SUPPLEMENTAL MATERIAL

Akihiro Mizutani,[1,2] Go Kato,[3,4] Koji Azuma,[5,4] Marcos Curty,[6] Rikizo Ikuta,[1]
Takashi Yamamoto,[1] Nobuyuki Imoto,[1] Hoi-Kwong Lo,[7] and Kiyoshi Tamaki[5,8]

[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501 Japan*
[3] *NTT Communication Science Laboratories, NTT Corporation, 3-1, Morinosato Wakamiya Atsugi-Shi, Kanagawa, 243-0198, Japan*
[4] *NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[5] *NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan*
[6] *EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[7] *Center for Quantum Information and Quantum Control, Department of Physics and Dept. of Electrical & Computer Engineering, University of Toronto, M5S 3G4 Toronto, Canada*
[8] *Graduate School of Science and Engineering for Research, University of Toyama, Gofuku 3190, Toyama, 930-8555, Japan*

In this supplemental material, we first summarize the notations used throughout this paper, and in Sec. II we describe Alice's sending states under the framework of SCIC. In Sec. III, we introduce the Modified Azuma's inequality that we use in the decoy-state method. Then, in Sec. IV, we explain our decoy-state method with the intensity fluctuations. Finally in Sec. V, we derive the number of phase errors for the untagged single-photon events.

I. SUMMARY OF NOTATIONS

A list of the parameters used throughout this paper together with their notation is provided in Tables I and II.

II. DESCRIPTION OF ALICE'S SENDING STATE

For later discussions, we introduce the following theorem about the description of Alice's sending states, which is a direct consequence of the assumptions (A-1)-(A-5) in the Results section.

Theorem 1 *From the assumptions (A-1)-(A-5), we have that all the $N_{\rm sent}$ sending states can be written as*

$$\sum_{\boldsymbol{g}^{N_{\rm sent}}}\sqrt{p(\boldsymbol{g}^{N_{\rm sent}})}|\boldsymbol{g}^{N_{\rm sent}}\rangle_{\boldsymbol{G}^{N_{\rm sent}}}\bigotimes_{i=1}^{N_{\rm sent}}\sum_{c^i,k^i}\sqrt{p(c^i)p(k^i)}|\hat{\rho}^i(\theta^i_{c^i,g^i},\mu^i_{k^i,g^i})\rangle_{N^iB^i}|c^i,k^i\rangle_{C^iK^i}|\theta^i_{c^i,g^i},\mu^i_{k^i,g^i}\rangle_{\Theta^i,M^i} \tag{II.1}$$

with $\boldsymbol{G}^{N_{\rm sent}}:=G^1,...,G^{N_{\rm sent}}$. Here, G^i, C^i, K^i, Θ^i and M^i denote the systems storing the information of g^i, c^i, k^i, θ^i and μ^i, respectively. According to the assumption (A-1), note that these five systems are possessed by Alice. This is to ensure that there is no side channel leaking information to Eve. Also, $|\hat{\rho}^i(\theta^i_{c^i,g^i},\mu^i_{k^i,g^i})\rangle_{N^iB^i}$ is a purified state of Eq. (2) with N^i being a system storing the number of photons contained in the $i^{\rm th}$ sending state, which has the form

$$|\hat{\rho}^i(\theta^i_{c^i,g^i},\mu^i_{k^i,g^i})\rangle_{N^iB^i}=\sum_{n^i}\sqrt{p(n^i|\mu^i_{k^i,g^i})}|n^i\rangle_{N^i}|\hat{\Upsilon}^i(\theta^i_{c^i,g^i},n^i)\rangle_{B^i}.$$

Proof of Theorem 1 For the most general case, the total $N_{\rm sent}$ sending states can be coherently written as

$$\sum_{\boldsymbol{g}^{N_{\rm sent}},\boldsymbol{\theta}^{N_{\rm sent}},\boldsymbol{\mu}^{N_{\rm sent}},\boldsymbol{c}^{N_{\rm sent}},\boldsymbol{k}^{N_{\rm sent}}}\sqrt{p(\boldsymbol{g}^{N_{\rm sent}},\boldsymbol{P}^{N_{\rm sent}})}\bigotimes_{i=1}^{N_{\rm sent}}|\hat{\rho}^i(\theta^i,\mu^i)\rangle_{N^i,B^i}|\theta^i\rangle_{\Theta^i}|\mu^i\rangle_{M^i}|c^i\rangle_{C^i}|k^i\rangle_{K^i}|g^i\rangle_{G^i}. \tag{II.2}$$

Random variables and sets	Meaning
$\boldsymbol{X}^i$	Abbreviation of $X^1, X^2, ..., X^i$ (X^i can be $c^i, k^i, \theta^i, \mu^i, P^i, g^i, n^i, y^i, b^i$)
$\mathcal{C}$	Set of bit and basis information: $\{0_Z, 1_Z, 0_X\}$
$c^i \in \mathcal{C}$	Alice's i^{th} choice of bit and basis information
$\mathcal{K}$	Set of intensity setting: $\{k_1, k_2, k_3\}$
$k^i \in \mathcal{K}$	Alice's i^{th} choice of intensity setting
$\theta^i \in [0, 2\pi)$	i^{th} relative phase between the signal and reference pulses
$\mu^i \in [0, \infty)$	i^{th} total intensity in both the signal and reference pulses
P^i	Shorthand of $c^i, k^i, \theta^i, \mu^i$
$\mathcal{G}^i_{\text{unt}}$	Untagged set of the i^{th} internal state of the source device
$g^i \in \mathcal{G}^i_{\text{unt}} \cup \overline{\mathcal{G}^i_{\text{unt}}}$	i^{th} internal state of Alice's source device
$\boldsymbol{g}^{\geq i}$	Abbreviation of $g^i, g^{i+1}, ..., g^{N_{\text{sent}}}$
$t^i \in \{u, t\}$	$t^i = u$ if $g^i \in \mathcal{G}^i_{\text{unt}}$ and $t^i = t$ if $g^i \notin \mathcal{G}^i_{\text{unt}}$
n_{tag}	Number of tagged signals: $\|\{i\|t^i = t\}\|$
$\boldsymbol{\mathcal{G}}^{N_{\text{sent}}}_{\text{good}}$	Set of $\boldsymbol{g}^{N_{\text{sent}}}$ where n_{tag} is upper bounded by a fixed number
$n^i \in [0, \infty)$	Total number of photons in the i^{th} signal and reference pulses
$\mathcal{B}$	Set of bases: $\{Z, X\}$
$a^i(b^i) \in \mathcal{B}$	Alice's (Bob's) i^{th} basis choice
$y^i \in \{0, 1, \emptyset\}$	Bob's i^{th} measurement outcome
$\boldsymbol{\chi}^i_A$	Shorthand of $\boldsymbol{c}^i, \boldsymbol{k}^i, \boldsymbol{g}^i, \boldsymbol{n}^i$
$\boldsymbol{\chi}^i_B$	Shorthand of $\boldsymbol{b}^i, \boldsymbol{y}^i$
$\boldsymbol{\chi}^i_{AB}$	Shorthand of $\boldsymbol{c}^i, \boldsymbol{k}^i, \boldsymbol{g}^i, \boldsymbol{n}^i, \boldsymbol{b}^i, \boldsymbol{y}^i$
$\mathcal{S}_{Z,Z,k,\text{det}}$	Set $\{i\|a^i = b^i = Z,\ k^i = k,\ y^i \neq \emptyset\}$
$\mathcal{S}_{Z,Z,\text{det}}$	Set $\{i\|a^i = b^i = Z,\ y^i \neq \emptyset\}$
$\mathcal{S}_{Z,Z,n,u,\text{det}}$	Set $\{i\|a^i = b^i = Z,\ n^i = n,\ t^i = u, y^i \neq \emptyset\}$
$\mathcal{S}_{c,k,\text{det},y,b}$	Set $\{i\|c^i = c, k^i = k, b^i = b,\ y^i = y\}$
$\mathcal{S}_{c,n,u,\text{det},y,b}$	Set $\{i\|c^i = c, n^i = n, t^i = u, b^i = b,\ y^i = y\}$
$\mathcal{S}_{\text{det}}$	Set $\{i\|y^i \neq \emptyset\}$
$\mathcal{S}^{\text{L}}_{Z,Z,1,u,\text{det}}$	Lower bound on $\|\mathcal{S}_{Z,Z,1,u,\text{det}}\|$
$N_{\text{ph},Z,Z,1,u,\text{det}}$	Number of phase errors in the set $\mathcal{S}_{Z,Z,1,u,\text{det}}$
$N^{\text{U}}_{\text{ph},Z,Z,1,u,\text{det}}$	Upper bound on $N_{\text{ph},Z,Z,1,u,\text{det}}$

TABLE I: Random variables and sets used throughout the paper

Next, we calculate $p(\boldsymbol{g}^{N_{\text{sent}}}, \boldsymbol{P}^{N_{\text{sent}}})$ using the assumptions (A-2)-(A-5).

$$\begin{aligned}
p(\boldsymbol{g}^{N_{\text{sent}}}, \boldsymbol{P}^{N_{\text{sent}}}) &= \Pi_{i=1}^{N_{\text{sent}}} p(g^i, P^i|\boldsymbol{g}^{i-1}, \boldsymbol{P}^{i-1}) \\
&= \Pi_{i=1}^{N_{\text{sent}}} p(P^i|\boldsymbol{g}^i, \boldsymbol{P}^{i-1}) p(g^i|\boldsymbol{g}^{i-1}, \boldsymbol{P}^{i-1}) \\
&= \Pi_{i=1}^{N_{\text{sent}}} p(P^i|\boldsymbol{g}^i, \boldsymbol{P}^{i-1}) p(g^i|\boldsymbol{g}^{i-1}) \\
&= \Pi_{i=1}^{N_{\text{sent}}} p(\theta^i, \mu^i|c^i, k^i, \boldsymbol{g}^i, \boldsymbol{P}^{i-1}) p(c^i, k^i|\boldsymbol{g}^i, \boldsymbol{P}^{i-1}) p(g^i|\boldsymbol{g}^{i-1}) \\
&= \Pi_{i=1}^{N_{\text{sent}}} \delta(\theta^i, \theta^i_{c^i,g^i}) \delta(\mu^i, \mu^i_{k^i,g^i}) p(c^i) p(k^i) p(g^i|\boldsymbol{g}^{i-1}),
\end{aligned}$$

where in the 3$^{\text{rd}}$ equation we use the assumption (A-2), and in the 5$^{\text{th}}$ equation we use the assumptions (A-3)-(A-5). With this expression, Eq. (II.2) results in Eq. (II.1), which ends the proof. ■

III. MODIFIED AZUMA'S INEQUALITY

Here, we introduce the Modified Azuma's inequality [3] that we use in the decoy-state method (see Sec. IV).

Quantum systems	Meaning	
C^i	Quantum system storing c^i possessed by Alice	
K^i	Quantum system storing k^i possessed by Alice	
Θ^i	Quantum system storing θ^i possessed by Alice	
M^i	Quantum system storing μ^i possessed by Alice	
G^i	Quantum system storing g^i possessed by Alice	
N^i	Quantum system storing n^i possessed by Alice	
B^i	i^{th} quantum system sent to Bob	
A^i	Alice's i^{th} quantum system defined iff $t^i = u$ and $n^i = 1$	
B'^i	Bob's i^{th} quantum system after Eve's intervention	
Symbols	**Meaning**	**Reference in main text**
N_{sent}	Number of pulse pairs (signal and reference pulses) sent by Alice	
$R_{\text{ph}}^{c^i}$	i^{th} interval of the relative phase θ^i for c^i	Eq. (10)
$R_{\text{int}}^{k^i}$	i^{th} interval of the intensity μ^i for k^i	Eq. (11)
N_{tag}	Predetermined upper bound on n_{tag}	Eq. (12)
p_{fail}	Upper bound on the probability that $\boldsymbol{g}^{N_{\text{sent}}} \notin \boldsymbol{\mathcal{G}}_{\text{good}}^{N_{\text{sent}}}$ occurs	Eq. (13)
N_{det}	Predetermined number of detection events $\lvert\mathcal{S}_{\text{det}}\rvert$	
$\boldsymbol{\kappa}_{A(B)}^{\text{sift}}$	Alice's (Bob's) sifted key	
$\boldsymbol{\kappa}_{B}^{\text{cor}}$	Bob's reconciled key	
$\boldsymbol{\kappa}_{A(B)}^{\text{fin}}$	Alice's (Bob's) final key	
ϵ_{sec}	Security parameter of the protocol	
ϵ_{s}	Secrecy parameter of the protocol	Eq. (19)
ϵ_{c}	Correctness parameter of the protocol	
ϵ_{PA}	Error probability of privacy amplification	Eq. (19)
ϵ_{Z}	Failure probability of the estimation of $\mathcal{S}_{Z,Z,1,u,\text{det}}^{\text{L}}$ given that $S_{\text{det}} = N_{\text{det}}$	Eq. (22)
$\epsilon_{\text{MA}}^{Z,k,u}$	Failure probability in estimating $S_{Z,Z,1,u,\text{det}}^{\text{L}}$ for $k^i = k$	Eq. (21)
$\epsilon_{\text{MA}}^{Z,1,u}$	Failure probability in estimating $S_{Z,Z,1,u,\text{det}}^{\text{L}}$ for $n^i = 1$	Eq. (21)
$\epsilon_{\text{A}}^{c,1,u,y,X}$	Failure probability in estimating $N_{\text{ph},Z,1,u,\text{det}}^{\text{U}}$ for $(c^i, n^i, y^i) = (c, 1, y)$	Eq. (24)
$\epsilon_{\text{A}}^{\text{ph},Z,1,u}$	Failure probability in estimating $N_{\text{ph},Z,1,u,\text{det}}^{\text{U}}$ for $n^i = 1$	Eq. (24)
$\epsilon_{\text{MA}}^{c,1,u,y,X}$	Failure probability in estimating $S'_{c,1,u,\text{det},y,X}$ for $(c^i, n^i, y^i) = (c, 1, y)$	Eqs. (26),(27)
$\epsilon_{\text{MA}}^{c,k,u,y,X}$	Failure probability in estimating $S'_{c,1,u,\text{det},y,X}$ for $(c^i, k^i, y^i) = (c, k, y)$	Eqs. (26),(27)
ϵ_{PH}	Failure probability of the estimation of $N_{\text{ph},Z,Z,1,u,\text{det}}^{\text{U}}$ given that $n_{\text{tag}} \le N_{\text{tag}}$ and $S_{\text{det}} = N_{\text{det}}$	Eq. (18)
ℓ	Length (in bits) of the final key	Eq. (20)

TABLE II: Quantum systems and symbols used throughout the paper

Theorem 2 *(Modified Azuma's inequality) [3]. Let Y_i be an i^{th} random variable with $Y_0 := 0$ $(0 \le i \le n)$ defined on the probability space $(\Omega, \mathcal{F}, p)$ with the filtration $\mathcal{F}_0 \subset \mathcal{F}_1 \subset \cdots \subset \mathcal{F}_n = \mathcal{F}$, where $\mathcal{F}_0$ is the trivial σ-algebra $\{\emptyset, \Omega\}$ and $\mathcal{F}$ is the power set of Ω (consisting of all the subsets of Ω). We suppose that the sequence of random variables $\{Y_j\}_{j=1}^n$ satisfies*

$$E[Y_j|\mathcal{F}_j] = Y_j, \tag{III.1}$$

the Martingale condition:

$$E[Y_j|\mathcal{F}_{j-1}] = Y_{j-1}, \tag{III.2}$$

the bounded difference condition:

$$|Y_j - Y_{j-1}| \le 1, \tag{III.3}$$

and the zero-difference condition:

$$p(|Y_j - Y_{j-1}| = 0|\mathcal{F}_{j-1}) \geq 1 - q \tag{III.4}$$

for a constant q $(0 \leq q \leq 1)$*. Then, for any* $\epsilon > 0$*, we have that*

$$p\Big(Y_n \geq g_{\mathrm{MA}}(\epsilon, q, n)\Big) \leq \epsilon \tag{III.5}$$

and

$$p\Big(Y_n \leq -g_{\mathrm{MA}}(\epsilon, q, n)\Big) \leq \epsilon \tag{III.6}$$

are satisfied, where $g_{\mathrm{MA}}(\epsilon, q, n)$ *is defined by*

$$g_{\mathrm{MA}}(\epsilon, q, n) := \frac{\sqrt{\ln\epsilon(\ln\epsilon - 18nq)} - \ln\epsilon}{3}. \tag{III.7}$$

For completeness, below we prove Theorem 2.

Proof of Theorem 2 For convenience, we define $\Delta_j := Y_j - Y_{j-1}$, and we have that for any $s > 0$

$$\begin{aligned} E[e^{s\Delta_j}|\mathcal{F}_{j-1}] &= E[1 + s\Delta_j + s^2\Delta_j^2 g(s\Delta_j)|\mathcal{F}_{j-1}] && \text{(III.8)}\\ &= 1 + s^2 E[\Delta_j^2 g(s\Delta_j)|\mathcal{F}_{j-1}] && \text{(III.9)}\\ &\leq 1 + s^2 g(s) E[\Delta_j^2|\mathcal{F}_{j-1}] && \text{(III.10)}\\ &\leq 1 + s^2 g(s) q && \text{(III.11)}\\ &\leq e^{s^2 g(s) q}, && \text{(III.12)} \end{aligned}$$

where $g(x) := (e^x - 1 - x)/x^2$ with $g(0) = 1/2$. Here, in Eq. (III.9) we use Eqs. (III.1) and (III.2), in Eq. (III.10) we use Eq. (III.3) and the fact that $g(x)$ is a monotonically increasing function, and finally in Eq. (III.11) we use Eqs. (III.3) and (III.4). We also have that for any $t > 0$,

$$\begin{aligned} p(Y_n \geq t) &\leq e^{-st} E[e^{sY_n}] && \text{(III.13)}\\ &= e^{-st} E[E[e^{s(Y_{n-1}+\Delta_n)}|\mathcal{F}_{n-1}]] && \text{(III.14)}\\ &= e^{-st} E[e^{sY_{n-1}} E[e^{s\Delta_n}|\mathcal{F}_{n-1}]] && \text{(III.15)}\\ &\leq e^{s^2 g(s) q} e^{-st} E[e^{sY_{n-1}}] && \text{(III.16)}\\ &\leq \cdots && \text{(III.17)}\\ &\leq e^{-st}\Pi_{i=1}^n e^{s^2 g(s) q} && \text{(III.18)}\\ &= e^{-st+(e^s-1-s)qn}. && \text{(III.19)} \end{aligned}$$

Here, Eq. (III.13) is due to the Markov's inequality, Eq. (III.14) is due to the tower rule of expectation, Eq. (III.15) is due to Eq. (III.1), Eq. (III.16) is due to Eq. (III.12), and in Eq. (III.17) we just employ the same discussion that we used to go from Eq. (III.14) to Eq. (III.16) to bound $E[e^{sY_{n-1}}]$. If we choose $s = \ln(1 + \frac{t}{nq})$, we obtain from Eq. (III.19) that

$$p(Y_n \geq t) \leq e^{-nq\phi(\frac{t}{nq})} \tag{III.20}$$

with $\phi(x) := (1 + x)\ln(1 + x) - x$. Finally, since $\phi(x) \geq \frac{x^2}{2(1+x/3)}$ for $x > -1$, we obtain

$$p(Y_n \geq t) \leq \exp\Big(-\frac{t^2}{2nq + 2t/3}\Big). \tag{III.21}$$

By setting $\exp\Big(-\frac{t^2}{2nq+2t/3}\Big) = \epsilon$, we obtain Eq. (III.5). Also, Eq. (III.6) can be proven in a similar way. ■

IV. DECOY-STATE METHOD

In this section, we present the decoy-state method that we use to estimate bounds on the parameters $S_{c,n,u,\mathrm{det},y,X}$ and $S_{Z,Z,n,u,\mathrm{det}}$ for $n=1$ in the presence of intensity fluctuations within the framework of SCIC. Here, $S_{c,n,u,\mathrm{det},y,X}$ denotes the cardinality of the set $\mathcal{S}_{c,n,u,\mathrm{det},y,X}=\{i|c^i=c,n^i=n,t^i=u,b^i=X,y^i=y\}$ (with $y\in\{0,1\}$). More precisely, the goal here is to bound the quantities

$$S_{c,n=1,u,\mathrm{det},y,X} \quad \text{and} \quad S_{Z,Z,n=1,u,\mathrm{det}} \tag{IV.1}$$

with the available experimentally observed data, that is,

$$\{S_{c,k,\mathrm{det},y,X}\}_{k\in\mathcal{K}} \quad \text{and} \quad \{S_{Z,Z,k,\mathrm{det}}\}_{k\in\mathcal{K}}, \tag{IV.2}$$

respectively. We first derive the upper and lower bounds on $S_{c,1,u,\mathrm{det},y,X}$ (see Sec. IV A), and after that we derive the lower bound on $S_{Z,Z,1,u,\mathrm{det}}$ (see Sec. IV B).

To achieve this goal, we divide the task into four steps. To illustrate the method, let us consider for instance the case for $S_{c,1,u,\mathrm{det},y,X}$. In step 1, we use the Modified Azuma's inequality to relate the numbers $S_{c,1,u,\mathrm{det},y,X}$ and $S_{c,k,u,\mathrm{det},y,X}$ with the quantities $\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}}$ in Eq. (IV.11) and $\langle S_{c,k,u,y,X}\rangle_{\mathrm{det}}$ in Eq. (IV.3), respectively. Here, $S_{c,k,u,\mathrm{det},y,X}$ denotes the cardinality of the set $\mathcal{S}_{c,k,u,\mathrm{det},y,X}=\{i|c^i=c,k^i=k,t^i=u,b^i=X,y^i=y\}$. In step 2, we derive the bounds on $\langle S_{c,k,u,y,X}\rangle_{\mathrm{det}}$ by using the functions $\{f_{c,n,u,y,X|\mathrm{det}}\}_n$ that are related to the quantities $\{\langle S_{c,n,u,y,X}\rangle_{\mathrm{det}}\}_n$. Here, $\langle S_{c,n,u,y,X}\rangle_{\mathrm{det}}$ and $f_{c,n,u,y,X|\mathrm{det}}$ are defined in Eqs. (IV.11) and (IV.22) respectively. In step 3, we derive the bounds on $\langle S_{c,n=1,u,y,X}\rangle_{\mathrm{det}}$ with $\{\langle S_{c,k,u,y,X}\rangle_{\mathrm{det}}\}_k$. In step 4, we finally combine Eqs. (IV.25) and (IV.30) with Eqs. (IV.10) and (IV.12) which are obtained by means of the Modified Azuma's inequality, and we obtain the bounds on $S_{c,n=1,u,\mathrm{det},y,X}$ with the observed data $\{S_{c,k,\mathrm{det},y,X}\}_{k\in\mathcal{K}}$.

A. Upper and lower bounds on $S_{c,1,u,\mathrm{det},y,X}$

1. *Step 1. Modified Azuma's inequality*

In order to obtain upper and lower bounds on $S_{c,1,u,\mathrm{det},y,X}$, we first relate the numbers $S_{c,1,u,\mathrm{det},y,X}$ and $S_{c,k,u,\mathrm{det},y,X}$ with the quantities $\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}}$ and $\langle S_{c,k,u,y,X}\rangle_{\mathrm{det}}$, respectively. In the discussion, we use a shorthand notation $\boldsymbol{\chi}_{AB}^{i-1}:=(\boldsymbol{c}^{i-1},\boldsymbol{k}^{i-1},\boldsymbol{g}^{i-1},\boldsymbol{n}^{i-1},\boldsymbol{b}^{i-1},\boldsymbol{y}^{i-1})$, $\boldsymbol{\chi}_{A}^{i-1}:=(\boldsymbol{c}^{i-1},\boldsymbol{k}^{i-1},\boldsymbol{g}^{i-1},\boldsymbol{n}^{i-1})$ and $\boldsymbol{\chi}_{B}^{i-1}:=(\boldsymbol{b}^{i-1},\boldsymbol{y}^{i-1})$, and $\langle S_{c,k,u,y,X}\rangle_{\mathrm{det}}$ is defined as

$$\langle S_{c,k,u,y,X}\rangle_{\mathrm{det}}=\sum_{i\in\mathcal{S}_{\mathrm{det}}}p(c^i=c,k^i=k,t^i=u,y^i=y|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset,b^i=X)\delta(b^i,X). \tag{IV.3}$$

Here, $\delta(x,y)$ denotes the Kronecker delta. To relate Eq. (IV.3) with the number $S_{c,k,u,\mathrm{det},y,X}$, we introduce the following random variable

$$Y_{c,k,u,y,X}^j:=\Lambda_{c,k,u,y,X}^j-\sum_{i\in\mathcal{S}_{\mathrm{det}}^j}p(c^i=c,k^i=k,t^i=u,y^i=y|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset,b^i=X)\delta(b^i,X), \tag{IV.4}$$

where $\mathcal{S}_{\mathrm{det}}^j$ is the set containing the first j elements of the set $\mathcal{S}_{\mathrm{det}}$, and $\Lambda_{c,k,u,y,X}^j$ denotes the number of instances where (c,k,u,X,y) is realised among the set $\mathcal{S}_{\mathrm{det}}^j$, namely, $\Lambda_{c,k,u,y,X}^j=\sum_{i\in\mathcal{S}_{\mathrm{det}}^j}\delta(c^i,c)\delta(k^i,k)\delta(t^i,u)\delta(y^i,y)\delta(b^i,X)$. Then, the random variables $\{Y_{c,k,u,y,X}^j\}_{j=1}^{N_{\mathrm{det}}}$ satisfy Eq. (III.1), the Martingale condition [see Eq. (III.2)], the bounded difference condition [see Eq. (III.3)] and the zero-difference condition [see Eq. (III.4)] [1] :

$$p(|Y_{c,k,u,y,X}^j-Y_{c,k,u,y,X}^{j-1}|=0|\mathcal{F}_{j-1})\geq 1-p_X^B. \tag{IV.6}$$

---

[1] This statement can be proven as follows. Since $Y_{c,k,u,y,X}^j-Y_{c,k,u,y,X}^{j-1}$ is written as

$$Y_{c,k,u,y,X}^j-Y_{c,k,u,y,X}^{j-1}=\sum_{i\in\mathcal{S}_{\mathrm{det}}^j\setminus\mathcal{S}_{\mathrm{det}}^{j-1}}\Big[\delta(c^i,c)\delta(k^i,k)\delta(t^i,u)\delta(y^i,y)-p(c^i=c,k^i=k,t^i=u,y^i=y|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset,b^i=X)\Big]\delta(b^i,X), \tag{IV.5}$$

Here, we identify the filtration $\mathcal{F}_{j-1}$ with the random variables $(\boldsymbol{\chi}_{AB}^{\max\{i|i\in\mathcal{S}_{\rm det}^{j}\}-1})$. Therefore, we can apply the Modified Azuma's inequality in Eqs. (III.5) and (III.6), and we obtain

$$p\Big(S_{c,k,u,{\rm det},y,X}-\langle S_{c,k,u,y,X}\rangle_{\rm det}\geq g_{\rm MA}(\epsilon_{\rm MA}^{c,k,u,y,X},p_X^B,N_{\rm det})\Big)\leq\epsilon_{\rm MA}^{c,k,u,y,X} \tag{IV.7}$$

and

$$p\Big(S_{c,k,u,{\rm det},y,X}-\langle S_{c,k,u,y,X}\rangle_{\rm det}\leq -g_{\rm MA}(\epsilon_{\rm MA}^{c,k,u,y,X},p_X^B,N_{\rm det})\Big)\leq\epsilon_{\rm MA}^{c,k,u,y,X}. \tag{IV.8}$$

Here, $\epsilon_{\rm MA}^{c,k,u,y,X}$ denotes the failure probability associated to the estimation of $\langle S_{c,k,u,y,X}\rangle_{\rm det}$, and the function $g_{\rm MA}(\epsilon_{\rm MA}^{c,k,u,y,X},p_X^B,N_{\rm det})$ is defined in Eq. (III.7). Note that the quantity $S_{c,k,u,{\rm det},y,X}$ in Eqs. (IV.7) and (IV.8) is not directly observed in the actual experiments, and we only know its range, given that the number of tagged signals $n_{\rm tag}$ is upper bounded by $N_{\rm tag}$, as

$$S_{c,k,u,{\rm det},y,X}^{-}:=S_{c,k,{\rm det},y,X}-N_{\rm tag}\leq S_{c,k,u,{\rm det},y,X}\leq S_{c,k,{\rm det},y,X}, \tag{IV.9}$$

where $S_{c,k,{\rm det},y,X}:=|\mathcal{S}_{c,k,{\rm det},y,X}|$. By combining Eqs. (IV.7), (IV.8) and (IV.9), we obtain

$$S_{c,k,u,{\rm det},y,X}^{-}-g_{\rm MA}(\epsilon_{\rm MA}^{c,k,u,y,X},p_X^B,N_{\rm det})\leq\langle S_{c,k,u,y,X}\rangle_{\rm det}\leq S_{c,k,{\rm det},y,X}+g_{\rm MA}(\epsilon_{\rm MA}^{c,k,u,y,X},p_X^B,N_{\rm det}) \tag{IV.10}$$

except for error probability $2\epsilon_{\rm MA}^{c,k,u,y,X}$. The bounds on $S_{c,n=1,u,{\rm det},y,X}$ will be expressed as a function of the rhs and the lhs of Eq. (IV.10).

Next, we define the quantity $\langle S_{c,n,u,y,X}\rangle_{\rm det}$ that will be related to the number $S_{c,n,u,{\rm det},y,X}$ through the Modified Azuma's inequality as

$$\langle S_{c,n,u,y,X}\rangle_{\rm det}:=\sum_{i\in\mathcal{S}_{\rm det}}p(c^i=c,n^i=n,t^i=u,y^i=y|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset,b^i=X)\delta(b^i,X), \tag{IV.11}$$

and we follow the above arguments about the Modified Azuma's inequality. As a result, we obtain

$$\langle S_{c,n,u,y,X}\rangle_{\rm det}-g_{\rm MA}(\epsilon_{\rm MA}^{c,n,u,y,X},p_X^B,N_{\rm det})\leq S_{c,n,u,{\rm det},y,X}\leq\langle S_{c,n,u,y,X}\rangle_{\rm det}+g_{\rm MA}(\epsilon_{\rm MA}^{c,n,u,y,X},p_X^B,N_{\rm det}) \tag{IV.12}$$

except for error probability $2\epsilon_{\rm MA}^{c,n,u,y,X}$.

From Eqs. (IV.10) and (IV.12) obtained by means of the Modified Azuma's inequality, we find that the remaining task is to bound $\langle S_{c,1,u,y,X}\rangle_{\rm det}$ with $\{\langle S_{c,k,u,y,X}\rangle_{\rm det}\}_k$ such that $S_{c,1,u,{\rm det},y,X}$ can be bounded by the observed data appearing in Eq. (IV.10). Next, in step 2, we relate the expectation $\langle S_{c,k,u,y,X}\rangle_{\rm det}$ with $\{\langle S_{c,n,u,y,X}\rangle_{\rm det}\}_n$ through some functions $\{f_{c,n,u,y,X|{\rm det}}\}_n$, and then by using this relation we bound $\langle S_{c,1,u,y,X}\rangle_{\rm det}$ with $\{\langle S_{c,k,u,y,X}\rangle_{\rm det}\}_k$ in step 3.

---

we can confirm that the Martingale condition

$$\begin{aligned}E[Y_j-Y_{j-1}|\mathcal{F}_{j-1}]&=E\left[\sum_{i\in\mathcal{S}_{\rm det}^{j}\setminus\mathcal{S}_{\rm det}^{j-1}}\Big[\delta(c^i,c)\delta(k^i,k)\delta(t^i,u)\delta(y^i,y)-p(c^i=c,k^i=k,t^i=u,y^i=y|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset,b^i=X)\Big]\delta(b^i,X)\middle|\mathcal{F}_{j-1}\right]\\&=\sum_{i\in\mathcal{S}_{\rm det}^{j}\setminus\mathcal{S}_{\rm det}^{j-1}}p(c^i=c,k^i=k,t^i=u,y^i=y|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset,b^i=X)p(b^i=X|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset)\\&-\sum_{i\in\mathcal{S}_{\rm det}^{j}\setminus\mathcal{S}_{\rm det}^{j-1}}p(c^i=c,k^i=k,t^i=u,y^i=y|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset,b^i=X)p(b^i=X|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset)\\&=0\end{aligned}$$

holds. Also, Eq. (IV.5) assures the bounded difference condition: $|Y_j-Y_{j-1}|\leq 1$. Finally, from Eq. (IV.5) and using the assumptions (B-1) and (B-2), we obtain the zero-difference condition in Eq. (IV.6) as $p(|Y_{c,k,u,y,X}^{j}-Y_{c,k,u,y,X}^{j-1}|=0|\mathcal{F}_{j-1})\geq p(\sum_{i\in\mathcal{S}_{\rm det}^{j}\setminus\mathcal{S}_{\rm det}^{j-1}}\delta(b^i,X)=0|\mathcal{F}_{j-1})=1-p_X^B$.

2. Step 2. Upper and lower bounds on $\langle S_{c,k,u,y,X}\rangle_{\rm det}$ with $\{f_{c,n,u,y,X|\rm det}\}_n$

In this step, we bound $\langle S_{c,k,u,y,X}\rangle_{\rm det}$ in Eq. (IV.3) with $\{\langle S_{c,n,u,y,X}\rangle_{\rm det}\}_n$ through the functions $\{f_{c,n,u,y,X|\rm det}\}_n$. In the following discussion, we use the notation $\boldsymbol{g}^{\geq i} := g^i, g^{i+1}, ..., g^{N_{\rm sent}}$.

First, from the law of total probability, the definition (D-1) in the Results section and Bayes' theorem, Eq. (IV.3) can be rewritten as

$$\begin{aligned}\langle S_{c,k,u,y,X}\rangle_{\rm det} &= \sum_{i\in\mathcal{S}_{\rm det}}\sum_n\sum_{g^i\in\mathcal{G}^i_{\rm unt}}\sum_{\boldsymbol{g}^{\geq i+1}} p(c^i=c,k^i=k,n^i=n,\boldsymbol{g}^{\geq i},y^i=y|\boldsymbol{\chi}^{i-1}_{AB},y^i\neq\emptyset,b^i=X)\delta(b^i,X)\\ &= \sum_{i\in\mathcal{S}_{\rm det}}\sum_n\sum_{g^i\in\mathcal{G}^i_{\rm unt}}\sum_{\boldsymbol{g}^{\geq i+1}} p(k^i=k|c^i=c,n^i=n,\boldsymbol{g}^{\geq i},y^i\neq\emptyset,y^i=y,\boldsymbol{\chi}^{i-1}_{AB},b^i=X)\\ &\quad\times p(c^i=c,n^i=n,\boldsymbol{g}^{\geq i},y^i=y|\boldsymbol{\chi}^{i-1}_{AB},y^i\neq\emptyset,b^i=X)\delta(b^i,X). \end{aligned}\tag{IV.13}$$

Next, we calculate the first factor of Eq. (IV.13) to obtain Eq. (IV.20) below.

$$p(k^i=k|c^i=c,n^i=n,\boldsymbol{g}^{\geq i},y^i\neq\emptyset,y^i=y,\boldsymbol{\chi}^{i-1}_{AB},b^i=X)$$

$$=p(k^i=k|c^i=c,n^i=n,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{AB},b^i=X)\tag{IV.14}$$

$$=p(k^i=k|c^i=c,n^i=n,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{AB})\tag{IV.15}$$

$$=p(k^i=k|c^i=c,n^i=n,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A})\tag{IV.16}$$

$$=\frac{p(n^i=n|c^i=c,k^i=k,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A})p(k^i=k|c^i=c,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A})}{p(n^i=n|c^i=c,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A})}\tag{IV.17}$$

$$=\frac{p_k p(n^i=n|c^i=c,k^i=k,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A})}{\sum_{k'}p_{k'}p(n^i=n|c^i=c,k^i=k',\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A})}\tag{IV.18}$$

$$=\frac{p_k\sum_{\mu^i}p(n^i=n|c^i=c,k^i=k,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A},\mu^i)p(\mu^i|c^i=c,k^i=k,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A})}{\sum_{k'}p_{k'}\sum_{\mu^i}p(n^i=n|c^i=c,k^i=k',\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A},\mu^i)p(\mu^i|c^i=c,k^i=k',\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{A})}\tag{IV.19}$$

$$=\frac{p_k\sum_{\mu^i}p(n^i=n|\mu^i)\delta(\mu^i,\mu^i_{k,g^i})}{\sum_{k'}p_{k'}\sum_{\mu^i}p(n^i=n|\mu^i)\delta(\mu^i,\mu^i_{k',g^i})},\tag{IV.20}$$

where in Eq. (IV.14) we use the decoy-state property, namely, $p(y^i\neq\emptyset,y^i=y|k^i=k,c^i=c,n^i=n,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{AB},b^i=X)=p(y^i\neq\emptyset,y^i=y|c^i=c,n^i=n,\boldsymbol{g}^{\geq i},\boldsymbol{\chi}^{i-1}_{AB},b^i=X)$ holds. This is because once $\boldsymbol{g}^{N_{\rm sent}}$ is fixed, Eq. (II.1) assures that the total $N_{\rm sent}$ sending states have a tensor product structure which implies that the information of k^i is only encoded in the $i^{\rm th}$ sending system B^i, and the n-photon state in the system B^i is the same for any choice of k^i. In Eq. (IV.15) we use the assumption (B-2) in the Results section, in Eq. (IV.16) we recursively use the decoy-state property and the assumption (B-2), in Eqs. (IV.17) and (IV.19) we use the Bayes' theorem, and finally in Eqs. (IV.18) and (IV.20) we use Eq. (II.1).

In Eq. (IV.20), from Eq. (11), $\forall i\in\mathcal{S}_{\rm det}$ and $\forall g^i\in\mathcal{G}^i_{\rm unt}$, $\sum_{\mu^i}p(n^i=n|\mu^i)\delta(\mu^i,\mu^i_{k,g^i})$ can be upper [lower] bounded by $e^{-\mu_k^-}$ $[e^{-\mu_k^+}]$ for $n=0$ and $\frac{e^{-\mu_k^+}(\mu_k^+)^n}{n!}$ $[\frac{e^{-\mu_k^-}(\mu_k^-)^n}{n!}]$ for $n\geq1$, which we denote by ${\rm Pois}^{\rm U}(n|k,u)$ $[{\rm Pois}^{\rm L}(n|k,u)]$. With these bounds, $\langle S_{c,k,u,y,X}\rangle_{\rm det}$ can be upper and lower bounded as

$$\begin{aligned}\langle S_{c,k,u,y,X}\rangle_{\rm det} \leq& p_k\sum_n{\rm Pois}^{\rm U}(n|k,u)\sum_{i\in\mathcal{S}_{\rm det}}\sum_{g^i\in\mathcal{G}^i_{\rm unt}}\frac{p(c^i=c,n^i=n,g^i,y^i=y|\boldsymbol{\chi}^{i-1}_{AB},y^i\neq\emptyset,b^i=X)}{\sum_{k'}p_{k'}\sum_{\mu^i}p(n^i=n|\mu^i)\delta(\mu^i,\mu^i_{k',g^i})}\delta(b^i,X)\\ =&p_k\sum_n{\rm Pois}^{\rm U}(n|k,u)f_{c,n,u,y,X|\rm det},\end{aligned}\tag{IV.21}$$

where we define the function

$$f_{c,n,u,y,X|\rm det}=\sum_{i\in\mathcal{S}_{\rm det}}\sum_{g^i\in\mathcal{G}^i_{\rm unt}}\frac{p(c^i=c,n^i=n,g^i,y^i=y|\boldsymbol{\chi}^{i-1}_{AB},y^i\neq\emptyset,b^i=X)}{\sum_{k'}p_{k'}\sum_{\mu^i}p(n^i=n|\mu^i)\delta(\mu^i,\mu^i_{k',g^i})}\delta(b^i,X)\tag{IV.22}$$

and

$$\langle S_{c,k,u,y,X}\rangle_{\rm det}\geq p_k\sum_n{\rm Pois}^{\rm L}(n|k,u)f_{c,n,u,y,X|\rm det},\tag{IV.23}$$

respectively. It is notable that Eq. (IV.21) represents a linear combination of $\{f_{c,n,u,y,X|\mathrm{det}}\}_n$, and $f_{c,n,u,y,X|\mathrm{det}}$ is *independent* of k, which is crucial in the next discussion.

3. Step 3. Upper and lower bounds on $\langle S_{c,n=1,u,y,X}\rangle_{\mathrm{det}}$ with $\{\langle S_{c,k,u,y,X}\rangle_{\mathrm{det}}\}_k$

In this step, we derive an upper and lower bounds on $\langle S_{c,n=1,u,y,X}\rangle_{\mathrm{det}}$ with $\{\langle S_{c,k,u,y,X}\rangle_{\mathrm{det}}\}_k$.

(i) Upper bound on $\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}}$

First, we derive an upper bound on $\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}}$. From Eqs. (IV.21) and (IV.23), we have two inequalities: $\langle S_{c,k_2,u,y,X}\rangle_{\mathrm{det}} \geq p_{k_2}\sum_n \mathrm{Pois}^{\mathrm{L}}(n|k_2,u) f_{c,n,u,y,X|\mathrm{det}}$ and $\langle S_{c,k_3,u,y,X}\rangle_{\mathrm{det}} \leq p_{k_3}\sum_n \mathrm{Pois}^{\mathrm{U}}(n|k_3,u) f_{c,n,u,y,X|\mathrm{det}}$. By combining them and using the conditions $1 > \mu_{k_2}^{+}$ and $\mu_{k_2}^{-} > \mu_{k_3}^{+}$ (which we actually imposed in the protocol), $f_{c,1,u,y,X|\mathrm{det}}$ is upper bounded by

$$f_{c,1,u,y,X|\mathrm{det}} \leq \frac{\langle S_{c,k_2,u,y,X}\rangle_{\mathrm{det}}\mathrm{Pois}^{\mathrm{U}}(0|k_3,u)/p_{k_2} - \langle S_{c,k_3,u,y,X}\rangle_{\mathrm{det}}\mathrm{Pois}^{\mathrm{L}}(0|k_2,u)/p_{k_3}}{\mathrm{Pois}^{\mathrm{L}}(1|k_2,u)\mathrm{Pois}^{\mathrm{U}}(0|k_3,u) - \mathrm{Pois}^{\mathrm{U}}(1|k_3,u)\mathrm{Pois}^{\mathrm{L}}(0|k_2,u)}. \tag{IV.24}$$

Substituting the definition in Eq. (IV.22) gives the upper bound on $\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}}$ as

$$\begin{aligned}\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}} &= \sum_{i\in\mathcal{S}_{\mathrm{det}}} p(c^i=c,n^i=1,t^i=u,y^i=y|\boldsymbol{\chi}_{AB}^{i-1},y^i\neq\emptyset,b^i=X)\delta(b^i,X)\\ &\leq \frac{\langle S_{c,k_2,u,y,X}\rangle_{\mathrm{det}}\mathrm{Pois}^{\mathrm{U}}(0|k_3,u)/p_{k_2} - \langle S_{c,k_3,u,y,X}\rangle_{\mathrm{det}}\mathrm{Pois}^{\mathrm{L}}(0|k_2,u)/p_{k_3}}{\mathrm{Pois}^{\mathrm{L}}(1|k_2,u)\mathrm{Pois}^{\mathrm{U}}(0|k_3,u) - \mathrm{Pois}^{\mathrm{U}}(1|k_3,u)\mathrm{Pois}^{\mathrm{L}}(0|k_2,u)}\mathrm{Pois}^{\mathrm{U}}(1|u).\end{aligned} \tag{IV.25}$$

Here, we define $\mathrm{Pois}^{\mathrm{U}}(1|u) = \sum_{k\in\mathcal{K}} p_k \mathrm{Pois}^{\mathrm{U}}(1|k,u)$.

(ii) Lower bound on $\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}}$

Next, we derive a lower bound on $\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}}$. For this, we first use Eqs. (IV.21) and (IV.23), and we have three inequalities:

$$\begin{aligned}e^{\mu_{k_2}^{-}}\langle S_{c,k_2,u,y,X}\rangle_{\mathrm{det}} &\leq e^{\mu_{k_2}^{-}} p_{k_2}\sum_n \mathrm{Pois}^{\mathrm{U}}(n|k_2,u) f_{c,n,u,y,X|\mathrm{det}},\\ e^{\mu_{k_3}^{+}}\langle S_{c,k_3,u,y,X}\rangle_{\mathrm{det}} &\geq e^{\mu_{k_3}^{+}} p_{k_3}\sum_n \mathrm{Pois}^{\mathrm{L}}(n|k_3,u) f_{c,n,u,y,X|\mathrm{det}},\\ e^{\mu_{k_1}^{+}}\langle S_{c,k_1,u,y,X}\rangle_{\mathrm{det}} &\geq e^{\mu_{k_1}^{+}} p_{k_1}\sum_n \mathrm{Pois}^{\mathrm{L}}(n|k_1,u) f_{c,n,u,y,X|\mathrm{det}}.\end{aligned} \tag{IV.26}$$

By combining the first two inequalities, it is easy to show that

$$(\mu_{k_2}^{+}-\mu_{k_3}^{-}) f_{c,1,u,y,X|\mathrm{det}} \geq \frac{e^{\mu_{k_2}^{-}}\langle S_{c,k_2,u,y,X}\rangle_{\mathrm{det}}}{p_{k_2}} - \frac{e^{\mu_{k_3}^{+}}\langle S_{c,k_3,u,y,X}\rangle_{\mathrm{det}}}{p_{k_3}} - \sum_{n=2}^{\infty}\frac{(\mu_{k_2}^{+})^n-(\mu_{k_3}^{-})^n}{n!} f_{c,n,u,y,X|\mathrm{det}}. \tag{IV.27}$$

If we assume $\mu_{k_1}^{-} > \mu_{k_2}^{+}+\mu_{k_3}^{+}$ (which we actually imposed in the protocol), we have that $(\mu_{k_1}^{-})^2[(\mu_{k_2}^{+})^n-(\mu_{k_3}^{-})^n] \leq [(\mu_{k_2}^{+})^2-(\mu_{k_3}^{-})^2](\mu_{k_1}^{-})^n$ holds for $n\geq 2$ [4]. Therefore, Eq. (IV.27) leads to

$$(\mu_{k_2}^{+}-\mu_{k_3}^{-}) f_{c,1,u,y,X|\mathrm{det}} \geq \frac{e^{\mu_{k_2}^{-}}\langle S_{c,k_2,u,y,X}\rangle_{\mathrm{det}}}{p_{k_2}} - \frac{e^{\mu_{k_3}^{+}}\langle S_{c,k_3,u,y,X}\rangle_{\mathrm{det}}}{p_{k_3}} - \frac{(\mu_{k_2}^{+})^2-(\mu_{k_3}^{-})^2}{(\mu_{k_1}^{-})^2}\sum_{n=2}^{\infty}\frac{(\mu_{k_1}^{-})^n}{n!} f_{c,n,u,y,X|\mathrm{det}}, \tag{IV.28}$$

which is equivalent to

$$\begin{aligned}f_{c,1,u,y,X|\mathrm{det}} \geq{}& \frac{\mu_{k_1}^{-}}{(\mu_{k_2}^{+}-\mu_{k_3}^{-})(\mu_{k_1}^{-}-\mu_{k_2}^{+}-\mu_{k_3}^{-})}\Big[\frac{e^{\mu_{k_2}^{-}}\langle S_{c,k_2,u,y,X}\rangle_{\mathrm{det}}}{p_{k_2}} - \frac{e^{\mu_{k_3}^{+}}\langle S_{c,k_3,u,y,X}\rangle_{\mathrm{det}}}{p_{k_3}}\\ &- \frac{(\mu_{k_2}^{+})^2-(\mu_{k_3}^{-})^2}{(\mu_{k_1}^{-})^2}\Big(\sum_{n=0}^{\infty}\frac{(\mu_{k_1}^{-})^n}{n!} f_{c,n,u,y,X|\mathrm{det}} - f_{c,0,u,y,X|\mathrm{det}}\Big)\Big].\end{aligned} \tag{IV.29}$$

If we assume $1 > \mu_{k_1}^+$ (which we actually imposed in the protocol), by using in Eq. (IV.29), the third inequality in Eq. (IV.26) and the definition of $f_{c,1,u,y,X|\mathrm{det}}$ in Eq. (IV.22), we obtain the lower bound on $\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}}$ as a function of $\{\langle S_{c,k,u,y,X}\rangle_{\mathrm{det}}\}_k$ as

$$\begin{aligned}\langle S_{c,1,u,y,X}\rangle_{\mathrm{det}} \geq & \frac{\mu_{k_1}^- \mathrm{Pois}^{\mathrm{L}}(1|u)}{(\mu_{k_2}^+ - \mu_{k_3}^-)(\mu_{k_1}^- - \mu_{k_2}^+ - \mu_{k_3}^-)}\Big\{\frac{e^{\mu_{k_2}^-}\langle S_{c,k_2,u,y,X}\rangle_{\mathrm{det}}}{p_{k_2}} - \frac{e^{\mu_{k_3}^+}\langle S_{c,k_3,u,y,X}\rangle_{\mathrm{det}}}{p_{k_3}} \\ & - \frac{(\mu_{k_2}^+)^2 - (\mu_{k_3}^-)^2}{(\mu_{k_1}^-)^2}\Big(\frac{e^{\mu_{k_1}^+}\langle S_{c,k_1,u,y,X}\rangle_{\mathrm{det}}}{p_{k_1}}\Big)\Big\}. \end{aligned} \tag{IV.30}$$

Here, we define $\mathrm{Pois}^{\mathrm{L}}(1|u) = \sum_{k\in\mathcal{K}} p_k \mathrm{Pois}^{\mathrm{L}}(1|k,u)$.

4. *Step 4. Upper and lower bounds on* $S_{c,n=1,u,\mathrm{det},y,X}$ *with* $\{S_{c,k,\mathrm{det},y,X}\}_k$

In this step, we finally derive the upper and the lower bounds on $S_{c,n=1,u,\mathrm{det},y,X}$ with experimentally observed data $\{S_{c,k,\mathrm{det},y,X}\}_k$.

(i) Upper bound on $\boldsymbol{S_{c,1,u,\mathrm{det},y,X}}$

We combine Eqs. (IV.10) and (IV.12), which result from the application of the Modified Azuma's inequality, with Eq. (IV.25) to derive the upper bound on $S_{c,1,u,\mathrm{det},y,X}$.

$$\begin{aligned}& S_{c,1,u,\mathrm{det},y,X} \leq S^{\mathrm{U}}_{c,1,u,\mathrm{det},y,X} := \\ & \frac{\frac{[S_{c,k_2,\mathrm{det},y,X} + g_{\mathrm{MA}}(\epsilon_{\mathrm{MA}}^{c,k_2,u,y,X}, p_X^B, N_{\mathrm{det}})]\mathrm{Pois}^{\mathrm{U}}(0|k_3,u)}{p_{k_2}} - \frac{[S^-_{c,k_3,u,\mathrm{det},y,X} - g_{\mathrm{MA}}(\epsilon_{\mathrm{MA}}^{c,k_3,u,y,X}, p_X^B, N_{\mathrm{det}})]\mathrm{Pois}^{\mathrm{L}}(0|k_2,u)}{p_{k_3}}}{\mathrm{Pois}^{\mathrm{L}}(1|k_2,u)\mathrm{Pois}^{\mathrm{U}}(0|k_3,u) - \mathrm{Pois}^{\mathrm{U}}(1|k_3,u)\mathrm{Pois}^{\mathrm{L}}(0|k_2,u)} \\ & \times \mathrm{Pois}^{\mathrm{U}}(1|u) + g_{\mathrm{MA}}(\epsilon_{\mathrm{MA}}^{c,1,u,y,X}, p_X^B, N_{\mathrm{det}}) \end{aligned} \tag{IV.31}$$

except for error probability

$$\epsilon_{\mathrm{U}}^{c,1,u,y,X} := \sum_{k=k_2,k_3} \epsilon_{\mathrm{MA}}^{c,k,u,y,X} + \epsilon_{\mathrm{MA}}^{c,1,u,y,X}. \tag{IV.32}$$

(ii) Lower bound on $\boldsymbol{S_{c,1,u,\mathrm{det},y,X}}$

Similarly, we combine Eqs. (IV.10) and (IV.12) with Eq. (IV.30) to derive the lower bound on $S_{c,1,u,\mathrm{det},y,X}$.

$$\begin{aligned} S_{c,1,u,\mathrm{det},y,X} \geq S^{\mathrm{L}}_{c,1,u,\mathrm{det},y,X} := & \frac{\mu_{k_1}^- \mathrm{Pois}^{\mathrm{L}}(1|u)}{(\mu_{k_2}^+ - \mu_{k_3}^-)(\mu_{k_1}^- - \mu_{k_2}^+ - \mu_{k_3}^-)}\Big\{\frac{e^{\mu_{k_2}^-}[S^-_{c,k_2,u,\mathrm{det},y,X} - g_{\mathrm{MA}}(\epsilon_{\mathrm{MA}}^{c,k_2,u,y,X}, p_X^B, N_{\mathrm{det}})]}{p_{k_2}} \\ & - \frac{e^{\mu_{k_3}^+}[S_{c,k_3,\mathrm{det},y,X} + g_{\mathrm{MA}}(\epsilon_{\mathrm{MA}}^{c,k_3,u,y,X}, p_X^B, N_{\mathrm{det}})]}{p_{k_3}} \\ & - \frac{(\mu_{k_2}^+)^2 - (\mu_{k_3}^-)^2}{(\mu_{k_1}^-)^2}\Big(\frac{e^{\mu_{k_1}^+}[S_{c,k_1,\mathrm{det},y,X} + g_{\mathrm{MA}}(\epsilon_{\mathrm{MA}}^{c,k_1,u,y,X}, p_X^B, N_{\mathrm{det}})]}{p_{k_1}}\Big)\Big\} + g_{\mathrm{MA}}(\epsilon_{\mathrm{MA}}^{c,1,u,y,X}, p_X^B, N_{\mathrm{det}}) \end{aligned} \tag{IV.33}$$

except for error probability

$$\epsilon_{\mathrm{L}}^{c,1,u,y,X} := \sum_{k\in\mathcal{K}} \epsilon_{\mathrm{MA}}^{c,k,u,y,X} + \epsilon_{\mathrm{MA}}^{c,1,u,y,X}. \tag{IV.34}$$

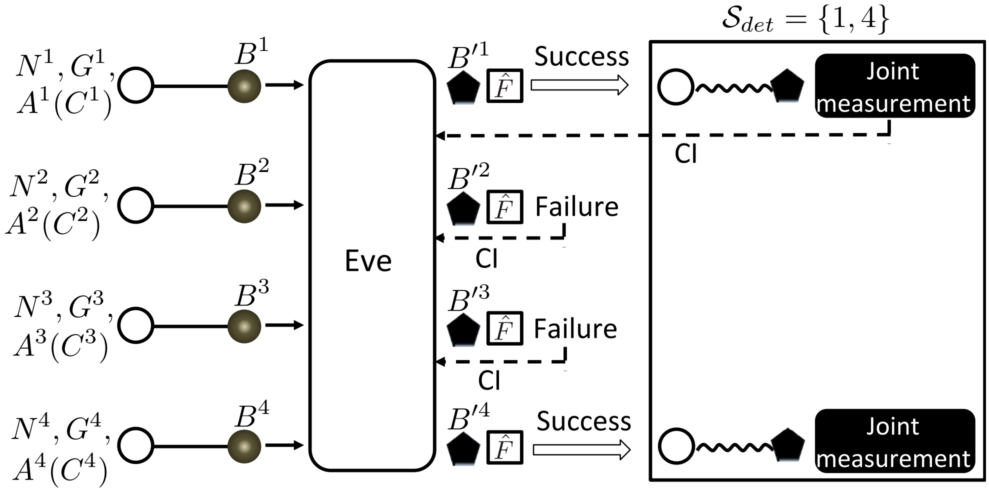

FIG. 1: Schematic representation of the virtual protocol for the case $N_{\rm sent} = 4$. For each i, Alice first sends the system B^i to Bob via the quantum channel. The eavesdropper performs an arbitrary operation on this system, and sends the system B'^i to Bob. Bob applies to the systems received the filter operation $\hat{F}$, and we classify the events into two cases depending on whether this filter operation is successful (the set of such successful events is denoted by $\mathcal{S}_{\rm det}$, in the example $\mathcal{S}_{\rm det} = \{1, 4\}$) or not. For the successful events, Alice and Bob perform a joint measurement on the systems $N^i, G^i, A^i(C^i)$ and B'^i depending if the outcomes of N^i and G^i are $n^i = 1$ and $g^i \in \mathcal{G}^i_{\rm unt}$ ($n^i \neq 1$ or $g^i \notin \mathcal{G}^i_{\rm unt}$), respectively. For the failure events, Alice performs a measurement on the systems N^i, G^i and C^i. In any case, once they have performed their measurements, Alice and Bob announce the relevant classical information (CI) over an authenticated public channel. This is illustrated with a dashed line in the figure. We can use this virtual protocol to prove the security of the actual protocol because the quantum and classical information that is accessible to Eve coincide in both cases (see Proposition 1).

B. Lower bound on $S_{Z,Z,1,u,\rm det}$

Just by following the same arguments that we use for the estimation of the bounds on $S_{c,1,u,{\rm det},y,X}$ in Secs. IV A 1-IV A 4, we find that $S_{Z,Z,1,u,\rm det}$ is lower bounded by the following quantity:

$$
\begin{aligned}
&S^{\rm L}_{Z,Z,1,u,\rm det} \\
&= \frac{\mu^-_{k_1}\sum_{k\in\mathcal{K}} p_k \mu^-_k e^{-\mu^-_k}}{(\mu^+_{k_2}-\mu^-_{k_3})(\mu^-_{k_1}-\mu^+_{k_2}-\mu^-_{k_3})}\Big\{\frac{e^{\mu^-_{k_2}}[S^-_{Z,Z,k_2,u,\rm det}-g_{\rm MA}(\epsilon^{Z,k_2,u}_{\rm MA},p^B_Z,N_{\rm det})]}{p_{k_2}} - \frac{e^{\mu^+_{k_3}}[S_{Z,Z,k_3,\rm det}+g_{\rm MA}(\epsilon^{Z,k_3,u}_{\rm MA},p^B_Z,N_{\rm det})]}{p_{k_3}} \\
&- \frac{(\mu^+_{k_2})^2-(\mu^-_{k_3})^2}{(\mu^-_{k_1})^2}\Big(\frac{e^{\mu^+_{k_1}}[S_{Z,Z,k_1,\rm det}+g_{\rm MA}(\epsilon^{Z,k_1,u}_{\rm MA},p^B_Z,N_{\rm det})]}{p_{k_1}}\Big)\Big\} + g_{\rm MA}(\epsilon^{Z,1,u}_{\rm MA},p^B_Z,N_{\rm det}) \qquad \text{(IV.35)}
\end{aligned}
$$

except for error probability

$$\epsilon_Z := \sum_{k\in\mathcal{K}} \epsilon^{Z,k,u}_{\rm MA} + \epsilon^{Z,1,u}_{\rm MA} + p_{\rm fail}. \qquad \text{(IV.36)}$$

Here, we define $S^-_{Z,Z,k_2,u,\rm det} := S_{Z,Z,k_2,\rm det} - N_{\rm tag}$.

V. DERIVATION OF THE PHASE ERROR RATE

In this section, we derive an upper bound on the phase error rate $e_{{\rm ph}|Z,Z,1,u,\rm det} = N_{{\rm ph},Z,Z,1,u,\rm det}/S_{Z,Z,1,u,\rm det}$. Importantly, the procedure introduced below is valid against coherent attacks. To derive an upper bound on $e_{{\rm ph}|Z,Z,1,u,\rm det}$, we need to obtain an upper bound on the number of phase errors $N_{{\rm ph},Z,Z,1,u,\rm det}$. Below, in the first subsection, we explain the derivation of $N_{{\rm ph},Z,Z,1,u,\rm det}$ with the restricted phase intervals in Eq. (23), and in the second subsection, we explain how to obtain $N_{{\rm ph},Z,Z,1,u,\rm det}$ with the general phase intervals in Eq. (10) from that with the restricted phase intervals.

A. Derivation of $N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$ with restricted phase intervals in Eq. (23)

First, from Eq. (II.1), we have that the total N_{sent} states can be expressed as

$$\sum_{\boldsymbol{g}^{N_{\mathrm{sent}}}} \sqrt{p(\boldsymbol{g}^{N_{\mathrm{sent}}})}|\boldsymbol{g}^{N_{\mathrm{sent}}}\rangle_{\boldsymbol{G}^{N_{\mathrm{sent}}}} \bigotimes_{i=1}^{N_{\mathrm{sent}}} |\Psi^i_{g^i}\rangle_{C^iK^iN^iB^i}|\theta^i_{c^i,g^i},\mu^i_{k^i,g^i}\rangle_{\Theta^iM^i} \tag{V.1}$$

with

$$|\Psi^i_{g^i}\rangle_{C^iK^iN^iB^i} := \sum_{c^i,k^i}\sqrt{p(c^i)p(k^i)}|c^i,k^i\rangle_{C^iK^i}\sum_{n^i}\sqrt{p(n^i|\mu^i_{k^i,g^i})}|n^i\rangle_{N^i}|\hat{\Upsilon}^i(\theta^i_{c^i,g^i},n^i)\rangle_{B^i}. \tag{V.2}$$

In particular, $|\hat{\Upsilon}^i(\theta^i_{c^i,g^i},1)\rangle_{B^i}$ can be expressed as

$$|\hat{\Upsilon}^i(\theta^i_{c^i,g^i},1)\rangle_{B^i} = (|1\rangle_{R^i}|0\rangle_{S^i} + e^{\mathrm{i}\theta^i_{c^i,g^i}}|0\rangle_{R^i}|1\rangle_{S^i})/\sqrt{2}, \tag{V.3}$$

and we define the eigenstates of the Y basis as $|Y\rangle_{B^i} := |1\rangle_{R^i}|0\rangle_{S^i}$ and $|Y^\perp\rangle_{B^i} := |0\rangle_{R^i}|1\rangle_{S^i}$, the ones of the Z basis are $|Z\rangle := (|Y\rangle+|Y^\perp\rangle)/\sqrt{2}$ and $|Z^\perp\rangle := (-\mathrm{i}|Y\rangle+\mathrm{i}|Y^\perp\rangle)/\sqrt{2}$, and the ones of the X basis are $|X\rangle := (|Z\rangle+|Z^\perp\rangle)/\sqrt{2}$ and $|X^\perp\rangle := (|Z\rangle-|Z^\perp\rangle)/\sqrt{2}$. This means that the state $|\hat{\Upsilon}^i(\theta^i_{c^i,g^i},1)\rangle_{B^i}$ can be rewritten in terms of the Z eigenstates as $|\hat{\Upsilon}^i(\theta^i_{c^i,g^i},1)\rangle_{B^i} = e^{\mathrm{i}\theta^i_{c^i,g^i}/2}(\cos\frac{\theta^i_{c^i,g^i}}{2}|Z\rangle_{B^i} + \sin\frac{\theta^i_{c^i,g^i}}{2}|Z^\perp\rangle_{B^i})$.

For convenience, we describe Alice's state preparation process of $|\Psi^i_{g^i}\rangle_{C^iK^iN^iB^i}$ for $g^i\in\mathcal{G}^i_{\mathrm{unt}}$ and $n^i=1$ by means of an entanglement-based scheme. That is, we assume that she first generates the state

$$|\Psi^i_{g^i,1}\rangle_{C^iK^iB^i} := \sum_{k^i}\sqrt{p(k^i)p(1|\mu^i_{k^i,g^i})}|k^i\rangle_{K^i}\left[\sqrt{p^A_Z}|\psi^i_Z(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i})\rangle_{C^iB^i} + \sqrt{p^A_X}e^{-\mathrm{i}\theta^i_{0_X,g^i}/2}|0_X\rangle_{C^i}|\hat{\Upsilon}^i(\theta^i_{0_X,g^i},1)\rangle_{B^i}\right] \tag{V.4}$$

with $|\psi^i_Z(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i})\rangle_{C^iB^i} := \sum_{x=0}^1 e^{-\mathrm{i}\theta^i_{x_Z,g^i}/2}|x_Z\rangle_{C^i}|\hat{\Upsilon}^i(\theta^i_{x_Z,g^i},1)\rangle_{B^i}/\sqrt{2}$, and afterwards she measures the system C^i to obtain c^i. In this subsection, given $c^i=c$ and $g^i\in\mathcal{G}^i_{\mathrm{unt}}$, we suppose that θ^i_{c,g^i} lies in the following interval for any i:

$$\theta^i_{0_Z,g^i}\in R^{0_Z}_{\mathrm{ph}} = [-\theta,\theta],\quad \theta^i_{1_Z,g^i}\in R^{1_Z}_{\mathrm{ph}} = [\pi-\theta,\pi+\theta],\quad \theta^i_{0_X,g^i}\in R^{0_X}_{\mathrm{ph}} = \left[\frac{\pi}{2}-\theta,\frac{\pi}{2}+\theta\right]\qquad\left(\text{with } 0\le\theta<\frac{\pi}{6}\right). \tag{V.5}$$

To prove the security of the key generated from the Z basis, we follow the definition of the phase error rate. That is, we consider Alice and Bob's hypothetical measurements on their systems C^i and B'^i (where B'^i represents the system B^i after Eve's intervention) in the X basis given that Alice prepared the state $|\psi^i_Z(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i})\rangle_{C^iB^i}$. In this virtual scenario, we have therefore, that Alice sends Bob the state $|\psi^i_{\mathrm{vir},m,g^i}\rangle_{B^i}$ with probability p^i_{vir,m,g^i} by projecting the system C^i in the basis $\{|+\rangle_{C^i},|-\rangle_{C^i}\}$ with $|\pm\rangle_{C^i} := (|0_Z\rangle_{C^i}\pm|1_Z\rangle_{C^i})/\sqrt{2}$, where

$$\begin{aligned}\hat{P}[|\psi^i_{\mathrm{vir},m,g^i}\rangle_{B^i}] =& \frac{\mathrm{tr}_{C^i}\left[\hat{P}[|m\rangle_{C^i}]\hat{P}[|\psi^i_Z(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i})\rangle_{C^iB^i}]\right]}{p^i_{\mathrm{vir},m,g^i}}\\ =&\begin{cases}\hat{P}[|\hat{\Upsilon}^i(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}}{2},1)\rangle_{B^i}] & (m=+),\\ \hat{P}[|\hat{\Upsilon}^i(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}}{2}+\pi,1)\rangle_{B^i}] & (m=-),\end{cases}\end{aligned} \tag{V.6}$$

and

$$p^i_{\mathrm{vir},\pm,g^i} = \mathrm{tr}\left[\hat{P}[|\pm\rangle_{C^i}]\hat{P}[|\psi^i_Z(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i})\rangle_{C^iB^i}]\right] = \frac{1\pm\cos\frac{\theta^i_{0_Z,g^i}-\theta^i_{1_Z,g^i}}{2}}{2}. \tag{V.7}$$

For later convenience, we define

$$\theta^i_{0_{\mathrm{vir}},g^i} := \frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}}{2},\quad \theta^i_{1_{\mathrm{vir}},g^i} := \frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}}{2}+\pi. \tag{V.8}$$

Thanks to Proposition 1 below, we are allowed to evaluate the security of the actual protocol by using the virtual scheme illustrated in Fig. 1. In particular, we consider a virtual protocol where for each signal emission, Alice can in principle prepare the following state if $g^i \in \mathcal{G}^i_{\text{unt}}$ and $n^i = 1$ instead of $|\Psi^i_{g^i,1}\rangle_{C^iK^iB^i}$ as

$$|\Psi^i_{g^i,1,\text{vir}}\rangle_{A^iK^iB^i} = \sum_{k^i} \sqrt{p(k^i)p(1|\mu^i_{k^i,g^i})}|k^i\rangle_{K^i} \left[\sum_{\alpha^i=0}^{4} \sqrt{p^i_{\alpha^i,g^i}}|\alpha^i\rangle_{A^i}|\psi^i_{\alpha^i,g^i}\rangle_{B^i}\right], \tag{V.9}$$

where the system A^i is stored by Alice in a quantum memory. Here, the states $\{|\psi^i_{\alpha^i,g^i}\rangle\}_{\alpha^i}$ are defined as

$$\begin{aligned} |\psi^i_{0,g^i}\rangle = |\psi^i_{\text{vir},+,g^i}\rangle,\ |\psi^i_{1,g^i}\rangle = |\psi^i_{\text{vir},-,g^i}\rangle, \\ |\psi^i_{2,g^i}\rangle = |\hat{\Upsilon}(\theta^i_{0_Z,g^i},1)\rangle,\ |\psi^i_{3,g^i}\rangle = |\hat{\Upsilon}(\theta_{1_Z,g^i},1)\rangle \text{ and } |\psi^i_{4,g^i}\rangle = |\hat{\Upsilon}(\theta_{0_X,g^i},1)\rangle, \end{aligned} \tag{V.10}$$

and the probabilities $\{p^i_{\alpha^i,g^i}\}_{\alpha^i}$ are given by

$$p^i_{0,g^i} = p^A_Z p^B_Z p^i_{\text{vir},+,g^i},\ p^i_{1,g^i} = p^A_Z p^B_Z p^i_{\text{vir},-,g^i},\ p^i_{2,g^i} = p^i_{3,g^i} = p^A_Z p^B_X/2 \text{ and } p^i_{4,g^i} = p^A_X. \tag{V.11}$$

Alice sends Bob the system B^i in Eq. (V.1), and Eve performs an arbitrary operation on this system. On the receiving side, thanks to the assumption (B-1) in the Results section, Bob can apply the filter operation $\hat{F}$ to the system B'^i to determine whether he will have a detection event ($y^i \neq \emptyset$) or not ($y^i = \emptyset$) prior to selecting the measurement basis, which is represented by the Kraus operators $\left\{\sqrt{\hat{I}_{B'^i} - \hat{M}_\emptyset}, \sqrt{\hat{M}_\emptyset}\right\}$. Depending on this result, we classify all the emissions into two types of events:

(i) a successful event (which is associated to the operator $\sqrt{\hat{I}_{B'^i} - \hat{M}_\emptyset}$),

and

(ii) a failure event (which is associated to the operator $\sqrt{\hat{M}_\emptyset}$).

We denote the set of successful events by $\mathcal{S}_{\text{det}} := \{i|y^i \neq \emptyset\}$ where $S_{\text{det}} := |\mathcal{S}_{\text{det}}|$. Afterwards, we consider that Alice and Bob perform joint measurements on all the signals. In particular, for the successful event identified above as (i), we suppose that Alice measures her systems N^i and G^i, and if the outcomes are $n^i = 1$ and $g^i \in \mathcal{G}^i_{\text{unt}}$, she measures the systems A^i to obtain the outcome $\alpha^i \in \{0,1,2,3,4\}$. If $\alpha^i \in \{0,1,2,3\}$, then Bob measures the system B'^i in the X basis to obtain the outcome $y^i \in \{0,1\}$, and if $\alpha^i = 4$, then Bob measures the system B'^i in the Z (X) basis with probability p^B_Z (p^B_X) and obtains the outcome $y^i \in \{0,1\}$. Also, among the successful events of the type (i), if $n^i \neq 1$ or $g^i \notin \mathcal{G}^i_{\text{unt}}$, Alice and Bob measure their systems C^i and B'^i and obtain the outcomes $c^i \in \mathcal{C}$ and $y^i \in \{0,1\}$.

For the failure event identified above as (ii), Alice measures her systems N^i, G^i and C^i and obtains the outcomes $n^i \in [0,\infty)$, $g^i \in \mathcal{G}^i_{\text{unt}} \cup \overline{\mathcal{G}^i_{\text{unt}}}$ and $c^i \in \mathcal{C}$, respectively. Importantly, it can be shown that, from Eve's perspective, this virtual protocol is completely equivalent to the actual protocol given that Alice and Bob's announcements and classical post-processing are chosen appropriately.

Proposition 1 *From Eve's perspective, the virtual protocol described above is equivalent to the actual protocol, namely, the quantum and classical information available to Eve are exactly the same for both protocols. Also, the correspondence between classical information* (c^i, k^i) *and the quantum state in the actual protocol is identical to the one of the virtual protocol.*

Proof of Proposition 1. First, we show that Eve's accessible quantum information is the same in both protocols. The case of the tagged signal ($t^i = t$) or non-single-photon ($n^i \neq 1$) emissions is clear, as the quantum states sent by Alice in both schemes coincide. Hence, the quantum information that is available to Eve is obviously the same in this case. As for the untagged single-photon emissions, we have that in the virtual protocol Alice sends Bob the virtual states [see Eq. (V.9)], while in the actual protocol, she does not. Still, we have that also in this case Eve's accessible quantum information of the system B^i is the same between the two protocols because the following relation

$$\text{tr}_{A^iK^i}\hat{P}[|\Psi^i_{g^i,1,\text{vir}}\rangle_{A^iK^iB^i}] = \text{tr}_{C^iK^i}\hat{P}[|\Psi^i_{g^i,1}\rangle_{C^iK^iB^i}] \tag{V.12}$$

holds. To conclude, we show that Eve's accessible classical information is also equal in both protocols. For the case of the tagged signal ($t^i = t$) or non-single-photon ($n^i \neq 1$) emission event, since the quantum states are the same in both the actual and virtual protocols, the classical information declared by Alice and Bob in both schemes coincide. Hence, we only need to consider the equivalence between both protocols for the case of $n^i = 1$ and $t^i = u$. For this, we suppose that after finishing each of their joint measurements, Alice and Bob announce the classical information as follows. Whenever their measurement outcome on the system A^i is $\alpha^i \in \{0,1\}$, Alice and Bob declare over an authenticated public channel the Z basis. Also, Alice (Bob) announces the Z basis (X basis and its measurement outcome) when $\alpha^i \in \{2,3\}$. Finally, if $\alpha^i = 4$ and Bob's basis choice is Z (X), Alice announces the X basis and Bob announces the Z (X) basis and its measurement outcome. This way, it is easy to see that the classical information announced in the actual and virtual protocols coincide. Furthermore, due to Eq. (V.2), we can confirm that the correspondence between the classical information (c^i, k^i) and the quantum state in the actual protocol is equivalent to the one of the virtual protocol. This ends the proof of the Proposition. ■

Thanks to this Proposition, the security statements that we derive for the virtual protocol can be applied as well to the actual protocol.

Next, we describe the state of the i^{th} systems G^i, C^i, K^i, N^i and B'^i from Alice and Bob's point of view. Given that Bob has finished measuring the $(i-1)^{\text{th}}$ incoming pulse, Alice and Bob obtained the measurement outcomes $\boldsymbol{\zeta}^{i-1} := (\boldsymbol{n}^{i-1}, \boldsymbol{g}^{i-1}, \boldsymbol{\gamma}^{i-1}, \boldsymbol{y}^{i-1})$ with γ^i being α^i or c^i depending on whether the measured system is A^i or C^i. Once the outcome $\boldsymbol{\zeta}^{i-1}$ and $\boldsymbol{g}^{\geq i}$ are fixed, the operation acting on the system B^i is mathematically modeled by the completely positive (CP) map $\Lambda^i_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}$ that includes Eve's operation depending on the iterative information $\boldsymbol{I}^{i-1}$ announced by Alice and Bob up to the $(i-1)^{\text{th}}$ trials. With this CP map, the state in the i^{th} systems G^i, C^i, K^i, N^i and B'^i is of the form

$$\frac{\hat{\sigma}_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1}}}{\mathrm{tr}[\hat{\sigma}_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1}}]}, \tag{V.13}$$

where $\hat{\sigma}_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1}}$ is defined as

$$\begin{aligned}
\hat{\sigma}_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1}} &:= \sum_{\boldsymbol{g}^{\geq i+1}} p(\boldsymbol{g}^{i-1}, \boldsymbol{g}^{\geq i+1}) \hat{P}\left[\sum_{g^i} \sqrt{p(g^i|\boldsymbol{g}^{i-1}, \boldsymbol{g}^{\geq i+1})}\Lambda^i_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}(|g^i\rangle_{G^i}|\Psi^i_{g^i}\rangle_{C^i,K^i,N^i,B^i})\right] \\
&= \sum_{s^i}\sum_{\boldsymbol{g}^{\geq i+1}} p(\boldsymbol{g}^{i-1}, \boldsymbol{g}^{\geq i+1}) \hat{P}\left[\sum_{g^i} \sqrt{p(g^i|\boldsymbol{g}^{i-1}, \boldsymbol{g}^{\geq i+1})}\hat{A}^i_{s^i,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}|g^i\rangle_{G^i}|\Psi^i_{g^i}\rangle_{C^i,K^i,N^i,B^i}\right].
\end{aligned} \tag{V.14}$$

Here, the set of Kraus operators $\{\hat{A}^i_{s^i,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\}_{s^i}$ acting on the system B^i depends on the measurement results $\boldsymbol{\zeta}^{i-1}$ and the iterative information $\boldsymbol{I}^{i-1}$ announced by Alice and Bob.

Let us now derive an upper bound on the number of phase errors $N_{\mathrm{ph},Z,Z,1,u,\mathrm{det}}$. For this, we consider the joint measurement performed by Alice and Bob on the i^{th} event with $i \in \mathcal{S}_{\mathrm{det}}$. In particular, we are interested in the probability of obtaining the measurement outcome $n^i = 1$ on the system N^i, the measurement outcome $g^i \in \mathcal{G}^i_{\mathrm{unt}}$ (namely, $t^i = u$) on the system G^i, the measurement outcome $\alpha^i = \alpha \in \{0,1,2,3,4\}$ on the system A^i, and the measurement outcome $y^i = y \in \{0,1\}$ in the X basis measurement on the system B'^i given that Bob's filter operation $\hat{F}$ was successful. Such probability can be expressed as

$$\begin{aligned}
&p(n^i = 1, t^i = u, \alpha^i = \alpha, b^i = X, y^i = y|\boldsymbol{\zeta}^{i-1}, y^i \neq \emptyset) \\
=&\mathrm{tr}\left\{\sum_{g^i\in\mathcal{G}^i_{\mathrm{unt}}} \hat{P}[|1\rangle_{N^i}|g^i\rangle_{G^i}|\alpha\rangle_{A^i}] \otimes q_\alpha \hat{M}_{y,X}\frac{\hat{\sigma}_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1}}}{\mathrm{tr}[\mathcal{E}^i(\hat{\sigma}_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1}})]}\right\} \\
=&\sum_{g^i\in\mathcal{G}^i_{\mathrm{unt}}}\sum_{\boldsymbol{g}^{\geq i+1}} p(\boldsymbol{g}^{N_{\mathrm{sent}}})\sum_{k^i} p(k^i)p(1|\mu_{k^i,g^i})\frac{\mathrm{tr}\left[q_\alpha p^i_{\alpha,g^i}\sum_{s^i}(\hat{A}^i_{s^i,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}})^\dagger \hat{M}_{y,X}(\hat{A}^i_{s^i,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}})\hat{P}[|\psi^i_{\alpha,g^i}\rangle_{B^i}\right]}{\mathrm{tr}[\mathcal{E}^i(\hat{\sigma}_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1}})]} \\
=&\left\langle C^i_{g^i} q_\alpha p^i_{\alpha,g^i}\mathrm{tr}\left[\hat{T}^i_{y,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{P}[|\psi^i_{\alpha,g^i}\rangle_{B^i}]\right]\right\rangle.
\end{aligned} \tag{V.15}$$

Here, we define $\mathcal{E}^i(\hat{\rho}) := \sqrt{\hat{I}_{B'^i} - \hat{M}_\emptyset}\hat{\rho}\sqrt{\hat{I}_{B'^i} - \hat{M}_\emptyset}^\dagger$, $C^i_{g^i} := \sum_{k^i} p(k^i)p(1|\mu_{k^i,g^i})$, $q_\alpha := 1$ for $\alpha \in \{0,1,2,3\}$ and $q_4 := p^B_X$. Also, we define the operator $\hat{T}^i_{y,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}$ as

$$\hat{T}^i_{y,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}} := \frac{\sum_{s^i}(\hat{A}^i_{s^i,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}})^\dagger \hat{M}_{y,X}(\hat{A}^i_{s^i,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}})}{\mathrm{tr}[\mathcal{E}^i(\hat{\sigma}_{\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1}})]}. \tag{V.16}$$

In Eq. (V.15), for convenience of notation, we have defined $\langle A\rangle := \sum_{g^i\in\mathcal{G}^i_{\rm unt}}\sum_{\boldsymbol{g}^{\geq i+1}} p(\boldsymbol{g}^{N_{\rm sent}})A$.

If we define $N_{1,u,\alpha,y,X}$ as the number of events where Alice obtains the measurement outcome $n^i=1$ on the system N^i, $g^i\in\mathcal{G}^i_{\rm unt}$ on the system G^i, $\alpha^i=\alpha\in\{0,1\}$ on her system A^i and Bob obtains the outcome $y^i=y\in\{0,1\}$ in the X basis measurement on the system B'^i, the phase error rate is defined as the rate at which Bob obtains the outcome $y^i=\alpha\oplus1$ on the system B'^i among $\sum_{\alpha=0,1,y=0,1}N_{1,u,\alpha,y,X}$. The phase error rate for the untagged single-photon emissions can be expressed as

$$e_{{\rm ph}|Z,Z,1,u,{\rm det}}=\frac{\sum_{\alpha=0}^{1}N_{1,u,\alpha,y=\alpha\oplus1,X}}{\sum_{\alpha=0}^{1}\sum_{y=0}^{1}N_{1,u,\alpha,y,X}}=:\frac{N_{{\rm ph},Z,Z,1,u,{\rm det}}}{\sum_{\alpha=0}^{1}\sum_{y=0}^{1}N_{1,u,\alpha,y,X}}=\frac{N_{{\rm ph},Z,Z,1,u,{\rm det}}}{S_{Z,Z,1,u,{\rm det}}}. \tag{V.17}$$

In the third equality, we use the assumption (B-1) in the Results section which states that the efficiency of Bob's measurement is the same for the bases Z and X. In Eq. (V.17), the denominator can be estimated directly with the decoy-state method. Next, we calculate an upper bound for the quantity $N_{{\rm ph},Z,Z,1,u,{\rm det}}$. For this, we first relate $N_{{\rm ph},Z,Z,1,u,{\rm det}}$ with the sum of the probabilities $\sum_{\alpha=0}^{1}p(n^i=1,t^i=u,\alpha^i=\alpha,b^i=X,y^i=\alpha\oplus1|\boldsymbol{\zeta}^{i-1},y^i\neq\emptyset)$ over $i\in\mathcal{S}_{\rm det}$. This can be done by using Azuma's inequality [2]; we obtain

$$p\left(N_{{\rm ph},Z,Z,1,u,{\rm det}}-\sum_{i\in\mathcal{S}_{\rm det}}\sum_{\alpha=0}^{1}p(n^i=1,t^i=u,\alpha^i=\alpha,b^i=X,y^i=\alpha\oplus1|\boldsymbol{\zeta}^{i-1},y^i\neq\emptyset)\geq g_{\rm A}(N_{\rm det},\epsilon_{\rm A}^{{\rm ph},Z,1,u})\right)\leq\epsilon_{\rm A}^{{\rm ph},Z,1,u}, \tag{V.18}$$

where $g_{\rm A}(x,y):=\sqrt{2x\ln1/y}$. From Eqs. (V.15) and (V.18), we have that $N_{{\rm ph},Z,Z,1,u,{\rm det}}$ can be upper-bounded by

$$N_{{\rm ph},Z,Z,1,u,{\rm det}}\leq\sum_{i\in\mathcal{S}_{\rm det}}\sum_{\alpha=0}^{1}\left\langle C^i_{g^i}p^i_{\alpha,g^i}{\rm tr}\left[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{P}[|\psi^i_{\alpha,g^i}\rangle_{B^i}]\right]\right\rangle+g_{\rm A}(N_{\rm det},\epsilon_{\rm A}^{{\rm ph},Z,1,u}) \tag{V.19}$$

except for error probability $\epsilon_{\rm A}^{{\rm ph},Z,1,u}$. The first term on the rhs represents the transmission rate of the virtual states $|\psi^i_{0,g^i}\rangle_{B^i}$ and $|\psi^i_{1,g^i}\rangle_{B^i}$. To upper bound this quantity using the experimentally available data, we express ${\rm tr}\left[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{P}[|\hat{\Upsilon}(\theta^i_{c,g^i},1)\rangle_{B^i}]\right]$ for $g^i\in\mathcal{G}^i_{\rm unt}$ and $c\in\mathcal{C}$, in terms of the transmission rates of the Pauli operators $\hat{I}_{B^i},\hat{X}_{B^i}$ and $\hat{Z}_{B^i}$. In particular, since $\hat{P}[|\hat{\Upsilon}(\theta,1)\rangle_{B^i}]$ can be decomposed as $\hat{P}[|\hat{\Upsilon}(\theta,1)\rangle_{B^i}]=(\hat{I}_{B^i}+\sin\theta\hat{X}_{B^i}+\cos\theta\hat{Z}_{B^i})/2$, we have that

$$\begin{pmatrix}{\rm tr}[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{P}[|\hat{\Upsilon}^i(\theta^i_{0_Z,g^i},1)\rangle_{B^i}]\\ {\rm tr}[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{P}[|\hat{\Upsilon}^i(\theta^i_{1_Z,g^i},1)\rangle_{B^i}]\\ {\rm tr}[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{P}[|\hat{\Upsilon}^i(\theta^i_{0_X,g^i},1)\rangle_{B^i}]\end{pmatrix}=M^i_{g^i}\begin{pmatrix}{\rm tr}[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{I}_{B^i}/2]\\ {\rm tr}[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{X}_{B^i}/2]\\ {\rm tr}[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{Z}_{B^i}/2]\end{pmatrix}, \tag{V.20}$$

where $M^i_{g^i}:=(\vec{V}^i_{0_Z,g^i},\vec{V}^i_{1_Z,g^i},\vec{V}^i_{0_X,g^i})^{\rm T}$ with $(\vec{V}^i_{c,g^i})^{\rm T}:=(1,\sin\theta^i_{c,g^i},\cos\theta^i_{c,g^i})$, and where T represents the transpose operator. To calculate ${\rm tr}[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{I}_{B^i}/2]$, ${\rm tr}[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{X}_{B^i}/2]$, and ${\rm tr}[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\geq i}}\hat{Z}_{B^i}/2]$, we use information from the states that are sent in the actual protocol. In doing so, we can upper-bound the first term of the rhs in Eq. (V.19) as

$$\begin{aligned}
&\sum_{i\in\mathcal{S}_{\rm det}}\sum_{\alpha=0}^{1}\Big\langle C^i_{g^i}p^i_{\alpha,g^i}{\rm tr}\Big[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\ge i}}\hat{P}[|\psi^i_{\alpha,g^i}\rangle_{B^i}]\Big]\Big\rangle\\
&\le\sum_{\alpha=0}^{1}p^{\rm U}_\alpha\sum_{i\in\mathcal{S}_{\rm det}}\Big\langle C^i_{g^i}{\rm tr}\Big[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\ge i}}\hat{P}[|\psi^i_{\alpha,g^i}\rangle_{B^i}]\Big]\Big\rangle\\
&=\sum_{\alpha=0}^{1}p^{\rm U}_\alpha\sum_{i\in\mathcal{S}_{\rm det}}\Big\langle C^i_{g^i}{\rm tr}\Big[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\ge i}}\Big(\hat{I}_{B^i}/2+\sin\theta^i_{\alpha_{\rm vir},g^i}\hat{X}_{B^i}/2+\cos\theta^i_{\alpha_{\rm vir},g^i}\hat{Z}_{B^i}/2\Big)\Big]\Big\rangle\\
&=\sum_{\alpha=0}^{1}p^{\rm U}_\alpha\sum_{i\in\mathcal{S}_{\rm det}}\Bigg\langle C^i_{g^i}\sum_{c\in\mathcal{C}}{\rm tr}\Big[\Gamma^i_{\alpha,c,g^i}\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\ge i}}\hat{P}[|\hat{\Upsilon}(\theta^i_{c,g^i},1)\rangle_{B^i}]\Big]\Bigg\rangle\\
&\le\sum_{\alpha=0}^{1}p^{\rm U}_\alpha\sum_{c\in\mathcal{C}}\Gamma^{\rm U}_{\alpha,c}\sum_{i\in\mathcal{S}_{\rm det}}\Big\langle C^i_{g^i}{\rm tr}\Big[\hat{T}^i_{\alpha\oplus1,X,\boldsymbol{\zeta}^{i-1},\boldsymbol{I}^{i-1},\boldsymbol{g}^{\ge i}}\hat{P}[|\hat{\Upsilon}(\theta^i_{c,g^i},1)\rangle_{B^i}]\Big]\Big\rangle\\
&=\sum_{\alpha=0}^{1}p^{\rm U}_\alpha\Big(\Gamma^{\rm U}_{\alpha,0_Z}\sum_{i\in\mathcal{S}_{\rm det}}p(n^i=1,t^i=u,\alpha^i=2,b^i=X,y^i=\alpha\oplus1|\boldsymbol{\zeta}^{i-1},y^i\neq\emptyset)/p^i_{2,g^i}\\
&+\Gamma^{\rm U}_{\alpha,1_Z}\sum_{i\in\mathcal{S}_{\rm det}}p(n^i=1,t^i=u,\alpha^i=3,b^i=X,y^i=\alpha\oplus1|\boldsymbol{\zeta}^{i-1},y^i\neq\emptyset)/p^i_{3,g^i}\\
&+\Gamma^{\rm U}_{\alpha,0_X}\sum_{i\in\mathcal{S}_{\rm det}}p(n^i=1,t^i=u,\alpha^i=4,b^i=X,y^i=\alpha\oplus1|\boldsymbol{\zeta}^{i-1},y^i\neq\emptyset)/p^B_Xp^i_{4,g^i}\Big).
\end{aligned}\tag{V.21}$$

In the first inequality, the parameter $p^{\rm U}_\alpha$ (with $\alpha\in\{0,1\}$) is an upper bound on $p^i_{0(1),g^i}:=p^A_Zp^B_Zp^i_{{\rm vir},+(-),g^i}$, where $p^i_{{\rm vir},\pm,g^i}$ is defined in Eq. (V.7), and these quantities are given by

$$p^{\rm U}_0=p^{\rm U}_1=p^A_Zp^B_Z(1+\sin\theta)/2.\tag{V.22}$$

In the first equality in Eq. (V.21), the parameters $\theta^i_{0_{\rm vir},g^i}$ and $\theta^i_{1_{\rm vir},g^i}$ are defined in Eq. (V.8). The second equality in Eq. (V.21) is due to Eq. (V.20) and the parameters $\{\Gamma^i_{\alpha,c,g^i}\}_{\alpha,c}$, which connect the transmission rates of the Pauli operators to those of the actual states, are respectively given by [1]

$$
\begin{aligned}
&\Gamma^i_{0,0_Z,g^i}(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i},\theta^i_{0_X,g^i})\\
&=\sin\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)\left[\sin\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)-\sin\left(\frac{-3\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}+2\theta^i_{0_X,g^i}}{4}\right)\right]^{-1},\\
&\Gamma^i_{0,1_Z,g^i}(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i},\theta^i_{0_X,g^i})\\
&=\sin\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)\left[\sin\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)+\sin\left(\frac{-\theta^i_{0_Z,g^i}+3\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)\right]^{-1},\\
&\Gamma^i_{0,0_X,g^i}(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i},\theta^i_{0_X,g^i})\\
&=\left[1-\cos\left(\frac{\theta^i_{0_Z,g^i}-\theta^i_{1_Z,g^i}}{2}\right)\right]\left[\cos\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{2}\right)-\cos\left(\frac{\theta^i_{0_Z,g^i}-\theta^i_{1_Z,g^i}}{2}\right)\right]^{-1},\\
&\Gamma^i_{1,0_Z,g^i}(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i},\theta^i_{0_X,g^i})\\
&=\cos\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)\left[\cos\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)-\cos\left(\frac{-3\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}+2\theta^i_{0_X,g^i}}{4}\right)\right]^{-1},\\
&\Gamma^i_{1,1_Z,g^i}(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i},\theta^i_{0_X,g^i})\\
&=\cos\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)\left[\cos\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)-\cos\left(\frac{-\theta^i_{0_Z,g^i}+3\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{4}\right)\right]^{-1},\\
&\Gamma^i_{1,0_X,g^i}(\theta^i_{0_Z,g^i},\theta^i_{1_Z,g^i},\theta^i_{0_X,g^i})\\
&=\left[-1-\cos\left(\frac{\theta^i_{0_Z,g^i}-\theta^i_{1_Z,g^i}}{2}\right)\right]\left[\cos\left(\frac{\theta^i_{0_Z,g^i}+\theta^i_{1_Z,g^i}-2\theta^i_{0_X,g^i}}{2}\right)-\cos\left(\frac{\theta^i_{0_Z,g^i}-\theta^i_{1_Z,g^i}}{2}\right)\right]^{-1}.
\end{aligned}
\tag{V.23}
$$

In addition, the parameter $\Gamma^{\rm U}_{\alpha,c}$ that appears in the second inequality within Eq. (V.21) represents an upper bound on Γ^i_{α,c,g^i} in the range of $g^i\in\mathcal{G}^i_{\rm unt}$. If the conditions stated in Eq. (V.5) are satisfied, we have that these quantities have the form [1]: $\Gamma^{\rm U}_{0,0_Z}=\frac{\sin\theta}{\sin\theta+\cos\frac{3}{2}\theta}$, $\Gamma^{\rm U}_{0,1_Z}=\Gamma^{\rm U}_{0,0_Z}$, $\Gamma^{\rm U}_{0,0_X}=\frac{1-\sin\theta}{\cos2\theta-\sin\theta}$, $\Gamma^{\rm U}_{1,0_Z}=\frac{\cos\theta}{\cos\theta-\sin\frac{3}{2}\theta}$, $\Gamma^{\rm U}_{1,1_Z}=\Gamma^{\rm U}_{1,0_Z}$, and $\Gamma^{\rm U}_{1,0_X}=-\frac{1-\sin\theta}{1+\sin\theta}$. Finally, the last equality in Eq. (V.21) is due to Eq. (V.15), where we note that p^i_{2,g^i},p^i_{3,g^i} and p^i_{4,g^i} are constant values [see Eq. (V.11)].

The next step is to relate the sum of the probabilities $\sum_{i\in\mathcal{S}_{\rm det}}p(n^i=1,t^i=u,\alpha^i=\beta,b^i=X,y^i=\alpha\oplus1|\boldsymbol{\zeta}^{i-1},y^i\neq\emptyset)$ with $\beta\in\{2,3,4\}$ that appear in Eq. (V.21) to the actual number of such events, which we denote by $S_{c,1,u,{\rm det},\alpha\oplus1,X}$ with $c\in\mathcal{C}$ [2]. For this, we again use Azuma's inequality [2], and we obtain

$$
\begin{aligned}
&p\Big(S_{c,1,u,{\rm det},\alpha\oplus1,X}-\sum_{i\in\mathcal{S}_{\rm det}}p(n^i=1,t^i=u,\alpha^i=\beta,b^i=X,y^i=\alpha\oplus1|\boldsymbol{\zeta}^{i-1},y^i\neq\emptyset)\leq-g_{\rm A}(N_{\rm det},\epsilon_{\rm A}^{c,1,u,\alpha\oplus1,X})\Big)\\
&\leq\epsilon_{\rm A}^{c,1,u,\alpha\oplus1,X}
\end{aligned}
\tag{V.24}
$$

and

$$
\begin{aligned}
&p\Big(S_{c,1,u,{\rm det},\alpha\oplus1,X}-\sum_{i\in\mathcal{S}_{\rm det}}p(n^i=1,t^i=u,\alpha^i=\beta,b^i=X,y^i=\alpha\oplus1|\boldsymbol{\zeta}^{i-1},y^i\neq\emptyset)\geq g_{\rm A}(N_{\rm det},\epsilon_{\rm A}^{c,1,u,\alpha\oplus1,X})\Big)\\
&\leq\epsilon_{\rm A}^{c,1,u,\alpha\oplus1,X}.
\end{aligned}
\tag{V.25}
$$

Now, if we combine Eqs. (V.19), (V.21), (V.24) and (V.25), we obtain the upper bound on $N_{{\rm ph},Z,Z,1,u,{\rm det}}$ in Eq. (V.17) as

$$
N_{{\rm ph},Z,Z,1,u,{\rm det}}\leq\sum_{\alpha=0}^{1}p^{\rm U}_\alpha\sum_{c\in\mathcal{C}}\Gamma^{\rm U}_{\alpha,c}\frac{S_{c,1,u,{\rm det},\alpha\oplus1,X}+{\rm sgn}(\Gamma^{\rm U}_{\alpha,c})g_{\rm A}(N_{\rm det},\epsilon_{\rm A}^{c,1,u,\alpha\oplus1,X})}{p(c)p^B_X}+g_{\rm A}(N_{\rm det},\epsilon_{\rm A}^{{\rm ph},Z,1,u})
\tag{V.26}
$$

[2] Note that $\beta=2,3,$ and 4 correspond to the case $c=0_Z$, 1_Z, and 0_X, respectively.

except for error probability

$$\epsilon^{1}_{\mathrm{PH}} := \sum_{\alpha=0}^{1}\sum_{c\in\mathcal{C}} \epsilon_{\mathrm{A}}^{c,1,u,\alpha,X} + \epsilon_{\mathrm{A}}^{\mathrm{ph},Z,1,u}. \tag{V.27}$$

Recall that $S_{c,1,u,\det,\alpha\oplus1,X}$ in Eq. (V.26) is the number of instances where Alice emits an untagged single-photon using the setting $\{c\in\mathcal{C}, b=X\}$ and Bob obtains a detection event with the measurement outcome $\alpha\oplus1\in\{0,1\}$. These quantities are not directly observed in the experiments, and hence we need to estimate them with the decoy-state method, as we have explained in Sec. IV. Importantly, this has to be done in such a way that one obtains an upper-bound on $N_{\mathrm{ph},Z,Z,1,u,\det}$. In the case of $S_{c,1,u,\det,\alpha\oplus1,X}$, we take the following upper or lower bounds, depending on the sign of $\Gamma^{\mathrm{U}}_{\alpha,c}$, such that $N_{\mathrm{ph},Z,Z,1,u,\det}$ takes its upper bound:

$$S^{\mathrm{U}}_{c,1,u,\det,\alpha\oplus1,X} \ \text{ if }\ \Gamma^{\mathrm{U}}_{\alpha,c}>0, \tag{V.28}$$

$$S^{\mathrm{L}}_{c,1,u,\det,\alpha\oplus1,X} \ \text{ if }\ \Gamma^{\mathrm{U}}_{\alpha,c}\le 0, \tag{V.29}$$

where $S^{\mathrm{U}}_{c,1,u,\det,\alpha\oplus1,X}$ and $S^{\mathrm{L}}_{c,1,u,\det,\alpha\oplus1,X}$ are defined in Eqs. (IV.31) and (IV.33), respectively. By substituting Eqs. (V.28) and (V.29) into the rhs of Eq. (V.26), we obtain $N^{\mathrm{U}}_{\mathrm{ph},Z,Z,1,u,\det}$.

Finally, we calculate the failure probability associated to the estimation of the upper bound on $N_{\mathrm{ph},Z,Z,1,u,\det}$ conditioned on $n_{\mathrm{tag}}\le N_{\mathrm{tag}}$ and $S_{\det}=N_{\det}$, which we denote by ϵ_{PH}. It is given by the sum of $\epsilon^{1}_{\mathrm{PH}}$ in Eq. (V.27) and $\epsilon^{2}_{\mathrm{PH}}$ that is the sum of the failure probabilities associated to the estimation of $\{S_{c,1,u,\det,\alpha,X}\}_{\alpha=0,1,c\in\mathcal{C}}$:

$$\epsilon_{\mathrm{PH}} = \epsilon^{1}_{\mathrm{PH}} + \epsilon^{2}_{\mathrm{PH}}. \tag{V.30}$$

The parameter $\epsilon^{2}_{\mathrm{PH}}$ has the form $\epsilon^{2}_{\mathrm{PH}}=\sum_{\alpha=0,1}\sum_{c\in\mathcal{C}}\epsilon^{c,1,u,\alpha,X}$ with $\epsilon^{c,1,u,\alpha,X}$ being the failure probability associated to the estimation of $S_{c,1,u,\det,\alpha,X}$ in Eq. (V.28) or Eq. (V.29), namely, $\epsilon^{c,1,u,\alpha,X}=\epsilon^{c,1,u,\alpha,X}_{\mathrm{U}}$ or $\epsilon^{c,1,u,\alpha,X}=\epsilon^{c,1,u,\alpha,X}_{\mathrm{L}}$ depending on whether we use the upper or the lower bound.

B. Derivation of $N_{\mathrm{ph},Z,Z,1,u,\det}$ with general phase intervals in Eq. (10)

In this subsection, we describe the expression of the upper bound on the number of phase errors $N_{\mathrm{ph},Z,Z,1,u,\det}$ with the general phase intervals that are shown in Eq. (10):

$$R^{0_Z}_{\mathrm{ph}}=[\theta^{\mathrm{L}}_{0_Z},\theta^{\mathrm{U}}_{0_Z}],\ \ R^{1_Z}_{\mathrm{ph}}=[\theta^{\mathrm{L}}_{1_Z},\theta^{\mathrm{U}}_{1_Z}],\ \ R^{0_X}_{\mathrm{ph}}=[\theta^{\mathrm{L}}_{0_X},\theta^{\mathrm{U}}_{0_X}], \tag{V.31}$$

where $-\frac{\pi}{6}<\theta^{\mathrm{L}}_{0_Z}\le0$, $0\le\theta^{\mathrm{U}}_{0_Z}<\frac{\pi}{6}$, $\frac{5\pi}{6}<\theta^{\mathrm{L}}_{1_Z}\le\pi$, $\pi\le\theta^{\mathrm{U}}_{1_Z}<\frac{7\pi}{6}$, $\frac{\pi}{3}<\theta^{\mathrm{L}}_{0_X}\le\frac{\pi}{2}$, and $\frac{\pi}{2}\le\theta^{\mathrm{U}}_{0_X}<\frac{2\pi}{3}$. In the estimation of the number of phase errors, the difference of the phase interval is only reflected in the upper bounds $\{\Gamma^{\mathrm{U}}_{\alpha,c}\}_{\alpha=0,1,c\in\mathcal{C}}$ on $\{\Gamma^{i}_{\alpha,c,g^i}\}_{\alpha=0,1,c\in\mathcal{C}}$ in Eq. (V.23) and $\{p^{\mathrm{U}}_{\alpha}\}_{\alpha=0,1}$ in Eq. (V.22), and hence we just need to replace $\{\Gamma^{\mathrm{U}}_{\alpha,c}\}_{\alpha=0,1,c\in\mathcal{C}}$ and $\{p^{\mathrm{U}}_{\alpha}\}_{\alpha=0,1}$ in Eq. (V.26). The explicit replacements can be obtained by considering partial difference functions of $\Gamma^{i}_{\alpha,c,g^i}$ in Eq. (V.23) with respect to $\{\theta^{i}_{c,g^i}\}_{c\in\mathcal{C}}$ and by deriving the parameters $\{\theta^{i}_{c,g^i}\}_{c\in\mathcal{C}}$ to achieve the maximum of $\Gamma^{i}_{\alpha,c,g^i}$. $\{p^{\mathrm{U}}_{\alpha}\}_{\alpha=0,1}$ can be obtained in a similar way. The results are summarised as follows.

$$\Gamma^{\mathrm{U}}_{0,0_Z}\to\Gamma^{i}_{0,0_Z,g^i}(\theta^{\mathrm{L}}_{0_Z},\theta^{\mathrm{L}}_{1_Z},\theta^{\mathrm{U}}_{0_X}),\ \Gamma^{\mathrm{U}}_{0,1_Z}\to\Gamma^{i}_{0,1_Z,g^i}(\theta^{\mathrm{U}}_{0_Z},\theta^{\mathrm{U}}_{1_Z},\theta^{\mathrm{L}}_{0_X}),\ \Gamma^{\mathrm{U}}_{0,0_X}\to\max_{x,y,z\in\{\mathrm{L},\mathrm{U}\}}\{\Gamma^{i}_{0,0_X,g^i}(\theta^{x}_{0_Z},\theta^{y}_{1_Z},\theta^{z}_{0_X})\},$$

$$\Gamma^{\mathrm{U}}_{1,0_Z}\to\Gamma^{i}_{1,0_Z,g^i}(\theta^{\mathrm{U}}_{0_Z},\theta^{\mathrm{L}}_{1_Z},\theta^{\mathrm{L}}_{0_X}),\ \Gamma^{\mathrm{U}}_{1,1_Z}\to\Gamma^{i}_{1,1_Z,g^i}(\theta^{\mathrm{U}}_{0_Z},\theta^{\mathrm{L}}_{1_Z},\theta^{\mathrm{U}}_{0_X}),$$

$$\Gamma^{\mathrm{U}}_{1,0_X}\to\begin{cases}\Gamma^{i}_{1,0_X,g^i}(\theta^{\mathrm{L}}_{0_Z},\theta^{\mathrm{U}}_{1_Z},\theta^{\mathrm{U}}_{0_X}) & \text{if }\ \theta^{\mathrm{U}}_{0_X}<\frac{\theta^{\mathrm{L}}_{0_Z}+\theta^{\mathrm{U}}_{1_Z}}{2},\\ \Gamma^{i}_{1,0_X,g^i}\left(\theta^{\mathrm{L}}_{0_Z},\theta^{\mathrm{U}}_{1_Z},\frac{\theta^{\mathrm{L}}_{0_Z}+\theta^{\mathrm{U}}_{1_Z}}{2}\right) & \text{if }\ \frac{\theta^{\mathrm{L}}_{0_Z}+\theta^{\mathrm{U}}_{1_Z}}{2}\in R^{0_X}_{\mathrm{ph}},\\ \Gamma^{i}_{1,0_X,g^i}(\theta^{\mathrm{L}}_{0_Z},\theta^{\mathrm{U}}_{1_Z},\theta^{\mathrm{L}}_{0_X}) & \text{if }\ \frac{\theta^{\mathrm{L}}_{0_Z}+\theta^{\mathrm{U}}_{1_Z}}{2}<\theta^{\mathrm{L}}_{0_X},\end{cases}$$

$$p^{\mathrm{U}}_{0}\to\frac{1+\cos\frac{\theta^{\mathrm{U}}_{0_Z}-\theta^{\mathrm{L}}_{1_Z}}{2}}{2},\ p^{\mathrm{U}}_{1}\to\frac{1-\cos\frac{\theta^{\mathrm{L}}_{0_Z}-\theta^{\mathrm{U}}_{1_Z}}{2}}{2}. \tag{V.32}$$

[1] Y. Nagamatsu *et al.*, Phys. Rev. A **93**, 042325 (2016).
[2] K. Azuma, Tohoku Math. J. **19**, 357 (1967).
[3] S. Lee and Z. Su, Stat. Probab. Letters **56**, 8391 (2002).
[4] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).