Fading channel estimation for free-space continuous-variable secure quantum communication

L. Ruppert[1], C. Peuntinger[2,†], B. Heim[2,‡], K. Günthner[2], V. C. Usenko[1], D. Elser[2], C. Marquardt[2], R. Filip[1], and G. Leuchs[2]

[1] Department of Optics, Palacky University Olomouc

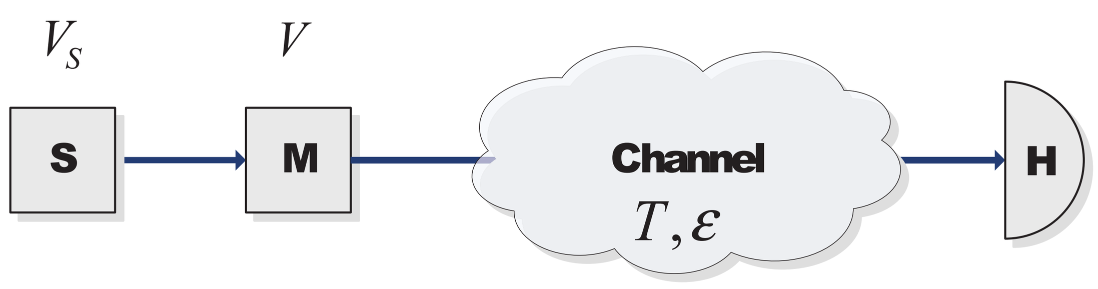
[2] Max-Planck-Institut für die Physik des Lichts / Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg

† Currently at inno-spec GmbH, ‡ Currently at OHB System AG

email: ruppert@optics.upol.cz

UNIVERZITA PALACKÉHO V OLOMOUCI

Model and experiment



The model:

- The effect of the channel: $x_B = \sqrt{T} \cdot (x_S + x_M) + \sqrt{1-T} \cdot x_0 + x_\varepsilon$, which can be rewritten as $x_B = \sqrt{T} \cdot x_M + x_N$.
- Key rate: $K = (1-r) \cdot \left[K_\infty(T^{LOW}, V_\varepsilon^{UP}) - \Delta\Big([1-r]N\Big) \right]$, with $K_\infty(T, V_\varepsilon) = \beta I(A:B) - S(B:E)$.

The experiment:

- The experiment was performed in the Erlangen rural area.
- The states were repeatedly sent over with an effective sending rate of $2.48 \cdot 10^6$ states per second $\Rightarrow$ we have a sample size of order 10^7.
- At the remote side the channel transmittance was monitored using a tap-off followed by an intensity measurement.

Effect of fluctuations

- The covariance matrix of outcomes of x_M and x_B is

$$\mathrm{Cov}(x_M, x_B) = \begin{pmatrix} V & \langle\sqrt{T}\rangle V \\ \langle\sqrt{T}\rangle V & \langle T\rangle V' + \varepsilon + 1 \end{pmatrix}$$

- It is equivalent to the fixed channel:

$$\mathrm{Cov}(x_M, x_B) = \begin{pmatrix} V & \sqrt{T_{\mathrm{eff}}} V \\ \sqrt{T_{\mathrm{eff}}} V & T_{\mathrm{eff}} V' + \varepsilon_{\mathrm{eff}} + 1 \end{pmatrix}$$

- The parameters are connected through:

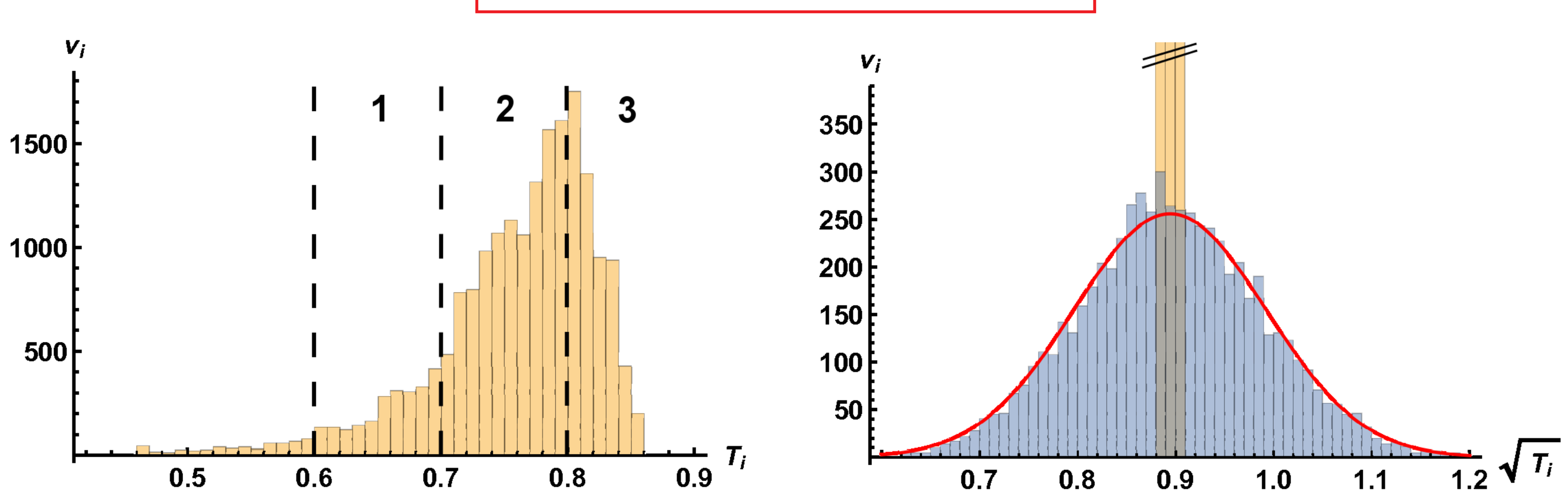
$$T_{\mathrm{eff}} = \langle\sqrt{T}\rangle^2, \quad \varepsilon_{\mathrm{eff}} = \varepsilon + \mathrm{Var}(\sqrt{T}) V'.$$

Package clusterization

The solution for handling a fading channel so far [1] has been to

- discard packages with T_i below a critical value,
- use 99% of states for estimation, 1% of states for communication.

Idea: More clusters! Optimal ratio!

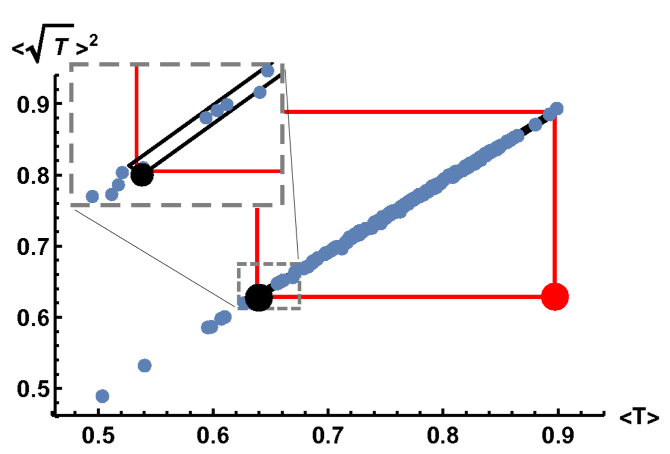


The individual packages can be estimated:

- Estimation of the transmittance $\widehat{\sqrt{T_i}} = \frac{1}{V} \cdot \widehat{C_{MB}}$, with maximum likelihood estimator $\widehat{C_{MB}} = \frac{1}{r \cdot n} \sum_{j=1}^{r \cdot n} M_j B_j$.
- We can obtain the variance of this estimator [2] (see the fit in the right figure):

$$\mathrm{Var}(\widehat{\sqrt{T_i}}) = \frac{1}{r \cdot n} \cdot T_i \left(2 + \frac{V_N}{T_i V}\right)$$

Confidence intervals for channel parameters



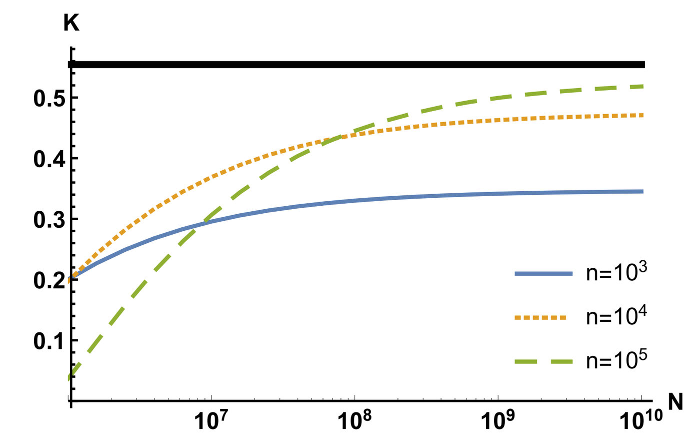
- Worst case (red): lower bound $\langle\sqrt{T}\rangle^{\mathrm{LOW}}$ and upper bounds $\langle T\rangle^{\mathrm{UP}}$ and $\varepsilon^{\mathrm{UP}}$.
- Instead use the transformed variables (black)

$$X_1 := \langle T\rangle - \langle\sqrt{T}\rangle^2 = \mathrm{Var}(\sqrt{T})$$
$$X_2 := \langle T\rangle + \langle\sqrt{T}\rangle^2$$

$\Rightarrow$ 20-30 times better estimation of fluctuation.

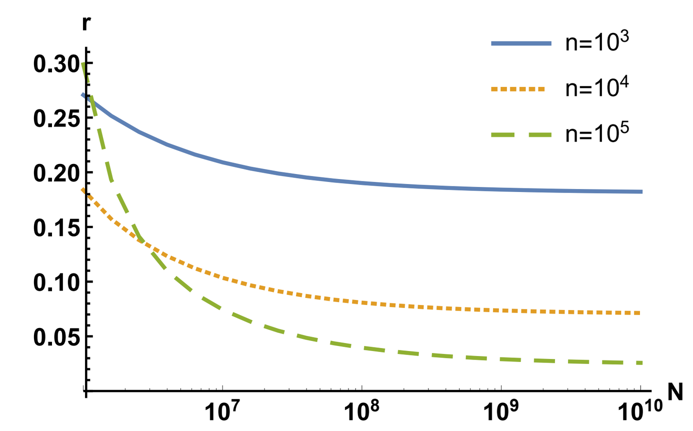
Semi-analytical investigation of the scheme

Dependence on the package size and total number of states



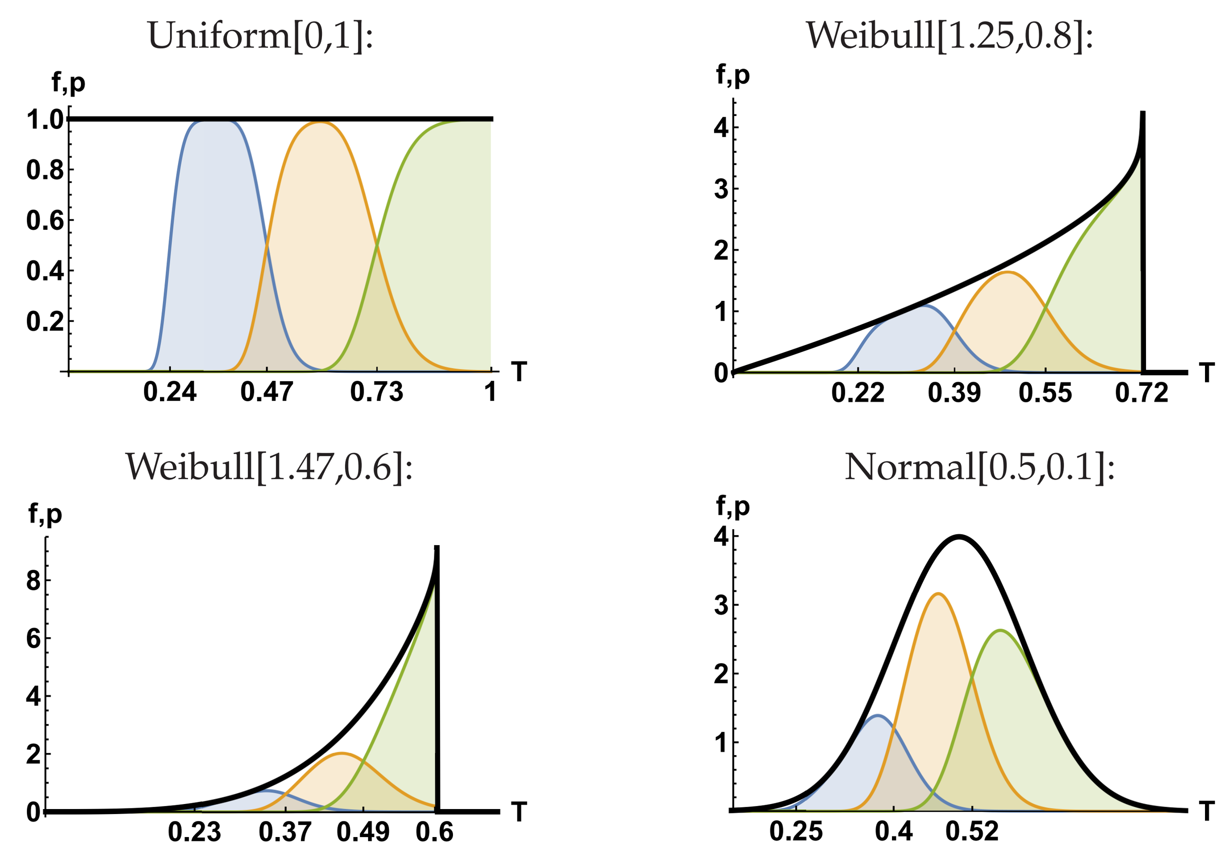
- for finite package sizes the key rate will saturate lower than the key rate of the reference
- the maximally achievable key rate increases with the number of states in each package (n)
- it is also important to have a reasonable number of packages (see the low N values in the figure)

Optimal ratio of states used for estimation

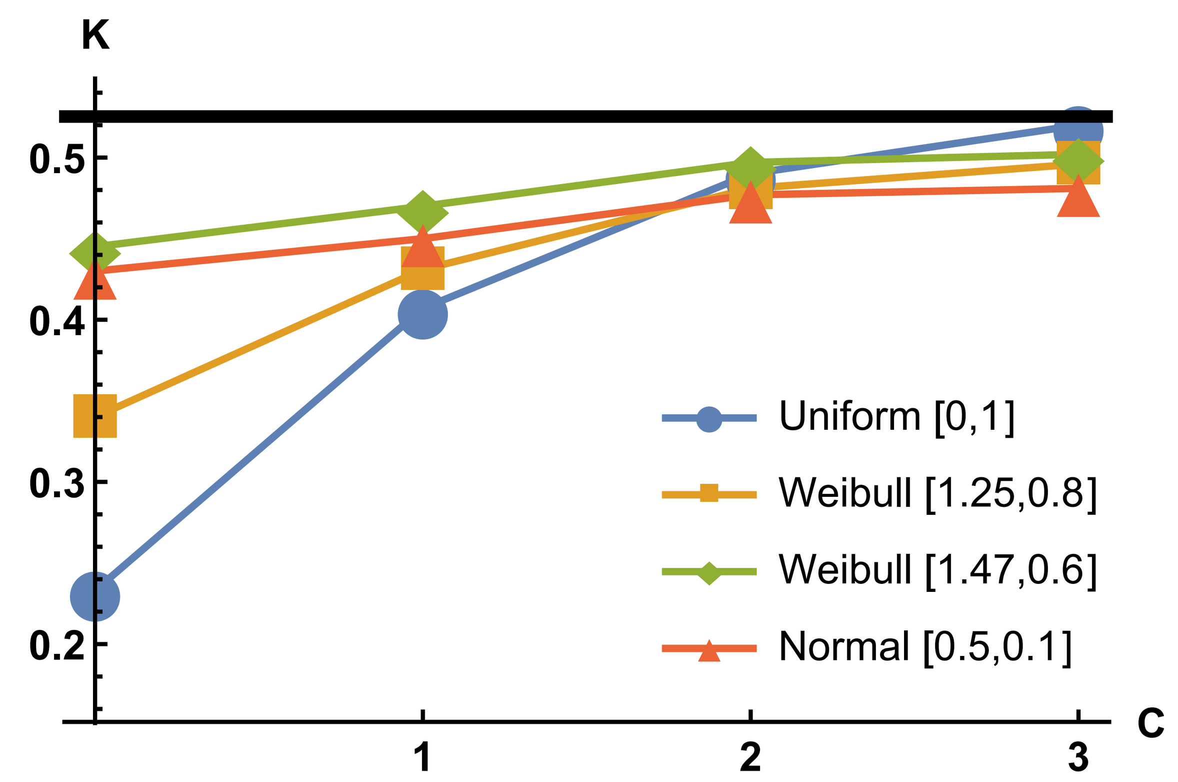


- a lower percentage of states (r) is sufficient for estimation if we have more states
- the values saturate at a non-zero level due to the uncertain estimation for fixed-size packages
- these values are quite low (much lower than the earlier suggested 99.9%)

The ideal clusterization for three clusters ($C = 3$)



The effect of clusterization



Conclusions [3]

- The variance of the estimator can be approximated beforehand $\Rightarrow$ experiment design.
- The optimal ratio of states used for estimation is much lower than in the literature.
- The estimation of the channel is a non-trivial, but important task in realistic QKD settings (especially for fluctuating channels).
- For a lightly fluctuating channel, one can obtain good results even without clusterization.
- For a heavily fluctuating channel, we can get close to the key rate of a fixed-transmission channel by using 2-3 clusters.

Acknowledgments

VCU acknowledges project LTC17086 of the INTER-EXCELLENCE program of the Czech Ministry of Education and acknowledges the support of project 19-23739S of the Czech Science Foundation. LR acknowledges the support of project 19-22950Y of the Czech Science Foundation. RF acknowledges support of project CZ.02.1.01/0.0/0.0/16_026/0008460 of the Czech Ministry of Education. The research leading to these results has received funding from the H2020 European Programme under Grant Agreement 820466 CIVIQ. The authors also acknowledge support from COST Action CA 15220 QTSpace.

References

[1] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs and R. Filip, New Journal of Physics 14 093048, 2012

[2] L. Ruppert, V. C. Usenko and R. Filip, Physical Review A 90 062310, 2014

[3] L. Ruppert, C. Peuntinger, B. Heim, K. Günthner, V. C. Usenko, D. Elser, C. Marquardt, R. Filip and G. Leuchs, New Journal of Physics 21 123036, 2019