A Simulation of Quantum Key Distribution Protocol with Enhancing Ability to Against PNS Attack

Phichai Youplao[1,a] and Sukhum Julajaturasiraratn[1,b]

[1]Department of Electrical Engineering, Faculty of Industry and Technology,
Rajamangala University of Technology Isan Sakon Nakhon Campus,
199 Village No. 3, Phungkon, Sakon Nakhon, Thailand

[a]<phichai.yo@rmuti.ac.th>, [b]sukhum.ju@rmuti.ac.th

ABSTRACT

This paper presents a modified quantum key distribution (QKD) protocol with an enhancing ability to restrict the probability that eavesdropper can recognize key bits information for her photon number splitting (PNS) strategy. The simulation results are demonstrated by the relationship between the secret key rates as a function of the transmission distance between the two parties. The system parameters are specified by; the pulse rate of 1 GHz, the photon number of μ = 1, the attenuations of 2, 0.35, and 0.25 dB/km, the detector efficiencies of 50%, 20%, and 10%, and the dark count probabilities of 10^{-7}, 10^{-5}, and 10^{-5}, for the light pulses of 800, 1300, and 1550 nm, respectively. From the simulation results, the secret key rate of approximately 24.2, 111.8, and 46.6 kbit/s can be achieved by each wavelength for the distances of 20, 80, and 100 km, respectively.

Keywords*: quantum cryptography, QKD protocol, PNS attack, information security*