Decoherence assisted Quantum Key Distribution: supplemental document

1. EVE'S DENSITY MATRIX

In this appendix, we derive the explicit form of the quantum state of Eve's probe photon when the controllable decoherence-assisted scheme is used in the entangling probe attack. When Alice sends an horizontal photon and Bob detects a photon with the same polarization, the quantum state of Eve's photon is

$$\hat{\rho}_H^{(\mathcal{E})} = \mathrm{Tr}_{\mathrm{env}}\{\, |\tilde{\psi}_H\rangle_{\mathcal{B},\mathcal{E}} \langle\tilde{\psi}_H|_{\mathcal{B},\mathcal{E}} \,\} \tag{S1}$$

where [see Eq. (13(a)]

$$|\tilde{\psi}_H\rangle_{\mathcal{B},\mathcal{E}} = \int dy f(y) |y\rangle_{\mathcal{B}} \left(\sqrt{1-S^2}\,|+\rangle_{\mathcal{E}} - \frac{S}{\sqrt{2}}\,|-\rangle_{\mathcal{E}}\right). \tag{S2}$$

One obtains

$$\hat{\rho}_H^{(\mathcal{E})} = \frac{1}{1-S^2/2}\Bigg[(1-S^2)\,|+\rangle_{\mathcal{E}}\langle+|_{\mathcal{E}} + \frac{S^2}{2}\,|-\rangle_{\mathcal{E}}\langle-|_{\mathcal{E}} - \frac{S\sqrt{1-S^2}}{\sqrt{2}}\,|-\rangle_{\mathcal{E}}\langle+|_{\mathcal{E}} - \frac{S\sqrt{1-S^2}}{\sqrt{2}}\,|+\rangle_{\mathcal{E}}\langle-|_{\mathcal{E}}\Bigg]. \tag{S3}$$

Similarly, for a photon with vertical polarization, one has $\hat{\rho}_V^{(\mathcal{E})} = \mathrm{Tr}_{\mathrm{env}}\{\, |\tilde{\psi}_V\rangle_{\mathcal{B},\mathcal{E}} \langle\tilde{\psi}_V|_{\mathcal{B},\mathcal{E}} \,\}$ with [see Eq. (13(b)]

$$|\tilde{\psi}_V\rangle_{\mathcal{B},\mathcal{E}} = \int dy f(y) |y\rangle_{\mathcal{B}} \left(\sqrt{1-S^2}\,|+\rangle_{\mathcal{E}} + \frac{S}{\sqrt{2}}\,|-\rangle_{\mathcal{E}}\right) \tag{S4}$$

that yields

$$\hat{\rho}_V^{(\mathcal{E})} = \frac{1}{1-S^2/2}\Bigg[(1-S^2)\,|+\rangle_{\mathcal{E}}\langle+|_{\mathcal{E}} + \frac{S^2}{2}\,|-\rangle_{\mathcal{E}}\langle-|_{\mathcal{E}} + \frac{S\sqrt{1-S^2}}{\sqrt{2}}\,|-\rangle_{\mathcal{E}}\langle+|_{\mathcal{E}} + \frac{S\sqrt{1-S^2}}{\sqrt{2}}\,|+\rangle_{\mathcal{E}}\langle-|_{\mathcal{E}}\Bigg] \tag{S5}$$

For diagonal polarization, $\hat{\rho}_D^{(\mathcal{E})} = \mathrm{Tr}_{\mathrm{env}}\{\, |\tilde{\psi}_D\rangle_{\mathcal{B},\mathcal{E}} \langle\tilde{\psi}_D|_{\mathcal{B},\mathcal{E}} \,\}$ with [see Eq. (13(c)]

$$|\tilde{\psi}_D\rangle_{\mathcal{B},\mathcal{E}} = \frac{1}{2}\int dy \left[f(y)\left(2\sqrt{1-S^2}\,|+\rangle_{\mathcal{E}}\right) + \frac{S}{\sqrt{2}}\Big(f(y-2d)+f(y+2d)\Big)\,|-\rangle_{\mathcal{E}}\right] |y\rangle_{\mathcal{B}} \tag{S6}$$

The quantum state is now

$$\hat{\rho}_D^{(\mathcal{E})} = \frac{1}{1+(\gamma_1/8-1)S^2}\Bigg[(1-S^2)\,|+\rangle_{\mathcal{E}}\langle+|_{\mathcal{E}} + \frac{S^2\gamma_1}{8}\,|-\rangle_{\mathcal{E}}\langle-|_{\mathcal{E}} + \frac{S\sqrt{1-S^2}}{2\sqrt{2}}\gamma_2\,|-\rangle_{\mathcal{E}}\langle+|_{\mathcal{E}} + \frac{S\sqrt{1-S^2}}{2\sqrt{2}}\gamma_2^*\,|+\rangle_{\mathcal{E}}\langle-|_{\mathcal{E}}\Bigg], \tag{S7}$$

where

$$\gamma_1 = \int_{-\infty}^{\infty} dy |f(y+2d)+f(y-2d)|^2 \tag{S8}$$

and

$$\gamma_2 = \int_{-\infty}^{\infty} dy f^*(y)\Big[f(y+2d)+f(y-2d)\Big] \tag{S9}$$

Finally, for anti-diagonal polarization, $\hat{\rho}_A^{(\mathcal{E})} = \mathrm{Tr}_{\mathrm{env}}\{\, |\tilde{\psi}_A\rangle_{\mathcal{B},\mathcal{E}}\, \langle\tilde{\psi}_A|_{\mathcal{B},\mathcal{E}}\,\}$ with [see Eq.13(d)]

$$|\tilde{\psi}_A\rangle_{\mathcal{B},\mathcal{E}} = \frac{1}{2}\int dy \left[f(y)\Big(|T_-\rangle_{\mathcal{E}} + |T_+\rangle_{\mathcal{E}} \Big) - \Big(f(y-2d) + f(y+2d) \Big) |T_E\rangle_{\mathcal{E}} \right] |y\rangle_{\mathcal{B}} \tag{S10}$$

The quantum state of Eve's photon is

$$\hat{\rho}_A^{(\mathcal{E})} = \frac{1}{1+(\gamma_1/8-1)S^2}\left[(1-S^2)\,|+\rangle_{\mathcal{E}}\,\langle+|_{\mathcal{E}} + \frac{S^2\gamma_1}{8}\,|-\rangle_{\mathcal{E}}\,\langle-|_{\mathcal{E}} \right. \tag{S11}$$
$$\left. - \frac{S\sqrt{1-S^2}}{2\sqrt{2}}\gamma_2\,|-\rangle_{\mathcal{E}}\,\langle+|_{\mathcal{E}} - \frac{S\sqrt{1-S^2}}{2\sqrt{2}}\gamma_2^*\,|+\rangle_{\mathcal{E}}\,\langle-|_{\mathcal{E}} \right]$$

2. CALCULATION OF THE TRACE DISTANCES

In order to calculate the Rényi information, it is necessary to obtain the trace distances $D(\rho_H^{(\mathcal{E})}, \rho_V^{(\mathcal{E})})$ and $D(\rho_D^{(\mathcal{E})}, \rho_A^{(\mathcal{E})})$, which corresponds to the quantum states that Eve needs to discriminate. The trace distance can be calculated by

$$D(\hat{\rho}_1^{(\mathcal{E})}, \hat{\rho}_2^{(\mathcal{E})}) = \frac{1}{2}\sum_i^n |\lambda_i^{(1,2)}|, \tag{S12}$$

where $\lambda_i^{(1,2)}$ are the eigenvalues of $\hat{\rho}_{(1,2)}^{(\mathcal{E})} = \hat{\rho}_2^{(\mathcal{E})} - \hat{\rho}_1^{(\mathcal{E})}$.

The eigenvalues of the density matrix

$$\hat{\rho}_{HV}^{(\mathcal{E})} = \hat{\rho}_V^{(\mathcal{E})} - \hat{\rho}_H^{(\mathcal{E})} = \frac{2}{1-S^2/2}\left[\frac{S\sqrt{1-S^2}}{\sqrt{2}}\,|-\rangle_{\mathcal{E}}\,\langle+|_{\mathcal{E}} + \frac{S\sqrt{1-S^2}}{\sqrt{2}}\,|+\rangle_{\mathcal{E}}\,\langle-|_{\mathcal{E}} \right], \tag{S13}$$

are $\lambda_{1,2}^{(H,V)} = \pm 2\sqrt{2}\,S\,\sqrt{1-S^2}/(2-S^2)$, so

$$D(\hat{\rho}_H^{(\mathcal{E})}, \hat{\rho}_V^{(\mathcal{E})}) = 2\sqrt{2}\frac{S\sqrt{1-S^2}}{2-S^2} \tag{S14}$$

The eigenvalues of the density matrix

$$\hat{\rho}_{DA}^{(\mathcal{E})} = \hat{\rho}_D^{(\mathcal{E})} - \hat{\rho}_A^{(\mathcal{E})} = \frac{1}{1+(\gamma_1/8-1)S^2}\left[\frac{S\sqrt{1-S^2}}{\sqrt{2}}\gamma_2^*\,|-\rangle_{\mathcal{E}}\,\langle+|_{\mathcal{E}} + \frac{S\sqrt{1-S^2}}{\sqrt{2}}\gamma_2\,|+\rangle_{\mathcal{E}}\,\langle-|_{\mathcal{E}} \right], \tag{S15}$$

are $\lambda_{1,2}^{(D,A)} = \pm 4\sqrt{2}\,S\,\sqrt{1-S^2}\,\gamma_2/[8+(\gamma_1-8)S^2]$, so

$$D(\hat{\rho}_D^{(\mathcal{E})}, \hat{\rho}_A^{(\mathcal{E})}) = 4\sqrt{2}\frac{S\sqrt{1-S^2}}{8+(\gamma_1-8)S^2}\gamma_2. \tag{S16}$$

For the case of a function $f(y)$ with spatial Gaussian shape,

$$f(y) = \Big(\frac{2}{\pi \mathrm{w}^2}\Big)^{1/4} \exp\,[-y^2/\mathrm{w}^2], \tag{S17}$$

the parameters γ_1 and γ_2 become $\gamma_1 = 2+2\gamma_0^4$ and $\gamma_2 = 2\gamma_0$ with $\gamma_0 = \exp(-2d^2/\mathrm{w}^2)$.

3. OBTAINING THE KEY FROM TIME STAMPINGS

In this appendix, we explain the detailed process of obtaining the key from the time stamping list. The process is as follows: after the position in the wave plates is set, Alice and Bob generate a file that contains the position of its own wave plate and a list that has the time stampings and the detector that produces the click. Afterwards, computationally Alice and Bob add one column to its own list that contains a number that indexes the position of each element of the list, this is illustrated by the gray column in Fig. S1.

Alice

Time index	Time stamp [81 ps]	CH
1	t_{1A}	0
2	t_{2A}	1
3	t_{3A}	0
. .	. .	. .
nA	t_{nA}	1

Public

Bob

Time index	Time stamp [81 ps]	CH
1	t_{1B}	2
2	t_{2B}	3
3	t_{3B}	2
. .	. .	. .
nB	t_{nB}	2

Public

Fig. S1. Scheme of data analysis to recognize HSPs. Alice and Bob add one index to each event. Afterwards, they share publicly a list with the time index and the time of each click.

To identify HSPs, Alice and Bob make public the portion of their own list that contains time stamps and time indexes. When the standard BB84 protocol is implemented, a HSP is identified as a joint count among $\tau_0 \pm 2\sigma$ in any of the $G^{(2)}$ measurements of Fig. S2. On the other hand, when the P-TBDs are introduced in the controllable decoherence-assisted scheme, the recognition of a HSP is given by any joint count among $\tau_0 \pm 2\sigma$ in any of the $G^{(2)}$ measurements of Fig. S3.

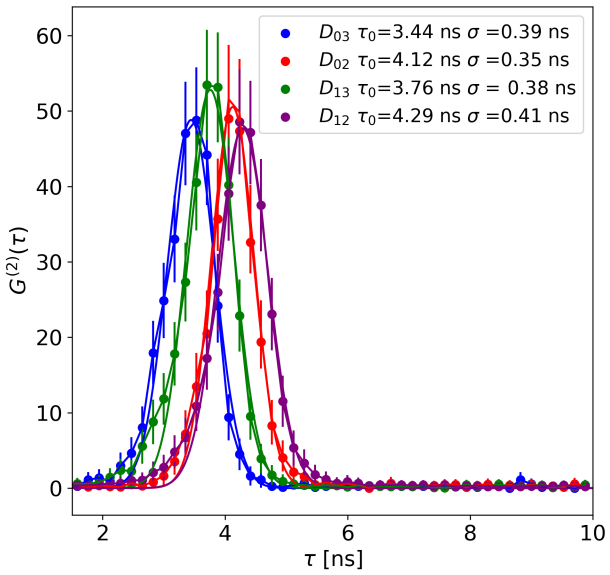

Fig. S2. Temporal characterization used to recognize heralded single-photons in the standard BB84 protocol.

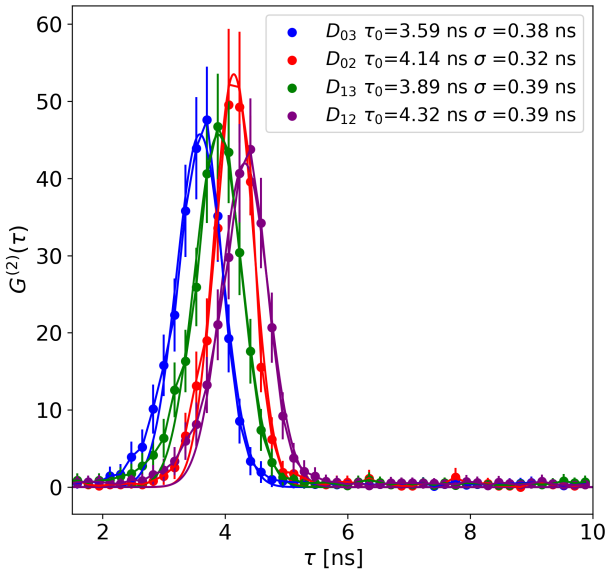

Fig. S3. Temporal characterization used to recognize heralded single-photons when the controllable decoherence-assisted scheme is used.

After the identification of HSPs, Alice and Bob save the time indexes of the joint counts without revealing the detector. Once the time indexes are saved, Alice and Bob assign bits to the detectors that led to a joint count: in Alice's arm, logical 0 and logical 1 are associated to clicks in D0 and D1, respectively. In Bob's arm, logical 0 and logical 1 are associated to clicks in D3 and D2, respectively. This is illustrated in Fig S4. The bits assigned will constitute the key.

Alice

Time index	CH	Bit
1	0	0
3	0	0
5	1	1
. .	. .	
nA	1	1

Bob

Time Index	CH	Bit
1	2	1
2	3	0
4	3	0
. .	. .	
nB	2	1

Fig. S4. Scheme of data analysis to generate the shared key. The empty boxes are due to the fact that the event was not taken into account because it is not a joint count.