QKD authentication and detector hack protection with secret basis shifts.

Y. Kurochkin, A. Fedorov, V. Ustimchik, A. Losev, A. Kanapin, A. Sokolov, A. Miller and V. Kurochkin

Russian Quantum Center, Skolkovo, Moscow 143025, Russia

Abstract: To protect QKD from the detector manipulation attacks and classical channel authentication challenges we demonstrate quantum key distribution protocol with floating basis. In this protocol we put additional secret basis shift which makes protocol tolerant to detector manipulation attack and man in the middle attack. We demonstrate this protocol realization over 25 km fiber channel.

Quantum key distribution real applications has number of technological challenges. The detector blinding attack have attracted a lot of interest [1]. Not only avalanche photodiodes manipulation was demonstrated but also superconducting single photon detectors can be hacked [2]. The main principle of detector hacking is following. Detectors are moved to linear regime with strong light. Eavesdropper Eve choose the additional light pulse power in the way that half of the pulse power produces no click while full pulse power guarantees click. To protect from this attack Alice and Bob can use secret basis shift for BB84. Knowing some initial secret Alice and Bob use for each laser pulse applied phase $\varphi_{Alice(Bob)} = \varphi(i,k) + \varphi_{BB84\_Alice(Bob)}$ where $\varphi(i,k)$ is some pseudorandom function, i – number of pulse, k – secret key known to Alice and Bob, and $\varphi_{BB84\_Alice(Bob)}$ – BB84 phase which Alice (Bob) chooses randomly from four (two) standard BB84 states [3]. In this case φ_{Alice} is uniformly distributed over all possible positions.

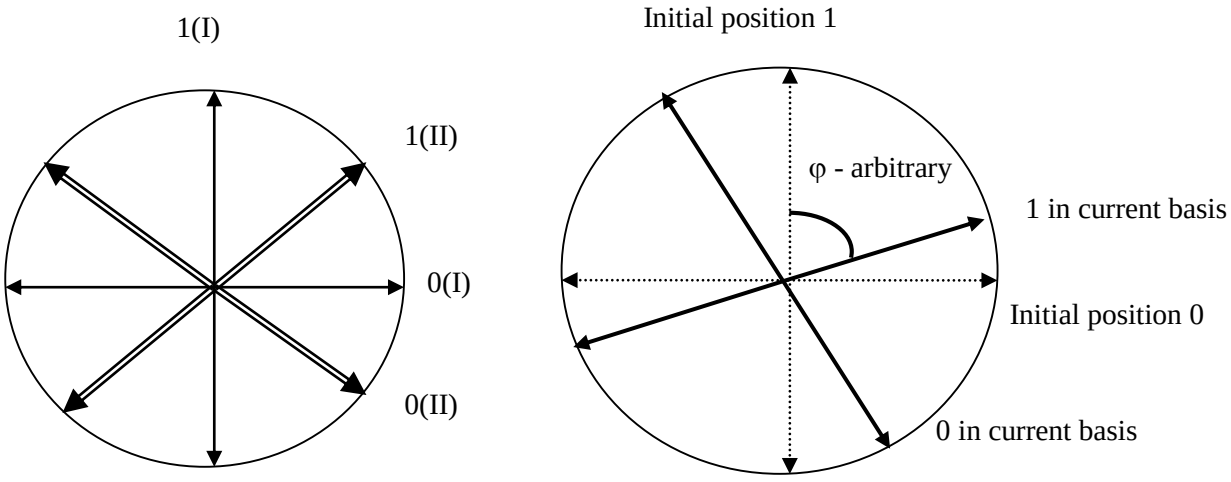

Fig. 1. BB84 (left) has four fixed states positions while in the floating basis protocol Eve can expect any possible state on the circle.

In this case the detector manipulation starts working probabilistically as soon as Eve basis can alter from Alice and Bobs choice on arbitrary angle. In this case if Bobs detector will click on the Eves signal placed on the angle no more that ε from original state, there is also ε probability for an Eve to have wrong output of the measurement. The wrong Eves measurement will cause ε error rate on Bobs side. To protect from this type of attack one can apply one of the following countermeasures. Actively change comparator level of the detector on $\pm\delta$ or take two detectors with different comparator levels or simply introduce additional loss before one of the detectors. In this case to produce clicks on both detectors Eve will cause more errors on the detector with lower comparator level or lower loss.

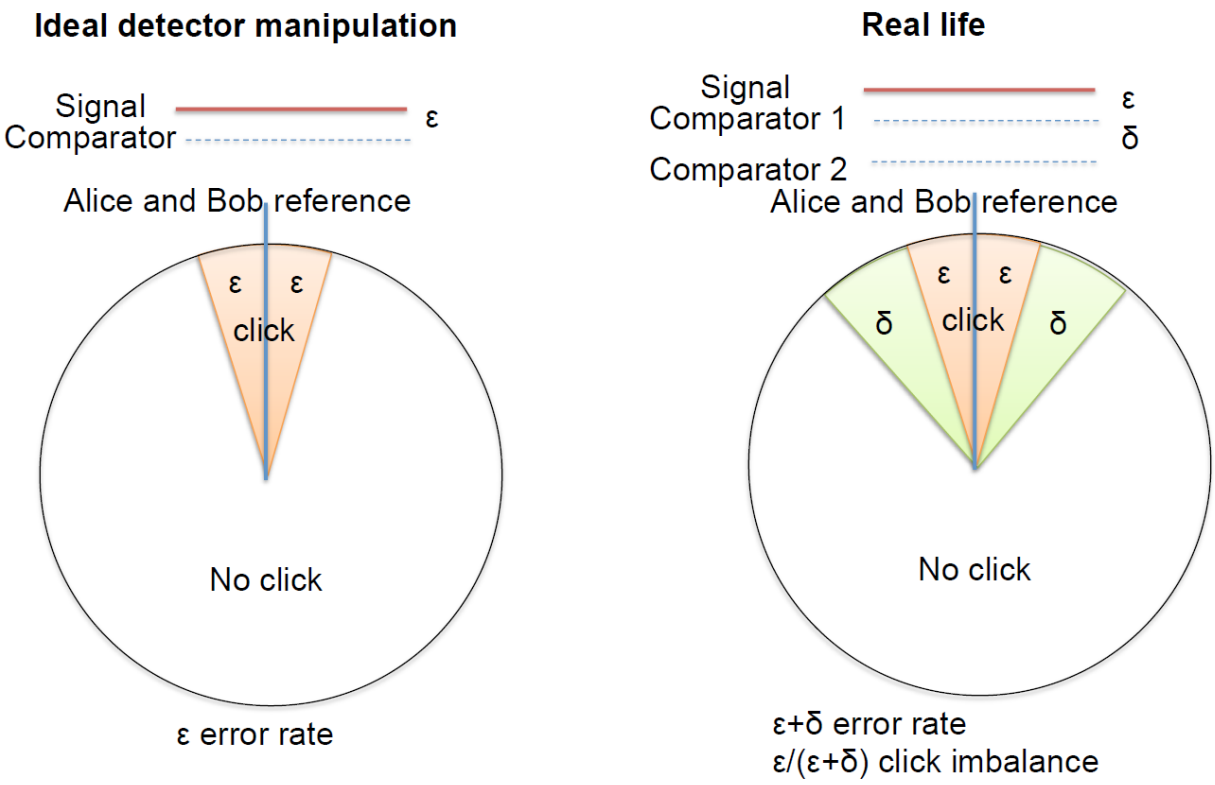

Fig. 2. If both detectors are perfectly same the Eve will introduce some errors according to the difference between comparator level and signal (left). If detectors are different there will be inevitable errors on the detector with lower comparator level.

The other advantage of secret basis shifts (or floating basis protocol [4]) is the built in authentication. In the original BB84 model Eve can listen public channel but don't modify it. The channel authentication consuming key. In the floating basis protocol the public channel modification doesn't give an approach to the key for an Eve. The reason is that even if Eve knows the $\varphi_{BB84\_Alice(Bob)}$, the $\varphi_{Alice(Bob)}$ is still unknown to the Eve. The floating basis protocol integrate the detector blinding protection and authentication on the protocol level.

To demonstrate the floating basis protocol experimentally we use QKD device with plug&play optical scheme and ID210 [5] single photon detectors. Electro-optical modulators are driven by digital-to-analog converters connected to the National Instruments board with FPGA on board. System operates at 10 Mhz pulse repetition rate. As the result we receive 2 kHz of sifted key rate with 2.7% QBER over 25 km. The additional basis shift $\varphi(i,k)$ is applied on the base of linear function $\varphi(i,k) = (a * \varphi(i-1,k) + b)\ mod\ 2\pi$ where a and b are secret parameters used for authentication.

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," Opt. Express 18, 27938–27954 (2010).
[2] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," New J. Phys. 13, 113042 (2011)

[3] C.H. Bennet and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Bangalore, India, December 9-12, 1984), p. 175.

[4] Yury Kurochkin Quantum cryptography with floating basis protocol. // Proc. SPIE. 2005. – Vol. 5833. – P. 213-221.

[5] http://www.idquantique.com/photon-counting/photon-counting-modules/id230/