Postselection strategies for CV-QKD protocols with quadrature phase-shift keying modulation

Florian Kanitschar[1,2] and Christoph Pacher[1]

[1] *AIT Austrian Institute of Technology, Center for Digital Safety & Security*

[2] *TU Wien, Faculty of Physics*

AUSTRIAN INSTITUTE OF TECHNOLOGY

Abstract

Continuous-variable quantum key distribution with phase-shift keying modulation is a promising candidate for practical applications of quantum cryptography due to high compatibility with existing telecommunication infrastructure. It is known that postselection, i.e., omitting those parts of the raw key where an adversary might have gained more information than the communicating parties, can improve the secure key rate significantly. We introduce a new cross-shaped postselection strategy and use a recent numerical security proof framework to compare it to other existing postselection strategies. Furthermore, we provide novel analytical results for the operators that define the respective postselection regions in phase space for each of the postselection strategies, enabling a quicker evaluation without introducing additional numerical errors. Motivated by the high computatoinal effort for the error-correction phase, we point out how postselection can be used to reduce the raw key (so, the data that has to be error-corrected) significantly without lowering the secure key rate considerably. As therefore Bob uses his measurement outcomes directly without requiring any additional computations, the cross-shaped scheme can be implemented easily both in new and existing QKD systems.

Theoretical background

We use a recent numerical security proof framework [1,2] to calculate a reliable lower bound on the secure key rate in the asymptotic limit. Therefore, for the case of reverse reconciliation, the secure key rate is given by

$$R^{\infty} = \min_{\rho_{AB} \in \mathcal{S}} D\left(\mathcal{G}(\rho_{AB}) || \mathcal{Z}(\mathcal{G}(\rho_{AB}))\right) - p_{\text{pass}} \delta_{EC},$$

where D is the quantum relative entropy, $\mathcal{G}$ and $\mathcal{Z}$ are maps depending on the protocol, δ_{EC} is the information-leakage per signal in the error-correction phase and p_{pass} is the sifting-probability. The set $\mathcal{S}$ is the feasible set of the optimisation and is given by a set of linear constraints

$$\mathcal{S} := \left\{ \rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB}) \mid \forall i \in I : \operatorname{Tr}\left[\Gamma_i \rho_{AB}\right] = \gamma_i \right\},$$

with Hermitian operators Γ_i and real numbers γ_i. The constraints are given by experimental observations and the fact that Eve does not have access to Alice's lab. It can be shown that the given problem is a semi-definite program (SDP). Since the objective-function $f(\rho) = D(\mathcal{G}(\rho)||\mathcal{Z}(\mathcal{G}(\rho)))$ is nonlinear, we solve the problem in a two-step process. In the first step, the linearised problem is solved iteratively using a modified Frank-Wolfe algorithm. Since we cannot expect to solve the numerical optimisation accurately, this gives only an upper bound on the secure key rate. In the second step, the obtained upper bound is converted into a lower bound, combining linearisation and the dual of the occurring SDP, taking numerical imprecisions into account. Finally, the information leakage δ_{EC} is given by

$$\delta_{EC} = (1-\beta) H(\mathbf{Z}) + \beta H(\mathbf{Z}|\mathbf{X}),$$

where β is the reconciliation efficiency of the used error-correction code and $\mathbf{X}$ and $\mathbf{Z}$ are Alice's and Bob's key-strings respectively.

Protocols and Postselection schemes

We examine prepare and measure (P&M) protocols with phase-shift keying modulation and signal states located on the diagonals of the quadrants. Thanks to the source-replacement scheme, our analysis is also valid for entanglement-based protocols. Alice starts the protocol with **state preparation**. She prepares one out of four coherent states $|\psi_k\rangle \in \left\{ \left| |\alpha| e^{i\frac{1\pi}{4}} \right\rangle, \left| |\alpha| e^{i\frac{3\pi}{4}} \right\rangle, \left| |\alpha| e^{i\frac{5\pi}{4}} \right\rangle, \left| |\alpha| e^{i\frac{7\pi}{4}} \right\rangle \right\}$, where $|\alpha| > 0$ is the coherent state amplitude, with equal probability and sends them to Bob. The states are associated with $x_k \in \{0,1,2,3\}$. Once Bob receives the states, he performs heterodyne measurement (**measurement phase**). This is followed by **parameter estimation**, where the communicating parties determine the amount of information an advisory might have gained about the key. Next, Bob applies a **key map** to link his measurement results with symbols $y_k \in \{0,1,2,3\}$. Depending on the chosen **postselection** strategy (see Fig. 1), he omits measurement results lying in certain regions of the phase space. Finally, Alice and Bob perform **error-correction and privacy amplification**.

The operators associated with the postselection areas depicted in Fig. 1 can be represented in the number-basis, $R_z = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n|R_z|m\rangle |n\rangle\langle m|$, where $z \in \{0,1,2,3\}$ is the symbol, associated with the four quadrants. The matrix elements (depending on the chosen postselection strategy) are given by

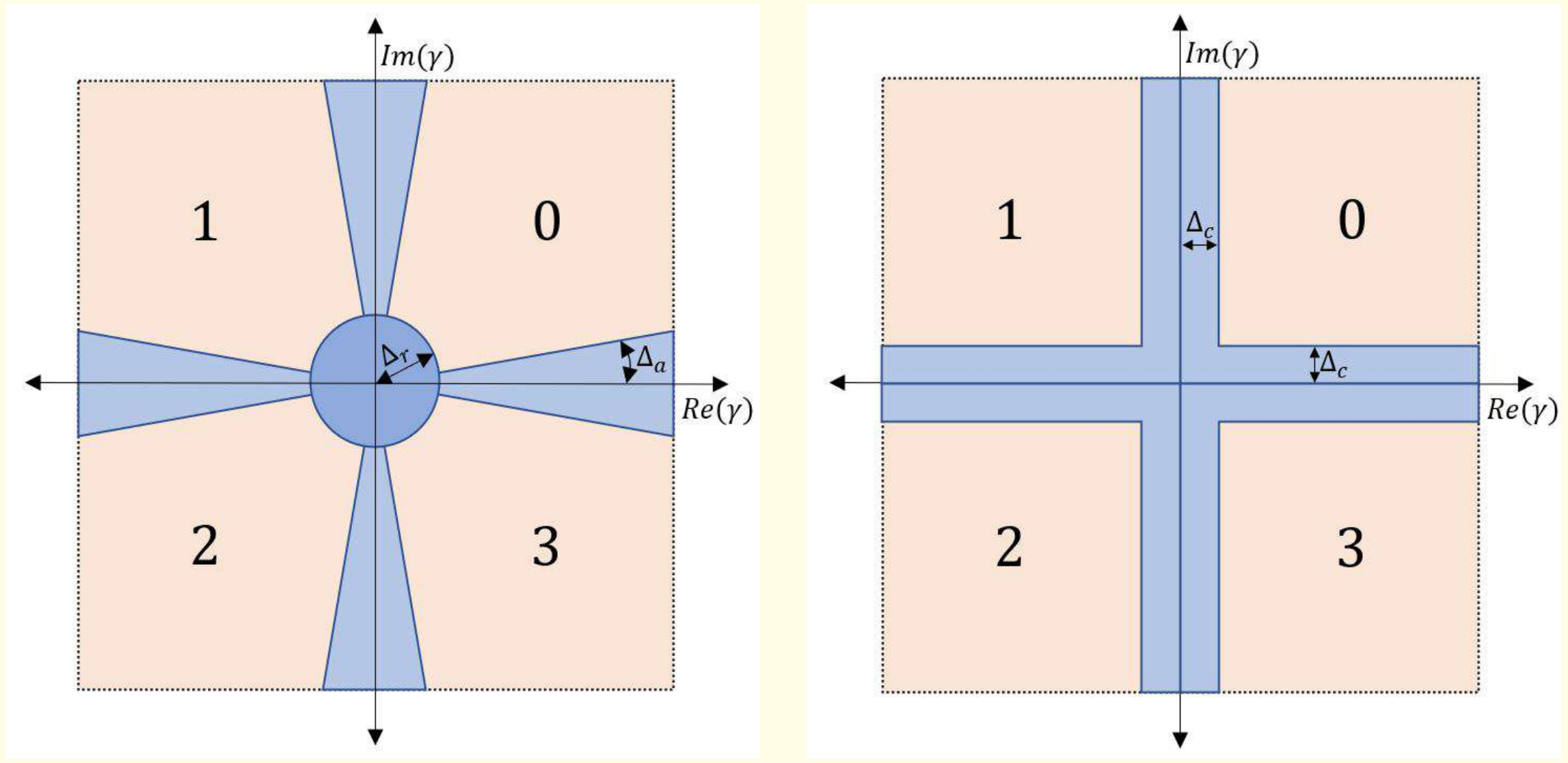


Figure 1: Sketch of the radial & angular (left) and cross-shaped (right) postselection strategy.

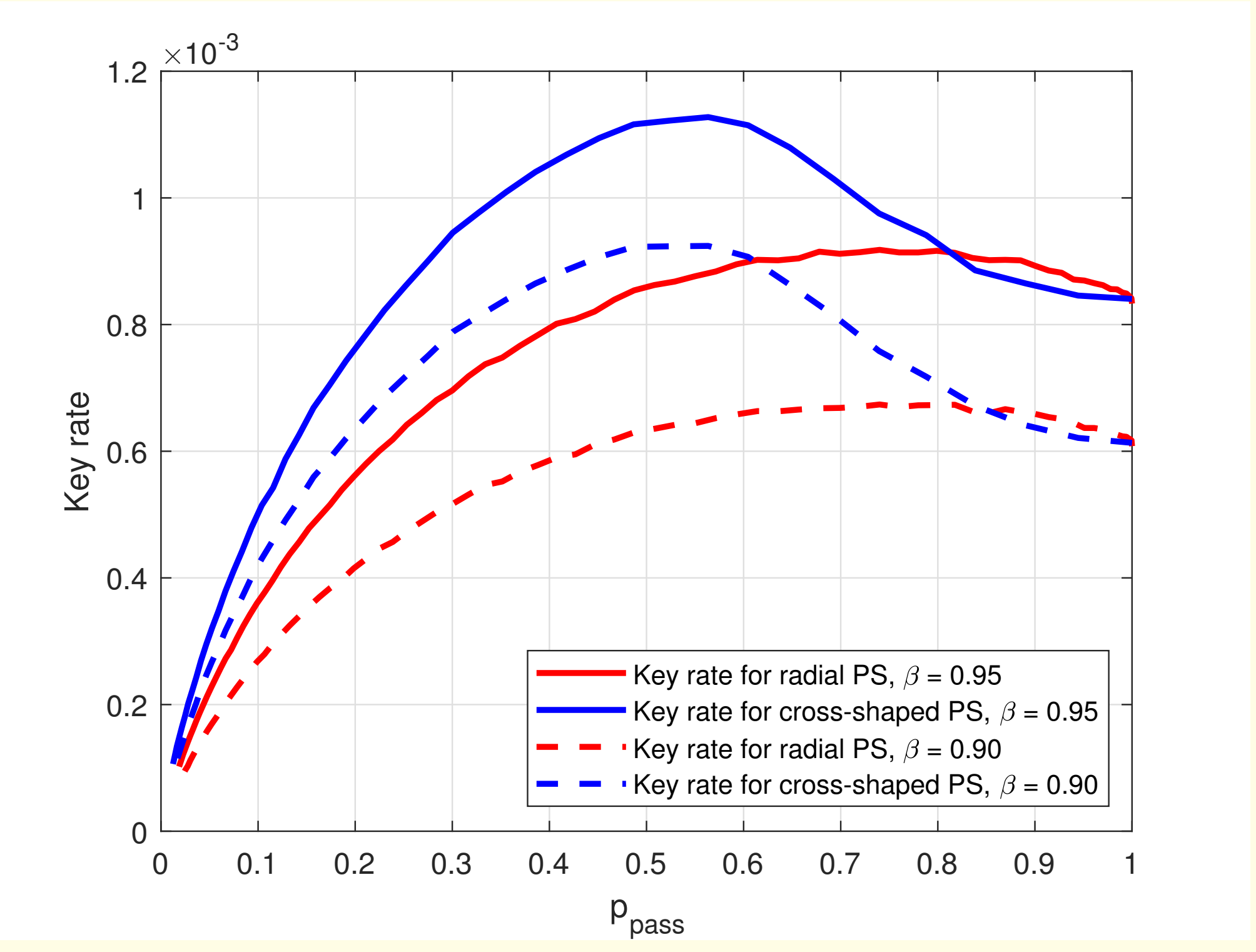
$$\langle n|R_z^{\text{ra}}|m\rangle = \begin{cases} \frac{\Gamma\left(n+1,\Delta_r^2\right)}{\pi(n!)} \left(\frac{\pi}{4} - \Delta_a\right) & n = m \\ \frac{\Gamma\left(\frac{m+n}{2}+1,\Delta_r^2\right)}{\pi(m-n)\sqrt{n!}\sqrt{m!}} e^{-i(m-n)\left(z+\frac{1}{2}\right)\frac{\pi}{2}} \sin\left[\left(\frac{\pi}{4} - \Delta_a\right)(m-n)\right] & n \neq m \end{cases}$$

$$\langle n|R_z^{\text{c}}|m\rangle = \begin{cases} \frac{1}{4\pi(n!)} \sum_{j=0}^{n} \binom{n}{j} \Gamma\left(j+\frac{1}{2},\Delta_c^2\right) \Gamma\left(n-j+\frac{1}{2},\Delta_c^2\right) & n = m \\ \frac{1}{4\pi\sqrt{n!}\sqrt{m!}} \sum_{j=0}^{n} \sum_{k=0}^{m} \binom{n}{j}\binom{m}{k} \Gamma\left(\frac{j+k+1}{2},\Delta_c^2\right) \Gamma\left(\frac{n+m-j-k+1}{2},\Delta_c^2\right) D_{j,k,m,n}^{(z)} & n \neq m \end{cases}$$

where $D_{j,k,m,n}^{(z)} = i^{n-m+k-j} \cdot \begin{cases} 1 & z = 0 \\ (-1)^{k-j} & z = 1 \\ (-1)^{n-m} & z = 2 \\ (-1)^{n-m+k-j} & z = 3 \end{cases}$, as we derived in [3].

Results

We investigated the secure key rate as a function of the sifting probability p_{pass}, which is the probability that a given round passes the postprocessing phase. Note that $1 - p_{\text{pass}}$ is equal to the fraction of the data that is omitted, i.e., does not have to be error-corrected. We observe that for low transmission distances the cross-shaped postselection scheme yields slightly lower secure key rates than the radial postselection scheme, while the cross-shaped scheme has a clear advantage for medium to high distances. In general, we observe that by a proper choice of the postselection parameter (which influences p_{pass} directly) one can increase the secure key rate while lowering the secure key rate. This effect intensifies for higher transmission distances. Since the error-correction phase is a well-known bottleneck in many implementations, one can think this idea even further. As can be seen in the plot on the right (where we chose an excess-noise level of $\xi = 0.01$, a transmission distance of $L = 100$km and we fixed the coherent-state amplitude to $|\alpha| = 0.7$.), one can reduce the raw key significantly while still obtaining the same secure key rate as one would have obtained without performing any postselection. While about half of the raw key can be omitted by radial postselection, using the cross-shaped postselection scheme, one can reduce the secure key rate by about 75% without decreasing the secure key rate at a transmission distance of 100km. Since postselection can be introduced easily to every QKD-system without requiring additional hardware, it provides an simple and low-threshold way to increase the secure key rate while lowering the raw key moderately or, alternatively, to reduce the raw key considerably, without a significant drop in the secure key rate compared to not performing postselection at all.



References

1. A. Winick, N.Lütkenhaus, and P.J. Coles, Reliable numerical key rates for quantum key distribution, Quantum 2, 77 (2018)
2. J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, Phys.Rev. X 9, 10.1103 (2019)
3. F. Kanitschar, and C. Pacher, Postselection strategies for continuous-variable quantum key distribution protocols with quadrature phase-shift keying modulation, arXiv:quant-ph/2107.06110 (2021)