Enabling a Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Network

Speaker: Wenyuan Wang

University of Toronto

Email: wenyuan.wang@mail.utoronto.ca

Theory: arXiv: 1807.03466

Experiment: arXiv: 1808.08584

QCrypt 2018, Shanghai

August 29th , 2018

Papers

Theory: arXiv: 1807.03466

Wenyuan Wang,[1] Feihu Xu,[2,3] Hoi-Kwong Lo[1]

1 Centre for Quantum Information and Quantum Control, Dept. of ECE and Dept. of Physics, University of Toronto;

Experiment: arXiv: 1808.08584

Hui Liu,[2,3,*] Wenyuan Wang,[1,*] Kejin Wei,[2,3] Xiaotian Fang,[2,3]
Li Li,[2,3] Nai-Le Liu,[2,3] Weijun Zhang,[4] Hao Li,[4] Lixing You,[4] Zhen Wang[4]
Hoi-Kwong Lo,[1] Teng-Yun Chen,[2,3] Feihu Xu,[2,3] Jian-Wei Pan[2,3]

2 Shanghai Branch, Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China;

3 CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China;

4 State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences;

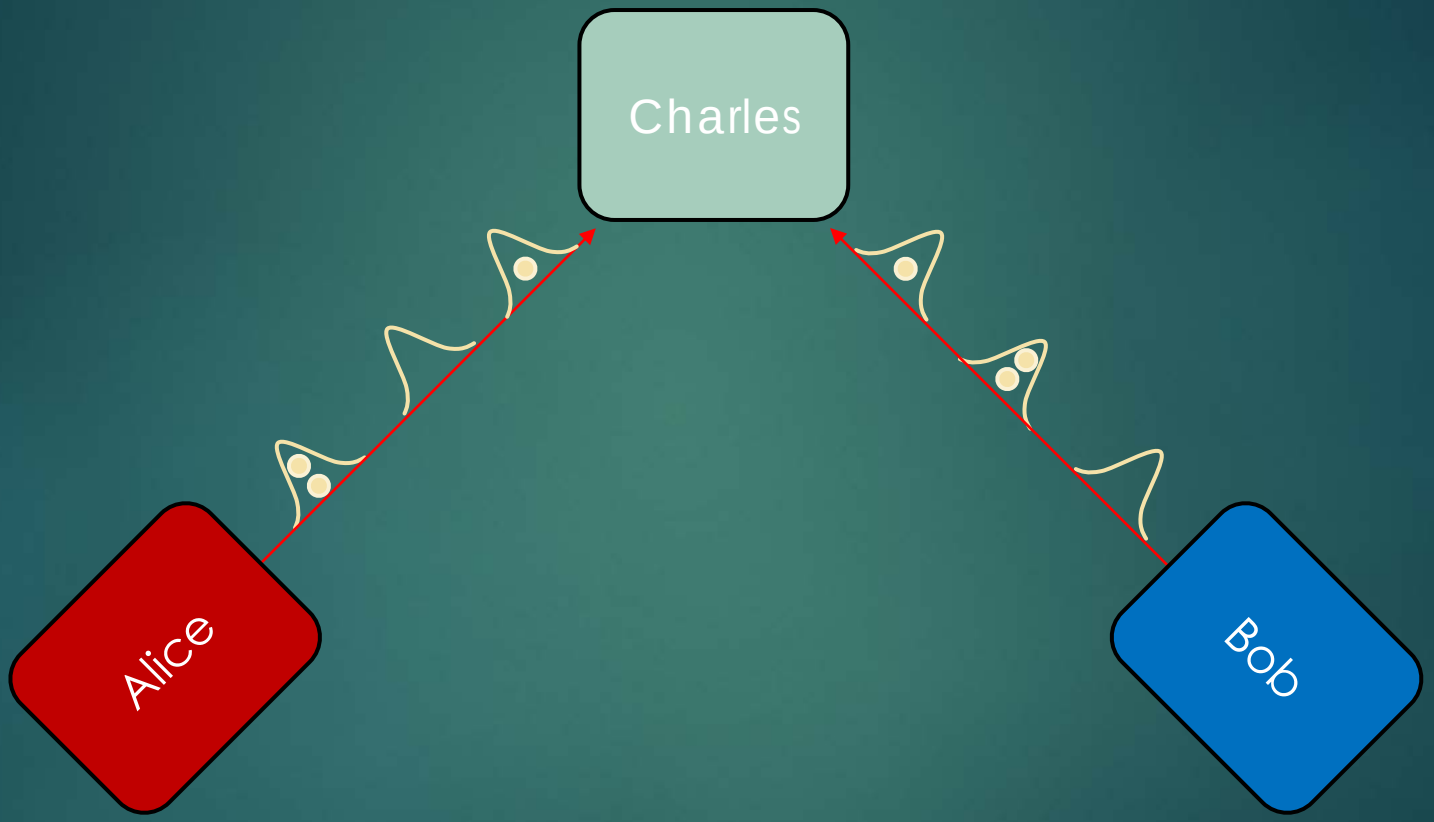
** These authors contributed equally to this work*

Outline

1. Background
    - Motivation: quantum network with untrusted relays
    - Previous MDI-QKD protocol and its limitation
2. Theoretical Results
    - New method: Using different Intensities to compensate channel asymmetry
    - Physical intuitions of the new method
    - Key challenge: parameter optimization
3. Simulation Results
4. Experimental Results

MDI-QKD

Detector Side Channels susceptible to attacks.



Measurement-Device-Independent QKD (MDI-QKD) [1] allows for untrusted measurement device.

[1] HK Lo, M Curty, and B Qi, "Measurement-device-independent quantum key distribution." Phys. Rev. Lett. 108.13, 130503 (2012)

MDI-QKD in Practice

- First demonstration of time-bin encoding MDIQKD (2013) [1,2]

- First demonstration of polarization-encoding MDIQKD (2014) [3,4]

- Current record of fibre-based MDI-QKD has been performed over 404km (2016) [5] and secret key rate up to 1 Mbits/s [6].

- Three-user demonstration of metropolitan MDI-QKD network (2016) [7]

[1] A Rubenok, JA Slater, P Chan, I Lucio-Martinez, and W Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks", Phys. Rev. Lett. 111.13, 130501 (2013)

[2] Y Liu, et al. "Experimental measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 111, p.130502 (2013)

[3] Z Tang, Z Liao, F Xu, B Qi, L Qian, HK Lo. "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution." Phys. Rev. Lett. 112.19, 190503 (2014)

[4] T Ferreira da Silva, D Vitoreti, GB Xavier, GC do Amaral, GP Temporão, and JP von der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," Phys. Rev. A, vol. 88, p. 052303 (2013)

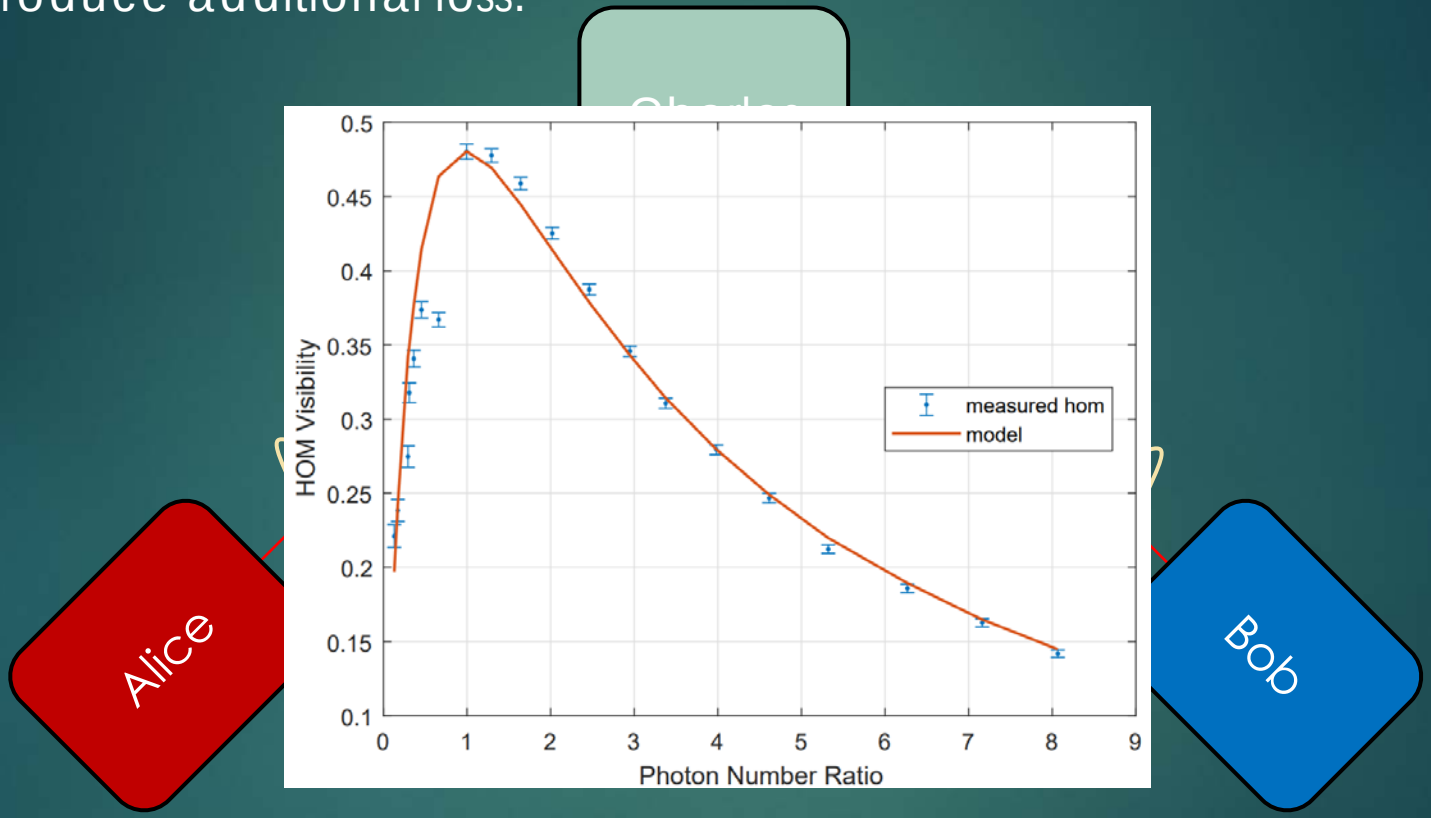
[5] Yin, Hua-Lei, et al. "Measurement-device-independent quantum key distribution over a 404 km optical fiber." Phys. Rev. Lett. 117.19, 190501 (2016):.

[6] LC Comandar, et al. "Quantum cryptography without detector vulnerabilities using optically-seeded lasers." Nat. Photon. 10, 312–315 (2016).

[7] YL Tang et al., Measurement-device-independent quantum key distribution over untrustful metropolitan network, Phys. Rev. X 6.1, 011024 (2016)

Limitation of MDI-QKD

All these experiments are either performed over near symmetric channels, or have to deliberately add a tailored length of fibre to introduce additional loss.



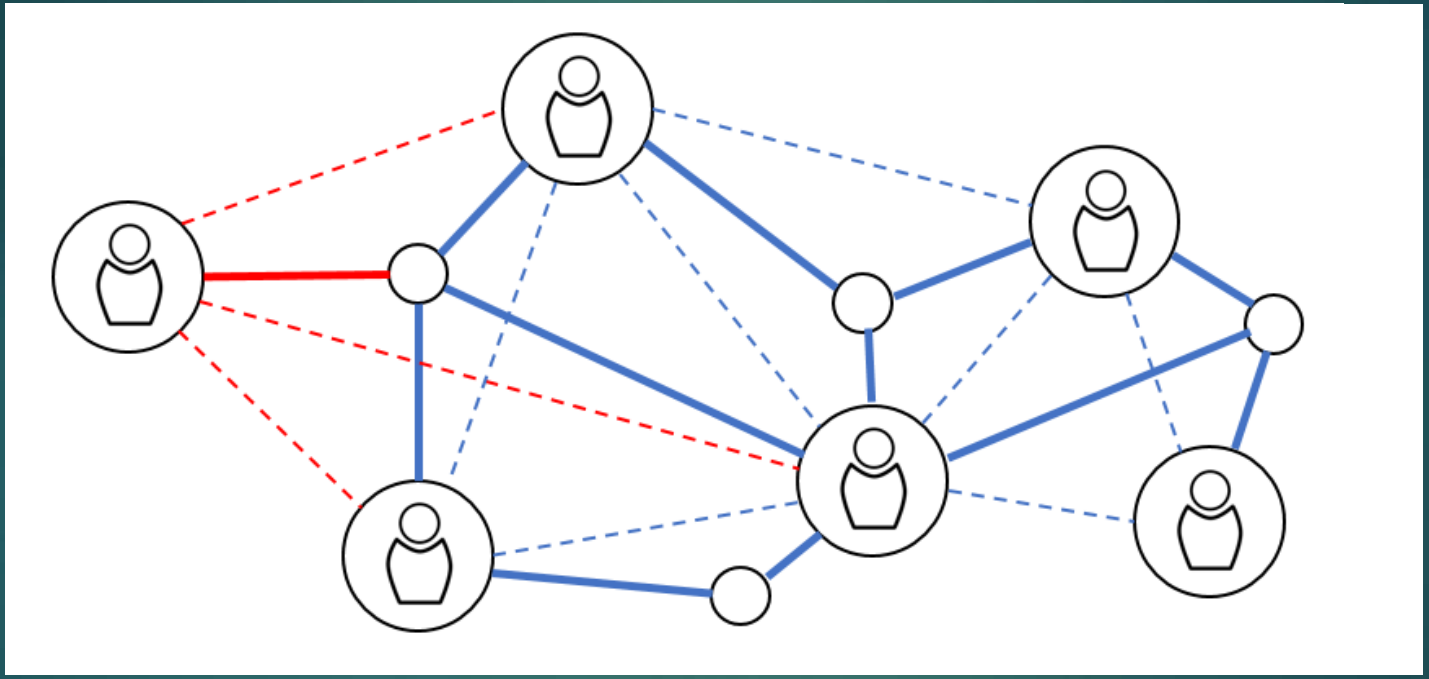
- In the X basis, MDI-QKD depends on two photon Hong-Ou-Mandel (HOM) interference, and thus depends on the symmetry of channel losses
- Asymmetry degrades the HOM visibility, thus causing larger X basis QBER and **lower** key rate

F Xu, M Curty, B Qi, HK Lo, New J. Phys. 15, 113007 (2013); E Moschandreou et al., arxiv:1804.02291 (2018)

MDI-QKD network

The future of MDI-QKD is to implement a MDI-QKD network.

Advantage: Enable the use of untrusted relays

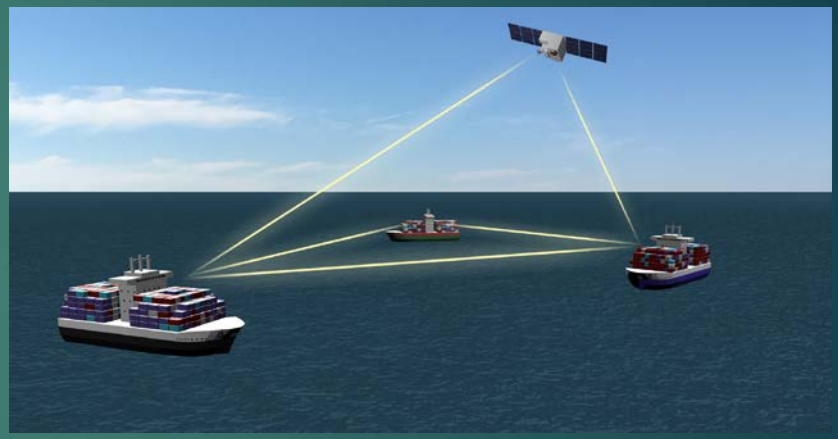


The network should be able to dynamically add/delete nodes.

Asymmetric channels in MDI-QKD network

In a real world network, it's very likely that one might encounter asymmetric channels.

Different Geographical locations

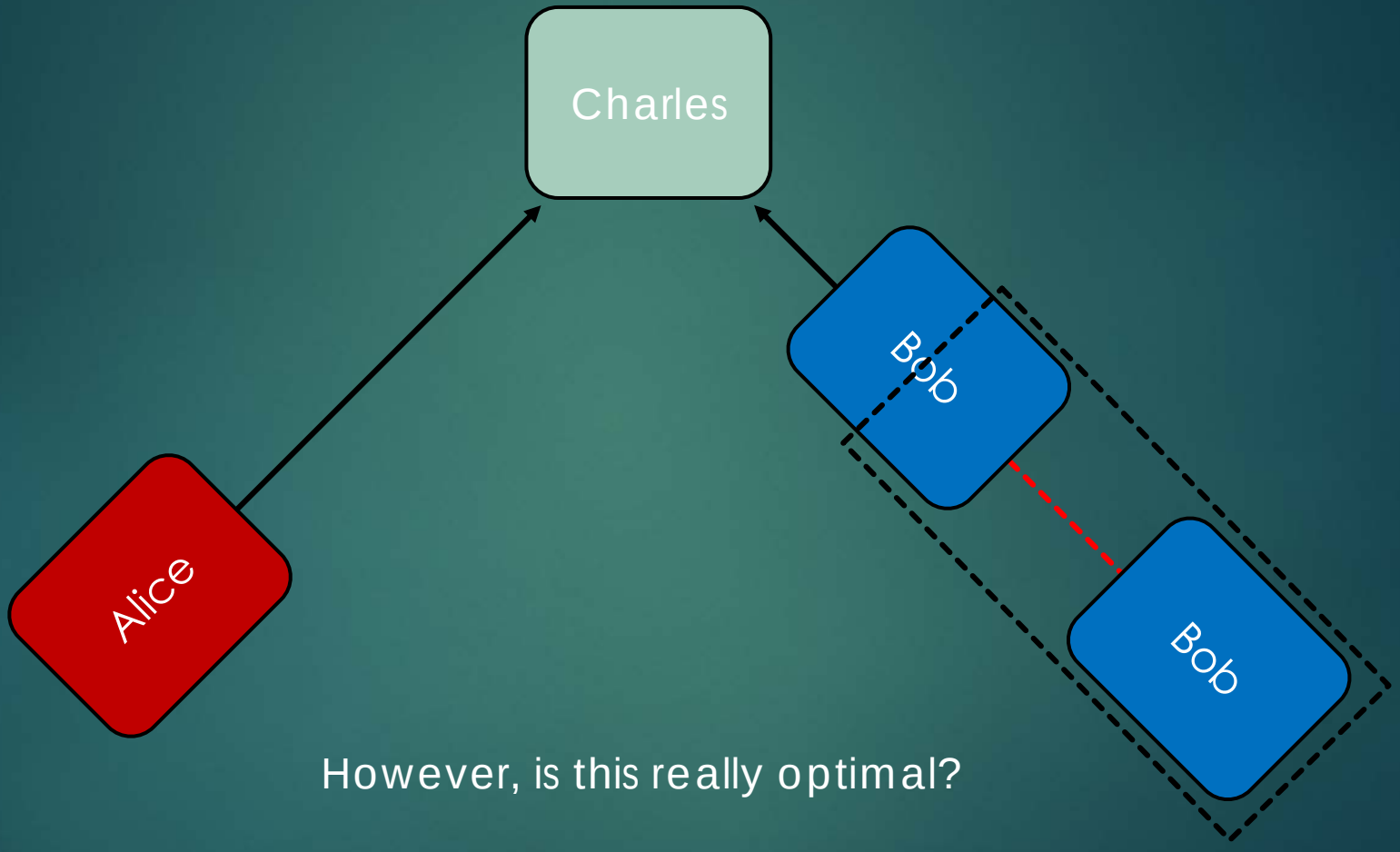


Moving platforms over free-space (e.g. ships, hot-balloons, satellite)

Left Fig. : A Rubenok, JA Slater, P Chan, I Lucio-Martinez, and W Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks", Phys. Rev. Lett. 111.13, 130501 (2013)

A makeshift solution: adding loss

Previously, in experiments with asymmetric channels, additional loss is deliberately added in exchange for better symmetry [1].



However, is this really optimal?

We will propose a new method to show that a dramatically higher key rate can be achieved by compensating the loss with intensities alone.

[1] A Rubenok, JA Slater, P Chan, I Lucio-Martinez, and W Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks", Phys. Rev. Lett. 111.13, 130501 (2013)

Theoretical Results

Decoupling X and Z basis

4-intensity Protocol [1]

s → Key Generation in Z basis

μ, ν, w → Estimate Gain and QBER in X basis only

Observables Q_{ss}^{Z} E_{ss}^{Z} Q_{ij}^{X} E_{ij}^{X}

Decoy-states

Using the entire Z basis for key generation:
more robust against finite-size effects

Single-Photon Contributions Y_{11}^{Z} ⇠ Y_{11}^{X} e_{11}^{X}

Rate $R = (P_s)^2 \times \{(se^{-s})^2 Y_{11}^{X}[1 - h_2(e_{11}^{X})] - Q_{ss}^{Z} f_e [1 - h_2(E_{ss}^{Z})]\}$

Privacy Amplification *Error Correction*

However, the 4-intensity protocol limits its discussions to symmetric case only (i.e. same intensities for Alice and Bob).

[1] YH Zhou, ZW Yu, and XB Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Phys. Rev. A 93.4, 042324 (2016)

Difference between previous method and ours

Previous method

$\{s, \mu, \nu, \omega\}$

	Alice	Bob
Z	s	s
X	μ	μ
X	ν	ν
X	ω	ω

Our method

$\{s_A, \mu_A, \nu_A, \omega, s_B, \mu_B, \nu_B, \omega\}$

	Alice	Bob
Z	s_A	s_B
X	μ_A	μ_B
X	ν_A	ν_B
X	ω	ω

Optimizable parameters:

$[s, \mu, \nu, P_s, P_\mu, P_\nu]$

$[s_A, \mu_A, \nu_A, P_{s_A}, P_{\mu_A}, P_{\nu_A}]$

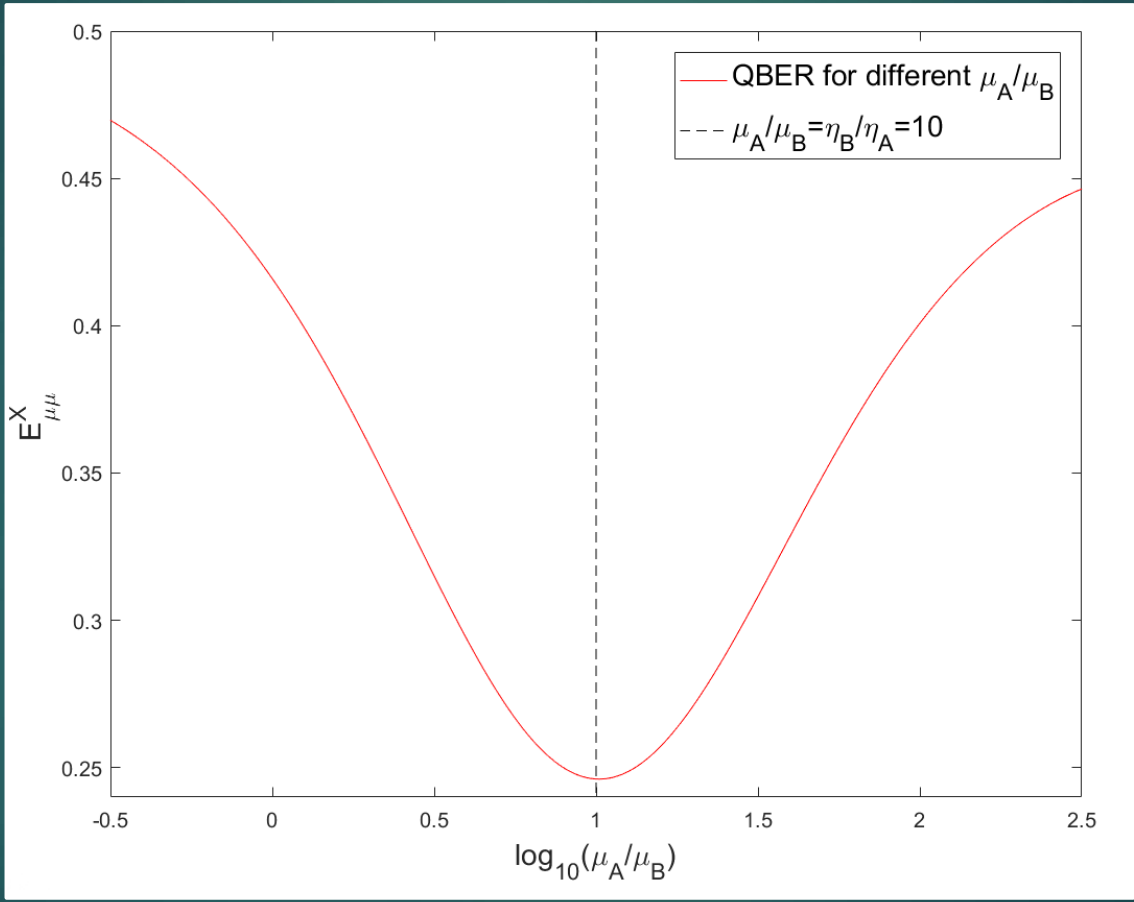
$[s_B, \mu_B, \nu_B, P_{s_B}, P_{\mu_B}, P_{\nu_B}]$

Physical intuition: QBER in X basis

Rate $R = (P_s)^2 \times \{s_A s_B e^{-(s_A+s_B)} Y_{11}^X [1 - h_2(e_{11}^X)] - Q_{ss}^Z f_e [1 - h_2(E_{ss}^Z)]\}$

Privacy Amplification *Error Correction*

X basis: Hong-Ou-Mandel Interference



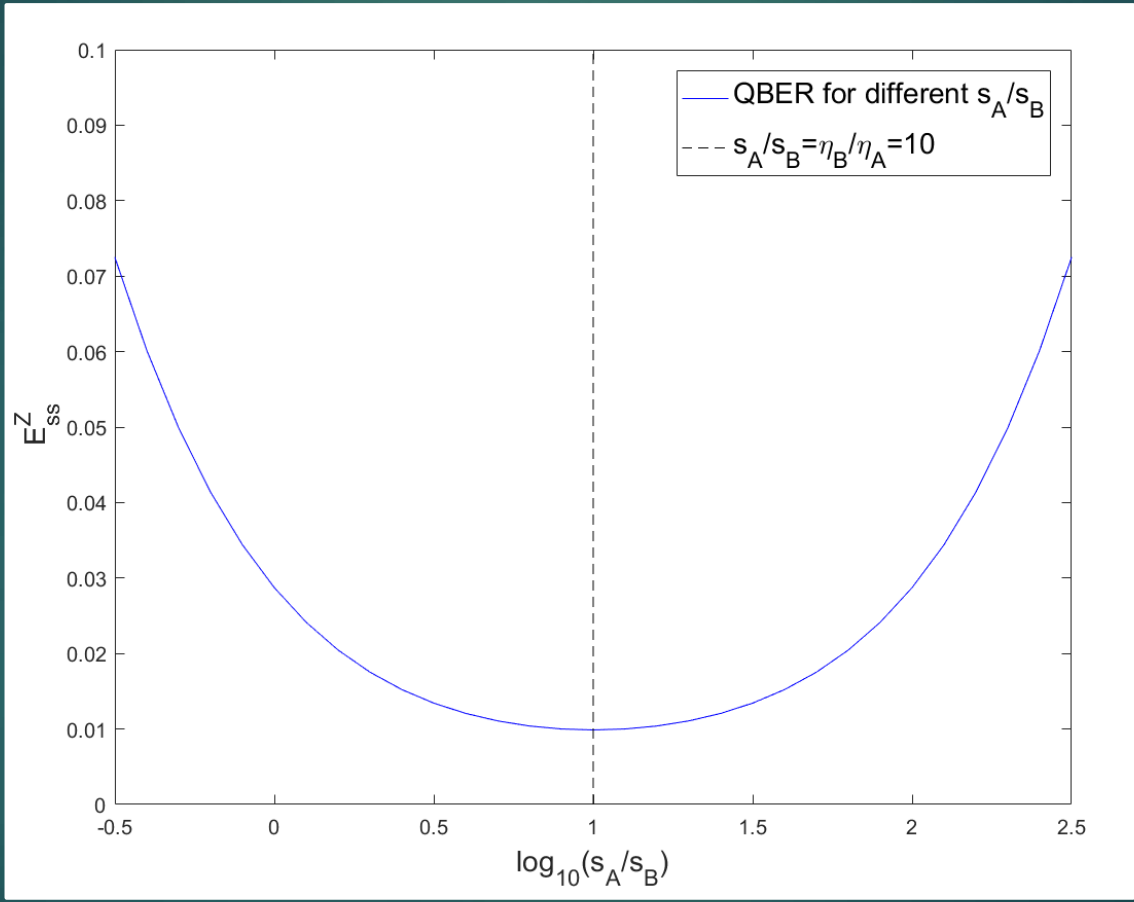
Requires highly symmetric arriving intensities at Charles, e.g. $\mu_A \eta_A = \mu_B \eta_B$

Physical intuition: QBER in Z basis

Rate $$R = (P_s)^2 \times \{s_A s_B e^{-(s_A+s_B)} Y_{11}^X [1 - h_2(e_{11}^X)] - Q_{ss}^Z f_e [1 - h_2(E_{ss}^Z)]\}$$

Privacy Amplification *Error Correction*

Z basis: **Not related** to HOM dip (QBER caused by imperfections, e.g. misalignment)



Much less sensitive to arriving intensities, needs a trade-off between $s_A s_B e^{-(s_A+s_B)}$ and error correction, generally $s_A \eta_A \neq s_B \eta_B$

Physical Intuition of our method

Rate $R = (P_s)^2 \times \{s_A s_B e^{-(s_A+s_B)} Y_{11}^X [1 - h_2(e_{11}^X)] - Q_{ss}^Z f_e [1 - h_2(E_{ss}^Z)]\}$

Privacy Amplification *Error Correction*

X basis requires highly balanced intensities. → Asymmetry Between Alice and Bob

(Compensating channel losses)

Z basis is less sensitive to asymmetry. → Asymmetry between X and Z bases

But it needs a trade-off between $s_A s_B e^{-(s_A+s_B)}$ and error correction.

(**Decoupling X and Z bases** for optimization)

Decoupling X and Z bases allows different strategies for $(\mu_A, \mu_B, \nu_A, \nu_B)$ and (s_A, s_B) to compensate for channel loss!

Challenge: parameter optimization

We need to optimize 12 parameters.
- Highly time and resource consuming

$$[s_A, \mu_A, \nu_A, P_{s_A}, P_{\mu_A}, P_{\nu_A}]$$

$$[s_B, \mu_B, \nu_B, P_{s_B}, P_{\mu_B}, P_{\nu_B}]$$

A powerful workstation PC can search 10^5 points/s.

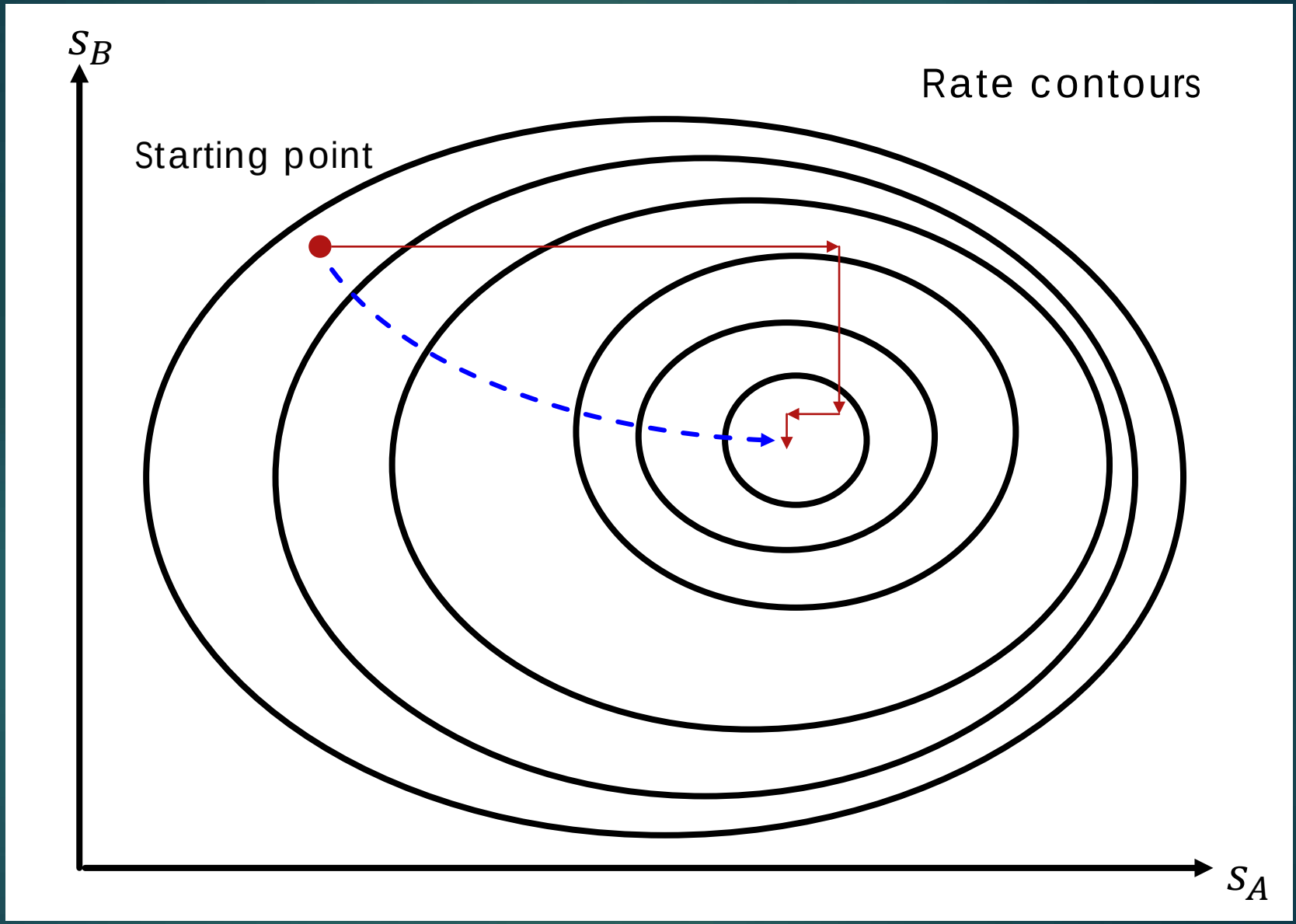
- A very coarse 10-point resolution takes approximately 4 months.

- A moderate 100-point resolution: search 10^{12} points approximately 3×10^{11} years! (Age of universe: 1.3×10^{10} years)

On the other hand, we can use a local search algorithm, named Coordinate Descent as proposed in Ref [1] (Xu, Xu, Lo, 2014).

[1] Xu, Feihu, He Xu, and Hoi-Kwong Lo. "Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution." Physical Review A 89.5 (2014): 052333.

Coordinate descent

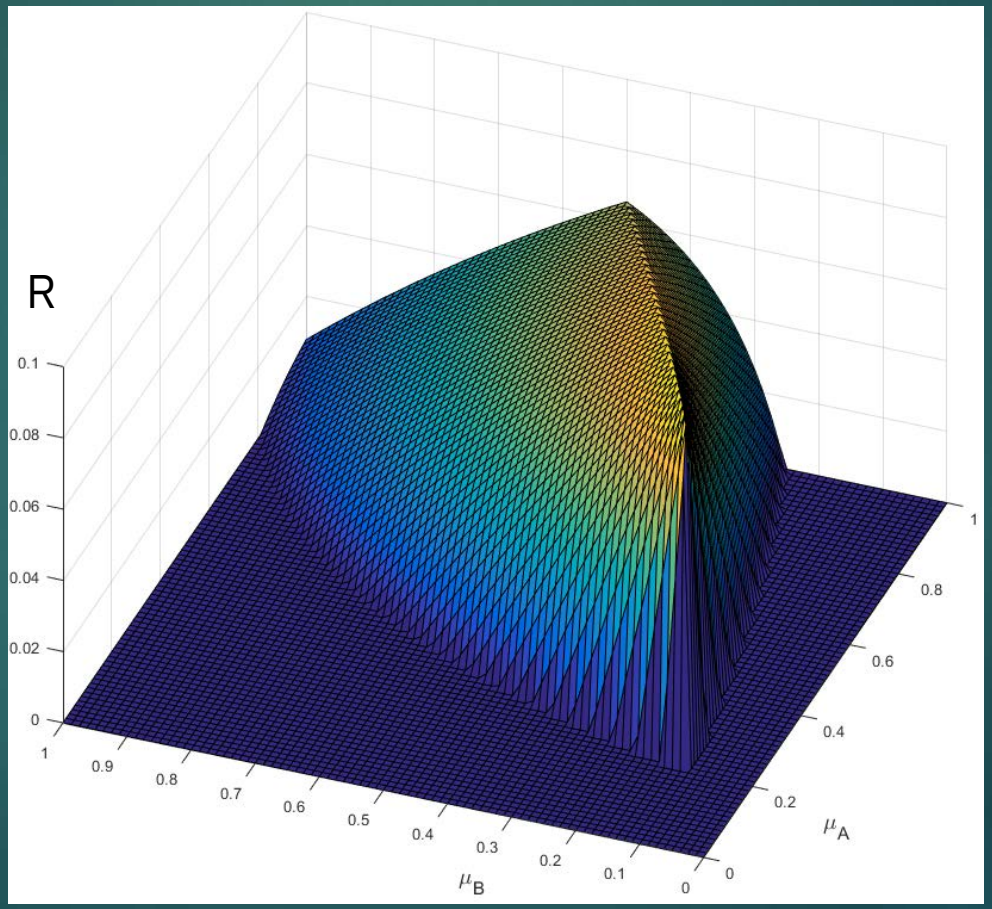


Search time is linearly, rather than exponentially, related to number of variables.

Problem: non-smooth functions

coordinate descent  non-smooth functions

Asymmetric MDI-QKD key rate versus μ_A, μ_B:



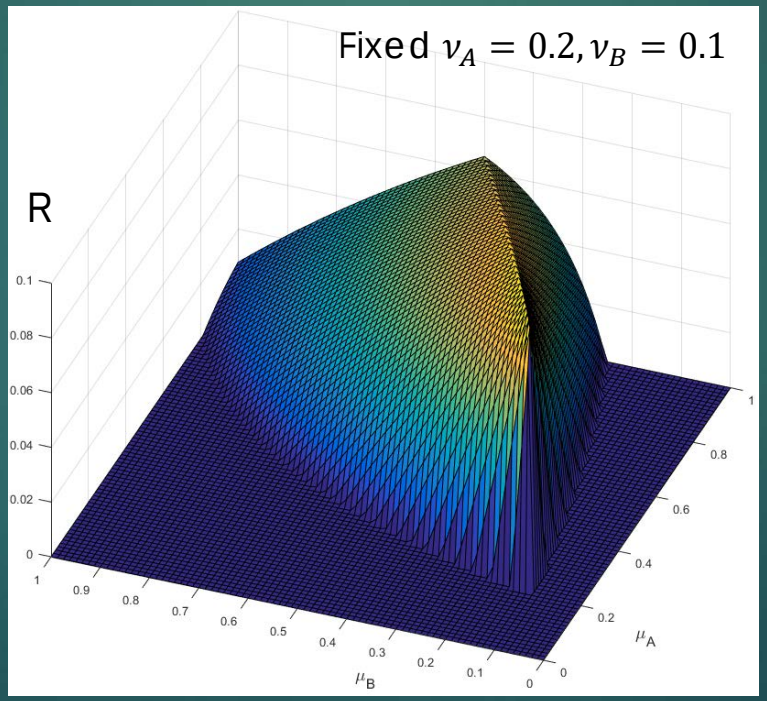
Two theorems for asymmetric MDI-QKD:

- Non-smoothness of key rate function vs decoy intensities $R(\mu_A, \mu_B, \nu_A, \nu_B)$

  There exists a sharp "ridge" at $\frac{\mu_A}{\mu_B} = \frac{\nu_A}{\nu_B}$.

- Proportionality of optimal Decoy Intensities $\frac{\mu_A^{opt}}{\mu_B^{opt}} = \frac{\nu_A^{opt}}{\nu_B^{opt}}$

  Optimal point is always found on the ridge.



Coordinate conversion

Cartesian

$$[(\mu_A, \mu_B), (\nu_A, \nu_B)]$$

Polar

$$[(r_\mu, \theta_\mu), (r_\nu, \theta_\nu)]$$

$$r_i = \sqrt{\mu_{iA}^2 + \mu_{iB}^2} \qquad \theta_i = \arctan\left(\frac{\mu_{iA}}{\mu_{iB}}\right) \qquad \mu_i = \{\mu, \nu\}$$

We know that $\theta_\mu = \theta_\nu$ (i.e. $\frac{\mu_A}{\mu_B} = \frac{\nu_A}{\nu_B}$),

thus we can set $\theta_\mu = \theta_\nu = \theta_{\mu\nu}$ and jointly search them.

Successful implementation of local search

$R(\theta_{\mu\nu})$ is now a smooth function, for which we can perform Coordinate Descent efficiently.

Optimizable parameters:

$$[r_s, \theta_s, r_\mu, r_\nu, \theta_{\mu\nu}]$$

$$[P_{s_A}, P_{\mu_A}, P_{\nu_A}, P_{s_B}, P_{\mu_B}, P_{\nu_B}]$$

On a quad-core i7 PC, it takes only 0.1 second to fully search any given position.

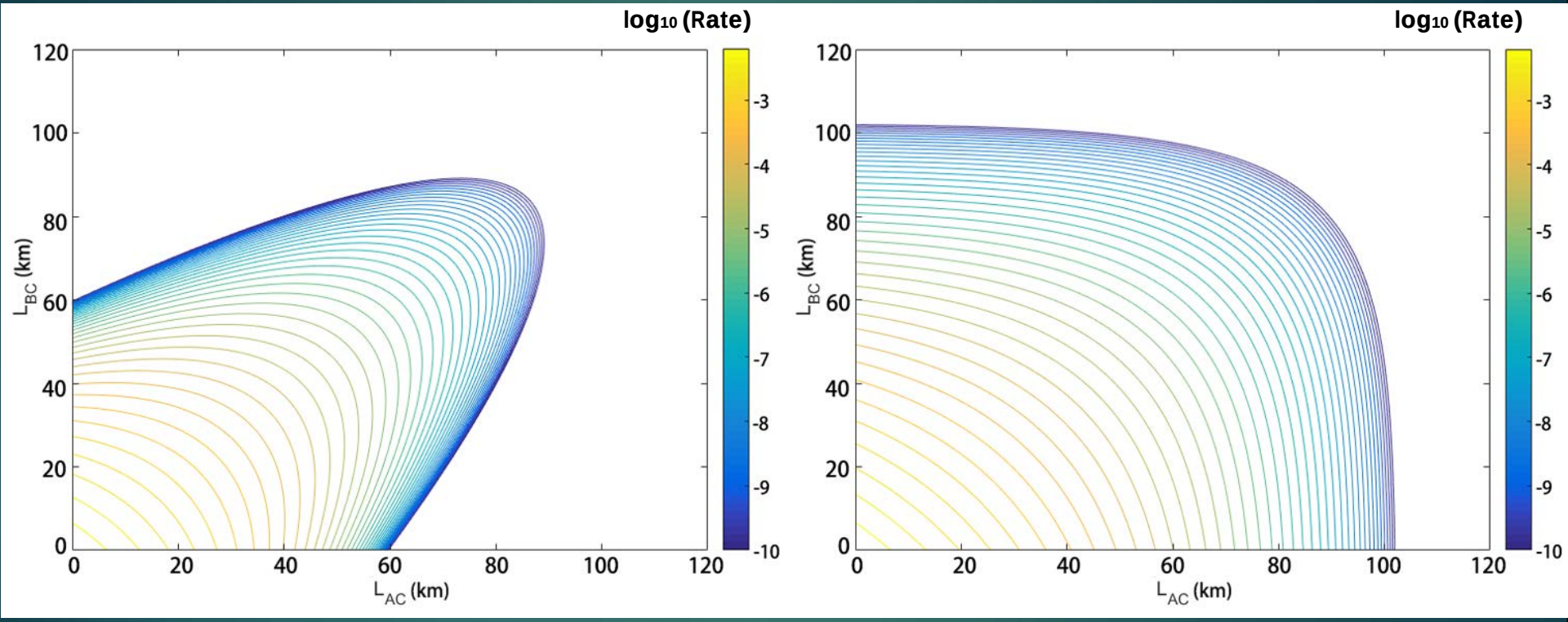
Over 100,000,000 times faster!

Simulation Results

Simulation results: applicable region

Previous results
(using symmetric intensities)

Our new results
(using fully optimized intensities)



$$\eta_d = 65\%, Y_0 = 8 \times 10^{-7}, e_d = 0.5\%, \epsilon = 10^{-7}, N = 10^{11}$$

Our method greatly extends the distance of MDI-QKD under asymmetric channel losses.

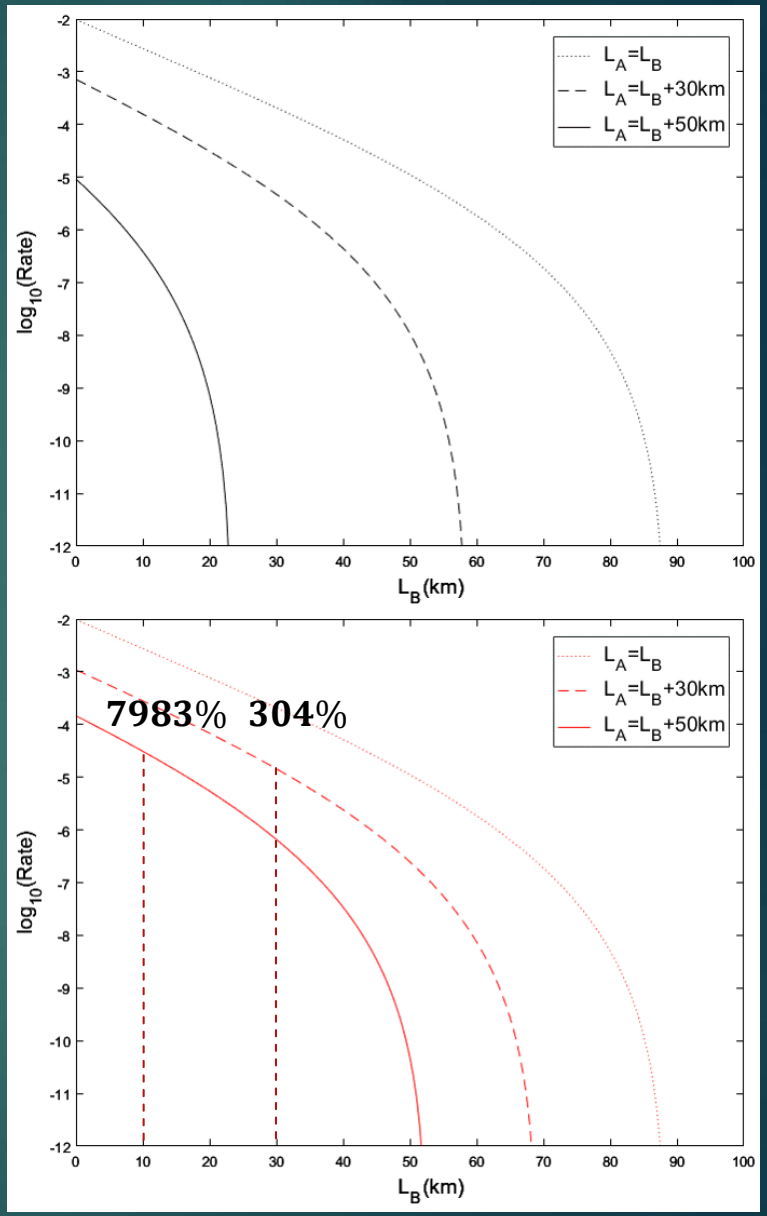
Simulation results: key rate

Previous results

(using symmetric intensities)

Our new results

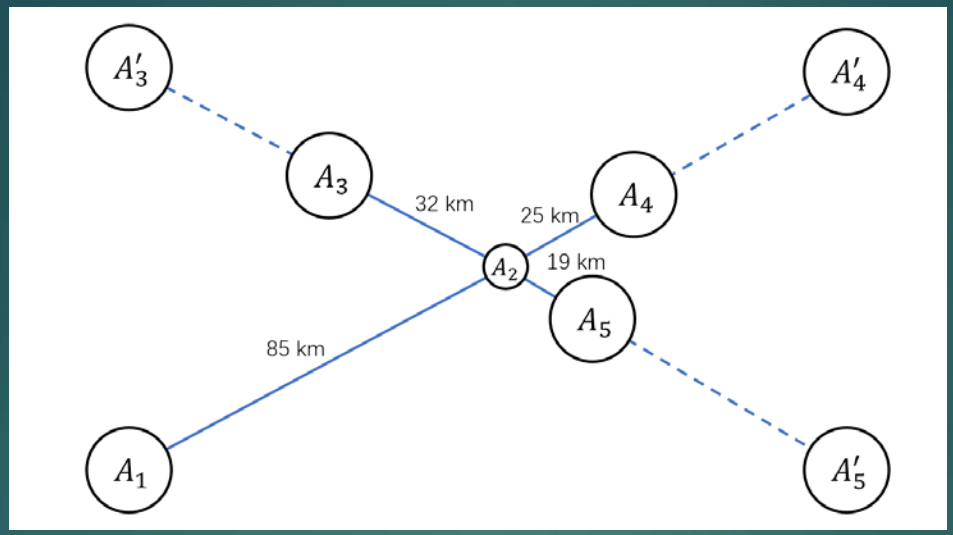
(using fully optimized intensities)



Our method greatly extends the distance and increases the key rate of MDI-QKD under asymmetric channel losses

Simulation results: realistic network

Realistic quantum network setting: Vienna QKD network [1]

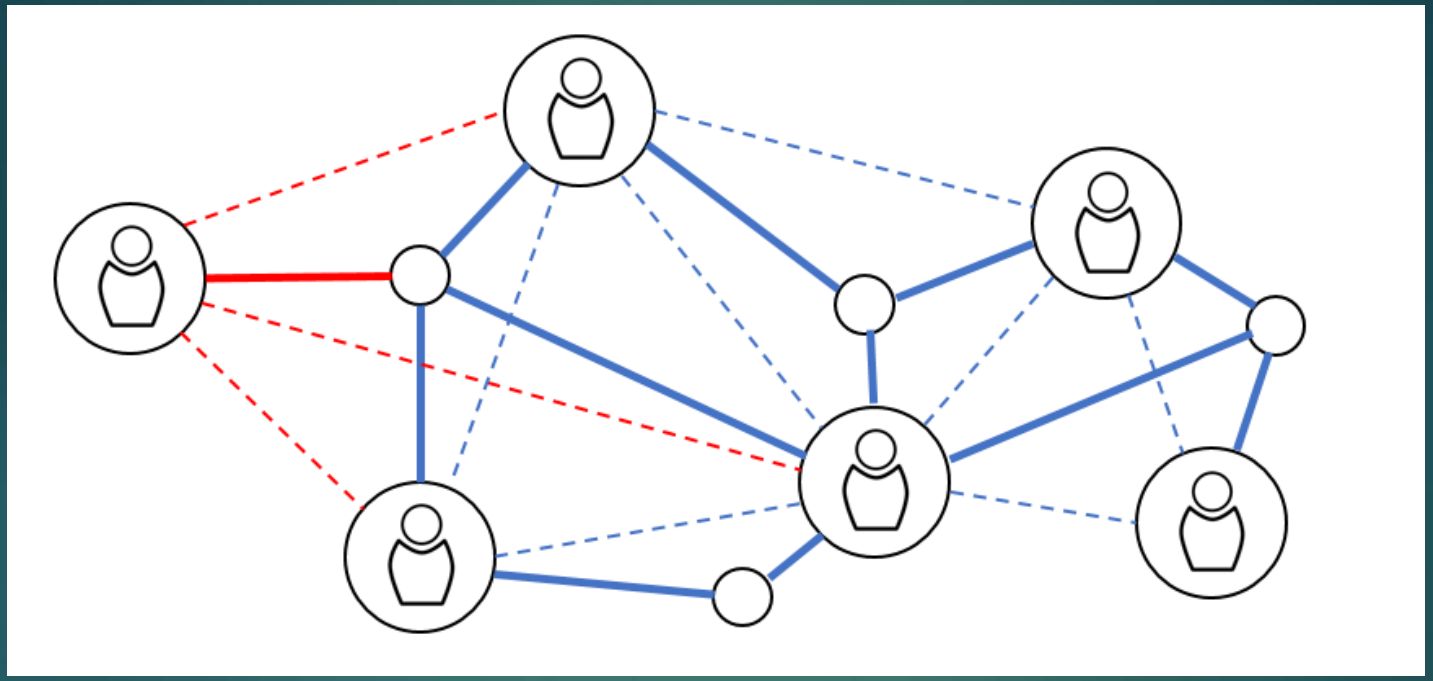


Method	$A_1 - A_3$
Previous method	0
Previous method, add fibre	10^{-10}
New method	10^{-7}

Scalability: adding new nodes does not affect existing nodes.

[1] M Peev et al., The SECOQC quantum key distribution network in Vienna, New Journal of Physics 11.7, 075001 (2009)

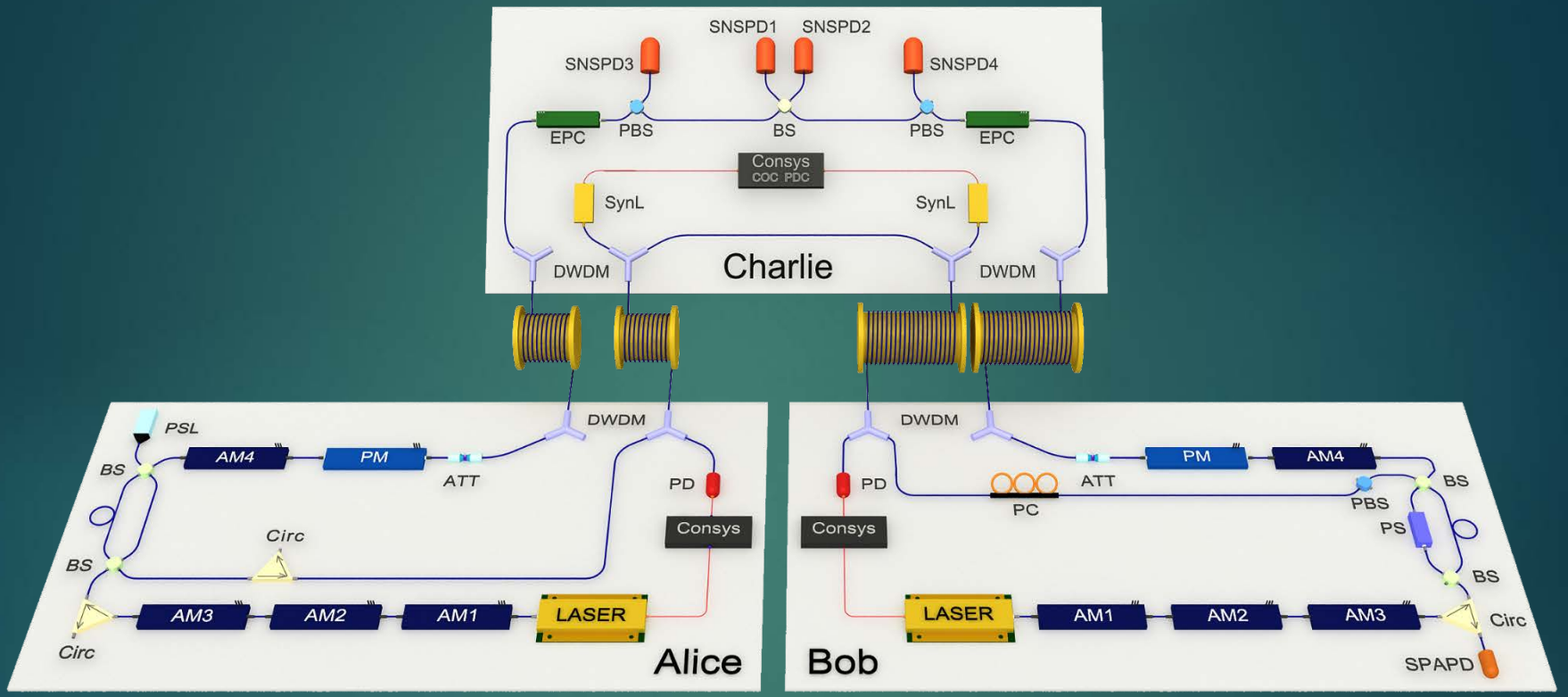
Requirement of a MDI-QKD network



The network should be able to dynamically add/delete nodes.

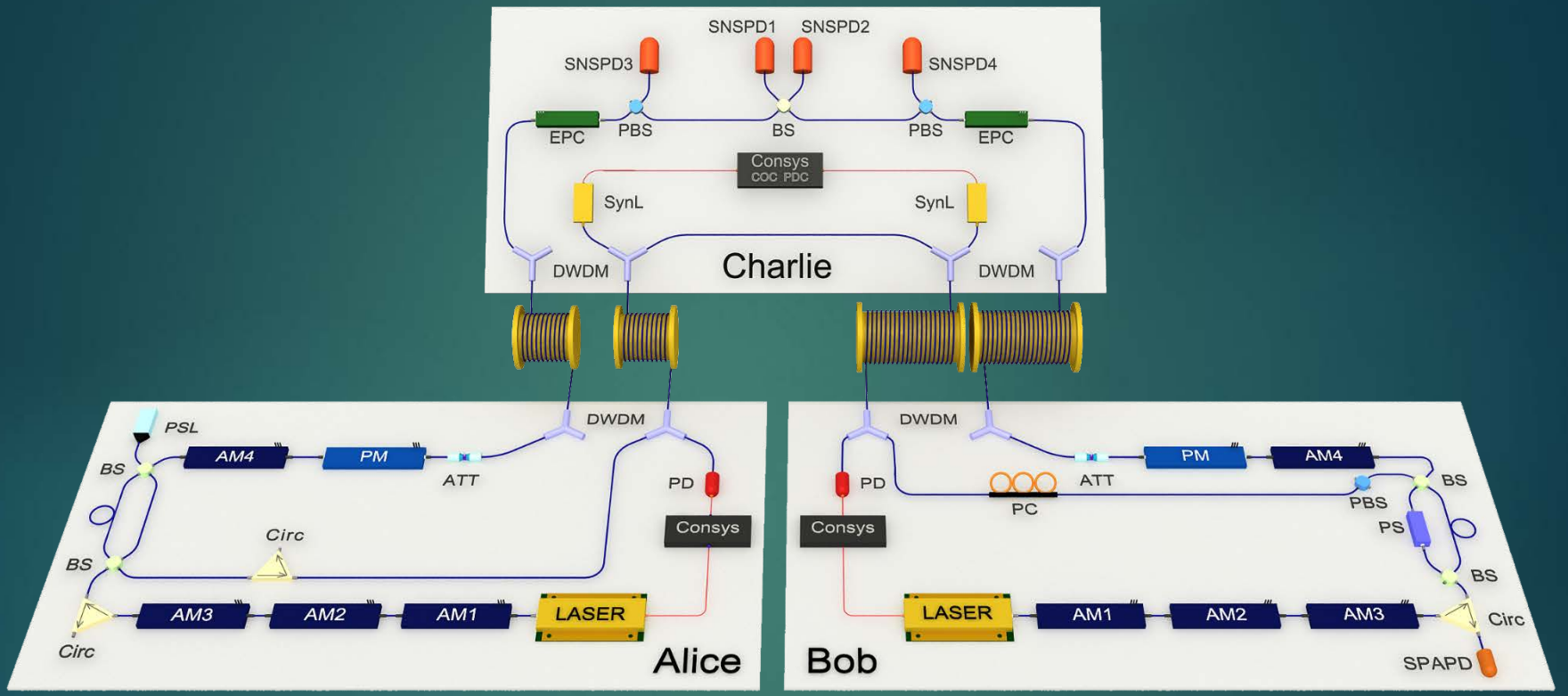
Experimental Results

Experimental system parameters



- Time-bin phase encoding
- HOM interference visibility ~ 46%
- AM extinction ratio > 23dB
- System clock rate = 75MHz
- Detector (SNSPD) efficiency ~70%
- Detector dark count rate: 6.4E-8/pulse

Automatic feedback system



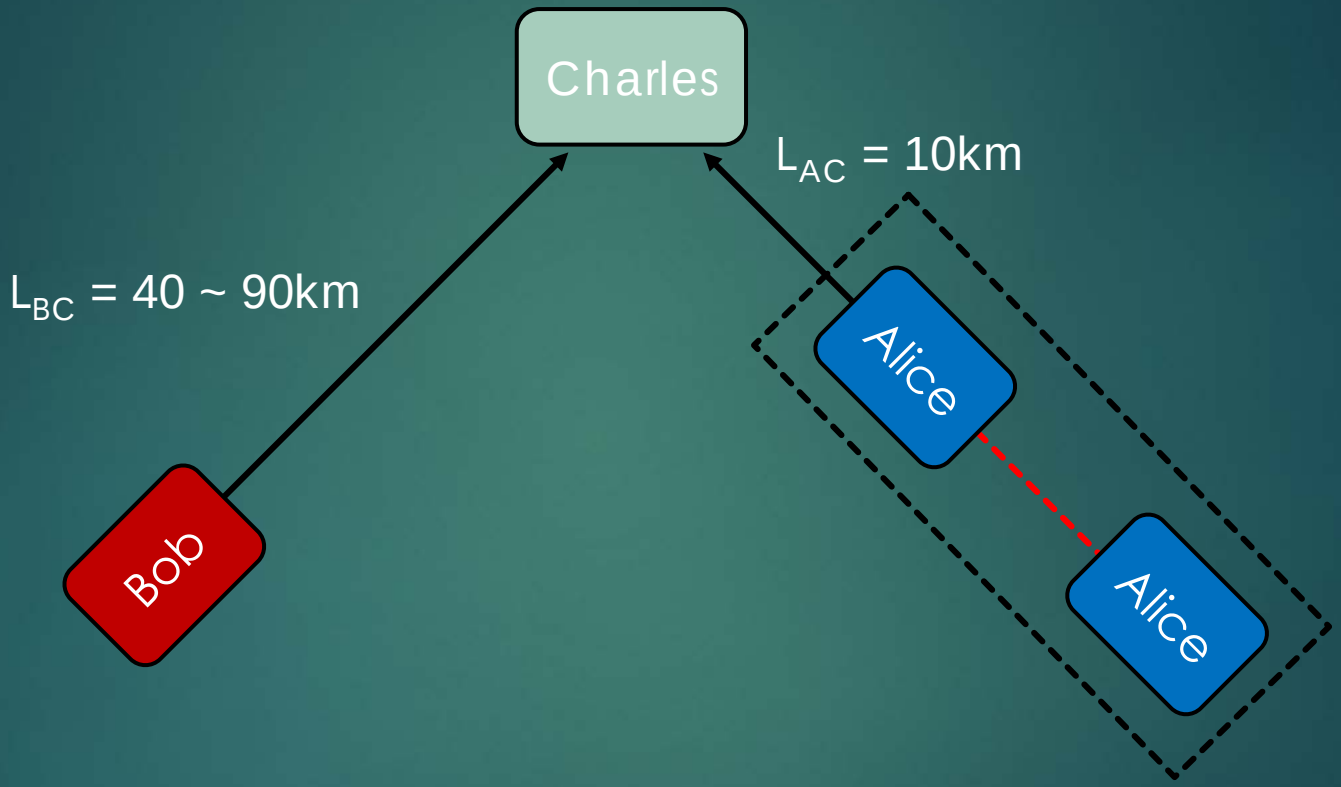
Automatic feedback system:

(1) guarantee the timing indistinguishability (2) eliminate spectrum detuning

(3) maintain the phase reference frames (4) recover the polarization alignment

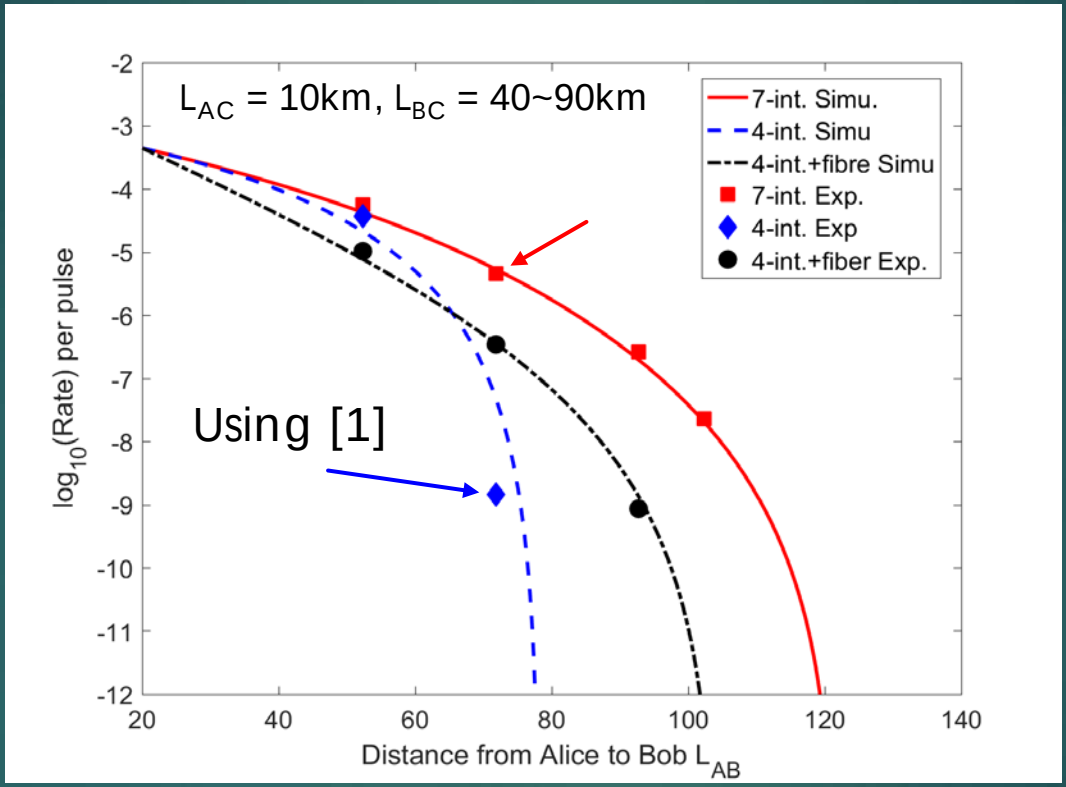
Long-term stability over tens of hours

Experimental setup 1



Experimental setup 1 results

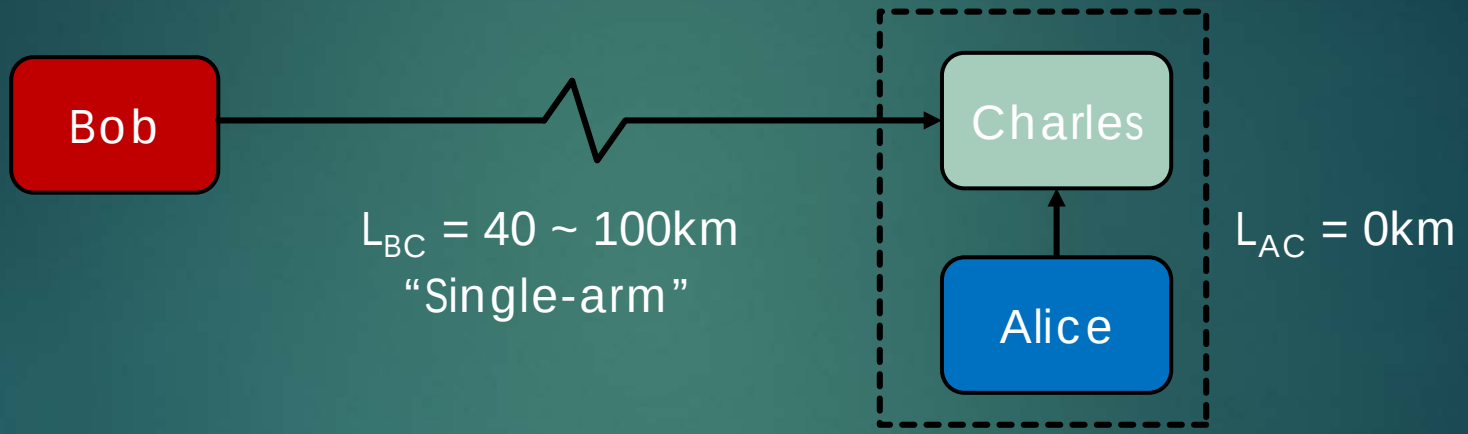
Rate vs total distance, simulation and experimental results



- At $L_B = 10km, L_A = 60km$, our rate is x3000 times higher than that using [1].
- With the new method, our distance is 40km longer than using [1].

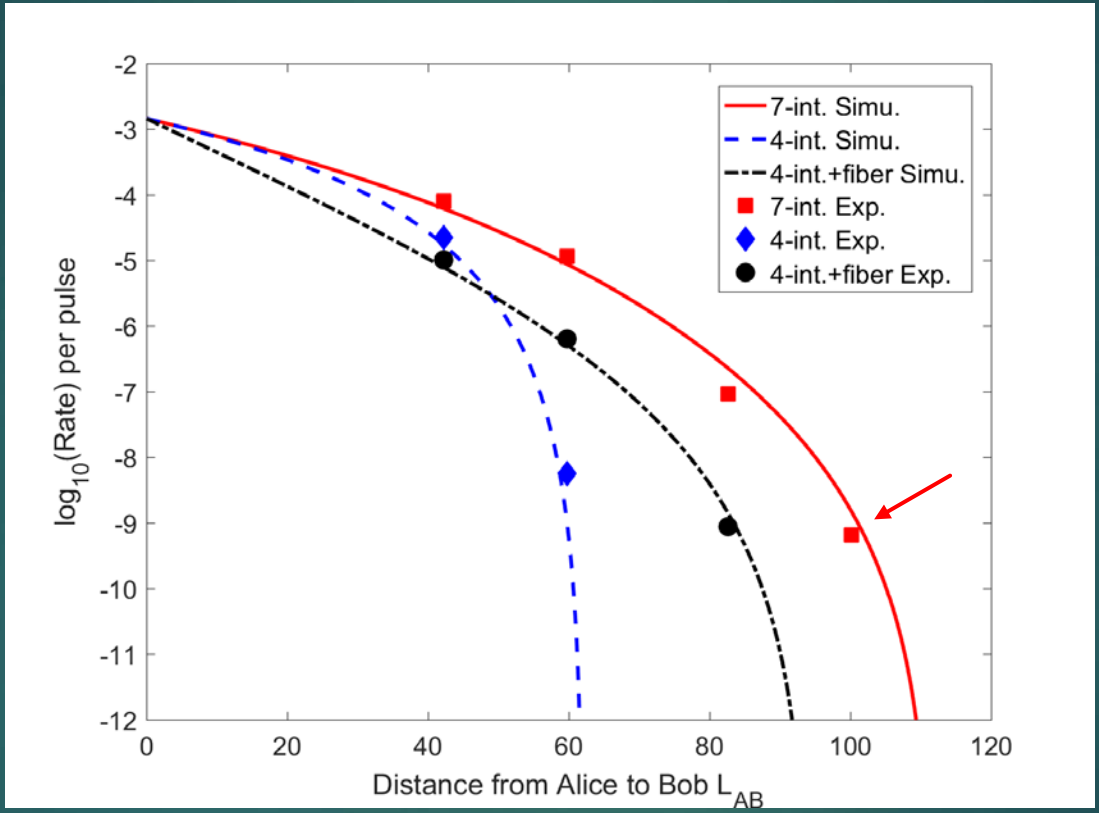
[1] YH Zhou, ZW Yu, and XB Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Phys. Rev. A 93.4, 042324 (2016)

Experimental setup 2



Experimental setup 2 results

Rate vs total distance, simulation and experimental results



- Our new method maintains $R = 7 \times 10^{-10}$ even when L_{BC} reaches 100km and $L_{AC} = 0km$.

Conclusion

1. Maintain good performance for arbitrary levels of asymmetry between channels

2. No need to add any loss, optimal key rate is achieved by only optimizing intensities

3. Extremely fast optimization in 0.1 second

4. Reconfigurability: dynamically adding/deleting nodes

Enable a high-rate scalable MDI-QKD network with arbitrarily placed nodes

Acknowledgment

This work was supported by
- the Natural Sciences and Engineering Research Council of Canada (NSERC)
- U.S. Office of Naval Research (ONR)
- the Fundamental Research Funds for the Central Universities of China
- National Natural Science Foundation of China Grants No. 61771443
- China 1000 Young Talents Program

Theory: arXiv: 1807.03466

Experiment: arXiv: 1808.08584

Contact: wenyuan.wang@mail.utoronto.ca

Thank you very much!

Questions?