Quantum key distribution rates from semidefinite programming

Mateus Araújo, Marcus Huber, Miguel Navascués, Matej Pivoluska, and Armin Tavakoli
Quantum 7, 1019 (2023) arXiv:2211.05725

Universidad de Valladolid

Device dependent QKD

- Alice and Bob share an untrusted quantum state. They make measurmeents on it with characterized measurement devices.
- From measurements in the key basis they obtain the raw key. From measurements in the test basis they try to detect an eavesdropper.
- They perform privacy amplification in order to remove any possible correlation with an eavesdropper, and information reconciliation to remove errors in the shared key.

Calculating the key distribution rate

- The asymptotic key rate is given by

$$K \geq H(A|E) - H(A|B)$$

where

$$H(A|E) = -D(\rho_{\tilde{A}E}||\mathbb{1}_A \otimes \rho_E)$$

$$D(\rho||\sigma) = \mathrm{tr}(\rho(\log_2 \rho - \log_2 \sigma))$$

Calculating the key distribution rate

- Analytical answers are known only for simple cases.
- Numerical approaches either give subotimal rates or are too cumbersome.
- An effective numerical technique was recently discovered for the device-independent case. Can we adapt it? (Brown et al., arXiv:2106.13692)

The idea behind it

$$\log(x) = \int_0^1 \mathrm{d}t \, \frac{x-1}{t(x-1)+1}$$

Gauss-Radau quadrature:

$$\int_0^1 \mathrm{d}t \, \frac{x-1}{t(x-1)+1} \geq \sum_{i=1}^{m} w_i \frac{x-1}{t_i(x-1)+1}$$

Pusz and Woronowicz, *Rep. Math. Phys.* (1975):

$$D(\rho||\sigma) \leq -\sum_{i=1}^{m} \frac{w_i}{t_i \log 2}$$
$$\inf_{Z_i} \left(1 + \mathrm{tr}\left[\rho(Z_i + Z_i^\dagger + (1-t_i)Z_i^\dagger Z_i)\right] + t_i \,\mathrm{tr}\left(\sigma Z_i Z_i^\dagger\right)\right)$$

Turning it into an SDP

- This is a non-commutative polynomial optimisation problem with dimension restriction.
- The NV hierarchy can solve it, but that's very inefficient.
- Instead, we use a block matrix version of NPA. Since it doesn’t have commutation constraints, it converges on the first level. (Navascués et al. 2014, arXiv:1308.3410)

The resulting SDP

$$\min_{\sigma,\{\zeta_i^a,\eta_i^a,\theta_i^a\}_{a,i}} c_m + \sum_{i=1}^{m}\sum_{a=0}^{n-1} \frac{w_i}{t_i \log 2} \operatorname{tr}\left[(A_0^a \otimes \mathbb{1}_B)\left(\zeta_i^a + \zeta_i^{a\dagger} + (1-t_i)\eta_i^a\right) + t_i\theta_i^a\right]$$

$$\text{s.t.} \quad \operatorname{tr}(\sigma) = 1, \quad \forall k \ \operatorname{tr}(E_k\sigma) = f_k$$

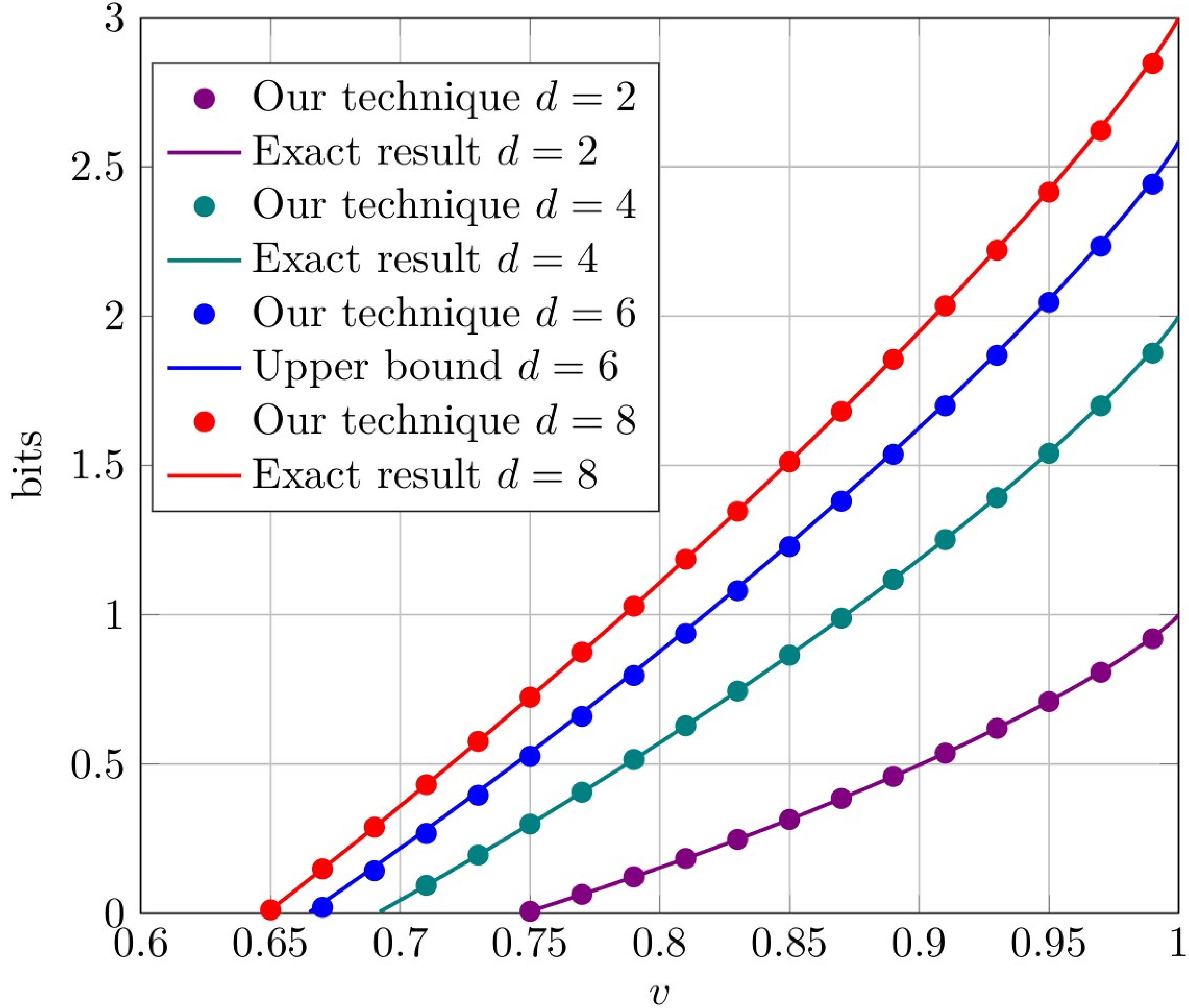
$$\forall a,i \quad \Gamma^1_{a,i} := \begin{pmatrix} \sigma & \zeta_i^a \\ \zeta_i^{a\dagger} & \eta_i^a \end{pmatrix} \geq 0, \quad \Gamma^2_{a,i} := \begin{pmatrix} \sigma & \zeta_i^{a\dagger} \\ \zeta_i^a & \theta_i^a \end{pmatrix} \geq 0.$$

$\{A_0^a\}_{a=0}^{n-1}$ are Alice's POVMs for the key basis,
E_k are the joint POVMS for the test bases, and
f_k the obtained probabilities.

Numerical results

MUBs protocol

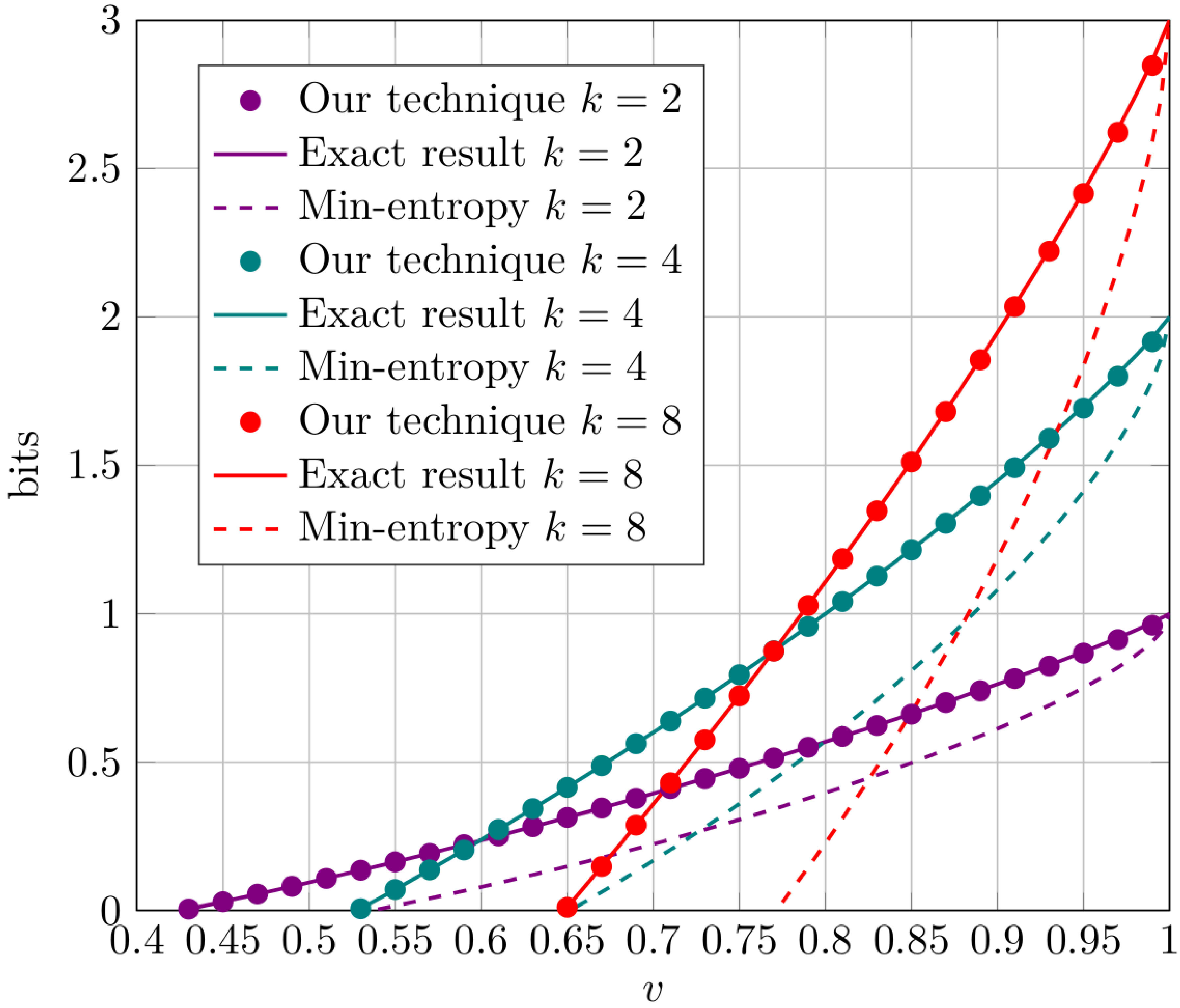
- Alice and Bob measure $d+1$ mutually unbiased bases in dimension d, use full data to compute the key rate.
- Previously the key rate could be computed only for prime d using a subset of the data. (Sheridan and Scarani 2010, arXiv:1003.5464)



Our technique d = 2
Exact result d = 2
Our technique d = 4
Exact result d = 4
Our technique d = 6
Upper bound d = 6
Our technique d = 8
Exact result d = 8
bits
v
0
0.5
1
1.5
2
2.5
3
0.6
0.65
0.7
0.75
0.8
0.85
0.9
0.95
1

MUBs in subspaces protocol

- Alice and Bob partition their Hilbert space into d/k subspaces of dimension k. They first check whether they are in the same subspace. If they are not, discard the round. Otherwise, proceed with the MUB protocol in that subspace.
- Previously the key rate was computed using the min-entropy. (Doda et al. 2021, arXiv:2004.12824)

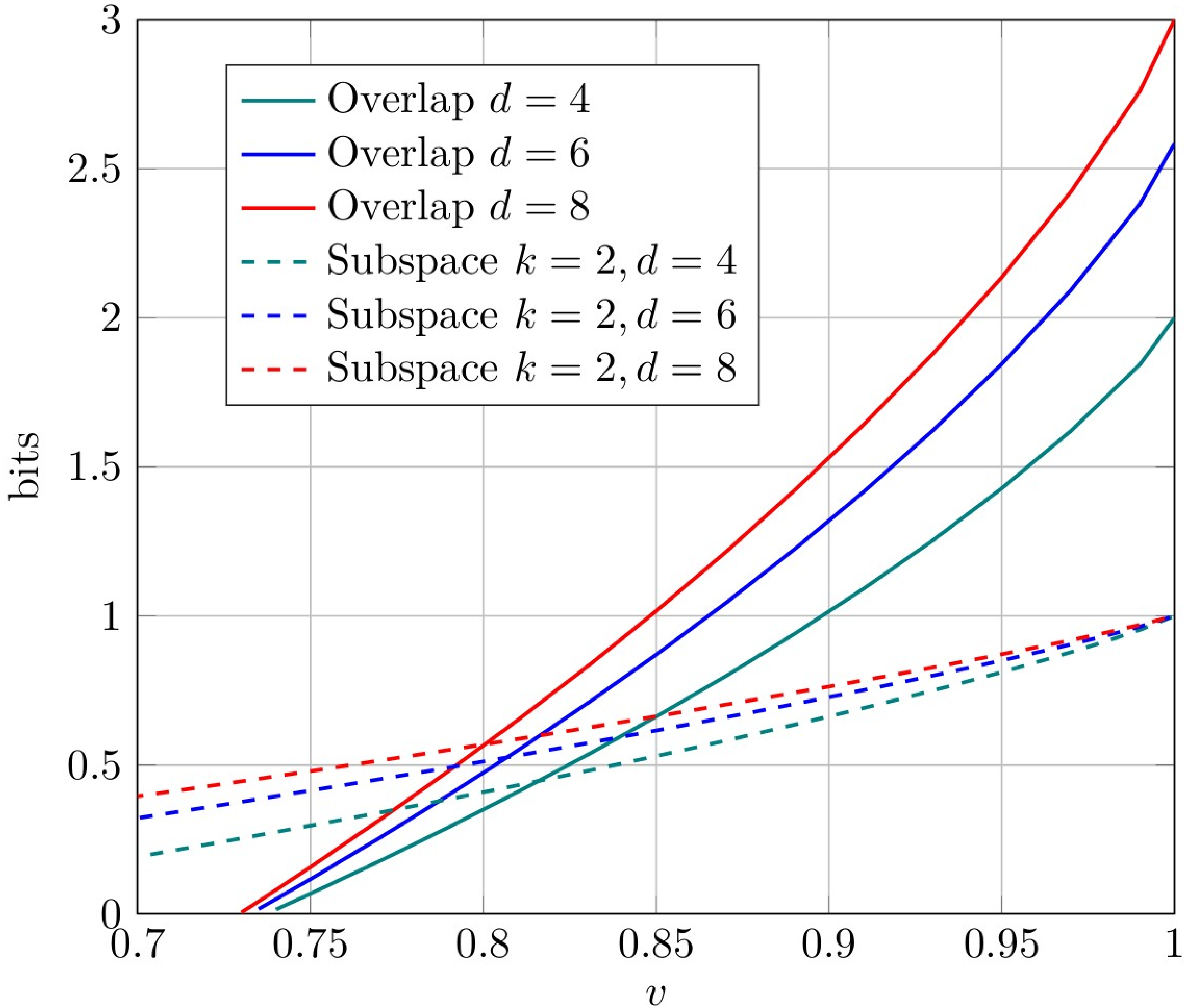


Our technique $k = 2$
Exact result $k = 2$
Min-entropy $k = 2$
Our technique $k = 4$
Exact result $k = 4$
Min-entropy $k = 4$
Our technique $k = 8$
Exact result $k = 8$
Min-entropy $k = 8$
bits
v
0
0.5
1
1.5
2
2.5
3
0.4
0.45
0.5
0.55
0.6
0.65
0.7
0.75
0.8
0.85
0.9
0.95
1

Overlapping bases protocol

- Alice and Bob measure a set of bases that only has superpositions of nearest neighbours. This is specially appropriate for experimental setups using time-bin qudits.
- For d=4 the bases are:

$$\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$$
$$\{|0\rangle + |1\rangle, |0\rangle - |1\rangle, |2\rangle + |3\rangle, |2\rangle - |3\rangle\}$$
$$\{|0\rangle, |1\rangle + |2\rangle, |1\rangle - |2\rangle, |3\rangle\}$$



Overlap $d = 4$
Overlap $d = 6$
Overlap $d = 8$
Subspace $k = 2, d = 4$
Subspace $k = 2, d = 6$
Subspace $k = 2, d = 8$
bits
v
0
0.5
1
1.5
2
2.5
3
0.7
0.75
0.8
0.85
0.9
0.95
1

Under the carpet

Dealing with experimental data

- How do we obtain the probabilities f_k needed for the SDP? Measuring them experimentally is fundamentally impossible.
- We measure relative frequencies, and with them we estimate that the probabilities are within some region with some level of confidence.
- We need to modify the SDP to minimize the key rate over the confidence region.

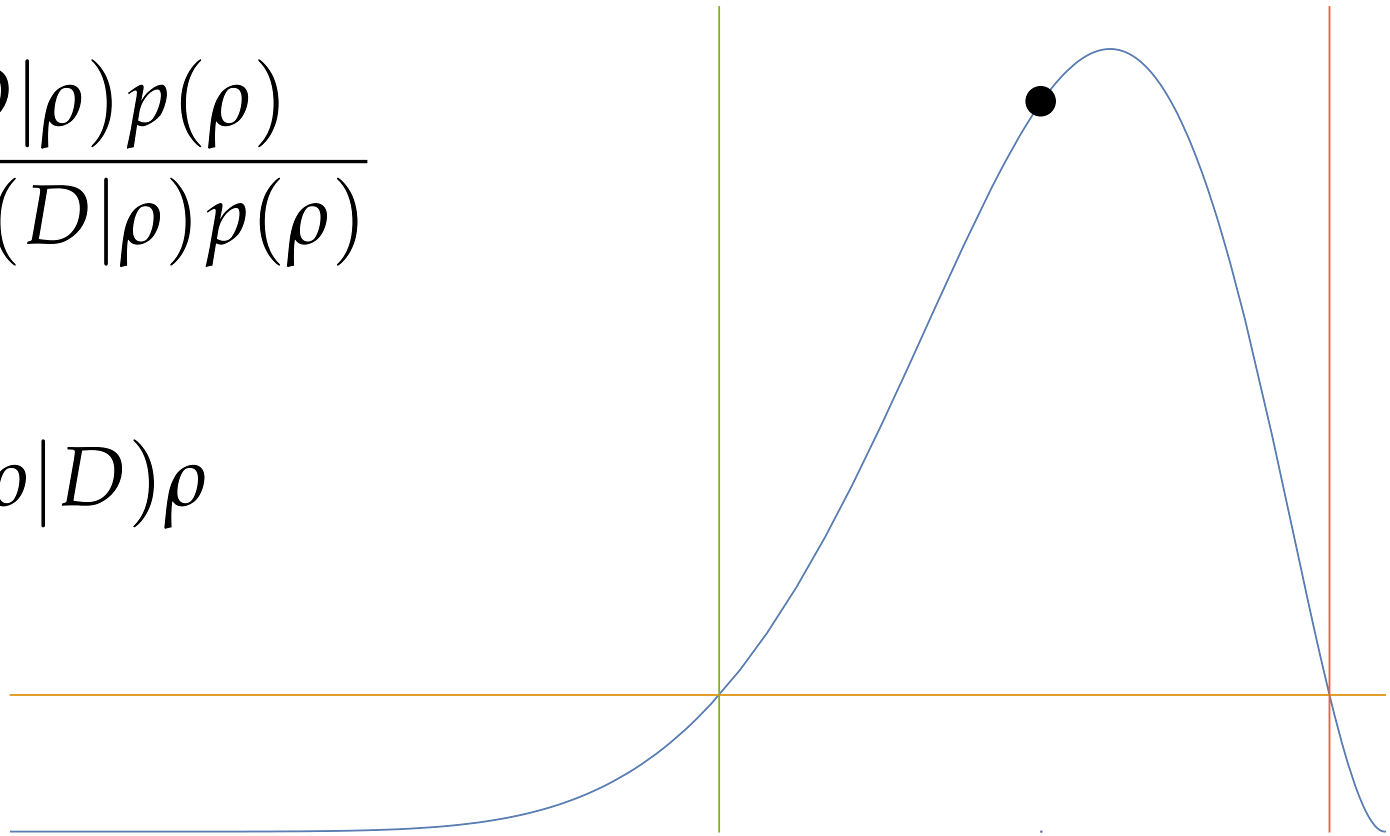
Calculating the confidence region

- We estimate the probabilities via Bayesian parameter estimation, as it naturally provides a confidence region in the form of the high-density posterior.
- Computing it analytically is feasible only in extremely simple scenarios.
- There exists a numerical technique – particle filtering – but it has exponential complexity.

Bayesian parameter estimation

$$p(\rho|D) = \frac{p(D|\rho)p(\rho)}{\int \mathrm{d}\rho\, p(D|\rho)p(\rho)}$$

$$\tilde{\rho} = \int \mathrm{d}\rho\, p(\rho|D)\rho$$



$$S_\gamma = \{\rho; p(\rho|D) \geq \gamma\}$$

$$\int_{S_\gamma} \mathrm{d}\rho\, p(\rho|D) \geq (1-\alpha)$$

Example

- Tomograph $|0\rangle$ from 10 measurements in the Z and X bases, with results 10 and 4.

$$p(D|\rho) = p_z^{10} p_x^4 (1 - p_x)^6$$

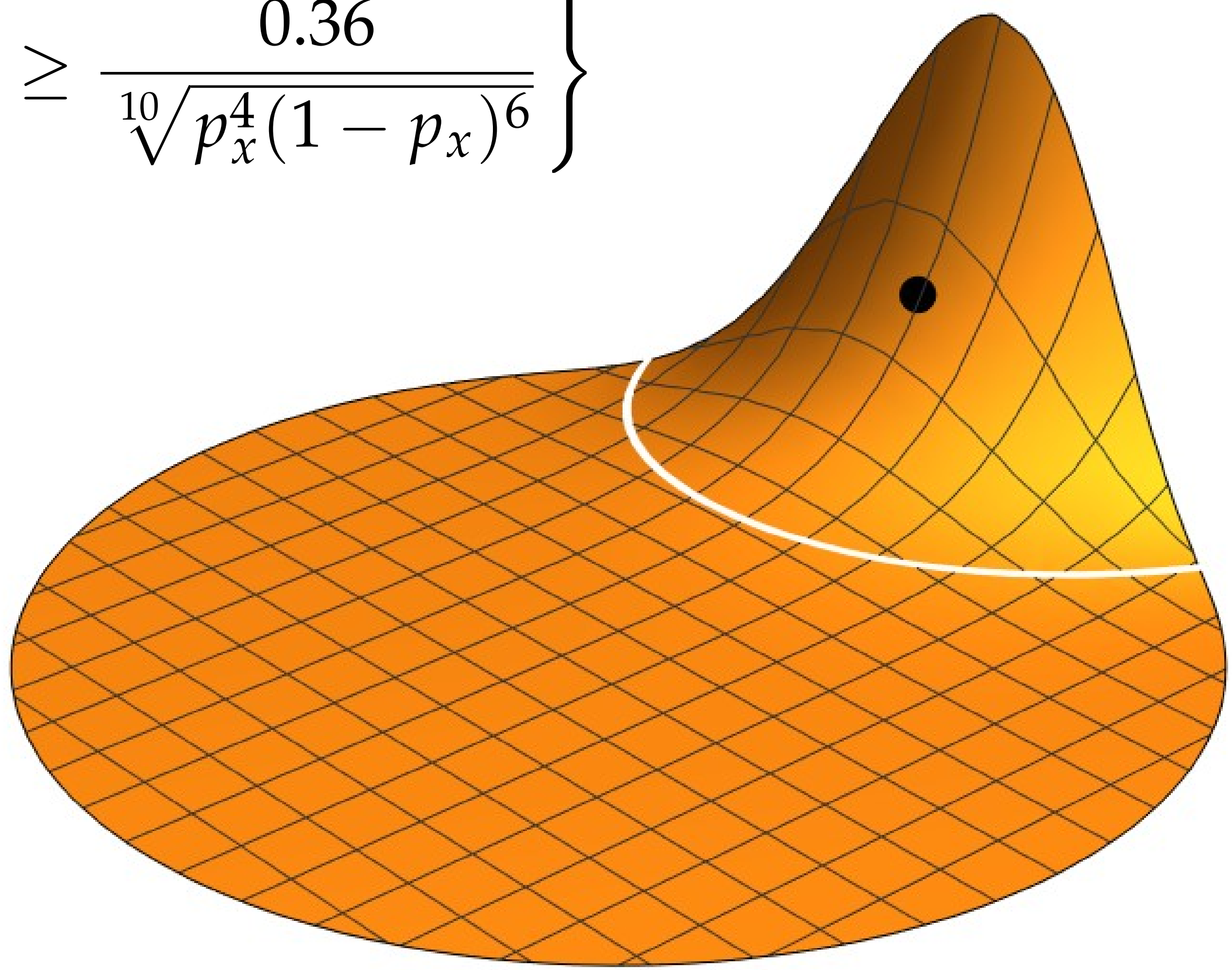
$$p(\rho) = \left[(2p_x - 1)^2 + (2p_z - 1)^2 \leq 1 \right]$$

$$\int_0^1 \mathrm{d}p_x \int_{\frac{1-\sqrt{1-(2p_x-1)^2}}{2}}^{\frac{1+\sqrt{1-(2p_x-1)^2}}{2}} \mathrm{d}p_z \, p_z^{10} p_x^4 (1 - p_x)^6 \approx 3.06 \times 10^{-5}$$

$$p(\rho|D) = 32644 p_z^{10} p_x^4 (1 - p_x)^6$$

$$\tilde{\rho} = \int \mathrm{d}\rho\, p(\rho|D)\rho = (\tilde{p}_x, \tilde{p}_z) \approx (0.44, 0.90)$$

$$C_{0.05} = \left\{ (p_x, p_z); \quad p_z \geq \frac{0.36}{\sqrt[10]{p_x^4 (1 - p_x)^6}} \right\}$$



Our method

- Approximate the likelihood function by a Gaussian.
- Estimate the mean and confidence region via Monte Carlo sampling.
- The resulting confidence region is the intersection of an ellipsoid with the quantum state space, which is SDP-representable.

Gaussian approximation

$$p(D|\rho) = \frac{n!}{\prod_i k_i!} \prod_i \mathrm{tr}(\rho E_i)^{k_i}$$

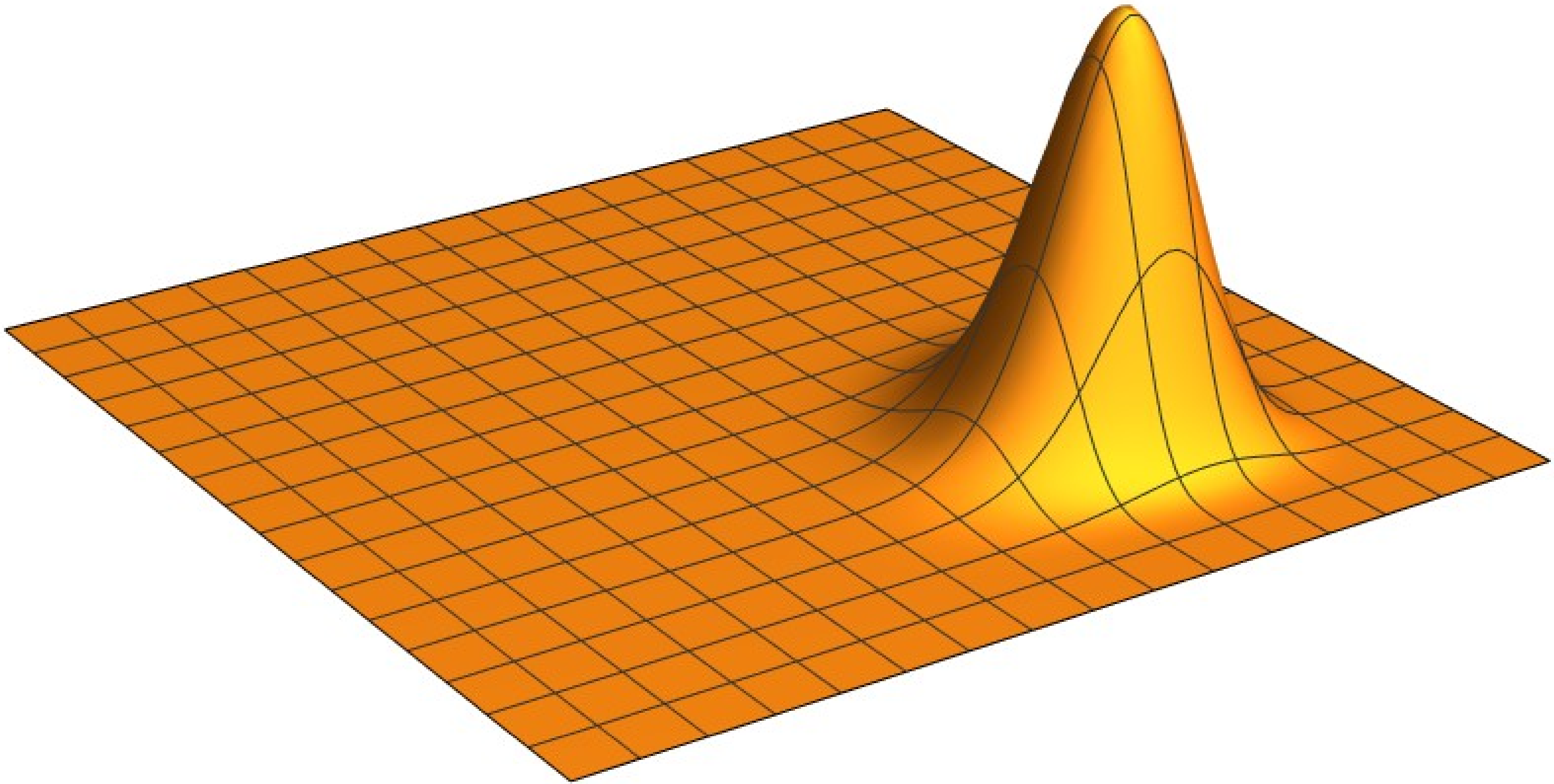
$$p(D|\rho) \approx \frac{1}{\sqrt{\det 2\pi n^2 \Sigma}} \exp\Big(-(\vec{x} - \vec{\mu})\Sigma^{-1}(\vec{x} - \vec{\mu}) \Big)$$

$$x_i := \mathrm{tr}(\rho E_i)$$

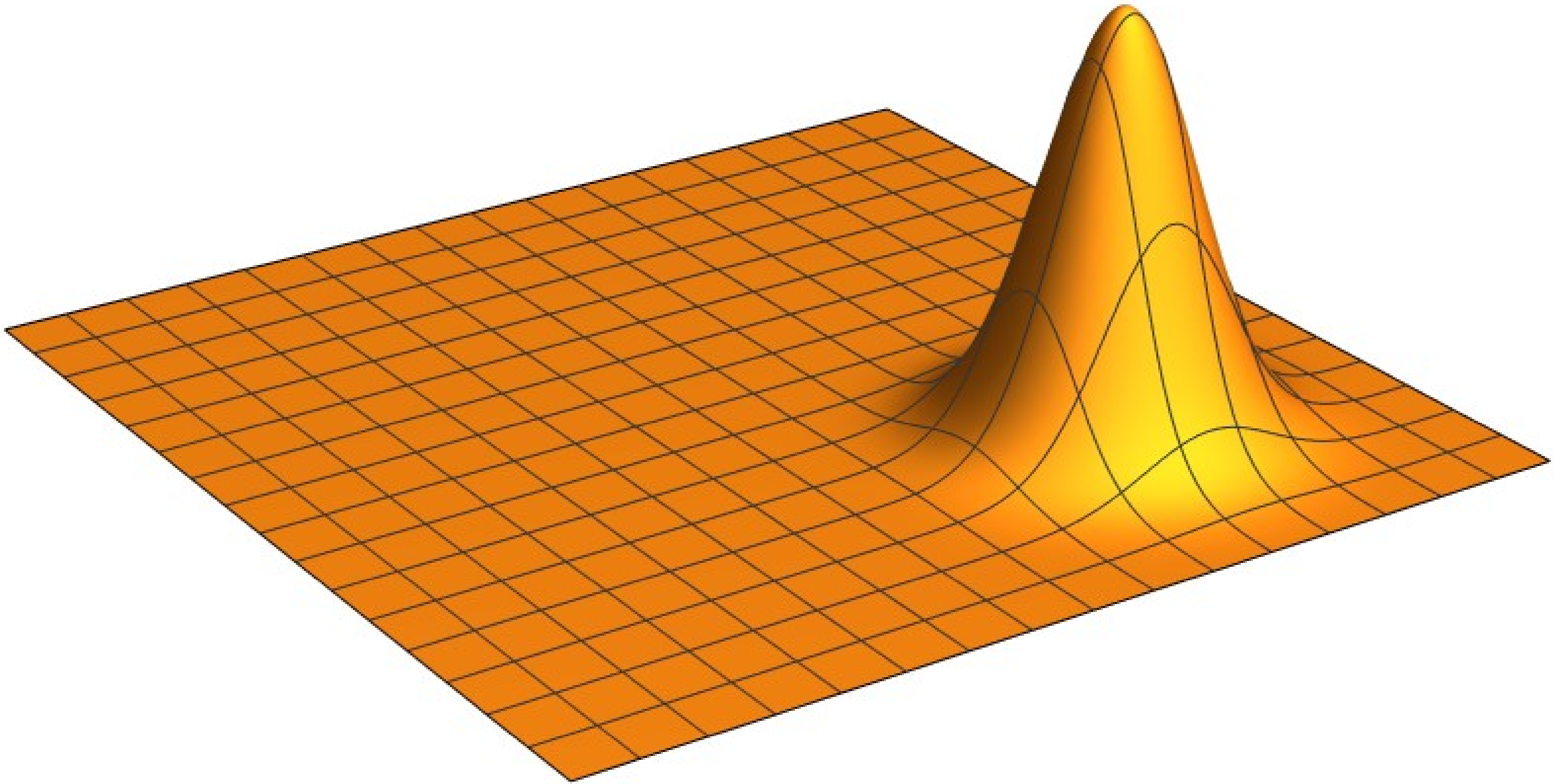
$$\mu_i := \frac{k_i}{n}$$

$$\Sigma_{ij} := \begin{cases} \frac{\mu_i(1-\mu_i)}{n} & \text{if } i = j \\ -\frac{\mu_i \mu_j}{n}, & \text{if } i \neq j \end{cases}$$

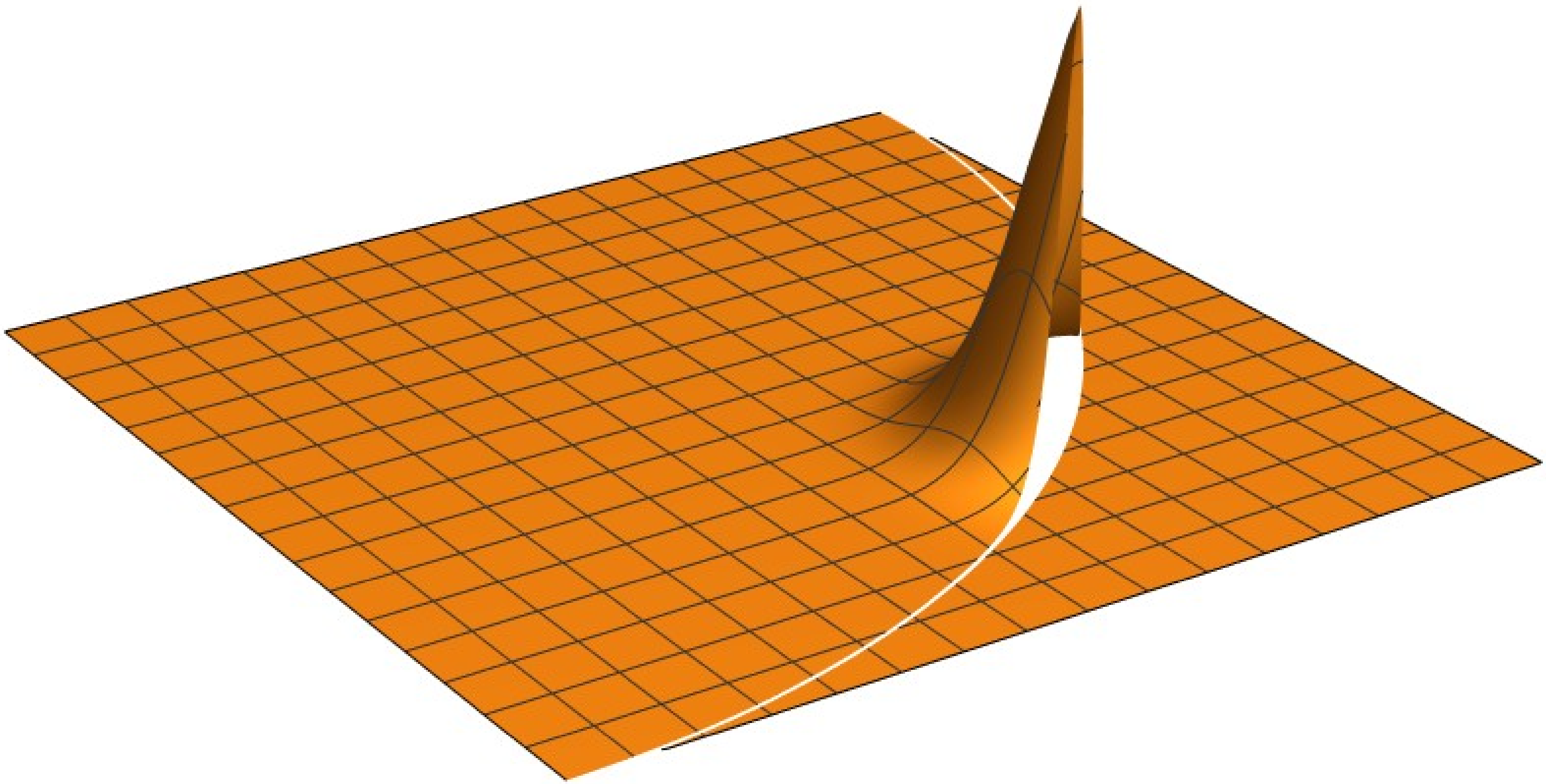
Likelihood



Gaussian approximation



Posterior



Modified SDP

$$\min_{\sigma,\boldsymbol{p},\{\zeta_i^a,\eta_i^a,\theta_i^a\}_{a,i}} c_m + \sum_{i=1}^{m}\sum_{a=0}^{n-1}\frac{w_i}{t_i\log 2}\,\mathrm{tr}\Big[(A_0^a\otimes \mathbb{1}_B)\Big(\zeta_i^a+\zeta_i^{a\dagger}+(1-t_i)\eta_i^a\Big)+t_i\theta_i^a\Big]$$

$$\text{s.t.}\quad \mathrm{tr}(\sigma)=1,\quad \mathrm{tr}(\boldsymbol{E}\sigma)=\boldsymbol{p},\quad \Big\langle \boldsymbol{p}-\boldsymbol{f},\Sigma^{-1}(\boldsymbol{p}-\boldsymbol{f})\Big\rangle\le\chi^2$$

$$\forall a,i\quad \Gamma^1_{a,i}:=\begin{pmatrix}\sigma & \zeta_i^a\\ \zeta_i^{a\dagger} & \eta_i^a\end{pmatrix}\ge 0,\quad \Gamma^2_{a,i}:=\begin{pmatrix}\sigma & \zeta_i^{a\dagger}\\ \zeta_i^a & \theta_i^a\end{pmatrix}\ge 0.$$

$\boldsymbol{f}$ is the vector of frequencies, $\boldsymbol{p}$ the vector of probabilities, Σ the covariance matrix, and χ the size of the confidence region.

Conclusion

- We developed an efficient and easy to use SDP hierarchy for computing key rates. It can handle real experimental data.
- Future directions include adapting it to protocols with different security assumptions, that overcome limitations of vanilla QKD, such as MDI QKD and twin-field.


Thanks for your attention!