Photonic Quantum Information Processing
OPTI 647: Lecture 25

Saikat Guha

November 19, 2019
College of Optical Sciences
Meinel 523

Recap and plan for today

- Holevo Capacity for Lossy-Noisy channel
- Wiretap channel – secure communication
- Quantum communication and entanglement distribution
- Quantum repeaters

Holevo capacity: Quantum limit to classical communication rate

THE UNIVERSITY OF ARIZONA

$$\sigma_x^B = \mathcal{N}(\rho_x^A)$$

X $\quad \{p(x), \rho_x^A\}, \; x \in \{1, \ldots, M\} \quad \boxed{\mathcal{N}} \quad \{p(x), \sigma_x^B\}, \; x \in \{1, \ldots, M\} \quad \boxed{\Pi_y} \quad y \in \{1, \ldots, K\}$ $\quad Y$

$$p_{Y|X}(y|x) = \mathrm{Tr}(\rho_x \Pi_y)$$

$$C_{\text{Shannon}} = \max_{p_X(x)} I(X;Y)$$

Function of the receiver choice

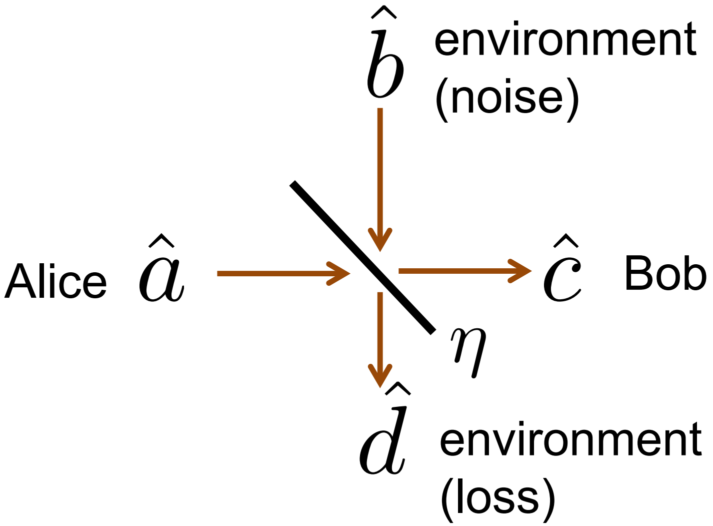
$$C_{\text{Holevo}} = \max_{p_X(x)} I(X;B)$$

$$I(X;B) = S\left(\sum p_X(x)\sigma_x^B\right) - \sum p_X(x) S(\sigma_x^B)$$

Single-mode bosonic channel

- The beamsplitter

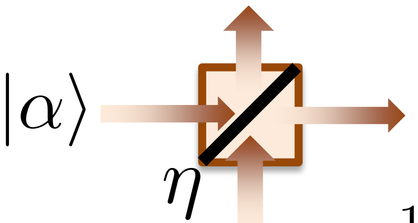
$$\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b}$$
$$\hat{d} = -\sqrt{1-\eta}\hat{a} + \sqrt{\eta}\hat{b}$$



- Single-mode bosonic channel, $\mathcal{N}_\eta^{N_b}$: $\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b}$
  - Pure loss: $\rho_b = |0\rangle\langle 0| \;\; (N_b = 0)$
  - Thermal noise: $\rho_b = (1/\pi N_b) \int e^{-|\alpha|^2/N_b} |\alpha\rangle\langle\alpha| d^2\alpha$
  - Mean power (photon number) constraint, $\langle \hat{a}^\dagger \hat{a}\rangle = N$
  - Only state that retains its purity through the pure loss channel is the coherent state, $|\alpha\rangle \rightarrow |\sqrt{\eta}\alpha\rangle$
  - Mean photon number at output, $\langle \hat{c}^\dagger \hat{c}\rangle = \eta N + (1-\eta)N_b$

Holevo capacity with loss and noise

THE UNIVERSITY OF ARIZONA



Coherent state modulation

$$\left\{ |\alpha\rangle, p(\alpha) = \frac{e^{-|\alpha|^2/N_S}}{\pi N_S} \right\}$$

$$\rho_{\rm th} = \frac{1}{N} \int e^{-|\mu|^2/N} |\mu\rangle\langle\mu| d^2\mu$$

Achievability $C(\eta, N_S, N) \geq g(\eta N_S + (1-\eta)N) - g((1-\eta)N)$

$$g(x) = (1+x)\log(1+x) - x\log x$$

Converse
$$\begin{aligned} C(\eta, N_S, N) &= \max_{\{p_j,\hat{\rho}_j\}} \left[S(\mathcal{E}_\eta^N(\sum_j p_j\hat{\rho}_j)) - \sum_j p_j S(\mathcal{E}_\eta^N(\hat{\rho}_j)) \right] \\ &\leq \max_{\{p_j,\hat{\rho}_j\}} \left[S(\mathcal{E}_\eta^N(\sum_j p_j\hat{\rho}_j)) \right] - \min_{\{p_j,\hat{\rho}_j\}} \left[\sum_j p_j S(\mathcal{E}_\eta^N(\hat{\rho}_j)) \right] \\ &\leq \max_{\{p_j,\hat{\rho}_j\}} \left[S(\mathcal{E}_\eta^N(\sum_j p_j\hat{\rho}_j)) \right] - \min_{\hat{\rho}} \left[S(\mathcal{E}_\eta^N(\hat{\rho})) \right], \\ &\leq g(\eta N_S + (1-\eta)N) - \min_{\hat{\rho}} \left[S(\mathcal{E}_\eta^N(\hat{\rho})) \right] \end{aligned}$$

Please note change in notation:
N_S = input photon number
N = thermal photon number

Minimum output entropy conjecture

V. Giovannetti, Guha, S. Lloyd, L. Maccone, J. H. Shapiro, Physical Review A 70, 032315 (2004)
V. Giovannetti, R. Garcia-Patron, N. J. Cerf, A. S. Holevo, Nature Photonics 8, 796-800 (2014)

“Vacuum or not” black box

THE UNIVERSITY OF ARIZONA

$$|\psi\rangle = \sum_{n=0}^{\infty} c_n|n\rangle \longrightarrow \boxed{\text{VON}}$$

$$\xrightarrow{p_0 = |c_0|^2} |\psi_0\rangle = |0\rangle$$

$$\xrightarrow{1 - p_0} |\psi_1\rangle = \frac{|\psi\rangle - c_0|0\rangle}{\sqrt{1 - |c_0|^2}}$$

$$\Pi_0 = |0\rangle\langle 0|$$

$$\Pi_1 = \hat{I} - |0\rangle\langle 0|$$

- How do we realize the VON measurement using beam-splitters, phase-shifters, squeezers and cross-Kerr gates: $U_\kappa = e^{i\kappa(\hat{a}^\dagger \hat{a} \hat{b}^\dagger \hat{b})}$?

Advanced Problem 19 (open)

The “vacuum or not” receiver to achieve the Holevo capacity

THE UNIVERSITY OF ARIZONA

- Random code with 2^{nR} codewords: A sequence of 2^{nR} “vacuum or not” binary non-destructive projective measurements plus phase-space displacements (beamsplitter & laser) can achieve capacity

$$|\boldsymbol{\alpha}^{(m)}\rangle = |\alpha_1^{(m)}\rangle|\alpha_2^{(m)}\rangle \ldots |\alpha_n^{(m)}\rangle$$

$$1 \leq m \leq nR$$

$(j \rightarrow j+1)$

$|\psi'_j\rangle$

Displacement by negative of j[th] c.w. $|\boldsymbol{\alpha}^{(j)}\rangle$: array of n BS + lasers

$$|\psi_j\rangle = |\psi'_{j-1} - \boldsymbol{\alpha}^{(j)}\rangle$$

$$\left\{\hat{P}, \hat{I}_n - \hat{P}\right\}$$

$$\frac{(\hat{I} - \hat{P})|\psi^n\rangle}{\langle\psi_n|\hat{I} - \hat{P}|\psi_n\rangle}$$

$$\frac{\hat{P}|\psi^n\rangle}{\langle\psi_n|\hat{P}|\psi_n\rangle} = |0\rangle^{\otimes n}$$

$$\hat{m} = j$$

$$\hat{P} = |0\rangle^{\otimes n}\langle 0|^{\otimes n}$$

Receiver cycles through multimode entangled coherent states…

Lloyd, Giovannetti, Maccone, Phys. Rev. Lett. 106, 250501 (2011)
Wilde, Guha, Tan, Lloyd, ArXiv: 1202.0518 (IEEE Int. Symp. Inf. Theory 2012)
”Measuring Nothing”, Oi, Potocek, Jeffers, ArXiv:1207.3011, (PRL, 2012)

Holevo attaining joint detection receivers

- “vacuum or not” meas. and coherent feedback

$$|\boldsymbol{\alpha}^{(m)}\rangle = |\alpha_1^{(m)}\rangle|\alpha_2^{(m)}\rangle \ldots |\alpha_n^{(m)}\rangle$$

$$1 \le m \le nR$$

$(j \to j+1)$ $\quad |\psi'_j\rangle$

$\boxed{\text{Displacement by negative of } j^{\text{th}} \text{ c.w. } |\boldsymbol{\alpha}^{(j)}\rangle\text{: array of n BS + lasers}}$

$$|\psi_j\rangle = |\psi'_{j-1} - \boldsymbol{\alpha}^{(j)}\rangle$$

$$\left\{\hat{P}, \hat{I}_n - \hat{P}\right\} \to \frac{(\hat{I} - \hat{P})|\psi^n\rangle}{\langle\psi_n|\hat{I} - \hat{P}|\psi_n\rangle}$$

$$\to \frac{\hat{P}|\psi^n\rangle}{\langle\psi_n|\hat{P}|\psi_n\rangle} = |0\rangle^{\otimes n} \to \hat{m} = j$$

$$\hat{P} = |0\rangle^{\otimes n}\langle 0|^{\otimes n}$$

Wilde, SG, Tan, Lloyd, ISIT 2012
Oi, Potocek, Jeffers, Phys. Rev. Lett. 110, 210504 (2013)

- Quantum polar code and successive cancellation

SG, Wilde, ISIT 2012
Wilde, SG, IEEE Trans. Inf. Theory, 59, no. 2, 1175-1187 (2013)

- Efficient joint measurements for symmetric codes

Krovi, SG, Dutton, da Silva, Phys. Rev. A 92, 062333 (2015)

- Slicing receiver

Da Silva, SG, Dutton, Phys. Rev. A 87, 052320 (2013)

Recap: channel capacity

$$\mathcal{N}$$

Alice $X \rightarrow \boxed{p_{Y|X}(y|x)} \rightarrow Y$ Bob

- Capacity, $C(\mathcal{N})$
  - At what rate (bits per channel use) can Alice send information *reliably* to Bob?

$$C(\mathcal{N}) = \max_{p_X(x)} I(X;Y)$$

Shannon, 1948

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= H(X) - H(X|Y) \end{aligned}$$

Wiretap channel: private communication

THE UNIVERSITY OF ARIZONA

$\mathcal{N}$

Alice $X \rightarrow \boxed{p_{Y,Z|X}(y,z|x)} \rightarrow Y$ Bob

$\downarrow$

Z Eve

Wyner, 1975

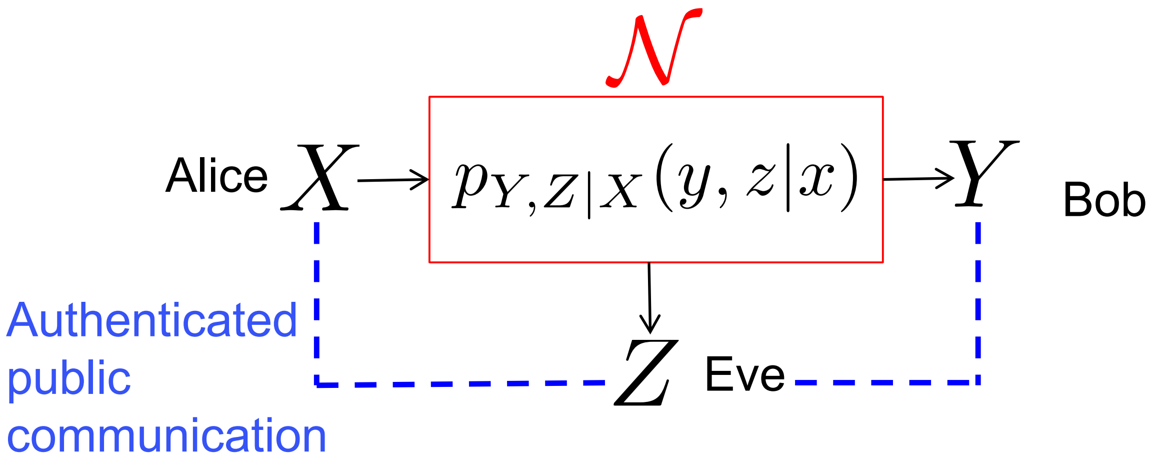
Csiszar and Korner, 1978

- Private capacity, $\mathcal{P}_1(\mathcal{N})$
  - Also referred to as: secrecy capacity, privacy capacity
- At what rate (bits per channel use) can Alice send information *reliably* and *privately* to Bob?

$$\begin{aligned}\mathcal{P}_1(\mathcal{N}) &= \max_{p_{UX}} \left[I(U;Y) - I(U;Z)\right] \\ &\geq \max_{p_X} \left[I(X;Y) - I(X;Z)\right] \\ &= \max_{p_X} \left[H(X|Z) - H(X|Y)\right]\end{aligned}$$

Equality holds if
$I(X;Y) \geq I(X;Z), \forall p_X$

Private communication with two-way public communication as ancilla resource



Maurer, 1993

Ahlswede and Csiszar, 1993

- Two-way private capacity, $\mathcal{P}_2(\mathcal{N})$
  - An exact formula not known. Only upper & lower bounds

$$\mathcal{P}_2(\mathcal{N}) \geq \max\left[\max_{p_X}[I(Y;X) - I(Z;X)],\ \max_{p_X}[I(X;Y) - I(Z;Y)]\right]$$

$$\mathcal{P}_2(\mathcal{N}) \leq \min\left[I(X;Y), I(X;Y|Z)\right]$$

$$\mathcal{P}_2(\mathcal{N}) \leq I(X;Y \downarrow Z) = \min_{Z \to Z'} I(X;Y|Z)$$

Intrinsic information (improved upper bound)

Binary symmetric channel

$$\underset{\in\{0,1\}}{X} \longrightarrow \overset{\mathcal{N}}{\boxed{p_{Y|X}(y|x)}} \longrightarrow \underset{\in\{0,1\}}{Y}$$

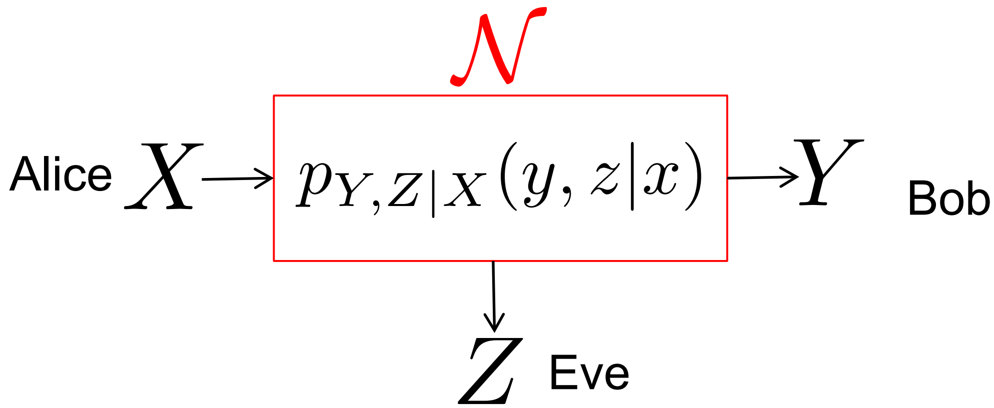
$$P_{Y|X}(y|x) = \epsilon, \ \text{if } x \neq y$$

- Capacity, $C(\mathcal{N}) = \max\limits_{p_X(x)} I(X;Y)$

$$= 1 - h(\epsilon)$$ bits per channel use

$$h(\epsilon) = -\epsilon \log_2(\epsilon) - (1-\epsilon)\log_2(1-\epsilon)$$

Binary symmetric wiretap channel



$$X \in \{0,1\}$$
$$Y \in \{0,1\}$$
$$Z \in \{0,1\}$$

$$P_{Y|X}(y|x) = \epsilon, \ \text{if } x \neq y$$
$$P_{Z|X}(z|x) = \delta, \ \text{if } x \neq y$$

- Private capacity,

$$\mathcal{P}_1(\mathcal{N}) = \begin{cases} h(\delta) - h(\epsilon), & \text{if } d > \epsilon \\ 0, & \text{otherwise} \end{cases}$$

Private communication to Eve is impossible if she has a better channel than Bob

Additive Gaussian noise channel

$$X \rightarrow \boxed{p_{Y|X}(y|x)} \rightarrow Y$$

$$\mathcal{N}$$

$X, Y \in \mathbb{R}$ $\qquad Y = X + V,\ V \sim \mathcal{N}(0, \sigma^2)$

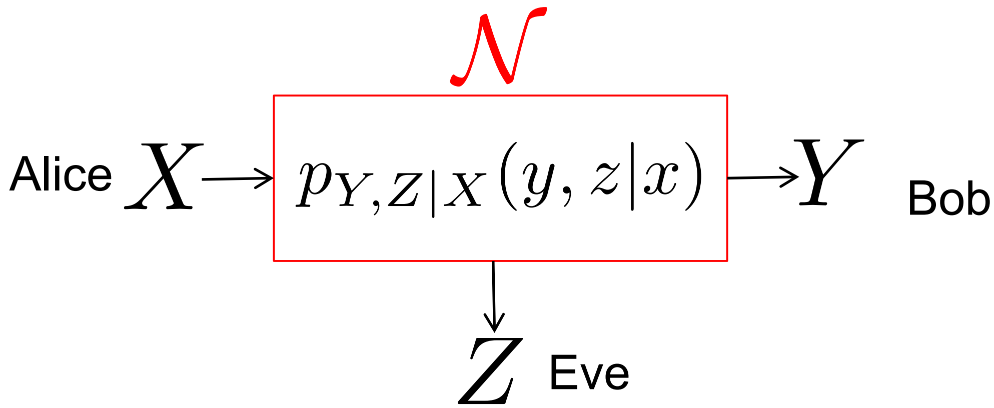
$E[X^2] \le P$ (input power constraint)

- Capacity, $C(\mathcal{N}) = \max\limits_{p_X(x)} I(X;Y)$

$$= \frac{1}{2}\log_2\left(1 + \frac{P}{\sigma^2}\right)$$ bits per channel use

Capacity increases indefinitely as transmit power is increased

Gaussian noise wiretap channel



$$X, Y, Z \in \mathbb{R}$$

$$Y = X + V_1, V_1 \sim \mathcal{N}(0, \sigma_b^2)$$
$$Z = X + V_2, V_2 \sim \mathcal{N}(0, \sigma_e^2)$$

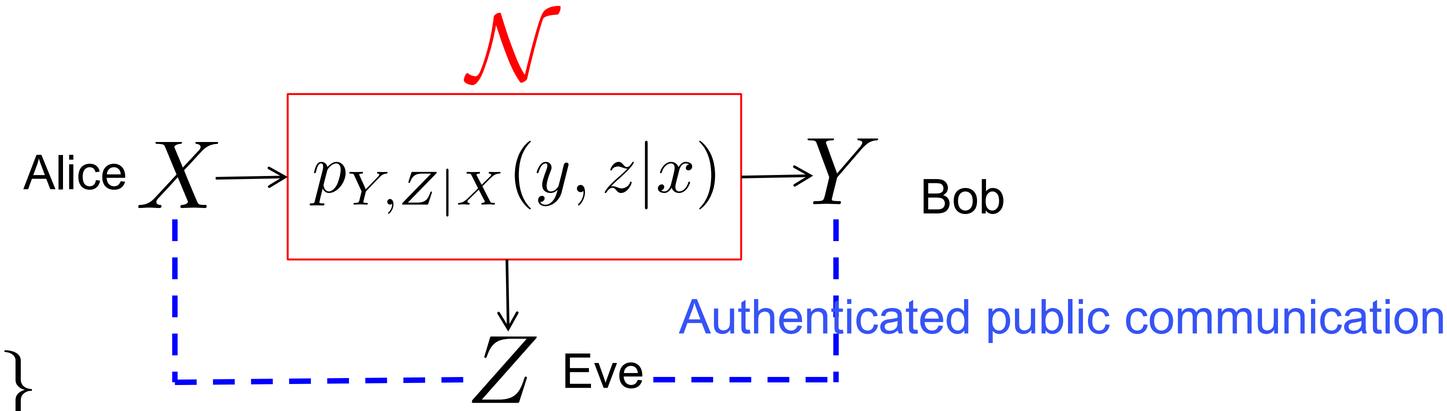
$$\mathcal{P}_1(\mathcal{N}) = \begin{cases} \frac{1}{2}\log_2\left(1 + \frac{P}{\sigma_b^2}\right) - \frac{1}{2}\log_2\left(1 + \frac{P}{\sigma_e^2}\right), & \text{if } \sigma_b^2 < \sigma_e^2 \\ 0, & \text{otherwise} \end{cases}$$

$$\mathcal{P}_1(\mathcal{N}) \to \log_2\left(\frac{\sigma_e^2}{\sigma_b^2}\right), \ \sigma_b^2 < \sigma_e^2$$

Private communication to Eve is impossible if she has a better channel than Bob.
Private capacity does NOT increase indefinitely with transmit power

Binary symmetric channel: private communication with two-way discussion

THE UNIVERSITY OF ARIZONA



$$X \in \{0,1\}$$
$$Y \in \{0,1\}$$
$$Z \in \{0,1\}$$

$$P_{Y|X}(y|x) = \epsilon, \;\; \text{if } x \neq y$$
$$P_{Z|X}(z|x) = \delta, \;\; \text{if } x \neq y$$

$$\mathcal{P}_1(\mathcal{N}) = \begin{cases} h(\delta) - h(\epsilon), & \text{if } d > \epsilon \\ 0, & \text{otherwise} \end{cases}$$

Without the public discussion channel

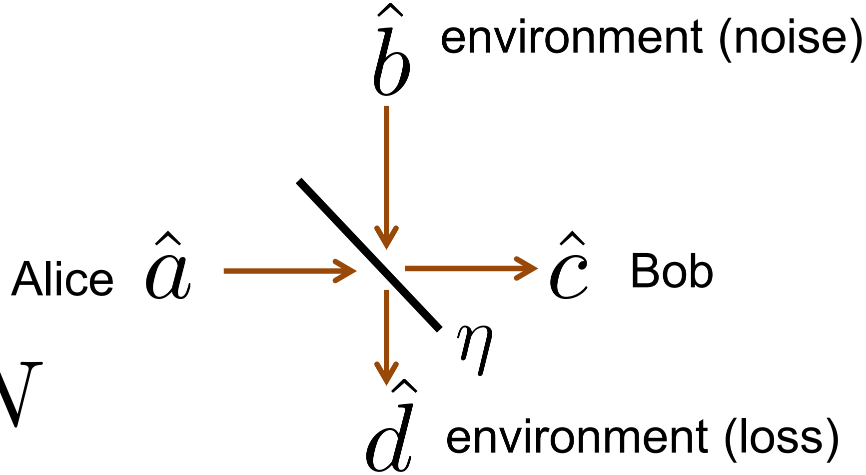
$$\mathcal{P}_2(\mathcal{N}) = h(\epsilon + \delta - 2\epsilon\delta) - h(\epsilon)$$

With public discussion

Maurer, 1993

Private communication = secret key generation (if authenticated public discussion available)

Lossy bosonic channel



$$\langle \hat{a}^\dagger \hat{a} \rangle \leq N$$

Mean photon
number constraint

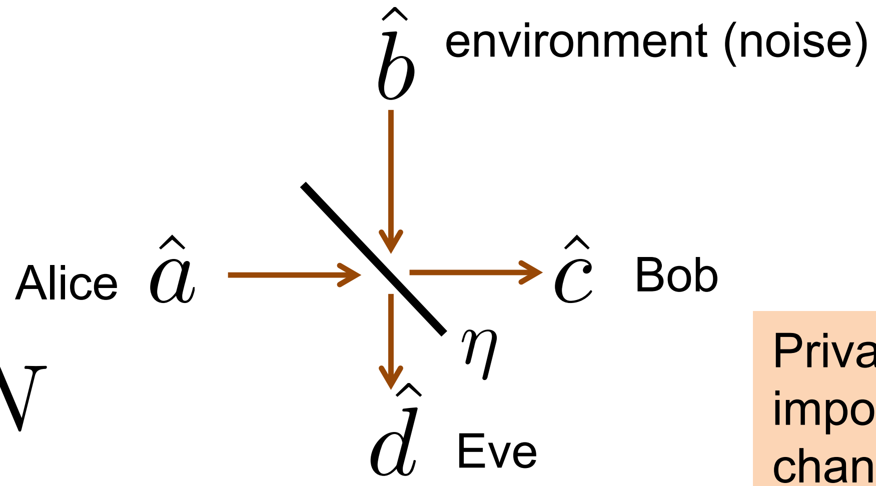
- Classical capacity, $C = g(\eta N)$ bits per mode
  - attained by coherent state inputs, joint-detection receiver
  - $g(x) = (1+x)\log_2(1+x) - x\log_2 x$

Capacity increases indefinitely as transmit power is increased

Giovannetti, Guha, Lloyd, Macconne, Shapiro, Yuen, PRL, 92, 027902 (2004)

Private communication with a quantum powerful adversary

THE UNIVERSITY OF ARIZONA



$$\langle \hat{a}^\dagger \hat{a} \rangle \leq N$$

Mean photon number constraint

Private communication to Eve is impossible if she has a better channel than Bob. Private capacity does NOT increase indefinitely with transmit power

- Private capacity of the bosonic wiretap channel

$$\mathcal{P}_1(\mathcal{N}) = \begin{cases} = g(\eta N) - g((1-\eta)N), & \text{if } \eta > \frac{1}{2} \\ 0, & \text{otherwise} \end{cases}$$

$$\rightarrow \log_2\left(\frac{\eta}{1-\eta}\right), \; N \rightarrow \infty$$

Prove this convergence result when N→ infinity

Prob m 93

Guha and Shapiro, 2007

Quantum equipped adversary

Without public discussion

$$C_s = \max_{U \to X \to Y,Z} [I(U;Y) - I(U,Z)]$$

(zero when Eve has a better channel)

Maurer, 1993; Ahlswede, Csiszar, 1993

We make Eve quantum by removing any restrictions on her receiver measurement. Replace Z everywhere by the quantum system E, Mutual information by Holevo information

With public discussion

(can be positive even if Eve's channel is better)

$$\mathrm{LB} \le C_s \le \mathrm{UB}$$

$$\mathrm{LB}_1 = \max_{p_X(x)} [I(X;Y) - I(Z;X)]$$

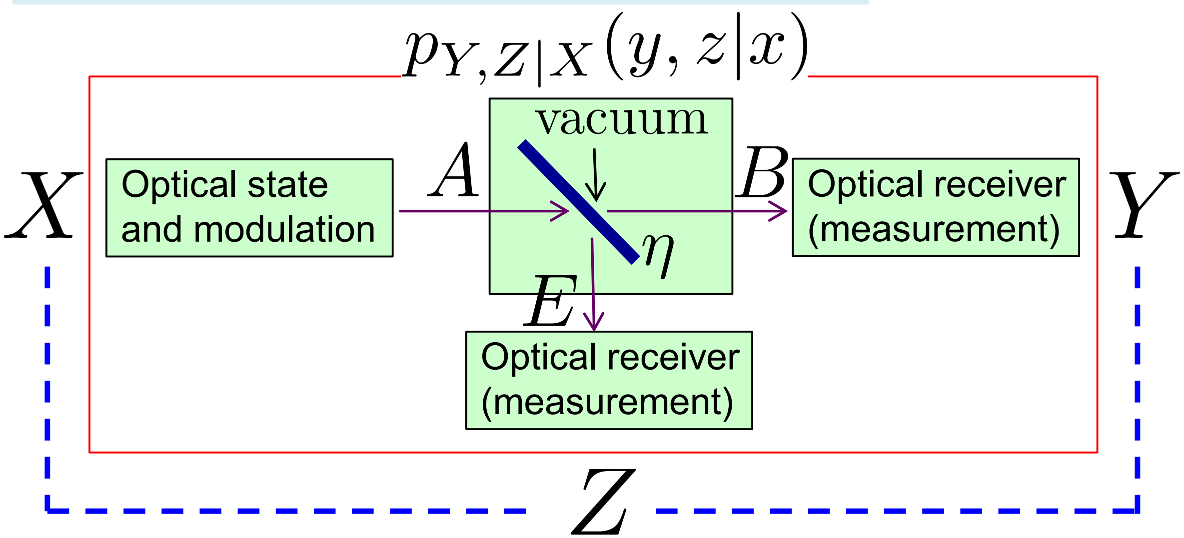
forward reconciliation

$$\mathrm{LB}_2 = \max_{p_X(x)} [I(X;Y) - I(Z;Y)]$$

reverse reconciliation

$$\mathrm{UB} = I(X;Y \downarrow Z) = \min \{ I(X;Y|Z') : Z \to Z'$$

"intrinsic information"

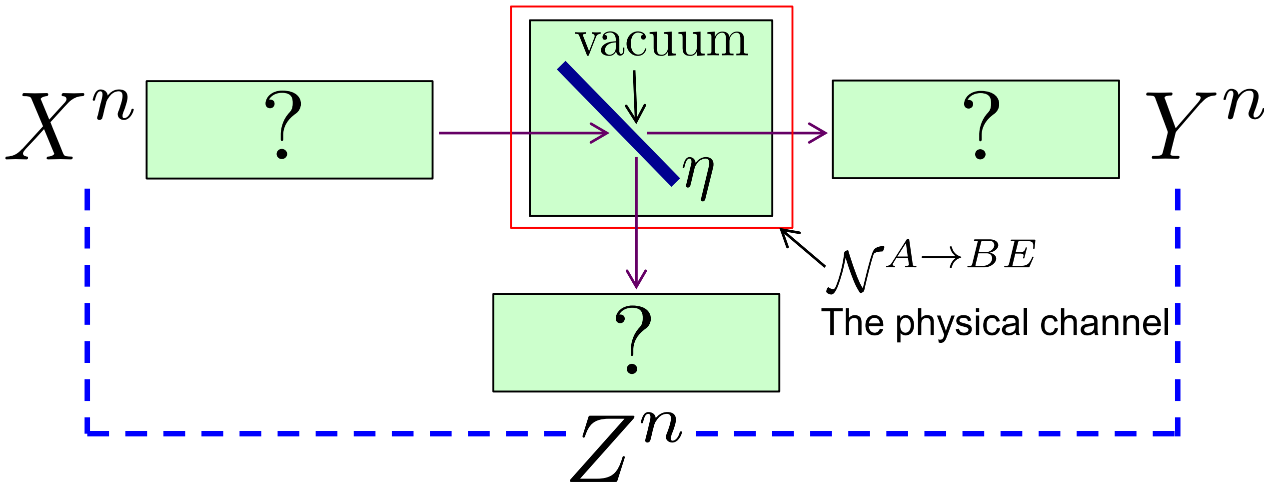


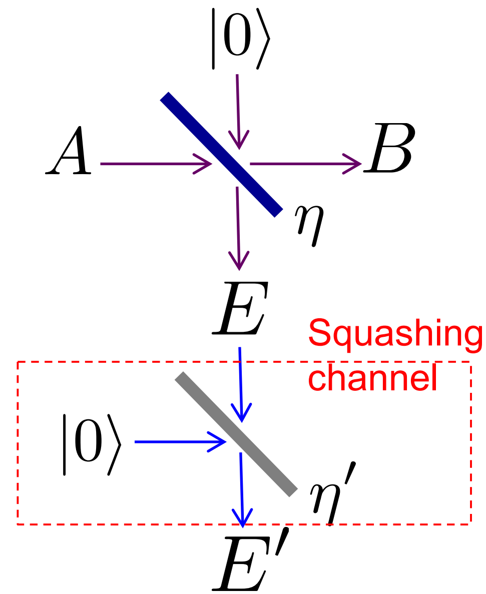
Private communication capacity ←→ secret key agreement capacity

$$\mathcal{P}_2 \equiv C_s$$

Both assuming availability of the public channel

Secure communication / key generation





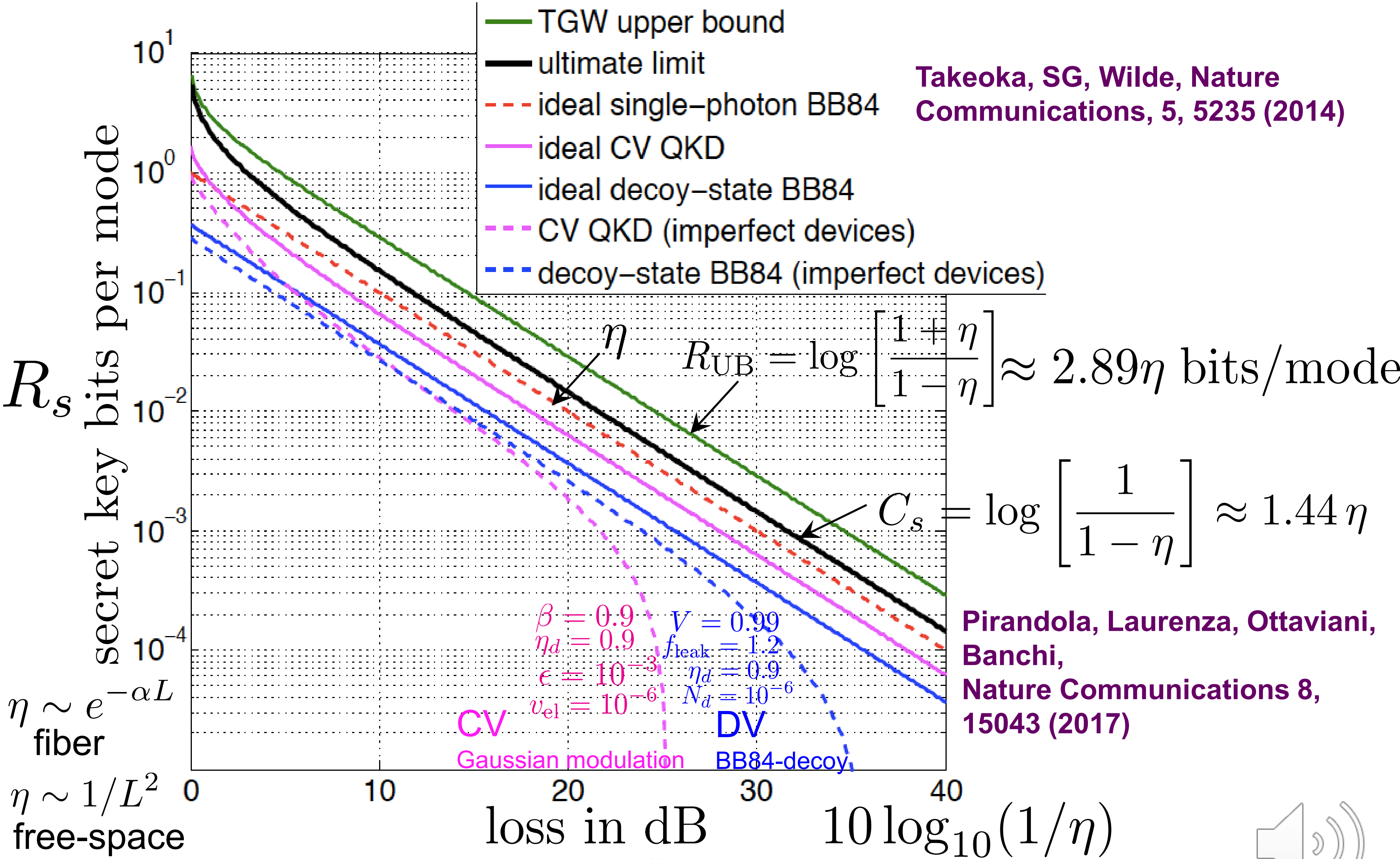
- Two-way private capacity of a quantum channel, $\mathcal{P}_2$
  - lower bounds known: reverse, and forward reconciliation
  - upper bound analogous to classical intrinsic information

$$C_s(\mathcal{N}) \leq I(A, B \downarrow E) \equiv \max_{|\phi\rangle_{A,A'}} \frac{1}{2} \inf_{\mathcal{S}_{E\to E'}} I(A; B|E')$$

Takeoka, Guha, Wilde, Nature Communications, 5, 5235, (2014)

  - Upper bound for the lossy bosonic channel $= \log_2 \left[\frac{1+\eta}{1-\eta}\right]$ bits/mode
- QKD
  - Secrete key generation without prior knowledge of channel $\mathcal{N}^{A\to BE}$

Private communication over lossy channel



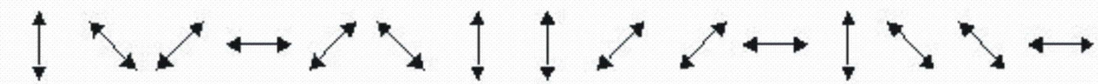
Takeoka, SG, Wilde, Nature Communications, 5, 5235 (2014)

Pirandola, Laurenza, Ottaviani, Banchi, Nature Communications 8, 15043 (2017)

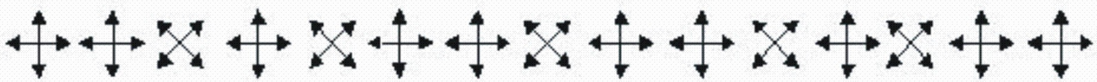
Quantum key distribution: BB84

1 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1

*Alice prepares random **values** for key bits.*

2 

*Alice transmits each random value encoded in a random, non-orthogonal **basis** on a "single photon."*

3 

Bob randomly selects a basis and measures each photon.

4 √ - √ √ √ - √ - - - - √ √ - √

Alice and Bob publicly communicate to determine matching bases, and discard all other bits ("sifting").

5 0 - 1 1 1 - 0 - - - - 0 0 - 1

*Now Alice and Bob share matching **values** for key bits (assuming no errors!).*

$$R = \eta/2 \text{ bits/mode}$$

After this, Alice and Bob communicate on the classical public channel to do error correction and privacy amplification: final shared key is **"quantum secure"**

Secure key rate depends upon how severe the channel (adversarial action) is.

Repeater-less QKD growing rapidly

THE UNIVERSITY OF ARIZONA

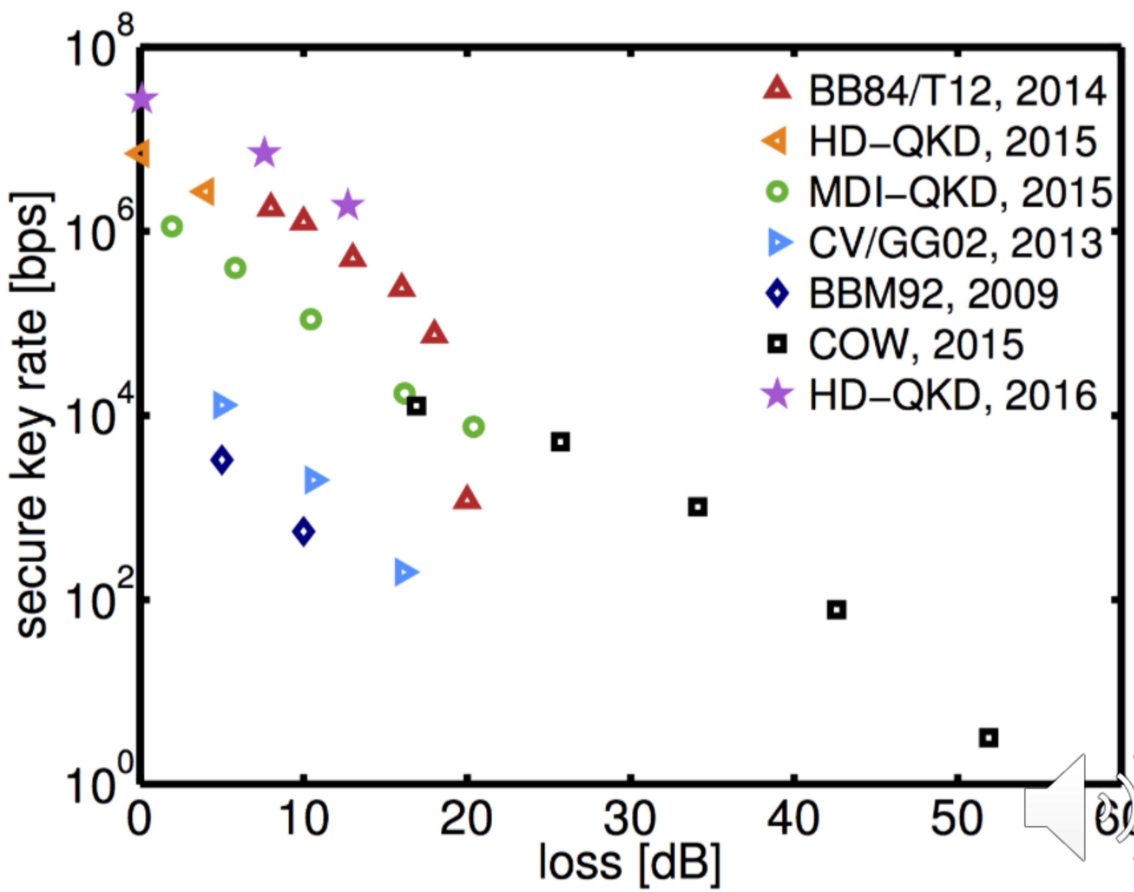
id Quantique

QuantumCTek

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

Quintessence labs
Quantum Cyber Defense™

research only:
NTT TOSHIBA



Repeater-less QKD growing rapidly

THE UNIVERSITY OF ARIZONA

id Quantique

QuantumCTek

SEQURENET

A QUANTUM KEY TO NETWORK SECURITY

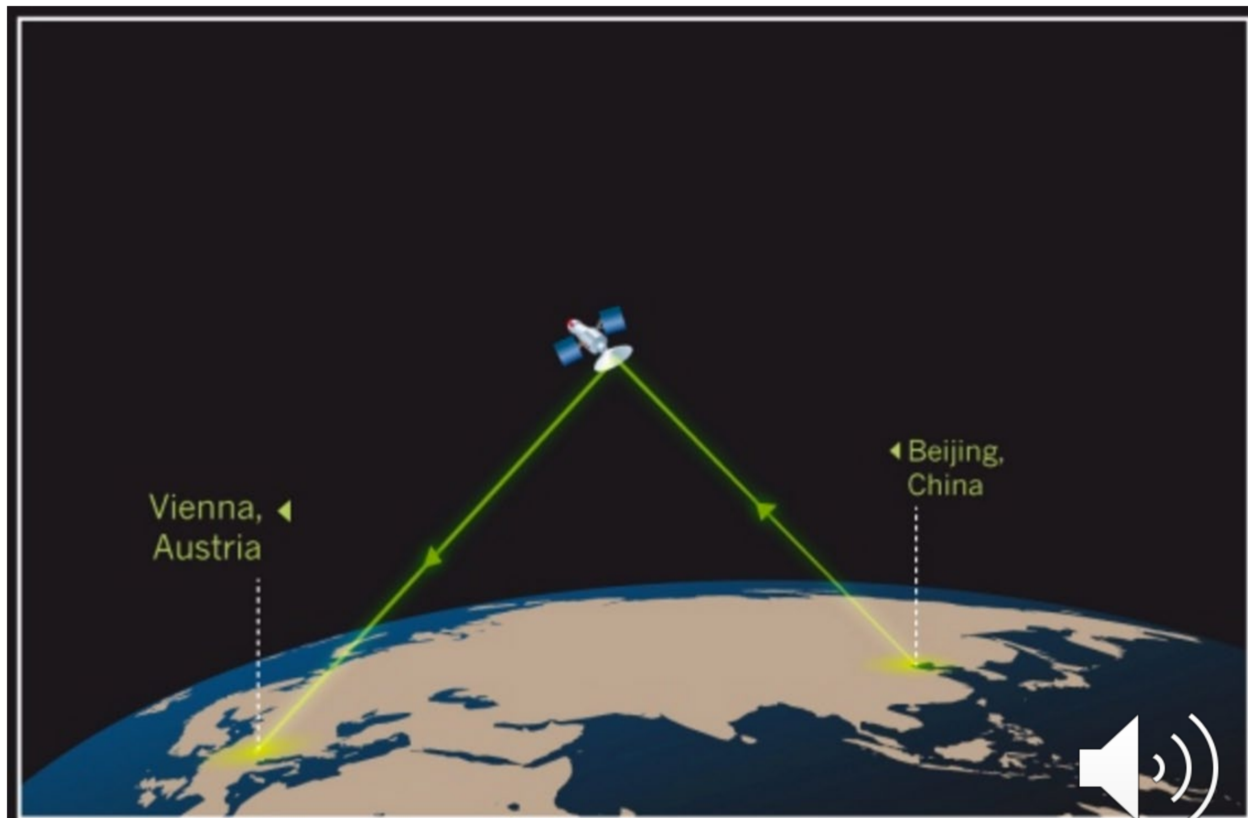
labs Quintessence

Quantum Cyber Defense™

research only:

NTT TOSHIBA

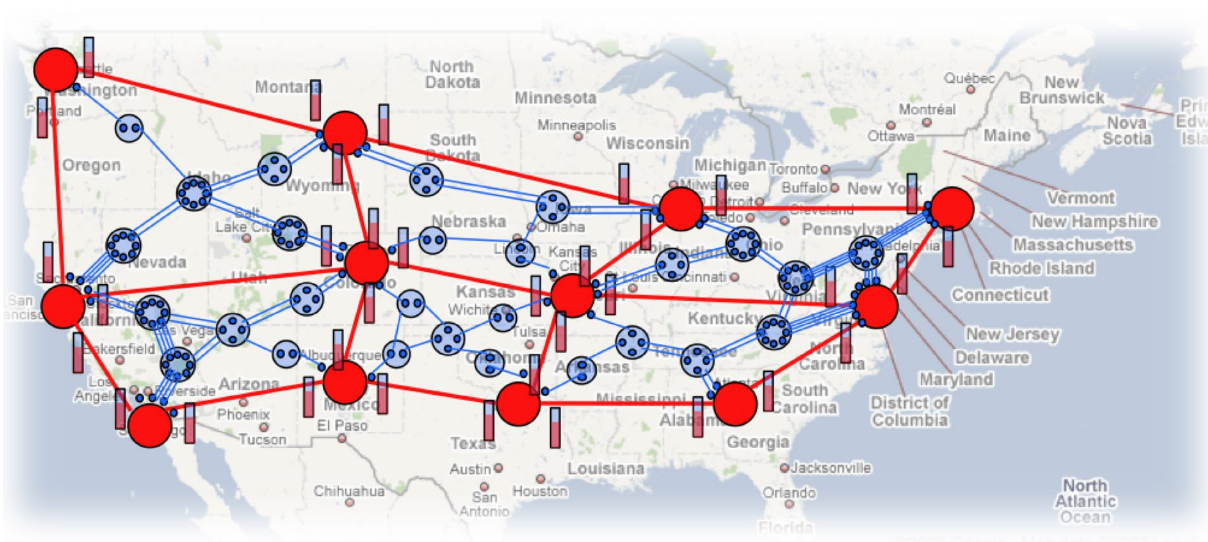
China Launches **Quantum Satellite** in Bid to Pioneer Secure ...
New York Times - Aug 16, 2016
BEIJING — **China** launched the world's first **quantum** communications **satellite** from the Gobi Desert early Tuesday, a major step in the country's ...
What the World's First **Quantum Satellite** Launch Means
Fortune - Aug 16, 2016



Quantum repeaters and networks

THE UNIVERSITY OF ARIZONA

- Long distance QKD and quantum repeaters
- Secure communication can be enabled by entanglement distribution.



  – Need *entanglement* and *quantum repeaters* to accomplish this (can beat the R ~ 1.44 η bits/mode limit)

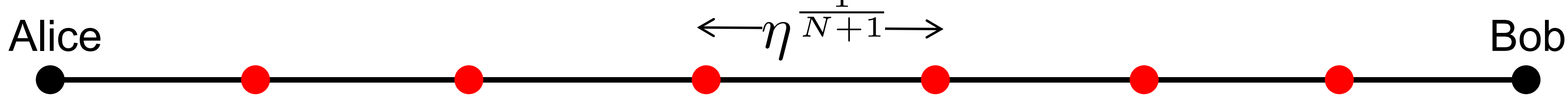
Entanglement distribution

THE UNIVERSITY OF ARIZONA

$$R_{\text{direct}}(\eta) = -\log(1-\eta) \approx 1.44\,\eta \text{ ebits/mode}$$

$$\longleftarrow \eta \sim e^{-\alpha L} \longrightarrow$$

$$\longleftarrow \eta^{\frac{1}{N+1}} \longrightarrow$$



Repeaters: a special purpose quantum processor

$$R \leq \log\left[\frac{1}{1-\eta^{\frac{1}{N+1}}}\right] \approx \eta^{\frac{1}{N+1}}$$

- More repeater nodes is better if the repeater nodes are perfect
- What if repeater nodes are constructed out of lossy / imperfect devices? What does is take to outperform R_{direct}?

Repeater based QKD: distributing entanglement and Bell state measurement

THE UNIVERSITY OF ARIZONA

- Bell basis for two qubits

Computational basis

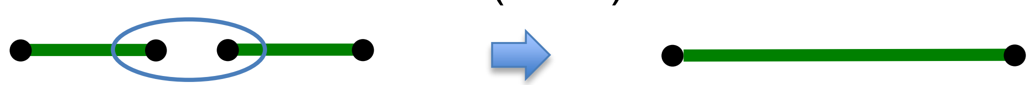
$$|0\rangle_A|0\rangle_B$$
$$|0\rangle_A|1\rangle_B$$
$$|1\rangle_A|0\rangle_B$$
$$|1\rangle_A|1\rangle_B$$

Bell basis

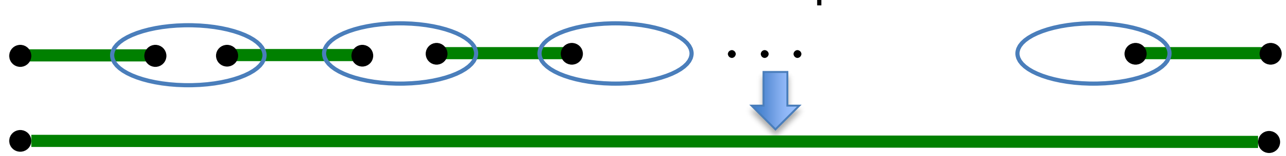
$$|\Phi^+\rangle_{AB} = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$$
$$|\Phi^-\rangle_{AB} = \frac{|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B}{\sqrt{2}}$$
$$|\Psi^+\rangle_{AB} = \frac{|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B}{\sqrt{2}}$$
$$|\Psi^-\rangle_{AB} = \frac{|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B}{\sqrt{2}}$$

- “Connecting” Bell states via a BSMs

Bell state measurement (BSM) on two EPR states



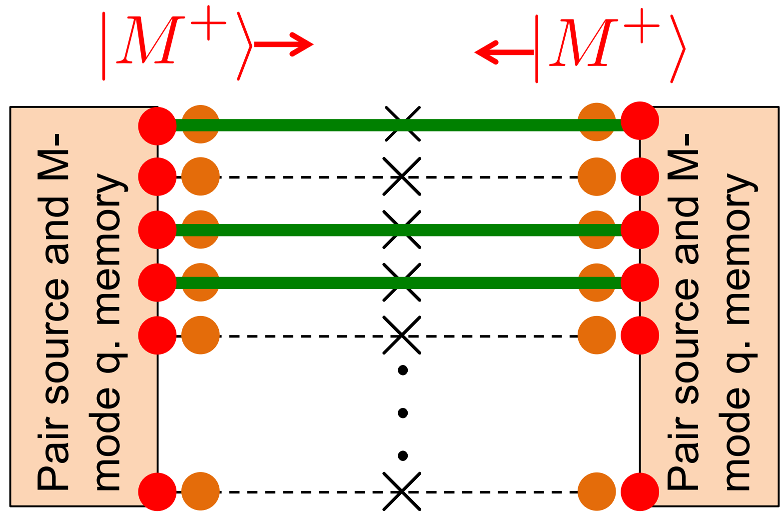
Simultaneous BSMs on multiple EPR states



Multiplexing-based repeater scheme

$$|M^+\rangle = \frac{|10,01\rangle + |01,10\rangle}{\sqrt{2}}$$

Bell state (in dual-rail single-photon encoding basis)



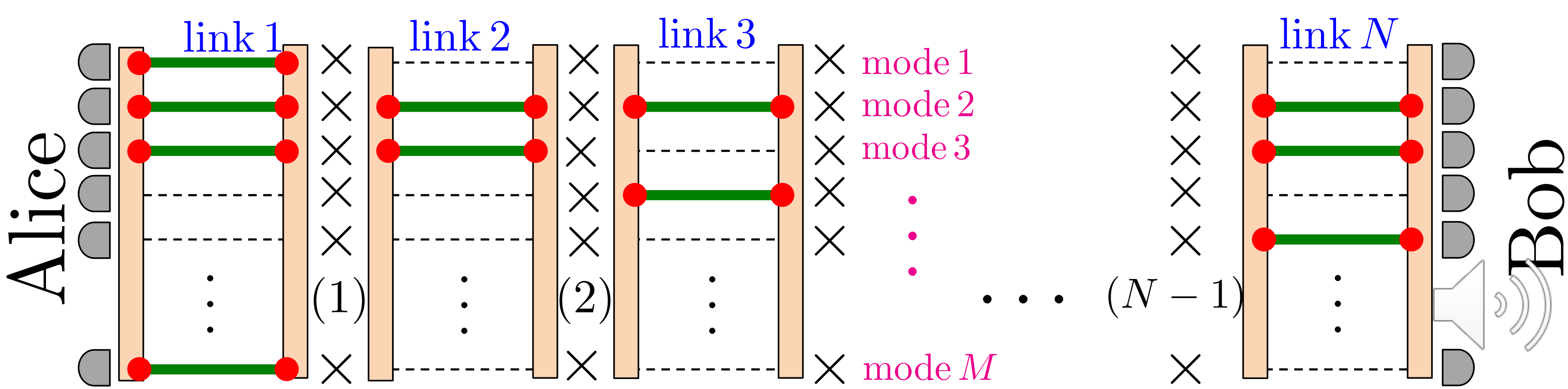
An “elementary link”

Each mode (e.g., spatial) heralds an EPR pair with probability, $p = c\eta^{1/N}$

Each repeater (node) performs a Bell meas. That succeeds with prob. q

N. Sinclair, et al., 2014
SG, et al., 2015

Entangled qubits emitted each T sec, and repeater nodes make simultaneous BSMs



Rate calculation

$$\eta = e^{-\alpha L}$$

$$p = c\eta^{1/N}$$

$$q = \text{BSM success prob at repeater node}$$

$$R = \frac{\left(1-(1-p)^M\right)^N q^{N-1}}{T} \text{ ebits/sec}$$

$$R(L) = \max_N R_N(L)$$

Show that: **Advanced Problem 20 (a)**

$$R(L) \sim \eta^s,\ s < 1 \Rightarrow R(L) \sim e^{-s\alpha L},\ s < 1$$

Find s as a function of c, q

Plot the entanglement generation rates:

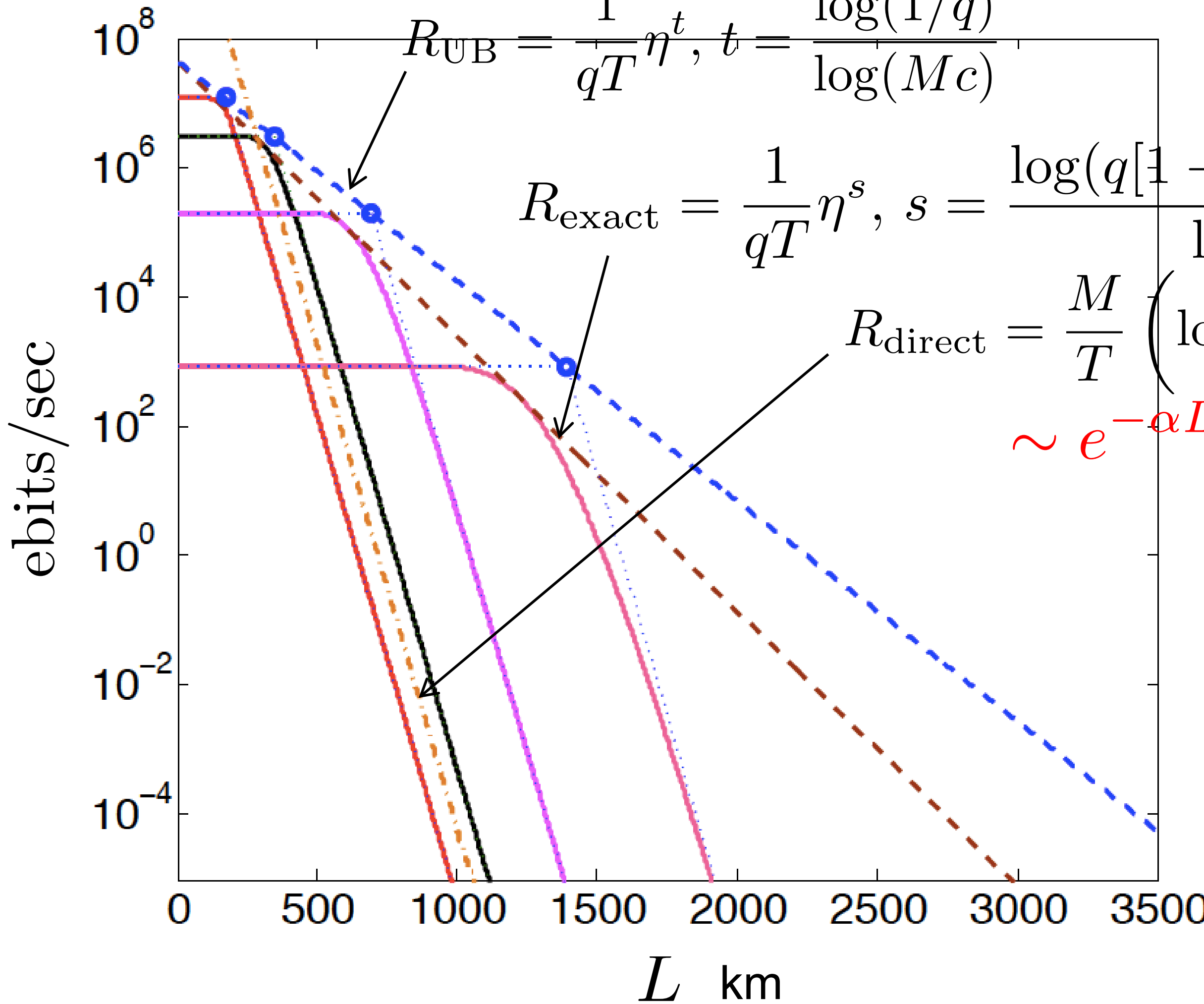
THE UNIVERSITY OF ARIZONA

$$R_{\mathrm{UB}} = \frac{1}{qT}\eta^t,\ t = \frac{\log(1/q)}{\log(Mc)}$$

$$R_{\mathrm{exact}} = \frac{1}{qT}\eta^s,\ s = \frac{\log(q[1-(1-cz)]^M)}{\log(z)} \sim e^{-s\alpha L},\ s<1$$

$$R_{\mathrm{direct}} = \frac{M}{T}\left(\log_2\frac{1}{1-\eta}\right) \approx \frac{M}{T}\frac{1}{\ln 2}\eta,\ \eta \ll 1$$

$$\sim e^{-\alpha L}$$



$$M = 1000$$

$$T = \frac{1}{30\times 10^6}$$

$$q = 0.255$$

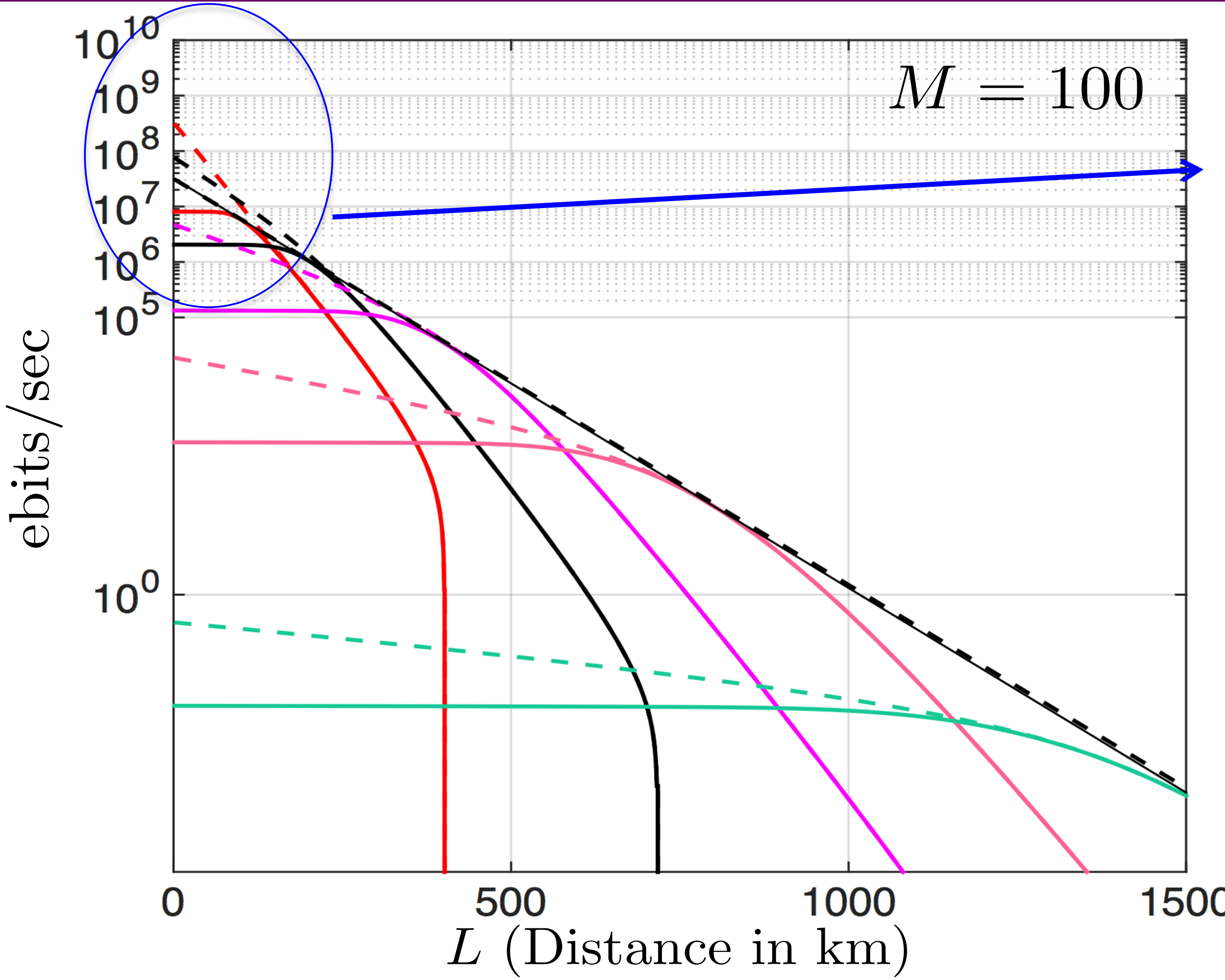
$$c = 0.405$$

Fiber loss (α), 0.2 dB/km

$$[1-(1-cz)^M]\log[q(1-(1-cz)^M)] = cMz\log(z)(1-cz)^{M-1}$$

SG et al., Phys. Rev. A 92, 022357, 2015

Using multiple successes within an elementary link can improve low-range rate



Low loss link range:

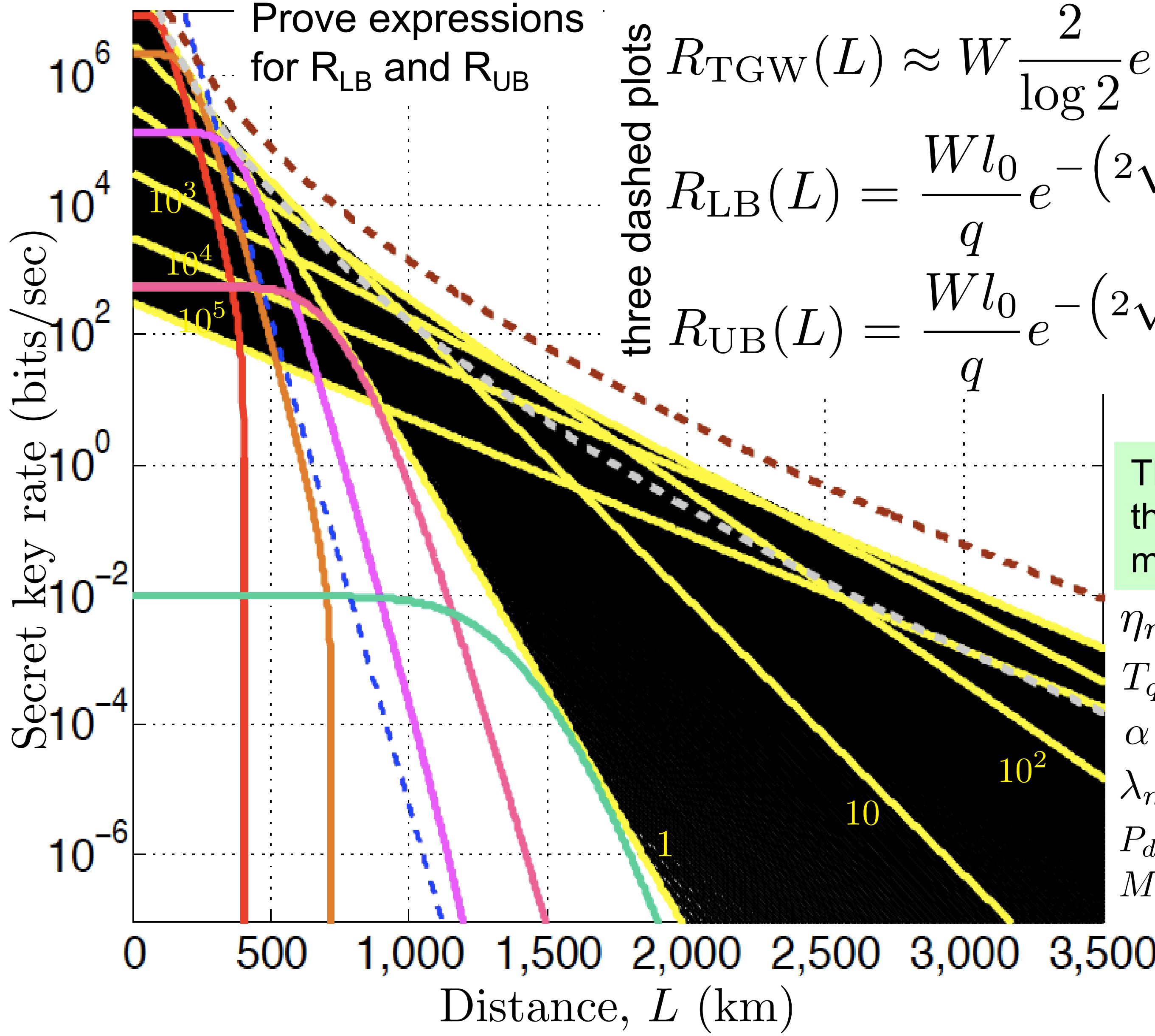
Multiplexing over multiple successful entanglements over links, using higher-order modulation, etc., can help improve rate.

Long range:

The simple single-photon dual-rail single-success-in-a-block protocol suffices

SG, et al., unpublished memo DARPA Quiness program

Multiplexing over time and frequency modes: sub-exponential rate-distance scaling



Prove expressions for R_{LB} and R_{UB}

three dashed plots

$$R_{\mathrm{TGW}}(L) \approx W \frac{2}{\log 2} e^{-\alpha L}$$

$$R_{\mathrm{LB}}(L) = \frac{W l_0}{q} e^{-\left(2\sqrt{\log([1-e^{-1}]/q)}\right)\sqrt{\alpha L}}$$

$$R_{\mathrm{UB}}(L) = \frac{W l_0}{q} e^{-\left(2\sqrt{\log(1/q)}\right)\sqrt{\alpha L}}$$

Advanced Problem 20 (b)

The numbers in yellow are the number of temporal modes, m

$$\eta_r = \eta_d = \eta_e = 0.9$$
$$T_q = 50\,\mathrm{ns}$$
$$\alpha = 0.15\,\mathrm{dB/km}$$
$$\lambda_m = 10^{-0.1\gamma_m},\ \gamma_m = 1(\mathrm{dB})$$
$$P_d = P_r = P_e = 3 \times 10^{-5}$$
$$M = 100, T = 50\,\mathrm{ns}, W = 2\,\mathrm{GHz}$$

Upcoming topics

- Quantum Networks
- Non-deterministic amplifiers and CV repeaters
- Bosonic codes (time permitting)