We use a recent numerical security proof technique to analyse three different postselection strategies for continuous-variable quantum key distribution protocols (CV-QKD) with quadrature phase-shift keying modulation. For all postselection strategies studied we provide novel analytical results for the operators that define the respective regions in phase space. In both, the untrusted and trusted detector model, a new, cross-shaped postselection strategy, clearly outperforms a state-of-the-art radial postselection scheme for higher transmission distances and higher values of noise. Motivated by the high computational effort for the error-correction phase we also studied the case when a large fraction of the raw key is eliminated by postselection: We observe that the secure key rate in case that only 20% of the raw key passes the cross-shaped postselection is still roughly 80% of the secure key rate without postselection for low values of excess noise and roughly 95% for higher values of excess noise. Furthermore, we examine a strategy with radial&angular postselection that combines both the advantages of state-of-the-art radial postselection schemes and our cross-shaped strategy at the cost of higher complexity due to a second parameter. Employing the cross-shaped postselection strategy, that can easily be introduced in the data processing, both new and existing CV-QKD systems can improve the achievable secure key rates significantly.

CONTENTS

I. Introduction 2
A. Organisation 2

II. The security proof approach 3
A. Finding an almost optimal attack 3
B. Obtaining a tight lower bound on the key rate 4
C. Specifying the optimisation problem 4
D. Trusted detector approach 5

III. Examined protocols 6

IV. Formalisation of the postprocessing steps 8
A. Partitioning of the phase-space 8
B. Region operators for the untrusted detector 8
C. Region operators for the trusted detector 9
D. Information-leakage during reconciliation 10

V. Implementation and validation of the method 10
A. Implementation 10
B. Validation for the noiseless channel 11
1. Optimal coherent state amplitude 11
2. Analytical vs. numerical secure key rates 11

VI. Postselection strategies for untrusted detectors 12
A. Cross-shaped postselection 13
1. Optimal coherent state amplitude 13
2. Key rates for different transmission distances and noise levels 13
B. Comparison of postselection strategies 15

VII. Postselection strategies for trusted detectors 17
A. Cross-shaped postselection 17
B. Comparison of postselection strategies 18
1. Key rates for low values of excess noise 18
2. Key rates for medium values of excess noise 19
3. Sensitivity of the key rate on the noise level 20
4. Resumé for trusted detectors 21

VIII. Conclusions 20

Acknowledgments 21
A. Fock-state representation of region operators for the untrusted noise scenario 21
1. Radial&angular postselection 22
2. Cross-shaped postselection 22
B. Fock-state representation of region operators for the trusted detector scenario 24
1. Radial&angular postselection 24
2. Cross-shaped postselection 25
3. First- and second-moment observables 26
C. Choice of the cutoff number $N_c$ 27
D. Symbols used 28
References 28
I. INTRODUCTION

Quantum key distribution (QKD) enables two authenticated, remote parties, commonly called Alice and Bob, to establish a shared (cryptographic) secret key without any assumptions on the computational power of a potential adversary. The first and maybe most famous cryptographic protocol based on quantum mechanics, BB84, was published by Bennett and Brassard [1] in 1984 and is based on (discretely) polarised photons. Discrete-variable (DV) QKD protocols like BB84 rely on single-photon detectors that are rather expensive components. In contrast, continuous-variable (CV) QKD protocols are based on the field quadratures of light that can be measured by homodyne or heterodyne detection using photodiodes, hence do not suffer from serious hardware limitations and rely on well-known and tested infrastructure like lasers and optical fibres. The first continuous-variable (CV) QKD protocol goes back to Ralph in 1999 [2] and is based on discrete modulation. It is known [3] that postselection can increase the secure key rate for continuous-variable QKD-protocols by lowering the information available to an adversary. A discussion about postselection areas for multi-letter phase-shift-keying protocols can be found in [4]. References [5–7] give comprehensive reviews over the entire field of quantum key distribution in general, about implementations and about QKD security proofs.

The process of finding a lower bound on the achievable secure key rate is called security proof. Analytical attempts to prove the security of a certain QKD protocol are often very technical, introduce looseness in the lower bounds and often cannot be generalised to other QKD protocols. A very recent and general attempt [8] gives an analytical lower bound on the secure key rate of CV-QKD protocols with arbitrary discrete modulation in the asymptotic limit, but does not consider postselection.

In contrast, numerical attempts are typically more flexible concerning changes in the protocol structure. On the other hand, numerical calculations have only finite precision, and we cannot expect that the involved optimisation tasks reach the optimum with arbitrary accuracy. In particular, for continuous-variable protocols, we have to approximate physical quantities that live in infinite-dimensional Hilbert spaces by finite-dimensional spaces to make the key-rate-finding problems computationally feasible, which brings another uncertainty in the security proof. Finally, as the most interesting Discrete Modulated (DM) CV-QKD protocols involve four or more states, the numerical tasks are very high-dimensional, hence computation time is another crucial point.

A powerful framework for calculating reliable numerical secure key rates for QKD protocols was published [9,10] being computationally efficient and taking numerical issues and imprecisions into account. The obtained bounds are tight, although it was presumed that it is sufficient to solve the occurring key rate finding problem on a truncated space. Very recently, this so-called photon-number cutoff assumption was removed in [11].

Our contribution in this paper is the introduction of a new postselection scheme (cross-shaped postselection), that turns out to yield higher secure key rates than similar protocols with radial postselection, in particular for higher transmission distances and higher values of excess noise. Furthermore, it offers the opportunity to reduce the amount of raw key (i.e., data that has to be error-corrected) significantly, only at the cost of a much smaller decrease in the amount of secure key. Therefore, it turns out to be beneficial for practical implementations, as it reduces the computational demand for error-correction, which often is a bottle-neck in experiments.

We use the aforementioned numerical security proof method to investigate the influence of three different postselection strategies on the secure key rate of continuous-variable quantum key distribution protocols with quadrature phase-shift keying modulation. We show how the postselection strategies can be used to increase the secure key rate under collective attacks in the asymptotic limit, both for the untrusted-detector and trusted-detector scenario. Quadrature phase-shift keying (QPSK) protocols in quantum communication use four (coherent) states that differ only by their phase to encode two bits of information. Furthermore, we give analytical expressions for occurring operators in the Fock basis, making a computationally efficient calculation possible.

A. Organisation

The remainder of this work is structured as follows. First, we give a brief summary of the numerical security proof approach we used both for the trusted and untrusted detector scenario in Section IV. In Section V we introduce the present QPSK protocol and the examined postselection schemes. In Section VI we give analytical expressions necessary for the postprocessing and summarize the postprocessing procedure. In Section VII we compare our implementation to analytical calculations to validate our results. In Sections VI and VII we examine the introduced cross-shaped postselection scheme and compare it to the radial and radial-angular scheme both for the trusted (Section VI) and untrusted (Section VII) detector scenario. This is followed by a discussion and interpretation of the results. Detailed derivations are given in Appendix A and B and a table of symbols used in Appendix D.

Readers who are mainly interested in the implications of our theoretical work for QKD system implementations may skip Sections II, IV and V.
II. THE SECURITY PROOF APPROACH

In the whole paper, we use natural units, i.e., the quadrature operators are defined as
\[
\hat{q} := \frac{1}{\sqrt{2}} (\hat{a} + \hat{a}^\dagger), \\
\hat{p} := \frac{i}{\sqrt{2}} (\hat{a} - \hat{a}^\dagger),
\]
where \(\hat{a}\) and \(\hat{a}^\dagger\) are the bosonic ladder-operators and the commutation relation between the \(q\)- and \(p\)-quadrature operators has the form
\[
[\hat{q}, \hat{p}] = i.
\]

First, we give a brief overview of the numerical security proof approach, following [10] and [12]. The well-known Devetak-Winter formula [13] gives the secret key rate in the asymptotic limit. In the case of reverse reconciliation, it can be reformulated [10] in terms of the quantum relative entropy
\[
D(\rho||\sigma) := \text{Tr} [\rho \log_2 (\rho) - \log_2 (\sigma)],
\]
a quantity measuring the distinguishability of two states \(\rho\) and \(\sigma\), the sifting probability \(p_{\text{pass}}\), and the amount of information leakage per signal in the error-correction phase
\[
\delta_{\text{EC}}
\]
as follows
\[
R^\infty = \min_{\rho_{AB} \in \mathcal{S}} D(\mathcal{G}(\rho_{AB})||\mathcal{G}(\rho_{AB})) - p_{\text{pass}} \delta_{\text{EC}}. \tag{1}
\]
Hereby, \(\mathcal{G}\) is a completely positive, trace non-increasing map describing classical postprocessing steps, and \(\mathcal{Z}\) is a pinching quantum channel required to ‘read out’ the results of the key map. We note that \(p_{\text{pass}}\) is contained implicitly in the first term of the target function. A more detailed explanation is given in [12]. The set \(\mathcal{S}\) is the feasible set of the minimisation, which is a subset of the set of density operators \(\mathcal{D}(\mathcal{H}_{AB})\), where \(\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B\), and is defined by a set of linear constraints,
\[
\mathcal{S} := \{\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB}) \mid \forall i \in I : \text{Tr} [\Gamma_i \rho_{AB}] = \gamma_i\}, \tag{2}
\]
with Hermitian operators \(\Gamma_i\), real numbers \(\gamma_i\) and some finite set \(I\). In what follows, we denote the objective function of this minimisation by \(f\).

The physical interpretation of this minimisation problem is the following. We search for the optimal attack, i.e., the density matrix that minimises the achievable secret key rate, while still being compatible with experimental data, which influence the constraints. Using Lindblad’s theorem [14] and the linearity of \(\mathcal{G}\) and \(\mathcal{Z}\), it can be shown that we face a convex minimisation problem with linear and semi-definite constraints, hence a semi-definite program (SDP). The present problem requires optimisation over a subset of the set of all density operators, which is an infinite-dimensional vector space. In order to make the problem computationally feasible, we approximate it by a finite-dimensional vector space. While Bob’s infinite-dimensional state space is spanned by the basis of Fock-states \(\{\ket{n} : n \in \mathbb{N}\}\), following the photon-number cutoff assumption in [12], we approximate the infinite-dimensional state space by \(\mathcal{H}_B^N := \text{span}\{\ket{n} : 0 \leq n \leq N_c\}\), where \(N_c \in \mathbb{N}\) is the cutoff number.

In contrast to most of the minimisation problems, here it is not sufficient to come close to the minimum as this would give us only an upper bound on the secure key rate. Therefore, the approach in [10] tackles the key rate finding problem in a two-step process to prove security against collective attacks in the asymptotic limit. First, a numerical solving algorithm is applied to find an eavesdropping attack that is close to optimal. Then, in a second step, this upper bound of the secure key rate is converted into a lower bound, taking numerical imprecision into account.

A. Finding an almost optimal attack

In the first step, we have to find an attack that is close to optimal. The objective-function
\[
f(\rho) = D(\mathcal{G}(\rho)||\mathcal{G}(\rho))
\]
is non-linear. Therefore, we tackle the problem iteratively by approximating \(f\) to first order solving a linear semi-definite program. Since we face a constrained optimisation problem, we require an iterative algorithm that is guaranteed to stay in the feasible set, like the Frank-Wolfe algorithm [15] (alternatively, we may apply an algorithm that leaves the feasible set, combined with a projection that brings us back). The classical Frank-Wolfe algorithm can be expedited, if one adds a line-search towards the found optimal direction. The following algorithm is suggested in [10].

**Algorithm 1** Modified Frank-Wolfe for step 1

1: Choose \(\epsilon_{FW} > 0\), \(\rho_0 \in \mathcal{S}\) and set \(k = 0\)
2: Find \(\Delta \rho := \arg \min_{\Delta \rho} \text{Tr} \left[ (\Delta \rho)^\dagger \nabla f(\rho_k) \right] \) subject to \(\rho_k + \Delta \rho \in \mathcal{S}\)
3: STOP if \(\text{Tr} \left[ (\Delta \rho)^\dagger \nabla f(\rho_k) \right] < \epsilon_{FW}\)
4: Find \(\lambda \in (0, 1)\) that minimises \(f(\rho_k + \lambda \Delta \rho)\)
5: \(\rho_{k+1} := \rho_k + \lambda \Delta \rho, k \leftarrow k + 1,\) proceed with 2.

The optimisation problem can be brought into a more advantageous form. Following [10], we orthonormalize the (cutoff-representation of) observables \(\Gamma_i\) and obtain an orthonormal set \(\{\hat{\Gamma}_i : i \in I\}\), which we extend to an orthonormal basis \(\{\hat{\Gamma}_i : i \in I\} \cup \{\hat{\Omega}_j : j \in J\}\) of \(\mathcal{D}(\mathcal{H}_{AB}^{N_c})\) with respect to the Hilbert-Schmidt norm, where \(\mathcal{H}_{AB}^{N_c} := \mathcal{H}_A \otimes \mathcal{H}_B^{N_c}\) and \(J\) is another finite set. The expectation values of the \(i\)-th orthonormalised operator is denoted by \(\overline{\gamma}_i\). Then, the feasible set can be reformulated as
\[
\mathcal{S} = \left\{ \sum_{i \in I} \gamma_i \hat{\Gamma}_i + \sum_{j \in J} \omega_j \hat{\Omega}_j \mid \omega \in \mathbb{R}^{|J|} \right\}, \tag{3}
\]
where the first part represents the subspace, fixed by the constraints, and the second part represents the free subspace. Finally, the present minimisation problem (with objective function \( f \)) in every Frank-Wolfe step reads

\[
\omega^* = \arg \min_{\omega} \sum_{j \in J} \omega_j \text{Tr} \left[ \Omega_j \nabla f(\rho_i) \right]
\]

subject to \( \sum_{j \in J} \omega_j \Omega_j + \rho_i \in \mathcal{D}(\mathcal{H}_A^N \otimes \mathcal{H}_B^N) \),

and the next iterate can be obtained by

\[
\rho_{i+1} = \rho_i + \lambda \sum_{j \in J} \omega_j^* \Omega_j,
\]

where \( \lambda \in \{0, 1\} \) can be found by a line-search to speed-up the algorithm (or set to 1 otherwise). For \( \lambda = \frac{2}{\epsilon + \epsilon_j} \), it is known \cite{16} that the Frank-Wolfe algorithm with target function \( f \) satisfies \( f(\rho_k) - f(\rho^*) \leq O(\frac{1}{k}) \), where \( \rho^* \) is the optimal solution and \( \rho_k \) is the \( k \)-th iterate. As performing a line-search includes the case of \( \lambda = \frac{2}{\epsilon + \epsilon_j} \), the Frank-Wolfe algorithm combined with a line-search is known to converge at least at that rate. For our application, we observed that the Frank-Wolfe algorithm with additional line-search converges considerably faster.

B. Obtaining a tight lower bound on the key rate

The second step aims to convert the upper bound, obtained in step 1, into a lower bound. We only state the basic idea, following \cite{16}, where step 2 is justified in a sequence of three theorems.

The basic idea of step 2 is to convert every upper bound on the secure key rate for a feasible \( \rho \), obtained from step 1, into a lower bound on the secure key rate by linearisation and solving the dual problem of the occurring semi-definite program. Therefore, both step 1 and step 2 involve the evaluation of the gradient of \( f \), which might not exist for every \( \rho \) (e.g., if \( \mathcal{G} \) has not full rank). To address this issue, a perturbed map

\[
\mathcal{G}_\epsilon(\rho) := \mathcal{D}_\epsilon(\mathcal{G}(\rho))
\]

is introduced, where \( 0 < \epsilon < 1 \) and

\[
\mathcal{D}_\epsilon(\rho) := (1 - \epsilon)\rho + \epsilon \frac{1}{\dim(\mathcal{G}(\rho))} \mathbb{I}_{N_c}.
\]

Computational evaluations and differences between the exact constraints and their representation due to finite precision can introduce little numerical errors in the secure key rate calculations and therefore have to be taken into account for a reliable security proof. Let us denote the computer representation of variables with tildes, for example, \( \tilde{\Gamma}_i \) is the representation of \( \Gamma_i \). It is shown in \cite{16} that if the constraints are satisfied up to some small number \( \epsilon' \in \mathbb{R}, \forall i \in I : \left| \text{Tr} \left[ \tilde{\Gamma}_i \rho - \tilde{\gamma}_i \right] \right| \leq \epsilon' \), the following statement holds.

Theorem:

Let \( \rho \in \mathcal{D}(\mathcal{H}_A^N \otimes \mathcal{H}_B^N) : \left| \text{Tr} \left[ \tilde{\Gamma}_i \rho - \tilde{\gamma}_i \right] \right| \leq \epsilon' \) where \( \epsilon' > 0 \) and \( 0 < \epsilon \leq \frac{1}{\epsilon_j} \). Then

\[
\min_{\rho \in \mathcal{S}} f(\rho) \geq \beta_{\epsilon'(\epsilon)}(\sigma) - \zeta
\]

where \( \zeta := 2\epsilon(\dim(\mathcal{G}(\rho)) - 1) \log \left( \frac{\dim(\mathcal{G}(\rho))}{\epsilon} \right) \) and

\[
\beta_{\epsilon'(\epsilon)}(\sigma) := f_\sigma(\sigma) - \text{Tr} \left[ \sigma^T \nabla f_\sigma(\sigma) \right] + \max \left\{ \bar{y}, \bar{z} \in \tilde{\mathcal{S}}_{\epsilon'}(\rho) : \tilde{\zeta} \cdot \bar{y} - \epsilon \sum_{i=1}^{[J]} y_i \tilde{\Gamma}_i \leq \nabla f_\sigma(\sigma) \right\}.
\]

The set \( \tilde{\mathcal{S}}_{\epsilon'}(\rho) \) is given by

\[
\tilde{\mathcal{S}}_{\epsilon'}(\rho) := \left\{ (\bar{y}, \bar{z}) \in (\mathbb{R}^{[J]} \otimes \mathbb{R}^{[J]} ) \left| - \bar{z} \leq \bar{y} \leq \bar{z}, \sum_{i=1}^{[J]} y_i \tilde{\Gamma}_i \leq \nabla f_\sigma(\sigma) \right. \}.
\]

C. Specifying the optimisation problem

Next, we have to find the relevant optimisation problem, i.e., we need to specify \( \Gamma \), as well as the right-hand sides \( \gamma_i \) to formulate the constraints, and the postprocessing map \( \mathcal{G} \) as well as the pinching channel \( \mathcal{Z} \).

In this work, we follow the (postprocessing-)framework of \cite{12} and the indices \( A, B, \) and \( R \) label Alice’s and Bob’s system and a classical register, respectively. Therefore, the occurring postprocessing map \( \mathcal{G}(\sigma) := K \sigma K^\dagger \) is defined by the Kraus operator

\[
K := \sum_{z=0}^{3} |z\rangle_R \otimes I_A \otimes \left( \sqrt{R_z} \right)_{B},
\]

where \( (R_z)_{z \in \{0,1,2,3\}} \) are the so-called region operators, whose form depends on the actual key map (they will be specified in Section III). If \( E_y \) denotes the POVM of Bob’s measurements, they are given by

\[
R_z := \int_{A_z} E_y \, d^2 y,
\]

where \( A_z \) is the set corresponding to the symbol \( z \) in the key map (see Section III). For ideal homodyne measurements the corresponding POVM \( \mathcal{E} \) is given by \( E_y = \frac{1}{2} |y \rangle \langle y | \).

Furthermore, the pinching channel \( \mathcal{Z} \) is given by

\[
\mathcal{Z}(\sigma) := \sum_{j=0}^{3} \langle j | \langle j | R \otimes I_{AB} \rangle \sigma \langle j | \langle j | R \otimes I_{AB} \rangle.
\]
Hence, we’ve completely specified the objective function $f(p)$.

To start the key generation process, Alice prepares states $|\psi_x\rangle$ with probability $p_x$ and sends them to Bob, using the quantum channel. Thanks to the source-replacement scheme \[15\] one can consider the corresponding formulation in the entanglement-based scheme, where Alice prepares the bipartite state $|\Psi\rangle_{AA'} = \sum_x \sqrt{p_x} |x\rangle_A |\psi_x\rangle_{A'}$. $A$ denotes the register that is kept by Alice and the state labelled with $A'$ is sent to Bob. The quantum channel is modelled as a completely positive trace preserving map $\mathcal{E}_{A'\rightarrow B}$. Hence, the bipartite state shared by Alice and Bob reads $\rho_{AB} = (1_A \otimes \mathcal{E}_{A'\rightarrow B}) (|\Psi\rangle_{AA'} \langle \Psi|_{AA'})$.

Bob performs heterodyne measurement, hence determines the first- and second moments of $\hat{q}$ and $\hat{p}$. These observations can be calculated to use the mean photon number $\bar{n} = \frac{1}{2} (\hat{q}^2 + \hat{p}^2 - 1)$ and $\bar{d} = \hat{q}^2 - \hat{p}^2$ to constrain the density matrix $\rho_{AB}$. Furthermore, we know that Eve has no access to Alice’s system hence she cannot modify the states held by Alice. That can be expressed mathematically as $\text{Tr}_B [\rho_{AB}] = \sum_{x,y=0}^1 \sqrt{p_x p_y} \langle \psi_y|\psi_x\rangle |x\rangle\langle y|_A$, which is a matrix-valued constraint. Here $p_x$ is the probability that the state $|\psi_x\rangle$ is prepared, $x \in \{0,1,2,3\}$. Therefore, we find the following semi-definite program \[12\]

$$\begin{align*}
\text{minimise} & \quad D(G(\rho_{AB}))|G(Z(\rho_{AB}))| \\
\text{subject to:} & \\
\text{Tr} [\rho_{AB} (|x\rangle\langle x|_A \otimes \hat{q})] & = p_x \langle \hat{q} \rangle_x \\
\text{Tr} [\rho_{AB} (|x\rangle\langle x|_A \otimes \hat{p})] & = p_x \langle \hat{p} \rangle_x \\
\text{Tr} [\rho_{AB} (|x\rangle\langle x|_A \otimes \bar{n})] & = p_x \langle \bar{n} \rangle_x \\
\text{Tr} [\rho_{AB} (|x\rangle\langle x|_A \otimes \bar{d})] & = p_x \langle \bar{d} \rangle_x \\
\text{Tr}_B [\rho_{AB}] & = \sum_{i,j=0}^3 \sqrt{p_i p_j} \langle \psi_j|\psi_i\rangle |i\rangle\langle j|_A \\
\rho_{AB} & \geq 0,
\end{align*}$$

where $x \in \{0,1,2,3\}$. Note that, in contrast to \[12\], we do not add the constraint $\text{Tr}[\rho_{AB}] = 1$. That is because we transform the matrix-valued constraint by quantum state tomography (see, e.g., \[20\]) into 16 scalar-valued constraints. Thereby, the basis of Alice’s system is chosen in a way such that the set of 32 constraints (16 from the measurements, 16 from the state-tomography) is sufficient to linear-combine the trace-equal-to-one condition with sufficient numerical accuracy without requiring this condition explicitly. For numerical reasons, it is beneficial to avoid (almost) linearly-dependent conditions in our set of constraints.

If we model the quantum channel as a phase-invariant Gaussian channel with transmittance $\eta$ and excess noise $\xi$, which is a common model for optical fibres, the right-hand sides of the constraints can be found similarly to \[12\], where the expectation values are calculated using Husimi-Q-functions. The rotation in the phase space that transforms the arrangement of the states on the axes to our ‘QPSK-like’ constellation does not lead to significant changes in that approach. We measure the excess noise in multiples of the shot noise. The expectation values read

$$\begin{align*}
\langle \hat{q} \rangle_x & = \sqrt{2\eta} \Re(\alpha_x), \\
\langle \hat{p} \rangle_x & = \sqrt{2\eta} \Im(\alpha_x), \\
\langle \bar{n} \rangle_x & = \eta |\alpha_x|^2 + \frac{\eta \xi}{2}, \\
\langle \bar{d} \rangle_x & = \eta (\alpha_x^2 + (\alpha_x^*)^2),
\end{align*}$$

for $x \in \{0,1,2,3\}$, where $\alpha_x$ is a complex number associated with the coherent state Alice prepares. Note that $\bar{n}$ and $\bar{d}$ are related to the second-moment observables $\hat{q}^2$ and $\hat{p}^2$. Therefore, one may replace the constraints for $\langle \bar{n} \rangle_x$ and $\langle \bar{d} \rangle_x$ by expressions for $\langle \hat{q}^2 \rangle_x$ and $\langle \hat{p}^2 \rangle_x$.

D. Trusted detector approach

Up to now, we have assumed to perform measurements with a perfect heterodyne detector. In the most conservative scenario, all deviations of realistic devices from that perfect detector are dedicated to Eve. However, as the detector is located in Bob’s lab, one may assume the detector as trusted, supposing that Eve cannot control or use detector losses and electronic noise. In \[21\], the numerical security proof method is extended to this “trusted” detector scenario. We give a brief summary of the adaptations introduced there. A (non-ideal) heterodyne detector is made out
of two homodyne detectors and a beam splitter, where each of the homodyne detectors has non-unity detector efficiency \( \eta_1, \eta_2 \) and suffers from electronic noise \( \nu_1, \nu_2 \). Similar to the excess noise, the electronic noise is measured in shot noise units. The quantum optical model by Lodewyck \cite{22} includes these quantities in the following way (see Figure 1). After the input signal is split into two parts at a 50 : 50 beamsplitter (where it is mixed with the vacuum-state) each part of the signal passes another beamsplitter with transmissions \( \eta_1 \) and \( \eta_2 \) (hence reflectances of \( 1 - \eta_1 \) and \( 1 - \eta_2 \)), respectively. There, we mix each part of the splitted signal with a thermal state with mean photon number \( \bar{n}_i = \frac{\nu_i}{2(1-\eta_i)} \), \( i \in \{1, 2\} \) we relate each thermal state to the corresponding amount of electronic noise introduced by the corresponding detector. Analogue to \cite{21}, we choose \( \eta_1 = \eta_2 =: \eta_d \) and \( \nu_1 = \nu_2 =: \nu_d \) for simplicity. Although we do not expect to hold two identical detectors in real world applications, one may choose \( \eta_d \) to be the minimum efficiency of both detectors and \( \nu_d \) to be the maximum of the measured electronic noises. Then, the obtained secure key rates are still a valid lower bound in the trusted-noise scenario for that system.

As we do not deal with ideal detectors any more, we have to replace \( E_y \) in equation (13) by a POVM corresponding to the aforementioned detector model. In \cite{21}, the following POVM elements

\[
G_y = \frac{1}{\eta_d \bar{n}} \hat{D} \left( \frac{y}{\sqrt{\eta_d}} \right) \rho_{th} \left( \frac{1 - \eta_d + \nu_d}{\eta_d} \right) \hat{D} ^{\dagger} \left( \frac{y}{\sqrt{\eta_d}} \right)
\]

have been derived, where \( \hat{D} \) is the displacement operator and \( \rho_{th}(\bar{n}) \) is a thermal state with mean photon number \( \bar{n} \). That POVM is used to define first- and second-moment observables

\[
\hat{F}_Q = \int \frac{y^* + y}{\sqrt{2}} G_y d^2 y, \quad (21)
\]
\[
\hat{F}_P = \int \frac{y^* - y}{\sqrt{2}} G_y d^2 y, \quad (22)
\]
\[
\hat{S}_Q = \int \left( \frac{y^* + y}{\sqrt{2}} \right)^2 G_y d^2 y, \quad (23)
\]
\[
\hat{S}_P = \int \left( \frac{y^* - y}{\sqrt{2}} \right)^2 G_y d^2 y \quad (24)
\]

with expectation values

\[
\langle \hat{F}_Q \rangle_x = \sqrt{2\eta_d} \eta \Re(\alpha_x), \quad (25)
\]
\[
\langle \hat{F}_P \rangle_x = \sqrt{2\eta_d} \eta \Im(\alpha_x), \quad (26)
\]
\[
\langle \hat{S}_Q \rangle_x = 2\eta_d (\Re(\alpha_x))^2 + 1 + \frac{1}{2}\eta \eta \xi + \nu_d, \quad (27)
\]
\[
\langle \hat{S}_P \rangle_x = 2\eta_d (\Im(\alpha_x))^2 + 1 + \frac{1}{2}\eta \eta \xi + \nu_d. \quad (28)
\]

Hence, for the trusted detector model, we face a slightly modified problem, where changes occur in the constraints due to measurements and the objective function (as the map \( \mathcal{G} \) depends on the region operators, hence on the POVM). For details regarding the trusted detector approach, we redirect the reader to \cite{21}.

\section{Examined Protocols}

In what follows, we introduce the protocols that we are going to examine in the upcoming sections. All three are prepare-and-measure (P&M) QPSK protocols of the same type as ‘Protocol 2’ in \cite{12}, and for the sake of uniformity, we will stick close to the notation of \cite{12}. In contrast to that work, we rotated the signal-states by \( \pi/4 \) in the \( p-q \)-plane such that they are not located on the axes but on the diagonals. This is in accordance with the constellation of the signal states in classical QPSK-schemes. In this work, we examine the effect of different postselection strategies on the key-rate. So, the main difference between the examined protocols will occur in 4) of the following description.

We consider two distant parties, the sender Alice and the receiver Bob, who want to establish secure communication. They are connected by an authenticated clas-
sical channel and a quantum channel. Eve, an adversary, can listen to the classical communication and listen and manipulate signals that are exchanged via the quantum channel. Although we deal with a prepare-and-measure scheme, the source replacement scheme allows us to switch between P&M and entanglement-based schemes, as neither Bob nor Eve can distinguish which scheme Alice used. So, if Alice prepares states $|\psi_\alpha\rangle$ with probability $p_\alpha$, the corresponding formulation in the entanglement-based scheme would be $|\Psi\rangle_{AA'} = \sum_{\alpha} \sqrt{p_\alpha} |\alpha\rangle_A |\psi_\alpha\rangle_{A'A'}$. A denotes the register that is kept by Alice and the state labelled with $A'$ is sent to Bob. Let $N \in \mathbb{N}$ be the raw key block size.

1) For every $k \leq N$ Alice prepares one out of four coherent states $|\psi_\alpha\rangle \in \{|\alpha|e^{i\frac{\pi}{4}}\rangle, |\alpha|e^{i\frac{3\pi}{4}}\rangle, |\alpha|e^{i\frac{5\pi}{4}}\rangle, |\alpha|e^{i\frac{7\pi}{4}}\rangle\}$, where $|\alpha| > 0$ (arbitrary but fixed) is the coherent state amplitude, according to some probability distribution. In the easiest case, this can be a uniform distribution. The first state $|\alpha|e^{i\frac{\pi}{4}}\rangle$ is associated with the symbol $x_k = 0$, the second one with the symbol $x_k = 1$, and so on. This phase is called state preparation. After preparing one of these states, Alice sends it to Bob using the quantum channel.

2) Once the state is transmitted to Bob, he performs heterodyne measurement and obtains some complex number $y_k$. That is called the measurement phase.

3) Next, Alice and Bob agree via the classical channel to choose some random subset $I_{\text{est}} \subset \{n \in \mathbb{N} : n \leq N\}$ and reveal the corresponding sent symbols $x_l$ and measurement results $y_l$ for $l \in I_{\text{key}}$ to perform parameter estimation, i.e., they determine the amount of information Eve might have gained about the key. The remaining rounds $I_{\text{key}} := \{n \in \mathbb{N} : n \leq N\} \setminus I_{\text{est}}$ will be used for key generation. For simplicity, assume that $I_{\text{key}}$ contains the first $m := |I_{\text{key}}|$ rounds that can be used for key-generation (this can be assumed without loss of generality, as we always find some bijective map that reorders the set). After this step, Alice holds a key string $X := (x_1, \ldots, x_m)$.

4) Now we apply a keymap to obtain Bob’s key string $Z = (z_j)_{j \in I_{\text{key}}}$, where Bob’s measurement outcomes $y_l$ for rounds $l \in I_{\text{key}}$ are assigned to some element in the set $\{0, 1, 2, 3, \perp\}$. The keymap differs, depending on the chosen postselection strategy. The areas, associated with the symbols in Figures (radial&angular) and (cPS) read

a) Radial Postselection (rPS) Fix some $0 \leq \Delta_r \in \mathbb{R}$ and determine Bob’s key string according to the following rule (see Figure 3).

$$z_j = \begin{cases} 0 & \text{if } \arg(y_j) \in \left[0, \frac{\pi}{2}\right) \land |y_j| \geq \Delta_r, \\ 1 & \text{if } \arg(y_j) \in \left[\frac{\pi}{2}, \pi\right) \land |y_j| \geq \Delta_r, \\ 2 & \text{if } \arg(y_j) \in \left[\pi, \frac{3\pi}{2}\right) \land |y_j| \geq \Delta_r, \\ 3 & \text{if } \arg(y_j) \in \left[\frac{3\pi}{2}, 2\pi\right) \land |y_j| \geq \Delta_r, \\ \perp & \text{otherwise.} \end{cases}$$

(29)

b) Radial&angular Postselection (raPS) Fix some $0 \leq \Delta_r \in \mathbb{R}$ and $0 \leq \Delta_\alpha \in \mathbb{R}$ and determine Bob’s key string according to the following rule (see Figure 3).

$$z_j = \begin{cases} 0 & \text{if } \arg(y_j) \in \left[\Delta_r, \frac{\pi}{2} - \Delta_\alpha\right) \land |y_j| \geq \Delta_r, \\ 1 & \text{if } \arg(y_j) \in \left[\frac{\pi}{2} - \Delta_\alpha, \pi - \Delta_\alpha\right) \land |y_j| \geq \Delta_r, \\ 2 & \text{if } \arg(y_j) \in \left[\pi - \Delta_\alpha, \frac{3\pi}{2} - \Delta_\alpha\right) \land |y_j| \geq \Delta_r, \\ 3 & \text{if } \arg(y_j) \in \left[\frac{3\pi}{2} - \Delta_\alpha, 2\pi - \Delta_\alpha\right) \land |y_j| \geq \Delta_r, \\ \perp & \text{otherwise.} \end{cases}$$

(30)

c) Cross-shaped Postselection (cPS) Fix some $0 \leq \Delta_\alpha \in \mathbb{R}$ and determine Bob’s key string according to the following rule (see Figure 4).

$$z_j = \begin{cases} 0 & \text{if } \Re(y_j) \geq \Delta_\alpha \land \Im(y_j) \geq \Delta_\alpha, \\ 1 & \text{if } \Re(y_j) \leq -\Delta_\alpha \land \Im(y_j) \geq \Delta_\alpha, \\ 2 & \text{if } \Re(y_j) \leq -\Delta_\alpha \land \Im(y_j) \leq -\Delta_\alpha, \\ 3 & \text{if } \Re(y_j) \geq -\Delta_\alpha \land \Im(y_j) \leq -\Delta_\alpha, \\ \perp & \text{otherwise.} \end{cases}$$

(31)
error correction. For example, Bob may transmit information about his bit-string and Alice corrects her share according to his instructions, which is called reverse reconciliation (since the information flow is contrariwise to the sent quantum signals). The used error correction routine cannot be expected to work perfectly, but with an efficiency of $0 < \beta < 1$. After finishing the error-correction, Alice and Bob use almost universal hash-functions to can upper-bound the probability that the error correction phase has failed. They omit the key if the hash-values do not coincide and restart the key generation process.

(6) Finally, Alice and Bob apply privacy amplification algorithms to reduce Eve’s knowledge about their shared key by omitting parts of their shared key, for example, by using seeded randomness extractor algorithms.

Note that all three postselection strategies coincide for $\Delta_r = \Delta_c = \Delta_\gamma = 0$, which is the case without any postselection, and that rPS is a special case of raPS for $\Delta_a = 0$. In [12, 21] the radial postselection parameter is called $\Delta_a$ and the angular postselection parameter is called $\Delta_\gamma$. However, to use indices that are directly related to the name of the corresponding postselection strategy and to avoid confusions, we choose different names.

IV. FORMALISATION OF THE POSTPROCESSING STEPS

A. Partitioning of the phase-space

According to the definition of the postselection maps in Section [III] we define the following subsets of the phase-space ($\mathbb{C}$):

$$
A_{0}^a := \{ z \in \mathbb{C} : \text{arg}(z) \in \left[\frac{\pi}{2} - \Delta_a, \frac{\pi}{2} - \Delta_a\right] \land |z| \geq \Delta_r \},
$$

$$
A_{1}^a := \{ z \in \mathbb{C} : \text{arg}(z) \in \left[\frac{\pi}{2} + \Delta_a, \pi - \Delta_a\right] \land |z| \geq \Delta_r \},
$$

$$
A_{2}^a := \{ z \in \mathbb{C} : \text{arg}(z) \in \left[\pi + \Delta_a, \frac{3\pi}{2} - \Delta_a\right] \land |z| \geq \Delta_r \},
$$

$$
A_{3}^a := \{ z \in \mathbb{C} : \text{arg}(z) \in \left[\frac{3\pi}{2} + \Delta_a, 2\pi - \Delta_a\right] \land |z| \geq \Delta_r \},
$$

and

$$
A_{0}^c := \{ z \in \mathbb{C} : \Re(z) \geq \Delta_c \land \Im(z) \geq \Delta_c \},
$$

$$
A_{1}^c := \{ z \in \mathbb{C} : \Re(z) \leq -\Delta_c \land \Im(z) \geq \Delta_c \},
$$

$$
A_{2}^c := \{ z \in \mathbb{C} : \Re(z) \leq -\Delta_c \land \Im(z) \leq -\Delta_c \},
$$

$$
A_{3}^c := \{ z \in \mathbb{C} : \Re(z) \geq \Delta_c \land \Im(z) \leq -\Delta_c \}. \tag{33}
$$

Here, the superscript labels the chosen postselection strategy, and the subscript labels the symbol we associate with the defined set. Note that the radial postselection-scenario is included in the radial/circular case by setting $\Delta_a = 0$, so we do not need to define separate sets for the radial scheme.

B. Region operators for the untrusted detector

We start with the untrusted detector scenario. As Bob performs heterodyne measurement of the incident quantum states, the POVM of an ideal, untrusted homodyne detector has the form $\{E_\gamma = \frac{1}{\pi} |\gamma\rangle\langle\gamma| : \gamma \in \mathbb{C}\}$. Then, the measurement operators, called region operators, corresponding to the symbol $z = k$, $k \in \{0, 1, 2, 3\}$, are defined by

$$
R_1^a := \int_{A_1^a} E_\gamma d^2 \gamma = \frac{1}{\pi} \int_{A_1^a} |\gamma\rangle\langle\gamma| d^2 \gamma \tag{34}
$$

$$
R_2^c := \int_{A_2^c} E_\gamma d^2 \gamma = \frac{1}{\pi} \int_{A_2^c} |\gamma\rangle\langle\gamma| d^2 \gamma. \tag{35}
$$

As we approximate later on the infinite-dimensional problem by a problem living in a finite-dimensional Fock-space, we express the region operators in the number
basis,

\[ R_{\text{za}}^{a} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n|R_{\text{za}}^{a}|m\rangle\langle m| \]  \hspace{1cm} \text{(36)}

Then, once it comes to numerical treatment, we may replace the upper limit in the occurring sums by the cutoff number \(N_\varepsilon\) (see Section II). It remains to find expressions for the matrix elements \(\langle n|R_{\text{za}}^{a}|m\rangle\) in (36) and \(\langle n|R_{\text{z}}^{c}|m\rangle\) in (37). We show in Appendix A that they can be calculated analytically and have the form

\[ \langle n|R_{\text{za}}^{a}|m\rangle = \begin{cases} \frac{\Gamma(n+1,\Delta_c^2)}{\pi(n!)} (\frac{z}{4} - \Delta_a) & n = m \\ \frac{\Gamma(m+n+1,\Delta_c^2)}{\pi(m-n)!n!\sqrt{m!}} e^{-i(m-n)(z+\frac{1}{2})} \sin \left( (\frac{z}{4} - \Delta_a) (m-n) \right) & n \neq m \end{cases} \]  \hspace{1cm} \text{(38)}

\[ \langle n|R_{\text{z}}^{c}|m\rangle = \begin{cases} \frac{1}{4\pi(n!)} \sum_{j=0}^{n} \binom{n}{j} \Gamma(j+\frac{1}{2},\Delta_c^2) \Gamma(n-j+\frac{1}{2},\Delta_c^2) & n = m \\ \frac{1}{4\pi\sqrt{m!}\sqrt{m}} \sum_{j=0}^{m} \sum_{k=0}^{m} \binom{n}{j} \binom{m}{k} \Gamma(\frac{j+k+1}{2},\Delta_c^2) \Gamma(\frac{n+m-j-k+1}{2},\Delta_c^2) D^{(z)}_{j,k,m,n} & n \neq m \end{cases} \]  \hspace{1cm} \text{(39)}

where

\[ D^{(z)}_{j,k,m,n} = i^{n-m+k-j} \cdot \begin{cases} 1 & z = 0 \\ (-1)^{k-j} & z = 1 \\ (-1)^{n-m} & z = 2 \\ (-1)^{n-m+k-j} & z = 3 \end{cases} \]  \hspace{1cm} \text{(40)}

These results are consistent with the numerical solutions of the occurring integrals with MATLAB\textsuperscript{\textsuperscript{TM}}, version R2020a, and additionally have been cross-checked with Wolfram Mathematica\textsuperscript{\textsuperscript{TM}}, version 11.1.1.

\section*{C. Region operators for the trusted detector}

Similarly, for the POVM corresponding to the trusted detector from Eq. (20), we need to express the region operators

\[ R_{\text{za}}^{a,\text{tr}} := \int_{A_{\text{za}}} G_\gamma d^2\gamma, \]  \hspace{1cm} \text{(41)}

\[ R_{\text{z}}^{c,\text{tr}} := \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n|R_{\text{z}}^{c,\text{tr}}|m\rangle\langle m| \]  \hspace{1cm} \text{(42)}

\[ R_{\text{z}}^{c,\text{tr}} := \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n|R_{\text{z}}^{c,\text{tr}}|m\rangle\langle m| \]  \hspace{1cm} \text{(43)}

\[ R_{\text{z}}^{c,\text{tr}} := \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n|R_{\text{z}}^{c,\text{tr}}|m\rangle\langle m| \]  \hspace{1cm} \text{(44)}

\[ \langle n|R_{\text{z}}^{c,\text{tr}}|m\rangle = \begin{cases} C_{n,n} (\frac{z}{4} - \Delta_a) \sum_{j=0}^{n} \binom{n}{j} \frac{\Gamma(j+1,\alpha\Delta_c^2)}{\alpha^{j+1}b^{j+1}} & n = m \\ \frac{C_{n,n}}{(m-n)!} e^{-i(m-n)(z+\frac{1}{2})} \sin \left( (\frac{z}{4} - \Delta_a) \sum_{j=0}^{n} \binom{n}{j} \frac{\Gamma(j+1,\alpha\Delta_c^2)}{\alpha^{j+1}b^{j+1}} \right) & n < m \\ \langle m|R_{\text{z}}^{c,\text{tr}}|n\rangle & n > m \end{cases} \]  \hspace{1cm} \text{(45)}

We show in Appendix B that the coefficients for the trusted noise scenario have the form
\[ \langle n | R_z^{-1} | m \rangle = \left\{ \begin{array}{ll}
C_{n,m} \sum_{j=0}^{n} \binom{n}{j} a^{j} b^{n-j} \sum_{k=0}^{j} \binom{j}{k} (j + \frac{1}{2}, a \Delta_z^2 \Gamma) (j - k + \frac{1}{2}, a \Delta_z^2 \Gamma) & n = m \\
\frac{C_{n,m}}{4a^{n-m}} \sum_{j=0}^{n} \binom{n}{m-j} \frac{1}{a^{j} b^{m-j}} \sum_{k=0}^{m-n} \binom{m-n}{k} D_{k,m,n} \sum_{l=0}^{j} \binom{j}{l} (l + \frac{k+1}{2}, a \Delta_z^2 \Gamma) (j - l + \frac{m-n-k+1}{2}, a \Delta_z^2 \Gamma) & n < m \\
& n > m
\end{array} \right. \]

where \( C_{n,m} := \frac{1}{\pi \alpha^{n-m+1}} \sqrt{\frac{n!}{m! (1 + \pi z)^{n-m+\alpha}}} \), \( a := \frac{1}{\pi \alpha (1 + \pi z)} \), and \( b := \eta_d \pi d (1 + \pi d) \) and

\[ D_{k,m,n}^{(z)} = i^{m-n-k}, \left\{ \begin{array}{ll}
(-1)^{m-n-k} & z = 0 \\
(-1)^{m-n} & z = 1 \\
(-1)^{k} & z = 2 \\
1 & z = 3
\end{array} \right. \] (47)

We note that \([21]\) derives an expression for non-rotated signal states (i.e., signal states lying on the axis) for the case with only radial postselection, relying on Taylor\&angular series expansion. In contrast, our result for the radial\&angular-case is more general, as it additionally includes angular postselection. Furthermore, we give a direct expression that does not require Taylor series coefficients. To the best of our knowledge, our result for the cross-shaped postselection scheme is novel. Again, both results have been validated with numerical solutions of the occurring integrals with MATLAB\textsuperscript{TM}, version R2020a.

Furthermore, for the sake of completeness, we give analytical expressions for the Fock-basis representation of the first- and second-moment observables \( F_Q, F_P, S_Q, S_P \) in Appendix B3.

We note that the usage of the analytical expressions instead of numerical solutions of the integrals is highly recommendable, as (1) the time saving even for small systems is formidable and (2) the numerical precision is higher.

**D. Information-leakage during reconciliation**

By construction, we find the probability that Bob obtains the symbol \( x = l \) conditioned that Alice has prepared the state \( x = k \) by

\[ P(z = k | x = l) = \text{Tr} \left( \rho_B R_k \right), \] (48)

where

\[ \rho_B^{j} = \frac{1}{p_l} \text{Tr}_A [\rho_{AB} (l | l)_A \otimes 1_B] \] (49)

and \( R_k \) denotes one of the region operators introduced in the subsequent sections. By knowing this and taking the error correction efficiency into account, we can calculate the information-leakage during reconciliation per signal \( \delta_{EC} \) and the probability that a signal passes the postselection phase \( p_{pass} \). Since Bob does not transmit the amplitudes of the measured quadrature values to Alice and errors in each of the bits are independent (see comment below Figure 2), the channel between Alice and Bob is a binary symmetric channel (BSC) (see, for example, \([23]\)). If we were able to perform information reconciliation at the Slepian-Wolf limit \([24]\) \( \delta_{EC} = H(Z|X) = H(Z) - I(X : Z) \) would hold, where \( H(Z) \) is the von-Neumann entropy of the string \( Z \), \( H(Z|X) \) is the conditioned von-Neumann entropy, and \( I(X : Z) \) denotes the mutual information between the strings \( Z \) and \( X \).

As we assume to perform error correction with efficiency \( \beta < 1 \) (depending on the error correction procedure), we replace the mutual information between \( Z \) and \( X \) by \( \beta I(X : Z) \) and then rewrite the expression in terms of entropies again. Therefore, we obtain

\[ \delta_{EC} = H(Z) - \beta (H(Z) - H(Z|X)) = (1 - \beta) H(Z) + \beta H(Z|X), \] (50)

The entropies can be calculated using the probabilities given in equation (48) and the total of law probability.

Furthermore, we obtain the probability that a signal passes the postselection phase by

\[ p_{pass} = \sum_{l=0}^{3} \sum_{k=0}^{3} p_l P(z = k | x = l), \] (51)

where \( p_l \) denotes the probability that Alice prepares the state corresponding to the symbol \( l \) (which is given in the protocol description; for symmetry reasons, we choose \( \forall l \in \{0, 1, 2, 3\} \ p_l = \frac{1}{4} \)).

**V. IMPLEMENTATION AND VALIDATION OF THE METHOD**

In this section, we are going to elaborate on the details and parameters of our implementation and compare our numerical secure key rates with secure key rates for special cases, where analytical solutions are available.
A. Implementation

The coding of the numerical method explained in Section 11 was carried out in MATLAB®R2020a, and we used CVX [25, 26] to model the linear semi-definite programs that appear in Step 1 and Step 2 and employed the MOSEK solver [27] as well as SDPT3 [28, 29] to dispense the SDP optimisation tasks. It turned out that the line search at the end of every (modified) Frank-Wolfe step,

\[
\text{minimize}_{\epsilon \in [0,1]} \ f(\rho_0 + t\Delta \rho),
\]

can be solved efficiently by bisection.

We found an initial value required to start the Frank-Wolfe algorithm in two different ways. The first method utilizes the SDP solver, where we formulate the problem exactly like in equation [15] but replace the target function by \( f(\rho) = 1 \). Then, the SDP solver returns a density matrix that satisfies all constraints, hence is lying in the feasible set \( \mathcal{S} \). The second method uses a model for two-mode Gaussian Channel (see [30]) with excess noise \( \xi \) and transmittance \( \eta \) to calculate a density matrix on Bob’s side, given Alice’s density matrix. The first method is faster, in particular for systems with cutoff numbers \( N_c \) and larger. On the other hand, the second method is numerically more stable and yields density matrices with only positive eigenvalues, even for very ‘exotic’ parameter regimes (e.g., very low \( \xi \), very high \( L \)), where solver imprecisions cause slightly negative eigenvalues for the first method.

In the rest of this work, we choose the sampling distribution to be the uniform distribution, i.e., \( \forall j \in \{0, 1, 2, 3\} : p_j = \frac{1}{4} \). If not mentioned otherwise, we used the cutoff number \( N_c = 12 \), which turned out to be an ideal compromise between accuracy and computation speed for most of the reasonable parameter-inputs. A more detailed discussion of that choice can be found in Appendix C. Therefore, all infinite-dimensional operators and quantities are replaced by their finite-dimensional representations in Fock-spaces of size \( N_c \). For example, the upper limit of the sum appearing in the Fock-representation of the region operators is replaced by \( N_c \). Furthermore, if not mentioned otherwise, we apply the following maximum numbers of Frank-Wolfe steps, \( N_{FW} = 30 \) if \( \xi = 0.01 \) and \( N_{FW} = 150 \) if \( \xi = 0.02 \). This values were chosen empirically, as it turned out that the obtained key rates do not change significantly for higher values of \( N_{FW} \). We chose the threshold for the Frank-Wolfe algorithm \( \epsilon_{FW} = 10^{-7} \) and the perturbation \( \tilde{\epsilon} = 10^{-11} \).

In this work, we performed all calculations with the following model for the transmittance, \( \eta = 10^{-0.02L} \). That is a transmittance of -0.2 dB or about 95.5% per kilometer, which is realistic for practical implementations. Recall, that both the excess noise \( \xi \) and the electronic noise \( \nu_e \) are measured in shot noise units. If not mentioned otherwise, we work with a reconciliation efficiency of \( \beta = 0.95 \). As a side note we mention that low-density parity-check (LDPC) codes with an efficiency of 0.95 for the binary symmetric channel are available for all relevant values of the error rate.

B. Validation for the noiseless channel

Next, we apply our numerical implementation to the noiseless channel, where the secure key rates can be calculated analytically. We generalised the analytical approach from [31] to four-state protocols with states apart from the axis. It is shown there that in the noiseless case, it is sufficient to consider the generalised beam-splitter attack, i.e., if Alice sends a coherent state with amplitude \( |\alpha| \), Bob receives a coherent state with amplitude \( \sqrt{\eta}|\alpha| \), while Eve holds another coherent state with amplitude \( \sqrt{1-\eta}|\alpha| \).

1. Optimal coherent state amplitude

Figure 5 illustrates the dependency of the (numerically calculated) secure key rate on \( |\alpha| \) for fixed transmission lengths of \( L = 20km \), \( L = 50km \), \( L = 70km \) and \( L = 100km \) in the absence of noise. For numerical reasons, we chose \( \xi = 10^{-5} \) instead of \( \xi = 0 \) and chose the photon-cutoff number \( N_c = 12 \). For example, higher values of \( N_c \) are required for larger values of the coherent state amplitude, as states with higher values of \( |\alpha| \) have a higher displacement from the origin of the state space.
Hence, it requires more number states to describe the corresponding coherent states properly. For the numerical search, we chose a step size of $\Delta_{|\alpha|} = 0.05$.

The maximal secure key rates for the curve for 20km can be found at $|\alpha| = 0.86$, the maximal secure key rate for $L = 50$km lies at $|\alpha| = 0.72$ and the maximal secure key rate for $L = 70$km and $L = 100$km are found at $|\alpha| = 0.70$. This matches the theoretical prediction by the aforementioned generalized model, as can be seen in Figure 6 which displays the (analytical) optimal coherent state amplitudes $|\alpha_{\text{opt}}|$ for lengths between 0 and 180 kilometers for a noiseless channel ($\xi = 0$) without postselection. The optimal analytical $|\alpha|$ was found by a fine-grained search over different state amplitudes for fixed length $L$ in steps of 0.02. The numerical calculations coincide with the theoretical prediction within the accuracy of the performed fine-grained search. Therefore, our numerical implementation is in excellent accordance with the analytical predictions for the noiseless channel. Furthermore, note that the maximal secure key rate for $L = 50$km is about 10 times higher than the maximal secure key rate for $L = 100$km, which meets the expectation for channel losses of 2dB/km. Finally, we remark that the gap between step 1 and step 2 of our algorithm is very small, as can be seen in Figure 6. Therefore, in what follows, we omit the curves for step 1 to improve lucidity.

In Figure 7 we compare the theoretical prediction for $\xi = 0$ with our numerical result for low noise ($\xi = 10^{-5}$). We had to choose a low but non-zero $\xi$ to guarantee numerical stability. Similar to previous calculations, we chose $N_e = 12$. The plot shows the lower bounds on the secure key rate (step 2) obtained by numerical calculation, as well as the theoretical prediction for transmission distances up to 180km. Except for the data points at 15km, 20km and 170km, the relative difference between the theoretical prediction and the numerical calculation is lower than 1.5%, where most of the points show a relative difference between 0.1% and 1%. As already indicated, we observed some numerical instabilities for very low values of excess noise (as in the present plot) which explains the comparably large relative difference of, for example, 2.8% at 20km. We did not observe such numerical instabilities for practical values of excess noise. Summing up, our numerical results are very satisfying, meeting with the theoretical predictions for noiseless channels.

VI. POSTSELECTION STRATEGIES FOR UNTRUSTED DETECTORS

In this section, we are going to present our numerical results and findings for the untrusted ideal detector scenario. Recall that in the whole paper, we work with a reconciliation-efficiency of $\beta = 0.95$ if not mentioned otherwise and measure the excess noise $\xi$ in shot noise units.
A. Cross-shaped postselection

The basic idea of introducing postselection is to increase the secure key rate by discarding noisy data, where Eve could have gained more information about the key than Alice and Bob did. Performing no postselection at all gives Eve an advantage if the signal is noisy, while, on the other hand, postselecting too much (or even all signals) does not leave back enough data to generate a secret key. Therefore, we expect that there is some sweet spot where Alice and Bob can take an optimal advantage. According to our cross-shaped scheme (see Section III), we expect that Eve can benefit most from noisy signals with quadratures close to the axis, where little noise suffices to convert one symbol into another one, i.e., where bit-flips are likely. In the cross-shaped postselection strategy, we determine the ratio of signals that are discarded by varying the postselection parameter $\Delta_c$. Hence, an important task will be to determine the optimal choice of $\Delta_c$ depending on the chosen $|\alpha|$ for every transmission length $L$.

1. Optimal coherent state amplitude

Before we investigate $\Delta_c$, we enquire about the influence of $|\alpha|$ on the secure key rate, as the optimal choice of $\Delta_c$ might heavily depend on the chosen $|\alpha|$. In Figure 8, we investigate the optimal choice of the coherent state amplitude $|\alpha|$ for different values of $\xi$ via coarse-grained search in steps of size 0.05 in the interval $|\alpha| \in [0.4, 1.2]$ and for lengths between 5km and 180km in the absence of postselection and compare our findings with the analytical curve for optimal $|\alpha|$ in the noiseless case. Our results show that the optimal coherent state amplitude in noisy channels is still close to the result for the noiseless case and the values for 20, 50, 80 and 100km match with the values reported by [12] for a similar protocol with rotated signal states. For example, they report optimal values of about 0.78 for 20km and 0.66 for 80km, while we obtained 0.80 and 0.65 respectively. Within the frame of the accuracy of our coarse-grained search with steps of $\Delta_{|\alpha|} = 0.05$ this coincides with our results. Furthermore, we observe that there are only minor differences between the found optimal values for different values of excess noise. Therefore, it is sufficient to search around $|\alpha_{opt}|$, obtained from the noiseless case, which will be useful for the following examinations.

2. Key rates for different transmission distances and noise levels

In Figures 9a and 9b, we plot second step of the secure key rate calculation versus the postselection parameter $\Delta_c$ for $\xi = 0.01$ (Fig. 9a) and $\xi = 0.02$ (Fig. 9b) for fixed distances $L = 50$km (solid lines) and $L = 100$km (dashed lines) on logarithmic scale. Note that the differences between the curves representing the first step and those representing the second step in each of the plots are very small, indicating small gaps between the calculated upper and lower bounds, hence tight bounds on the secure key rates.

One observes a very different behaviour of the curves for $L = 50$km and $L = 100$km for both values of excess noise. First, we investigate $\xi = 0.01$, depicted in Figure 9a, beginning with the curves with solid lines, representing a transmission distance of 50km. The curve for $|\alpha| = 0.75$ does not show a maximum in the interior of the interval [0, 0.55] but attains its maximum at $\Delta_c = 0$, which means no postselection at all. If we raise $|\alpha|$ to 0.90, the curve is still flat in the interval [0, 0.25] but starts forming a maximum around $\Delta_c = 0.25$. Increasing $|\alpha|$ to 1.00, leads to a distinct maximum at $\Delta_c = 0.35$. Therefore, the maximal secure key rate does not move from $\Delta_c = 0$ to higher values slowly when increasing $|\alpha|$ but changes rapidly from zero to some value in the middle of the interval.

We do not observe ‘flat’ secure key rate curves without a pronounced maximum for $L = 100$km. The corresponding curves are represented by dashed lines in Figure 9b. Here, already the curve for $|\alpha| = 0.75$ shows a distinct maximum, as well as the curve for $|\alpha| = 0.90$, indicating that Alice and Bob can increase their secure
Thus, increased excess noise requires postselection for all examined values of $|\alpha|$ for fixed transmission length $L$.

We observe that the differences between the secure key rate for $\Delta_c = 0$ and the secure key rate for the optimal choice of $\Delta_c$ differ significantly for various values of excess noise and several transmission distances. For example, the difference between the maximal secure key rate and that at $\Delta_c = 0$ for $\xi = 0.02$ and $|\alpha| = 0.75$ at $L = 50\text{km}$ is about 5%, while the difference at $L = 100\text{km}$ is about 240%. That highlights the increasing role of postselection for higher transmission distances. We observe a similar behaviour when we optimise over $\Delta_c$ for the plot of the maximal achievable secure key rate versus transmission length.

Next, we compare the decrease of the maximal secure key rates for fixed $|\alpha|$ and $L$ and different values of $\xi$. The maximal secure key rate for $|\alpha| = 0.75$ and $L = 50\text{km}$ for $\xi = 0.01$ is about $10 \times 10^{-3}$, where the corresponding curve for $\xi = 0.02$ attains a maximum secure key rate of about $6.8 \times 10^{-3}$. So, the optimal secure key rate drops by a factor of about 1.5. Similarly, we find a factor of about 1.5 when we compare the maximal secure key rates for $|\alpha| = 0.90$. In contrast, if we compare the corresponding curves for $L = 100\text{km}$, we find for $|\alpha| = 0.75$ maximal secure key rates of $11 \times 10^{-4}$ and $9.5 \times 10^{-4}$. Thus, the factor drops to approximately 1.15, similarly as for $|\alpha| = 0.90$. Therefore, postselection reduces the relative difference between secure key rates for low and high noise with ascending transmission length $L$. That can be explained as follows. For $L = 50\text{km}$, the optimal secure key rates for $\xi = 0.01$ are obtained (almost) without postselection, while higher values of excess noise, such as $\xi = 0.02$, require Bob to perform postselection (with postselection parameters around $\Delta_c = 0.35$). In contrast, for $L = 100\text{km}$ Bob has to perform postselection for both values of $\xi$ to obtain the maximal secure key rate and it turned out that the optimal values for the postselection parameters ($\Delta_c = 0.25$ for $\xi = 0.01$ versus $\Delta_c = 0.35$ for $\xi = 0.02$) differ less than for $L = 50\text{km}$. Therefore, the reduction of the raw key rate due to postselection is smaller for $L = 100\text{km}$ compared to $L = 50\text{km}$, leading to a smaller difference between the corresponding secure key rates. Thus, we expect the curves for the secure key rate for different values of excess noise to approach closer to each other for higher distances (of course, providing that the parameters allow the calculation of secure key rates at all). This observation underlines the advantage of performing postselection for higher values of excess noise.

Both curves for $100\text{km}$ in Figure 9a show a distinct maximum around $\Delta_c = 0.25$ while the curves for $|\alpha| = 1.0$ and $|\alpha| = 0.95$ for $L = 50\text{km}$ show only a comparably weak maximum around $\Delta_c = 0.30$, and the curve for $|\alpha| = 0.75$ is monotonically decreasing, i.e., attains its global maximum for $\Delta_c = 0$. That supports
our observation that for transmission distances of 50km and lower the optimal postselection parameter for the optimal choice of $|\alpha|$, i.e., the parameter-set yielding the highest secure key rate, is $\Delta_c = 0$.

We conclude with a remark about the choices of $|\alpha|$ in Figures 9a and 9b. The coherent state amplitude $|\alpha| = 0.75$ is close to the optimal value for a transmission length of 50km, according to the theoretical calculations. As can be seen in Figure 8, the optimal choice for $|\alpha|$ raises rapidly if one lowers the transmission distances. Hence, the coherent state amplitude has to be adapted accordingly, in order to achieve the maximal secure key rate. Therefore, we additionally examined $|\alpha| = 0.90$, which can be a sound compromise, yielding high secure key rates for most of the relevant transmission lengths.

B. Comparison of postselection strategies

Now, after confirming the advantageous effect of postselection on the secure key rate and getting an idea of the magnitude for different scenarios, we are going to examine the three postselection strategies introduced in section III. In the whole section, we fix the excess noise to $\xi = 0.01$. First, we compare the cross-shaped postselection scheme with the radial scheme.

1. Cross-shaped vs. radial postselection

In the previous section, we learned that cross-shaped postselection does not outperform the secure key rates obtained without postselection for a transmission length of 50km. It turns out that the same applies to distances lower than 50km and that the outperformance starts at about 70km. The optimal values for the parameter of the cross-shaped postselection strategy turn out to be 0 for values below 60km and differs from 0 for $L = 60$km and higher. Therefore, we cannot expect the cross-shaped scheme to outperform the radial scheme in this region as for the radial scheme, for consistency reasons, the secure key rate for the choice $\Delta_r = 0$ is equal to those for the cross-shaped postselection scheme with $\Delta_c = 0$. Furthermore, the secure key rate for that choice of $\Delta_r$ is a lower bound on the maximal achievable secure key rate for the radial postselection scheme, i.e., the maximal secure key rate for transmission lengths lower than 70km cannot be smaller. Therefore, for the first region, the main question will be whether, and if yes, how much the radial postselection scheme performs better. In the second region, where transmission lengths are higher than 60km, we cannot draw similar conclusions in advance.

Figure [10] illustrates that both postselection strategies perform very similarly for transmission distances up to 70km, as expected. A more detailed analysis shows that the radial strategy outperforms the cross-shaped strategy by about 8% in this region. That is because it turned out that the optimal choice for $\Delta_r$, indeed, is greater than zero. Contrarily, for distances higher than 70km, one observes a definite outperformance of the cross-shaped postselection strategy, compared with the radial strategy, yielding an increase in secure key rate by a factor of up to 5/3. This can be seen in Figure 10, where the relative difference between the cross-shaped and the radial scheme turns from negative to positive. We note that, again, we observed a rapid change in the optimal value for the postselection parameter $\Delta_c$, being 0 for $L = 50$km and being 0.25 for $L = 60$km. This can be explained, similarly to Section IV, by the development of a maximum apart from $\Delta_c = 0$.

2. Radial&angular postselection

The comparison between the radial and the cross-shaped postselection scheme confirms the initial presumption that measurement results close to the axis but apart from the origin tend to be faulty. On the other hand, the cross-shaped postselection scheme performs slightly worse for low transmission distances. While the cross-shaped scheme is the simplest and computationally most efficient scheme, one might aim to maximise the secure key rate. An alternative scheme that has the potential to combine the advantages of both the radial and the cross-shaped scheme is the third scheme, introduced
in Section III with radial&angular postselection. Figure 10 shows that the radial&angular scheme performs very similar to the cross-shaped postselection scheme for distances higher than 60km and yields the same secure key rates as the radial postselection scheme for transmission distances lower or equal to 60km. In particular, our research shows that the optimal choice for the angular postselection parameter $\Delta_\alpha$ differed from 0 only for transmission lengths greater than 60km.

Note that the difference between the radial&angular and the radial scheme in Figure 10 for lengths of 70km and lower is 0. Therefore, the curve corresponding to the relative difference drops to zero at 70km. This is because for distances lower than 70km, the optimal choice for the angular postselection parameter is $\Delta_\alpha = 0$.

Summing up, the radial&angular scheme succeeds over the whole examined interval between 0 and 180km. This matches with the idea that noise increases the probability for bit-flips, hence postselecting measurement results close to the boundaries of the regions, associated with different symbols, is expected to reduce such errors, but is opposed to [12], where they state that angular postselection has no significant effect on the secure key rate. According to our examination, this is only true for low transmission lengths, but does not hold for medium and high distances. According to the examinations for the noiseless channel, one can expect a negative impact of regions in the phase-space, lying close to the axes.

C. Influence of the probability to pass the postselection step on the secure key rate

Next, we are going to have a more detailed view on the cross-shaped and the circular postselection. Therefore, we fix $|\alpha| = 0.7$ and compare both postselection strategies for $L = 50\text{km}$, where the radial scheme has the edge over the cross-shaped postselection scheme, and for $L = 100\text{km}$, where the cross-shaped strategy has an advantage concerning maximising secure key rates. In Figures 11a and 11b we plotted the achievable secure key rates over $p_{\text{pass}}$, which is the probability of passing the postselection phase for two different values for the reconciliation efficiency, $\beta = 0.90$ and $\beta = 0.95$. Note that $1 - p_{\text{pass}}$ is the fraction of signals which is removed by the postselection, and hence is not fed into the error correction and privacy amplification routines.

For $L = 50\text{km}$ (see Figure 11a), we find that the radial postselection scheme achieves higher secure key rates, which confirms our earlier results. The curve representing the radial scheme attains its maximum at $p_{\text{pass}} = 0.75$, while the curve representing the cross-shaped scheme increases monotonically, obtaining its maximum at $p_{\text{pass}} = 1$. This coincides with our previous results, stating that the optimal choice for low transmission distances is $\Delta_c = 0$. Furthermore, we observe that for passing probabilities lower than 37.5%, the cross-shaped scheme yields greater secure key rates than the radial scheme.

For $L = 100\text{km}$ (see Figure 11b), we observe a totally different behaviour. Here, the cross-shaped postselection scheme outperforms the radial scheme in the interval $[0, 0.8]$ very clearly and attains a much higher maximum than the radial scheme. Again, this is in accordance with our earlier results. Furthermore, we observe that the maximum of the cross-postselection scheme is attained at $p_{\text{pass}} = 0.55$, while the (much lower) maximum of the radial scheme is attained at $p_{\text{pass}} = 0.8$. Therefore, using the cross-shaped postselection strategy, the secure key
rates are increased by about 35%, while simultaneously the raw key is reduced by almost 50%. That reduces the data required to undergo classical error correction and privacy amplification steps considerably and is a clear advantage for the cross-shaped postselection scheme, as the computations for those steps often are bottlenecks in practical systems. For reference, in [21] they report for the radial postselection scheme at \( L = 75 \text{km} \) to reduce the raw key by 20–30% while increasing the secure key rate by 5–8%, which highlights the advantage of the cross-shaped scheme over the radial scheme.

One can think this idea even further. If one aims to reduce the raw key drastically, for example, by 65% or even more, the cross-shaped scheme yields higher secure key rates both for lengths of 50km and 100km. Therefore, if one aims to remove 80% of the raw key, for \( L = 50 \text{km} \), the secure key rate drops merely by about 20%, compared to the case without postselection. For 100km, the secure key rate is almost the same as without postselection if one reduces the raw key by 80%.

Summing up, the cross-shaped postselection strategy performs slightly worse than the radial strategy for low distances but shows a distinct outperformance for higher transmission distances. The cross-shaped scheme yields higher secure key rates than the radial scheme if one chooses low passing probabilities. The observed effects do not depend on the reconciliation efficiency \( \beta \). Additionally, the cross-shaped postselection strategy is easy to implement in real-world systems, as heterodyne detectors directly measure the \( p \)- and \( q \)-quadrature. Therefore, the cross-shaped postselection can be applied directly to the measurement results without any further computations.

### VII. POSTSELECTION STRATEGIES FOR TRUSTED DETECTORS

In this section, we examine the three different postselection strategies in the trusted noise scenario. For the whole section, we used \( \eta_d = 0.72 \) and \( \nu_{el} = 0.04 \), which coincide with the early stage data of a practical CV-QKD system currently built at AIT.

It turns out that the optimal choice of the coherent state amplitude \( |\alpha| \), depending on the transmission length \( L \), in the trusted detector scenario is identical to the values obtained for the untrusted detector scenario, given in Figure [12a and 12b]. Therefore, we proceed by examining the cross-shaped postselection scheme for the trusted detector scenario.

We begin by examining the cross-shaped scheme, followed by a comparison with other postselection strategies.

#### A. Cross-shaped postselection

Similar to the preceding sections, we are interested in the secure key rates as a function of the postselection parameter \( \Delta_c \) for fixed transmission lengths \( L \) and values of excess noise \( \xi \). Recall that we measure both the excess noise and the electronic noise in shot noise units and fix the reconciliation efficiency \( \beta \) to 0.95 for the whole paper.

For the sake of consistency, we chose to investigate the secure key rates for \( L = 50 \text{km} \) and \( L = 100 \text{km} \) with excess noise \( \xi = 0.01 \) and \( \xi = 0.02 \), which are the same values as in the investigation of the untrusted detector scenario. In addition to the excess noise, we have some trusted electronic noise, so the curves investigated in this section have a higher total noise compared to those we examined in the untrusted scenario. Furthermore, now we consider non-ideal detectors. Therefore, we expect lower secure key rates than in the previous section.

With one little exception, the curves in this section show very small gaps between the first and the second step of the secure key rate calculation, indicating that the bounds on the secure key rates are tight. Therefore, to improve readability of the plots, we do not plot the first step.

For \( L = 50 \text{km} \), we observe a very similar behaviour as in the previous chapter (see solid lines in Figures 12a and 12b). The curves for \( \xi = 0.01 \) do not show a distinct maximum at all, so the maximal secure key rate is attained for \( \Delta_c = 0 \), which means no postselection. If we increase the excess noise to \( \xi = 0.02 \), we see that the curve for \( |\alpha| = 0.90 \) forms a maximum, but the curve for \( |\alpha| = 0.75 \), which is the (theoretical) optimal value for the coherent state amplitude for a transmission distance of \( L = 50 \text{km} \), does not. Afresh, we conclude that the optimal choice of \( \Delta_c \) does not grow slowly from \( \Delta_c = 0 \) to larger values, but changes rapidly from zero to values around \( \Delta_c = 0.4 \), when the maximum starts to shape. So, when searching for the optimal value of \( \Delta_c \), one has to be careful and needs to examine the whole interval for every transmission distance, and not only values of \( \Delta_c \) that are close to the optima for neighbouring values of \( L \), as ‘flat’ secure key rate curves without distinct maximum start to form a distinct maximum within a small interval.

For \( L = 100 \text{km} \), the curves show pronounced maxima for both choices of \( |\alpha| \), where we observe that increasing \( \xi \) shifts the maximum to the right, i.e., the maximal secure key rates are obtained with higher values of the postselection parameter \( \Delta_c \). This is in accordance with our observations in the untrusted detector scenario and with the notion that higher noise requires more postselection. In general, these results are in accordance with our expectations, as we did not suppose significant impact of the trusted detector assumption on the qualitative
1. Key rates for low values of excess noise

For $\xi = 0.01$ we compare the radial, the cross-shaped and the radial\&angular postselection schemes (see Figure 13a) and plot both the obtained secure key rates as well as the relative differences of the radial, the cross-shaped and the radial\&angular scheme compared to the secure key rates obtained without postselection. The radial postselection scheme yields slightly higher secure key rates than the cross-shaped scheme for transmission lengths $L \leq 80\text{km}$. The outperformance in this region is smaller than 10%, as indicated by the difference between the corresponding dot-dashed curves in Figure 13a. For transmission distances greater or equal than 80km, the cross-shaped postselection scheme starts outperforming the radial scheme by up to 60%, where the advantage raises with increasing transmission length. We note that the cross-shaped postselection strategy starts outperforming the radial scheme around 80km, indicated by the crossing of the dot-dashed brown and the dot-dashed yellow curve in Figure 13a.

Summing up, for distances lower or equal to 80km the cross-shaped scheme in the trusted detector scenario performs slightly worse than the radial postselection scheme but has a clear advantage (up to almost 60%) for higher transmission distances. According to our examination, the secure key rates obtained with radial postselection for $\xi = 0.01$ are up to 13% (dot-dashed yellow curve in Figure 13a) higher than those without any postselection. Contrarily, the cross-shaped postselection strategy shows an improvement of about 70% compared to the case where we do not perform postselection at all (dot-dashed brown curve in Figure 13a). As the choice $\Delta_r = 0$ includes the case without postselection, the secure key rate obtained using the cross-shaped postselection scheme is always an upper bound for the secure key rates obtained without postselection. Furthermore, the comparison between the radial and the cross-shaped scheme in Section VI B for the untrusted detector scenario stays valid. In particular, the cross-shaped postselection scheme yields higher secure key rates than the radial postselection scheme if one decides to cut out large parts of the raw key, reducing the amount of data to be processed in the error correction phase.

The radial\&angular postselection scheme combines the advantages of the other two schemes. It has the same performance as the radial postselection scheme for low transmission distances, as the optimisation shows that for transmission lengths lower than 80km the optimal values for the angular postselection parameter $\Delta_\psi$ is zero. Therefore, the dot-dashed purple curve, representing the relative difference of the secure key rates obtained using the radial\&angular postselection

B. Comparison of postselection strategies

Finally, we are going to examine the effect of the three different postselection strategies on the secure key rates. Therefore, we investigated $\xi = 0.01$ and $\xi = 0.02$ and optimized the secure key rate over the coherent state amplitude $|\alpha|$ and the postselection parameter $\Delta_c$ using coarse-grained search in steps of $0.05$ for $|\alpha| \in [0.4, 1.2]$ and in steps of $0.025$ for the postselection parameters $\Delta_c \in [0, 0.45], \Delta_r \in [0, 0.55]$ and $\Delta_\psi \in [0, 0.35]$. The behaviour of the secure key rate curves, hence, all considerations carried out in Section VI A stay valid for the trusted detector scenario.
scheme with the secure key rates obtained without any postselection, in Figure 13a overlaps with the dot-dashed yellow curve representing the corresponding relative difference for the radial postselection strategy. For higher transmission distances the radial-angular postselection scheme has a clear advantage of up to 70% over the radial postselection scheme and performs comparable to the cross-shaped postselection scheme, as shown by the violet dashed line in Figure 13a. The advantage over the secure key rates obtained by radial postselection grows with raising $L$ and is slightly greater than the advantage of the secure key rates obtained by cross-shaped postselection over those obtained by radial postselection. The advantage over the secure key rates calculated without any postselection is up to 85%, as displayed by the dot-dashed purple curve in Figure 13a.

2. Key rates for medium values of excess noise

We observe qualitatively similar results for $\xi = 0.02$, but find that the difference between the radial scheme and the other schemes intensifies (see Figure 13b). Note that we had to increase the number of Frank-Wolfe iterations to $N_{FW} = 150$ as for $N_{FW} = 30$ we observed large gaps between the results of the first and the second step, indicating that the algorithm terminated reaching the iteration limit. Again, the cross-shaped and the radial-angular scheme are clearly ahead the radial postselection scheme. As visualised by the dot-dashed purple and brown lines in Figure 13b, the outperformances of the cross-shaped and the radial-angular postselection scheme, compared to the radial scheme or the case without any postselection is apparent. In concrete numbers, one observes an increase in the secure key rate of up to outstanding 900% comparing the cross-shaped or the radial-angular postselection strategy with the case without postselection and an increase of up to 700% compared with radial postselection. So, the secure key rate can be increased by a factor of up to 9 when choosing an optimised postselection strategy, compared to no postselection. For $\xi = 0.02$ the ratio between the secure key rates obtained with radial postselection and those obtained without any postselection is up to 23%, according to our investigation (dot-dashed yellow curve in Figure 13b). Therefore the increase in the secure key rate for the radial postselection strategy compared to the secure key rate obtained without postselection is comparably small.

The differences between the cross-shaped and the radial-angular scheme are small, with little advantage for the radial-angular scheme. Furthermore, note that the distances where the cross-shaped and the radial-angular postselection strategies start outperforming the radial scheme are now around 70km, i.e., were shifted to the left compared to the plot for $\xi = 0.01$. This means both the cross-shaped and the radial-angular postselection scheme start outperforming the radial scheme earlier, i.e., at lower transmission distances. This meets our expectations, as more noise increases the demand for postselection already at lower distances. We expect that this shift towards lower distances proceeds if one
Relative differences between secure key rates for excess noise $\xi = 0.01$ and $\xi = 0.02$ using various postselection strategies in the trusted detector scenario. Here $\Delta_{\text{xPS}}$ is a short notation for the difference between the secure key rates obtained for $\xi = 0.01$ and $\xi = 0.02$ using the postselection strategy 'x', where $x \in \{r, c, r, a\}$. Furthermore, $(xPS)_{\xi=0.01}$ denotes the secure key rate obtained with 'x' postselection for $\xi = 0.01$. The same applies for $(xPS)_{\xi=0.02}$ with excess noise $\xi = 0.02$.

For the trusted detector scenario, the secure key rate obtained with the radial&angular strategy yields the highest secure key rates for all examined values of excess noise and transmission length. The latter performs merely slightly worse and outperforms the radial postselection strategy clearly. The outperformance of the cross-shaped and the radial&angular postselection schemes compared to the radial scheme for higher transmission distances can be explained by the postselection of measurement results close to the borders of the key map. As the scenario of no postselection is included in every of the mentioned schemes by choosing all corresponding postselection parameters equal to zero, it is evident that all secure key rates obtained with postselection are upper bounds on the secure key rates without postselection.

In contrast, if one aims to reduce the computational effort of the postprocessing steps, one may choose the cross-shaped postselection strategy without a significant drop in the secure key rate.

VIII. CONCLUSIONS

We introduced a new cross-shaped postselection strategy for QPSK-CV-QKD protocols that eliminates measurement results with small values of $q$ and/or $p$, i.e., data points close to one axis or both axes which are the boundaries of regions associated with different symbols in our keymap. Furthermore, we examined this cross-shaped postselection and a strategy with angular and radial postselection using a recent numerical security
proof method. We derived several analytical expressions for operators that are used in the secure key rate calculation, yielding a significant speed-up compared with numerical calculations.

The cross-shaped postselection strategy is easy to implement in practical QKD systems, as it uses the measurement results directly, requiring just one comparison per raw key bit. We showed that this strategy offers a clear advantage for medium and high transmission distances over radial postselection schemes and protocols without any postselection and is competitive with the radial scheme for low transmission lengths, both in the untrusted and trusted detector scenario. For an excess noise of $\xi = 0.01$, the advantage over radial and no postselection increases with rising transmission distances up to 70% and 85% respectively, compared with secure key rates obtained with radial and without postselection. Furthermore, the observed advantage rises with increasing noise, yielding considerably higher secure key rates, up to factors of 8 to 9 compared with radial and no postselection for excess noise of $\xi = 0.02$.

Additionally, the cross-shaped postselection strategy yields significantly higher secure key rates for a low probability of passing the postselection phase, $p_{\text{pass}}$, compared to the radial postselection strategy. This means that one can use our strategy to reduce the raw key rate significantly, while still obtaining comparably high secure key rates. For example, for $\xi = 0.01$ one can omit 80% of the raw key while the secure key rate drops only by a factor of about 20% for a transmission distance of 50km, and only by $5 \sim 8\%$ for a transmission length of 100km. As the outperformance of the cross-shaped postselection strategy, compared to the radial strategy, intensifies for higher values of excess noise, we anticipate this effect to increase for higher values of excess noise. We expect this to be of practical relevance, as the error correction phase is computationally expensive.

Furthermore, we examined a strategy with radial-angular postselection, which performs equally to the radial postselection scheme for low transmission lengths and even slightly better than the cross-shaped scheme for medium and high transmission distances. Compared to the cross-shaped postselection strategy, it shows a slight outperformance over the whole examined interval.

ACKNOWLEDGMENTS

We want to thank Martin Suda for beneficial discussions about various topics related to quantum optics and for proofreading early versions of this manuscript. Furthermore, we thank Michael Hentschel for discussing and providing realistic parameters for experimental implementations.

This work has received funding from the EU Horizon-2020 research and innovation programme under grant agreement No 857156 (OpenQKD) and 820466 (CiViQ).

Appendix A: Fock-state representation of region operators for the untrusted noise scenario

Here, we present the explicit calculations leading to the matrix representations of the region operators with respect to the Fock basis, as stated in Section IV. Both for the calculation of the radial-angular and the cross-shaped postselection strategy, the projection of a coherent state with amplitude $|\alpha|$ and phase $\theta$ on a number state

$$\langle |\alpha|e^{i\theta} |n \rangle = e^{-|\alpha|^2} |\alpha|^n e^{-in\theta} \sqrt{n!},$$

(A1)

or, in Cartesian coordinates, $|\alpha|e^{i\theta} = x + iy$,

$$\langle x + iy |n \rangle = e^{-x^2+y^2} (x - iy)^n \sqrt{n!}$$

(A2)

will be useful. This relation is obtained readily by expressing the coherent state in the number basis and applying the inner product with $|n\rangle$.

Before we start with the calculation, we derive an integral that occurs multiple times in the following derivations. For $p > 0$ and $k > 0$ we have

$$\int_{\Delta} \gamma^p e^{-k\gamma^2} d\gamma = \frac{1}{2k^{p+1} \Gamma\left(\frac{p+1}{2},k\Delta^2\right)}.$$
This can be seen as follows. Using the substitution \( z := k \gamma^2 \) we derive
\[
\int_{\Delta} \gamma^p e^{-k\gamma^2} \, d\gamma = \frac{1}{2k^{p+1}} \int_{k\Delta^2}^{\infty} z^{\frac{p+1}{2}} e^{-z} \, dz = \frac{1}{2k^{p+1}} \int_{k\Delta^2}^{\infty} z^{\frac{p+1}{2}-1} e^{-z} \, dz.
\]
According to the definition of the incomplete gamma function, the integral in the last line is equal to \( \Gamma \left( \frac{p+1}{2}, k\Delta^2 \right) \).

1. Radial\&angular postselection

We start with the expression for the region operators given in equation (34) and insert the definition of the sets \( A_0^a, A_1^a, A_2^a \) and \( A_3^a \) from (32),
\[
R_z^a = \frac{1}{\pi} \int_{\Delta_r} \int_{\frac{z}{\Delta} + \Delta} \gamma |\gamma e^{i\theta}| \langle \gamma e^{i\theta} \rangle \, d\theta \, d\gamma.
\]
Note that we transformed the integral to polar coordinates, which explains the additional \( \gamma \) coming from the Jacobi-determinant. By using the completeness relation, \( \mathbb{1} = \sum_n |n\rangle \langle n| \), twice, we obtain
\[
R_z^a = \frac{1}{\pi} \int_{\Delta_r} \int_{\frac{z}{\Delta} + \Delta} \gamma \sum_{n,m} |n\rangle \langle m| \gamma |\gamma e^{i\theta}| \langle \gamma e^{i\theta} \rangle |m\rangle \, d\theta \, d\gamma
\]
\[
= \frac{1}{\pi} \sum_{n,m} |n\rangle \langle m| \int_{\Delta_r} \gamma^{n+m+1} e^{-\gamma^2} \, d\gamma \int_{\frac{z}{\Delta} + \Delta} e^{i\theta(n-m)} \, d\theta.
\]
The radial integral can be expressed by the incomplete gamma function \( \Gamma(x, a) \) using the integral given in eq. (A3),
\[
\int_{\Delta_r} \gamma^{n+m+1} e^{-\gamma^2} \, d\gamma = \frac{1}{2\sqrt{m!} n!} \Gamma \left( \frac{m+n+1}{2}, \frac{1}{2}, \Delta^2 \right).
\]
If \( m = n \), the angular integral simplifies to \( \frac{\pi}{2} - 2\Delta_a \). For the case \( m \neq n \) we obtain
\[
\frac{2}{m-n} e^{-i(m-n)(z+\frac{1}{2})^2} \sin \left[ \left( \frac{\pi}{4} - \Delta_a \right) (m-n) \right].
\]
In conclusion, we have
\[
R_z^a := \frac{1}{2\pi} \sum_n \sum_m \frac{\Gamma \left( \frac{m+n+1}{2}, \frac{1}{2}, \Delta^2 \right)}{\sqrt{m! n!}} |n\rangle \langle m| \cdot \left\{ \begin{array}{ll}
\frac{\pi}{2} - 2\Delta_a & m = n \\
\frac{2}{m-n} e^{-i(m-n)(z+\frac{1}{2})^2} \sin \left[ \left( \frac{\pi}{4} - \Delta_a \right) (m-n) \right] & m \neq n
\end{array} \right.
\]
\[ (A5) \]

2. Cross-shaped postselection

We start by using the definition of the region operators in equation (35) and the sets \( A_0^c, A_1^c, A_2^c \) and \( A_3^c \) from equation (33),
\[
R_0^c = \frac{1}{\pi} \int_{\Delta_r} \int_{\Delta_c} |x + iy\rangle \langle x + iy| \, dy \, dx,
\]
\[
R_1^c = \frac{1}{\pi} \int_{\Delta_r} \int_{\Delta_c} |x + iy\rangle \langle x + iy| \, dy \, dx,
\]
\[
R_2^c = \frac{1}{\pi} \int_{\Delta_r} \int_{\Delta_c} |x + iy\rangle \langle x + iy| \, dy \, dx,
\]
\[
R_3^c = \frac{1}{\pi} \int_{\Delta_r} \int_{\Delta_c} |x + iy\rangle \langle x + iy| \, dy \, dx.
\]
All integrals have the same form and differ only by the boundaries of the occurring integrals. Hence, we derive only the expression for \( R_0^c \) and argue to obtain the remaining integrals. We start by using the completeness relation, \( \mathbb{1} = \sum_n |n\rangle \langle n| \), twice and obtain
\[ R_0^c = \frac{1}{\pi} \sum_{n,m} |n\rangle \langle m| \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} (n|x + iy\rangle \langle x + iy|m| \ dy \ dx = \frac{1}{\pi} \sum_{n,m} |n\rangle \langle m| \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-(x^2+y^2)}(x+iy)^n(x-iy)^m \ dy \ dx. \]

For \( m = n \) we find
\[
\int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-(x^2+y^2)}(x+iy)^n(x-iy)^m \ dy \ dx = \sum_{k=0}^{n} \binom{n}{k} \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-x^2} x^{2k} \ dx \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-y^2} y^{2(n-k)} \ dy
\]
\[
= \frac{1}{4} \sum_{k=0}^{n} \binom{n}{k} \Gamma \left( k + \frac{1}{2}, \Delta_\epsilon^2 \right) \Gamma \left( n - k + \frac{1}{2}, \Delta_\epsilon^2 \right).
\]

Where we used eq. (A3) to express the occurring integrals by the incomplete gamma function.

For \( m \neq n \) we deduce
\[
\int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-(x^2+y^2)}(x+iy)^n(x-iy)^m \ dy \ dx
\]
\[
= \frac{1}{4} \sum_{j=0}^{m} \sum_{k=0}^{n} \binom{n}{j} \binom{m}{k} \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-x^2} x^{j+k} \ dx \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-y^2} y^{n+m-j-k}(-1)^{m-k} i^n m^j \ dy
\]
\[
= \frac{1}{4} \sum_{j=0}^{m} \sum_{k=0}^{n} \binom{n}{j} \binom{m}{k} (-1)^{m-k} i^n m^j \Gamma \left( j + \frac{1}{2}, \Delta_\epsilon^2 \right) \Gamma \left( n + m - j - k + \frac{1}{2}, \Delta_\epsilon^2 \right). \tag{A6}
\]

We observe that the integral for the case \( m = n \) consists only of squares of \( x \) and \( y \), hence this part is not sensitive to sign-changes and therefore equal for all four operators \( R_0^c \), \( z = 0, 1, 2, 3 \).

For \( m \neq n \), when we calculate \( R_1^c \), we face an integral of the same form as we do for \( R_0^c \) once we substitute \( x \mapsto -\bar{x} \). This leads to
\[
\int_{-\infty}^{-\Delta_\epsilon} e^{-x^2} x^{j+k} \ dx = (-1)^{j+k} \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-\bar{x}^2} \bar{x}^{j+k} \ d\bar{x}.
\]

So, this substitution introduces a factor of \((-1)^{j+k}\) leaving the remaining expression unchanged. If we substitute \( y \mapsto -\bar{y} \), as required for the calculation of \( R_3^c \), we find
\[
\int_{-\infty}^{-\Delta_\epsilon} e^{-y^2} y^{n+m-j-k} \ dy = (-1)^{n+m-j-k} \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-\bar{y}^2} \bar{y}^{n+m-j-k} \ d\bar{y}.
\]

Here, we obtain a factor of \((-1)^{n+m-j-k} \). Finally, the calculation for \( R_3^c \) requires two substitutions, namely \( x \mapsto -\bar{x} \) and \( y \mapsto -\bar{y} \), which introduces a factor of \((-1)^{j+k}(-1)^{m+n-j-k} \). Let us denote the power of \(-1\) that occurs in the expression for the region operator \( z \) by \( D_{j,k,m,n}^{(z)} \). According to the consideration above, we find
\[
D_{j,k,m,n}^{(0)} = 1,
\]
\[
D_{j,k,m,n}^{(1)} = (-1)^{j+k} = (-1)^k \epsilon^{-j},
\]
\[
D_{j,k,m,n}^{(2)} = (-1)^{j+k}(-1)^{m+n-j-k} = (-1)^m - (-1)^n = (-1)^{n-m},
\]
\[
D_{j,k,m,n}^{(3)} = (-1)^{n+m-j-k} = (-1)^n m^k - j. \tag{A7}
\]

To include the power of \( i \) in this factor, we define \( D_{j,k,m,n}^{(z)} := D_{j,k,m,n}^{(z)} i^{n+m-j-k} \). Therefore, we finally arrive at
\[
R_z^c = \sum_{n,m} |n\rangle \langle m| \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-x^2} x^{j+k} \ dx \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-y^2} y^{n+m-j-k} \ dy.
\]

So, the final expression for \( R_z^c \) is given by
\[
R_z^c = \sum_{n,m} |n\rangle \langle m| \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-x^2} x^{j+k} \ dx \int_{\Delta_\epsilon} \int_{\Delta_\epsilon} e^{-y^2} y^{n+m-j-k} \ dy.
\]

Finally, we obtain a factor of \((-1)^{n+m-j-k} \).
Appendix B: Fock-state representation of region operators for the trusted detector scenario

First we express the POVM Element, given in equation (20) in the number basis, where we use equations (6.13) and (6.14) in [32]. After defining $C_{n,m} := \frac{1}{\pi_{14}^{m}} \frac{1}{\sqrt{m!}} \sqrt{m!} \frac{\eta_{d}}{\eta_{a}}$, $a := \frac{1}{\eta_{a}}$, and $b := \eta_{d}(1 + \eta_{d})$, we obtain for $n \leq m$

$$\langle n | G_{y} | m \rangle = C_{n,m} e^{-\alpha |y|^2} (y^*)^{m-n} L_{n}^{(m-n)} \left( -\frac{|y|^2}{b} \right), \quad \text{(B1)}$$

where

$$L_{k}^{\alpha}(x) = \sum_{j=0}^{k} (-1)^{j} \binom{k + \alpha}{k - j} \frac{x^j}{j!} \quad \text{(B2)}$$

is the generalized Laguerre polynomial of degree $k$ and with parameter $\alpha$ [33].

1. Radial&angular postselection

We start with the expression for the region operators given in equation (34), where we replaced the POVM for the ideal homodyne detector by that for the nonideal, trusted detector, and inserted the definition of the sets $A_{1}^{ra}, A_{1}^{ta}, A_{2}^{ra}$ and $A_{2}^{ta}$ from equation (32),

$$R^{ra, \ tr}_{z} = \int_{-\Delta_{a}}^{\infty} \frac{\pi}{\Delta_{a}} \gamma G_{\gamma} e^{i\theta} d\theta d\gamma = \sum_{n=0}^{N_{c}} \sum_{m=0}^{N_{c}} |n\rangle \langle m| \int_{-\Delta_{a}}^{\infty} \frac{\pi}{\Delta_{a}} \gamma e^{i\theta} L^{(0)}_{n}(\gamma) \left( -\frac{\gamma^2}{b} \right) d\gamma \int_{-\Delta_{a}}^{\infty} \frac{\pi}{\Delta_{a}} \gamma e^{i\theta} \gamma^{m-n+1} L^{(m-n)}_{n} \left( -\frac{\gamma^2}{b} \right) d\gamma.$$

Inserting the expression for $G_{y}$ from equation (B1) yields

$$R^{ra, \ tr}_{z} = \sum_{n=0}^{N_{c}} \sum_{m=0}^{N_{c}} C_{n,m} |n\rangle \langle m| \int_{-\Delta_{a}}^{\infty} e^{-\alpha \gamma^2} \gamma^{m-n+1} L^{(m-n)}_{n} \left( -\frac{\gamma^2}{b} \right) d\gamma \int_{-\Delta_{a}}^{\infty} e^{-i\theta(m-n)} d\theta.$$

For $n = m$ the angular integral simplifies to $\frac{\pi}{\Delta_{a}} - 2\Delta_{a}$ and the radial integral can be expressed as

$$\int_{-\Delta_{a}}^{\infty} e^{-\alpha \gamma^2} L^{(0)}_{n} \left( -\frac{\gamma^2}{b} \right) d\gamma = \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^{j+1}} \int_{-\Delta_{a}}^{\infty} \gamma^{2j+1} e^{-\alpha \gamma^2} d\gamma,$$

where we used the sum-representation (B2) of the generalised Laguerre polynomials. Using eq. (A3), we obtain

$$\langle n | R^{ra, \ tr}_{z} | n \rangle = \frac{C_{n,n}}{2} \left( -\Delta_{a} \right) \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{a^{j+1} b^{j+1}} \Gamma \left( j + 1, a \Delta_{a}^2 \right).$$

For $n \neq m$, we obtain for the angular integral $\frac{2}{(m-n)} e^{-i(m-n)(z+\frac{j}{2})} \sin \left[ (m-n) \left( \frac{\pi}{2} - \Delta_{a} \right) \right]$ and derive for the radial integral

$$\int_{-\Delta_{a}}^{\infty} e^{-\alpha \gamma^2} \gamma^{m-n+1} L^{(m-n)}_{n} \left( -\frac{\gamma^2}{b} \right) d\gamma = \sum_{j=0}^{n} \binom{m}{m-j} \frac{1}{a^{j+1} b^{j+1}} \Gamma \left( j + 1, a \Delta_{a}^2 \right).$$

We do not need to calculate the matrix element for $m < n$ separately, as the region operator has to be Hermitian. In conclusion, we found for $R^{ra, \ tr}_{z} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} |n\rangle \langle m| R^{ra, \ tr}_{z} | n \rangle |m\rangle$ the matrix elements

$$\langle n | R^{ra, \ tr}_{z} | m \rangle = \begin{cases} \frac{C_{n,n}}{2} \left( -\Delta_{a} \right) \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{a^{j+1} b^{j+1}} \Gamma \left( j + 1, a \Delta_{a}^2 \right) & n = m \\ \frac{C_{n,m}}{m-n} e^{-i(m-n)(z+\frac{j}{2})} \sin \left[ (m-n) \left( \frac{\pi}{2} - \Delta_{a} \right) \right] \sum_{j=0}^{n} \binom{m}{m-j} \frac{1}{a^{j+1} b^{j+1}} \Gamma \left( j + 1, a \Delta_{a}^2 \right) & n < m \\ \frac{1}{m} R^{ra, \ tr}_{z} | m \rangle & n > m \end{cases} \quad \text{B3}$$
2. Cross-shaped postselection

Similarly to the calculations for the untrusted scenario, we start by using the definition of the region operators in equation (35) and the sets $A_0, A_1, A_2$ and $A_3$ from equation (32).

\[
R_{0, \text{tr}}^c = \int_{-\Delta_e}^{\infty} \int_{-\Delta_e}^{\infty} G_{x+iy} \ dy \ dx,
\]
\[
R_{1, \text{tr}}^c = \int_{-\infty}^{-\Delta_e} \int_{-\Delta_e}^{\infty} G_{x+iy} \ dy \ dx,
\]
\[
R_{2, \text{tr}}^c = \int_{-\infty}^{\infty} \int_{-\Delta_e}^{-\Delta_e} G_{x+iy} \ dy \ dx,
\]
\[
R_{3, \text{tr}}^c = \int_{\Delta_e}^{\infty} \int_{-\infty}^{-\infty} G_{x+iy} \ dy \ dx.
\]

Again, all integrals have the same form and differ only by the boundaries of the occurring integrals. Hence, we derive only the expression for $R_{0, \text{tr}}^c$ and reason the changes to obtain the remaining integrals.

For $n \leq m$ we obtain

\[
R_{0, \text{tr}}^c = \sum_{n,m} \langle n | m \rangle \int_{-\Delta_e}^{\infty} \int_{-\Delta_e}^{\infty} \langle n | G_{x+iy} | m \rangle \ dy \ dx
\]
\[
= \sum_{n,m} \langle n | C_{n,m} \int_{-\infty}^{\infty} \int_{-\Delta_e}^{\infty} e^{-a(x^2+y^2)} (x - iy)^{m-n} L_n^{(m-n)} \left( -\frac{x^2 + y^2}{b} \right) \ dy \ dx,
\]

where we inserted the expression for $G_y$ from equation (B1) in the last line.

First, we treat the case $m = n$, where we have

\[
\langle n | R_{0, \text{tr}}^c | m \rangle = C_{n,n} \int_{-\Delta_e}^{\infty} \int_{-\Delta_e}^{\infty} e^{-a(x^2+y^2)} L_n^{(0)} \left( -\frac{x^2 + y^2}{b} \right) \ dy \ dx
\]
\[
= C_{n,n} \sum_{j=0}^{n} \binom{n}{n-j} \frac{(-1)^j}{j!} \int_{-\Delta_e}^{\infty} \int_{-\Delta_e}^{\infty} e^{-a(x^2+y^2)} \left( \frac{x^2 + y^2}{by} \right)^j \ (-1)^j \ dy \ dx
\]
\[
= C_{n,n} \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^j j!} \sum_{k=0}^{j} \binom{j}{k} \int_{-\Delta_e}^{\infty} e^{-ax^2} x^{2k} \ dx \int_{-\Delta_e}^{\infty} e^{-ay^2} y^{2(j-k)} \ dy.
\]

For the second equality we inserted the sum representation of the Laguerre polynomials (B2) and for the third equality we used the binomial theorem to express $(x^2 + y^2)^j$ as sum. Both the integrals over $x$ and $y$ are of the same form as discussed in eq. (A3), therefore we obtain

\[
\langle n | R_{0, \text{tr}}^c | n \rangle = C_{n,n} \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^j j!} \sum_{k=0}^{j} \binom{j}{k} \frac{1}{a^{j+1}} \Gamma \left( k + \frac{1}{2}, a \Delta_e \right) \Gamma \left( j - 1 + \frac{1}{2}, a \Delta_e \right).
\]

(B4)

Second, we deal with $n < m$. We have

\[
\langle m | R_{0, \text{tr}}^c | n \rangle = C_{m,n} \int_{-\Delta_e}^{\infty} \int_{-\Delta_e}^{\infty} e^{-a(x^2+y^2)} L_n^{(m-n)} \left( -\frac{x^2 + y^2}{b} \right) \ dy \ dx
\]
\[
= C_{m,n} \sum_{j=0}^{m} \binom{m}{m-j} \frac{1}{b^j j!} \int_{-\Delta_e}^{\infty} \int_{-\Delta_e}^{\infty} e^{-a(x^2+y^2)} (x - iy)^{m-n} (x^2 + y^2)^j \ dy \ dx
\]
\[
= C_{m,n} \sum_{j=0}^{m} \binom{m}{m-j} \frac{1}{b^j j!} \sum_{l=0}^{j} \binom{j}{l} \sum_{k=0}^{m-n} \binom{m-n}{k} (-1)^{m-n-k} \int_{-\Delta_e}^{\infty} e^{-ax^2} x^{k+2l} \ dx \int_{-\Delta_e}^{\infty} e^{-ay^2} y^{2j-2l+m-n-k} \ dy.
\]
For the second equality we inserted the sum representation of the Laguerre polynomials \(B2\) and for the third equality we used the binomial theorem twice; first, to express \((x^2 + y^2)^j\) as sum and second, to write \((x - iy)^{m-n}\) as a sum too. Again, the occurring integrals are of the form given in equation \(A3\). Therefore, we obtain

\[
\langle m|R_0^{c, \text{tr}}|n \rangle = \frac{C_{n,m}}{4} \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^j} \int_0^1 \frac{j}{l} \sum_{k=0}^{m-n} \binom{m-n-k}{k} \frac{\Gamma \left( l + k + \frac{1}{2}, a\Delta_z \right)}{\Gamma \left( j - l + \frac{m-n-k+1}{2}, a\Delta_z \right)} \ . 
\]

(B5)

As the region operators have to be Hermitian, we do not need to calculate the matrix elements for \(n > m\) separately. Summing up, we found for \(R_0^{c, \text{tr}} = \sum_{n,m} |n\rangle \langle m| R_0^{c, \text{tr}} |m\rangle\) the matrix elements

\[
\langle n|R_0^{c, \text{tr}}|m \rangle = \begin{cases} 
\frac{C_{n,m}}{4} \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^j} \int_0^1 \frac{j}{l} \sum_{k=0}^{m-n} \binom{m-n-k}{k} \frac{\Gamma \left( k + \frac{1}{2}, a\Delta_z \right)}{\Gamma \left( j - k + \frac{1}{2}, a\Delta_z \right)} \ , & n = m \\
\frac{C_{n,m}}{4} \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^j} \int_0^1 \frac{j}{l} \sum_{k=0}^{m-n} \binom{m-n-k}{k} \frac{\Gamma \left( l + k + \frac{1}{2}, a\Delta_z \right)}{\Gamma \left( j - l + \frac{m-n-k+1}{2}, a\Delta_z \right)} \ , & n > m 
\end{cases}
\]

(B6)

Similarly to the cross-shaped postselection in the untrusted scenario, we observe that the integral for \(m = n\) contains only even powers of \(x\) and \(y\). Hence, this part is not affected by sign-changes in the boundaries of the occurring integrals. In contrast for \(n < m\) we have odd powers of \(x\) and \(y\), so we expect additional powers of \(-1\) in the expressions for \(\langle n|R_z^{c, \text{tr}}|m \rangle, z \in 1, 2, 3\) compared to \(\langle n|R_0^{\text{tr}}|m \rangle\). By similar considerations as carried out in Section [A2] we obtain

\[
\hat{D}_{k,m,n} = \begin{cases} 
(-1)^{m-n-k}, & n = m \\
(-1)^{m-n}, & n < m < m \\
(-1)^k, & n > m \end{cases}
\]

where \(\hat{D}_{m,n,k}\) denotes the power of \(-1\) that occurs in the expression for the region operator \(z\). Note that we have already included the factor \((-1)^{m-n-k}\) which occurs in the expression for all \(z\). We define \(D_{m,n,k}^{(z)} := \hat{D}_{m,n,k}^{(z)} i^{m-n-k}\) and obtain for \(R_z^{c, \text{tr}} = \sum_{n,m} |n\rangle \langle m| R_z^{c, \text{tr}} |m\rangle\) the representation with respect to the number basis

\[
\langle n|R_z^{c, \text{tr}}|m \rangle = \begin{cases} 
\frac{C_{n,m}}{4} \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^j} \int_0^1 \frac{j}{l} \sum_{k=0}^{m-n} \binom{m-n-k}{k} \frac{\Gamma \left( l + k + \frac{1}{2}, a\Delta_z \right)}{\Gamma \left( j - l + \frac{m-n-k+1}{2}, a\Delta_z \right)} \ , & n = m \\
\frac{C_{n,m}}{4} \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^j} \int_0^1 \frac{j}{l} \sum_{k=0}^{m-n} \binom{m-n-k}{k} D_{k,m,n} \Gamma \left( l + k + \frac{1}{2}, a\Delta_z \right) \Gamma \left( j - l + \frac{m-n-k+1}{2}, a\Delta_z \right) \ , & n > m 
\end{cases}
\]

(B7)

3. First- and second-moment observables

For the sake of completeness, we give explicit number-basis representations of the first- and second-moment observables, defined in equations \([21][24]\). We note that \([21]\) gives explicit representations in the appendix, too, which again depend on the coefficients of some Taylor expansion. In contrast to, we give explicit expressions and solve the integrals similar to our calculations for the region operators in the preceding sections. In what follows, we give only expressions for \(n \leq m\), as all operators need to be Hermitian, hence \(\langle k|\hat{O}|l \rangle = \langle l|\hat{O}|k \rangle\) gives the missing matrix elements.

We start with \(\hat{F}_Q\), whose matrix elements with respect to the number basis are given by

\[
\langle n|\hat{F}_Q|m \rangle = \frac{1}{\sqrt{2}} \int (y + y^*) \langle n|G_y|m \rangle
\]
Choosing polar coordinates and inserting the expression for $G_{c,e}$ from equation (B1) leads to

$$
\langle n|\hat{F}_Q|m\rangle = \frac{C_{m,n}}{\sqrt{2}} \int_0^{2\pi} (e^{i\theta} + e^{-i\theta}) e^{-i\theta(m-n)} d\theta \int_0^\infty \gamma^{m-n+2} e^{-a\gamma^2} L_n^{(m-n)} \left(-\frac{\gamma^2}{b}\right) d\gamma
$$

$$
= 2\pi C_{m,n} \delta_{m,n\pm1} \int_0^\infty \gamma^{m-n+2} e^{-a\gamma^2} L_n^{(m-n)} \left(-\frac{\gamma^2}{b}\right) d\gamma
$$

$$
= 2\pi C_{m,n} \delta_{m,n\pm1} \sum_{j=0}^n \left(\frac{m}{n-j}\right) (-1)^j \frac{1}{b^j j!} \int_0^\infty \gamma^{m-n+j+2} e^{-a\gamma^2} d\gamma.
$$

The remaining integral can be solved using (A3) for the special case where $\Delta = 0$. Therefore, we obtain

$$
\langle n|\hat{F}_Q|m+1\rangle = \frac{\pi C_{m,n+1}}{\sqrt{2}} \sum_{j=0}^n \left(\frac{n+1}{n-j}\right) \frac{1}{a^{j+2} b^j} \Gamma(j+2) = \frac{\pi C_{m,n+1}}{\sqrt{2}} \sum_{j=0}^n \left(\frac{n+1}{n-j}\right) \frac{j+1}{a^{j+2} b^j} \tag{B8}
$$

and $\langle n|\hat{F}_Q|m\rangle = 0$ for $m \neq n \pm 1$, where we used the definition of the gamma function. Similarly, starting from equation (22), we derive

$$
\langle n|\hat{F}_P|m+1\rangle = \frac{i \pi C_{m,n+1}}{\sqrt{2}} \sum_{j=0}^n \left(\frac{n+1}{n-j}\right) \frac{j+1}{a^{j+2} b^j} = i \langle n|\hat{F}_Q|m+1\rangle \tag{B9}
$$

and $\langle n|\hat{F}_P|m\rangle = 0$ if $m \neq n \pm 1$.

The matrix elements of the second-moment observables read

$$
\langle n|\hat{S}_Q|n\rangle = -\langle n|\hat{S}_P|n\rangle = \pi C_{m,n} \sum_{j=0}^n \left(\frac{n}{n-j}\right) \frac{j+1}{a^{j+2} b^j}, \tag{B10}
$$

$$
\langle n|\hat{S}_Q|n+2\rangle = -\langle n|\hat{S}_P|n+2\rangle = \pi C_{m,n+2} \sum_{j=0}^n \left(\frac{n+2}{n-j}\right) \frac{(j+2)(j+1)}{a^{j+3} b^j} \tag{B11}
$$

and $\langle n|\hat{S}_Q|m\rangle = \langle n|\hat{S}_P|m\rangle = 0$ otherwise.

### Appendix C: Choice of the cutoff number $N_c$

In this section, we briefly discuss the choice of the photon cutoff number $N_c$. Following [12], we assume that it suffices to use the first $N_c$ Fock states to describe Bob’s infinite-dimensional Hilbert space with sufficient accuracy. Choosing $N_c$ too small leads to inaccurate results, while choosing $N_c$ too large makes the problem computationally infeasible, as the problem size increases with increasing $N_c$. Therefore, we examined the change in the secure key rate when increasing $N_c$ for different transmission distances and different postselection parameter for fixed parameters $\beta = 0.95$ and $\xi = 0.01$. The result is visualised in Figure [13] where one observes that the secure key rate remains (almost) constant for $N_c \geq 12$ for all three curves. The relative changes between neighbouring data points for $N_c \geq 12$ are lower than 0.5% and for $N_c \geq 14$ lower than 0.2%. This fluctuations are mainly caused by the gap between step 1 and step 2, which is more sensitive to numerical errors. The relative differences between neighbouring data-points of the results of the first steps are smaller than 0.01% for $N_c \geq 12$. This motivates our choice of $N_c = 12$ for the present paper, being a good compromise between accuracy and computational feasibility.
FIG. 15. Secure key rate versus chosen cutoff-number $N_c$ for three different distances and choices of postselection parameter. For all three curves, we set $\beta = 0.95$ and $\xi = 0.01$.

Appendix D: Symbols used

| Symbol | Description |
|--------|-------------|
| $\alpha$ | coherent state amplitude |
| $\beta$ | reconciliation efficiency |
| $\Delta_a$ | angular postselection parameter |
| $\Delta_c$ | cross-shaped postselection parameter |
| $\Delta_r$ | radial postselection parameter |
| $\eta$ | channel transmittance |
| $\eta_d$ | detector efficiency |
| $\epsilon$ | small perturbation |
| $\epsilon_{FW}$ | threshold of the Frank-Wolfe algorithm |
| $\epsilon'$ | magnitude of constraint-violations |
| $N_c$ | photon cut-off number |
| $N_{FW}$ | number of Frank-Wolfe iterations |
| $\nu_{el}$ | electronic noise |
| $p_z$ | probability that state $z$ is prepared |
| $\xi$ | excess noise |

TABLE I. Experimental and numerical quantities used

| Symbol | Description |
|--------|-------------|
| $d$ | operator defined by $d = \hat{q}^2 - \hat{p}^2$ |
| $D$ | quantum relative entropy |
| $\delta_{EC}$ | leakage per signal |
| $E_y$ | POVM of ideal homodyne detector |
| $\hat{F}_{Q,P}$ | first-moment observables $(q, p)$ |
| $G$ | CPTP map |
| $G_y$ | POVM of trusted homodyne detector |
| $\hat{n}$ | number operator |
| $\hat{p}$ | $p$-quadrature operator |
| $\hat{q}$ | $q$-quadrature operator |
| $p_{pass}$ | probability of passing the postselection phase |
| $R^\infty$ | secure key rate in the asymptotic limit |
| $R_{xPS}$ | region operator, corresponding to protocol $x$ |
| $\hat{S}_{Q,P}$ | second-moment observables $(q, p)$ |
| $Z$ | pinching quantum channel |

TABLE II. Further variables used

[1] 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 (India, 1984) p. 175.
[2] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A 61, 010303 (1999).
[3] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Continuous variable quantum cryptography: Beating the 3 db loss limit, Phys. Rev. Lett. 89, 167901 (2002).
[4] D. Sych and G. Leuchs, Coherent state quantum key distribution with multi letter phase-shift keying, New Jour-
[8] A. Denys, P. Brown, and A. Leverrier, Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation of coherent states (2021). arXiv:2103.13945 [quant-ph]

[9] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Numerical approach for unstructured quantum key distribution, Nature Communications 7, 11712 (2016).

[10] A. Winick, N. Lütkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution. Quantum 2, 77 (2018).

[11] T. Upadhyaya, T. van Himbeeck, J. Lin, and N. Lütkenhaus, Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols, PRX Quantum 2, 10.1103/prxquantum.2.020325 (2021).

[12] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, Physical Review X 9, 10.1103/physrevx.9.041064 (2019).

[13] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. 461, 207 (2005).

[14] G. Lindblad, Expectations and entropy inequalities for finite quantum systems, Communications in Mathematical Physics 39, 111 (1974).

[15] M. Jaggi and P. Wolfe, An algorithm for quadratic programming, Naval Research Logistics Quarterly 3, 95 (1956).

[16] M. Jaggi, Revisiting Frank-Wolfe: Projection-free sparse convex optimization, in Proceedings of the 30th International Conference on Machine Learning Proceedings of Machine Learning Research, Vol. 28-1, edited by S. Dasgupta and D. McAllester (PMLR, Atlanta, Georgia, USA, 2013) pp. 427–435.

[17] T. Tyc and B. C. Sanders, Operational formulation of homodyne detection, Journal of Physics A: Mathematical and General 37, 7341–7357 (2004).

[18] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a precondition for secure quantum key distribution, Phys. Rev. Lett. 92, 217903 (2004).

[19] A. Ferenczi and N. Lütkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, Phys. Rev. A 85, 052310 (2012).

[20] J. Altepeter, E. Jeffrey, and P. Kwiat, Photonic state tomography, in Advances in Atomic, Molecular and Optical Physics, edited by P. Berman and C. Lin (2005) pp. 105–159.

[21] J. Lin and N. Lütkenhaus, Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution, Physical Review Applied 14, 10.1103/physrevapplied.14.064030 (2020).

[22] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Taulelle-Broui, S. W. McLaughlin, and et al., Quantum key distribution over 25km with an all-fiber continuous-variable system, Physical Review A 76, 10.1103/physreva.76.042305 (2007).

[23] T. M. Cover and J. A. Thomas, Elements of Information Theory (Wiley-Interscience, USA, 1991).

[24] D. Slepian and J. Wolf, Noiseless coding of correlated information sources, IEEE Transactions on Information Theory 19, 471 (1973).

[25] M. Grant and S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.1, http://cvxr.com/cvx (2014).

[26] M. Grant and S. Boyd, Graph implementations for nonsmooth convex programs, in Recent Advances in Learning and Control, Lecture Notes in Control and Information Sciences, edited by V. Blondel, S. Boyd, and H. Kimura (Springer-Verlag Limited, 2008) pp. 95–110, http://stanford.edu/~boyd/graph_dcp.html.

[27] M. ApS, The MOSEK optimization toolbox for MATLAB manual. Version 9.0. (2019).

[28] K. C. Toh, M. J. Todd, and R. H. Tutuncu, Sdpt3 — a matlab software package for semidefinite programming, version 1.3, Optimization Methods and Software 11, 545 (1999) https://doi.org/10.1080/10556789908805762.

[29] R. H. Tutuncu, K. C. Toh, and M. J. Todd, Solving semidefinite-quadratic-linear programs using sdpt3, Mathematical Programming 95, 189 (2003).

[30] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. 84, 621 (2012).

[31] M. Heid and N. Lütkenhaus, Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction, Phys. Rev. A 73, 052316 (2006).

[32] B. R. Mollow and R. J. Glauber, Quantum theory of parametric amplification. i, Phys. Rev. 160, 1076 (1967).

[33] K. Oldham, J. Myland, and J. Spanier, The laguerre polynomials Ln(x), in Atlas of Functions (Springer, New York, NY, 2008) pp. 209–216.