Optimization Problem

- Variables: the elements in Eve's matrix

$$M_E = \left(a_{i,j}\right)_{(n^m)\times(n^m)}$$

- Goal: the maximal total phase error rate in a block

$$P_{\max}^{ph} = \max\left(\sum_{l=1}^{n-1} P_l^{ph} / P^{eff}\right)$$

- Constraints:
  - Matrix requirements $|a_{i,j}| \le 1$
  - Channel efficiency in every time slot is $\eta/(n\text{-}1)$

$$P_l^{eff} = \eta/(n-1), \forall l \in \{1,\cdots,n-1\}$$

  - Bit error rate in every time slot is e_b

$$P_l^{bit} / P_l^{eff} = e_b, \forall l \in \{1,\cdots,n-1\}$$

Optimization Range

- Typical values for our optimization
  - m = 2~4
  - n = 8~20
  - e_b = 1%~4%
  - η = 1e-2~1e-5
- Calculation takes an order of $2^n n^m$

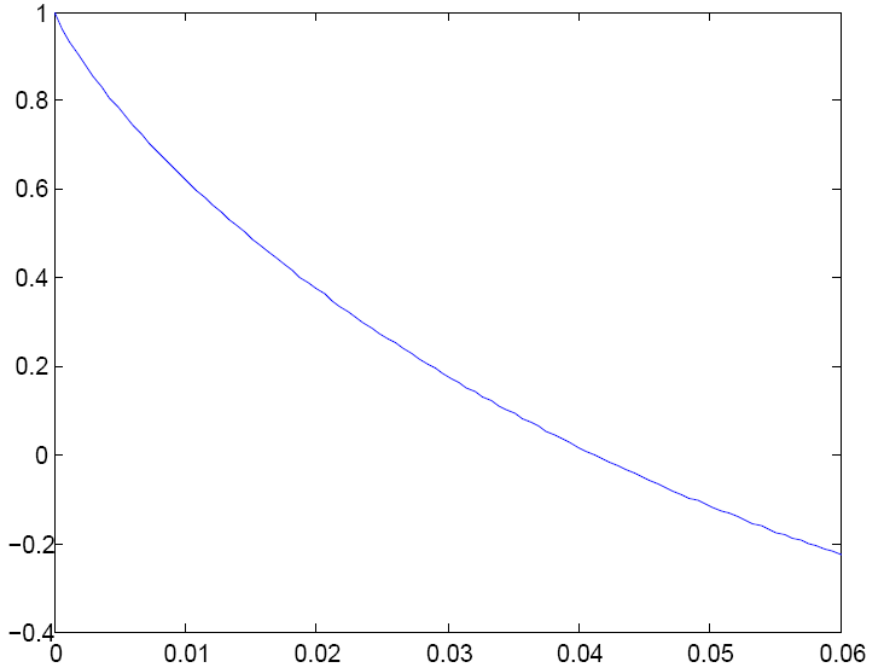
Analytical Result for [1,n] DPS-QKD

- Bit error rates:

$$p_l^{bit} = \frac{1}{4n}[|a_{l-1,l-1} - a_{l,l}|^2 + |a_{l-1,l} - a_{l,l-1}|^2 + (|a_{l-1,1}|^2 + \cdots + |a_{l-1,l-2}|^2 + |a_{l-1,l+1}|^2 + \cdots + |a_{l-1,n}|^2) + (|a_{l,1}|^2 + \cdots + |a_{l,l-2}|^2 + |a_{l,l+1}|^2 + \cdots + |a_{l,n}|^2)],$$

- Phase error rates:

$$p_l^{ph} = \frac{1}{2n}[|a_{l,1}|^2 + \cdots + |a_{l,l-1}|^2 + |a_{l-1,l}|^2 + \cdots + |a_{l-1,n}|^2]$$



- The relation between two types:

$$P^{ph} \le (3+\sqrt{5})P^{bit}$$

- Secure key generation rate:

$$R \ge 1 - H(e_b) - H\left((3+\sqrt{5})e_b\right)$$

  - Unconditional secure if e_b <= 4.12%
- Observe the expressions
  - Both constraints and goals are quadratic.
  - Non-convex problem.
  - Variables can be reduce to real numbers.

K. Wen, K. Tamaki and Y. Yamamoto, arXiv:0806.2684 (2008)

Multiple-photon cases

- Multiple-photon: $m>1$
- Nonlinear optimization, using optimization solver KNITRO on NEOS server
  - Only find the local maxima
- Reduce the dimension of the variables
  - Complex->Real variables (?)
  - Dimension of the matrix: $n^m \times n^m \rightarrow n \times n^m$
- Precalculate all the matrices and load them as the data file in AMPL.
- Use sparse matrices to reduce the memory consumption.

[2,8] DPS-QKD Result

- KNITRO output
  - dps_2_8_interp.txt
  - About 2-3 hours
- The properties of the result
  - P^{ph} / P^{eff} only depends on P^{bit} / P^{eff} , rather than the absolute values.
  - The maxima should be at the constraint boundary.
- Typical experiment has e_b >= 1%.