Decoy state quantum key distribution with imperfect source

Anqi Huang,[1, 2] Shi-Hai Sun,[3, *] Zhihong Liu,[4] and Vadim Makarov[5, 2]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3] *College of Science, National University of Defense Technology, Changsha 410073, P.R.China*
[4] *College of Mechatronic Engineering and Automation,*
National University of Defense Technology, Changsha 410073, P.R.China
[5] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*

Introduction.–Unconditional secret information transmission is always the terminal goal of cryptography. It is an impossible task for classical cryptography, which is based on the mathematical complexity. However, quantum cryptography based on the solid basis of quantum mechanics provides a way to reach such terminal goal. Recently some quantum cryptography primitives have been implemented, such as quantum key distribution (QKD) [1], quantum coin tossing (QCT) [2], quantum digital signature (QDS) [3] and quantum secret sharing (QSS) [4]. A weak coherence source (WCS) is widely used in practical quantum cryptography systems. However, multiphoton pulses in the WCS leaks information to Eve by performing a photon-number-splitting (PNS) attack [5]. Fortunately, the decoy state protocol [6] was proposed to defeat any photon-number-dependent attacks. In the decoy state protocol, an important assumption is the indistinguishability of signal and decoy states. However, this assumption may not be guaranteed in practical decoy state protocol [7–10].

This work has three main contributions. First, we show a specific side-channel in the time domain to distinguish the signal state and the decoy state in a QKD system. Thus, we demonstrate a PNS attack to pass by the decoy state protocol. Second, from Alice and Bob's point of view, we give a general model to analyze the security of decoy state protocol with an imperfection source, in which the signal state and the decoy state are partially distinguishable in any degrees of freedom. Third, two approaches, a hardware modification and an advanced theoretical model, are discussed to improve the secure key rate.

PNS attack to an imperfect decoy state source.–To evaluate the realization of the decoy state protocol, we test a QKD system, in which different intensities are modulated by applying different driven current on a laser diode. We get the normalized probability distribution of emitting photons over timing as shown in Fig. 1. The emission mismatch of the signal state and the decoy state violates the basic assumption of indistinguishability in the decoy state protocol. Thus, benefiting from partial distinguishability in the time domain, Eve could break the protection of the decoy state protocol by performing the following hacking strategy. Eve selects time windows W_s and W_d to observe states sent by Alice. In W_s (W_d) Eve treats all observed states as the signal state (the decoy state). Then she performs a PNS attack.

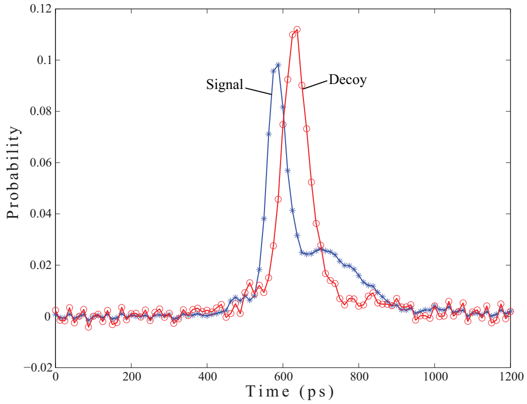

FIG. 1. Normalized intensity distribution of the signal state and the decoy state measured from a QKD system.

Following the criteria of a successful attack proposed in Ref 9, the success ability of the attack could be analysed by comparing a lower bound of the key rate under Alice and Bob's estimation, R^l, and an upper bound of the key rate under Eve's attack, R^u. R^l is the one used in the decoy state protocol [11]:

$$R^l = -Q_\mu H(E_\mu) f(E_\mu) + Y_1^\mu \mu e^{-\mu}[1 - H(e_1^\mu)]. \qquad (1)$$

Y_1^μ and e_1^μ are single-photon yield and error rate in the normal decoy state protocol [11] respectively. It is the secure key rate from Alice and Bob's point of view, when they do not notice Eve's attack. The actual upper bound of key rate under the PNS attack is

$$R^u = Y_1^{\mu_{Eve}} \mu e^{-\mu}, \qquad (2)$$

where $Y_1^{\mu_{Eve}}$ is the real overall single-photon detection yield under Eve's attack [9]. Once R^l is even higher than R^u, the shared final key must be partially insecure. That is the result Eve's attack would like to reach. Therefore, the criteria of a successful attack is

$$R^l > R^u. \qquad (3)$$

Apparently, the goal of our attack is minimizing the R^u in Eq. (2) to achieve the successful condition in Eq. (3),

[*] shsun@nudt.edu.cn

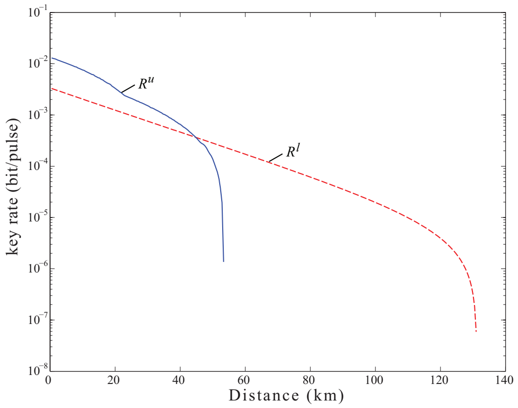

FIG. 2. Lower bound R^l and optimized upper bound R^u of key rate. The parameters used in the simulation are from the GYS experiment [12], which are $Y_0 = 1.7 \times 10^{-6}$, $e_0 = 0.5$, $\eta_{Bob} = 0.045$, $e_{detector} = 0.033$ and $f(E_\mu) = 1.22$. The quantum channel loss is 0.21 dB/km. The mean photon numbers are $\mu = 0.6$ for the signal state and $\nu = 0.2$ for the weak decoy state.

while following the same measurement statistics of Bob, hiding the attack from being noticed. Based on the measurement result in Fig. 1, we simulate R^l and R^u as shown in Fig. 2. Note that in our simulation, we follow the analysis in Ref 11 to employ the detection parameters in Gobby-Yuan-Shields (GYS) experiment [12]. According to the condition as Eq. (3), Eve could successfully hack it when the distance between Alice and Bob is longer than 53 km.

Tightened secure key rate with an imperfect source.– To protect a QKD system from above attack, we modify the security model of the decoy state protocol. More generally, an imperfect source that has the side-channel to distinguish signal and decoy states in any possible degrees of freedom is taken into account. In the security model, we use the weak+vacuum decoy state protocol [11]. The intensities of Alice's pulses are noted as $\omega = \{\mu, \nu, \nu_1\}$ ($\nu_1 = 0$ in the weak+vacuum decoy state protocol [11]). If the imperfection of source is taken into account, the density matrix of Alice's states can be rewritten as

$$\rho'_\omega = \rho_\omega \otimes \rho_\omega(\lambda) = \sum_{n=0}^{\infty} \sum_{\lambda} P_n^\omega f_\omega(\lambda) |n, \lambda\rangle\langle n, \lambda|. \quad (4)$$

Here $\rho_\omega(\lambda)$ is the quantum state used by Eve to distinguish either the signal state or the decoy state for each pulse. $f_\omega(\lambda)$ is the probability distribution of λ, which is normalized $\sum_\lambda f_\omega(\lambda) = 1$ and depends on the intensities of Alice's pulse ω. Thus, the total gain and error rate of Alice's states should be rewritten as

$$\begin{aligned} Q_\omega &= \sum_{n=0}^{\infty} P_n^\omega Y_n^\omega = \sum_{n=0}^{\infty} P_n^\omega \sum_\lambda f_\omega(\lambda) Y_n(\lambda), \\ Q_\omega E_\omega &= \sum_{n=0}^{\infty} P_n^\omega Y_n^\omega e_n^\omega = \sum_{n=0}^{\infty} P_n^\omega \sum_\lambda f_\omega(\lambda) Y_n(\lambda) e_n(\omega), \end{aligned} \quad (5)$$

where $Y_n(\lambda)$ and $e_n(\lambda)$ are the yield and error rate given that Alice sends a n-photon pulse and Eve obtains λ in her measurement. Since Eve will try to distinguish ω for each pulse by measuring λ, the imperfection of source can be characterized by the distance between $\rho_\omega(\lambda)$ and $\rho_{\omega'}(\lambda)$, which is given by

$$D_{\omega\omega'} = \frac{1}{2} tr(|\rho_\omega - \rho_{\omega'}|) = \frac{1}{2} \sum_\lambda |f_\omega(\lambda) - f_{\omega'}(\lambda)|. \quad (6)$$

Here $\omega, \omega' \in \{\mu, \nu, \nu_1\}$, and $tr|x|$ is the trace distance of quantum state. From Eq. (6), it is easy to obtain

$$\begin{aligned} |Y_n^\omega - Y_n^{\omega'}| &\leq 2D_{\omega\omega'}, \\ |Y_n^\omega e_n^\omega - Y_n^{\omega'} e_n^{\omega'}| &\leq 2D_{\omega\omega'}. \end{aligned} \quad (7)$$

Thus, the lower bound of Y_1^μ can be rewritten as

$$Y_1^\mu \geq \frac{\mu}{\mu\nu - \nu^2}[e^\nu Q_\nu - \frac{\nu^2}{\mu^2} e^\mu Q_\mu - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 - 2D_{\mu\nu}(e^\nu - 1)]. \quad (8)$$

The upper bound of e_1^μ can be estimated by

$$e_1^\mu \leq \min\{\frac{e^\mu Q_\mu E_\mu - e_0 Y_0}{\mu Y_1^\mu}, \frac{e^\nu Q_\nu E_\nu - e_0 Y_0 + 2\nu D_{\mu\nu}}{\nu Y_1^\mu}, \frac{e^\mu Q_\mu E_\mu - e^\nu Q_\nu E_\nu + 2D_{\mu\nu}(e^\nu - 1)}{(\mu - \nu) Y_1^\mu}\}. \quad (9)$$

The estimated key rate is shown in Fig. 3. It shows that the imperfection of source will reduce the key rate. For example, when the source is perfect, the maximal distance is about 141 km, but the maximal distances are reduced to 48 km, 92 km, 124 km for $D_{\mu\nu} = 10^{-3}$, $D_{\mu\nu} = 10^{-4}$, $D_{\mu\nu} = 10^{-5}$, respectively.

Key rate improvement.–To obtain key rate as high as possible, two approaches could improve the secure key rate. The first method is a hardware patch. The mismatch of the signal and decoy states in time domain as presented in Fig. 1 is due to improper modulation method. We test another modulation method employed in some QKD systems: a laser source generates optical pulses with a constant intensity which is then randomly modulated by an intensity modulator to generate signal and decoy states. The measured result shows in Fig. 4. it

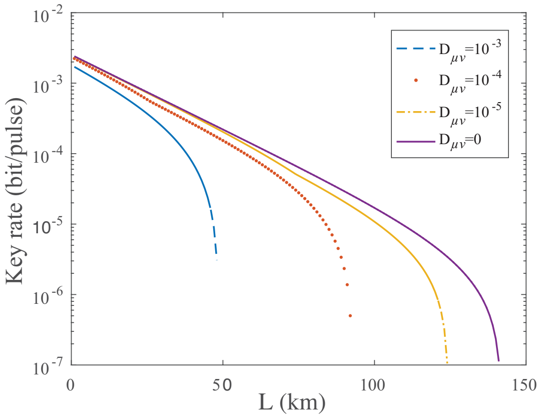

FIG. 3. Estimated key rate for different $D_{\mu\nu}$. The parameters used here are the same as in Fig. 2. The intensities of the signal state and the decoy state are optimized with step 0.01 from $\mu \in [0.01, 0.5]$, $\nu \in [0.01, 0.2]$.

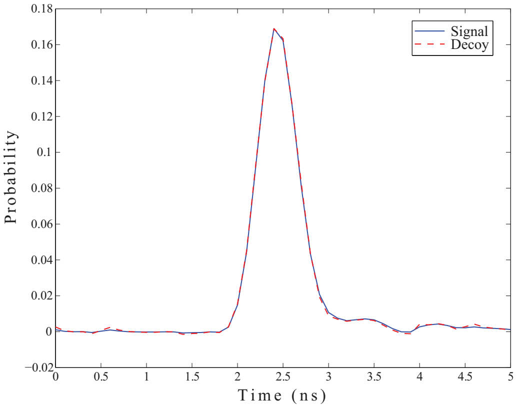

FIG. 4. Normalized intensity distribution of the signal state and the decoy state measured from a homemade laser source with an intensity modulator.

is clear that the timing mismatch between the signal state and the decoy state becomes neglectable. This countermeasure is a hardware substitute of the direct laser diode modulation, closing the timing mismatch between the signal state and the decoy state.

An alternative option is an advanced theoretical model. If the transmission efficiency of Bob's optical devices is calibrated as η_{Bob}^{cal}, the secure key rate can be theoretically improved. Then Eq. (7) can be rewritten as

$$\begin{aligned} |Y_n^{\omega} - Y_n^{\omega'}| &\leq 2D_{\omega\omega'}[1-(1-\eta_{Bob}^{cal})^n], \\ |Y_n^{\omega}e_n^{\omega} - Y_n^{\omega'}e_n^{\omega'}| &\leq 2D_{\omega\omega'}[1-(1-\eta_{Bob}^{cal})^n]. \end{aligned} \tag{10}$$

Thus, we could estimate the final key rate with the same method given above. The estimation result in Fig. 5 clearly shows that the final key rate and the maximal distance are improved, when the loss of Bob's optical devices is taken into account. For example, in the case that $D_{\mu\nu} = 10^{-3}$, the maximal distance increases to 105 km from 48 km.

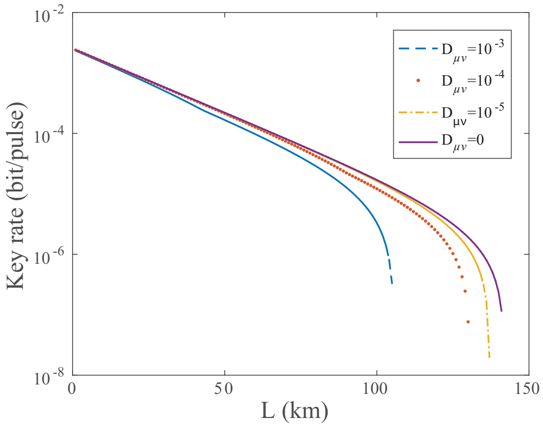

FIG. 5. Estimated key rate for different $D_{\mu\nu}$. The parameters used here are the same as in Fig. 2.

Conclusion.–In this work we show a side-channel in the time domain of decoy state modulation, and a corresponding PNS attack to hack this imperfect source. From a security proof point of view, we modify the decoy state model to consider a general imperfect source in which a signal state and a decoy state are distinguishable in any degrees of freedom. To improve the secure key rate, we test a hardware patch, and propose a theory modification.

[1] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).

[2] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, Nat. Commun. **5**, 3717 (2014).

[3] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, arXiv:1608.04220 [quant-ph].

[4] J. Bogdanski, N. Rafiei, and M. Bourennane, Phys. Rev. A **78**, 062307 (2008).

[5] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[6] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[7] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, New J. Phys. **11**, 065001 (2009).

[8] M.-S. Jiang, S.-H. Sun, C.-Y. Li, and L.-M. Liang, Phys. Rev. A **86**, 032310 (2012).

[9] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).

[10] K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).

[11] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[12] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).