Quantum Random Number Generator

Jaroslav HRUBY
Group of Cryptology
Union of Czech Mathematicians and Physicists
P.O.B.2100 , 160 49 PRAHA 6, Czech Republic

May 2000

Abstract

A physical quantum random number generator based on the random events which are realized by the choice of single photons between the two outputs of a beamsplitter is presented.

1 Introduction

Random numbers are employed today as well for numerical simulations as for cryptography.Random numbers are critical in every aspect of cryptography.To encrypt digitally sign documents, e-mail, or spend money in electronic cash over the internet, we need random numbers. A physical quantum random generator can give new way in generating random numbers for cryptographic applications.

Randomness is connected with the notions of unpredictability, disorder, chaos and unintentionality. Classical computers are very good at following clear precise instructions but they cannot be programmed to do something unpredictable, such a pick a random number.

Quantum mechanical indeterminism, the inability to predict into which state a superposition will appear to callapse upon being measured, does provide exactly the right solution.As quantum theory is intrisically random, a quantum process is an ideal base for a physical random number generator.

Starting from quantum cryptographic device which was presented in [1,2] we realized optical random number generator.

2 Description of the device

One of the fundamental quantum process is deviding the photonic beam by the beamsplitter. The principle of the generator is illustrated in the

figure 1. In the case of the one photon, which cannot be devide, the way to the one of the two detectors is full random .

Mathematically it means, that the light pulse with one photon with the statistical division $p(n) = \delta_{n,1}$ is going through the beamsplitter, then for the probability of detection on both detectors A and B at the same moment is $P_{A,B} = p_A(n)p_B(n)[\langle n^2\rangle - \langle n\rangle] = 0$ because for one photon state $\langle n^2\rangle = \langle n\rangle = 1$.

Physical realisation is the following: Weak pulses of a 830 nm LED are coupled into a monomode fibre. The lenght of laser pulses is from $400ps$ to $4ns$ with the repetition frequence from $100Hz$ to $1MHz$ Laser pulses has Poisson statistics in number photons per pulse $p(n) = \frac{\alpha^n}{n!}\exp^{-\alpha}$, where α is average number of photons per pulse.For $\alpha = 0,1$ we get $p(1) = 9\%, p(0) = 90,5\%, p(\rangle 2) = 0,5\%,$. In this way laser pulses are attenuated by a computer-controlled attenuator so that the intensity level at the output is below one photon per pulse on the average.

Polarization properties of light are controlled by polarization controllers.

The light is chaotically devided by the polarization beamsplitter and detected by detectors. The beamsplitter has the fixed ratio $p_A p_B = 96\%44\%$.

The dectors are single photon counting modules with Si-avalanche photodiodes. Their output signals are processed by detection electronics base on time-to-amplitude converters and single channel analyzers.Both terminals are fully driven by computers (see figure 2).

The whole device and both detectors are placed in polystyrene thermoisolating boxes (see fig.3,4) .

3 Results

The randomness of a sequence of numbers generated by our generator was extensively tested and on rough data was applied both the von Neumann and Y.Perese iteraction methods.

It was shown that the results are determined by the physical process, where true random data are proceed via apparatus and statistical quality of the product can be stabilized and all negative factors can be extracted .

In the case of true random generator it is the ratio between signs "0" and "1". It is known that in the case of physical random numbers generators based on the noise of diods the maximal equable of occurrence "0" and "1" is about $e \sim 0.001$, where $Pr(x = \text{"0"}) = 0.5 + e$ or $Pr(x = \text{"0"}) = 0.5 - e$.

The production of quantum number generator was realized in 1 gigabit files. On such files we can tested the equable of occurrence "0" and "1" about $e \sim 0.0001$

At this moment we can conclude that results from optical quantum number generator are better then from the other physical generators. The data generated from this quantum generator sucessfully passed DIEHARD statistical tests and also cryptological tests (QUT Brisbane, Information

research centre) for measuring the randomness of large binary streams. The author of the DIEHARD statistical tests G.Marsaglia (http//stat.fsu.edu/geo)

The research in this direction is in progress.

We conclude, we demonstrated a random number generator using a basic quantum process with super small correlation between succesive bits.Such generator behaves like a perfect random source, which is better then other for us known physical random sources.

This work was supported by Grants RN 1998 2003 012 and RN 1998 2003 013, which are done at the Joint Institute of Optical Laboratory UP and Institute of Physics AV CR in Olomouc.

References

[1] J.Hruby "Trends in quantum cryptography in Czech Republic", Lecture Notes in Comp.Sci.1438,Springer (1998)pp.261-272.

[2] M.Dusek,O.Haderka,M.Hendrych,J.Hruby,R.Myska,"Secure identification system based on Quantum Key distribution",presented on the rump session Eurocrypt99, published in Phys.Rev.A. July 1999