Security Analysis of the 1-Decoy State QKD Protocol with a Leaky Intensity Modulator

Weilong Wang, Xiangdong Meng, Yangyang Fei, Yuanhao Li and Zhi Ma

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, China

Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, Henan, 450001, China

Motivation

- The finite-key security of three-intensity decoy-state quantum key distribution (QKD) with information leakage has been extensively studied.
- The finite-key security and practicality of 1-decoy state QKD without information leakage has been proved.
- We fill this gap by presenting a finite-key security analysis method for estimating the key parameters in the security proof of the 1-decoy state QKD protocol with a leaky intensity modulator.

1-Decoy State QKD Protocol

In the protocol implemented with weak coherent pulses, Alice sends mixtures of Fock states to Bob with the form:

$$\rho^{\gamma^j}=\sum_{n=0}^{\infty}p_n^j|n\rangle\langle n|,$$

where $p_n^j=\left(\gamma^j\right)^n e^{-\gamma^j}/n!$ is the probability that the optical pulse sent by Alice contains n photons when she selects the intensity setting j.

- Alice randomly chooses one of two intensities $\{\gamma^{s},\gamma^{v}\}$ with probabilities $\{p_s,p_v\}$ respectively, and a basis $\Omega\in\{Z,X\}$ with probabilities $\{p_Z,p_X\}$, respectively.
- Bob randomly selects a basis $\Omega\in\{Z,X\}$ with probabilities $\{p_Z,p_X\}$, respectively, to measure the state coming from Alice.
- After N rounds of quantum transmission and measurement, they post-process the raw data to distill the secure keys.

Results

THA against the Intensity Modulator (IM)

$$N_{\mathrm{click},1,\gamma^{s}|\chi}+\delta_{1,\chi}^{s}\geq\frac{p_s(\gamma^{s})^2e^{\gamma^{v}-\gamma^{s}}}{p_v\gamma^{v}(\gamma^{s}-\gamma^{v})}(N_{\mathrm{click},\gamma^{v}|\chi}+\delta_{\chi}^{v})-\frac{\gamma^{v}}{\gamma^{s}-\gamma^{v}}(N_{\mathrm{click},\gamma^{s}|\chi}+\delta_{\chi}^{v})-\frac{\gamma^{s}+\gamma^{v}}{\gamma^{v}}(N_{\mathrm{click},0,\gamma^{s}|\chi}+\delta_{0,\chi}^{s})-\frac{N_\chi p_s(\gamma^{s})^2e^{\gamma^{v}-\gamma^{s}}}{\gamma^{v}\left(\gamma^{s}-\gamma^{v}\right)}\Delta^{vs}$$

$$e_{\mathrm{ph}}^{U}=\frac{1}{N_{\mathrm{click},1,\gamma^{s}|Z}^{L}}\min\left\{\left[N_{\mathrm{click},1,\gamma^{s}|Z}^{L}\frac{N_{\mathrm{error},1,\gamma^{s}|X}^{U}}{N_{\mathrm{click},1,\gamma^{s}|X}^{L}}+\left(N_{\mathrm{click},1,\gamma^{s}|Z}^{L}+N_{\mathrm{click},1,\gamma^{s}|X}^{L}\right)\times Y\left(N_{\mathrm{click},1,\gamma^{s}|Z}^{L},N_{\mathrm{click},1,\gamma^{s}|X}^{L},\varepsilon'\right)\right],N_{\mathrm{click},1,\gamma^{s}|Z}^{L}\right\}$$

where:
$N_{\mathrm{click},1,\gamma^{s}|\chi}$ is the actual number of events where Bob observes a click when Alice sends a single-photon pulse with intensity γ^{s} and both Alice and Bob select the χ basis, and $\delta_{1,\chi}^{s}$ denotes the deviation term due to the statistical fluctuations when using Azuma's inequality. Δ^{vs} is the deviation term coming from the information leakage out of the IM. The other parameters are defined in an analogous way. e_{ph}^{U} is the upper bound on the phase error rate.

These equations imply that Eve could know partial information about Alice's intensity settings by a THA against the IM, which violates a key assumption of the decoy-state method. As a result, the estimation method for the relevant parameters needed to calculate the key rate should be modified!

Simulation of the key generation rate

Secret key length [1]:

$$\ell\geq N_{\mathrm{click},0,\gamma^{s}|Z}^{L}+N_{\mathrm{click},1,\gamma^{s}|Z}^{L}\left[1-H\left(e_{\mathrm{ph}}^{U}\right)\right]-leak_{\mathrm{EC}}-\log_2\frac{2}{\varepsilon_{\mathrm{sec}}^2-\varepsilon}-\log_2\frac{2}{\varepsilon_{\mathrm{cor}}}$$

For illustration purposes, we simulate the secure key rate by maximizing ℓ over the set of the parameters controlled by Alice and Bob and minimizing it over the set of parameters controlled by Eve, who implements a Trojan-horse attack (THA) shown in the figure below.

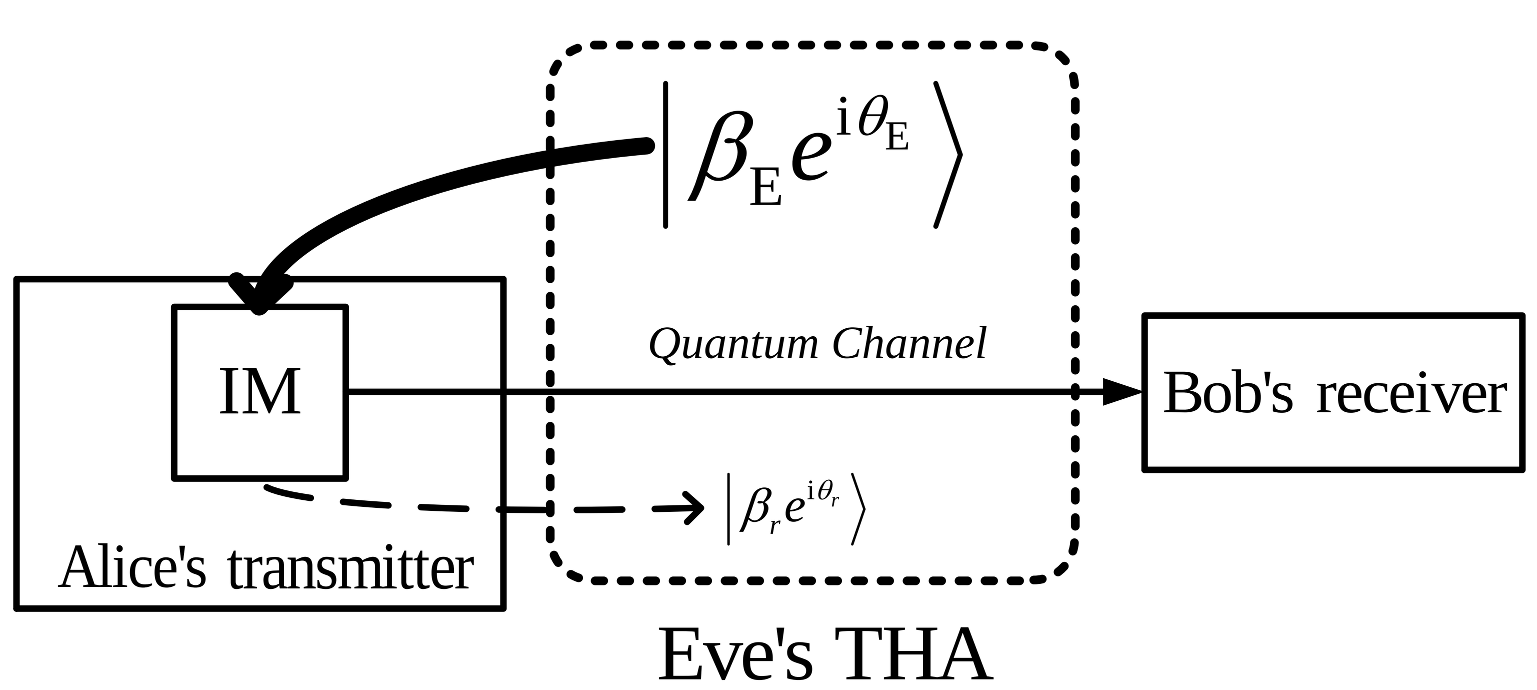

Figure. THA against the intensity modulator (IM) of Alice's transmitter. Eve sends Alice a high intensity single-mode coherent state $|\beta_E e^{i\theta_E}\rangle$ represented by the thick arrow. The back-reflected light from the IM to Eve has the form $|\beta_r e^{i\theta_r}\rangle$ represented by the dashed arrow.

[1] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, *Phys. Rev. A* **89**, 022307 (2014).
[2] K. Tamaki, M. Curty, and M. Lucamarini, *New J. Phys.* **18**, 065008 (2016).
[3] W. Wang, K. Tamaki, and M. Curty, *New J. Phys.* **20**, 083027 (2018).

Experimental parameters used for the simulations:

e_d	p_d	η_{det}	α	f_{EC}
0.01	5×10^{-6}	0.25	0.2	1.2

Resulting secret key rate: