Supplementary material: Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol

Akihiro Mizutani,[1] Kiyoshi Tamaki,[2] Rikizo Ikuta,[1] Takashi Yamamoto,[1] and Nobuyuki Imoto[1]

[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *NTT Basic Research Laboratories, NTT Corporation,*
3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan

I. DETAILS OF THE SIMULATION

Here we describe the details of our simulation. The quantum efficiency and the dark counting of the detectors are $\eta = 0.045$ and $d = 8.5 \times 10^{-7}$, respectively. The loss coefficient of the quantum channel is $\xi = 0.21$dB/km. We denote $a = \cos(\pi/8)$ and $b = \sin(\pi/8)$. We define that $p_{i,ab}^{(n,m)}$ is a probability that the photons are detected as the successful event of Type i conditioned that Alice and Bob emit n and m photons in the states $|\varphi_a\rangle$ and $|\varphi_b\rangle$ for $a, b = 0, \dots, 3$, respectively. $q_{i,ab}$ is the probability of the successful detection of Type i conditioned that Alice and Bob emit photons in $|\varphi_a\rangle$ and $|\varphi_b\rangle$, respectively. Assuming that Eve is in the middle of Alice and Bob, the channel transmittance to Eve from Alice is the same as that from Bob. Denoting that l is the distance between Alice and Bob, the channel transmittance for Alice and Bob is

$$T = 10^{-\xi 0.5l/10}. \tag{1}$$

In the following, we give the experimental data for the simulation (i) when Eve postselects the events with $n \leq 1$ and $m \leq 1$ by the QND measurement before mixing the pulses from Alice and Bob (see Fig. 2(a)), and (ii) when Alice and Bob use quasi single photon sources by the SPDC (see Fig. 2(b)).

A. Case (i) Eve performs the QND measurement.

Each of Alice and Bob uses a phase randomized weak coherent pulse with the mean photon number of μ. The probability p_n for n-photon emission is

$$p_n(\mu) = e^{-\mu}\frac{\mu^n}{n!}. \tag{2}$$

For later use, we define the equations

$$\begin{aligned} f_1 &= (1-d)^2(2\eta^2a^2b^2(1+3d) + 2\eta(1-\eta)d + 2(1-\eta)^2d^2), & (3)\\ f_2 &= f_1 - (1-d)^2 2a^2b^2\eta^2, & (4)\\ f_3 &= (1-d)^2(\eta d + 2(1-\eta)d^2), & (5)\\ f_4 &= (1-d)^2 2d^2, & (6)\\ f_5 &= (1-d)^2(2\eta^2a^2b^2(1+d) + 2\eta(1-\eta)d + 2(1-\eta)^2d^2). & (7) \end{aligned}$$

In the following, we give $Q_i^{(n,m)}$ and $e_{\mathrm{i,bit}}^{(n,m)}$.

For Type1, we have

$$\begin{aligned} Q_1^{(1,1)} &= p_1^2(\mu)(2p_{1,00}^{(1,1)} + p_{1,01}^{(1,1)} + p_{1,12}^{(1,1)})/4, & (8)\\ e_{1,\mathrm{bit}}^{(1,1)} &= p_1^2(\mu)p_{1,00}^{(1,1)}/(2Q_1^{(1,1)}), & (9)\\ Q_1^{(1,2)} &= p_1(\mu)p_2(\mu)(2p_{1,00}^{(1,2)} + p_{1,01}^{(1,2)} + p_{1,12}^{(1,2)})/4, & (10)\\ e_{1,\mathrm{bit}}^{(1,2)} &= p_1(\mu)p_2(\mu)p_{1,00}^{(1,2)}/(2Q_1^{(1,2)}), & (11)\\ Q_1^{\mathrm{tot}} &= (2q_{1,00} + q_{1,01} + q_{1,12})/4, & (12)\\ e_1^{\mathrm{tot}} &= q_{1,00}/(2Q_1^{\mathrm{tot}}). & (13) \end{aligned}$$

Here the probabilities are expressed as

$$\begin{aligned}
p_{1,00}^{(1,1)} &= T^2 f_2 + 2T(1-T)f_3 + (1-T)^2 f_4, && (14)\\
p_{1,01}^{(1,1)} &= T^2 f_1 + 2T(1-T)f_3 + (1-T)^2 f_4, && (15)\\
p_{1,12}^{(1,1)} &= T^2 f_5 + 2T(1-T)f_3 + (1-T)^2 f_4, && (16)\\
p_{1,00}^{(1,2)} &= (1-T)(T^2 f_2 + T(1-T)f_3 + p_{1,00}^{(1,1)}), && (17)\\
p_{1,01}^{(1,2)} &= (1-T)(T^2 f_1 + T(1-T)f_3 + p_{1,01}^{(1,1)}), && (18)\\
p_{1,12}^{(1,2)} &= (1-T)(T^2 f_5 + T(1-T)f_3 + p_{1,12}^{(1,1)}), && (19)\\
q_{1,00} &= p_0^2(T\mu)f_4 + 2p_0(T\mu)p_1(T\mu)f_3 + p_1^2(T\mu)f_2, && (20)\\
q_{1,01} &= p_0^2(T\mu)f_4 + 2p_0(T\mu)p_1(T\mu)f_3 + p_1^2(T\mu)f_1, && (21)\\
q_{1,12} &= p_0^2(T\mu)f_4 + 2p_0(T\mu)p_1(T\mu)f_3 + p_1^2(T\mu)f_5. && (22)
\end{aligned}$$

For Type2, we have

$$\begin{aligned}
Q_2^{(1,1)} &= p_1^2(\mu)(p_{2,00}^{(1,1)} + p_{2,01}^{(1,1)})/4, && (23)\\
e_{2,\mathrm{bit}}^{(1,1)} &= p_1^2(\mu)p_{2,01}^{(1,1)}/(4Q_2^{(1,1)}), && (24)\\
Q_2^{(1,2)} &= p_1(\mu)p_2(\mu)(p_{2,00}^{(1,2)} + p_{2,01}^{(1,2)})/4, && (25)\\
e_{2,\mathrm{bit}}^{(1,2)} &= p_1(\mu)p_2(\mu)p_{2,01}^{(1,2)}/(4Q_2^{(1,2)}), && (26)\\
Q_2^{\mathrm{tot}} &= (q_{2,00} + q_{2,01})/4, && (27)\\
e_2^{\mathrm{tot}} &= q_{2,01}/(4Q_2^{\mathrm{tot}}), && (28)
\end{aligned}$$

where

$$\begin{aligned}
p_{2,00}^{(1,1)} &= p_{1,01}^{(1,1)}, && (29)\\
p_{2,01}^{(1,1)} &= p_{1,00}^{(1,1)}, && (30)\\
p_{2,00}^{(1,2)} &= p_{1,01}^{(1,2)}, && (31)\\
p_{2,01}^{(1,2)} &= p_{1,00}^{(1,2)}, && (32)\\
q_{2,00} &= q_{1,01}, && (33)\\
q_{2,01} &= q_{1,00}. && (34)
\end{aligned}$$

B. Case (ii) Alice and Bob use the heralded single photon sources.

From Ref. [1], the probability distribution function of the thermal state conditioned that the detector D_0 clicked in Fig. 2(b) is

$$P_n = \frac{1}{P_{\mathrm{click}}}\frac{\mu^n(1-(1-\eta)^n + d)}{(1+\mu)^{n+1}}, \quad (35)$$

where P_{click} is the probability that the detector D_0 clicks, which is described by

$$P_{\mathrm{click}} = \frac{(1+d)(1+\mu\eta) - 1}{1+\mu\eta}. \quad (36)$$

By defining $\eta_{\mathrm{in}} = \eta T$, the probability that n photons exist before the BS conditioned on the click of D_0 is

$$Q_n = \frac{1}{P_{\mathrm{click}}}\left(\frac{(1+d)(\mu\eta_{\mathrm{in}})^n}{(1+\mu\eta_{\mathrm{in}})^{n+1}} - \frac{(\mu\eta_{\mathrm{in}}(1-\eta))^n}{(1+\mu(\eta_{\mathrm{in}}+\eta-\eta_{\mathrm{in}}\eta))^{n+1}}\right). \quad (37)$$

For Type1, the relevant equations for $Q_1^{(n,m)}$ and $e_{1,\mathrm{bit}}^{(n,m)}$ are expressed by

$$\begin{align}
Q_1^{(1,1)} &= P_1^2(2p_{1,00}^{(1,1)}+p_{1,01}^{(1,1)}+p_{1,12}^{(1,1)})/4, \tag{38}\\
e_1^{(1,1)} &= P_1^2 p_{1,00}^{(1,1)}/(2Q_1^{(1,1)}), \tag{39}\\
Q_1^{(1,2)} &= P_1P_2(2p_{1,00}^{(1,2)}+p_{1,01}^{(1,2)}+p_{1,12}^{(1,2)})/4, \tag{40}\\
e_1^{(1,2)} &= P_1P_2 p_{1,00}^{(1,2)}/(2Q_1^{(1,2)}), \tag{41}\\
Q_1^{\mathrm{tot}} &= (2q_{1,00}+q_{1,01}+q_{1,12})/4, \tag{42}\\
e_1^{\mathrm{tot}} &= q_{1,00}/(2Q_1^{\mathrm{tot}}), \tag{43}
\end{align}$$

where

$$\begin{align}
p_{1,00}^{(1,1)} &= \eta_{\mathrm{in}}^2 g_4+2\eta_{\mathrm{in}}(1-\eta_{\mathrm{in}})g_2+(1-\eta_{\mathrm{in}})^2 g_1, \tag{44}\\
p_{1,01}^{(1,1)} &= \eta_{\mathrm{in}}^2 g_3+2\eta_{\mathrm{in}}(1-\eta_{\mathrm{in}})g_2+(1-\eta_{\mathrm{in}})^2 g_1, \tag{45}\\
p_{1,12}^{(1,1)} &= \eta_{\mathrm{in}}^2 g_8+2\eta_{\mathrm{in}}(1-\eta_{\mathrm{in}})g_2+(1-\eta_{\mathrm{in}})^2 g_1, \tag{46}\\
p_{1,00}^{(1,2)} &= \eta_{\mathrm{in}}^3 g_6+2\eta_{\mathrm{in}}^2(1-\eta_{\mathrm{in}})g_4+\eta_{\mathrm{in}}^2(1-\eta_{\mathrm{in}})g_7+3\eta_{\mathrm{in}}(1-\eta_{\mathrm{in}})^2 g_2+(1-\eta_{\mathrm{in}})^3 g_1, \tag{47}\\
p_{1,01}^{(1,2)} &= \eta_{\mathrm{in}}^3 g_5+2\eta_{\mathrm{in}}^2(1-\eta_{\mathrm{in}})g_3+\eta_{\mathrm{in}}^2(1-\eta_{\mathrm{in}})g_7+3\eta_{\mathrm{in}}(1-\eta_{\mathrm{in}})^2 g_2+(1-\eta_{\mathrm{in}})^3 g_1, \tag{48}\\
p_{1,12}^{(1,2)} &= \eta_{\mathrm{in}}^3 g_9+2\eta_{\mathrm{in}}^2(1-\eta_{\mathrm{in}})g_8+\eta_{\mathrm{in}}^2(1-\eta_{\mathrm{in}})g_7+3\eta_{\mathrm{in}}(1-\eta_{\mathrm{in}})^2 g_2+(1-\eta_{\mathrm{in}})^3 g_1, \tag{49}\\
q_{1,00} &= Q_0^2 g_1+2Q_0Q_1g_2+Q_1^2g_4+2Q_0Q_2g_7+2Q_1Q_2g_6+\sum_{n,m=2}^{\infty}Q_nQ_m \tag{50}\\
q_{1,01} &= Q_0^2 g_1+2Q_0Q_1g_2+Q_1^2g_3+2Q_0Q_2g_7+2Q_1Q_2g_5 \tag{51}\\
q_{1,12} &= Q_0^2 g_1+2Q_0Q_1g_2+Q_1^2g_8+2Q_0Q_2g_7+2Q_1Q_2g_9. \tag{52}
\end{align}$$

We note that in equation (50), we took the pessimistic scenario that all of the events for $n \geq 2$ and $m \geq 2$ are detected as the bit error. Here $g_1, \ldots, g_9$ are given by

$$\begin{align}
g_1 &= (1-d)^2 2d^2, \tag{53}\\
g_2 &= (1-d)^2 d, \tag{54}\\
g_3 &= (1-d)^2(2a^2b^2+(a^4+b^4)d), \tag{55}\\
g_4 &= g_3-(1-d)^2 2a^2b^2, \tag{56}\\
g_5 &= (1-d)^2(9(a^4b^2+a^2b^4)+3(a^6+b^6)d)/4, \tag{57}\\
g_6 &= (1-d)^2((a^4b^2+a^2b^4)+3(a^6+b^6)d)/4, \tag{58}\\
g_7 &= g_3/2, \tag{59}\\
g_8 &= (1-d)^2 2a^2b^2(1+d), \tag{60}\\
g_9 &= (1-d)^2(a^6+b^6+3(a^4b^2+a^2b^4)d)/4. \tag{61}
\end{align}$$

For Type2, we have

$$\begin{align}
Q_2^{(1,1)} &= P_1^2(p_{2,00}^{(1,1)}+p_{2,01}^{(1,1)})/4, \tag{62}\\
e_2^{(1,1)} &= P_1^2 p_{2,01}^{(1,1)}/(4Q_2^{(1,1)}), \tag{63}\\
Q_2^{(1,2)} &= P_1P_2(p_{2,00}^{(1,2)}+p_{2,01}^{(1,2)})/4, \tag{64}\\
e_2^{(1,2)} &= P_1P_2 p_{2,01}^{(1,2)}/(4Q_2^{(1,2)}), \tag{65}\\
Q_2^{\mathrm{tot}} &= (q_{2,00}+q_{2,01})/4, \tag{66}\\
e_2^{\mathrm{tot}} &= q_{2,01}/(4Q_2^{\mathrm{tot}}), \tag{67}
\end{align}$$

where

$$\begin{aligned} p_{2,00}^{(1,1)} &= p_{1,01}^{(1,1)}, & (68)\\ p_{2,01}^{(1,1)} &= p_{1,00}^{(1,1)}, & (69)\\ p_{2,00}^{(1,2)} &= p_{1,01}^{(1,2)}, & (70)\\ p_{2,01}^{(1,2)} &= p_{1,00}^{(1,2)}, & (71)\\ q_{2,00} &= q_{1,01}, & (72)\\ q_{2,01} &= q_{1,00}. & (73) \end{aligned}$$

[1] Zhou, C. *et al.* Phase-encoded measurement-device-independent quantum key distribution with practical spontaneous-parametric-down-conversion sources. *Phys. Rev. A* **88**, 052333 (2013).