Fundamental rate-loss tradeoff for optical quantum key distribution

Masahiro Takeoka (NICT)

Saikat Guha (BBN)

Mark M. Wilde (LSU)

Quantum Krispy Kreme Seminar @LSU

January 30, 2015

Outline

- Motivation

- Main result

- Problem setting (generic QKD protocol)
  and proof outline

- Future outlook

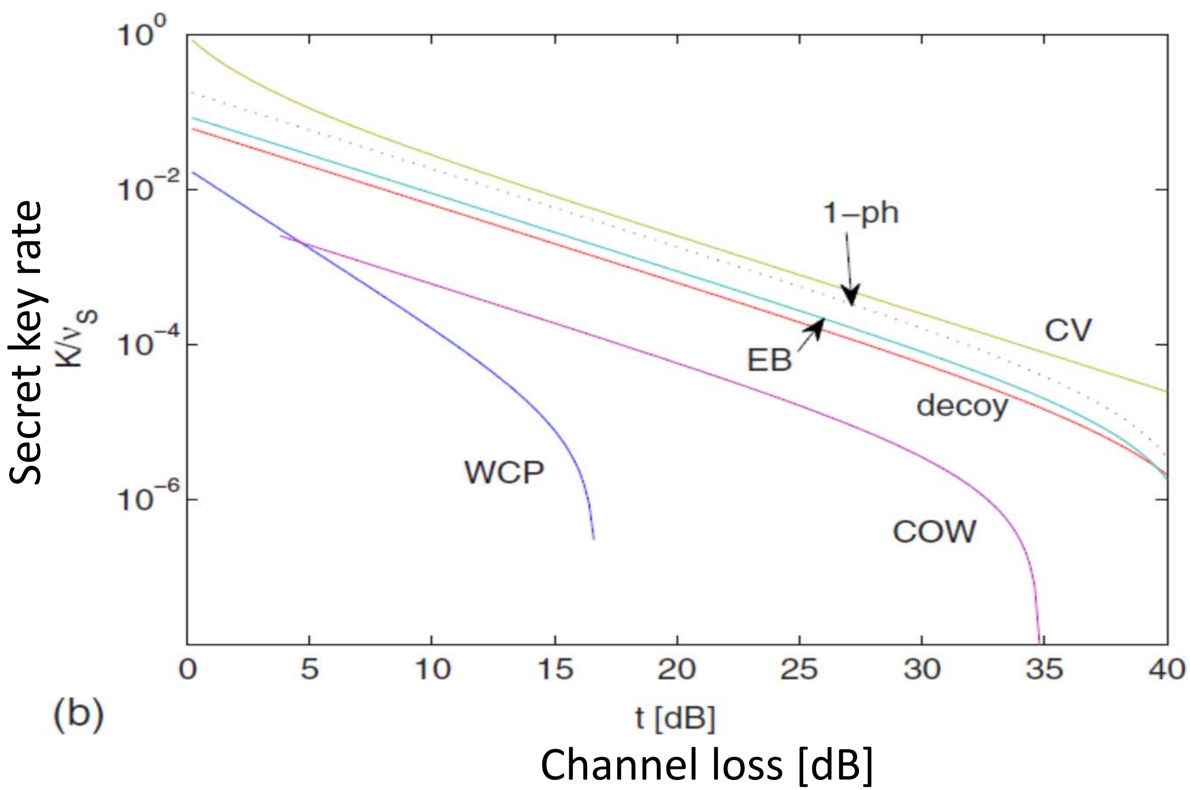
Motivation

- Quantum Key Distribution can generate a shared key perfectly secret against any eavesdropper.

- Various (repeaterless) QKD protocols have been proposed so far.

- In all known protocols, the key rate decreases linearly with respect to the channel loss.

Various QKD protocols



Platform	Parameter	Set 1	Set 2
BB84, COW	μ (mean intensity)	(Opt.)	(Opt.)
	V (visibility): P&M	0.99	0.99
	V (visibility): EB	0.96	0.99
	t_B (transmission in Bob's device)	1	1
	η (detector efficiency)	0.1	0.2
	p_d (dark counts)	10^{-5}	10^{-6}
	ε (COW) (bit error)	0.03	0.01
	ζ (EB) (coherent four photons)	0	0
	Leak (EC code)	1.2	1
CV	$v=v_A+1$ (variance)	(Opt.)	(Opt.)
	ε (optical noise)	0.005	0.001
	η (detector efficiency)	0.6	0.85
	v_{el} (electronic noise)	0.01	0
	β (EC code)	0.9	0.9

Scarani et al., Rev. Mod. Phys. 81, 1301 (2009)

Example1: Ideal single-photon BB84

- Secret key generation rate for the single-photon effcient BB84

Scarani et al., RMP 81, 1301 (2009)

$$\boxed{R = p_{\mathrm{sift}}\eta\eta_B\eta_D(1-2h(Q))/2}$$

η: channel transmissivity
η_B: Bob's device efficiency
η_D: Bob's detector efficiency
Q: QBER
p_{sift}: sifting rate
$h(\cdot)$: binary entropy

- Ideal case

$$\eta_B = \eta_D = 1, \quad Q = 0$$

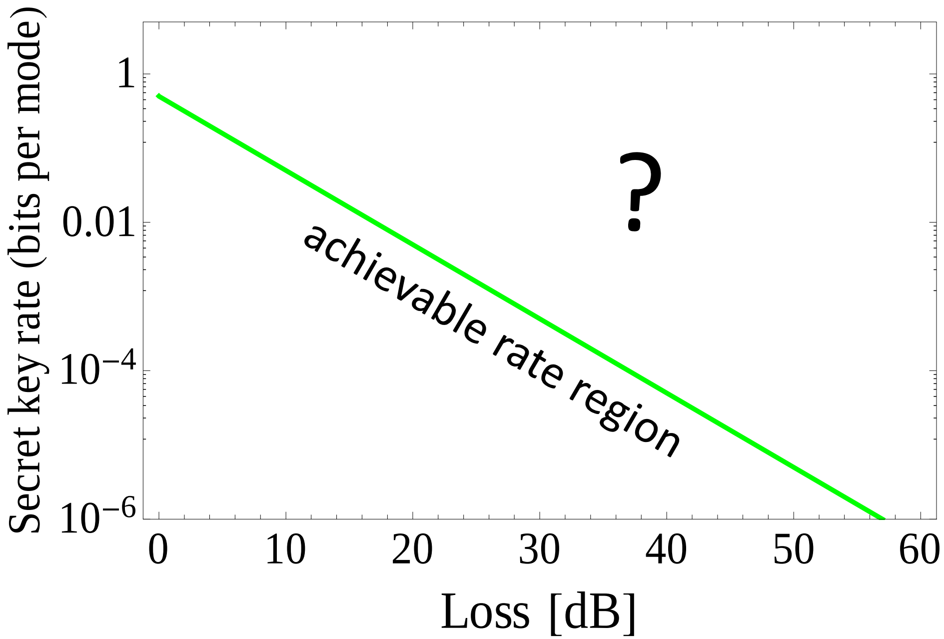
$$p_{\mathrm{sift}} \to 1$$

(efficient BB84 protocol)

Lo et al., J. Crypt. 18, 133 (2006)

Key rate (per mode, pulse)

$$\boxed{R = \eta/2}$$



Example2: CV-QKD (GG02)

Scarani et al., RMP 81, 1301 (2009)

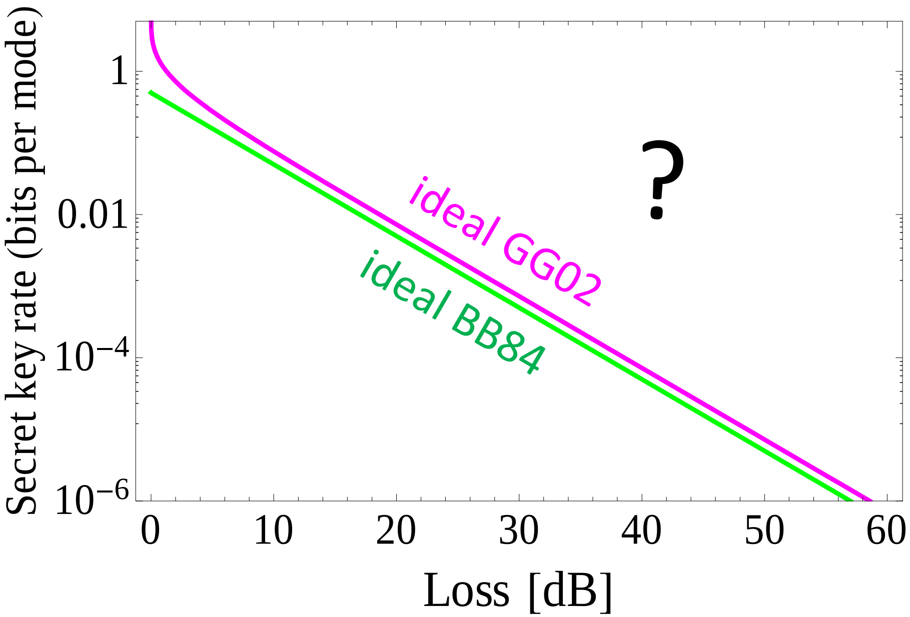
$$R = \beta I(A;B) - \chi(B;E)$$

ϵ: optical noise
η_D: Bob's detector efficiency
v_D: electronics noise
β: EC efficiency

- Ideal case

$$\eta_D = 1, \quad \epsilon = v_D = 0$$

$$\beta = 1$$



Example3: Reverse Coherent Information

Garcia-Patron et al., PRL 102, 210501 (2009)
Pirandola et al., PRL 102, 050503 (2009)

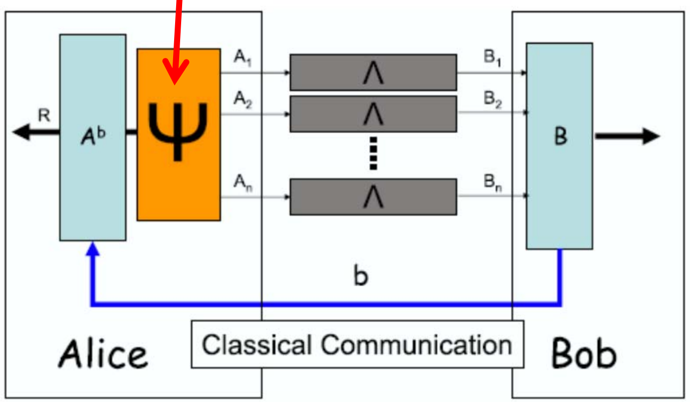
$$R = \max_{\rho} I_R(\rho_{RB})$$

Reverse coherent information

$$I_R(\rho_{RB}) = H(R)_\rho - H(RB)_\rho$$

$H(R)_\rho$: von Neumann entropy of $\mathrm{Tr}_B[\rho_{RB}]$

$\psi^{\otimes n}$

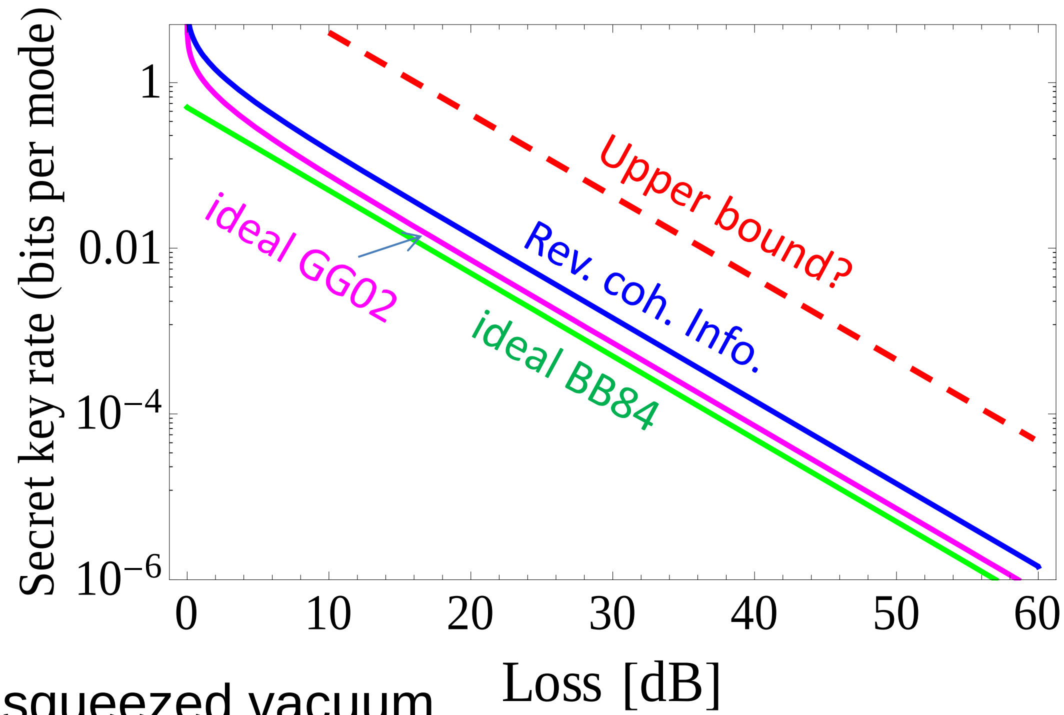


Garcia-Patron et al., PRL 102, 210501 (2009)

For a lossy channel

$$\max_{\rho} I_R(\rho_{RB}) = \log_2 \frac{1}{1-\eta}$$

with (infinitely strong) two-mode squeezed vacuum



Question

Is this a fundamental rate-loss tradeoff in any optical QKD?

Are there yet-to-be-discovered optical QKD protocols that could circumvent the linear rate-loss tradeoff (without repeaters or trusted notes)?

Our result

MT, S. Guha, M. M. Wilde, Nat. Commun. 5; 5235 (2014)

- We show that this is the rate-loss trade off is a fundamental limit.

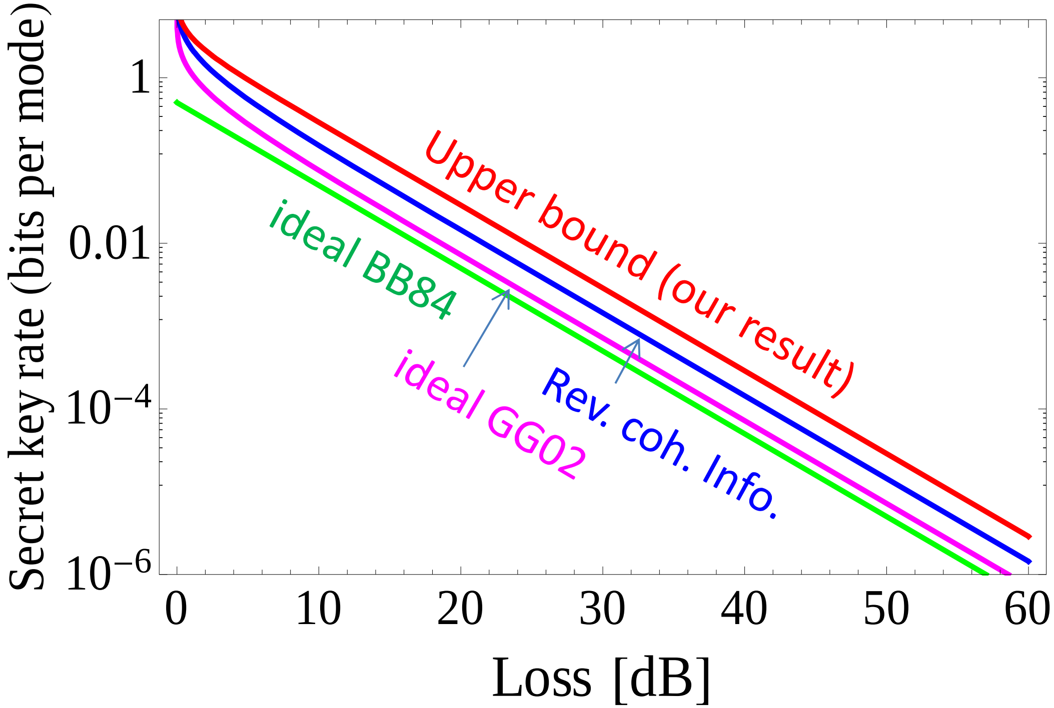
- We prove that the secret key agreement capacity (private capacity) of a lossy optical channel assisted by two-way public classical communication is *upper bounded* by:

$$\log_2 \frac{1+\eta}{1-\eta}$$

$$\Updownarrow$$

$$\log_2 \frac{1}{1-\eta}$$

(Rev. coh. info. LB)



η: channel transmittance

Rest of the talk

- Generic point-to-point QKD protocol and its capacity
  (secret key agreement capacity assisted by two-way
  public classical communication)

- Squashed entanglement of a quantum channel
  as an upper bound on the two-way assisted SKA capacity

- Pure-loss optical channel

- Loss and noise optical channel

- Summary

Rest of the talk

- Generic point-to-point QKD protocol and its capacity (secret key agreement capacity assisted by two-way public classical communication)

- Squashed entanglement of a quantum channel as an upper bound on the two-way assisted SKA capacity

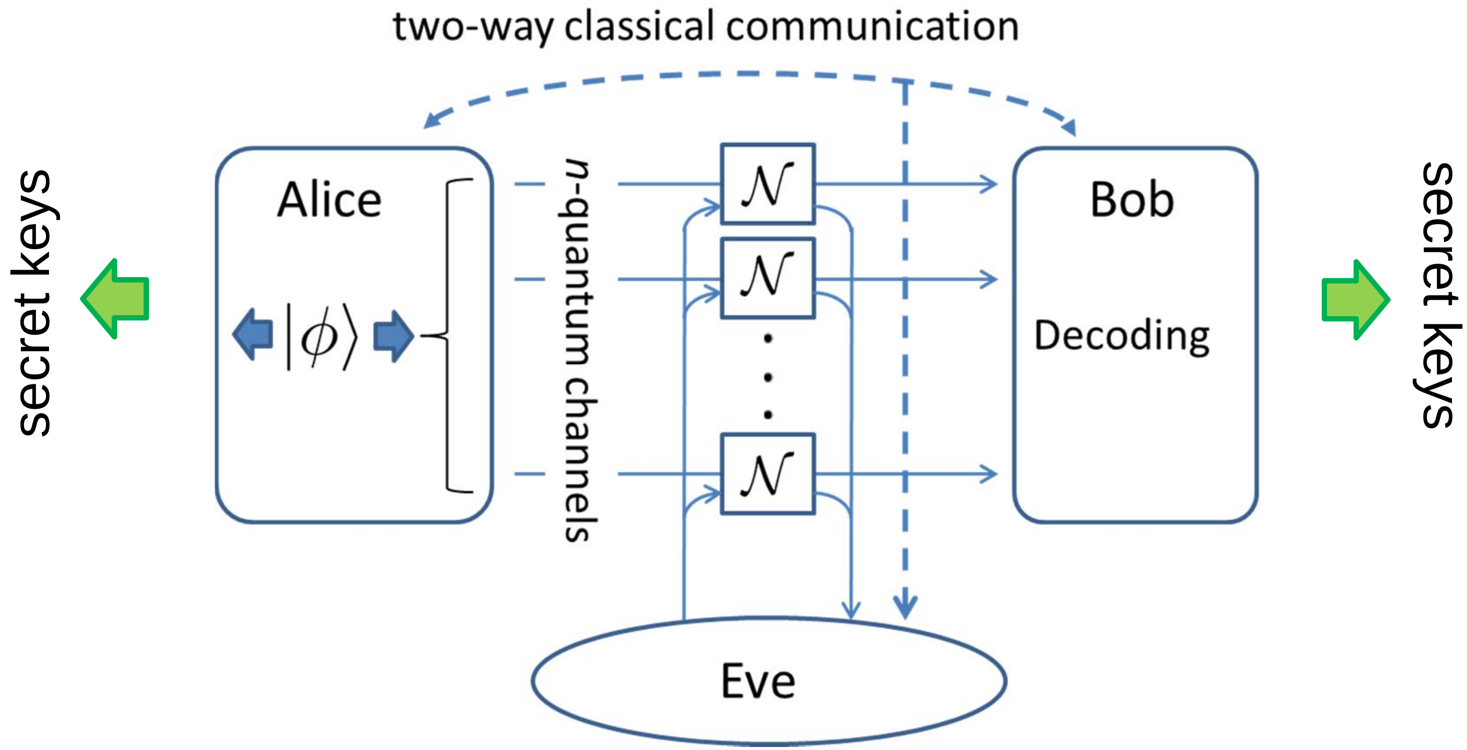
- Pure-loss optical channel

- Loss and noise optical channel

- Summary

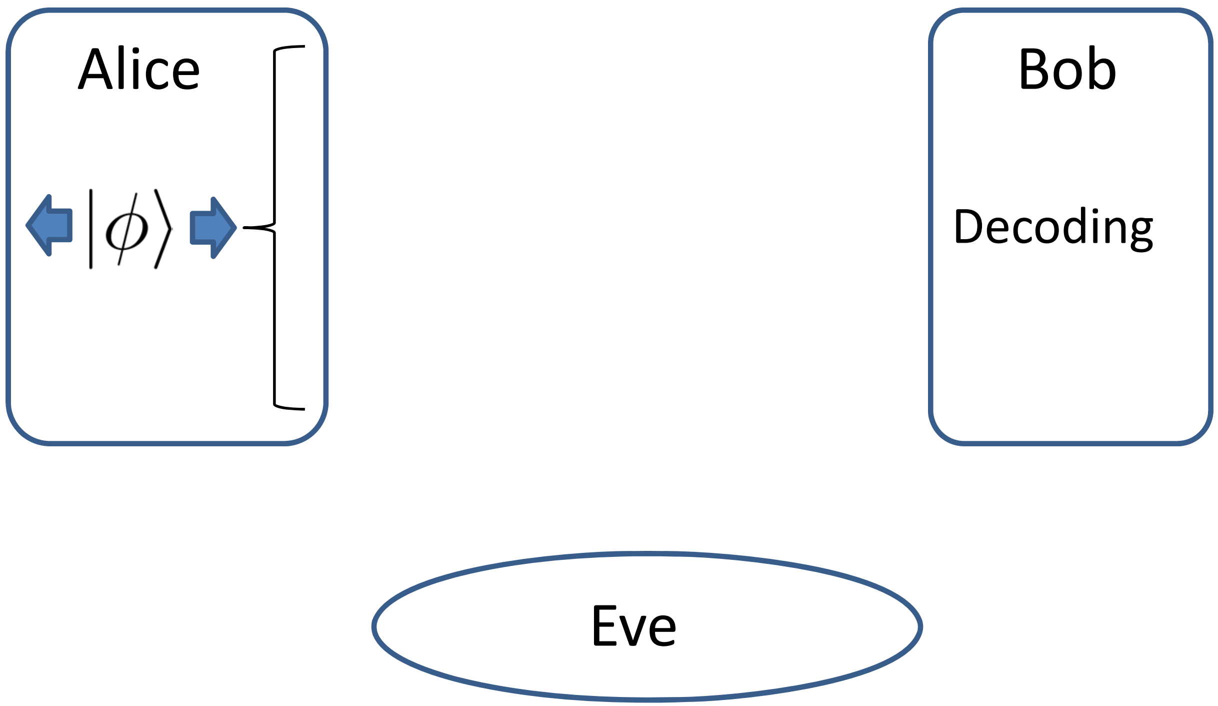
General point-to-point QKD

General secret key agreement assisted by
unlimited two-way public classical communication

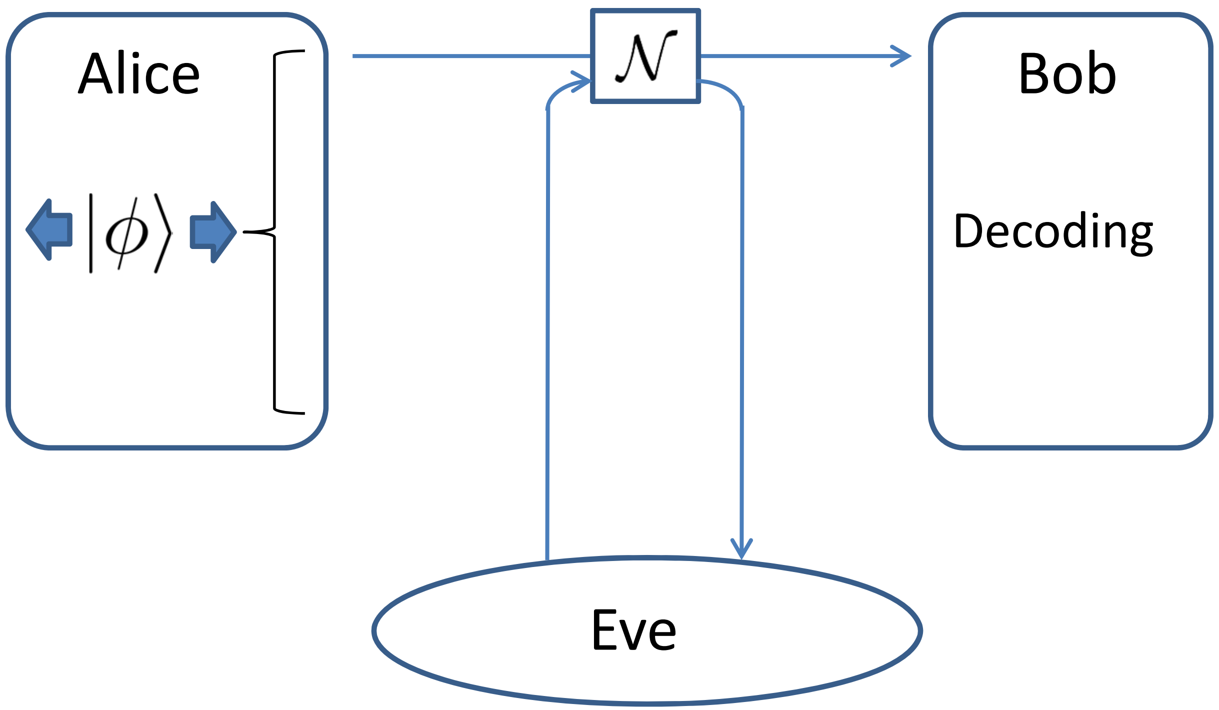


General secret key agreement assisted by
unlimited two-way public classical communication

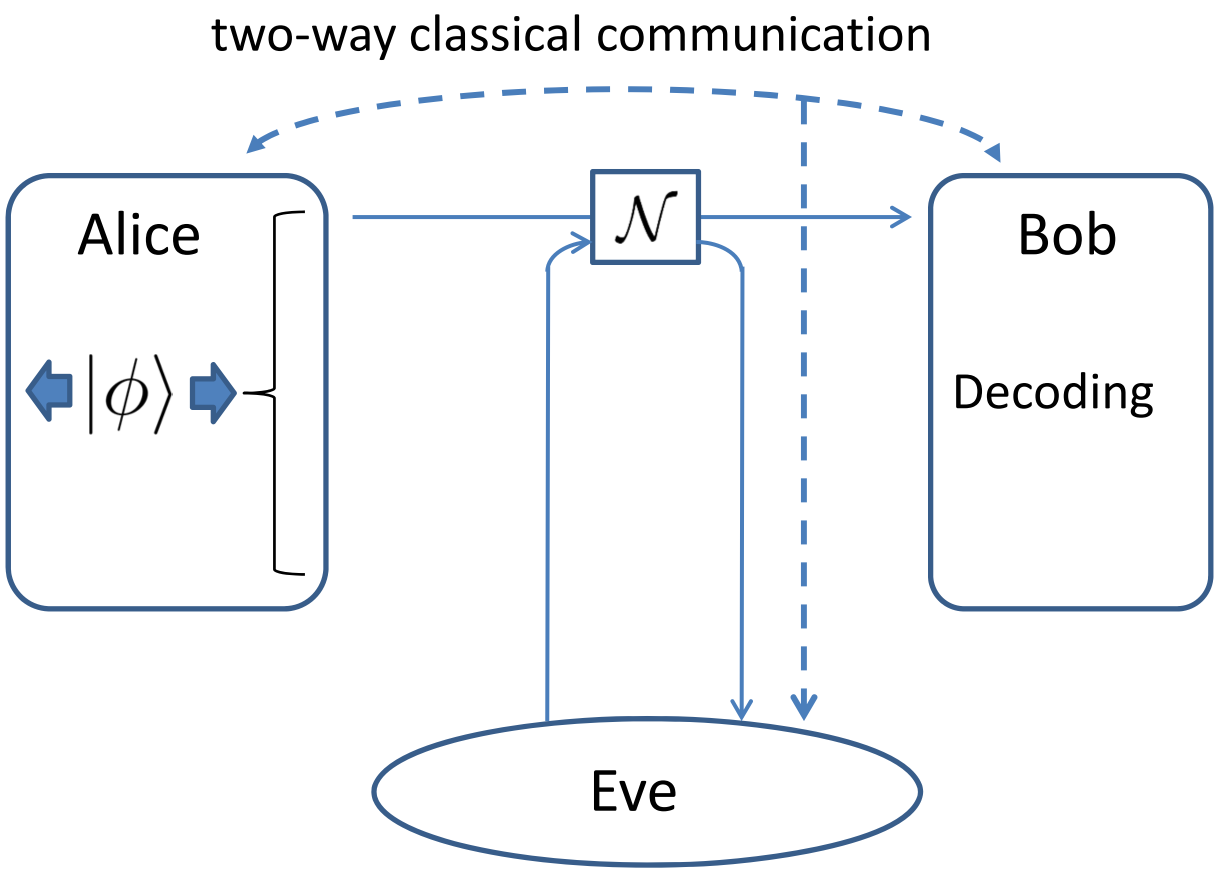
General point-to-point QKD



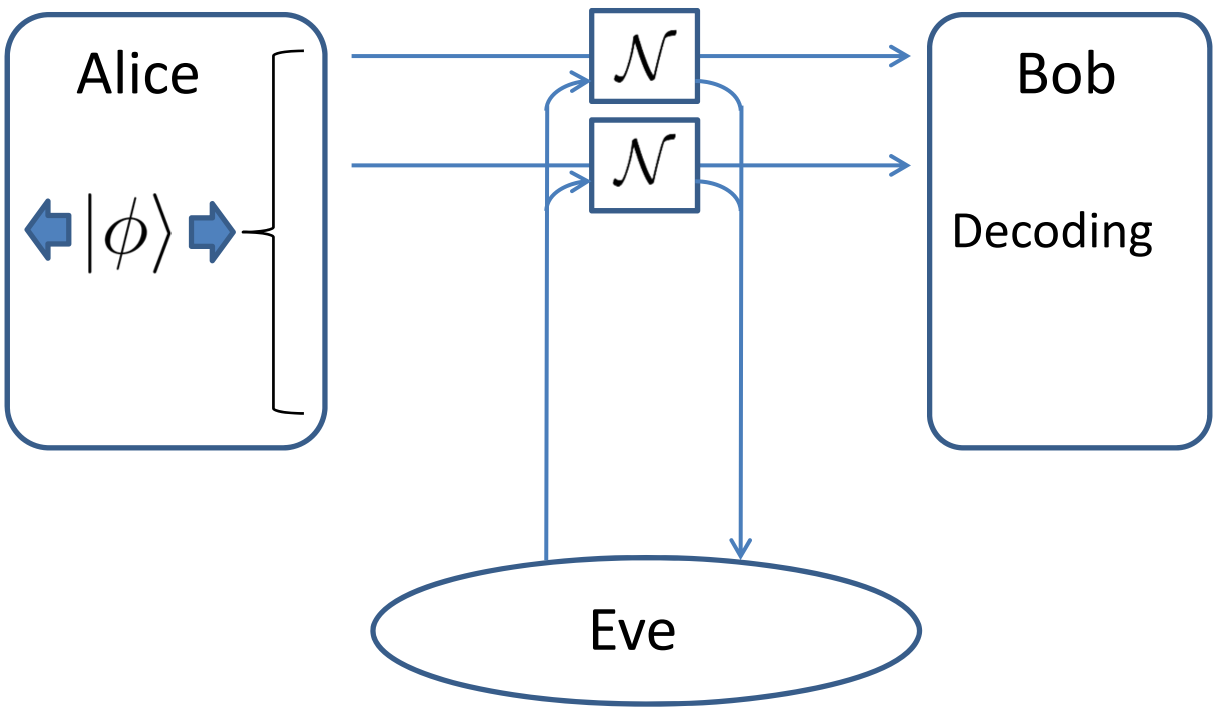
General point-to-point QKD



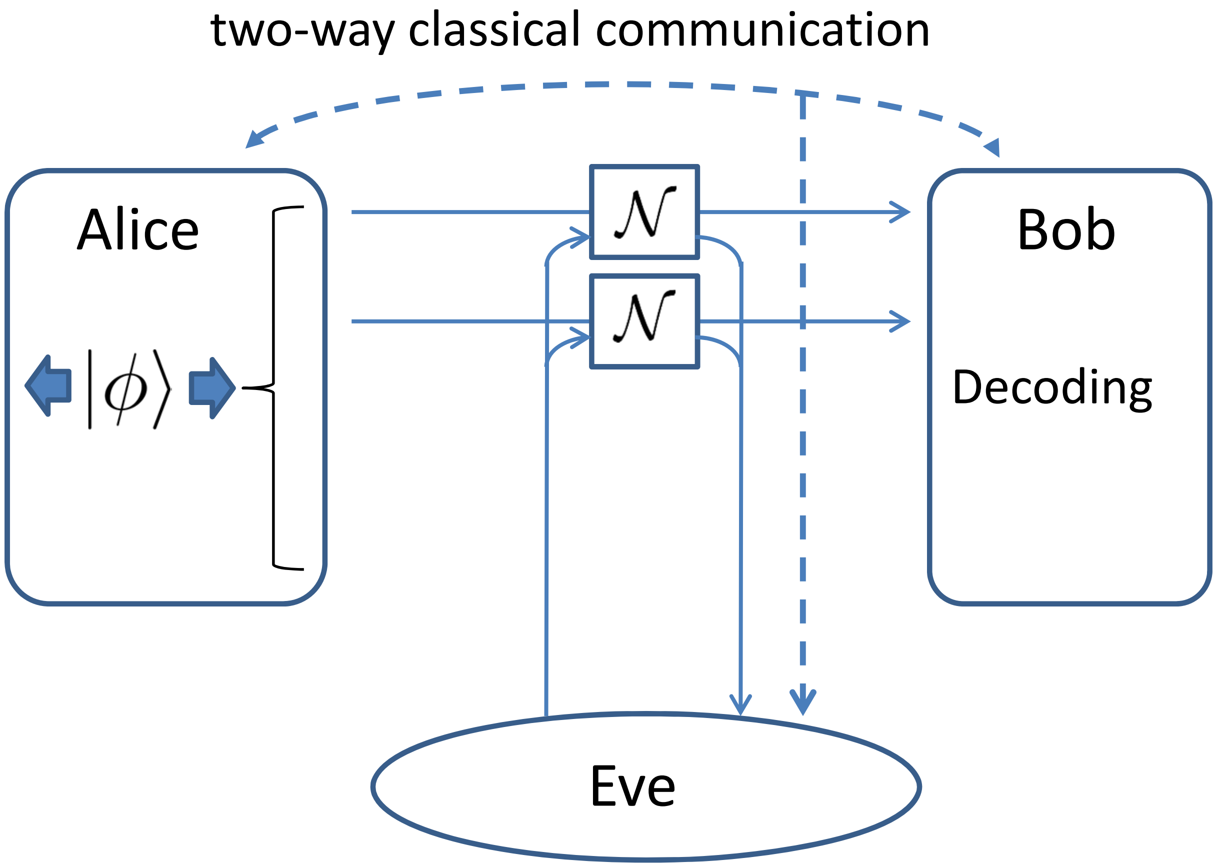
General point-to-point QKD



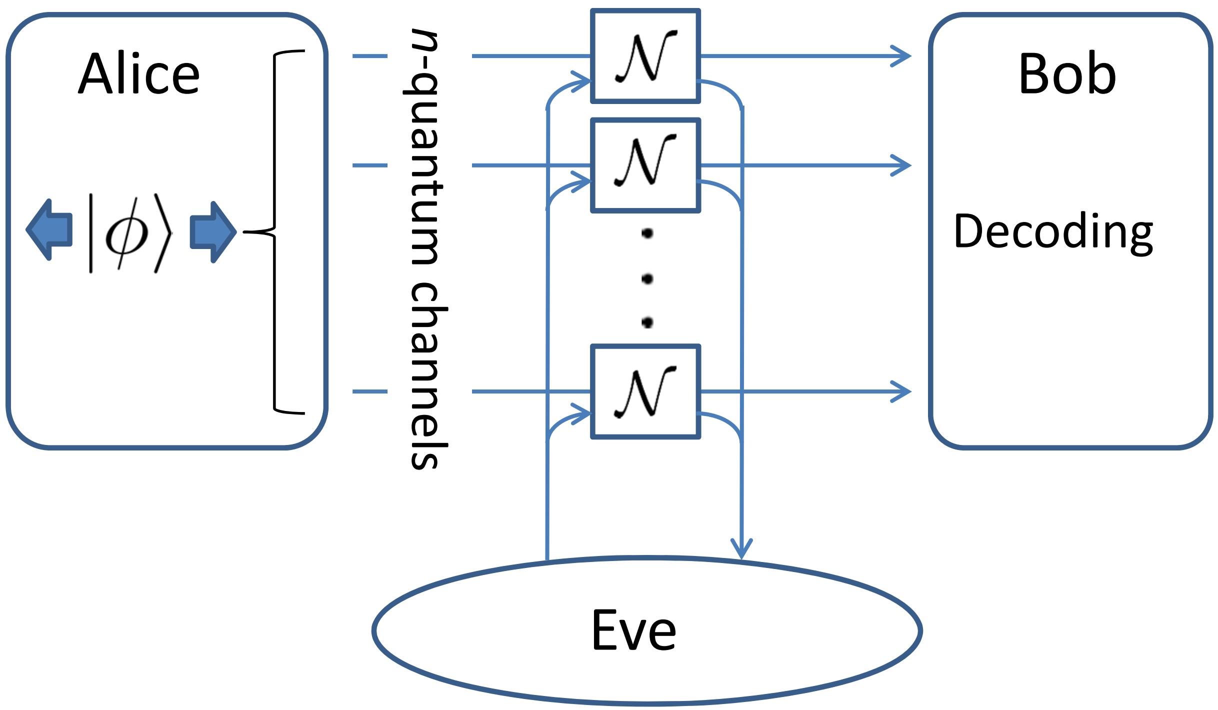
General point-to-point QKD



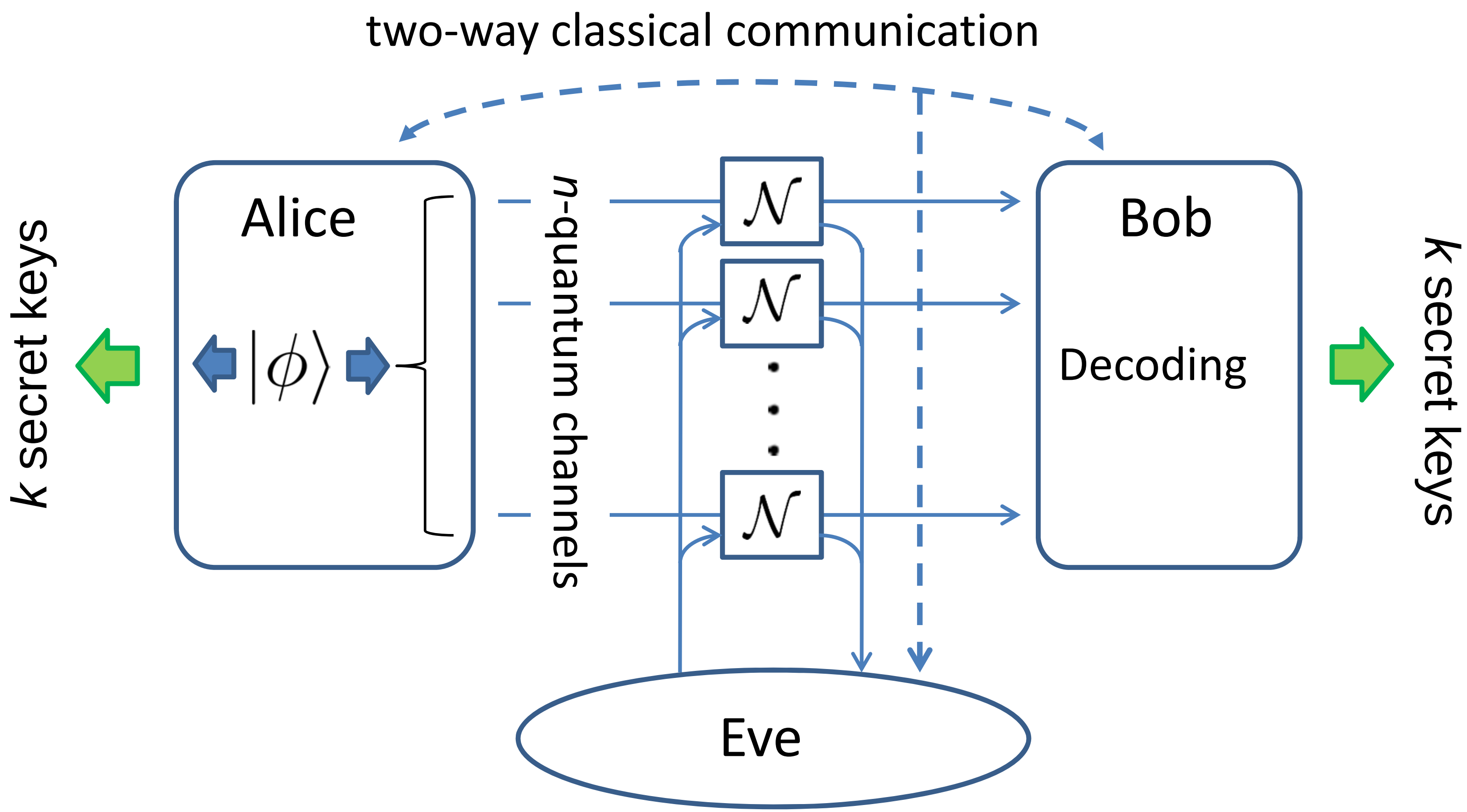
General point-to-point QKD



General point-to-point QKD



General point-to-point QKD



Secret key generation rate: $R=k/n$

Rest of the talk

- Generic point-to-point QKD protocol and its capacity
  (secret key agreement capacity assisted by two-way
  public classical communication)

- Squashed entanglement of a quantum channel
  as an upper bound on the two-way assisted SKA capacity

- Pure-loss optical channel

- Loss and noise optical channel

- Summary

Upper bound on the key rate: squashed entanglement of a quantum channel

$$\boxed{R \leq E_{\mathrm{sq}}(\mathcal{N}) = \max_{|\psi\rangle_{AA'}} E_{\mathrm{sq}}(A;B)_{\rho}}$$

$E_{\mathrm{sq}}(\mathcal{N})$: Squashed entanglement of a quantum channel

MT, Guha, Wilde, IEEE Trans. Info. Theory 60, 4987 (2014)

$E_{\mathrm{sq}}(A;B)_{\rho}$: Squashed entanglement
(of a bipartite state ρ_{AB})

Christandl, Winter, J. Math. Phys. 45, 829 (2004)

Squashed entanglement

Squashed entanglement: $E_{sq}(A;B)$

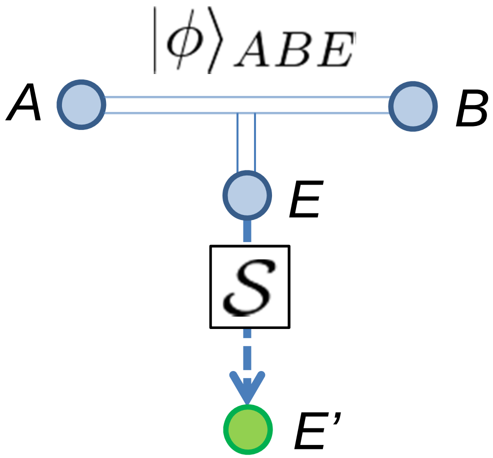
Christandl, Winter, J. Math. Phys. 45, 829 (2004)

$$E_{sq}(A;B)_\rho \equiv \frac{1}{2} \inf_{S_{E\to E'}} I(A;B|E')_\rho$$

$I(A;B|E')_\rho$ conditional quantum mutual information

$$= H(AE')_\rho + H(BE')_\rho - H(ABE')_\rho - H(E')_\rho$$

$$H(A)_\rho = -\mathrm{Tr}[\rho_A \log \rho_A]$$



$$\rho_{AB} = \mathrm{Tr}_E[|\phi\rangle\langle\phi|_{ABE}]$$

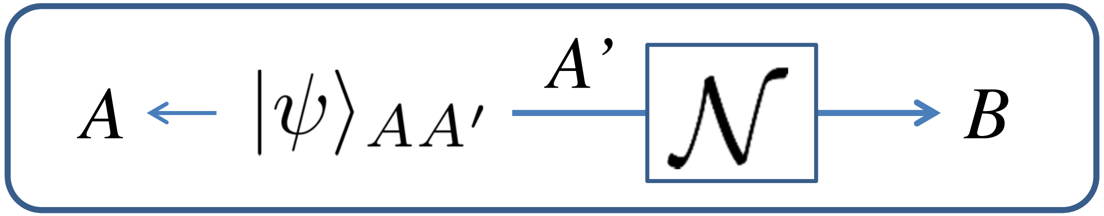
Channel *S* should be chosen to *squash* the quantum correlations between Alice and Bob (the squashing channel)

- Entanglement measure for a bipartite state (LOCC monotone, …)
- Inspired by secrecy capacity upper bound in classical theory (intrinsic information)

Squashed entanglement of a quantum channel

Definition:

$$E_{sq}(\mathcal{N}) = \max_{|\psi\rangle_{AA'}} E_{sq}(A;B)_\rho \quad \text{where} \quad \rho_{AB} = \mathcal{N}_{A'\to B}(|\psi\rangle\langle\psi|_{AA'})$$



Main theorem

Theorem1

$E_{\mathrm{sq}}(N)$ is an upper bound on the secret key generation rate *R*

$$R \leq E_{\mathrm{sq}}(\mathcal{N})$$

MT, Guha, Wilde, IEEE Trans. Info. Theory 60, 4987 (2014)

Proof outline

1. Secret key distillation upper bound

   Christandl, et al., arXiv:quant-ph/0608119

2. New subadditivity inequality
   for the squashed entanglement

Proof outline

1. Secret key distillation upper bound

Theorem 3.7. Squashed entanglement $E_{\rm sq}(A;B)_\rho$ is an upper bound on the distillable key rate from a tensor product state $\rho_{AB}^{\otimes n}$

Christandl, et al., arXiv:quant-ph/0608119

The statement is proved by using the following four properties:

1. Monotonicity (does not increase under LOPC)
2. Continuity: if $||\rho - \sigma||_1 \leq \epsilon$ then $|E_{\rm sq}(A;B)_\rho - E_{\rm sq}(A;B)_\sigma| \leq f(\epsilon)$ $\left(\lim_{\epsilon \to 0} f(\epsilon) \to 0\right)$
3. Normalization: $E_{\rm sq}(A;B)_\gamma \geq \log d$ γ: private state Horodecki et al, PRL 94, 160502 (2005)
4. Subadditivity on tensor product states: $\boxed{E_{\rm sq}(A^n;B^n)_{\rho^{\otimes n}} \leq n E_{\rm sq}(A;B)_\rho}$

The similar technique is applicable to the channel scenario *except 4*.

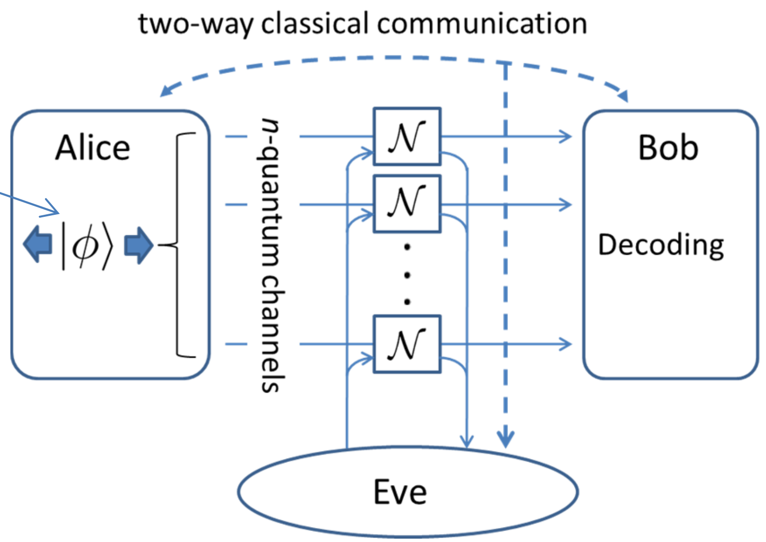
Proof outline

4. Subadditivity on tensor product states: $E_{\rm sq}(A^n;B^n)_{\rho^{\otimes n}} \le nE_{\rm sq}(A;B)_\rho$

Product state

Can be replaced by $E_{\rm sq}(\mathcal{N}^n) \le nE_{\rm sq}(\mathcal{N})$?

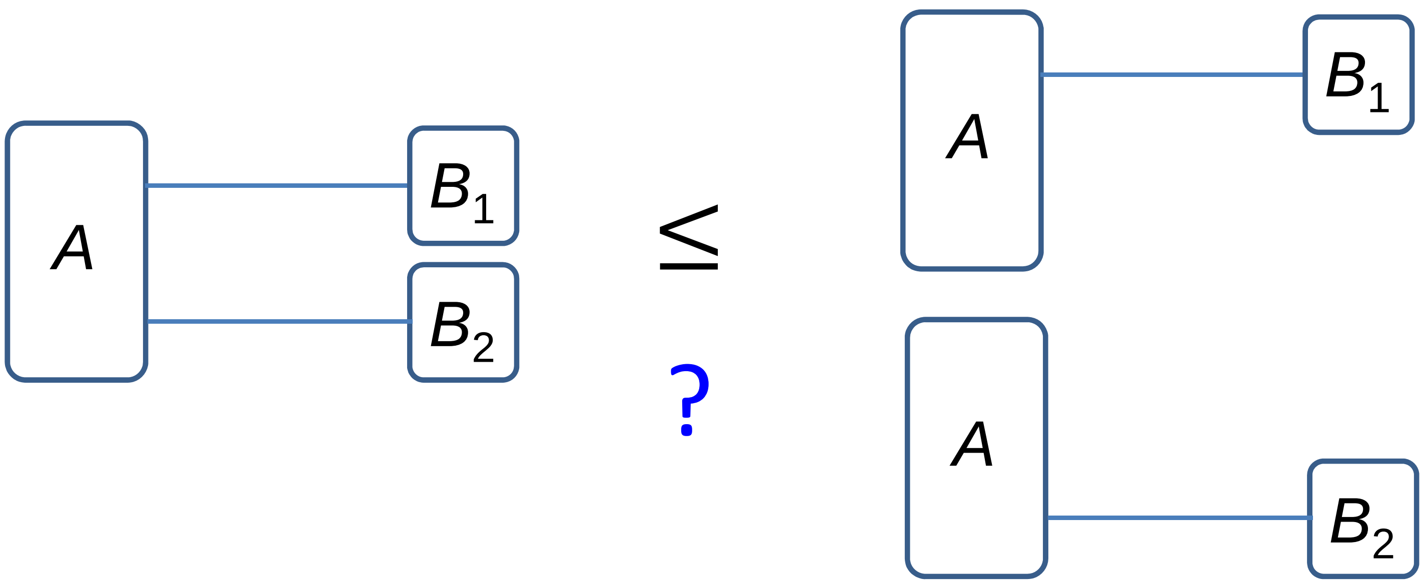
Could be entangled over *n*-channel use!



Subadditivity of $E_{sq}(N)$?

$E_{\mathrm{sq}}(\mathcal{N}^n) \leq n E_{\mathrm{sq}}(\mathcal{N})$ is true if one can show something like

$$E_{sq}(A;B_1B_2)_\rho \leq E_{sq}(A;B_1)_\rho + E_{sq}(A;B_2)_\rho \quad \left[A = A_1A_2\right]$$



Proof outline

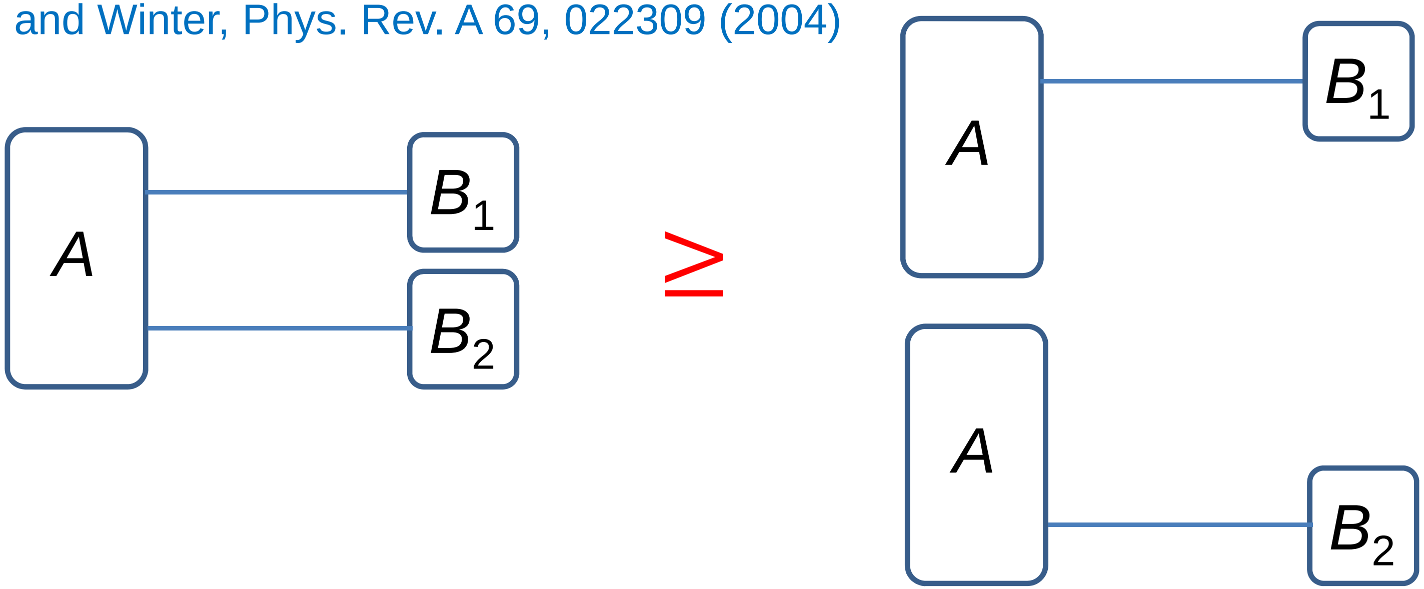
Subadditivity of E_{sq} ?

$E_{\mathrm{sq}}(\mathcal{N}^n) \le n E_{\mathrm{sq}}(\mathcal{N})$ is true if one can show something like

$$\xcancel{E_{sq}(A;B_1B_2)_\rho \le E_{sq}(A;B_1)_\rho + E_{sq}(A;B_2)_\rho} \qquad [A = A_1A_2]$$

$$\boxed{\begin{array}{l}\text{Monogamy of entanglement}\\ \quad E_{sq}(A;B_1B_2)_\rho \ge E_{sq}(A;B_1)_\rho + E_{sq}(A;B_2)_\rho\end{array}}$$

Koashi and Winter, Phys. Rev. A 69, 022309 (2004)



Proof outline

New subadditivity-like inequality

$E_{sq}(A;B_1B_2)_\rho \leq E_{sq}(A;B_1)_\rho + E_{sq}(A;B_2)_\rho$ is not possible.

However, we are able to show the following inequality:

Lemma

For any five-party pure state $\psi_{AB_1E_1B_2E_2}$

$$E_{sq}(A;B_1B_2)_\psi \leq E_{sq}(AB_2E_2;B_1)_\psi + E_{sq}(AB_1E_1;B_2)_\psi$$

holds.

MT, Guha, Wilde, IEEE Trans. Info. Theory 60, 4987 (2014)

Proof consists of a chain of (in)equalities based on

-Duality of conditional entropy $H(K|L) + H(K|M) = 0$ for $|\psi\rangle_{KLM}$

-Strong subadditivity $I(K;L|M)_\rho \geq 0$ for ρ_{KLM}

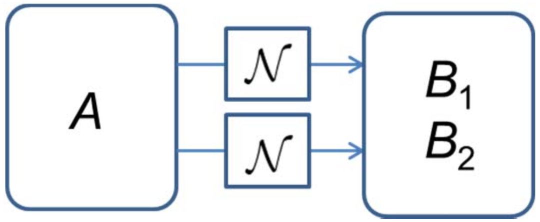
Proof outline

Additivity of $E_{\rm sq}(\mathcal{N})$

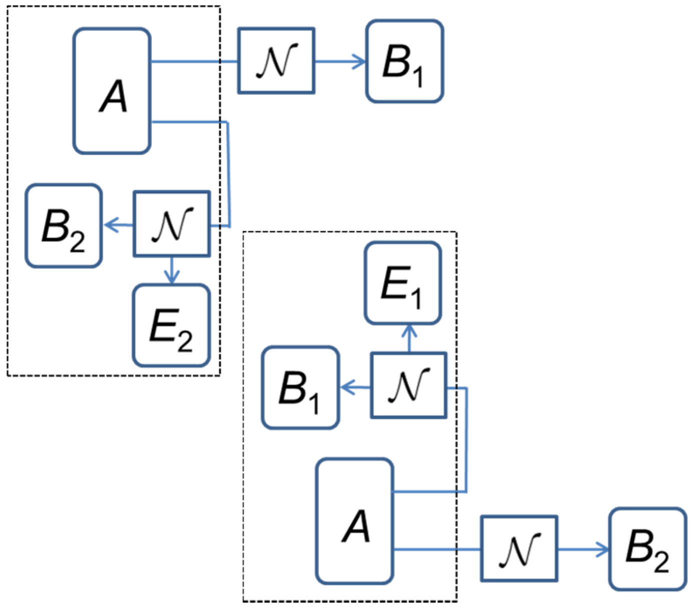
$$E_{sq}(A;B_1B_2)_\psi \le E_{sq}(AB_2E_2;B_1)_\psi + E_{sq}(AB_1E_1;B_2)_\psi$$

implies $E_{\rm sq}(\mathcal{N}^2) \le 2E_{\rm sq}(\mathcal{N})$

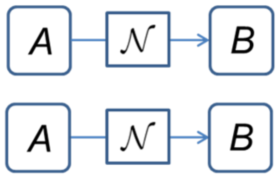
$$E_{\rm sq}(\mathcal{N}^2) = E_{\rm sq}(A;B_1B_2)_\varphi$$



$$\le E_{\rm sq}(AB_2E_2;B_1)_\varphi$$
$$+E_{\rm sq}(AB_1E_1;B_2)_\varphi$$



$$\le 2E_{\rm sq}(\mathcal{N})$$



$$\boxed{E_{\rm sq}(\mathcal{N}) \equiv \max_{|\phi\rangle_{AA'}} E_{\rm sq}(A;B)_\rho}$$

$$|\varphi\rangle_{AB_1E_1B_2E_2} \equiv U^{\mathcal{N}}_{A_1\to B_1E_1} \otimes U^{\mathcal{N}}_{A_2\to B_2E_2}|\phi\rangle_{AA_1A_2}$$

Proof outline

From the following four conditions:

1. Monotonicity (does not increase under LOPC)

2. Continuity: if $||\rho - \sigma||_1 \leq \epsilon$ then $|E_{\rm sq}(A;B)_\rho - E_{\rm sq}(A;B)_\sigma| \leq f(\epsilon)$ $\left[\lim_{\epsilon \to 0} f(\epsilon) \to 0 \right]$

3. Normalization: $E_{\rm sq}(A;B)_\gamma \geq \log d$ $\left[\gamma\text{: private state} \right]$

4. Additivity: $E_{\rm sq}(\mathcal{N}^n) \leq n E_{\rm sq}(\mathcal{N})$

One can show

$$\Rightarrow \quad \boxed{R \leq E_{\rm sq}(\mathcal{N}) + f(\epsilon)}$$

$$f(\epsilon) = \left(16\sqrt{\epsilon}\log d + 4h_2(2\sqrt{\epsilon})\right)/n$$

For the details of the proof, see

MT, Guha, Wilde, IEEE Trans. Info. Theory 60, 4987 (2014)

Rest of the talk

- Generic point-to-point QKD protocol and its capacity (secret key agreement capacity assisted by two-way public classical communication)

- Squashed entanglement of a quantum channel as an upper bound on the two-way assisted SKA capacity

- Pure-loss optical channel

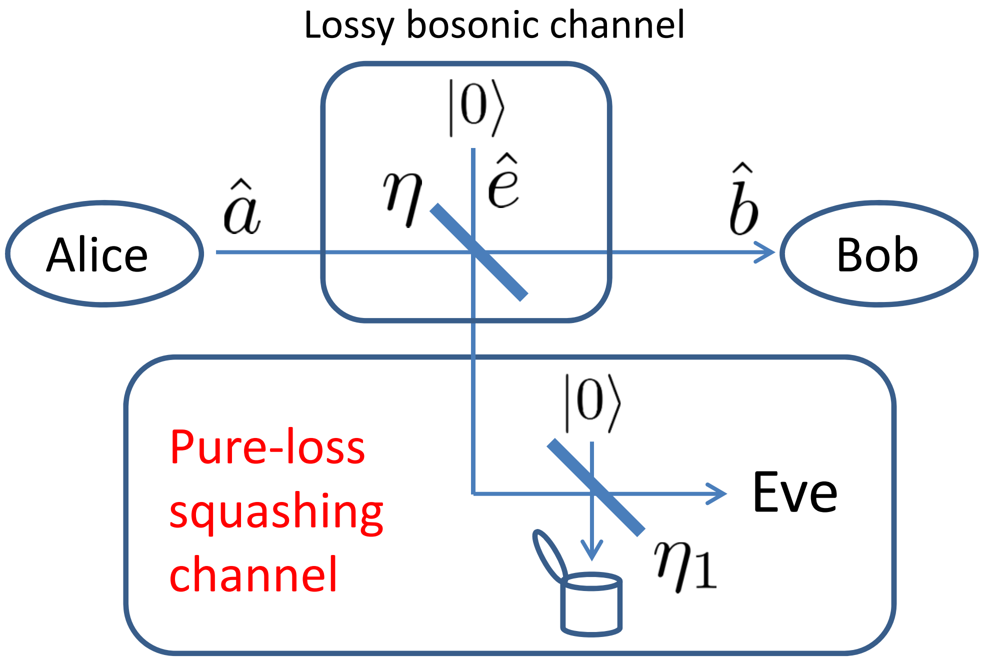
- Loss and noise optical channel

- Summary

Lossy bosonic channel

$$E_{sq}(\mathcal{N}_{LB}) = \max_{|\psi\rangle_{AA'}} E_{sq}(A;B)_\rho$$
$$= \max_{|\psi\rangle_{AA'}} \boxed{\inf_{\mathcal{S}_{E\to E'}}} \frac{1}{2} I(A;B|E')$$

Need to find a good squashing channel
(in a heuristic way...)



$I(A;B|E')$

minimized at $\eta_1 = 1/2$

maximized with $|\psi\rangle_{AA'}^{TMSV}$

(Two-mode squeezed
vacuum)

Lossy bosonic channel

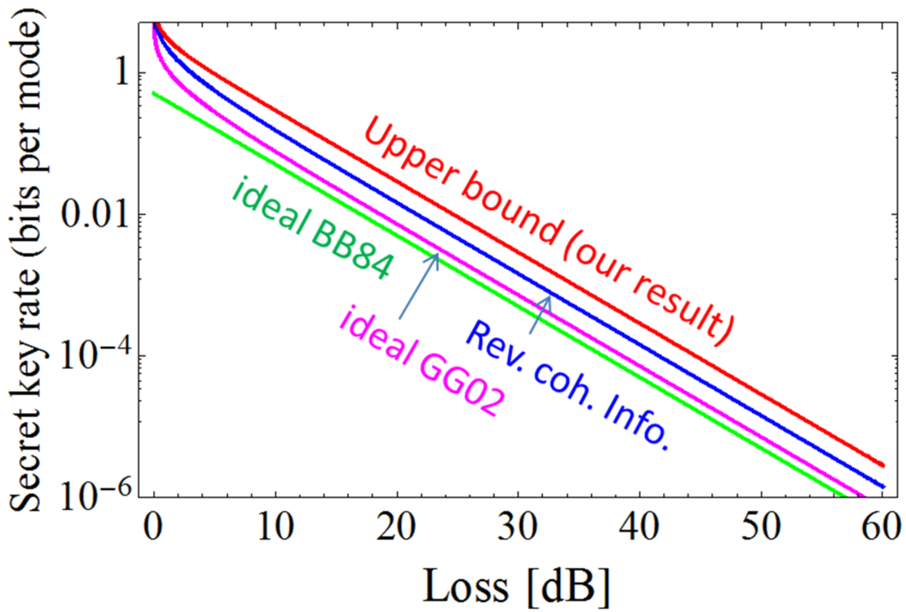
$$E_{sq}(\mathcal{N}_{LB}) \leq g((1+\eta)N_s/2) - g((1-\eta)N_s/2)$$

$$g(x) = (x+1)\log_2(x+1) - x\log_2 x$$

N_s: a mean input power
(average photon number of one share of the TMSV)

$$N_s \to \infty$$

$$\boxed{E_{sq}(\mathcal{N}_{LB}) \leq \log_2 \frac{1+\eta}{1-\eta}}$$



Rest of the talk

- Generic point-to-point QKD protocol and its capacity (secret key agreement capacity assisted by two-way public classical communication)

- Squashed entanglement of a quantum channel as an upper bound on the two-way assisted SKA capacity

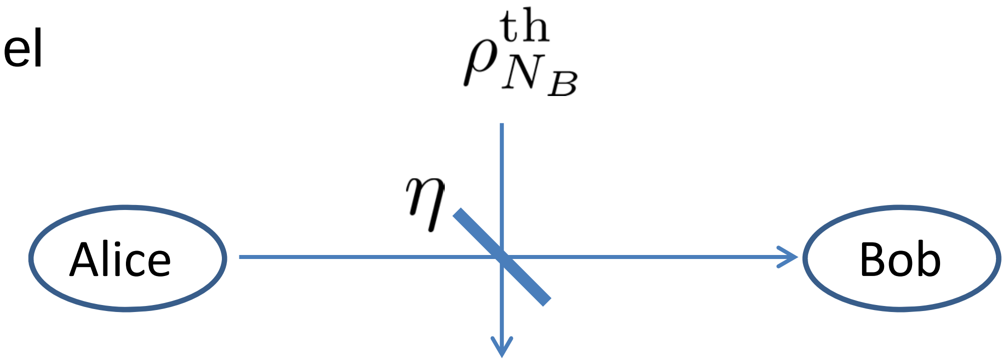
- Pure-loss optical channel

- Loss and noise optical channel

- Summary

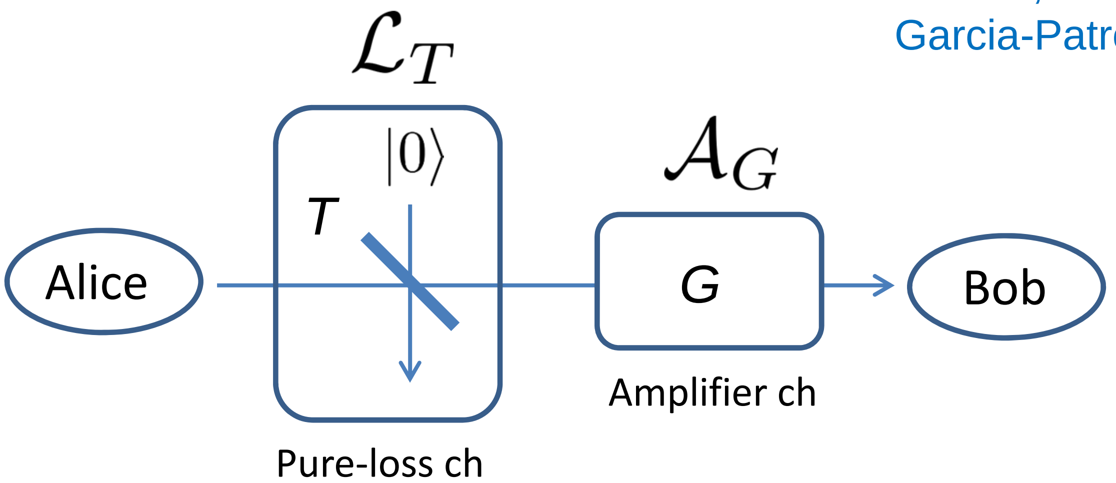
Loss and thermal noise channel

Channel model



Decomposition of the phase-insensitive Gaussian channel

Caruso, Giovannetti, Holevo, NJP 8, 310 (2006)
Garcia-Patron et al., PRL 108, 110505 (2012)



$$T = \frac{\eta}{(1-\eta)N_B + 1}$$

$$G = (1-\eta)N_B + 1$$

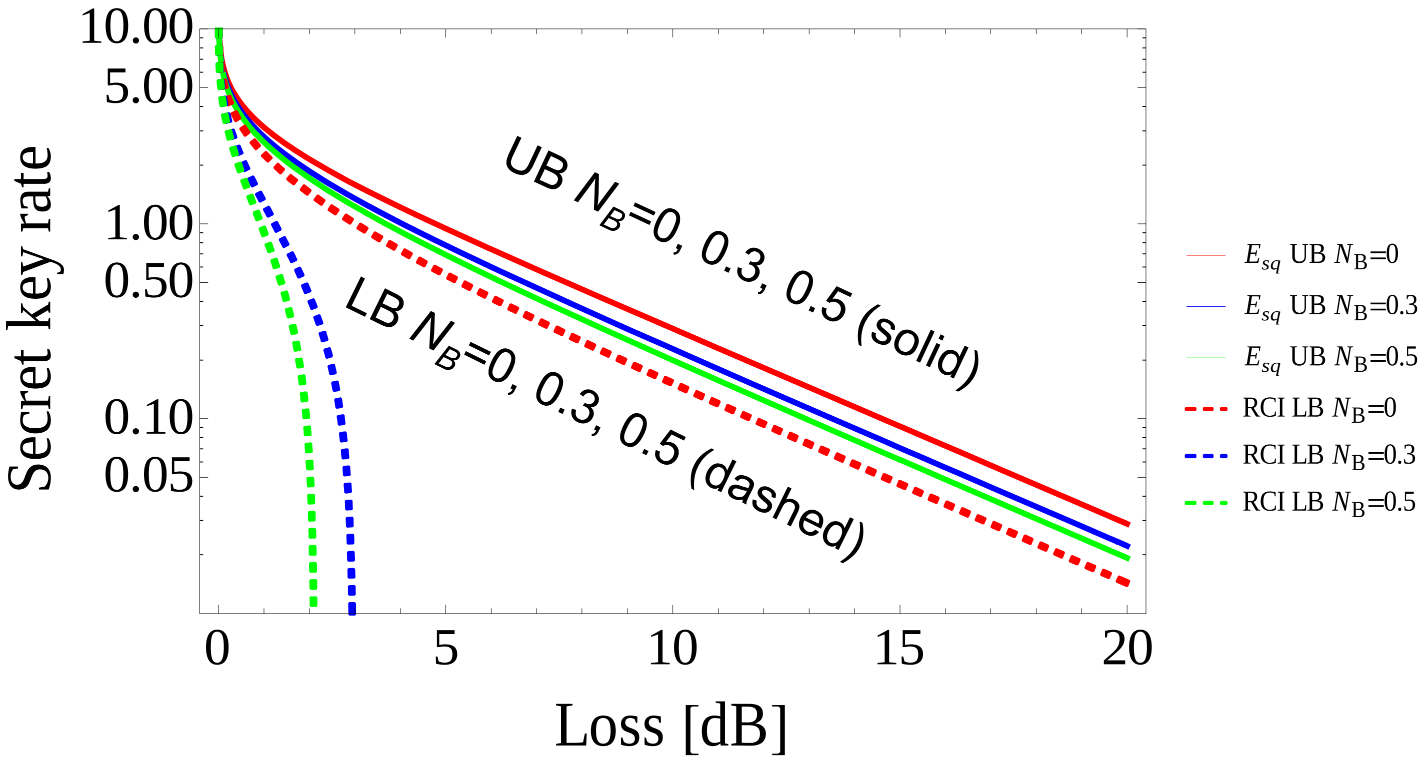
Loss and thermal noise channel

$$E_{sq}(\mathcal{N}) = E_{sq}(\mathcal{A}_G \circ \mathcal{L}_T) \leq E_{sq}(\mathcal{L}_T)$$

Data processing inequality
for quantum conditional mutual information

$$\Rightarrow \quad P_2(\mathcal{N}),\, Q_2(\mathcal{N}) \leq \log_2 \frac{1+T}{1-T} = \log_2 \frac{(1-\eta)N_B + 1 + \eta}{(1-\eta)N_B + 1 - \eta}$$

Out[17]=



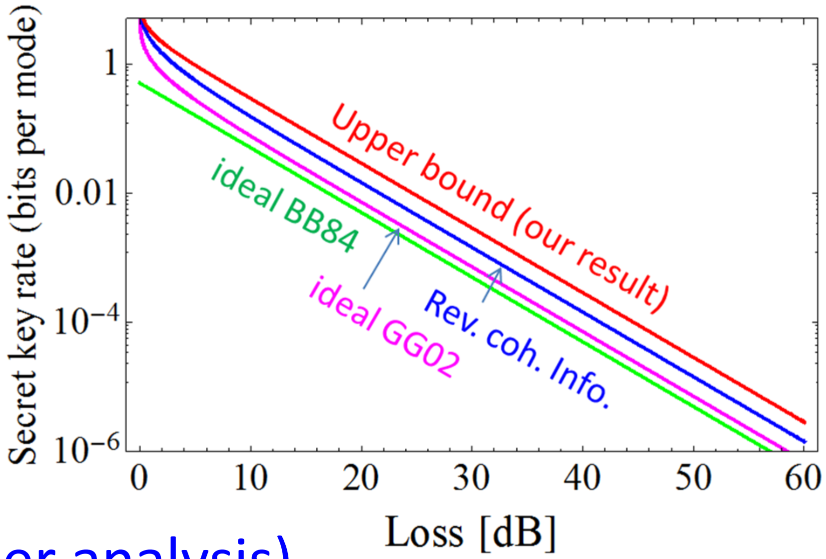
Summary

MT, Guha, Wilde, Nat. Commun. 5; 5235 (2014)
MT, Guha, Wilde, IEEE Trans. Info. Theory 60, 4987 (2014)

- The secret key rate of *any* repeaterless QKD protocols in a lossy optical channel is upper bounded by

$$\log_2 \frac{1+\eta}{1-\eta} \quad \text{(weak converse)}$$

- The bound is based on the squashed entanglement of a quantum channel, which is a general upper bound on the two-way classically assisted secret key agreement capacity.



- Open problems
  - True two-way assisted capacity?
  - Tight bound for noisy channel?
  - Finite block code analysis (needs strong converse or second order analysis)

Finite *n* analysis

- Our upper bound is a *weak converse*

  ⇒ For a tight upper bound on finite block length, a *strong converse* or a *second order analysis* should be established.

- However, we can estimate the effect of finite block length from our result.

$$R \leq E_{\mathrm{sq}}(\mathcal{N}) + f(\epsilon)$$

$$f(\epsilon) = \left(16\sqrt{\epsilon}\log d + 4h_2(2\sqrt{\epsilon})\right)/n$$

⇓

$$R \leq \frac{1}{1-16\sqrt{\epsilon}}\left(E_{\mathrm{sq}}(\mathcal{N}) + 4h_2(2\sqrt{\epsilon})/n\right)$$

Finite *n* analysis

$$R \leq \frac{1}{1-16\sqrt{\epsilon}} \left(E_{\rm sq}(\mathcal{N}) + 4h_2(2\sqrt{\epsilon})/n \right)$$

ε: secrecy (based on the trace distance criteria)
n: code length

Example in a pure-loss optical channel:

200 km fiber (0.2dB/km loss)

$\epsilon = 10^{-10}$, $n = 10^4$

$$1/(1-16\sqrt{\epsilon}) \approx 1.0002$$

$$4h_2(2\sqrt{\epsilon})/n \approx 1.36 \times 10^{-7}$$

$$R \leq 2.887 \times 10^{-4}$$

$$\log_2 \frac{1+\eta}{1-\eta}$$

$$\approx 2.885 \times 10^{-4}$$

MT, Guha, Wilde, Nat. Commun. 5; 5235 (2014)

Few more slides…

Extension of the results to

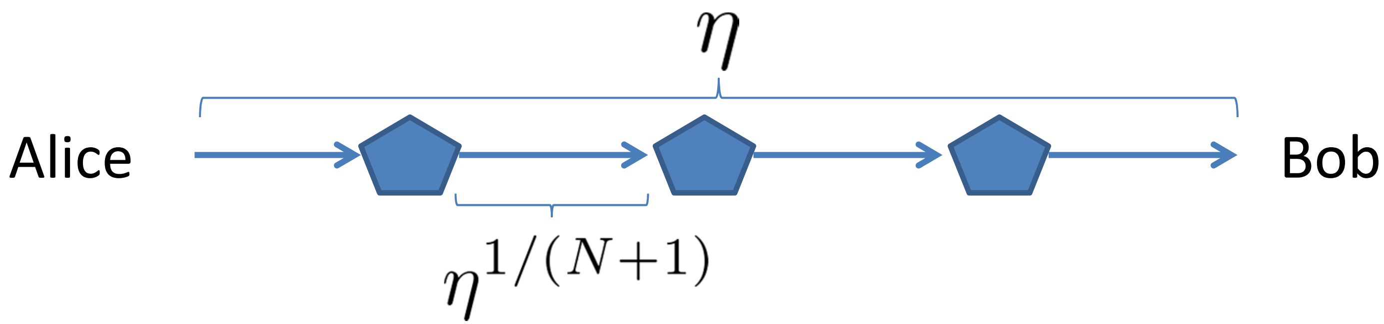
- Quantum repeaters
- Multipartite secret key sharing

Ads..

- QCrypt2015
- Summer internship at NICT

Upper bound on quantum repeaters

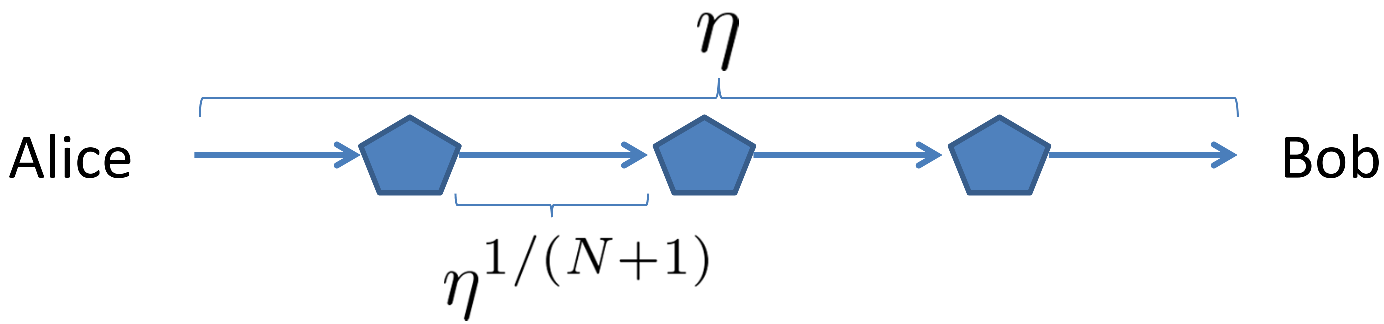
Quantum communication with *N* repeater stations:



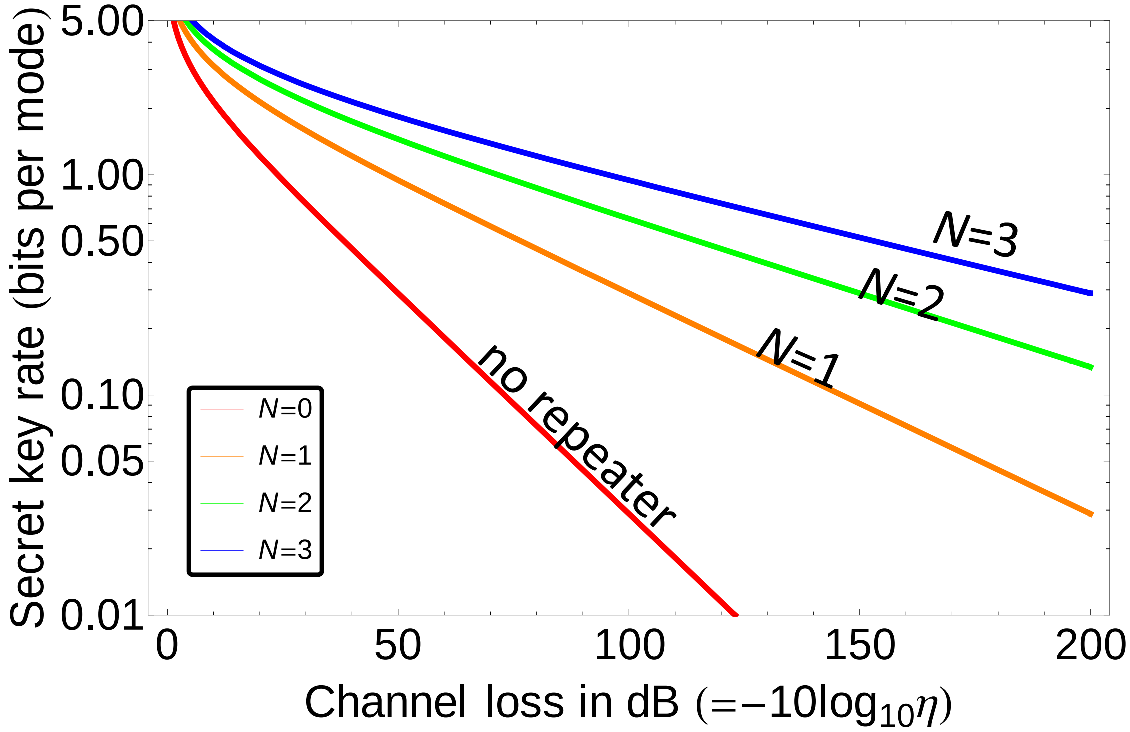
$$\boxed{R \leq \log_2 \frac{1+\eta}{1-\eta} \quad \Rightarrow \quad R \leq \log_2 \frac{1+\eta^{1/(N+1)}}{1-\eta^{1/(N+1)}}}$$

Upper bound on quantum repeaters

Quantum communication with *N* repeater stations:

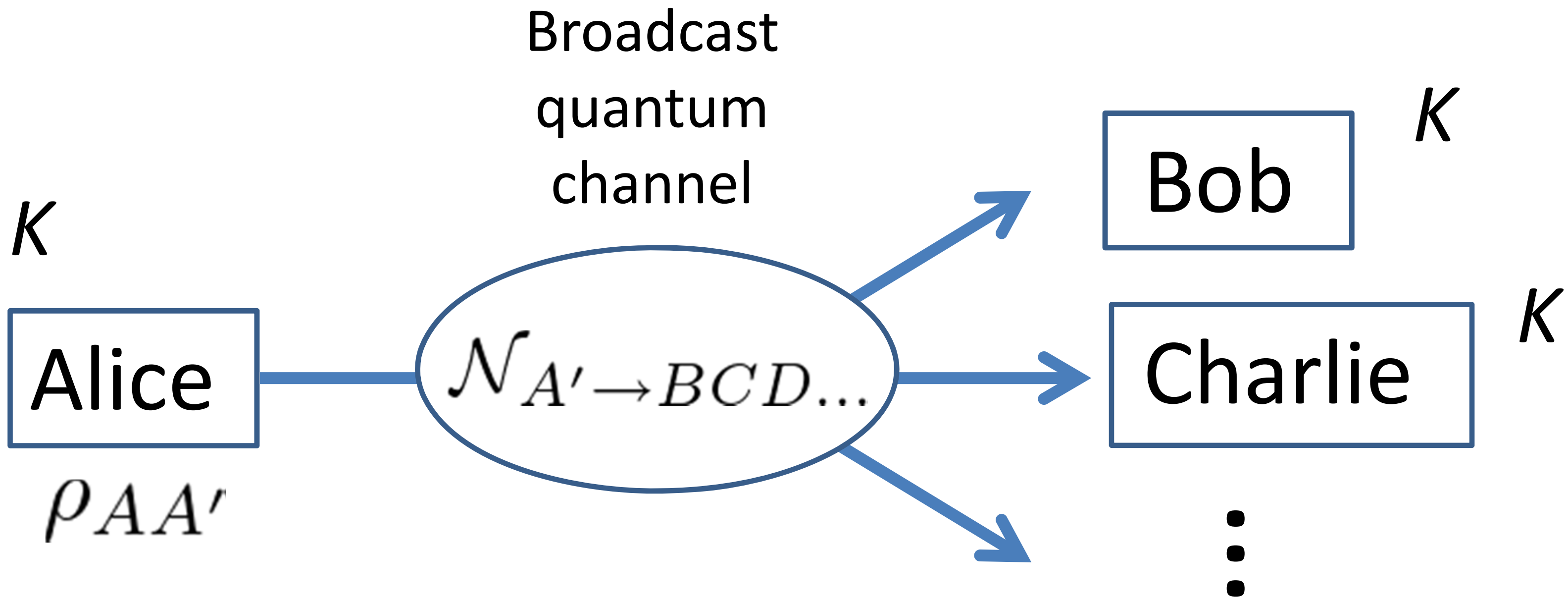


$$R \leq \log_2 \frac{1+\eta^{1/(N+1)}}{1-\eta^{1/(N+1)}}$$



Compare with the existing repeater protocols?

Multi-party key distribution



Key rate upper bound

$$\boxed{R \leq \frac{1}{m} E_{\rm sq}^{(m)}(\mathcal{N})}$$

$$E_{\rm sq}^{(m)}(\mathcal{N}) \equiv \max_{|\phi\rangle_{AA'}} E_{\rm sq}(A; B^{(1)}; B^{(2)}; \cdots; B^{(m)})_\rho,$$

Squashed entanglement of
a quantum broadcast channel

- Channel examples?
- How tight?

Few more slides…

Extension of the results to

- Quantum repeaters
- Multipartite secret key sharing

Ads..

- QCrypt2015
- Summer internship at NICT

QCrypt2015 & UQCC2015

Tokyo, Japan September 28 - October 2, 2015

QCrypt2015 (4.5days)

Discuss the latest theory
and experiments on quantum
cryptography and related fields

http://2015.qcrypt.net/

UQCC2015 (0.5days, Sep 28)

Invites engineers, potential users, media etc, to show the SOTA QKD performance & applications and discuss the possible business solutions

http://2015.uqcc.org/

Fig. 1 Network Layout of the Tokyo QKD Network

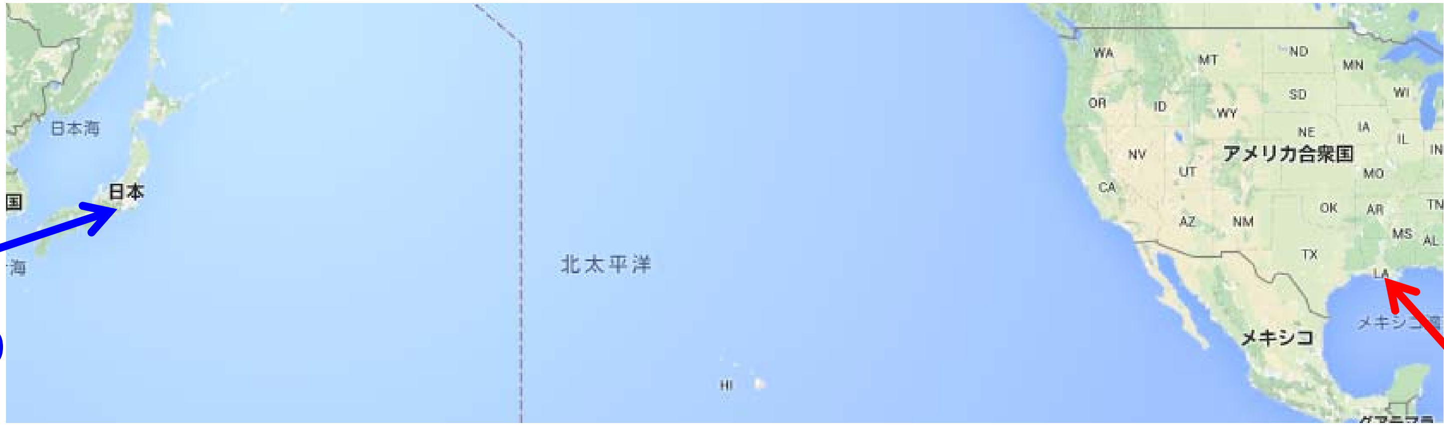

QKD platform

QCrypt2015 & UQCC2015

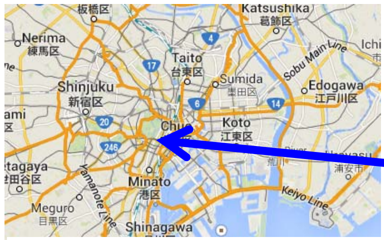
September 28 - October 2, 2015

Where? Tokyo, Japan

Tokyo



Baton Rouge



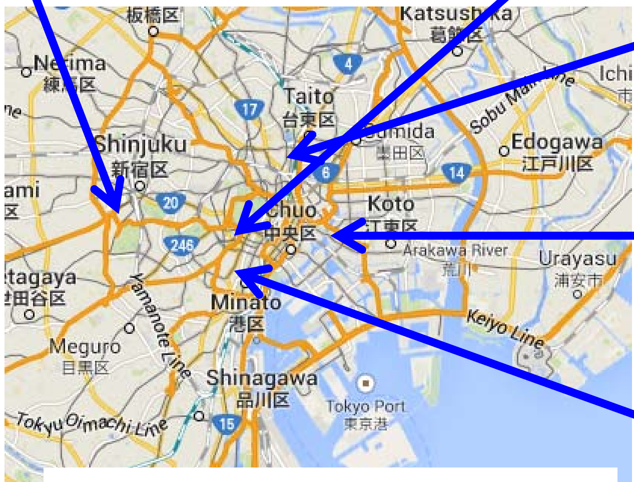
Central area of Tokyo

QCrypt2015 & UQCC2015

Imperial Palace

Shinjuku

Asakusa Temple



Central are of Tokyo

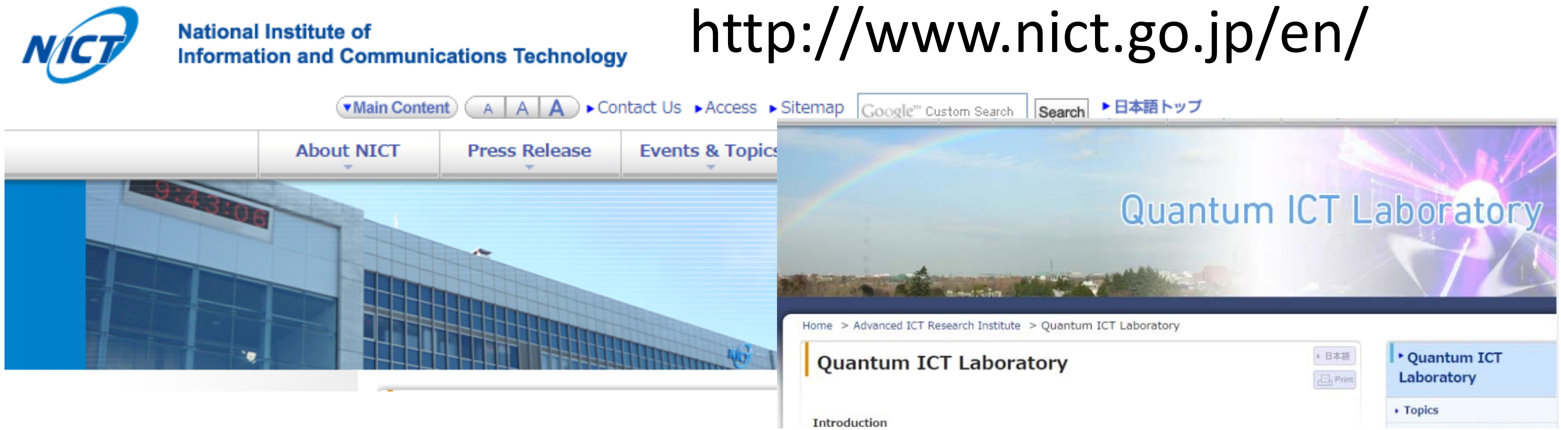
Akihabara

http://2015.qcrypt.net/

Oral presentation submission deadline: April 27

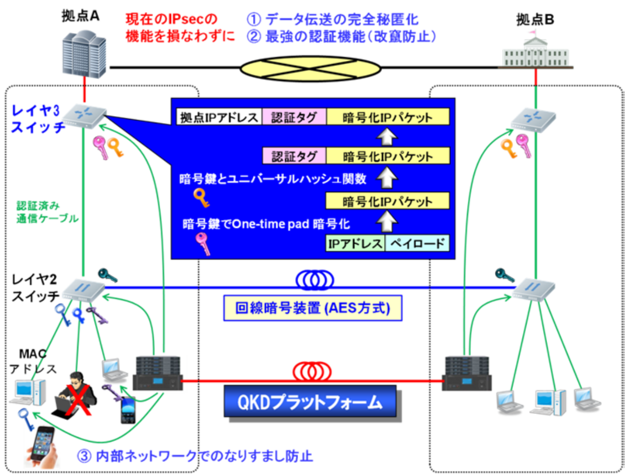
Summer internship at Quantum ICT Lab in NICT

http://www.nict.go.jp/en/

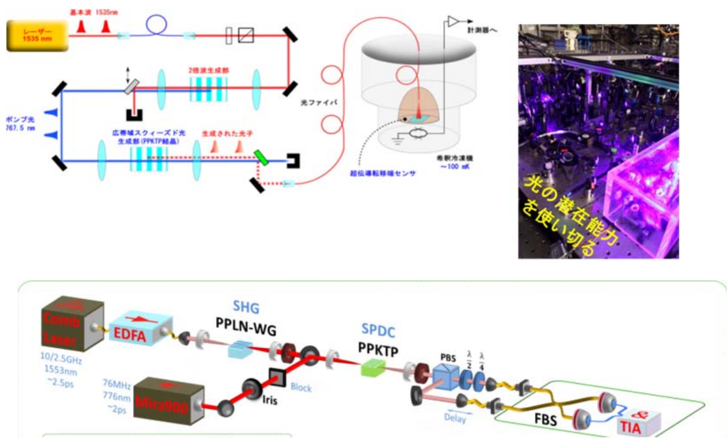


Leader
Masahide
Sasaki

QKD network, architecture, applications



Quantum optics: Entangled sources, PNRD, QIP protocols



Collaborative projects

-Optical space communication G
-Nano ICT G
-Frequency
 standard G

Theory: quantum information theory, quantum optics, physical layer security…