# Wavelength-selected photon-number-splitting attack against "*plug-and-play*" quantum key distribution systems with Decoy States

Mu-Sheng Jiang[1], Shi-Hai Sun[1], Chun-Yan Li[1], Lin-Mei Liang[1,2,*]
[1]*Department of Physics, National University of Defense Technology, Changsha 410073, P. R. China and*
[2]*State Key Laboratory of High performance Computing,*
*National University of Defense Technology, Changsha 410073, P. R. China*

Since a single photon source is not available for practical quantum key distribution (QKD) systems nowadays, weak coherent state are widely used in practical systems which suffers from the photon-number-splitting (PNS) attack. Fortunately, the decoy state method is proposed to defeat it, in which there is an important assumption that the signal state and decoy state is not distinguishable for Eve. However, in practical systems, this assumption is invalid in some situations, then the security of decoy state method will be compromised. Actually, a wavelength-selected PNS (WSPNS) is proposed by our group to break the security of decoy state "*plug-and-play*" QKD systems by exploiting the imperfection of the intensity modulator (IM) that used to generate the signal state and decoy state. Our analysis shows that Eve can use our attack to determinately distinguish the signal state and decoy state, then the security of decoy state method is broken.

In the decoy state "*plug-and-play*" QKD systems, Alice must randomly modulate the intensity of each light pulse to either signal state level or decoy state level before sending it back to Bob. Usually, an intensity modulator in Alice is used to produce different signal strengths. Here we take the weak+vacuum decoy state method based on $LiNbO_3$ waveguide-based Mach-Zehnder-type electro-optic IM for example. To generate the signal state, decoy state and vacuum state with average photon number of $\mu$, $\nu$ and 0 respectively, the IM can work as follows: intensity modulation does not perform on the signal state but on the signal pulse and the reference pulse of the vacuum state and the decoy state, with their intensities modulated to a proportion of $0 : \nu : \mu$, then an attenuator attenuates them to their own intensity level 0, $\nu$ and $\mu$ with the same attenuation factor.

For normal operation, the modulation voltage *V(t)* is a constant when the electron-optic effect happens in the $LiNbO_3$ waveguides, so that the time-dependent phase difference $\Delta\varphi(t)$ and the time-dependent output phase $\varphi(t)$ of the light pulse are also constants, which corresponds to pure intensity modulation and fits the model in the security proofs of Decoy-State method. However, once *V(t)* is not a constant any more, $\Delta\varphi(t)$ will contribute to the frequency shift of the light pulse, which is no longer pure intensity modulation and deviates from the model in the security proofs of Decoy-State method.

Unfortunately, in current QKD systems, Alice does not monitor the arrival times of the signal pulse and the reference pulse. In this case, Eve can time shift the light pulse during the device calibration routine and through the whole duration of QKD, so that the electron-optic effect will happen at the rising edge of intensity modulation voltage, with a time-dependent *V(t)*. Thus frequency shift will be introduced to the light pulses. On the one hand, since the vacuum state has an intensity of average photon number 0, Eve need not to do anything on it. On the other hand, since the intensity modulator does not perform on the signal state but on the decoy state, the signal state will always retain its original frequency, while the decoy state may be introduced a frequency shift once Eve performs corresponding time shift. Analysis show that if we set $\mu$=0.48, $\nu = 0.05$, which are the optimal value under the experimental parameters of GYS , the frequency shift introduced by Eve is about hundreds of Megahertz, depending on the rise time of modulation voltage.

Therefore, the decoy state and the signal state can be distinguished by wavelength measurement based on wavelength division multiplex (WDM) technology without error. Then Eve can perform our WSPNS attack to beat the Decoy-State method: Eve firstly performs frequency shift and wavelength-selected to pick out the signal state and the decoy state, then applies PNS on the signal state and the decoy state respectively to collect information about the key.

When we set $\mu$=0.48 and $\nu = 0.05$, which are the optimal values under the experimental parameters of GYS, other parameters are the same as those in GYS, simulation results show that the maximal secure distance of Bob is only 24.6 km under WSPNS attack, while it is 140.55 km without our attack. When transmission distance is larger than 13.6 km, Eve can get partial information about the key generated between the legitimate parties. Specially, when transmission distance is larger than 24.6 km, Eve can get full information about the key just like PNS attack was performed in "*plug-and-play*" QKD systems without Decoy-State method, which has shown the strong capability of WSPNS attack.

It is worthwhile to point out here that our WSPNS attack against Decoy-State method in "*plug-and-play*" QKD systems is universal. Firstly, such a loophole that frequency shift will be introduced when Eve performs appropriate

[*] Email:nmliang@nudt.edu.cn

time shift appears in several kinds of intensity modulators used in Decoy-State method, such as electro-absorption modulator and acousto-optic modulator. Secondly, similar results can be obtained in the other decoy state method, since different frequency shift will be introduced for different light intensities, which corresponds to different decoy states.

Of course, WSPNS attack is not omnipotent for breaking the security of decoy state method, but only fits to beat decoy state "*plug-and-play*" QKD systems since Eve must perform time shift to introduce frequency shift. However, we demonstrate for the first time that Decoy-State method itself may introduce another loophole while it has closed the loophole of multi-photon pulses. Commonly, any improved protocol for patching loopholes may introduce other new loopholes while it has closed the existent ones. Thus, we will never be too careful to proof the security of an improved protocol for patching existent loopholes. We believe that our finding is valuable for improving the security of practical QKD.