Quantum hacking of two-way continuous-variable quantum key distribution using Trojan-horse attack*

Hong-Xin Ma(马鸿鑫)[1,2], Wan-Su Bao(鲍皖苏)[1,2,†], Hong-Wei Li(李宏伟)[1,2], and Chun Chou(周淳)[1,2]

[1] *PLA Information Engineering University, Zhengzhou* 450001, *China*

[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 12 February 2016; revised manuscript received 19 April 2016; published online 25 June 2016)

We present a Trojan-horse attack on the practical two-way continuous-variable quantum key distribution system. Our attack mainly focuses on the imperfection of the practical system that the modulator has a redundancy of modulation pulse-width, which leaves a loophole for the eavesdropper inserting a Trojan-horse pulse. Utilizing the unique characteristics of two-way continuous-variable quantum key distribution that Alice only takes modulation operation on the received mode without any measurement, this attack allows the eavesdropper to render all of the final keys shared between the legitimate parties insecure without being detected. After analyzing the feasibility of the attack, the corresponding countermeasures are put forward.

Keywords: quantum hacking, two-way, continuous-variable, quantum key distribution, Trojan-horse

PACS: 03.67.Hk, 03.67.–a, 03.67.Dd **DOI:** 10.1088/1674-1056/25/8/080309

1. Introduction

Quantum key distribution (QKD)[1] enables two authenticated users, Alice and Bob, to share secure private keys in the presence of eavesdroppers. Quantum physics allows for unconditionally secure communication through insecure communication channels. The QKD protocols are classified into two main classes: discrete-variable (DV)QKD[2–5] and continuous-variable (CV) QKD,[6–10] both of whose unconditional security have been proved in theory.[11–14] The first proposed QKD protocol[2] is based on discrete variables, such as the polarization of a single photon. In CVQKD, the information is encoded on the continuous variables, such as the position or momentum quadratures of coherent states. In recent years, CVQKD has received close attention in the research area of quantum communication. One of the most outstanding CVQKD protocols is the Gaussian-modulated coherent state protocol,[9] whose composable security has been fully proven.[15] This protocol has been experimentally demonstrated both in laboratory[16,17] and field tests.[18] In the last few years, the high-speed CVQKD has been experimentally demonstrated,[19] and the high-bit-rate CVQKD system over 50-km fiber channel has successfully passed the field tests.[20] Moreover, a recent work shows that the secure transmission of CVQKD can be extended to 150 km.[21]

In comparison to DVQKD, CVQKD has some advantages. On one hand, the modulation of continuous variables relies on Gaussian modulation of the light field quadratures, which is a mature technology in experiment. On the other hand, CVQKD can achieve higher detection efficiency, which may lead to higher bit rate of the secure key. Furthermore, most of the operation in CVQKD can be implemented efficiently by standard telecommunication networks and technologies that are currently available and in widespread use, which means CVQKD can be integrated into the current telecommunication networks by using well-established optical fiber networks and practical devices.

In spite of the above advantages, the general one-way CVQKD still has serious shortcomings. In the case of direct reconciliation, GG02 protocol has the limitation of 3 dB,[9] which means there is no secret key when channel attenuation exceeds 3 dB. Although people put forward the post-processing[22] and reverse reconciliation[16] method to overcome 3-dB limit, the problem that one-way CVQKD is susceptible to excessive noise has not yet been resolved. No matter if there is direct reconciliation or reverse reconciliation, secret key rate will be affected by excess noise obviously, which severely restricts the security transmission distance. In order to enhance the tolerable excess noise, Stefano Pirandola[23] first proposed the two-way CVQKD protocol, which overcomes 3-dB limit and tolerates more excess noise than one-way protocols. Furthermore, Alice only needs one modulator in the two-way CVQKD protocol, which makes the hardware requirements on Alice's side in two-way CVQKD protocol lower than the one in one-way protocol. This characteristic gives the two-way CVQKD protocol a unique advantage in

*Project supported by the National Basic Research Program of China (Grant No. 2013CB338002) and the National Natural Science Foundation of China (Grant Nos. 11304397 and 61505261).

†Corresponding author. E-mail: 2010thzz@sina.com

© 2016 Chinese Physical Society and IOP Publishing Ltd

the situation in which Alice can only equip a small number of devices.

Recently, breakthrough progress has been made the in the security analysis of the two-way CVQKD protocol in theory. Carlo Ottavini[24] proved the security of the two-way CVQKD protocol under coherent attacks in direct reconciliation. However, the practical QKD systems have imperfections that cannot satisfy the assumptions of ideal devices in theoretical security proofs. The imperfect devices in commercial quantum key distribution systems open security loopholes that an eavesdropper may exploit. In the two-way CVQKD protocol, Alice only takes modulation operation on the received mode without any measurement. Moreover, the modulator has a redundancy of modulation pulse-width in the practical system, which leaves loopholes for Eve to take an attack strategy. Based on the above two factors, we propose a Trojan-horse attack strategy on the two-way CVQKD protocol, which allows the eavesdropper to render all of the final keys shared between the legitimate parties insecure without being detected. We discuss the feasibility of this attack and suggest countermeasures to prevent such an attack.

The paper is organized as follows. In Section 2, the general two-way CVQKD protocol is briefly introduced followed by the proposed Trojan-horse attack strategy on the two-way CVQKD protocol in Section 3. In Section 4, the feasibility of the Trojan-horse attack strategy is analyzed in detail and the corresponding countermeasures are put forward. The conclusion is drawn in Section 5.

2. The general two-way CVQKD protocol

In the one-way CVQKD protocol, the quantum states encoding information is always sent by Alice and detected by Bob after passing through the quantum channel, where the signal source is only controlled by Alice. The two-way CVQKD protocol proposed by Stefano Pirandola broke the fixed thinking that the signal source should only be controlled by Alice, where the signal sources are symmetrically distributed on both sides of Alice and Bob. In their protocol, Bob initially sends a mode to Alice and Alice encodes her information by applying a random displacement operator to the received mode and sends it back to Bob, where Bob detects both his original mode and the received mode to decode Alice's modulations.

The procedure of implementing the general two-way CVQKD protocol with homodyne detection is illustrated in Fig. 1 and can be described as follows.

Step 1 Before the communication, Bob prepares EPR pairs with variance V, then he keeps one mode B_1 and sends the other mode B_1' to Alice through the forward quantum channel.

Step 2 Alice applies a random phase-space displacement operator $D(\alpha)$ on her received mode A_1 to encode her information, obtaining the mode A_2. Then she sends the mode A_2 back to Bob through the backward quantum channel. Note that $\alpha = (Q_A + \mathrm{i}P_A)/2$, where Q_A and P_A follow the Gaussian distribution with the variance of $V - 1$.

Step 3 Bob performs homodyne detections on both his original mode B_1 and received mode B_2 to obtain the variables x_{B_1} (or p_{B_1}) and x_{B_2} (or p_{B_2}), respectively.

Step 4 Alice and Bob implement the reconciliation and privacy amplification to obtain a string of identical keys that Eve does not know. In this step, Bob uses the measurement values of the modes B_1 and B_2 to construct the optimal estimation to Alice's corresponding variables Q_A (P_A).

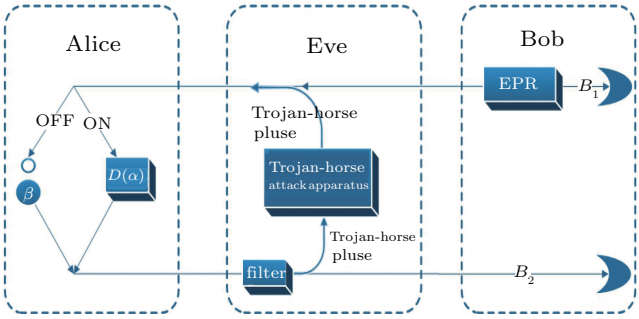


Fig. 1. (color online) The entanglement-based (EB) scheme of general two-way CVQKD protocol with homodyne detection.

3. Trojan-horse attack strategy on the two-way CVQKD system

Our attack mainly focuses on the imperfection in the practical system that the modulator has a redundancy of modulation pulse-width and the unique characteristics of two-way CVQKD systems that Alice only takes modulation operation on the received mode without any measurement. By implanting a Trojan-horse pulse, our proposed attack strategy can partially or fully obtain the information transmitted between the two legal communication sides without being detected. Our attack strategy can be divided into two parts, which is illustrated in the Eve part of Fig. 1.

Attack part 1 Eve intercepts the signal pulse sent by Bob in the forward channel and then implants a Trojan-horse pulse after the original signal pulse. Eve notes the time domain implanting Trojan-horse pulse and sends the processed pulse to Alice.

Attack part 2 After Alice modulates the received pulse, Eve intercepts the modulated pulse sent by Alice in the backward channel, picks up the modulated Trojan-horse pulse according to the time domain noted in part 1 and sends the remaining pulse to Bob. Then Bob takes homodyne detection on the quantum state of the extracted pulse. Combined with the

quadrature component of the implanted Trojan-horse pulse in part 1, Bob finally obtains the information encoded by Alice.

Here we need to note that the security of the general two-way CVQKD protocol against coherent attacks can be achieved by switching randomly between one-way (switch OFF, where Alice detects the incoming mode and sends a new state back to Bob) and two-way schemes (switch ON),[23] as shown in Fig. 1. When Alice switches OFF, the two-way CVQKD protocol turns into a one-way protocol, where we can take the existing Trojan-horse attacks strategy proposed by Khan[25] to hack the communication system. Our attack strategy mainly focuses on the situation that Alice switches ON, where the protocol performs truly two-way communication.

4. Feasibility analysis and Countermeasures

According to the attack steps and the loophole which is utilized, the feasibility of the Trojan-horse attack strategy is mainly based on the following three factors.

Firstly, in two-way CVQKD systems, Alice only takes modulation operation on the received mode without any measurement. Therefore, the Trojan-horse pulse implanted by Eve can smoothly enter the modulator of Alice's side without being detected. Secondly, for the convenience of operation in practical experiments, the modulation pulse-width of the modulator is always larger than the pulse-width of each signal pulse. Eve can make full use of the redundancy of modulation pulse-width to make the Trojan-horse pulse receiving the same modulation process as the original signal pulse, which is the linchpin of successfully eavesdropping the key information. Finally, throughout the attack process, Eve does not take any measurement operation on the original quantum signal, which means that Eve's behavior will not introduce any excess noise under ideal conditions.

According to the above three factors, we can conclude that Eve's attack cannot be detected by Alice and Bob. Meanwhile, the information hacked by Eve cannot be eliminated by Alice and Bob through the reconciliation and privacy amplification. Thence, the Trojan-horse attack strategy allows the eavesdropper to render all of the final keys shared between the legitimate parties insecure without being detected.

However, in practical operations, the added Trojan-horse pulse and original signal pulse may have crosstalk, which may affect the final secret key rate. In order to judge the attack impact of our Trojan-horse attack strategy, we need to quantitative describe the effect of crosstalk between the Trojan-horse pulse and original signal pulse. For simplicity in security analysis, we replace Alice's displacement operation with a beam splitter and EPR pairs,[26] which has been illustrated in Fig. 2. The transmission of the beam splitter is T_A. Here we denote the crosstalk as the excess noise introduced into the backward channel, which can be described in formula as $\chi_c = n_c\varepsilon\sqrt{T \cdot T_A}$, where n_c is the coefficient representing the degree of the crosstalk. For example, $n_c = 0$ represents that the Trojan-horse pulse and original signal pulse has no crosstalk.

The Gaussian attack is optical in the security analysis of two-way CVQKD protocol as the corresponding covariance matrix of the state $B_2B_1A_2A_1$ is known to Alice and Bob.[27] In the following security analysis, we note that the Eve mentioned is the one taking Gaussian collective attack instead of the one taking Trojan-horse attack.

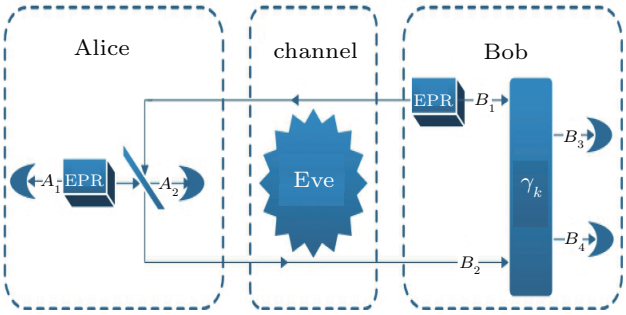


Fig. 2. (color online) The equivalent scheme to figure 1 with post processing when Alice is switched ON.

In Fig. 1, the final key rate of the two-way CVQKD protocol with homodyne detection in reverse reconciliation is[28]

$$K_R = \beta I_{BA} - \chi_{BE}, \tag{1}$$

where I_{BA} is the mutual information between Alice and Bob, χ_{BE} are the Holevo bounds between Bob and Eve, which put an upper limit on the information available to Eve on Bob's key. $\beta \in [0,1]$ is the reconciliation efficiency. The classical mutual information between Alice and Bob can be written as

$$I_{BA} = \frac{1}{2}\log_2 \frac{V_{A^M}}{V_{A^M|B}}, \tag{2}$$

where $V_{A^M} = (1/2)(V_A + 1)$ is Alice's variance, and $V_{A^M|B}$ is Alice's conditional variance on Bob, which can be obtained with Alice's and Bob's data. According to Holevo bound, χ_{BE} can be obtained as[29]

$$\chi_{BE} = S(\rho_E) - \int \mathrm{d}m_B\, p(m_B) S\left(\rho_E^{m_B}\right), \tag{3}$$

where S is the von Neumann entropy of the quantum state ρ. m_B represents the measurement of Bob, and it can take the form $m_B = x_B$ for a homodyne detector. $\rho_E^{m_B}$ is Eve's state conditional on Bob's measurement result, $p(m_B)$ is the probability density of the measurement.

Since the state $\rho_{B_2B_1A_2A_1E}$ is a pure state,

$$S(\rho_E) = S(\rho_{B_2B_1A_2A_1}).$$

As the entropy can be calculated from its corresponding covariance matrix for the Gaussian state,[30] the corresponding

covariance matrix of state $\rho_{B_2B_1A_2A_1}$ is obtained that

$$\gamma_{B_2B_1A_2A_1} = \begin{pmatrix} \gamma_{B_2} & C_1 & C_2 & C_3 \\ C_1 & V\boldsymbol{\Pi}_2 & C_4 & 0 \\ C_2 & C_4 & \gamma_{A_2} & C_5 \\ C_3 & 0 & C_5 & V_A\boldsymbol{\Pi}_2 \end{pmatrix}, \tag{4}$$

where $\boldsymbol{\Pi}_2$ is a 2×2 identity matrix, the diagonal elements stand for the variance quadratures of the mode B_2, B_1, A_2, A_1 in turn, and the nondiagonal elements stand for the convariance between these modes. For example,

$$\gamma_{B_2} = \mathrm{diag}\left(\langle x_{B_2}^2\rangle, \langle p_{B_2}^2\rangle\right), \quad C_1 = \mathrm{diag}\left(\langle x_{B_2}x_{B_1}\rangle, \langle p_{B_2}p_{B_1}\rangle\right).$$

Then Eve's von Neumann entropy can be obtained by

$$S(\rho_{B_2B_1A_2A_1}) = \sum_{i=1}^{4} G(\lambda_i) = \sum_{i=1}^{4} G\left(f_{\lambda_i}(\alpha_{mn})\right), \tag{5}$$

where $\lambda_i = f_{\lambda_i}(\alpha_{mn})$ is the symplectic eigenvalues of the covariance matrix $\gamma_{B_2B_1A_2A_1}$ characterizing the state $\rho_{B_2B_1A_2A_1}$, which is the function of element α_{mn} of $\gamma_{B_2B_1A_2A_1}$.[23] We have

$$G(\lambda_i) = \frac{\lambda_i+1}{2}\log\frac{\lambda_i+1}{2} - \frac{\lambda_i-1}{2}\log\frac{\lambda_i-1}{2}. \tag{6}$$

For simplicity to calculate the final key rate, we apply a symplectic transformation γ_k to the modes B_2 and B_1, obtaining the modes B_4 and B_3, which is illustrated in Fig. 2. Then we can get m_B by measuring the quadrature of B_4 (or B_3). The corresponding covariance matrix of the state $\rho_{B_4B_3A_2A_1}$ is

$$\gamma_{B_4B_3A_2A_1} = [\gamma_k \oplus \boldsymbol{\Pi}_4]\,\gamma_{B_2B_1A_2A_1}\,[\gamma_k \oplus \boldsymbol{\Pi}_4]^{\mathrm{T}}, \tag{7}$$

where $\boldsymbol{\Pi}_4 = \oplus_1^4\boldsymbol{\Pi}$, γ_k is a continuous-variable C-NOT gate:[31]

$$\gamma_k = \begin{pmatrix} 1 & 0 & -k & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & k & 0 & 1 \end{pmatrix}. \tag{8}$$

As the symplectic transformation γ_k does not change the von Neumann entropy of the state $\rho_{B_2B_1A_2A_1}$, Eve's von Neumann entropy and conditional von Neumann entropy on Bob in Fig. 2 is equivalent to those in Fig. 1. As the state $\rho_{B_3A_2A_1E}$ is a pure state when Bob obtains m_B by measuring the quadrature of B_4, we have

$$S(\rho_{\mathrm{E}}^{m_B}) = S(\rho_{B_3A_2A_1}^{m_B}).$$

The corresponding covariance matrix of the state $S(\rho_{B_3A_2A_1})$ conditioned on m_B is[32]

$$\gamma_{B_3A_2A_1}^{m_B} = \gamma_{B_3A_2A_1} - C_{B_4}[X_x\gamma_{B_4}X_x]^{MP}C_{B_4}, \tag{9}$$

where $X_x = \mathrm{diag}(1,0)$, C_{B_4} is their correlation matrix, MP denotes the inverse on the range $\gamma_{B_3A_2A_1}$ and γ_{B_4} are the corresponding reduced matrixes of the states $\rho_{B_3A_2A_1}$ and ρ_{B_4} in $\rho_{B_4B_3A_2A_1}$. Similar to Eq. (5), we obtain

$$S(\rho_{B_3A_2A_1}^{m_B}) = \sum_{i=1}^{3} G(\lambda'_i) = \sum_{i=1}^{3} G\left(f_{\lambda'_i}(\alpha'_{mn})\right), \tag{10}$$

where $\lambda' = f_{\lambda'_i}(\alpha'_{mn})$ is the symplectic eigenvalue of $\gamma_{B_3A_2A_1}^{m_B}$, which is the function of the element α'_{mn} of $\gamma_{B_3A_2A_1}^{m_B}$. It can be found that the von Neumann conditional entropy $S(\rho_{B_3A_2A_1}^{m_B})$ does not depend on Bob's measurement m_B. Therefore, the Holevo bound χ_{BE} is simply equal to

$$\chi_{\mathrm{BE}} = S(\rho_{B_2B_1A_2A_1}) - S(\rho_{B_3A_2A_1}^{m_B}). \tag{11}$$

Then the final key rate is obtained

$$K_{\mathrm{R}} = \beta\frac{1}{2}\log_2\frac{V_{A^M}}{V_{A^M|B}} - \sum_{i=1}^{4} G\left(f_{\lambda_i}(\alpha_{mn})\right) + \sum_{i=1}^{3} G\left(f_{\lambda'_i}(\alpha'_{mn})\right). \tag{12}$$

In practice, Alice and Bob calculate α_{mn} and α'_{mn} by measuring the variance quadratures of the mode B_2, B_1, A_2, A_1. For simplicity, we assume that the forward and backward channels are independent and linear with the same transmittances T. The noise referred to the input is $\chi_1 = (1-T)/T + \varepsilon$, where ε is the channel excess noises referred to the input. Because we assume the crosstalk between Trojan-horse pulse and original signal pulse as the noise introduced into the backward channel, which is formulated as $\chi_{\mathrm{c}} = n_{\mathrm{c}}\varepsilon\sqrt{T\cdot T_A}$, the noise referred to the input of the backward channel is

$$\chi_2 = \chi_1 + \chi_{\mathrm{c}} = \chi_1 + n_{\mathrm{c}}\varepsilon\sqrt{T\cdot T_A}. \tag{13}$$

We can calculate the elements of Eq. (4),

$$\begin{aligned} \gamma_{B_2} &= \{1 + T[V_A - T_AV_A + TT_A(V+\chi_1) + \chi_2]\}\boldsymbol{\Pi}_2, \\ \gamma_{A_2} &= [T_AV_A + T_1(1-T_A)(V+\chi_1)]\boldsymbol{\Pi}_2, \\ C_1 &= T\sqrt{T_A(V^2-1)}\sigma_z, \\ C_2 &= [V_A - T(V+\chi_1)]\sqrt{T(1-T_A)T_A}\boldsymbol{\Pi}_2, \\ C_3 &= \sqrt{T(1-T_A)({V_A}^2-1)}\sigma_z, \\ C_4 &= -\sqrt{T(1-T_A)(V^2-1)}\sigma_z, \\ C_5 &= \sqrt{T_A({V_A}^2-1)}\sigma_z, \end{aligned} \tag{14}$$

and

$$I_{BA} = \frac{1}{2}\log_2\frac{1 + T^2T_AH + T(V_A - T_AV_A + \chi_2)}{1 + T^2T_AH + T(1 - T_A + \chi_2)}, \tag{15}$$

where

$$\sigma_z = \mathrm{diag}(1,-1), \quad H = \chi_1 + 2V - 2\sqrt{V^2-1},$$

T_A is the transmittance of the beam splitter on Alice's side in Fig. 2.

When $n_c = 0$, there is no crosstalk between the Trojan-horse pulse and original signal pulse, which means that the operation of Trojan-horse attack does not introduce any excess noise in the communication. Figure 3 shows the "secret key rate" of the two-way CVQKD protocol against Trojan-horse attack as a function of the transmittance. The "secret key rate" is the final key rate shared between the legitimate parties, which is rendered totally insecure by the Trojan-horse attacker. Clearly, the "secret key rate" decreases with the increase of n_c. However, the legitimate parties cannot detect the existence of the Trojan-horse attacker through the variation of the "secret key rate". The reason is as follows: The observable result introduced by crosstalk between the Trojan-horse pulse and original signal pulse is the enlargement of excess noise. However, the source of the increased excess noise is blind for legitimate parties. They do not know where the increased excess noise comes from, maybe due to the imperfection of the device, or because of a mutation in the surrounding environment. The only requirement to consider during the attack is the "secret key rate" should be positive. Only in this situation can the communication between Alice and Bob be realized successfully, and Eve can effectively obtain the key information through the Trojan-horse attack.

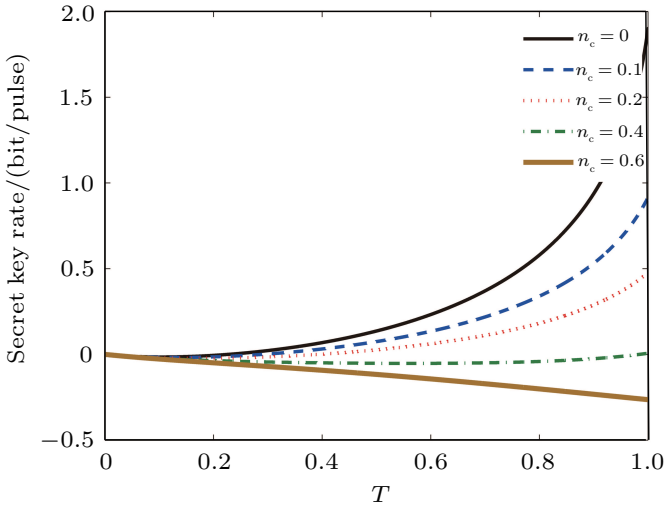


Fig. 3. (color online) "Secret key rate" of the two-way CVQKD protocol against Trojan-horse attack as a function of the transmittance of the channel for $n_c = 0, 0.1, 0.2, 0.4, 0.6$. The curve is plotted for $V = V_A = 16$, $\varepsilon = 0.65$, $\beta = 0.9$, $T_A = 0.7$.

From Fig. 3 we can find that the final key becomes negative when $n_c \geq 0.4$, which means that the legitimate parties share nothing about the final key at this moment. This makes our attack lose the original impact. In order to carry out the Trojan-horse attack more viably and efficiently, we need to cut down the crosstalk between the Trojan-horse pulse and original signal pulse, bringing $0 \leq n_c < 0.4$. The most effective solution is making the wavelength of the Trojan-horse pulse different from the one of the original signal pulse.

To prevent the Trojan-horse attack, the most efficient way is monitoring and removing the Trojan pulse. In one-way CVQKD system, installing isolators and wavelength filters on Bob's side have been the most suitable countermeasures against Trojan-horse attack.[33,34] However in the two-way CVQKD system, the former one cannot be used, which will hinder the normal communication. But the latter one can certainly be useful. Therefore, the technical countermeasure specifically for the two-way CVQKD system is as follows: Bob implants a tag frame into the original signal pulse every time interval t, and a waveform detector is added before the modulator on Alice's side, which is used to detect the tag frames. When the signal pulse passes through the waveform detector, Alice records the time interval between every two adjacent tag frames. If the time interval is t, the pulse between the two tag frames is reserved into the modulator; otherwise, the pulse is removed. This countermeasure can effectively eliminate the Trojan pulse, but it will also increase the complexity of the devices on Alice's side, which weakens the superiority of two-way CVQKD system.

5. Conclusion

In conclusion, the Trojan-horse attack on the two-way CVQKD system is proposed by inserting a Trojan-horse pulse into the original signal pulse. If the legitimate users do not take any necessary countermeasures, the final secret key will be totally insecure under this attack, where the attacker can obtain all the information about the final key without being detected. After analyzing the feasibility of the attack, we give the limitation of successfully carrying out the attack. Finally, a technical countermeasure is provided to resist the Trojan-horse attack on the two-way CVQKD system.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, p. 175
[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[4] Bennet C H 1992 *Phys. Rev. Lett.* **68** 3121
[5] Chen M and Liu X 2011 *Chin. Phys. B* **20** 100305
[6] Ralph T C 1999 *Phys. Rev. A* **61** 010303
[7] Hillery M 2000 *Phys. Rev. A* **61** 022309
[8] Zhao J, Guo X, Wang X, Wang N, Li Y and Peng K 2013 *Chin. Phys. Lett.* **30** 60302
[9] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[10] Wang X, Bai Z, Wang S, Li Y and Peng K 2013 *Chin. Phys. Lett.* **30** 010305
[11] Lo H K and Chau H F 1999 *Science* **283** 2050
[12] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[13] Yang W, Bao W, Li H, Zhou C and Li Y 2014 *Chin. Phys. B* **23** 080303
[14] Leverrier A, Garcia-Patron R, Renner R and Cerf N J 2013 *Phys. Rev. Lett.* **110** 030502
[15] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501
[16] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238

[17] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nat. Photon.* **7** 378
[18] Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouri R and Grangier P 2009 *New. J. Phys.* **11** 045023
[19] Huang D, Lin D, Wang C, Liu W, Fang S, Peng J, Huang P and Zeng G 2015 *Opt. Express* **23** 17511
[20] Wang C, Huang D, Huang P, Lin D, Peng J and Zeng G 2015 *Sci. Rep.* **5** 14607
[21] Huang D, Huang P, Lin D and Zeng G 2016 *Sci. Rep.* **6** 19201
[22] Silberhorn C, Ralph T C, Lutkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901
[23] Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 *Nat. Phys.* **4** 726
[24] Ottaviani C, Mancini S and Pirandola S 2015 *Phys. Rev. A* **92** 062323
[25] Khan I, Jain N, Stiller B, Jouguet P, Kunz-Jacques S, Diamanti E, Marquardt C and Leuchs G, 2014 *QCrypt* 2014, Paris, France, pp. 1–5
[26] Sun M, Peng X, Shen Y and Guo H 2012 *Int. J. Quantum Infor.* **10** 1250059
[27] Garcéa-Patron R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[28] Leverrier A, Alleaume R, Boutros J, Zéemor G and Grangier P 2008 *Phys. Rev. A* **77** 042325
[29] Weedbrook C, Pirandola S, Garcéa-Patron R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
[30] Serafini A 2006 *Phys. Rev. Lett.* **96** 110402
[31] Yoshikawa J I, Miwa Y, Huck A, Andersen U L, van Loock P and Furusawa A 2008 *Phys. Rev. Lett.* **101** 250501
[32] Eisert J and Plenio M B 2003 *Int. J. Quantum Infor.* **1** 479
[33] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C and Leuchs G 2014 *New J. Phys.* **16** 123030
[34] Jain N, Stiller B, Khan I, Makarov V, Marquardt C and Leuchs G 2015 *IEEE J. Selec. Top. Quantum Electron.* **21** 168