls the trigger, and only then, emits one and only one photon. Hence the name photon gun. Although photon anti-bunching has been demonstrated already years ago [7], a practical and handy device is still awaited. At present, there are essentially three different experimental approaches that come more or less close to this ideal.

A first idea is to work with a single two-level quantum system that can obviously not emit two photons at a time. The manipulation of single trapped atoms or ions requires a much too involved technical effort. Single organics dye molecules in solvents [9] or solids [10], [12] are easier to handle but only offer limited stability at room temperature. Promising candidates, however, are nitrogen-vacancy centers in diamond, a substitutional nitrogen atom with a vacancy trapped at an adjacent lattice position [14], [15]. It is possible to excite individual nitrogen atoms with a 532 nm laser beam, which will subsequently emit a fluorescence photon around 700 nm (12ns decay time). The fluorescence exhibits strong photon anti-bunching and the samples are stable at room temperature. However, the big remaining experimental challenge is to increase the collection efficiency (currently about 0.1%) in order to obtain mean photon numbers close to 1. To obtain this, an optical cavity or a photonic bandgap structure must suppress the emission in all spatial modes but one. In addition, the spectral bandwith of this type of source is broad (of the order of 100 nm), enhancing the effect of pertubations in a quantum channel. A second approach is to generate photons by single electrons in a mesoscopic p-n junction. The idea is to take profit of the fact that thermal electrons show antibunching (Pauli exclusion principle) in contrast to photons [16]. First experimental results have been presented [17], however with extremely low efficiencies, and only at a temperature of 50mK!

Finally, another approach is to use the photon emission of electron-hole pairs in a semiconductor quantum dot. The frequency of the emitted photon depends on the number of electron-hole pairs present in the dot. After one creates several such pairs by optical pumping, they will sequentially recombine and hence emit photons at different frequencies. Therefore, by spectral filtering a single-photon pulse can be obtained [20], [21]. These dots can be integrated in solid-states microcavities with strong enhancements of the spontaneous emission [19].

In summary, today's photon guns are still too complicated to be used in a QC-prototype. Moreover, due to their low quantum efficiencies they do not offer an advantage with respect to faint laser pulses with extremely low mean photon numbers *ì*.

5. CONCLUSION

Quantum cryptography could well be the first application of quantum mechanics at the individual quanta level. The very fast progress in both theory and experiments over the recent years are reviewed, with emphasis on open questions and technological issues. Most of the research so far uses optical fibers to guide the photons from Alice to Bob and we shall mainly concentrate here on such systems. There is, however, also some very significant research on photon generation and transmission. In this paper we have considered the main technological issue of photon source for quantum cryptography and focused on the question "how to proudce photons ?" Finally we compared the advantages and disadvantages of both the sources.

REFERENCES

[1] Lutkenhaus, N.,"Security Against Individual Attacks for Realistic Quantum Key Distribution", *Phys. Rev. A*, **61**, 052304, 2000.

[2] Hong, C.K. and L. Mandel, "Experimental Realization of a Localized One-photon State", *Phys. Rev. Lett.*, **56**, 58-60, 1986.

[3] Walls, D.F. and G.J. Milburn, "Quantum Optics", *Springer-verlag*, 1995.

[4] Ribordy, G., J. Brendel, J.D. Gautier, N. Gisin, and H. Zbinden, "Long Distance Entanglement Based Quantum Key Distribution", *Phys. Rev. A*, **63**, 012309, 2001.

[5] Jan Peřina, Jr., Ondřej Haderka, and Jan Soubusta, "Quantum Cryptography Using a Photon Source Based on Postselection from Entangled Two-photon States" *Phys. Rev. A 64*, 052305, 2001.

[6] Tittel, W., J. Brendel, H. Zbinden, and N. Gisin, "Violation of Bell Inequalities by Photons More than 10 km Apart", Phys. Rev. Lett. 81, 3563-3566, 1998.

[7] Kimble, H. J., M. Dagenais, and L. Mandel, "Photon Antibunching in Resonance Fluorescence", *Phys. Rev. Lett.*, **39**, 691-694, 1977.

[8] Anirban Pathak,"A Mathematical Criterion for Single Photon Sources Used in Quantum Cryptography" *Indian J. Phys.*, **80**, pp. 495-499, 2006 http://arxiv.org/abs/0705.1600

[9] Kitson, S.C.,P. Jonsson, J.G. Rarity, and P.R. Tapster, "Intensity Fluctuation Spectroscopy of Small Numbers of Dye Molecules in a Microcavity", *Phys. Rev. A 58*, 620-6627, 1998.

[10] Brunel, Ch., B. Lounis, Ph. Tamarat, and M. Orrit, "Triggered Source of Single Photons based on Controlled Single Molecule Fluorescence", *Phys. Rev. Lett. 83*, 2722-2725, 1999.

[11] N. Akopian, N. H. Lindner, E. Poem, Y. Berlatzky, J. Avron, D. Gershoni, B. D. Gerardot, and P. M. Petroff, "Entangled Photon Pairs from Semiconductor Quantum Dots," *Phys. Rev. Lett.*, **96**, p. 130501, Apr. 2006.

[12] Fleury, L., J.-M. Segura, G. Zumofen, B. Hecht, and U.P. Wild, "Nonclassical Photon Statistics in Single-Molecule Fluorescence at Room Temperature", *Phys. Rev. Lett. 84*, 1148-1151, 2000.

[13] *Anand Sharma*, Ramesh Chandra Belwal, Vishal Goar, Vibha Ojha, "Quantum Cryptography – The Concept and

Challenges " *in Proceeding of 2nd International Conference on Computer and Automation Engineering (ICCAE 2010) Singapore*, pp. 710-714, 2010.

[14] Kurtsiefer, Ch., S. Mayer, P. Zarda, and H. Weinfurter, "Stable Solid-State Source of Single Photons", *Phys. Rev. Lett.*, **85**, 290-293, 2000.

[15] Brouri, R., A. Beveratios, J.-P. Poizat, P. Grangier, "Photon Antibunching in the Fluorescence of Individual Colored Centers in Diamond", *Opt. Lett.*, **25**, 1294-1296, 2000.

[16] Imamoglu, A., and Y. Yamamoto, "Turnstile Device for Heralded Single Photons : Coulomb Blockade of Electron and Hole Tunneling in Quantum Confined p-i-n Heterojunctions", *Phys. Rev. Lett. 72*, 210-213, 1994.

[17] Kim, J., O. Benson, H. Kan, and Y. Yamamoto, "A Single-photon Turnstile Device", *Nature*, **397**, 500-503, 1999.

[18] Thomas M. Babinec, Birgit J. M. Hausmann, M.K., Yinan Zhang, Jeronimo R. Maze, Philip R. Hemmer & Marko Lončar, "A Diamond Nanowire Single-photon Source" *Nature Nanotechnology,* **5**, 195-199, 2010.

[19] G´erard, J.-M., B. Sermage, B. Gayral, B. Legrand, E. Costard, and V. Thierry-Mieg, "Enhanced Spontaneous Emission by Quantum Boxes in a Monolithic Optical Microcavity", *Phys. Rev. Lett.*, **81**, 1110-1113, 1998.

[20] G´erard, J.-M., and B. Gayral, "Strong Purcell Effect for InAs Qantum Boxes in Three-Dimensional Solid-State Microcavities", *J. Lightwave Technology*, **17**, 2089-2095, 1999.

[21] Santori, C., M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, "Triggered Single Photons from a Quantum Dot" (Stanford University, Palo Alto, California), 2000.

[22] Martin J. Stevens, Robert H. Hadfield, Robert E. Schwall, Sae Woo Nam, and Richard P. Mirin,"Quantum Dot Single Photon Sources Studied with Superconducting Single Photon Detectors", *IEEE Jour. of Selected Topics in Quan. Electronics*, **12**, No. 6, pp.1255-1268, 2006.

[23] H. S. Eisenberg, G. Khoury, G. A. Durkin, C. Simon, and D. Bouwmeester, "Quantum Entanglement of a Large Number of Photons," *Phys. Rev. Lett.*, **93**, pp. 193901-1–193901-4, Nov. 2004.