optica

Robust countermeasure against detector control attack in practical quantum key distribution system: supplementary material

YONG-JUN QIAN[1,2,3,†], DE-YONG HE[1,2,3,†], SHUANG WANG[1,2,3,*], WEI CHEN[1,2,3], ZHEN-QIANG YIN[1,2,3], GUANG-CAN GUO [1,2,3], AND ZHENG-FU HAN[1,2,3]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*
[2] *CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*
[3] *State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China*
[*] *Corresponding author:wshuang@ustc.edu.cn*
[†] *These authors contributed equally to this work*

Published 11 September 2019

This document provides supplementary information to "Robust countermeasure against detector control attack in practical quantum key distribution system," https://doi.org/10.1364/optica.6.001178.

1. ANALYSIS OF THE DIFFERENCE OF VA'S VALUE

Here we explain the reason why the VA's value should differ 3 dB. Assume that the attenuation value of VA in each VA-SPD is randomly set to $x\ dB$ and $y\ dB$ ($x < y$). As mentioned above in Sec. II, after the announcement of basis choices, $\{R_x, R_y\}$ and $\{e_x, e_y\}$ denotes the detection rates and QBERs with $x\ dB$ and $y\ dB$, respectively. For the QKD system in normal operation, the ratio between detection rates of one VA-SPD with $x\ dB$ and $y\ dB$ attenuation satisfies

$$\alpha^* = \frac{R_x}{R_y} > 1, \tag{S1}$$

similarly, the QBERs with $x\ dB$ and $y\ dB$ attenuation should be less than the threshold. We get

$$\{e_x, e_y\} < e_{th}. \tag{S2}$$

In detector control attack without blinding light, $P_{f,x}$ is defined as the detection probability with full optical power when the attenuation is $x\ dB$. $P_{f,y}$ is likewise defined when the attenuation is $y\ dB$; similarly, with half power, $P_{h,x}$ and $P_{h,y}$ are defined as the detection probabilities when the attenuation are $x\ dB$ and $y\ dB$, respectively. Suppose Eve select two measurement basis with equal probability. Then the detection rates with two attenuation values can be given by

$$R_x^{atk} = \frac{1}{4}P_{f,x} + \frac{1}{4}(2P_{h,x}), \tag{S3}$$

$$R_y^{atk} = \frac{1}{4}P_{f,y} + \frac{1}{4}(2P_{h,y}). \tag{S4}$$

For simplicity, we analyse the case that both VA-SPDs have the same attenuation value ($x\ dB$ or $y\ dB$). Then the QBERs of Bob's one VA-SPD with $x\ dB$ and $y\ dB$ attenuation values are given by

$$e_{x(s)}^{atk} = \frac{2P_{h,x} - P_{h,x}^2}{2P_{f,x} + 2(2P_{h,x} - P_{h,x}^2)}, \tag{S5}$$

$$e_{y(s)}^{atk} = \frac{2P_{h,y} - P_{h,y}^2}{2P_{f,y} + 2(2P_{h,y} - P_{h,y}^2)}. \tag{S6}$$

By substituting Eq. (S3)–Eq. (S4) into the Eq. (S5)–Eq. (S6) respectively, we get

$$2P_{h,x} - P_{h,x}^2 < 2\alpha^* e_{th}(P_{f,y} + 2P_{h,y}) - 2e_{th}P_{h,x}^2, \tag{S7}$$

$$\alpha^*(2P_{h,y} - P_{h,y}^2) < 2\alpha^* e_{th}(P_{f,y} + 2P_{h,y} - P_{h,y}^2). \tag{S8}$$

By adding both sides of these inequalities, we deduce that

$$\begin{aligned}(2P_{h,x} - P_{h,x}^2) - 4\alpha^* e_{th} P_{f,y} + \alpha^*(2 - P_{h,y} - 8e_{th})P_{h,y} +\\ 2e_{th}P_{h,x}^2 + 2\alpha^* e_{th} P_{h,y}^2 < 0.\end{aligned} \tag{S9}$$

As $e_{th} < 11\%$, $0 \le \{P_{f,x},\ P_{h,x},\ P_{f,y},\ P_{h,y}\} \le 1$ and $\alpha^* > 1$, we know that $(2P_{h,x} - P_{h,x}^2) + \alpha^*(2 - P_{h,y} - 8e_{th})P_{h,y} + 2e_{th}P_{h,x}^2 + 2\alpha^* e_{th}P_{h,y}^2 \ge 0$, $-4\alpha^* e_{th} P_{f,y} \le 0$. To make an effective countermeasure criteria, It should be guaranteed that Eq. (S9) can not be satisfied for all the values of α^*, there are two following cases:

If $P_{h,x} \neq P_{f,y}$, whether the Eq. (S9) can be satisfied depends on the value of $P_{h,x}$, $P_{f,y}$, α^* and $P_{h,y}$, which means that the countermeasure criteria is not general.

If $P_{h,x} = P_{f,y}$, then $(2P_{h,x} - P_{h,x}^2) - 4\alpha^* e_{th} P_{f,y} \geq 0$, all the factors on the left of Eq. (S9) is greater than 0, which is contradictory to the right result of Eq. (S9). It means the two sub-cases: The one is the optical power before entering SPDs are equal, then half power with $x\ dB$ is equal to the full power with $y\ dB$, so the difference of VA's value between y and x is $3\ dB$. It meets the requirement of generalization of criteria; The other one is the optical power before entering SPDs are different, but their detection probabilities are equal. Therefore, the countermeasure is influenced by the specific detector probabilities and is not general.

2. CALCULATION PROCESS IF ONE RELATIONSHIP IS SATISFIED

When both VA-SPDs in the same basis have the same attenuation value, and in the case that both QBERs ($e_{0(s)}^{atk}$ and $e_{3(s)}^{atk}$) are less than e_{th} (Eq. (3) is satisfied), in order to deduce the range of $\frac{R_{0(s)}^{atk}}{R_{3(s)}^{atk}}$, let $\frac{1}{2e_{0(s)}^{atk}} - 1 = m_1$, $\frac{1}{2e_{3(s)}^{atk}} - 1 = m_2$. Then Eqs. (6) and (7) can be converted into

$$P_{f,0} = m_1(2P_{h,0} - P_{h,0}^2), \tag{S10}$$

$$P_{f,3} = m_2(2P_{h,3} - P_{h,3}^2). \tag{S11}$$

With $0 \leq P_{f,0} \leq 1$ and $P_{h,0} = P_{f,3}$ we get

$$0 \leq P_{h,0} \leq 1 - \sqrt{1 - \frac{1}{m_1}}. \tag{S12}$$

Then $\frac{R_{0(s)}^{atk}}{R_{3(s)}^{atk}}$ is given by

$$\frac{R_{0(s)}^{atk}}{R_{3(s)}^{atk}} = \frac{m_1(2P_{h,0} - P_{h,0}^2) + 2P_{h,0}}{P_{h,0} + 2 - 2\sqrt{1 - \frac{P_{h,0}}{m_2}}}. \tag{S13}$$

Define $m = \min\{m_1, m_2\}$, then $m \geq \frac{1}{2e_{th}} - 1$. Let $1 - \sqrt{1 - \frac{1}{m}} = x$, with Eq. (S12) we have

$$\frac{R_{0(s)}^{atk}}{R_{3(s)}^{atk}} \geq \frac{m(2x - x^2) + 2x}{x + 2 - 2\sqrt{1 - \frac{x}{m}}}. \tag{S14}$$

We can simulate the lower bound of $\frac{R_{0(s)}^{atk}}{R_{3(s)}^{atk}}$, the result is shown with the red line in Fig. 2.

Similarly, when both VA-SPDs in the same basis have the opposite attenuation value, and both QBERs ($e_{0(opp)}^{atk}$ and $e_{3(opp)}^{atk}$) are less than e_{th}, let $\frac{1}{2e_{0(opp)}^{atk}} - 1 = m_3$, $\frac{1}{2e_{3(opp)}^{atk}} - 1 = m_4$. Then Eqs. (12) and (13) can be converted into

$$P_{f,0} = m_3(2P_{h,0} - P_{h,0}P_{h,3}), \tag{S15}$$

$$P_{f,3} = m_4(2P_{h,3} - P_{h,0}P_{h,3}). \tag{S16}$$

With Eq. (S16), we get $P_{h,0} = \frac{2m_4 P_{h,3}}{1 + m_4 P_{h,3}}$, substitute it in Eq. (S15), as $0 \leq P_{f,0} \leq 1$, we have

$$0 \leq \frac{2P_{h,3} - P_{h,3}^2}{1 + m_4 P_{h,3}} \leq \frac{1}{2m_3 m_4}. \tag{S17}$$

Then we get the range of $P_{h,3}$

$$0 \leq P_{h,3} \leq \frac{4m_3m_4 - m_4 - \sqrt{(4m_3m_4 - m_4)^2 - 8m_3m_4}}{4m_3m_4}. \tag{S18}$$

Then $\frac{R_{0(opp)}^{atk}}{R_{3(opp)}^{atk}}$ is given by

$$\frac{R_{0(opp)}^{atk}}{R_{3(opp)}^{atk}} = \frac{m_3m_4(2 - P_{h,3}) + 2m_4}{m_4 + 1 + m_4 P_{h,3}}. \tag{S19}$$

Define $m = \min\{m_3, m_4\}$, then $m \geq \frac{1}{2e_{th}} - 1$, we have

$$\frac{R_{0(opp)}^{atk}}{R_{3(opp)}^{atk}} \geq \frac{4m^2 + 9m + m\sqrt{16m^2 - 8m - 7}}{8m + 3 - \sqrt{16m^2 - 8m - 7}}. \tag{S20}$$

We simulate the lower bound of $\frac{R_{0(opp)}^{atk}}{R_{3(opp)}^{atk}}$, the result is shown with the blue dashed line in Fig. 2.

Under the detector control attack, since Eve could control transmittance and number of trigger pulses to guarantee the detection rates unchanged, t is the attack transmission parameter which satisfies $t \geq 1$, then we have

$$R_0^{atk} = tR_0. \tag{S21}$$

In the case that the relationship of Eq. (2) is satisfied, Eq. (4) and Eq. (5) can be converted into

$$P_{f,0} + 2P_{h,0} = 4tR_0, \tag{S22}$$

$$P_{f,3} + 2P_{h,3} = \frac{4tR_0}{\alpha}. \tag{S23}$$

As $0 \leq \{P_{f,0},\ P_{h,0},\ P_{f,3},\ P_{h,3}\} \leq 1$, by using Eq. (S22) and Eq. (S23), we have

$$0 \leq tR_0 \leq 0.75. \tag{S24}$$

When both VA-SPDs in the same basis have the same attenuation value, then $e_{0(s)}^{atk}$, $e_{3(s)}^{atk}$ can be converted into

$$e_{0(s)}^{atk} = \frac{2P_{h,0} - P_{h,0}^2}{8tR_0 - 2P_{h,0}^2}, \tag{S25}$$

$$e_{3(s)}^{atk} = \frac{2P_{h,3} - P_{h,3}^2}{\frac{8tR_0}{\alpha} - 2P_{h,3}^2}. \tag{S26}$$

According Eq. (S26) and Eq. (S23), we get

$$P_{f,3} = P_{h,0} = \frac{1 + \frac{4tR_0}{\alpha} e_{3(s)}^{atk} - \frac{2tR_0}{\alpha}}{e_{3(s)}^{atk} - \frac{1}{2}} - \frac{\sqrt{(1 + \frac{4tR_0}{\alpha} e_{3(s)}^{atk} - \frac{2tR_0}{\alpha})^2 + 2(e_{3(s)}^{atk} - \frac{1}{2})^2(\frac{8tR_0}{\alpha} - 8(\frac{tR_0}{\alpha})^2)}}{e_{3(s)}^{atk} - \frac{1}{2}}, \tag{S27}$$

thus we substitute Eq. (S27) to Eq. (S25). We can simulate the relationship of the QBERs with $0\ dB$ ($e_{0(s)}^{atk}$) and $3\ dB$ ($e_{3(s)}^{atk}$), we set $tR_0 = 0.75$ for Eq. (S24), because $e^{atk}_{0(s)}$ and $e^{atk}_{3(s)}$ are increasing with decreasing tR_0. If Eq. (S27) is larger than 1 (smaller than 0), we take 1(0) for $P_{f,3}$. The result is shown with red and blue lines in Fig. 2.

Similarly, when both VA-SPDs in the same basis have the opposite attenuation value, $e^{atk}_{0(opp)}$, $e^{atk}_{3(opp)}$ can be converted into

$$e^{atk}_{0(opp)} = \frac{2P_{h,0} - P_{h,0}P_{h,3}}{8tR_0 - 2P_{h,0}P_{h,3}}, \tag{S28}$$

$$e^{atk}_{3(opp)} = \frac{2P_{h,3} - P_{h,0}P_{h,3}}{\frac{8tR_0}{\alpha} - 2P_{h,0}P_{h,3}}. \tag{S29}$$

According Eq. (S23) and Eq. (S29), we get $P_{h,3} = \frac{2tR_0}{\alpha} - \frac{1}{2}P_{f,3}$.

$$P_{f,3} = P_{h,0} = \frac{\frac{2tR_0}{\alpha} + 1 - \frac{4tR_0}{\alpha}e^{atk}_{3(opp)}}{1 - 2e^{atk}_{3(opp)}} - \frac{\sqrt{(\frac{4tR_0}{\alpha}e^{atk}_{3(opp)} - \frac{2tR_0}{\alpha} - 1)^2 - 4(e^{atk}_{3(opp)} - \frac{1}{2})^2(\frac{8tR_0}{\alpha})}}{1 - 2e^{atk}_{3(opp)}}. \tag{S30}$$

Take these equation to Eq. (S28). We can simulate the relationship of the QBERs with 0 dB ($e^{atk}_{0(opp)}$) and 3 dB ($e^{atk}_{3(opp)}$), we set $tR_0 = 0.75$ for Eq. (S24), because $e^{atk}_{0(opp)}$ and $e^{atk}_{3(opp)}$ are increasing with decreasing tR_0. Similarly, if Eq. (S27) is larger than 1(smaller than 0), we take 1(0) for $P_{f,3}$. The result is shown with red and blue dashed lines in Fig. 3.