Harnessing high-dimensional temporal entanglement using limited interferometric setups

Alexandra Bergmayr-Mann,[1,*] Florian Kanitschar,[1,2,†] Matej Pivoluska,[1,3,4,‡] and Marcus Huber[1,5,§]

[1] *Vienna Center for Quantum Science and Technology (VCQ), Atominstitut, Technische Universität Wien, Stadionallee 2, 1020 Vienna, Austria*
[2] *AIT Austrian Institute of Technology, Center for Digital Safety & Security, Giefinggasse 4, 1210 Vienna, Austria*
[3] *Institute of Computer Science, Masaryk University, 602 00 Brno, Czech Republic*
[4] *Institute of Physics, Slovak Academy of Sciences, 845 11 Bratislava, Slovakia*
[5] *Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*

(Dated: November 22, 2024)

High-dimensional entanglement has been shown to provide significant advantages in quantum communication. One of its most promising implementations is available in the time-domain routinely produced in spontaneous parametric down-conversion (SPDC). While advantageous in the sense that only a single detector channel is needed locally, it is notoriously hard to analyze, especially in an assumption-free manner that is required for quantum key distribution applications. We develop the first complete analysis of high-dimensional entanglement in the polarization-time-domain and show how to efficiently certify relevant density matrix elements and security parameters for Quantum Key Distribution (QKD). In addition to putting past experiments on rigorous footing, we also develop a physical noise model and propose a novel setup that can further enhance the noise resistance of free-space quantum communication.

I. INTRODUCTION

Quantum entanglement is the defining feature of quantum mechanics. It serves as the main resource for the envisioned "quantum internet" [1], which enables novel communication protocols such as super-dense coding [2], quantum teleportation [3], and, notably, Quantum Key Distribution (QKD) [4, 5]. QKD allows two remote parties to establish secret keys, even in the presence of an eavesdropper having access to unlimited computational resources. The keys obtained then can be used in any broader cryptographic setting, such as encrypting secret messages. The main technical challenge in building a robust large-scale quantum network is the unavoidable exponential signal loss introduced by optical fibers [6]. In contrast to classical information, unknown quantum states cannot be copied [7]; therefore, signal amplification by means of repeaters is impossible for quantum signals. One could resort to building quantum repeaters based on entanglement swapping, however, existing repeater designs are very far from being practical [8]. An alternative approach to overcome the exponential loss in optical fibers is satellite-based Quantum Key Distribution. This method allows the connection of two distant communicating sites on Earth through links with substantially reduced loss, benefiting from signal loss scaling only quadratically with the distance. Unfortunately, satellite-earth links are inherently vulnerable to outside noise, entering the measurement devices from the channel, hence basically limited to nighttime operations (see Refs. [9–15] for recent advances to extend the operation time towards daylight operations by mainly experimental adaptations). This severely limits the practicality of such systems. In particular, for long-distance satellite links, this presents a heavy reduction of potential links and up-times. High-Dimensional (HD) entanglement [14, 16–23] has proven to enhance background noise resistance [24] in entanglement-distribution tasks, with HD entanglement in the time-domain [25] being its most promising implementation for free-space applications. Previous work has successfully demonstrated the feasibility and advantages of HD entanglement in entanglement distribution and QKD [22, 26, 27], but analyses have been rather heuristic and have relied on assumptions on the source-state that are not compatible with the security requirements of QKD. In this work, we provide a rigorous and clean theoretical analysis of a high-dimensional interferometry setup and show how it can be used to harness entanglement in the polarization-time domain for QKD. We develop a realistic noise model and propose an altered scheme that is experimentally simpler and removes assumptions on the entangled state present in previous work. An additional benefit of the proposed setup is an improved noise tolerance by a factor of almost two. This theoretically shifts operation hours from dawn to daytime without relying on substantial technological innovations, marking an important step towards full daytime operations.

* These authors contributed equally, the order was chosen randomly; alexandra.bergmayr@gmx.at
† These authors contributed equally, the order was chosen randomly; florian.kanitschar@outlook.com
‡ pivoluskamatej@gmail.com
§ marcus.huber@tuwien.ac.at

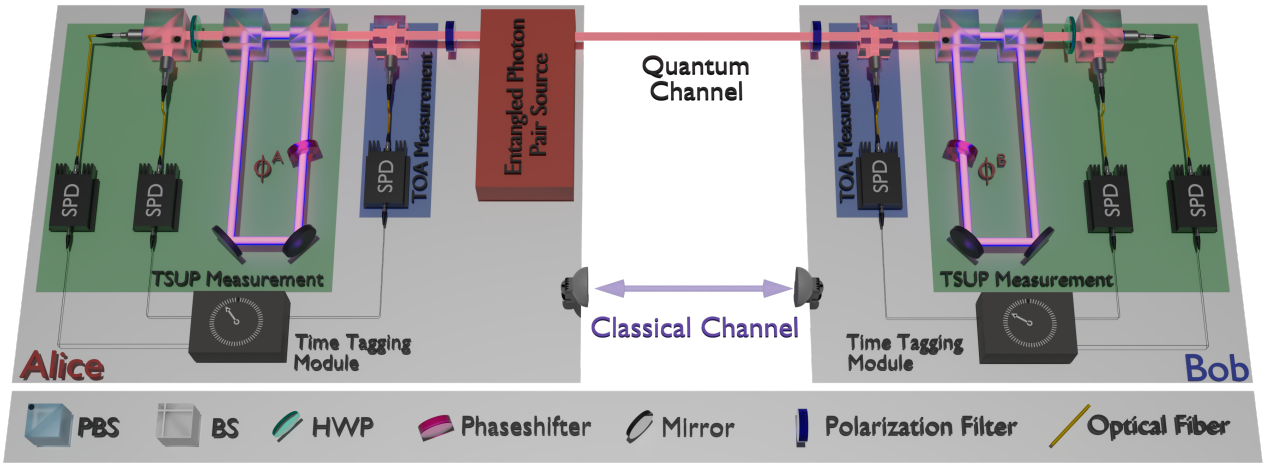

FIG. 1. Sketch of the setup analyzed. A photon source prepares entangled photons and sends them to two identical labs. Each of the labs is equipped with a polarizing filter which can be either inserted (Protocol 1) or removed (Protocol 2). Then an $\eta : 1-\eta$ beamsplitter allows a choice between two measurements, followed by a time-resolving photon detector, which allows measuring the arrival time of incoming photons (TOA). In the second measurement setup, two polarizing beamsplitters (PBSs) and two mirrors allow the superposition of neighboring time-bins. Finally, a half-wave plate (HWP) that can be either inserted or removed together with another PBS and two time-resolving photon detectors (SPD) allow us to perform Time-Superposition (TSUP) measurements. Furthermore, both labs are connected via a classical channel, allowing authenticated classical messages to be exchanged.

II. SETUP DESCRIPTION & ANALYSIS

The HD-QKD setup analyzed is built upon two identical measurement devices, which are placed in the communicating parties' labs, as well as an entangled photon pair source, which can be placed either in one of the parties' labs or in the middle and does not need to be trusted. For the present work, we assume the photon source is being placed in Alice's lab. However, we want to stress that our method applies to both scenarios.

We define the parties' time-reference points via synchronized coincidence windows which will henceforth be called 'time-frames'. If the source is placed in one of the parties' labs, the delay in arrival time in comparison to the lab of the second party is accounted for, i.e., the time-reference points of detection are brought into agreement. The source produces general polarized, time-entangled photon pairs in $(\mathcal{H}_{\text{Pol}} \otimes \mathcal{H}_{\text{Time}})^{\otimes 2}$, $\left|\Psi^{\text{ideal}}_{\text{target}}\right\rangle := \sum_{p_A,p_B\in\{H,V\}} \int_0^\infty \Psi(p_A,p_B,t)\left|p_A,p_B,t,t\right\rangle \ \mathrm{d}\mu(t)$, where $\mu(t)$ is some appropriate measure. Here, $\mathcal{H}_{\text{Pol}}$ is a two-dimensional Hilbert space representing the polarization degree of freedom, while, in principle, we require an infinite-dimensional Hilbert space $\mathcal{H}_{\text{Time}}$ to represent the temporal degree of freedom. However, any realistic time-resolving photon measurement discretizes the temporal degree of freedom into detection events of finitely many time-bins.

Let us call $T > 0$, chosen such that $\forall p_A, p_B \in \{\mathrm{H},\mathrm{V}\}$: $\Psi(p_A,p_B,t)$ is almost constant in $[t_0, t_0+T]$ for some t_0, time-frame length and let d be the number of time-bins. Consequently, the length of a single time-bin is given by $t_B := \frac{T}{d}$. Hence, effectively, we require a d-dimensional Hilbert space $\mathcal{H}_T$ to capture the temporal aspects of the photons under consideration. Then, our effective target state reads

$$\left|\Psi^{\text{eff}}_{\text{target}}\right\rangle := \sum_{p_A,p_B\in\{\mathrm{H},\mathrm{V}\}} c_{p_A,p_B}\left|p_A,p_B\right\rangle \otimes \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\left|kk\right\rangle, \quad (1)$$

where $c_{p_A,p_B} \in \mathbb{C}$ with $\sum_{p_A,p_B}|c_{p_A,p_B}|^2 = 1$. The shares of the photon pair are transmitted to Alice and Bob, respectively.

Each of their labs is equipped with a measurement setup described in Figure 1, where incoming photons pass an $\eta : 1-\eta$ beamsplitter, which, with probability η, allows them to measure the Time-of-Arrival (TOA), and with probability $1-\eta$ the Temporal-Superposition (TSUP) of neighboring time-bins. We note that the same measurements can also be realized with active choice instead of the beamsplitter, such that both measurements are performed with only two detectors. For simplicity, we discuss the passive choice setup, however, the following analysis is also valid for active basis choice. The first arm of this setup consists of a simple time-resolving photon detector to capture the arrival time of incoming photons. In the second arm, two polarizing beamsplitters (PBSs) and two mirrors build a Franson interferometer [28], allowing to superpose two (not necessarily neighboring)

time-bins. Finally, a half-wave plate (HWP) that can be either inserted or removed, together with another PBS and two time-resolving photon detectors (SPD) perform TSUP measurements.

For what follows, we adjust the long arm of the Franson interferometer such that it causes a delay by one time-bin, i.e., vertically polarized light with time-stamp $i-1$ meets horizontally polarized light with time-stamp i. While a possible basis for $\mathcal{H}_{\text{Pol}}$ is given by $\{|\text{H}\rangle, |\text{V}\rangle\}$, consisting of vectors corresponding to horizontally and vertically polarized photons, a basis of $\mathcal{H}_{\text{T}}$ is given by the "time-bin states" $\{|n\rangle\}_{n=0}^{d-1}$. This allows us to define the time-shift operation by its action on basis states, $\hat{T}: \mathcal{H}_T \to \mathcal{H}_T,\ |n\rangle \mapsto |n+1\rangle$ and the phase-shift operator $\hat{Q}_\phi : \mathcal{H}_{\text{Pol}} \otimes \mathcal{H}_T \to \mathcal{H}_{\text{Pol}} \otimes \mathcal{H}_T,\ |p,n\rangle \to e^{i\phi}|p,n\rangle$. Having introduced this notation, we can start to describe the action of the measurement setup. Let $\rho_{AB} \in \mathcal{D}\left(\mathcal{H}^A \otimes \mathcal{H}^B\right)$ be the joint quantum state that enters Alice's and Bob's lab. The action of the TOA measurement setup on this state is straightforward, as a detection event at time i simply corresponds to a projection of the incoming state onto $|i\rangle$. Thus, the corresponding measurement operator for Alice and Bob respectively reads

$$M^{A/B}(i) = \mathbb{1}_{\text{Pol}} \otimes |i\rangle\langle i| \,. \tag{2}$$

It remains to find the corresponding operators for TSUP measurements. We show in Appendix A that the unitary representing the action of the TSUP measurement setup is given by

$$\begin{aligned}\hat{U} :=& |\text{HH}\rangle\langle\text{HH}| \otimes \mathbb{1}_T \otimes \mathbb{1}_T + |\text{HV}\rangle\langle\text{HV}| \otimes \mathbb{1}_T \otimes \hat{Q}_\phi \hat{T} \\ &+ |\text{VH}\rangle\langle\text{VH}| \otimes \hat{Q}_\phi \hat{T} \otimes \mathbb{1}_T + |\text{VV}\rangle\langle\text{VV}| \otimes \hat{Q}_\phi \hat{T} \otimes \hat{Q}_\phi \hat{T}.\end{aligned} \tag{3}$$

Note that the interferometer is followed by an half-wave plate that rotates the plane of polarization by $\frac{\pi}{4}$, mapping $|\text{H}\rangle$ to $|\text{D}\rangle$ and $|\text{V}\rangle$ to $|\text{A}\rangle$. This finally allows us to find the 'effective measurement' performed on the input state ρ_{AB}, i.e., if M_k denotes the measurement performed on the state ρ_{out} after passing the TSUP setup (but before the detectors), we aim for $\tilde{M}_k := \left|\tilde{\Psi}_k\right\rangle\!\left\langle\tilde{\Psi}_k\right|$ such that

$$\text{Tr}\left[\rho_{AB}\tilde{M}_k\right] = \text{Tr}\left[\rho_{\text{out}} M_k\right] = \text{Tr}\left[\hat{U}\rho_{AB}\hat{U}^\dagger M_k\right] \tag{4}$$

$$= \text{Tr}\left[\rho_{AB}\hat{U}^\dagger M_k \hat{U}\right]. \tag{5}$$

Let $a, b \in \{1,2\}$ label Alice's and Bob's detectors and denote by i and j their respective time-stamps. Then, we obtain the effective measurement operators $\tilde{M}_{a,b}(i,j,\phi^A,\phi^B) = \left|\tilde{\Psi}_{a,b}(i,j,\phi^A,\phi^B)\right\rangle\!\left\langle\tilde{\Psi}_{a,b}(i,j,\phi^A,\phi^B)\right|$,

$$\begin{aligned}\left|\tilde{\Psi}_{1,1}(i,j,\phi^A,\phi^B)\right\rangle :=& \hat{U}^\dagger |\text{DD},i,j\rangle \\ =& \left|\tilde{\Psi}_1(i,\phi^A)\right\rangle \otimes \left|\tilde{\Psi}_1(j,\phi^B)\right\rangle,\end{aligned} \tag{6}$$

$$\begin{aligned}\left|\tilde{\Psi}_{1,2}(i,j,\phi^A,\phi^B)\right\rangle :=& \hat{U}^\dagger |\text{DA},i,j\rangle \\ =& \left|\tilde{\Psi}_1(i,\phi^A)\right\rangle \otimes \left|\tilde{\Psi}_2(j,\phi^B)\right\rangle,\end{aligned} \tag{7}$$

$$\begin{aligned}\left|\tilde{\Psi}_{2,1}(i,j,\phi^A,\phi^B)\right\rangle :=& \hat{U}^\dagger |\text{AD},i,j\rangle \\ =& \left|\tilde{\Psi}_2(i,\phi^A)\right\rangle \otimes \left|\tilde{\Psi}_1(j,\phi^B)\right\rangle,\end{aligned} \tag{8}$$

$$\begin{aligned}\left|\tilde{\Psi}_{2,2}(i,j,\phi^A,\phi^B)\right\rangle :=& \hat{U}^\dagger |\text{AA},i,j\rangle \\ =& \left|\tilde{\Psi}_2(i,\phi^A)\right\rangle \otimes \left|\tilde{\Psi}_2(j,\phi^B)\right\rangle,\end{aligned} \tag{9}$$

where we defined

$$\left|\tilde{\Psi}_x(i,\phi)\right\rangle := \frac{1}{\sqrt{2}}\left(|\text{H},i\rangle + (-1)^{x-1}e^{-i\phi}|\text{V},i-1\rangle\right), \tag{10}$$

for $x \in \{1,2\}$. To ease notation, we define $\tilde{M}_a^A(i,\phi^A) := \left|\tilde{\Psi}_a(i,\phi^A)\right\rangle\!\left\langle\tilde{\Psi}_a(i,\phi^A)\right|$ and $\tilde{M}_b^B(j,\phi^B) := \left|\tilde{\Psi}_b(j,\phi^B)\right\rangle\!\left\langle\tilde{\Psi}_b(j,\phi^B)\right|$, for $a,b \in \{1,2\}$ indicating which detector clicks and $i,j \in \{0,...,d-1\}$ marking the time-stamps on each side. These measurements with time-stamp i correspond to positive operator-valued measure (POVM) elements associated with the detection time of a photon emitted at time t_i that traveled the short interferometer path, or, equivalently, with the detection time of a photon emitted at time $t_i - 1$ that traveled the long interferometer path.

Over the course of their experiment, Alice and Bob each measure either in the TOA or in the TSUP setting, recording clicks with time-stamps that are stored in different coincidence-click matrices. Let $a, b \in \{1,2\}$ label Alice's and Bob's detectors and denote by i and j their respective time-stamps. Depending on which measurement (TOA or TSUP) they chose, we obtain four possible measurement combinations that are stored in four different kinds of coincidence-click matrices. Note that we only need to label which detector clicked if a TSUP measurement was performed, as clicks in TOA do not discriminate polarization. In what follows, we use the following notation. If both measured the time of arrival, the corresponding coincidence-click element is $\text{TT}(i,j)$ and if both measured temporal superposition, the corresponding coincidence-click element is given by $\text{SS}_{a,b}(i,j)$, where a and b indicate which detector clicked. Since Alice and Bob each have two detectors for that case, we obtain four SS coincidence-click matrices in total. We follow the same naming convention for those rounds where Alice and Bob chose different measurements: if Alice measured TOA while Bob measured TSUP, we denote the corresponding coincidence-click element by $\text{TS}_b(i,j)$, while for the opposite case where Alice measured TSUP and Bob TOA it reads $\text{ST}_a(i,j)$, with two matrices for each of

the cases. Based on the performed measurements, the coincidence-click matrix elements obtained by the present setup read

$$\mathrm{TT}(i,j) := \mathrm{Tr}\left[\rho_{AB}\left(\mathbb{1}_{\mathrm{Pol}}^{\otimes 2}\otimes|i,j\rangle\langle i,j|\right)\right] \tag{11}$$

$$\mathrm{SS}_{a,b}(i,j,\phi^A,\phi^B) := \mathrm{Tr}\left[\rho_{AB}\tilde{M}_{a,b}(i,j,\phi^A,\phi^B)\right] \tag{12}$$

$$\mathrm{TS}_b(i,j,\phi^B) := \mathrm{Tr}\left[\rho_{AB}\left((\mathbb{1}_{\mathrm{Pol}}\otimes|i\rangle\langle i|)\otimes\tilde{M}_b\left(j,\phi^B\right)\right)\right] \tag{13}$$

$$\mathrm{ST}_a(i,j,\phi^A) := \mathrm{Tr}\left[\rho_{AB}\left(\tilde{M}_a(i,\phi^A)\otimes(\mathbb{1}_{\mathrm{Pol}}\otimes|j\rangle\langle j|)\right)\right]. \tag{14}$$

III. PROBLEM AND SOLUTION

In general, Alice and Bob obtain a quantum state $\rho\in\mathcal{D}\left((\mathcal{H}_{\mathrm{Pol}}\otimes\mathcal{H}_T)^{\otimes 2}\right)$. Both record time-stamped clicks and correlate the ones within the temporal margin of the time-frame as coincidence-click matrices $\mathrm{CC}(i,j) :=$ *#Clicks per frame in time-bin i and j* which leads to the four different kinds of coincidence-click matrices given in Eqs. (11) - (14).

While we can choose the state prepared by the source, the state Alice and Bob receive (or only Bob receives, in case the source is located in Alice's lab) is unknown, as in QKD, the channel connecting Alice and Bob is assumed to be fully under the control of an eavesdropper, called Eve. By performing measurements, Alice and Bob aim to certify that the temporal part of their shared state is entangled and decoupled from Eve's part.

In general, the interpretation of the measurements and their meaning for the time part of the density matrix depends on the polarization degree of freedom of the state Alice and Bob receive. A common approach so far has been to *assume* (a) that temporal and polarization degrees of freedom are actually independent of each other, $\rho=\rho_{\mathrm{Pol}}\otimes\rho_T$, or (b) that the polarization degree of freedom does not change while the photons travel through the quantum channel. The assumed perfect knowledge of the polarization degree of freedom has allowed us to directly interpret the measurements' effect on the time part of the density matrix. Alternatively, one could lift assumption (b) by performing state tomography of the polarization density matrix by adding and using an additional measurement arm at the cost of losing a certain fraction of the signals and making the analysis significantly more complicated.

In what follows, we propose a solution that simultaneously removes both assumptions (a) and (b) while, as a beneficial side-effect, improving the noise resistance of the setup and easing the practical complexity of the experiment significantly. As shown in Figure 1, we suggest adding an additional polarization filter set to let D-polarized photons pass at the entrance of both Alice's and Bob's lab before the signal meets the first beamsplitter and tune the source to produce D-polarized photon pairs. Thus, compared to earlier setups [27], we require only one time-resolving photon detector in the TOA measurement (and do not need an additional measurement arm to perform state tomography, as required under (b)). While this simple modification eases the experimental setup considerably, by forcing Alice's and Bob's joint state to be $|DD\rangle\langle DD|\otimes\rho_T$ after the polarization filters, we are able to go without any assumptions about the internal structure of the state that enters the lab and without requiring that only the time part is manipulated while passing the quantum channel. Furthermore, we expect our proposed protocol to be more favorable in the finite-size regime as we need to account for finite-size effects for fewer measurements.

IV. QUANTUM KEY DISTRIBUTION

Having clarified the setup (see Figure 1), let us now detail the proposed High-Dimensional (HD) Discrete-Variable (DV) Quantum Key Distribution (QKD) protocol. Therefore, Alice and Bob execute the following protocol.

1) ***State Preparation***— A source generates photon pairs entangled in polarization and time

$$\left|\Psi_{\mathrm{target}}^{\mathrm{P1}}\right\rangle := |\mathrm{DD}\rangle\otimes\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|kk\rangle\,, \tag{15}$$

and sends them to Alice and Bob.

2) ***Measurement***— Alice and Bob each perform either a TOA or a TSUP measurement, depending on independent random bits $\mathbb{P}_{A/B}\in\{0,1\}$. This step can be implemented passively via a beamsplitter.

Steps 1) and 2) are repeated N-times, where N is assumed to be very large.

3) ***Announcement & Sifting***— Alice and Bob publicly announce their measurement choices for every round via the classical channel and sift rounds where they have performed different measurements.

4) ***Parameter Estimation & Key Generation***— Next, they disclose some of their results from measurements of each basis to perform statistical tests. If the tests are passed, they use the TOA measurements to create a common raw key by performing a key map, where logical bit-values are assigned to the measurement results. Otherwise, they abort the protocol and start again at step 1).

5) ***Error-correction & Privacy Amplification***— By means of classical algorithms Alice and Bob reconcile their raw keys and perform privacy amplification to eliminate the potential eavesdropper's knowledge about the key.

We take our proposed protocol ('Protocol 1') as an example to illustrate our method and compare it to a protocol used in earlier work [22, 27], which relied on assumptions (a) and (b) discussed in the previous section. For this protocol ('Protocol 2'), the source is set to prepare

$$\left|\Psi^{\mathrm{P2}}_{\mathrm{target}}\right\rangle := \frac{|\mathrm{HH}\rangle + |\mathrm{VV}\rangle}{\sqrt{2}} \otimes \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |kk\rangle\,, \tag{16}$$

and the polarization filters at the entrance of both Alice's and Bob's labs are removed. Note that the rates reported for this protocol are only upper bounds, while the key rates we report for Protocol 1 are reliable lower bounds.

Let us start with the discussion of Protocol 1. By construction, independently of what happens to the quantum signal while traveling through the quantum channel, Alice's and Bob's joint quantum state ρ_{AB} reads $|\mathrm{DD}\rangle\langle\mathrm{DD}|\otimes\rho_T$, where ρ_T is an arbitrary quantum state in $\mathcal{D}(\mathcal{H}_T^{\otimes 2})$. We apply Eqs. (11) - (14) to relate coincidence-click matrix elements with density matrix elements. For the TOA measurements, it follows directly that the coincidence-clicks correspond to the diagonal entries of the time-density matrix,

$$\mathrm{TT}(i,j) = \langle i,j|\rho_T|i,j\rangle\,. \tag{17}$$

For the TSUP measurements, using the D/A representation from Eq. (10), we obtain

$$\mathrm{SS}_{1,1}(i,j) = \frac{1}{4}\langle i+, j+|\rho_T|i+, j+\rangle\,, \tag{18}$$

$$\mathrm{SS}_{1,2}(i,j) = \frac{1}{4}\langle i+, j-|\rho_T|i+, j-\rangle\,, \tag{19}$$

$$\mathrm{SS}_{2,1}(i,j) = \frac{1}{4}\langle i-, j+|\rho_T|i-, j+\rangle\,, \tag{20}$$

$$\mathrm{SS}_{2,2}(i,j) = \frac{1}{4}\langle i-, j-|\rho_T|i-, j-\rangle\,, \tag{21}$$

where $i,j \in \{1,2,\ldots,d-1\}$ and $|i\pm\rangle := \frac{|i\rangle \pm |i-1\rangle}{\sqrt{2}}$, i.e., we set $\phi^A = \phi^B = 0$. To ease notation, we omitted the arguments ϕ^A and ϕ^B. Note that these click events have a direct physical interpretation. If on both sides detector 1 clicks, this means both have measured a positive phase between two neighboring time-bins labeled by i and j, while clicks of detector 2 on both sides indicate a negative phase. If opposite detectors click, this indicates that they have measured different phases between neighboring time-bins.

Finally, the mismatched measurements yield

$$\mathrm{TS}_1(i,j) = \frac{1}{2}\langle i, j+|\rho_T|i, j+\rangle\,, \tag{22}$$

$$\mathrm{TS}_2(i,j) = \frac{1}{2}\langle i, j-|\rho_T|i, j-\rangle\,, \tag{23}$$

$$\mathrm{ST}_1(i,j) = \frac{1}{2}\langle i+, j|\rho_T|i+, j\rangle\,, \tag{24}$$

$$\mathrm{ST}_2(i,j) = \frac{1}{2}\langle i-, j|\rho_T|i-, j\rangle\,. \tag{25}$$

For ease of presentation, we assume now that d is even in what follows, in order to explain how these click matrices can be interpreted. We want to emphasize that our method is not limited to this case and that this choice is solely made for illustration purposes and generalizes straight-forwardly to arbitrary dimensions.

Note that the right-hand sides of the click equations are composed of matrix elements of the time-density matrix. It can be seen directly that the TOA clicks (TT) already correspond to a POVM,

$$\mathcal{M}_0^{P1} := \{|i,j\rangle\langle i,j|\}_{i,j=0}^{d-1}\,, \tag{26}$$

giving rise to a basis $\mathcal{B}_0 := \mathcal{B}_0^A \otimes \mathcal{B}_0^B$, where $\mathcal{B}_0^{A/B} := \{|i\rangle\}_{i=0}^{d-1}$ spans single time-bin subspaces. The corresponding 'basis-click matrix' reads

$$C_{\mathcal{M}_0^{P1}}(i,j) := \mathrm{TT}(i,j), \tag{27}$$

where we use the natural order $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$.

In contrast, the TSUP measurements can even be used to construct two POVM measurements. For the first of the two corresponding bases, $\mathcal{B}_1 := \mathcal{B}_1^A \otimes \mathcal{B}_1^B$, notice that $|i\pm\rangle$ for fixed i spans two-dimensional time-bin subspaces. Thus, we first consider odd i and obtain $\mathcal{B}_1^{A/B} := \{|(2k-1)\pm\rangle\}_{k=1}^{\frac{d}{2}}$ as a basis for Alice's, respectively Bob's, d-dimensional temporal Hilbert space. Consequently, a short calculation shows that

$$\begin{aligned}\mathcal{M}_1^{P1} := \{&|i+, j+\rangle\langle i+, j+|\,, |i+, j-\rangle\langle i+, j-|\,,\\ &|i-, j+\rangle\langle i-, j+|\,, |i-, j-\rangle\langle i-, j-|\}_{i,j \text{ odd}}\end{aligned} \tag{28}$$

forms another POVM, induced by the bases $\mathcal{B}_1^{A/B}$ on Alice's and Bob's side, respectively. The corresponding click-matrix reads

$$C_{\mathcal{M}_1^{P1}} := 4 \begin{pmatrix} \mathrm{SS}_{1,1}(1,1) & \mathrm{SS}_{1,2}(1,1) & \mathrm{SS}_{1,1}(1,3) & \mathrm{SS}_{1,2}(1,3) & \ldots & \mathrm{SS}_{1,1}(1,d-1) & \mathrm{SS}_{1,2}(1,d-1) \\ \mathrm{SS}_{2,1}(1,1) & \mathrm{SS}_{2,2}(1,1) & \mathrm{SS}_{2,1}(1,3) & \mathrm{SS}_{2,2}(1,3) & \ldots & \mathrm{SS}_{2,1}(1,d-1) & \mathrm{SS}_{2,2}(1,d-1) \\ \mathrm{SS}_{1,1}(3,1) & \mathrm{SS}_{1,2}(3,1) & \mathrm{SS}_{1,1}(3,3) & \mathrm{SS}_{1,2}(3,3) & \ldots & \mathrm{SS}_{1,1}(3,d-1) & \mathrm{SS}_{1,2}(3,d-1) \\ \mathrm{SS}_{2,1}(3,1) & \mathrm{SS}_{2,2}(3,1) & \mathrm{SS}_{2,1}(3,3) & \mathrm{SS}_{2,2}(3,3) & \ldots & \mathrm{SS}_{2,1}(3,d-1) & \mathrm{SS}_{2,2}(3,d-1) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathrm{SS}_{1,1}(d-1,1) & \mathrm{SS}_{1,2}(d-1,1) & \mathrm{SS}_{1,1}(d-1,3) & \mathrm{SS}_{1,2}(d-1,3) & \ldots & \mathrm{SS}_{1,1}(d-1,d-1) & \mathrm{SS}_{1,2}(d-1,d-1) \\ \mathrm{SS}_{2,1}(d-1,1) & \mathrm{SS}_{2,2}(d-1,1) & \mathrm{SS}_{2,1}(d-1,3) & \mathrm{SS}_{2,2}(d-1,3) & \ldots & \mathrm{SS}_{2,1}(d-1,d-1) & \mathrm{SS}_{2,2}(d-1,d-1) \end{pmatrix}, \tag{29}$$

where we have ordered the basis vectors $\{|1+\rangle, |1-\rangle, |3+\rangle, |3-\rangle, \ldots, |(d-1)+\rangle, |(d-1)-\rangle\}$.

Finally, for the last basis, $\mathcal{B}_2 := \mathcal{B}_2^A \otimes \mathcal{B}_2^B$, we consider even i. Based on our measurement setup we are not able to directly measure elements spanning the boundary subspaces span$\{|0\rangle\}$ and span$\{|d-1\rangle\}$ in the TSUP basis with even i and hence need to substitute them by combinations of elements where the parties have used different measurements (so, the TS- and ST-clicks). We obtain $\mathcal{B}_2^{A/B} := \{|(2k)\pm\rangle\}_{k=1}^{\frac{d}{2}-1} \cup \{|0\rangle, |d-1\rangle\}$. This translation of projective measurements resulting in coincidence-click matrices to POVM elements on only the temporal Hilbert space allows us now to normalize the click matrices correctly. We obtain for the third POVM

$$\mathcal{M}_2^{P1} := \{|i\pm, j\pm\rangle\langle i\pm, j\pm|\}_{\substack{i,j>0,\\ \text{even}}} \cup \{|i, j\pm\rangle\langle i, j\pm|\}_{\substack{i\in\{0,d-1\}\\ j>0,\ \text{even}}} \cup \{|i\pm, j\rangle\langle i\pm, j|\}_{\substack{i>0,\ \text{even}\\ j\in\{0,d-1\}}} \cup \{|i, j\rangle\langle i, j|\}_{i,j\in\{0,d-1\}}\,. \tag{30}$$

The corresponding click-matrix reads

$$C_{\mathcal{M}_2^{P1}} := \begin{pmatrix} \text{TT}(0,0) & 2\text{TS}_1(0,2) & 2\text{TS}_2(0,2) & 2\text{TS}_1(0,4) & 2\text{TS}_2(0,4) & \ldots & 2\text{TS}_2(0,d-2) & \text{TT}(0,d-1) \\ 2\text{ST}_1(2,0) & 4\text{SS}_{1,1}(2,2) & 4\text{SS}_{1,2}(2,2) & 4\text{SS}_{1,1}(2,4) & 4\text{SS}_{1,2}(2,4) & \ldots & 4\text{SS}_{1,2}(2,d-2) & 2\text{ST}_1(2,d-1) \\ 2\text{ST}_2(2,0) & 4\text{SS}_{2,1}(2,2) & 4\text{SS}_{2,2}(2,2) & 4\text{SS}_{2,1}(2,4) & 4\text{SS}_{2,2}(2,4) & \ldots & 4\text{SS}_{2,2}(2,d-2) & 2\text{ST}_2(2,d-1) \\ 2\text{ST}_1(4,0) & 4\text{SS}_{1,1}(4,2) & 4\text{SS}_{1,2}(4,2) & 4\text{SS}_{1,1}(4,4) & 4\text{SS}_{1,2}(4,4) & \ldots & 4\text{SS}_{1,1}(4,d-2) & 2\text{ST}_1(4,d-1) \\ 2\text{ST}_2(4,0) & 4\text{SS}_{2,1}(4,2) & 4\text{SS}_{2,2}(4,2) & 4\text{SS}_{2,1}(4,4) & 4\text{SS}_{2,2}(4,4) & \ldots & 4\text{SS}_{2,2}(4,d-2) & 2\text{ST}_2(4,d-1) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \\ 2\text{ST}_2(d-2,0) & 4\text{SS}_{2,1}(d-2,2) & 4\text{SS}_{2,2}(d-2,2) & 4\text{SS}_{2,1}(d-2,4) & 4\text{SS}_{2,2}(d-2,4) & \ldots & 2\text{SS}_{2,2}(d-2,d-2) & 2\text{ST}_2(d-2,d-1) \\ \text{TT}(d-1,0) & 2\text{TS}_1(d-1,2) & 2\text{TS}_2(d-1,2) & 2\text{TS}_1(d-1,4) & 2\text{TS}_2(d-1,4) & \ldots & 2\text{TS}_2(d-1,d-2) & \text{TT}(d-1,d-1) \end{pmatrix}, \tag{31}$$

where the order of the basis vectors is $\{|0\rangle, |2+\rangle\, |2-\rangle, \ldots, |(d-2)+\rangle, |(d-2)-\rangle, |d-1\rangle\}$. Note that the different weight factors ensure the correct normalization of the click-matrix. Finally, we want to emphasize the importance of the overlap between the subspaces spanned by $\mathcal{B}_1$ and $\mathcal{B}_2$, which allows us to certify high-dimensional entanglement.

For comparison, we conduct a similar analysis for Protocol 2 under the assumption that the polarization degree of freedom is known. Therefore, the rates reported for this protocol represent only upper bounds on the secure key rate. For details, we refer the reader to Appendix B.

V. NOISE MODEL

Entangled photons are produced by the source and then travel through a (free-space) quantum channel before entering imperfect detection devices, where they cause clicks. In this section, we physically model how various physical processes influence the coincidence-click matrices used to calculate key rates for our setup. Similarly to Refs. [26] and [29], besides loss — i.e., the process that a photon coming from the source is lost on its way to the detectors — we identify two main origins of noise, i.e., processes that add photons, hence detector clicks. While photons are traveling through the free-space channel, some of the photons may scatter on molecules present in the direct line between the source and the detector. Thus, the probability of losing a photon increases with increasing distance between sender and receiver and is given by a probability of photon loss P_{loss}^A (for the channel between Alice and the source) and P_{loss}^B (for the channel between Bob and the source). Due to imperfections in the detection process, not all incoming photons cause a detector click. We measure the click probability for a given photon by a number $\eta_D \in [0,1]$, called the detection efficiency. For simplicity we assume that the detector efficiency is the same for all the detectors in our setup.

Next, let us turn to processes that insert photons to our setup that do not originate from the source. The main source of this type of noise is environmental photons (like those coming from the Sun) being detected. Besides that, detector imperfections sometimes cause clicks even if no photons are present. Such clicks are called dark counts and we measure this effect as dark count rate (in dark counts per second).

We provide a detailed derivation of our noise model in Appendix C and give here only the key ideas. Due to the independent nature of all processes described, it is reasonable to model both the photon pair production and the dark counts as well as environmental photons as Poisson-distributed quantities. The pair production rate, the dark count rate, etc. are then simply given by the expectation of the corresponding Poisson-distributed random variable. Again, motivated by the independent nature of all sources of noise, we aim to quantify the influence of noise by one single parameter, the isotropic noise parameter such that

$$\rho(v) = v\,|\Psi_{\text{target}}\rangle\langle\Psi_{\text{target}}| + (1-v)\frac{1}{d^2}\mathbb{1}_{d^2\times d^2}, \tag{32}$$

where $v = \frac{P_{\text{Good}}}{P_{\text{CC}}(1,1)}$. Here, P_{Good} denotes the probability that a coincidence-click is caused by a photon pair originating from the source, while $P_{\text{CC}}(1,1)$ is the probability for one coincidence-click. In Appendix C, we derive expressions for P_{Good} and $P_{\text{CC}}(1,1)$ for both protocols.

In what follows, we assume that the source is placed in Alice's lab, which is in line with the practical implementation of entanglement-based QKD setups, such as the free-space link between Vienna and Bisamberg [22, 27]. Thus, Alice's share of the entangled photon pair is not subject to channel loss ($P^A_{\text{loss}} = 0$) and does not experience noise due to environmental photons.

Note that we do not consider detector jitter in our noise model. This is an effect, in which the time of arrival of photons is mislabeled due to the clock imprecision. One would expect that the effect of detector jitter on the observed key rate of protocols is non-negligible, especially for higher values of d, which are obtained by making the time-bins rather short. While this is true for the time frame and time-bin definition presented in this manuscript, in practical implementations, one can mitigate this effect by using non-neighboring time-bins to define the time-frames, as discussed in [27]. In particular, a d-dimensional time-frame is defined as a collection of d non-neighboring time-bins that are separated by time intervals equal to the interferometer delay, which is typically much larger than the length of a time-bin. Defining the frames in this way makes mislabelling due to jitter very likely to produce two single-click events in non-matched time-frames, which are then discarded as single-click events. This reduction in error, however comes at the cost of reduced coincidence rate, therefore optimal key rate per coincidence and optimal key rate per second are typically not achieved for the same local dimension. Finally, defining time-frames in this way does not affect the analysis of the protocol and we have opted for a more traditional time-frames definition in this manuscript for simplicity.

VI. NUMERICAL METHOD

The asymptotic secure key rate R^∞ of a QKD protocol is lower-bounded by the Devetak-Winter bound [30], which reads

$$R^\infty \geq S(A|E) - H(A|B), \tag{33}$$

where $S(A|E)$ is the conditional von Neumann entropy of Alice's key register given Eve's quantum register, quantifying the amount of information not known by Eve, and $H(A|B)$ is the Shannon entropy between Alice's and Bob's raw key, representing the amount of information leaked during the error-correction phase of the protocol. While the latter quantity is accessible from the observed statistics, to obtain the first, we have to minimize over all quantum states ρ_{ABE} compatible with Alice's and Bob's observations. Therefore, we use a method developed in Ref. [31] that exploits a semi-definite program (SDP) hierarchy converging to the first term in the Devetak-Winter formula. The first term can be rewritten by means of the quantum relative entropy $D(\rho||\sigma) := \text{Tr}\left[\rho\log(\rho)\right] - \text{Tr}\left[\rho\log(\sigma)\right]$ for density matrices ρ and σ and reads

$$S(A|E) = -D\left(\rho_{\tilde{A}E}||\mathbb{1}_A \otimes \rho_E\right), \tag{34}$$

where $\rho_{\tilde{A}E} := \sum_a |a\rangle\langle a| \otimes \text{Tr}_{AB}\left[(|a\rangle\langle a| \otimes \mathbb{1}_{BE})\rho_{ABE}\right]$. Following Ref. [32] one then can obtain a convergent sequence of semi-definite programs for the quantum relative entropy using Gauß-Radau quadrature. We implement this numerical method and solve semi-definite programs (SDP) with Gauß-Radau parameter $m = 10$, to find lower bounds on the secure key rate for protocol 1 (and upper bounds for protocol 2). Experimental observations then serve as constraints for this semi-definite program. Hence, the optimization for our particular problem reads

$$\begin{aligned}
\min_{\sigma,\{\zeta_i^a,\eta_i^a,\theta_i^a\}_{a,i}} \; & c_m + \sum_{i=1}^{m}\sum_{a=0}^{d-1} \frac{w_i}{t_i \log(2)} \text{Tr}\left[(|a\rangle\langle a| \otimes \mathbb{1}_B)\left(\zeta_i^a + \zeta_i^{a\dagger} + (1-t_i)\eta_i^a\right) + t_i\theta_i^a\right] \\
\text{s.t.} \quad & \\
& \text{Tr}\left[\sigma\right] = 1, \\
& \forall a,i: \; \Gamma^1_{a,i} := \begin{pmatrix} \sigma & \zeta_i^a \\ \zeta_i^{a\dagger} & \eta_i^a \end{pmatrix} \geq 0, \\
& \forall a,i: \; \Gamma^2_{a,i} := \begin{pmatrix} \sigma & \zeta_i^{a\dagger} \\ \zeta_i^a & \theta_i^a \end{pmatrix} \geq 0, \\
& \forall k: \; \text{Tr}\left[E_k\sigma\right] = f_k,
\end{aligned} \tag{35}$$

where we defined $\Theta(M) := \text{Tr}_E\left[\rho_{ABE}(\mathbb{1}_{AB} \otimes M_E^\top)\right]$ and set

$$\sigma := \Theta(\mathbb{1}) \tag{36}$$
$$\zeta_i^a := \Theta(Z_i^a) \tag{37}$$
$$\eta_i^a := \Theta(Z_i^{a\dagger} Z_i^a) \tag{38}$$
$$\theta^a := \Theta(Z_i^a Z_i^{a\dagger}) \tag{39}$$

and the Z_i^a are arbitrary complex matrices. Furthermore $c_m := \sum_{i=1}^m \frac{w_i}{t_i \log(2)}$, where the $w_i > 0$, $\sum_i w_i = 1$, $w_m = \frac{1}{m^2}$ are Gauß-Radau weights and $t_i \in (0, 1]$, $t_m = 1$. For more details we refer interested readers to Ref. [31].

The constraints of the form $\mathrm{Tr}\,[E_k \sigma] = f_k$ are due to our experimental observations, i.e., the operators E_k are chosen from $\{\mathcal{M}_0^{P_z}, \mathcal{M}_1^{P_z}, \mathcal{M}_2^{P_z}\}$ and the corresponding scalar right-hand sides f_k are given by the matrices $C_{\mathcal{M}_0^{P_z}}, C_{\mathcal{M}_1^{P_z}}$ and $C_{\mathcal{M}_2^{P_z}}$, where $z \in \{1, 2\}$ selects between the two protocols we consider (see Section IV and Appendix B).

VII. RESULTS

We illustrate our method under the realistic noise model we derived (see Section V and Appendix C), taking photon losses, background noise induced by solar photons, detector inefficiencies, and dark counts into account. Recall that in Protocol 1, the source prepares the state

$$|\Psi_1\rangle = |\mathrm{DD}\rangle \otimes \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |kk\rangle\,, \tag{40}$$

and Alice and Bob each add a polarization filter, which is set to D, right after the photon enters their respective lab, such that they are aligned on polarization of the target state. Consequently, as outlined earlier, the state after the polarization filter has the form $\rho_{AB} = |\mathrm{DD}\rangle\langle\mathrm{DD}| \otimes \rho_T$. We wish to highlight that neither the form of the polarization part nor the tensor product structure are mere assumptions, as they are enforced by the filter. This allows a direct and clean analysis of the QKD setup without any additional, unjustified assumptions. For comparison, we also consider a second protocol, which was already discussed in earlier works [22, 27]. There, the source produces the target state

$$|\Psi_2\rangle = \frac{|\mathrm{HH}\rangle + |\mathrm{VV}\rangle}{\sqrt{2}} \otimes \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |kk\rangle\,. \tag{41}$$

The original motivation to consider a QKD protocol where a state with maximally entangled polarization degree of freedom (DOF) (41) is distributed, was to implement a postselection free Franson interferometer. In other words, in case of noiseless polarization propagation through the channel, Alice's and Bob's photons would always take the same path (long-long or short-short) through the Franson interferometer, thus decreasing the number of coincidences that are not directly useful to witness entanglement. Such a setup, however, leads to some experimental restrictions. First of all, one cannot put any polarization filter in the entry of Alice's respectively Bob's lab. In addition, one also needs to enforce certain restrictions on the capability of the adversary, which is undesirable in adversarial scenarios. Namely, either one has to assume that (a) the polarization remains unchanged over the channel (which is a very strong assumption as one would expect noise to primarily affect the polarization-degree of freedom) and still forms a tensor product with the time part,

$$\rho_{AB} = \frac{|\mathrm{HH}\rangle\langle\mathrm{HH}| + |\mathrm{HH}\rangle\langle\mathrm{VV}| + |\mathrm{VV}\rangle\langle\mathrm{HH}| + |\mathrm{VV}\rangle\langle\mathrm{VV}|}{2} \otimes \rho_T, \tag{42}$$

or (b) the received state has at least tensor-product structure, $\rho_{AB} = \rho_{\mathrm{Pol}} \otimes \rho_T$ (also an unjustified assumption), where ρ_{Pol} might have changed over the channel, and needs to be determined by performing additional tomography in the polarization degree of freedom. Assumption (b) is technically weaker than assumption (a), but, it is also much harder to analyze because a change in the polarization would lead to different overall measurements implemented by the Franson interferometer. In this case one would hope that the implemented tomography reveals a high fidelity of the polarization DOF to the maximally entangled state so that the postselection free property would still be present and contribute to the overall key rate. Since this assumption was used in the existing literature [22], we decided to use it for compar-

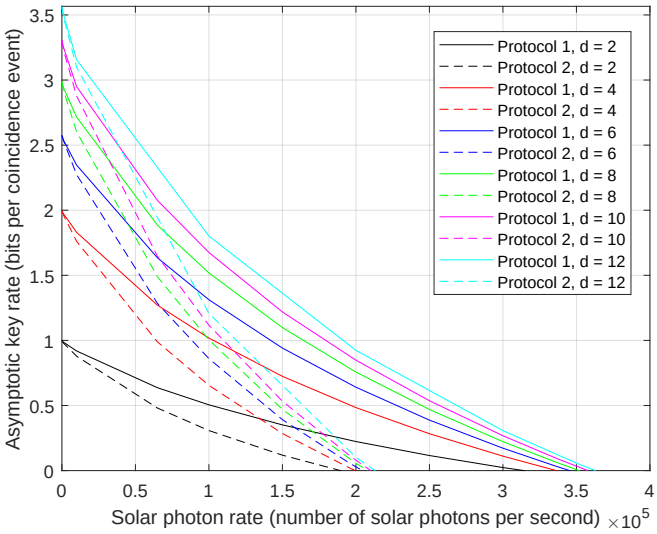

FIG. 2. Lower bounds on the secure key rate for Protocol 1 (solid) and upper bounds on the secure key rate for Protocol 2 (dashed) for various dimensions as a function of the solar photon rate. We set the time-frame length to $T = 5.4 \times 10^{-9} s$ and the probability of channel loss to 99.7%, which corresponds to 25.2 dB loss. Furthermore, we assume a detection efficiency of 90% as well as a dark count rate of $100/s$. Finally, we set the pair production rate to $0.1/T$, which corresponds to approximately 18.5×10^6 photons per second.

ison. We refer to a protocol with entangled polarization and assumption (a) as Protocol 2 and label Protocol 1 as our new results with polarization prepared in the $|\mathrm{DD}\rangle$ state and polarization filters in both measurement apparatuses. We emphasize that this leads to a comparison of a lower bound on the secure key rate of Protocol 1 with an upper bound for Protocol 2. Besides allowing a clean and rigorous analysis without any assumptions, we intuitively expect the additional polarization filter to increase the resistance against solar photons, which are the main source of noise in free-space and satellite QKD applications, as half of the unpolarized solar photons are blocked, while (in the ideal case) none or (in reality) only a small fraction of the source photons are.

For our simulations, we used specific parameter values in accordance with the Free-Space Link experiment between Vienna and Bisamberg [22, 27]. The length of a time-frame was set to $T_0 := 5.4 \times 10^{-9} s$, the dark count rate to $100/s$, the detection efficiency to $\eta_D = 90\%$, the channel loss to $P_{\text{loss}} = 99.7\%$, corresponding to a loss of $25.2dB$, and the pair production rate to 0.1 per time-frame, corresponding to roughly 18.5 MHz repetition rate. Further, consistent with the experiments that inspired our work, we assume that the photon source is located in Alice's lab. In Figure 2, we present secure key rates for Protocol 1 and compare them to upper bounds on the secure key rate for Protocol 2 for time dimensions of $d = 2, 4, 6, 8, 10$ and 12. This means we keep the time-frame size T fixed while changing the number of time-bins d. It is common to plot secure key rates over the error rate which is related to the visibility via $1 - v - \frac{1-v}{d}$. However, depending on the particular noise model, the visibility may be a function of the dimension and protocol specifics and, therefore, is a suboptimal measure to compare different dimensions. Thus, we have chosen to compare the protocols and various dimensions as a function of the solar photon rate, which, in our opinion, provides a fair and practical comparison.

We note that one should not directly read the values for different dimensions d as the optimal performance for QKD implementations at different dimensions in general. For such a comparison, one would need to optimize the photon pair production and the time-frame size for each value of d for the largest achievable key rate per second, which is dependent on many parameters beyond the scope of this work. In Figure 3, we compare the performance of our protocol with BBM92 regarding loss. Therefore, we keep all system parameters the same as in Figure 2, but vary the photon loss probability and plot curves for different solar photon rates. Again, we employ the noise model presented in Appendix C to relate physical parameters to click matrices and we derive the comparison key rates for the BBM92 protocol using the fact that our Protocol 1 reduces to the BBM92 protocol if two time-bins are used in a single frame. Technically, this case is a special case of our protocol, as we envision choosing the optimal dimension dynamically depending on background noise and loss. To keep the comparison meaningful, we always compare a situation where the photon pair production rate, the solar photon rate, and the clock precision (bin size) are the same and vary the probability of loss. This means we compare Protocol 1 with frame-size fixed to $T = 5.4 \times 10^{-9}$ and local dimension d to a BBM92 protocol with the same bin size and local dimension 2 (i.e., the frame size of the BBM92 protocol is equal to $T/(d/2)$. This comparison is meaningful, as we assume that the source brightness is at a point that saturates the detectors on one side of a free-space link and cannot be increased anymore. In Figure 3 we present key rate curves comparing Protocol 1 for $d = 8$ with BBM92 for solar photon rate $n_{\text{sol}} \in \{10^2, 10^4\}$. One can observe that our protocol outperforms BBM92 in lower loss regions up to approximately 39dB. In particular, our protocol outperforms BBM92 also when the loss is approximately 25dB, (which is consistent with the experiment reported in Ref. [22] and the loss in LEO satellite scenarios [33]) and the background solar photon rate is set to 10^4 per second, which is roughly consistent with the light conditions at sunrise (see Ref. [22]). However, we also see that the region where Protocol 1 outperforms BBM92 shrinks with increasing background photon rate.

Lastly, we note that we assume ideal one-way error correction [34] and we leave performance optimizations and examination of alternative reconciliation routines [35–37] for future work. Our new protocol (Protocol 1) consistently exhibits significantly higher key rates, even compared to the upper bound for the existing protocol (Protocol 2), especially as the number of solar photons increases. Additionally, Protocol 1 demonstrates tolerance to nearly twice as many solar photons per second as Protocol 2. It is crucial to reiterate that the curves presented for Protocol 2 rely on unjustified assumptions (see our earlier discussion), serving as mere upper bounds, while the analysis of Protocol 1 avoids these assumptions, offering reliable lower bounds, which is the main point of our paper.

VIII. DISCUSSION

Previous works have successfully demonstrated the distribution and certification of high-dimensional entanglement. While certain assumptions are suitable for these scenarios, in order to utilize high-dimensional entanglement for quantum key distribution, one requires an assumption-free analysis of the measurement setups used. In this work, we discuss assumptions present in previous works and suggest a simple modification of the measurement setup that helps to remove those assumptions. Our main contribution is a clean and rigorous analysis of a modified measurement setup, suitable not only for high-dimensional entanglement distribution but also for high-dimensional quantum key distribution. We also develop a realistic noise model for free-space QKD links, taking external factors such as solar light, atmospheric channel loss, and imperfections of the measurement devices,

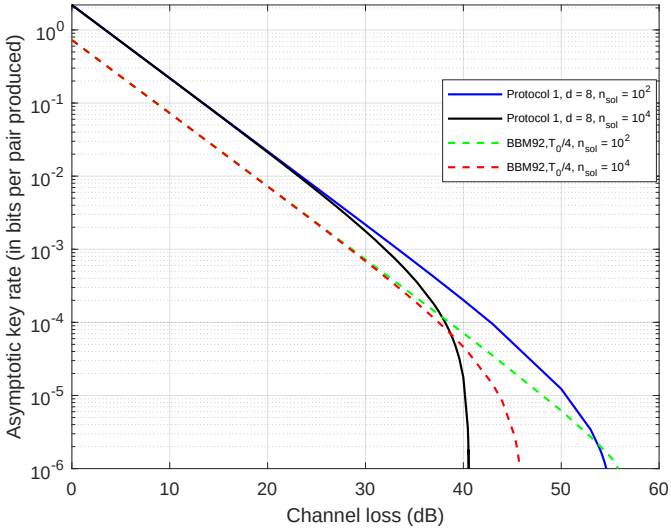

FIG. 3. Comparison of Protocol 1 (solid lines) for $d = 8$ with the corresponding key rates obtained for BBM92 (dashed lines) for solar photon rates of $n_{\text{sol}} \in \{10^2, 10^4\}$.

such as dark counts and detector inefficiencies, into account. Then, we apply a numerical security proof method to calculate lower bounds on the asymptotic secure key rate under the noise model developed. For comparison, we also consider a previously used measurement setup, that relies on certain assumptions that are not compatible with the requirements of QKD. Therefore, rates reported for that setup are only upper bounds. Nevertheless, our analysis shows that the rigorous lower bounds obtained for our proposed setup outperform the upper bounds obtained for the previous setup relying on unjustified assumptions both in terms of key rate and noise tolerance. Additionally, our modification simplifies the experimental setup significantly. We also compare our proposed protocol to BBM92 and observe better performance w.r.t. loss for relevant loss regimes.

Given that the unmodified setup (within the frame of mentioned assumptions) was able to transmit key during early daytime in summer [22] in urban atmospheric conditions, this seemingly modest increase of a factor of almost 2 in solar photons is actually a significant advance towards a full-day operation. Technical improvements such as sharper frequency filters and adaptive optics to correct for atmospheric turbulences are expected to improve key rate and noise tolerance further (see, for example, the experimental improvements in Refs. [9–15]). While the key rates presented are asymptotic, we anticipate that the advantages of our new protocol will become even more pronounced in the finite-size regime due to our simplified setup, which necessitates fewer measurements. The experimental simplicity of our proposal (only one interferometer needs to be stabilized), together with the results of our analysis, guides a practical path toward full-day satellite QKD. Besides a detailed finite-size analysis, interesting future directions include finding rapidly computable quantifiers instead of numerical SDPs, required to employ online adaptive subspace postselection, which can increase noise tolerance further [26, 38].

ACKNOWLEDGMENTS

We thank Mateus Araújo for numerous discussions about SDP implementations.

This work has received funding from the Horizon-Europe research and innovation programme under grant agreement No 101070168 (HyperSpace).

Co-funded by the European Union

[1] H. J. Kimble, The quantum internet, Nature **453**, 1023 (2008).
[2] C. H. Bennett and S. J. Wiesner, Communication via one- and two-particle operators on einstein-podolsky-rosen states, Phys. Rev. Lett. **69**, 2881 (1992).
[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels, Phys. Rev. Lett. **70**, 1895 (1993).
[4] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, India, 1984) p. 175.
[5] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).
[6] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nature Communications **8**, 15043 (2017).
[7] W. Wooters and W. Zurek, A single quantum cannot be cloned, Nature **299**, 802 (1982).
[8] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, Quantum repeaters: From quantum networks to the quantum internet, Reviews of Modern Physics **95**, 10.1103/revmodphys.95.045006 (2023).
[9] L. Han, Y. Li, P. Xu, X. Tao, W. Luo, W. Cai, S. Liao, and C. Peng, Integrated fabry–perot filter with wideband noise suppression for satellite-based daytime quantum key distribution, Appl. Opt. **61**, 812 (2022).
[10] M. Abasifard, C. Cholsuk, R. G. Pousa, A. Kumar, A. Zand, T. Riel, D. K. L. Oi, and T. Vogl, The ideal wavelength for daylight free-space quantum key distribution, APL Quantum **1**, 10.1063/5.0186767 (2024).
[11] A. Krzic, D. Heinig, M. Goy, and F. Steinlechner, Dual-downlink quantum key distribution with entangled photons: prospects for daylight operation, in *International Conference on Space Optics — ICSO 2022*, Vol. 12777, edited by K. Minoglou, N. Karafolas, and B. Cugny,

International Society for Optics and Photonics (SPIE, 2023) p. 1277726.
[12] Y.-H. Li, S.-L. Li, X.-L. Hu, C. Jiang, Z.-W. Yu, W. Li, W.-Y. Liu, S.-K. Liao, J.-G. Ren, H. Li, L. You, Z. Wang, J. Yin, F. Xu, Q. Zhang, X.-B. Wang, Y. Cao, C.-Z. Peng, and J.-W. Pan, Free-space and fiber-integrated measurement-device-independent quantum key distribution under high background noise, Phys. Rev. Lett. **131**, 100802 (2023).
[13] F. Bouchard, D. England, P. J. Bustard, K. L. Fenwick, E. Karimi, K. Heshami, and B. Sussman, Achieving ultimate noise tolerance in quantum communication, Phys. Rev. Appl. **15**, 024027 (2021).
[14] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics, npj Quantum Information **7**, 93 (2021).
[15] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, Long-distance free-space quantum key distribution in daylight towards inter-satellite communication, Nature Photonics **11**, 10.1038/nphoton.2017.116 (2017).
[16] P. G. Kwiat, Hyper-entangled states, Journal of Modern Optics **44**, 2173 (1997).
[17] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Generation of hyperentangled photon pairs, Phys. Rev. Lett. **95**, 260501 (2005).
[18] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, Phys. Rev. A **82**, 030301 (2010).
[19] A. Martin, T. Guerreiro, A. Tiranov, S. Designolle, F. Fröwis, N. Brunner, M. Huber, and N. Gisin, Quantifying photonic high-dimensional entanglement, Phys. Rev. Lett. **118**, 110501 (2017).
[20] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, Science Advances **3**, e1701491 (2017), https://www.science.org/doi/pdf/10.1126/sciadv.1701491.
[21] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons, Quantum **2**, 111 (2018).
[22] L. Bulla, M. Pivoluska, K. Hjorth, O. Kohout, J. Lang, S. Ecker, S. P. Neumann, J. Bittermann, R. Kindler, M. Huber, M. Bohmann, and R. Ursin, Nonlocal temporal interferometry for highly resilient free-space quantum communication, Phys. Rev. X **13**, 021001 (2023).
[23] K. Sulimany, G. Pelc, R. Dudkiewicz, S. Korenblit, H. S. Eisenberg, Y. Bromberg, and M. Ben-Or, High-dimensional coherent one-way quantum key distribution (2023), arXiv:2105.04733 [quant-ph].
[24] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, Overcoming noise in entanglement distribution, Phys. Rev. X **9**, 041042 (2019).
[25] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, High-dimensional quantum communication: Benefits, progress, and future challenges, Adv. Quant. Tech. **2**, 1900038 (2019).
[26] M. Doda, M. Huber, G. Murta, M. Pivoluska, M. Plesch, and C. Vlachou, Quantum key distribution overcoming extreme noise: simultaneous subspace coding using high-dimensional entanglement, Phys. Rev. Applied **15**, 034003 (2021).
[27] L. Bulla, K. Hjorth, O. Kohout, J. Lang, S. Ecker, S. P. Neumann, J. Bittermann, R. Kindler, M. Huber, M. Bohmann, R. Ursin, and M. Pivoluska, Distribution of genuine high-dimensional entanglement over 10.2 km of noisy metropolitan atmosphere, Physical Review A **107**, 10.1103/physreva.107.l050402 (2023).
[28] J. D. Franson, Bell inequality for position and time, Phys. Rev. Lett. **62**, 2205 (1989).
[29] J. C. Chapman, C. C. W. Lim, and P. G. Kwiat, Hyper-entangled time-bin and polarization quantum key distribution, Phys. Rev. Applied **18**, 044027 (2022).
[30] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A **461**, 207 (2005).
[31] M. Araújo, M. Huber, M. Navascués, M. Pivoluska, and A. Tavakoli, Quantum key distribution rates from semidefinite programming, Quantum **7**, 1019 (2023).
[32] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von neumann entropy, Quantum **8**, 1445 (2024).
[33] M. T. Gruneisen, M. L. Eickhoff, S. C. Newey, K. E. Stoltenberg, J. F. Morris, M. Bareian, M. A. Harris, D. W. Oesch, M. D. Oliker, M. B. Flanagan, B. T. Kay, J. D. Schiller, and R. N. Lanning, Adaptive-optics-enabled quantum communication: A technique for daytime space-to-earth links, Phys. Rev. Appl. **16**, 014067 (2021).
[34] G. Brassard and L. Salvail, Secret-key reconciliation by public discussion, in *Advances in Cryptology — EUROCRYPT '93*, edited by T. Helleseth (Springer Berlin Heidelberg, Berlin, Heidelberg, 1994) pp. 410–423.
[35] G. Brassard and L. Salvail, Secret-key reconciliation by public discussion, in *Advances in Cryptology — EUROCRYPT '93*, edited by T. Helleseth (Springer Berlin Heidelberg, Berlin, Heidelberg, 1994) pp. 410–423.
[36] D. Tupkary and N. Lütkenhaus, Using cascade in quantum key distribution, Phys. Rev. Appl. **20**, 064040 (2023).
[37] A. Mink and A. Nakassis, LDPC for QKD reconciliation, CoRR **abs/1205.4977** (2012), 1205.4977.
[38] X.-M. Hu, C. Zhang, Y. Guo, F.-X. Wang, W.-B. Xing, C.-X. Huang, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, X. Gao, M. Pivoluska, and M. Huber, Pathways for entanglement-based quantum communication in the face of high noise, Phys. Rev. Lett. **127**, 110505 (2021).

Appendix A: Analysis of the Franson Setup

In what follows, we derive the measurement operators for Time-Superposition measurements in more detail than in the main part.

Denote by x and y the horizontal and vertical input ports of a polarizing beamsplitter, respectively, and by x' and y' the corresponding outputs. Note that in our setup, the first beamsplitter has only one input port and the second beamsplitter has only one output port. Then, the action of a PBS is given by the unitary

$$\hat{U}_{\mathrm{PBS}} = \left(|\mathrm{H}\rangle\langle\mathrm{H}| \otimes \mathbb{1}_T \otimes |x'\rangle\langle x| + |\mathrm{H}\rangle\langle\mathrm{V}| \otimes \mathbb{1}_T \otimes |x'\rangle\langle y| + |\mathrm{V}\rangle\langle\mathrm{H}| \otimes \mathbb{1}_T \otimes |y'\rangle\langle x| + |\mathrm{V}\rangle\langle\mathrm{V}| \otimes \mathbb{1}_T \otimes |y'\rangle\langle y|\right). \tag{A1}$$

According to the description of our measurement setup above, only those parts in the upper y'-part experience a time as well as a phase shift. Thus, let

$$\hat{T}_y := \mathbb{1}_{\mathrm{Pol}} \otimes \mathbb{1}_T \otimes |x'\rangle\langle x'| + \mathbb{1}_{\mathrm{Pol}} \otimes \hat{T} \otimes |y'\rangle\langle y'| \tag{A2}$$

$$\hat{Q}_y := \mathbb{1}_{\mathrm{Pol}} \otimes \mathbb{1}_T \otimes |x'\rangle\langle x'| + \hat{Q}_\phi \otimes |y'\rangle\langle y'| \tag{A3}$$

be the operators describing these shifts. They allow us to describe the action of the whole setup by applying them one after another in the correct order

$$\hat{U}_I := \hat{U}_{\mathrm{PBS}}\hat{Q}_y\hat{T}_y\hat{U}_{\mathrm{PBS}}. \tag{A4}$$

As the output of the first PBS is directed to the input of the second PBS, we simply write (x', y') for the input ports of the second PBS, while we proceed with (x'', y'') for its outputs. We obtain

$$\hat{U}_I = \left(|\mathrm{H}\rangle\langle\mathrm{H}| \otimes \mathbb{1}_T + |\mathrm{V}\rangle\langle\mathrm{V}| \otimes \hat{Q}_\phi\hat{T}\right) \otimes |x''\rangle\langle x| + \left(|\mathrm{H}\rangle\langle\mathrm{H}| \otimes \hat{Q}_\phi\hat{T} + |\mathrm{V}\rangle\langle\mathrm{V}| \otimes \mathbb{1}_T\right) \otimes |y''\rangle\langle y|. \tag{A5}$$

Note that in our case, input y is empty, so effectively, we only need to consider the first term – horizontally polarized states pass the interferometer untouched while vertically polarized states experience a time as well as a phase shift. As we put our measurement devices in the output port x'' of the interferometer, we can drop the register x'' for ease of notation.

Finally, we obtain the unitary operator representing the action of the whole interferometer setup on Alice's and Bob's joint state ρ_{AB},

$$\begin{aligned}\hat{U} &:= \hat{U}_I \otimes \hat{U}_I \\ &= |\mathrm{HH}\rangle\langle\mathrm{HH}| \otimes \mathbb{1}_T \otimes \mathbb{1}_T + |\mathrm{HV}\rangle\langle\mathrm{HV}| \otimes \mathbb{1}_T \otimes \hat{Q}_\phi\hat{T} + |\mathrm{VH}\rangle\langle\mathrm{VH}| \otimes \hat{Q}_\phi\hat{T} \otimes \mathbb{1}_T + |\mathrm{VV}\rangle\langle\mathrm{VV}| \otimes \hat{Q}_\phi\hat{T} \otimes \hat{Q}_\phi\hat{T}.\end{aligned} \tag{A6}$$

The interferometer is followed by a half-wave plate and another polarizing beamsplitter, followed by two detectors, one in each arm of the PBS such that the right detector measures horizontally polarized photons, while the upper detector measures vertically polarized photons. However, the half-wave plate rotates the plane of polarization as $U_{\mathrm{HWP}}|\mathrm{H}\rangle = |\mathrm{D}\rangle$ and $U_{\mathrm{HWP}}|\mathrm{V}\rangle = |\mathrm{A}\rangle$, i.e., it allows us to measure diagonally polarized photons in the right arm and antidiagonally polarized photons in the upper arm. The corresponding measurements project onto $|\mathrm{D}, i\rangle$ and $|\mathrm{A}, i\rangle$ respectively. This can be used to derive the effective measurements, as carried out in the main part of this manuscript.

Appendix B: Analysis of Protocol 2

Finally, we turn to the second protocol where the target state is $|\Psi_{\mathrm{target}}\rangle = \frac{|\mathrm{HH}\rangle+|\mathrm{VV}\rangle}{\sqrt{2}} \otimes \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|kk\rangle$. Unlike in Protocol 1, there is no polarization filter, so we have to *assume* that the polarization remains unchanged when the state passes the quantum channel. Thus, Alice's and Bob's shared state reads $\rho_{AB} = \frac{|\mathrm{HH}\rangle\langle\mathrm{HH}|+|\mathrm{HH}\rangle\langle\mathrm{VV}|+|\mathrm{VV}\rangle\langle\mathrm{HH}|+|\mathrm{VV}\rangle\langle\mathrm{VV}|}{2} \otimes \rho_T$. As for Protocol 1, it follows directly that the coincidence-clicks for the TOA measurements correspond to the diagonal entries of the time-density matrix,

$$\mathrm{TT}(i,j) = \langle i,j|\rho_T|i,j\rangle. \tag{B1}$$

Applying Eq. (12) to ρ_{AB} yields

$$\mathrm{SS}_{1,1}(i,j) = \frac{1}{8}\left(\langle i+, j+|\rho_T|i+, j+\rangle + \langle i+, j+|\rho_T|i-, j-\rangle + \langle i-, j-|\rho_T|i+, j+\rangle + \langle i-, j-|\rho_T|i-, j-\rangle\right) \tag{B2}$$

$$= \mathrm{SS}_{2,2}(i,j), \tag{B3}$$

$$\mathrm{SS}_{1,2}(i,j) = \frac{1}{8}\left(\langle i+, j-|\rho_T|i+, j-\rangle + \langle i+, j-|\rho_T|i-, j+\rangle + \langle i-, j+|\rho_T|i+, j-\rangle + \langle i-, j+|\rho_T|i-, j+\rangle\right) \tag{B4}$$

$$= \mathrm{SS}_{2,1}(i,j). \tag{B5}$$

As $\mathrm{SS}_{1,1}(i,j)$ and $\mathrm{SS}_{2,2}(i,j)$ as well as $\mathrm{SS}_{1,2}(i,j)$ and $\mathrm{SS}_{2,1}(i,j)$ are equal, we can combine those elements respectively into 'same phase' and 'opposite phase' clicks,

$$\mathrm{SS}_s(i,j) := \mathrm{SS}_{1,1}(i,j) + \mathrm{SS}_{2,2}(i,j) \tag{B6}$$
$$\mathrm{SS}_o(i,j) := \mathrm{SS}_{1,2}(i,j) + \mathrm{SS}_{2,1}(i,j). \tag{B7}$$

For the mismatched measurements, we obtain from Eqs. (13)-(14)

$$\mathrm{TS}_1(i,j) = \frac{1}{2}\langle i,j+|\rho_T|i,j+\rangle\,, \tag{B8}$$
$$\mathrm{TS}_2(i,j) = \frac{1}{2}\langle i,j-|\rho_T|i,j-\rangle\,, \tag{B9}$$
$$\mathrm{ST}_1(i,j) = \frac{1}{2}\langle i+,j|\rho_T|i+,j\rangle\,, \tag{B10}$$
$$\mathrm{ST}_2(i,j) = \frac{1}{2}\langle i-,j|\rho_T|i-,j\rangle\,. \tag{B11}$$

As for Protocol 1, one can see immediately that

$$\mathcal{M}_0^{P1} := \{|i,j\rangle\langle i,j|\}_{i,j=0}^{d-1} \tag{B12}$$

forms a POVM induced by the bases $\mathbb{B}_0^{A/B}$ on Alice's and Bob's side respectively with corresponding click-matrix

$$C_{\mathcal{M}_0^{P1}}(i,j) := \mathrm{TT}(i,j), \tag{B13}$$

where we have chosen the natural order $\{|0\rangle, |1\rangle, ..., |d-1\rangle\}$. Next, we aim to find a second POVM, which requires some preparations. From the definitions made in Eqs. (B6) and (B7), it follows directly that

$$\mathrm{SS}_s(i,j) = \frac{1}{2}\mathrm{Tr}\left[\rho_T \left|\Phi_s^{A,B}(i,j)\right\rangle\!\left\langle\Phi_s^{A,B}(i,j)\right|\right] \tag{B14}$$
$$\mathrm{SS}_o(i,j) = \frac{1}{2}\mathrm{Tr}\left[\rho_T \left|\Phi_o^{A,B}(i,j)\right\rangle\!\left\langle\Phi_o^{A,B}(i,j)\right|\right], \tag{B15}$$

with

$$\left|\Phi_s^{A,B}(i,j)\right\rangle := \frac{1}{\sqrt{2}}\left(|i+,j+\rangle + |i-,j-\rangle\right), \tag{B16}$$
$$\left|\Phi_o^{A,B}(i,j)\right\rangle := \frac{1}{\sqrt{2}}\left(|i+,j-\rangle + |i-,j+\rangle\right). \tag{B17}$$

A short calculation shows that

$$\left|\Phi_s^{A,B}(i,j)\right\rangle\!\left\langle\Phi_s^{A,B}(i,j)\right| + \left|\Phi_o^{A,B}(i,j)\right\rangle\!\left\langle\Phi_o^{A,B}(i,j)\right| = |i,j\rangle\langle i,j| + |i-1,j-1\rangle\langle i-1,j-1|$$

and

$$|i,j+\rangle\langle i,j+| + |i,j-\rangle\langle i,j-| = |i,j\rangle\langle i,j| + |i,j-1\rangle\langle i,j-1|$$
$$|i+,j\rangle\langle i+,j| + |i-,j\rangle\langle i-,j| = |i,j\rangle\langle i,j| + |i-1,j\rangle\langle i-1,j|\,.$$

Next, we combine those measurement operators and obtain

$$\begin{aligned}
&\sum_{i,j=1}^{d-1}\left(\left|\Phi_s^{A,B}(i,j)\right\rangle\!\left\langle\Phi_s^{A,B}(i,j)\right| + \left|\Phi_o^{A,B}(i,j)\right\rangle\!\left\langle\Phi_o^{A,B}(i,j)\right|\right)\\
&+\sum_{j=1}^{d-1}\left(|0,j+\rangle\langle 0,j+| + |0,j-\rangle\langle 0,j-| + |d-1,j+\rangle\langle d-1,j+| + |d-1,j-\rangle\langle d-1,j-|\right)\\
&+\sum_{i=1}^{d-1}\left(|i+,0\rangle\langle i+,0| + |i-,0\rangle\langle i-,0| + |i+,d-1\rangle\langle i+,d-1| + |i-,d-1\rangle\langle i-,d-1|\right)\\
&+\left(\mathbb{1}_{d^2\times d^2} - |00\rangle\langle 00| - |d-1,d-1\rangle\langle d-1,d-1|\right)\\
&=3\mathbb{1}_{d^2\times d^2}.
\end{aligned}$$

Thus, after scaling all elements by $\frac{1}{3}$, we obtain the second POVM,

$$\mathcal{M}_1^{P2} := \Big\{ \frac{1}{3}\left(\mathbb{1}_{d^2\times d^2} - |00\rangle\langle 00| - |d-1,d-1\rangle\langle d-1,d-1|\right), \frac{1}{3}\left|\Phi_s^{A,B}(i,j)\rangle\langle\Phi_s^{A,B}(i,j)\right|, \frac{1}{3}\left|\Phi_o^{A,B}(i,j)\rangle\langle\Phi_o^{A,B}(i,j)\right|, \\ \frac{1}{3}|0,j+\rangle\langle 0,j+|, \frac{1}{3}|0,j-\rangle\langle 0,j-|, \frac{1}{3}|d-1,j+\rangle\langle d-1,j+|, \frac{1}{3}|d-1,j+\rangle\langle d-1,j+|, \\ \frac{1}{3}|i+,0\rangle\langle i+,0|, \frac{1}{3}|i-,0\rangle\langle i-,0|, \frac{1}{3}|i+,d-1\rangle\langle i+,d-1|, \frac{1}{3}|i-,d-1\rangle\langle i-,d-1| \Big\}_{i,j=1}^{d-1}. \tag{B18}$$

Consequently, taking both the renormalization by $\frac{1}{3}$ and Eqs. (B6) - (B11) into account, the corresponding clicks are normalized as follows,

$$\begin{aligned} 1 = {} & \frac{1}{3}\left(1 - \mathrm{TT}(0,0) - \mathrm{TT}(d-1,d-1)\right) + \frac{2}{3}\sum_{i,j=1}^{d-1}\left(\mathrm{SS}_s(i,j) + \mathrm{SS}_o(i,j)\right) \\ & + \frac{2}{3}\sum_{j=1}^{d-1}\left(\mathrm{TS}_1(0,j) + \mathrm{TS}_2(0,j) + \mathrm{TS}_1(d-1,j) + \mathrm{TS}_2(d-1,j)\right) \\ & + \frac{2}{3}\sum_{i=1}^{d-1}\left(\mathrm{ST}_1(i,0) + \mathrm{ST}_2(i,0) + \mathrm{ST}_1(i,d-1) + \mathrm{ST}_2(i,d-1)\right). \end{aligned} \tag{B19}$$

As we have already used the clicks from the computational basis measurement (TT-clicks), we do not expect any contribution to the key rates from these clicks. Since they simply introduce redundant constraints into our semi-definite program, we can remove those elements/clicks when we formulate the SDP as long as we account for them during normalization.

In contrast to Protocol 1, we have already exhausted our measurements so that we cannot build a third POVM.

Appendix C: Details regarding the noise model

As already mentioned in the main text, we have to consider various origins of noise. In particular, there are noise effects due to the interaction of the photons with the environment, mainly photons coming from the Sun, and due to the imperfect channels and detectors, so we take into account four different kinds of imperfections:

(1) Channel loss: Photons might get lost on the way from the source to the labs.

(2) Detection inefficiency: Due to detection inefficiencies, incoming photons cause a click with probability $\eta_D \in [0,1]$.

(3) Environmental photons: Photons coming from the residual environment (like those coming from the Sun) can cause clicks.

(4) Dark counts: Imperfections of the detectors can cause clicks even in the absence of photons.

Let $P_{\mathrm{prod}}(n)$ be the probability distribution of n polarized photon pairs produced by the source per time-frame, let P_{loss}^A and P_{loss}^B denote the probabilities for source photons to get lost on their way from the source to Alice's and Bob's lab, respectively, and let η_A and η_B be the detection efficiency parameters of Alice's and Bob's detectors respectively. The probability that the environment, including the Sun, produces n (unpolarized) photons per time-frame on Alice's side is given by $P_{\mathrm{env}}^A(n)$ and on Bob's side by $P_{\mathrm{env}}^B(n)$. In case the incoming photons pass a polarization filter that is aligned with the polarization produced by the source (Protocol 1), on average, half of the (unpolarized) environmental photons are blocked. Moreover, for each of the detectors, n dark counts per time-frame may occur with a probability of $P_{\mathrm{dark}}(n)$. These considerations yield:

- The probability that n photon pairs are produced per time-frame T is given by $P_{\mathrm{prod}}(n)$.

- Some photons get lost, so the probability of having b_1 (respectively b_2) photons left for Alice and Bob after the

lossy channel is given by

$$P_1^A(b_1) = \sum_{i=b_1}^{\infty} P_{\text{prod}}(i)(1-P_{\text{loss}}^A)^{b_1} P_{\text{loss}}^{i-b_1} \binom{i}{b_1},$$
$$P_1^B(b_2) = \sum_{i=b_2}^{\infty} P_{\text{prod}}(i)(1-P_{\text{loss}}^B)^{b_2} P_{\text{loss}}^{i-b_2} \binom{i}{b_2}$$

respectively. These remaining photons are still polarized.

- The probability of q sunlight and further environmental photons being produced within one time-frame T on Alice's and Bob's side is $P_{\text{env}}^A(q)$ and $P_{\text{env}}^B(q)$, respectively.

- When the photons pass the polarization filter (which is placed only in Protocol 1), photons coming from the source remain mainly untouched, while half of the photons stemming from the Sun get blocked. Therefore, the probabilities that e_1 (respectively e_2) environmental photons pass Alice's and Bob's PBS are given by

$$P_{\text{env}}'^A(e_1) = \sum_{j=e_1}^{\infty} P_{\text{env}}^A(j) \left(\frac{1}{2}\right)^{e_1} \left(1-\frac{1}{2}\right)^{j-e_1} \binom{j}{e_1} = \sum_{j=e_1}^{\infty} \binom{j}{e_1} \left(\frac{1}{2}\right)^{j} P_{\text{env}}^A(j),$$
$$P_{\text{env}}'^B(e_2) = \sum_{j=e_2}^{\infty} \binom{j}{e_2} \left(\frac{1}{2}\right)^{j} P_{\text{env}}^B(j)$$

respectively.

- Now the environmental photons are combined with the photons coming from the source. The probability of having f_1 photons in Alice's lab after the polarization filter therefore is given by

$$\begin{aligned} P_2^A(f_1) &= \sum_{l=0}^{f_1} P_1^A(l) P_{\text{env}}'^A(f_1-l) \\ &= \sum_{l=0}^{f_1} \sum_{i=l}^{\infty} P_{\text{prod}}(i)(1-P_{\text{loss}}^A)^l (P_{\text{loss}}^A)^{(i-l)} \binom{i}{l} \sum_{j=f_1-l}^{\infty} \binom{j}{f_1-l} \left(\frac{1}{2}\right)^j P_{\text{env}}^A(j) \\ &= \sum_{l=0}^{f_1} \sum_{i=l}^{\infty} \sum_{j=f_1-l}^{\infty} \binom{i}{l}\binom{j}{f_1-l} P_{\text{prod}}(i) P_{\text{env}}^A(j)(1-P_{\text{loss}}^A)^l (P_{\text{loss}}^A)^{(i-l)} \left(\frac{1}{2}\right)^j \end{aligned}$$

and similarly for Bob the probability of having f_2 photons in his lab after the filter is

$$P_2^B(f_2) = \sum_{l=0}^{f_2} \sum_{i=l}^{\infty} \sum_{j=f_2-l}^{\infty} \binom{i}{l}\binom{j}{f_2-l} P_{\text{prod}}(i) P_{\text{env}}^B(j)(1-P_{\text{loss}}^B)^l (P_{\text{loss}}^B)^{(i-l)} \left(\frac{1}{2}\right)^j.$$

Since the source produces photon pairs, the joint probability of Alice and Bob having n_1 and n_2 photons

respectively after the filter is found to be

$$P(n_1,n_2)=\sum_{s=0}^{\infty}\sum_{m_1=0}^{\min\{s,n_1\}}\sum_{m_2=0}^{\min\{s,n_2\}}P_{\mathrm{prod}}(s)(1-P_{\mathrm{loss}}^A)^{m_1}(P_{\mathrm{loss}}^A)^{(s-m_1)}\binom{s}{m_1} \tag{C1}$$

$$\cdot(1-P_{\mathrm{loss}}^B)^{m_2}(P_{\mathrm{loss}}^B)^{(s-m_2)}\binom{s}{m_2}P'^A_{\mathrm{env}}(n_1-m_1)P'^B_{\mathrm{env}}(n_2-m_2) \tag{C2}$$

$$=\sum_{s=0}^{\infty}\sum_{m_1=0}^{\min\{s,n_1\}}\sum_{m_2=0}^{\min\{s,n_2\}}\binom{s}{m_1}\binom{s}{m_2}P_{\mathrm{prod}}(s)(1-P_{\mathrm{loss}}^A)^{m_1}(P_{\mathrm{loss}}^A)^{(s-m_1)}(1-P_{\mathrm{loss}}^B)^{m_2}(P_{\mathrm{loss}}^B)^{(s-m_2)} \tag{C3}$$

$$\cdot\sum_{j=n_1-m_1}^{\infty}\binom{j}{n_1-m_1}\left(\frac{1}{2}\right)^j P_{\mathrm{env}}^A(j)\sum_{k=n_2-m_2}^{\infty}\binom{k}{n_2-m_2}\left(\frac{1}{2}\right)^k P_{\mathrm{env}}^B(k) \tag{C4}$$

$$=\sum_{s=0}^{\infty}\sum_{m_1=0}^{\min\{s,n_1\}}\sum_{m_2=0}^{\min\{s,n_2\}}\sum_{j=n_1-m_1}^{\infty}\sum_{k=n_2-m_2}^{\infty}\binom{s}{m_1}\binom{s}{m_2}\binom{j}{n_1-m_1}\binom{k}{n_2-m_2}P_{\mathrm{prod}}(s)P_{\mathrm{env}}^A(j)P_{\mathrm{env}}^B(k) \tag{C5}$$

$$\cdot(1-P_{\mathrm{loss}}^A)^{m_1}(1-P_{\mathrm{loss}}^B)^{m_2}(P_{\mathrm{loss}}^A)^{(s-m_1)}(P_{\mathrm{loss}}^B)^{(s-m_2)}(P_{\mathrm{loss}}^A)^{(s-m_1)}(P_{\mathrm{loss}}^B)^{(s-m_2)}\left(\frac{1}{2}\right)^{(j+k)}. \tag{C6}$$

- Next, we take dark counts and detector inefficiencies into account. As the protocol discards all the events where there is a multiclick or no click in a time-frame, we only have to examine the case with exactly one dark count and no genuine photon being detected or when there is no dark count, and exactly one photon causes a detector click. This yields the probabilities for Alice and Bob each having exactly one click per time-frame in the same time-bin when there are n_1 (source or environmental) photons left on Alice's side and n_2 (source or environmental) photons left on Bob's side,

$$P(\text{click}|n_1\text{ photons})=P_{dark}(1)(1-\eta_A)^{n_1}+P_{dark}(0)(1-\eta_A)^{(n_1-1)}\eta_A\binom{n_1}{1}$$
$$P(\text{click}|n_2\text{ photons})=P_{dark}(1)(1-\eta_B)^{n_2}+P_{dark}(0)(1-\eta_B)^{(n_2-1)}\eta_B\binom{n_2}{1}.$$

- Finally, the probability of exactly one coincidence click per time-frame in the same time-bin can be calculated as

$$P_{TT}(1,1):=\sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty}P(\text{click}|n_1\text{ photons})P(\text{click}|n_2\text{ photons})P(n_1,n_2).$$

All photon contributions mentioned are independent of each other and also photons from each of the origins mentioned are produced independently of other photons of the same origin. Hence, one can model these influences by Poisson distributions:

$$P_{\mathrm{prod}}(n)=\frac{(\lambda_pT)^ne^{-\lambda_p(T)}}{n!}=:\frac{C_p^ne^{-C_p}}{n!},\qquad P_{\mathrm{dark}}(n)=\frac{(\lambda_dT)^ne^{-\lambda_d(T)}}{n!}=:\frac{C_d^ne^{-C_d}}{n!}$$

$$P_{\mathrm{env}}^A(n)=\frac{(\lambda_e^AT)^ne^{-\lambda_e^A(T)}}{n!}=:\frac{(C_e^A)^ne^{-C_e^A}}{n!},\qquad P_{\mathrm{env}}^B(n)=\frac{(\lambda_e^BT)^ne^{-\lambda_e^B(T)}}{n!}=:\frac{(C_e^B)^ne^{-C_e^B}}{n!}$$

Using the distribution of $P_{\mathrm{env}}^{A/B}(n)$, we see that $P'^{A/B}_{\mathrm{env}}(n)$ is distributed according to

$$P'^{A/B}_{\mathrm{env}}(n)=\sum_{k=n}^{\infty}\binom{k}{n}\left(\frac{1}{2}\right)^k\frac{(C_e^{A/B})^ke^{-C_e^{A/B}}}{k!}=e^{-C_{e,A/B}}\sum_{k=n}^{\infty}\frac{k!}{n!(k-n)!}\frac{(C_{e,A/B})^k}{k!\cdot 2^k}$$
$$=\frac{e^{-C_e^{A/B}}}{n!}\sum_{k=n}^{\infty}\frac{(C_e^{A/B})^k}{2^k(k-n)!}\overset{j:=k-n}{=}\frac{e^{-C_{e,A/B}}}{n!}\sum_{j=0}^{\infty}\frac{(C_e^{A/B})^{j+n}}{2^{j+n}\cdot j!}=\frac{e^{-C_e^{A/B}}(C_e^{A/B})^n}{n!\cdot 2^n}\sum_{j=0}^{\infty}\frac{(C_e^{A/B})^j}{2^j\cdot j!}$$
$$=\frac{e^{-C_e^{A/B}}}{n!}\left(\frac{C_e^{A/B}}{2}\right)^n e^{\frac{C_e^{A/B}}{2}}=\frac{e^{\frac{-C_e^{A/B}}{2}}}{n!}\left(\frac{C_e^{A/B}}{2}\right)^n.$$

Plugging C_e into (C1), we obtain

$$P(n_1,n_2)=\sum_{s=0}^{\infty}\sum_{m_1=0}^{\min\{s,n_1\}}\sum_{m_2=0}^{\min\{s,n_2\}}\sum_{j=n_1-m_1}^{\infty}\sum_{k=n_2-m_2}^{\infty}\binom{s}{m_1}\binom{s}{m_2}\binom{j}{n_1-m_1}\binom{k}{n_2-m_2}P_{\text{prod}}(s)\frac{\left(C_e^A\right)^j e^{-C_e^A}}{j!} \tag{C7}$$

$$\frac{\left(C_e^B\right)^k e^{-C_e^B}}{k!}(1-P_{\text{loss}}^A)^{m_1}(1-P_{\text{loss}}^B)^{m_2}(P_{\text{loss}}^A)^{(s-m_1)}(P_{\text{loss}}^B)^{(s-m_2)}\left(\frac{1}{2}\right)^{(j+k)}. \tag{C8}$$

With the formulas for $P_{\text{env}}^{\prime A/B}$, this yields

$$\begin{aligned}P(n_1,n_2)=e^{-\frac{(C_e^A+C_e^B)}{2}}\cdot\sum_{s=0}^{\infty}P_{\text{prod}}(s)\cdot(s!)^2\cdot\sum_{m_1=0}^{\min\{s,n_1\}}\frac{(1-P_{\text{loss}}^A)^{m_1}(P_{\text{loss}}^A)^{s-m_1}(\frac{C_e^A}{2})^{n_1-m_1}}{m_1!(s-m_1)!(n_1-m_1)!}\\ \cdot\sum_{m_2=0}^{\min\{s,n_2\}}\frac{(1-P_{\text{loss}}^B)^{m_2}(P_{\text{loss}}^B)^{s-m_2}(\frac{C_e^B}{2})^{n_2-m_2}}{m_2!(s-m_2)!(n_2-m_2)!}.\end{aligned} \tag{C9}$$

To ease notation, we define

$$I^{A/B}(s,n_j):=\sum_{m_i=0}^{\min\{s,n_j\}}\frac{(1-P_{\text{loss}}^{A/B})^{m_j}(P_{\text{loss}}^{A/B})^{s-m_j}(\frac{C_e^{A/B}}{2})^{n_j-m_j}}{m_j!(s-m_j)!(n_j-m_j)!},\qquad j\in\{1,2\}.$$

For practical reasons, we choose C_p such that the expected number of photon pairs per time-frame is much lower than 1 so that the probability of more than one photon pair is close to zero, $P_{\text{prod}}(s>1)\approx 0$. We use this assumption, that it is extremely rare that more than one photon pair is emitted by the source in one time-frame and therefore can be neglected, also in our code for the calculation of the key rates.
Then, we obtain

$$\begin{aligned}I^{A/B}(0,n)&=\frac{(C_e^{A/B})^n}{n!},\\ I^{A/B}(1,n)&=\begin{cases}P_{\text{loss}}^{A/B},n=0,\\ \frac{P_{\text{loss}}^{A/B}\left(\frac{C_e^{A/B}}{2}\right)^n}{n!}+\frac{(1-P_{\text{loss}}^{A/B})\left(\frac{C_e^{A/B}}{2}\right)^{n-1}}{(n-1)!},n\in\mathbb{N}^+.\end{cases}\end{aligned}$$

Consequently, we can write expression (C9) for $P(n_1,n_2)$ as

$$P(n_1,n_2)=e^{-\frac{C_e^A+C_e^B+2C_p}{2}}\left(I^A(0,n_1)I^B(0,n_2)+C_pI^A(1,n_1)I^B(1,n_2)\right).$$

It remains to find an expression for the probability of a 'good' coincidence click, i.e., a click originating from two source photons taking place in the same time-frame. This probability is given by the event that exactly one photon pair is produced, arrives in Alice's and Bob's labs, and is detected while no dark counts occur and no environmental photons meet Alice's and Bob's detectors,

$$P_{\text{Good}}=P_{\text{prod}}(1)(1-P_{\text{loss}}^A)(1-P_{\text{loss}}^B)\eta^A\eta^B(P_{\text{dark}}(0))^2\left(\sum_{k=0}^{\infty}P_{\text{env}}^{\prime A}(k)(1-\eta^A)^k\right)\left(\sum_{k=0}^{\infty}P_{\text{env}}^{\prime B}(k)(1-\eta^A)^k\right).$$

Finally, the isotropic noise parameter is given by $v=\frac{P_{\text{Good}}}{P_{\text{TT}}(1,1)}$, such that

$$\rho(v)=v\left|\Psi_{\text{target}}\right\rangle\!\left\langle\Psi_{\text{target}}\right|+(1-v)\frac{1}{d^2}\mathbb{1}_{d^2\times d^2}. \tag{C10}$$

In what follows, we assume that the photon source is placed in Alice's lab, which is in accordance with many practical realizations of QKD setups, such as the Free-Space Link between Vienna and Bisamberg. This means that Alice's source photons experience no channel loss and that there is no noise due to environmental photons on Alice's side, i.e. $P_{\text{loss}}^A=0, C_e^A=0$. The indicated realistic and practical setting leads to the following simplified expressions.

For Protocol 1 (where we place a polarization filter at the entrance of Bob's lab), we obtain

$$\begin{aligned} P_{\mathrm{TT}}(1,1) =& \frac{1}{2} e^{-2C_{\mathrm{d}} - C_{\mathrm{p}} - \frac{C_e^B}{2}\eta_D} \\ & \cdot \left[C_{\mathrm{p}} \eta_D^2 \left(2 + C_e^B - 2P_{\mathrm{loss}}^B - C_e^B (1 - P_{\mathrm{loss}}^B)\eta_D\right) + C_{\mathrm{d}}^2 \left(2 + 2C_{\mathrm{p}}(1-\eta_D)\left(1 - \eta_D(1 - P_{\mathrm{loss}}^B)\right)\right) \right. \\ & \left. \quad + C_{\mathrm{d}} \eta_D \left(C_e^B + C_{\mathrm{p}}\left(4 - 2P_{\mathrm{loss}}^B - 4\eta_D + 4P_{\mathrm{loss}}^B \eta_D + C_e^B (1-\eta_D)\left(1 - (1 - P_{\mathrm{loss}}^B)\eta_D\right)\right)\right) \right] \end{aligned} \tag{C11}$$

and

$$P_{\mathrm{Good}} = C_{\mathrm{p}} (1 - P_{\mathrm{loss}}^B) \eta_D^2 e^{-2C_{\mathrm{d}} - C_{\mathrm{p}} - \frac{C_e^B}{2}\eta_D}, \tag{C12}$$

while for Protocol 2, we obtain

$$\begin{aligned} P_{\mathrm{TT}}(1,1) =& e^{-2C_{\mathrm{d}} - C_{\mathrm{p}} - C_{e^B}\eta_D} \\ & \cdot \left[C_{\mathrm{d}}^2 (1 + C_{\mathrm{p}}) + C_{\mathrm{d}} \left(C_e^B + C_{\mathrm{p}}\left(2 + C_e^B - C_{\mathrm{d}}(2 - P_{\mathrm{loss}}^B) - P_{\mathrm{loss}}^B\right)\right)\eta_D \right. \\ & \quad + C_{\mathrm{p}} \left(1 + C_e^B - P_{\mathrm{loss}}^B + C_{\mathrm{d}}\left(C_{\mathrm{d}} - 2(1 + C_e^B) - C_{\mathrm{d}} P_{\mathrm{loss}}^B + (2 + C_{\mathrm{e},B}) P_{\mathrm{loss}}^B\right)\right)\eta_D^2 \\ & \left. \quad + (1 - C_{\mathrm{d}}) C_{\mathrm{p}} C_e^B (-1 + P_{\mathrm{loss}}^B)\eta_D^3 \right] \end{aligned} \tag{C13}$$

and

$$P_{\mathrm{Good}} = C_{\mathrm{p}} (1 - P_{\mathrm{loss}}^B) \eta_D^2 e^{-2C_{\mathrm{d}} - C_{\mathrm{p}} - C_e^B \eta_D}. \tag{C14}$$

We note that this model covers all major contributions to white noise, which also represents the most dominant sources of noise and we leave more sophisticated noise models for future work.