Characterising the photon-number distribution of quantum channels with double-decoy method and its application to quantum cryptography

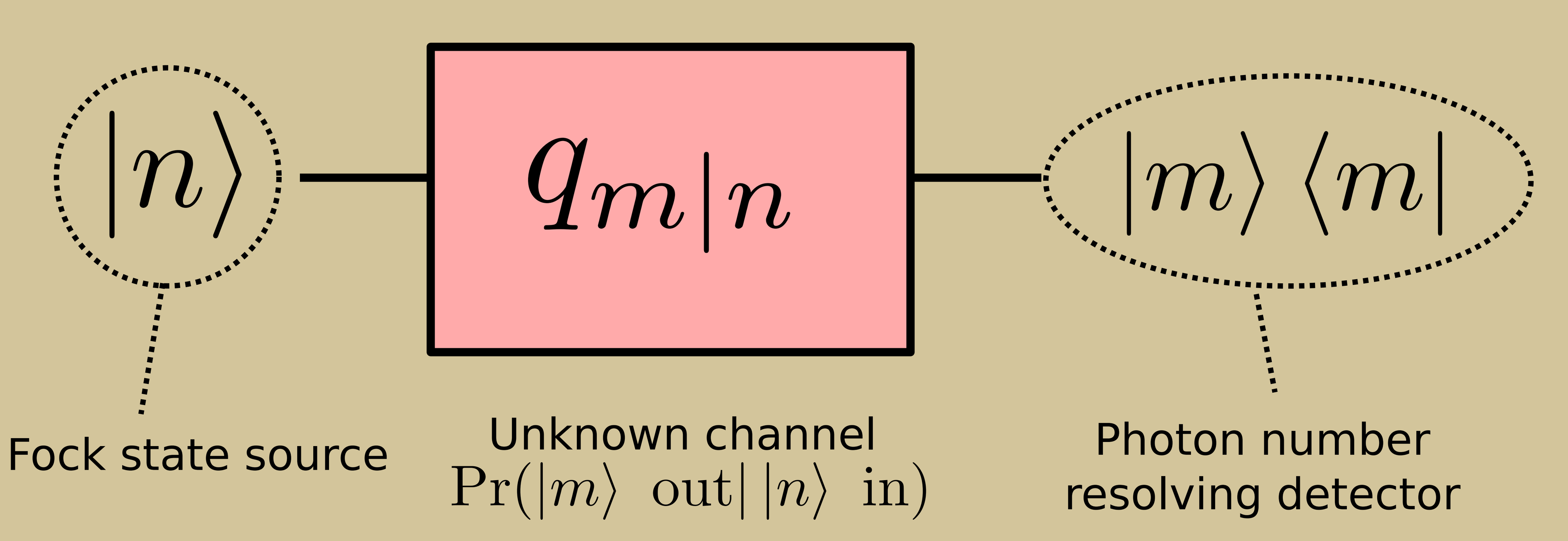
Emilien Lavie[1*], Ignatius William Primaatmaja[2], Charles Ci Wen Lim[12]

1 Department of Electrical & Computer Engineering, National University of Singapore
2 Centre for Quantum Technologies, National University of Singapore
* emilien.lavie@u.nus.edu

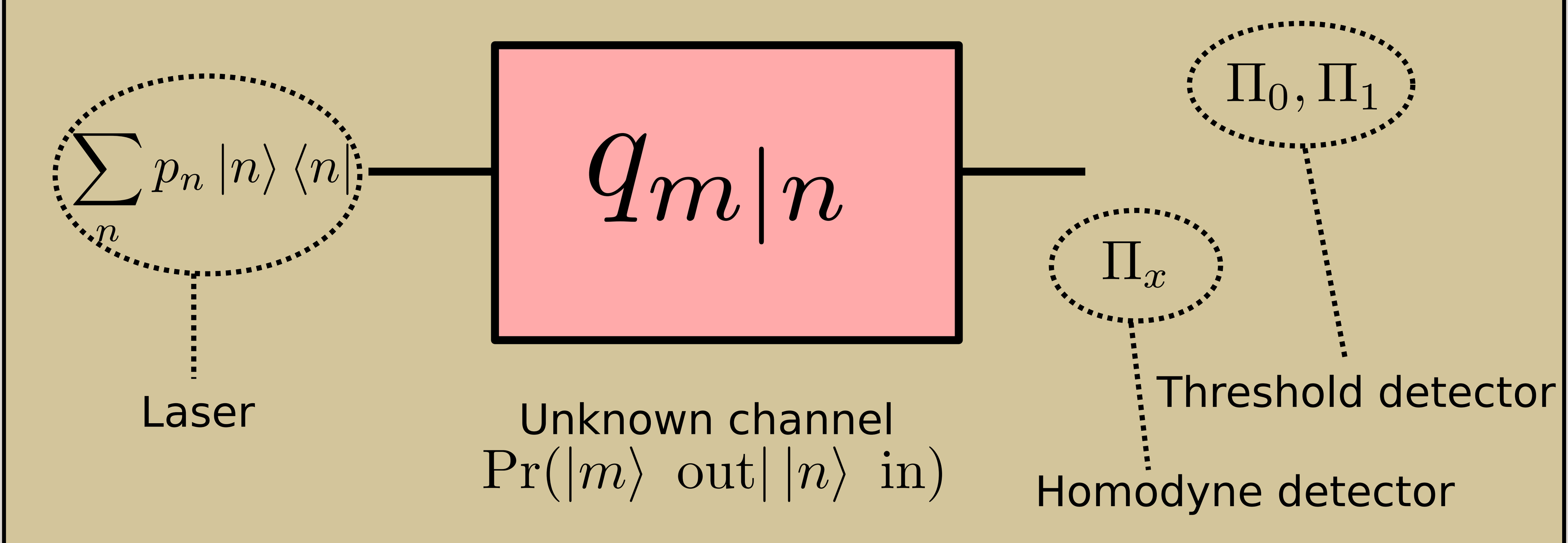
Introduction

In theory, we can compute the effect of an unknown channel using exact photon number states and photon number resolving detectors.
Practically, we want to do the same using only conventional laser source and common noisy detectors (device dependent case).
We generalised the decoy states[ab] method to "double decoy" with both source and detector modulation and broadened its scope of application.

Ideal hardware



Real hardware



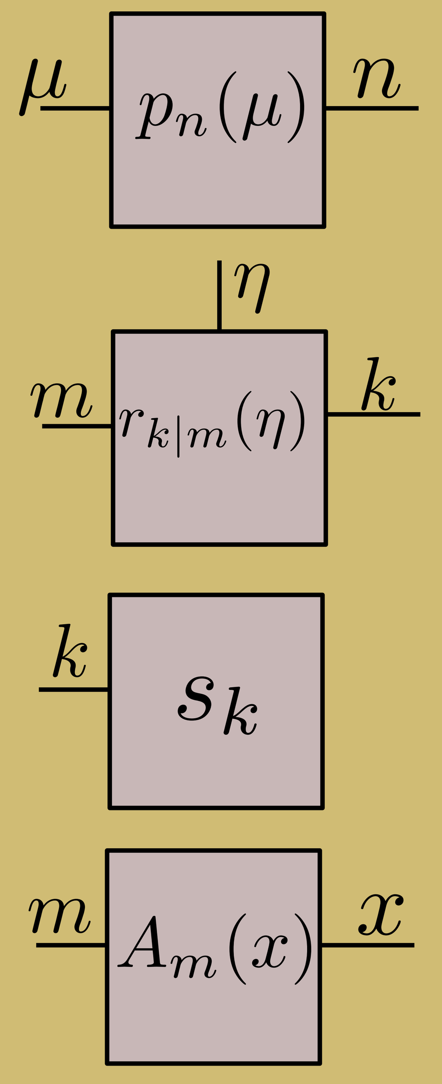
Tensor network modeling

Poissonian light source $\quad p_n(\mu) = e^{-\mu}\dfrac{\mu^n}{n!}$

Loss Intensity modulator $\quad r_{k|m}(\eta) = \binom{m}{k}\eta^k(1-\eta)^{m-k}$

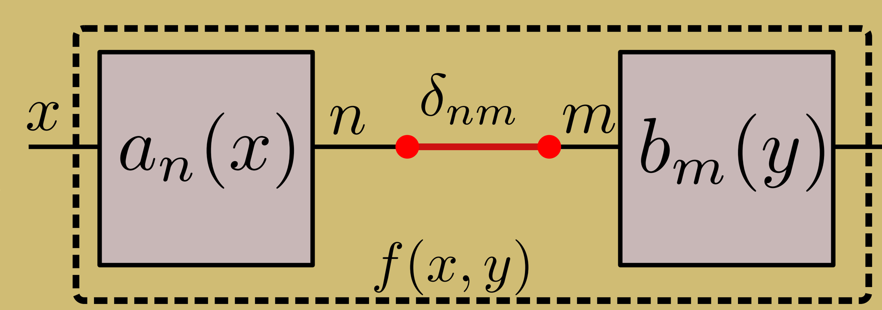
Threshold detector $\quad s_k = \begin{cases} p_{\mathrm{dc}}, & \text{if } k=0 \\ 1 & \text{otherwise} \end{cases}$

Homodyne detector[c] $\quad A_m(x) = |\langle x|m\rangle|^2$

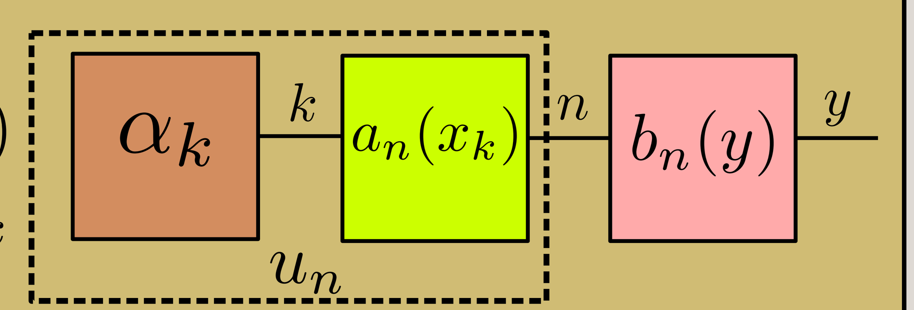


Recomputing probabilities

Contraction of indices - wiring
$f(x,y) = \sum_{nm} a_n(x) b_m(y) \delta_{nm}$



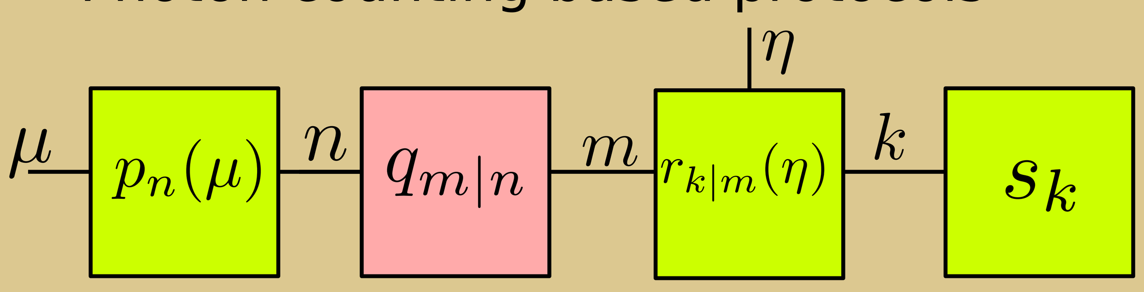
We can recompute $b_{n^*}(y)$
using $f(x_0, y), \ldots, f(x_{n_0}, y)$
We choose real numbers α_k
such that $u_n \approx \delta_{n=n^*}$



Eg: Take α the n^*-th column of M^{-1}
with M $= [a_i(x_j)]_{0\le i,j\le n_0}$ and bound the estimation error

Application to double decoy QKD

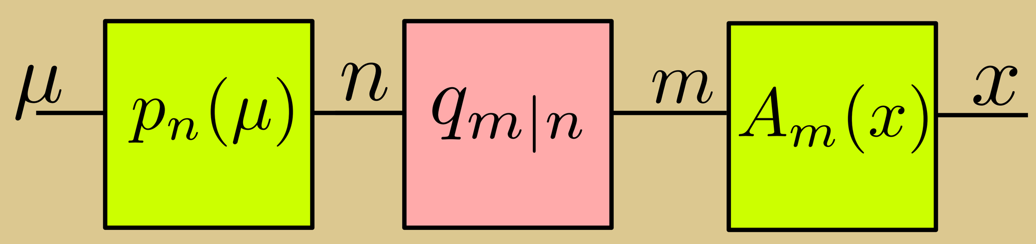
Photon counting based protocols

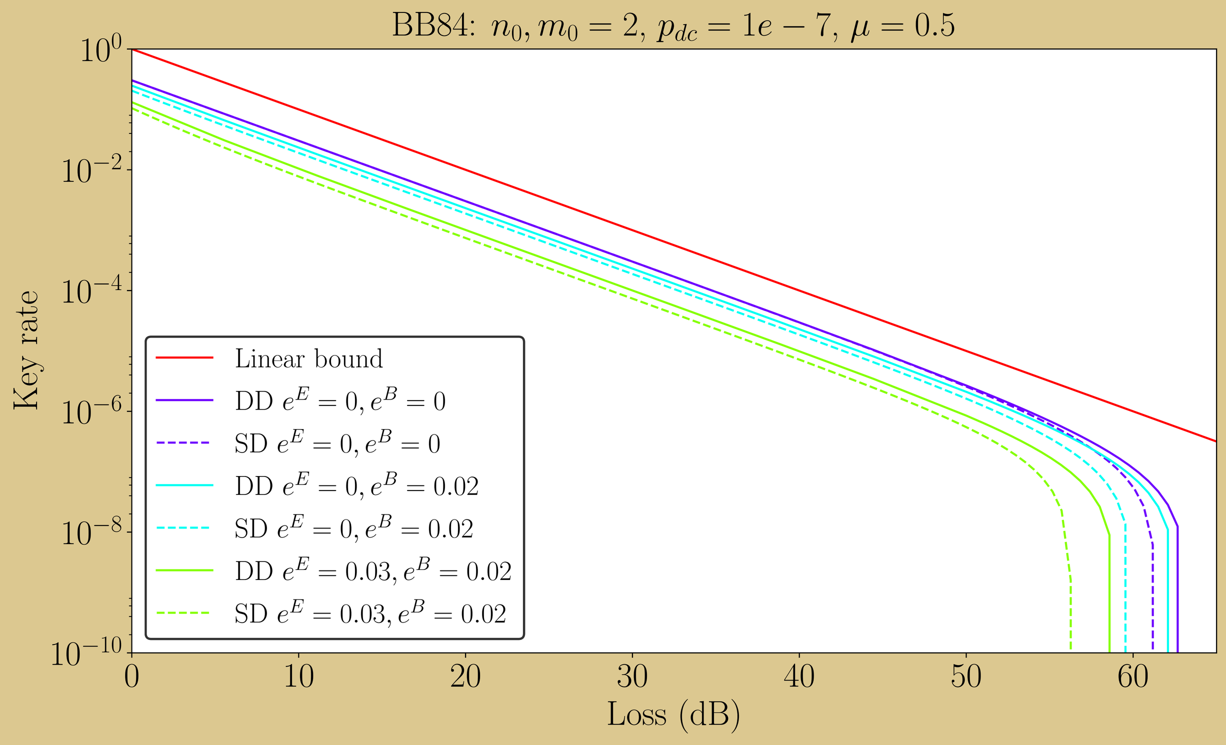


Trusted block

Untrusted block

Homodyne based protocols



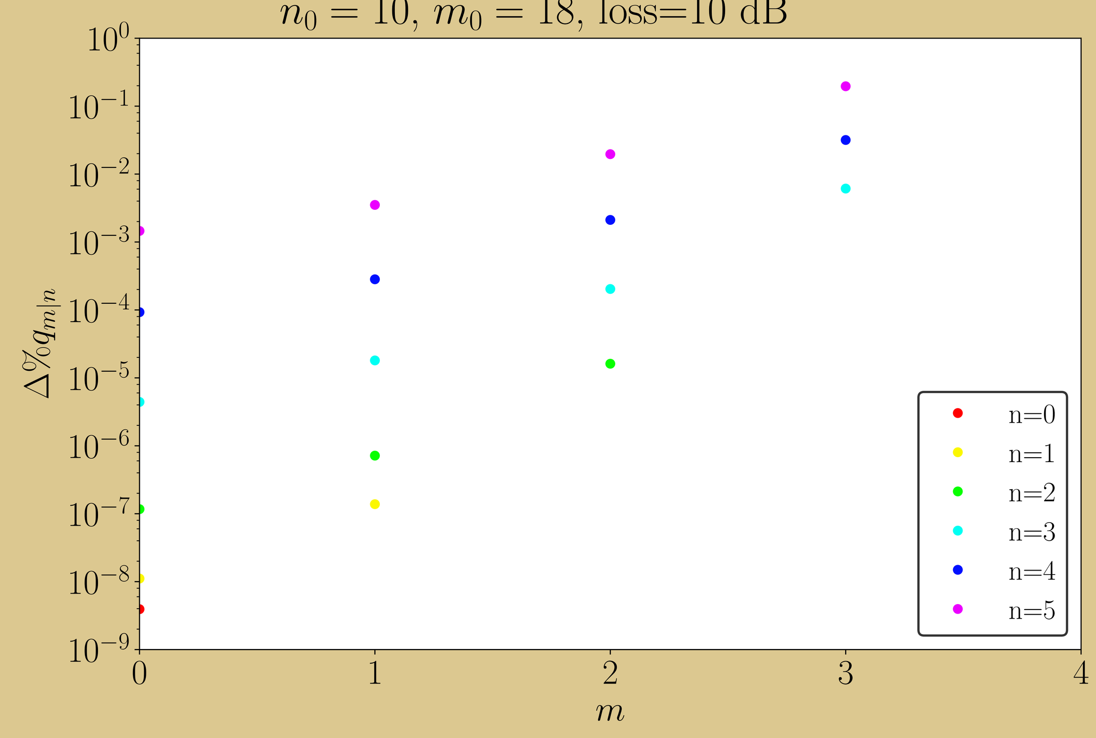


SD: Simple decoy states as in Ref. a
DD: Double decoy states, our contribution

Our error model considered independent contributions to errors:
e^E: Error introduced by Eve
e^B: Error introduced by Bob

$$K_r^{\mathrm{DD}} \ge \begin{array}{l} p_0(\mu) q_{0|0} s_0 \\ + \; p_1(\mu) q_{1|1} s_1 (1 - h_2(e^E_{1,1})) \\ - \; Q(\mu,\eta) h_2(E(\mu,\eta)) \end{array}$$

Relative error on $q_{m|n}$: $\Delta\% = \frac{q_{upp} - q_{low}}{q_{est}}$
$n_0 = 10$, $m_0 = 18$, loss=10 dB



Conclusion

Applicable to any use case requiring the estimation of average photon-number statistics of a channel
Provable upper and lower bounds without cutoff assumption, not tight in general but reasonably good up to $n, m \leqslant 3 \sim 5$
Potential other application: other crypto protocols, delegated quantum computing, sensing, quantum lidar etc

References

a H.-K. Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution,” Phys. Rev. Lett., vol. 94, no. 23, p. 230504, 2005.
b T. Moroder, M. Curty, and N. Lütkenhaus, “Detector decoy quantum key distribution,” New J. Phys., vol. 11, no. 4, p. 045008, 2009.
c S. M. Tan, “An inverse problem approach to optical homodyne tomography,” Journal of Modern Optics, vol. 44, no. 11–12, pp. 2233–2259, 1997.