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

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

\textsuperscript{1}CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China
\textsuperscript{2}CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
\textsuperscript{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

\[ \alpha^* = \frac{R_x}{R_y} > 1, \]  

(S1)

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

\[ |e_x, e_y| < e_{th}. \]  

(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

\[ R_{x}^{atk} = \frac{1}{4} P_{f,x} + \frac{1}{4} (2 P_{h,x}), \]  

(S3)

\[ R_{y}^{atk} = \frac{1}{4} P_{f,y} + \frac{1}{4} (2 P_{h,y}). \]  

(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

\[ e_{x}(S) = \frac{2 P_{h,x} - P_{h,x}^2}{2 P_{f,x} + 2 (2 P_{h,x} - P_{h,x}^2)}, \]  

(S5)

\[ e_{y}(S) = \frac{2 P_{h,y} - P_{h,y}^2}{2 P_{f,y} + 2 (2 P_{h,y} - P_{h,y}^2)}. \]  

(S6)

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

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

(S7)

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

(S8)

By adding both sides of these inequalities, we deduce that

\[ (2 P_{h,x} - P_{h,x}^2) - 4 \alpha^* e_{th} P_{f,y} + \alpha^* (2 - P_{h,y} - 8 e_{th}) P_{h,y} + 2 e_{th} P_{h,x}^2 + 2 \alpha^* e_{th} P_{h,y}^2 \geq 0, \]  

(S9)

As \(e_{th} < 11\%\), \(0 \leq \{P_{f,x}, P_{h,x}, P_{f,y}, P_{h,y}\} \leq 1\) and \(\alpha^* > 1\), we know that \((2 P_{h,x} - P_{h,x}^2) + \alpha^* (2 - P_{h,y} - 8 e_{th}) P_{h,y} + 2 e_{th} P_{h,x}^2 + 2 \alpha^* e_{th} P_{h,y}^2 \geq 0, -4 \alpha^* e_{th} P_{f,y} \leq 0\). To make an effective countermeasure criteria, It should be guaranteed that Eq. (S9) cannot be satisfied for all the values of \(\alpha^*\), 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 $P_{h,x}$, $P_{f,y}$, $\alpha^*$ and $P_{h,y}$, which means that the countermeasure criteria is not general.

If $P_{h,x} = P_{f,y}$, then $(2P_{h,x} - P_{h,x}^2) - 4a^*e_{ih}P_{f,y} \geq 0$, 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 half power with $x$ dB, with Eq. (S12) we have

\[
0 \leq \frac{2P_{h,x} - P_{h,x}^2}{1 + m_4P_{h,x}^2} \leq \frac{1}{2m_3m_4}.
\]  

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

\[
0 \leq P_{h,x} \leq 4m_3m_4 - m_4 - \sqrt{(4m_3m_4 - m_4)^2 - 8m_3m_4}.
\]  

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

\[
\frac{R_{3(opp)}^\text{atk}}{R_{3(opp)}^\text{atk}} = \frac{m_3m_4(2 - P_{h,x}) + 2m_4}{m_4 + 1 + m_4P_{h,x}}.
\]  

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

\[
R_{3(opp)}^\text{atk} = tR_0.
\]  

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

\[
P_{f,0} + 2P_{h,0} = 4R_0,
\]  

\[
P_{f,3} + 2P_{h,3} = \frac{4R_0}{\alpha}.
\]  

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

\[
0 \leq tR_0 \leq 0.75.
\]  

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

\[
e_{\text{atk}}^\text{0(s)} = \frac{2P_{h,0} - P_{h,0}^2}{8R_0 - 2P_{h,0}},
\]  

\[
e_{\text{atk}}^\text{3(s)} = \frac{2P_{h,3} - P_{h,3}^2}{8R_0 - 2P_{h,3}}.
\]  

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

\[
P_{f,3} = P_{h,0} = 1 + \frac{4tR_0}{\alpha}e_{\text{atk}}^\text{3(s)} - \frac{2tR_0}{\alpha^2}.
\]  

\[
0 \leq \left(1 + \frac{4tR_0}{\alpha}e_{\text{atk}}^\text{3(s)} - \frac{2tR_0}{\alpha^2}\right)^2 + 2(\frac{e_{\text{atk}}^\text{3(s)}}{2})^2\frac{8tR_0}{\alpha^2} - 8(tR_0)^2.
\]  

thus we substitute Eq. (S27) to Eq. (S25). We can simulate the relationship of the QBERs with $0 dB (e_{\text{atk}}^\text{0(s)})$ and $3 dB (e_{\text{atk}}^\text{3(s)})$, we
set $tR_0 = 0.75$ for Eq. (S24), because $e_{atk}^{0(\text{opp})}$ and $e_{atk}^{3(\text{opp})}$ 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, $e_{atk}^{0(\text{opp})}$, $e_{atk}^{3(\text{opp})}$ can be converted into

$$e_{atk}^{0(\text{opp})} = \frac{2P_{h,0} - P_{h,0}P_{h,3}}{8tR_0 - 2P_{h,0}P_{h,3}}, \quad (S28)$$

$$e_{atk}^{3(\text{opp})} = \frac{2P_{h,0} - P_{h,0}P_{h,3}}{8tR_0 - 2P_{h,0}P_{h,3}}. \quad (S29)$$

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

$$P_{f,3} = P_{h,0} = \frac{2tR_0}{a} + 1 - \frac{4tR_0}{a}e_{atk}^{3(\text{opp})}$$

$$= \sqrt{\left(\frac{2tR_0}{a}e_{atk}^{3(\text{opp})} - \frac{2tR_0}{a} - 1\right)^2 - 4\left(e_{atk}^{3(\text{opp})} - \frac{1}{2}\right)^2 \left(\frac{8tR_0}{a}\right)^2}.$$  \quad (S30)

Take these equation to Eq. (S28). We can simulate the relationship of the QBERs with $0\,\text{dB}$ ($e_{atk}^{0(\text{opp})}$) and $3\,\text{dB}$ ($e_{atk}^{3(\text{opp})}$), we set $tR_0 = 0.75$ for Eq. (S24), because $e_{atk}^{0(\text{opp})}$ and $e_{atk}^{3(\text{opp})}$ 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.