Experimental Implementation of Active Basis Choice for QKD with Entangled States

P M Vinetskaya[1,2], N A Borshchevskaia[1], V V Tretyakov[1], and S P Kulik[1]

[1] *Quantum Technology Centre, M V Lomonosov Moscow State University, Moscow, Russia*
[2] *Physics, National Research University Higher School of Economics, Moscow, Russia*
Contact Email: polinvin@gmail.com

QKD protocols allows generation of common secret keys for independent interlocutors through the open channels. Although entangled based protocol BBM92 has many advantages in theoretical research, in original form it requires 8 SPDs (single photon detectors), which makes it inefficient compared with other schemes. In this study we consider active basis choice BBM92 implementation, compare it with original setup and give experimental results of its implementation.

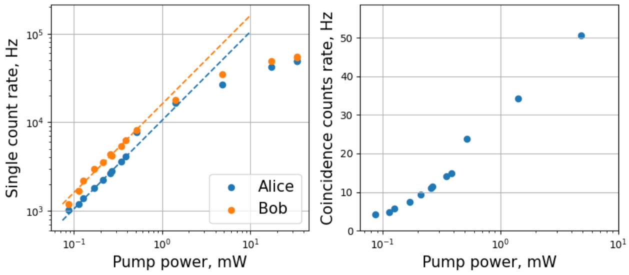

Figure 1: Measured counting rate

Entangled pair generation is based on the type-II spontaneous down-conversion effect: under the action of a pump photon pairs with orthogonal polarisation are emitted. Adjusting the crystal parameters affects the condition of quasi-phase matching and makes it possible to achieve a situation in which signal and idler photons propagate in the same direction and have the same wavelength.

The Sagnac interferometer is widely used as Bell states generator. The pump radiation, polarized at an angle of 45°, gets split into two beams by PBS, which, passing through the crystal, generate $|HV\rangle$ and $|VH\rangle$ pairs.

Generated state is the singlet Bell state:

$$|\Psi_0\rangle = \frac{|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B}{\sqrt{2}} \tag{1}$$

Originally a measurement in 2 non-orthogonal bases is implemented by a symmetric beamsplitter (passive scheme), so both Alice and Bob need 4 SPDs for state measurement. It can be proved that a non-linear crystal with a random number generator can replace SBS and reduce the number of detectors down to 2 for each side and do not affect the probability distribution and other theoretical aspects of the protocol.

In the presence of a voltage U applied along H or V axis (assuming Z is horizontal), the Z-cut $LiNbO_3$ crystal develops a birefringence with the fast/slow axes at 45° to H and V. It allows to measure the state in one of the two different bases: H-V ($U = 0$) or R-L ($U = U_{\pi/2}$) by random choice of one of two voltage values $0, U_{\pi/2}$.

BBM92 protocol with active basis choice was implemented with a pump wavelength of 780 ± 0.02 nm. Since the quantum efficiency of the detectors at a wavelength of 1560 nm is 20%, and the dead time is 15 μs, at frequencies of the order of 10 kHz, the measurements no longer reliably reflect the number of generated pairs (Fig. 1).