Practical long-distance quantum communication via concatenated entanglement swapping

Aeysha Khalique
&
Barry C. Sanders

September 7, 2016

Alberta Innovates Technology Futures

NSERC CRSNG

千人計劃

RECRUITMENT PROGRAM OF GLOBAL EXPERTS

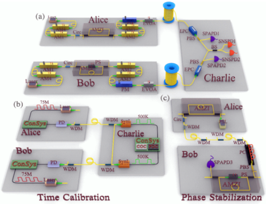
WESTGRID

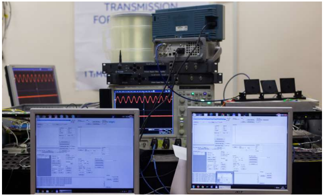
AK Tittel Sanders *PRA* **88** 022336 (2013)
AK Sanders *PRA* **90** 032304 (2014)
AK Sanders *JOSAB* **32** 2382 (2015)

Long-distance quantum communication

http://goo.gl/RNDB6t

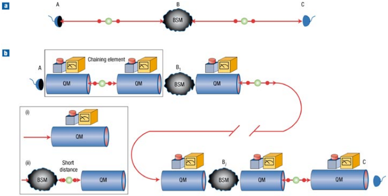
Long-distance quantum communication





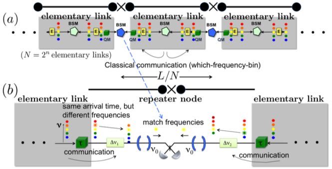
http://goo.gl/IL95bJ

200 km QKD: Tang et al. *PRL* (2014) 250 km QKD: Gleim et al. *OE* (2016)

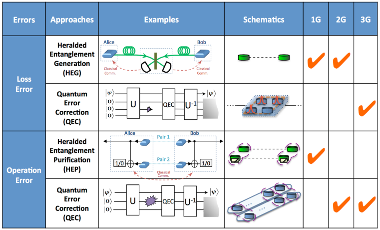


Gisin & Thew *Nature Photon.* (2007)

Modeling Repeaters

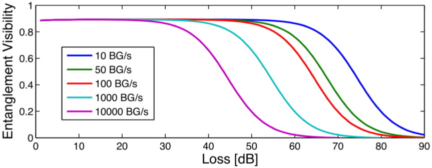


Guha et al. *PRA* (2015)



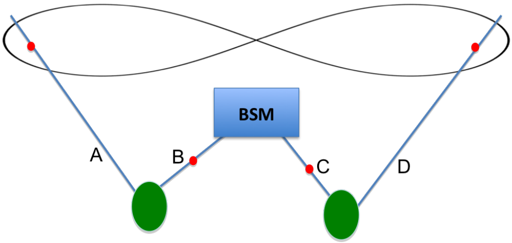
Errors	Approaches	Examples	Schematics	1G	2G	3G
Loss Error	Heralded Entanglement Generation (HEG)			✔	✔	
	Quantum Error Correction (QEC)					✔
Operation Error	Heralded Entanglement Purification (HEP)			✔		
	Quantum Error Correction (QEC)				✔	✔

Muralidharan et al. *Sci. Rep.* (2015)



Bourgoin et al. *NJP* (2013)

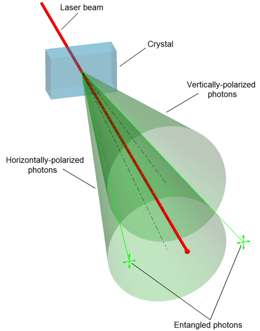
Entanglement swapping



$$\left|\psi^+\right\rangle_{\mathrm{AB}}\left|\psi^+\right\rangle_{\mathrm{CD}} = \frac{1}{2}\Big[\left|\psi^+\right\rangle_{\mathrm{AD}}\left|\psi^+\right\rangle_{\mathrm{BC}} + \left|\psi^-\right\rangle_{\mathrm{AD}}\left|\psi^-\right\rangle_{\mathrm{BC}} + \left|\phi^+\right\rangle_{\mathrm{AD}}\left|\phi^+\right\rangle_{\mathrm{BC}} + \left|\phi^-\right\rangle_{\mathrm{AD}}\left|\phi^-\right\rangle_{\mathrm{BC}}\Big]$$

Zukowski Zeilinger Horne Ekert *PRL* (1993)

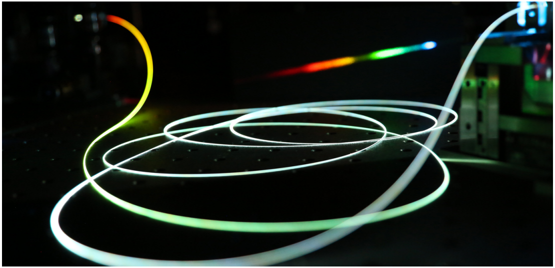
Source



http://goo.gl/AvIyW8

$$|\chi\rangle = e^{i\chi\left(\hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger}+\mathrm{hc}\right)}|\mathrm{vac}\rangle = \operatorname{sech}^2\chi e^{i\tanh\chi\left(\hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger}+\hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger}\right)}|\mathrm{vac}\rangle$$

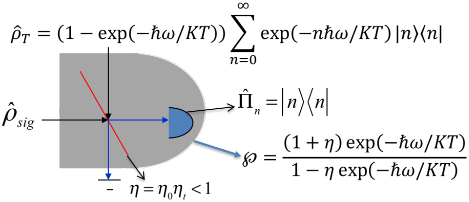
Channel



http://goo.gl/40gB72

$$\eta_t = \mathrm{e}^{-(\alpha\ell+\alpha_0)/10}$$

Detector



http://goo.gl/EJY6wj

$$P\left(q=0|i\right) = \left(1-\wp\right)\left[1-\eta\left(1-\wp\right)\right]^i = 1 - P\left(q=1|i\right)$$

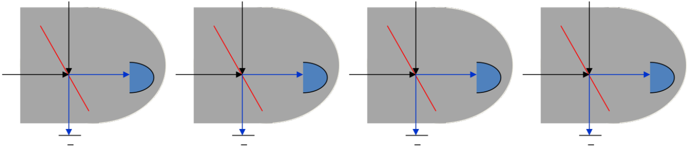
Rohde Ralph *J. Mod. Opt.* (2006)

PNR Detectors

$$
\begin{aligned}
P(q|i) =& \frac{(1-\eta)(1-\wp)}{1-\eta(1-\wp)} \left(\frac{\eta}{1-\eta}\right)^q (1-\eta)^i G(i,q;\eta,\wp) \quad \text{for } i \geq q \\
=& \frac{(1-\eta)(1-\wp)}{1-\eta(1-\wp)} \left[\frac{1-\eta}{\eta} b(\eta,\wp)\right]^{q-i} \eta^i G(q,i;\eta,\wp) \quad \text{for } q \geq i
\end{aligned}
$$

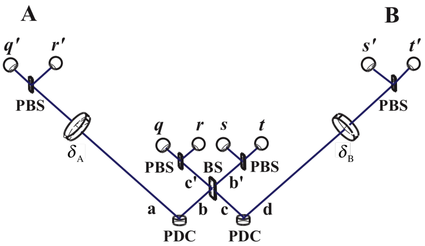
$$
\begin{aligned}
b(\eta,\zeta_{dc}) :=& \left[1+\frac{1-\eta}{\eta\wp}\right]^{-1} \\
G(\kappa,\lambda;\eta,\wp) =& \sum_{n=0}^{\infty} \binom{\kappa}{\lambda} \binom{\kappa-\lambda+n}{\kappa-\lambda} [b(\eta,\wp)]^n \\
& \times \left[{}_2F_1\left(-n,-\lambda;\kappa-\lambda+1;\frac{\eta-1}{\eta}\right)\right]^2 \quad \text{for } \kappa \geq \lambda \\
G(\kappa,\lambda;\eta,\wp) :=& 0 \quad \text{for } \kappa < \lambda
\end{aligned}
$$

Four detectors



$$P\left(qrst|ijkl\right) = P(q|i)P(r|j)P(s|k)P(t|l)$$

Ideal single swap for 2 photons @ BSM



Bell state	$(qrst)$
$\|\psi^+\rangle$	(1010) ∨ (0101)
$\|\psi^-\rangle$	(0110) ∨ (1001)
$\|\phi^\pm\rangle$	(2000) ∨ (0200) ∨ (0020) ∨ (0002)

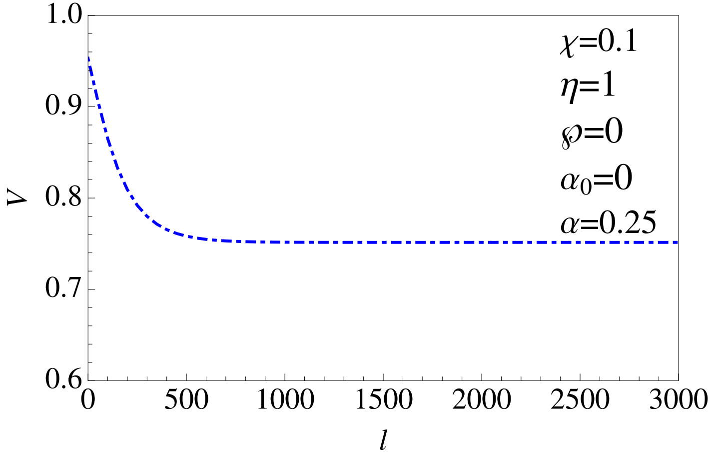
Conditional coincidence probability and visibility

$$Q(q'r's't'|qrst;\chi,\wp,\eta)$$

$$Q_{\text{ext}}(qrst) = \underset{q'r's't'}{\text{ext}}\, Q(q'r's't'|qrst;\chi,\wp,\eta)$$

$$V(\chi,\wp,\eta) = \frac{Q_{\max} - Q_{\min}}{Q_{\max} + Q_{\min}}$$

Ideal detectors



Single swap

$$|\chi\rangle_{\mathsf{AB}}|\chi\rangle_{\mathsf{CD}} \xrightarrow{\mathrm{B}^{\mathrm{inn}}} |\Xi\rangle \xrightarrow[\mathrm{Proj}]{\text{Fock}} \frac{\Pi^{\mathrm{inn}}_{ijkl}|\Xi\rangle}{\sqrt{P(ijkl)}} =: |\tilde{\Xi}\rangle^{\text{out}}_{ijkl}$$

$$P(ijkl) = \langle\Xi|\Pi^{\mathrm{inn}}_{ijkl}|\Xi\rangle$$

$$|\tilde{\Xi}\rangle^{\text{out}}_{ijkl}\langle\tilde{\Xi}| \xrightarrow[\text{noisy detection}]{\mathrm{Inner}} \rho^{\text{out}}_{qrst} = \sum P(ijkl|qrst)\,|\tilde{\Xi}\rangle^{\text{out}}_{ijkl}\langle\tilde{\Xi}|$$

$$\rho^{\text{out}}_{qrst} \xrightarrow[\text{polarization rotators}]{\text{Ideal counts on outer detectors given actual on inner}}$$

$$P(i'j'k'l'|qrst) = \langle i'j'k'l'|\,U(\delta_A)U(\delta_B)\rho^{\text{out}}_{qrst}U^{\dagger}(\delta_B)U^{\dagger}(\delta_A)\,|i'j'k'l'\rangle$$

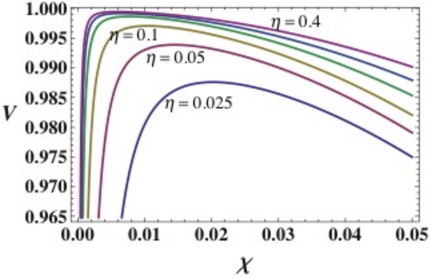
Single swap

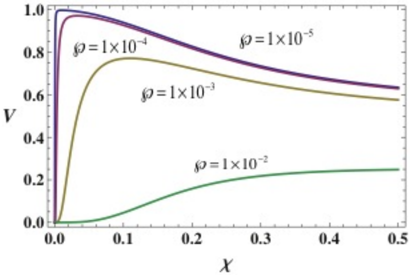
$$P(ijkl|qrst) = \frac{P(qrst|ijkl)P(ijkl)}{P(qrst)}$$
$$= P(q|i)P(r|j)P(s|k)P(t|l)P(ijkl)/P(qrst)$$

$$Q(q'r's't'|qrst) = \sum P(q'r's't'|i'j'k'l';\wp,\eta)P(i'j'k'l'|qrst;\chi,\wp,\eta)$$

Scherer Howard Sanders Tittel *PRA* (2009)

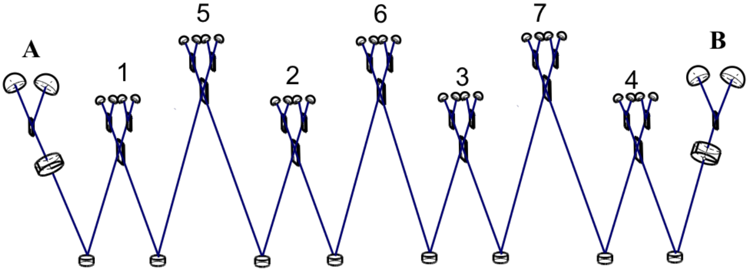
Single-swap visibility





Scherer Howard Sanders Tittel *PRA* (2009)

N swaps with $2N-1$ BSMs



$$Q_{\text{ext}}(qrst) = \underset{q'r's't'}{\text{ext}}\, Q(q'r's't'|\boldsymbol{qrst};\chi,\wp,\eta)$$

Khalique Tittel Sanders *PRA* (2013)

BSM connecting adjacent swaps

$$\Omega(\mu_n, \lambda_n, i_{N+n}, l_{N+n}) = \sum_{\gamma=0}^{\mu_n+\lambda_n} \binom{\mu_n + \lambda_n}{\gamma} \binom{i_{N+n} + l_{N+n} - \mu_n - \lambda_n}{i_{N+n} - \gamma} (-1)^{\mu_n+\lambda_n-\gamma}.$$

Closed-form solution

$$P\left(i'j'k'l'|\mathbf{qrst}\right)=\sum_{\mathbf{ijkl}}P\left(\mathbf{ijkl}|\mathbf{qrst}\right)\langle i'j'k'l'|\,U(\alpha)U(\delta)\,|\tilde{\Xi}\rangle^{\text{out}}_{\mathbf{ijkl}}\langle\tilde{\Xi}|\,U^{\dagger}(\alpha)U^{\dagger}(\delta)\,|i'j'k'l'\rangle$$

$$=\sum_{\mathbf{ijkl}}\frac{P\left(\mathbf{qrst}|\mathbf{ijkl}\right)}{P\left(\mathbf{qrst}\right)}\left(\frac{1}{\sqrt{2^{i_1+j_1+k_1+l_1}i_1!j_1!k_1!l_1!}}\frac{(\tanh\chi)^{i_1+j_1+k_1+l_1}}{\cosh^{4N}\chi}\sum_{\mu_1=0}^{i_1}\sum_{\nu_1=0}^{j_1}\sum_{\kappa_1=0}^{k_1}\sum_{\lambda_1=0}^{l_1}(-1)^{\mu_1+\nu_1}\binom{i_1}{\mu_1}\binom{j_1}{\nu_1}\right.$$

$$\times\binom{k_1}{\kappa_1}\binom{l_1}{\lambda_1}\ldots\frac{1}{\sqrt{2^{i_N+j_N+k_N+l_N}i_N!j_N!k_N!l_N!}}\frac{(\tanh\chi)^{i_N+j_N+k_N+l_N}}{\cosh^{4N}\chi}$$

$$\left.\times\sum_{\mu_N=0}^{i_N}\sum_{\nu_N=0}^{j_N}\sum_{\kappa_N=0}^{k_N}\sum_{\lambda_N=0}^{l_N}(-1)^{\mu_N+\nu_N}\binom{i_p}{\mu_N}\binom{j_N}{\nu_N}\binom{k_N}{\kappa_N}\binom{l_N}{\lambda_N}\right)$$

$$\times\prod_{n=1}^{N-1}\Omega\left(\mu_n,\lambda_n,i_{N+n},l_{N+n}\right)\Omega\left(\nu_n,\kappa_n,j_{N+n},k_{N+n}\right)\frac{\sqrt{i_{N+n}!j_{N+n}!k_{N+n}!l_{N+n}!}}{\sqrt{2}^{i_{N+n}+j_{N+n}+k_{N+n}+l_{N+n}}}$$

$$\times\delta_{i_{N+n}+l_{N+n},\mu_n+\lambda_n+i_{n+1}+l_{n+1}-\mu_{n+1}-\lambda_{n+1}}\delta_{j_{N+n}+k_{N+n},\nu_n+\kappa_n+j_{n+1}+k_{n+1}-\nu_{n+1}-\kappa_{n+1}}$$

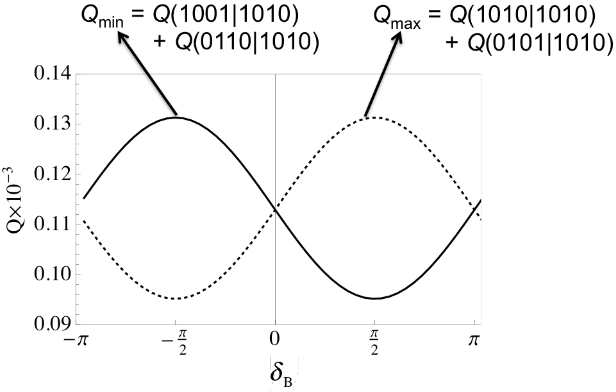
$$\times(\nu_N+\kappa_N)!\,(j_1+k_1-\nu_1-\kappa_1)!\sqrt{\frac{j'!k'!}{i'!l'!}}\sum_{n_a=0}^{\min\left[j',\nu_N+\kappa_N\right]}\sum_{n_d=0}^{\min\left[k',j_1+k_1-\nu_1-\kappa_1\right]}$$

$$\times\left(\mathrm{i}\tan\frac{\delta_A}{2}\right)^{\nu_N+\kappa_N+j'-2n_a}\left(\cos\frac{\delta_A}{2}\right)^{i'+j'-2n_a}\left(\mathrm{i}\tan\frac{\delta_B}{2}\right)^{k'+j_1+k_1-\nu_1-\kappa_1-2n_d}\left(\cos\frac{\delta_B}{2}\right)^{l'+k'-2n_d}$$

$$\times\frac{(i'+j'-n_a)!(l'+k'-nd)!}{n_a!n_d!\,(j'-n_a)!\,(k'-n_d)!\,(\nu_N+\kappa_N-n_a)!\,(j_1+k_1-\nu_1-\kappa_1-n_d)!}$$

$$\times\delta_{i'+j',\mu_N+\nu_N+\kappa_N+\lambda_N}\delta_{k'+l',i_1+j_1+k_1+l_1-\mu_1-\nu_1-\kappa_1-\lambda_1}.$$

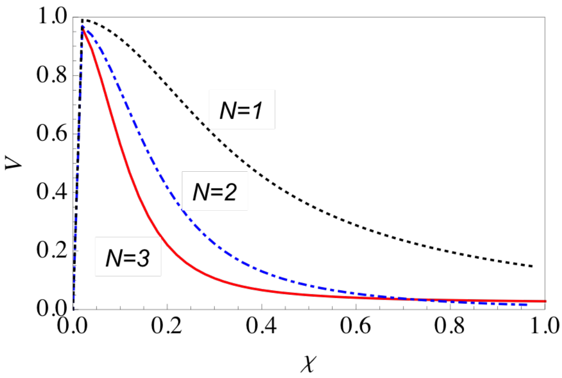
$N = 3$; $V = 0.16$ @ $\delta = \pm\pi/2$



$\chi = 0.24$
$\eta = 0.04$
$\wp = 1 \times 10^{-5}$
$\delta_{\text{A}} = \pi/2$

Khalique Sanders *PRA* (2014)

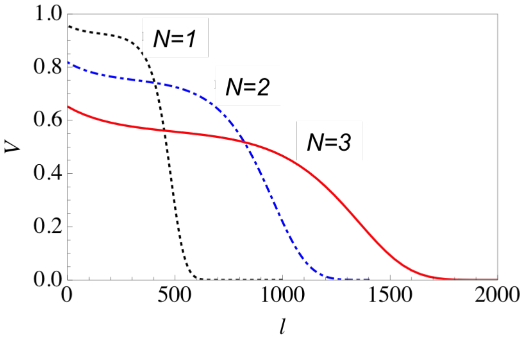
$N \leq 3$; V @ $\delta_{\mathrm{B}} = \pm\pi/2$



$\eta = 0.04$
$\wp = 1 \times 10^{-5}$

Khalique Sanders *PRA* (2014)

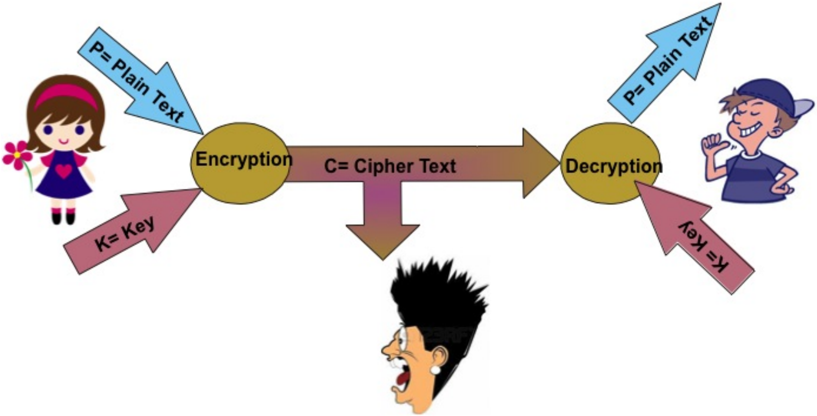
$N \leq 3$; V @ $\delta_{\text{B}} = \pm\pi/2$



$\chi = 0.1$
$\eta_0 = 0.70$
$\wp = 1 \times 10^{-5}$
$\alpha = 0.25$ dB/km
$\alpha_0 = 4$ dB

Khalique Sanders *PRA* (2014)

Quantum Cryptography



Perfect Secrecy: The Vernam Cipher

P = 0 1 1 0 1 0 0 1 0 1

K = 1 0 1 1 1 0 1 1 0 0

C = **P** $\oplus$ **K**

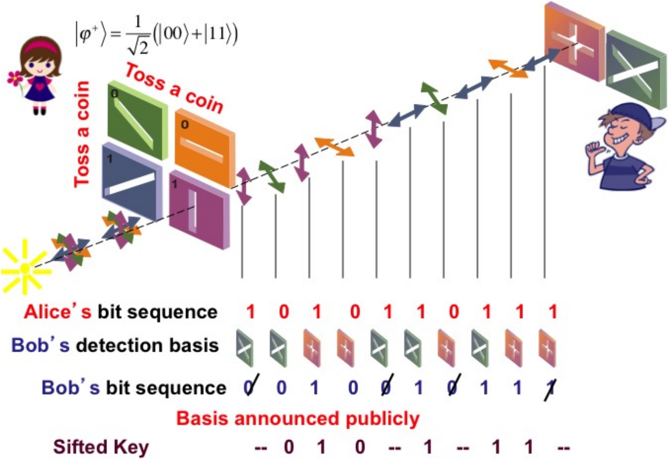
1 1 0 1 0 0 1 0 0 1

Impossible to break **iff** **K** is

- Long as **P**
- Random
- Secret
- Used only once (One time pad)

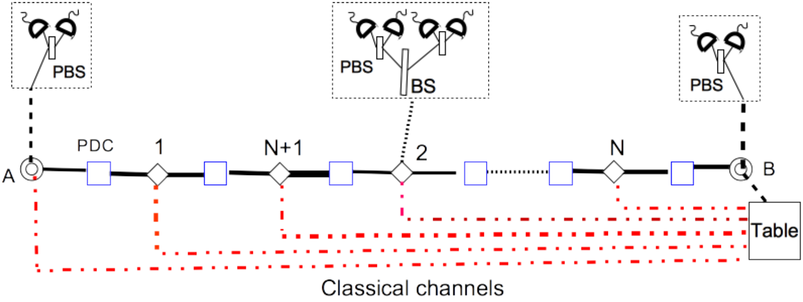
Vernam *J. Am. Inst. Elec. Eng* (1926)

Perfect Secrecy: QKD: BB84 Protocol



Bennett Brassard *IEEE* (1984)

Long-distance QKD Protocol



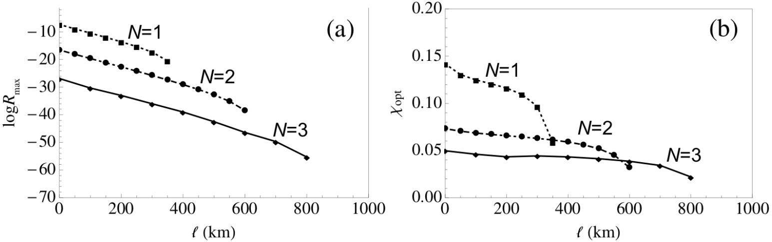
$$R = R_{\text{Shor-Preskill}} R_{\text{sifted}}$$

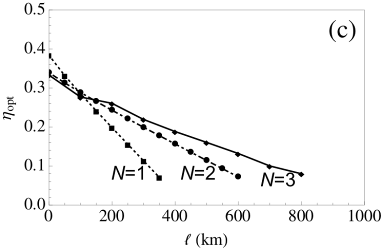
$$R_{\text{sifted}} = \frac{1}{2}(\chi^2)^{2N} 10^{(-\alpha l/40N)4N} (\eta^2/2)^{2N-1} \eta^2.$$

$$R_{\text{Shor-Preskill}} = 1 - \kappa H_2(Q) - H_2(Q); \quad Q = (1 - V)/2$$

Khalique Sanders *JOSA B* (2015)

Long-distance QKD





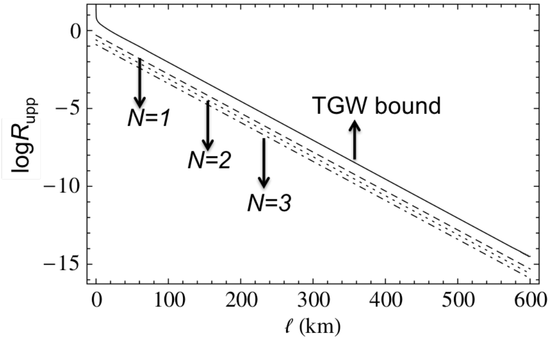
$\wp = Ae^{B\eta}$

For InGaAs detector

$A = 6.1 \times 10^{-7}$, $B = 17$

Khalique Sanders *JOSA B* (2015)

R_{upp} vs TGW bound for single photons



$\wp = 0$
$\eta = 1$
$\alpha = 0.25$

$R_{\text{Shor-Preskill}} = 1$
$R = R_{\text{sifted}}$

Khalique Sanders *JOSA B* (2015)

Truncated summation → Metropolis-Hastings sampling

With Liu Yaxiong and Zhang Pengqing (USTC)

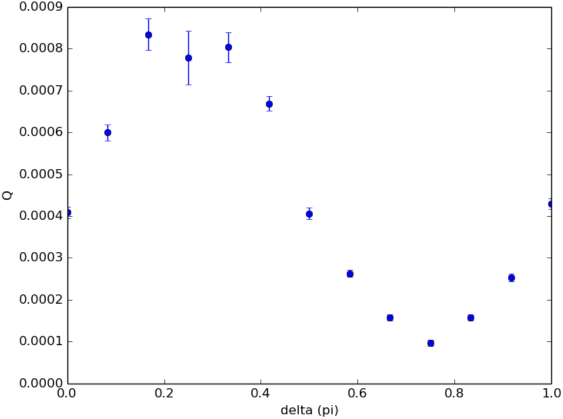
$$Q(q'r's't'|\boldsymbol{qrst}) = \sum_{i'j'k'l'} P(q'r's't'|i'j'k'l')P(i'j'k'l'|\boldsymbol{qrst})$$

$$P(i'j'k'l'|\boldsymbol{qrst}) = \sum_{\boldsymbol{ijkl}} P(\boldsymbol{ijkl}|\boldsymbol{qrst}) \times \underbrace{\langle i'j'k'l'|\, U(\alpha)U(\delta)\, |\tilde{\Xi}\rangle^{\text{out}}_{\boldsymbol{ijkl}}\langle\tilde{\Xi}|\, U^\dagger(\alpha)U^\dagger(\delta)\, |i'j'k'l'\rangle}_{A^{i'j'k'l'}_{\boldsymbol{ijkl}}\ \text{(hard)}}$$

- Before: $4 \times (2N-1)$-dimension hypercube truncation
- Now: Metropolis-Hastings sampling of $\boldsymbol{ijkl}$ from distribution of $\langle A^{i'j'k'l'}_{\boldsymbol{ijkl}} \rangle$ to obtain

$$Q(q'r's't'|\boldsymbol{qrst}) = \langle A^{i'j'k'l'}_{\boldsymbol{ijkl}} \rangle$$

Sampling result for single swap



2^{17}samples per point
$\chi = 0.24$
$\eta = 0.05$
$\wp = 10^{-5}$
$\delta_{\mathrm{A}} = \pi/4$

Conclusions

- Developed a tractable model for practical quantum relay
- Quantified upper bounds for visibility
- In QKD, smaller N yields higher key-generation rate and larger N yields larger distances
- Next steps: Monte Carlo sampling and including quantum memory