Recent Advancement in Measurement-Device-Independent Quantum Key Distribution

Xiongfeng Ma
xma@tsinghua.edu.cn
Center for Quantum Information, IIIS, Tsinghua

清華大學 交叉信息研究院
Tsinghua University Institute for Interdisciplinary Information Sciences

Outline

- Introduction
  - QKD protocols
  - Qubit encoding and decoding with optics
- Measurement-device-independent schemes
  - Detection problems
  - Twin-field
- Mode-pairing encoding
  - Experimental realization
- Conclusion and outlook

Introduction

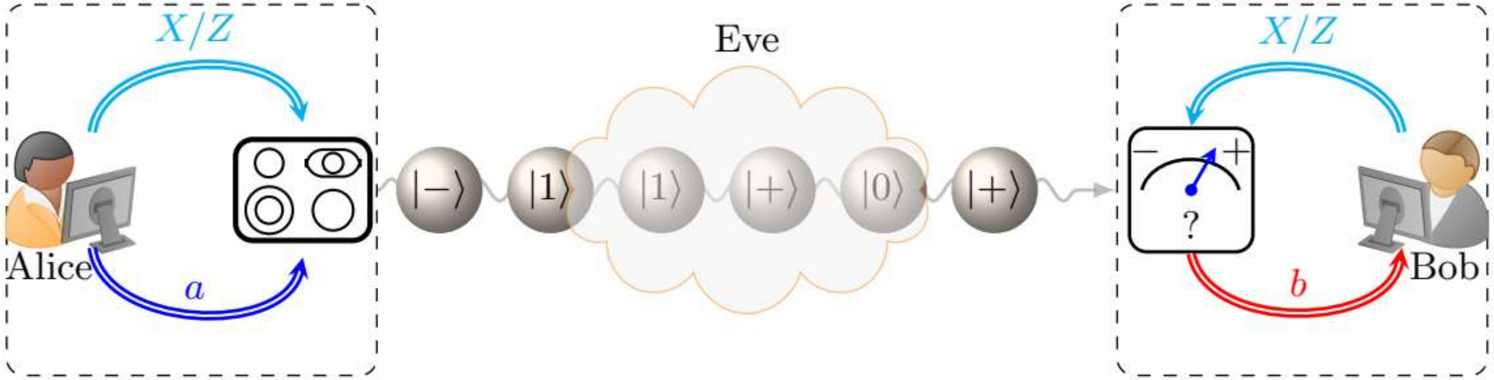
Prepare-and-measure: BB84, B92, six-state, …

(1) *State Preparation:* Alice prepares qubits randomly in states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, forming the Z and X bases.

(2) *Transmission and Measurement:* Alice transmits qubits to Bob who randomly measures each in the Z or X basis.

(3) *Sifting:* Alice and Bob announce their basis choices publicly and keep the bits where they use the same bases, yielding a sifted key.

(4) *Key Distillation:* Alice and Bob perform classical postprocessing, including information reconciliation and privacy amplification, to generate a secret key.



Entanglement-distribution-based: Ekert91, BBM92, …

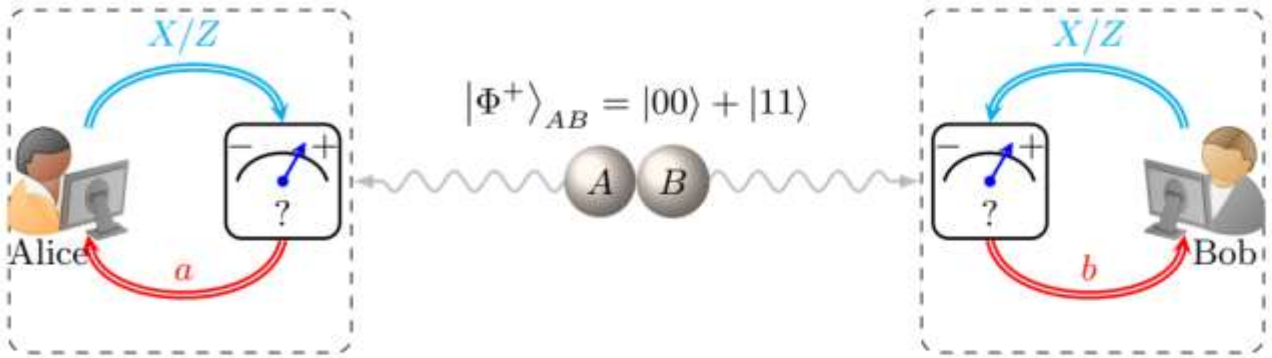
(1) *State Preparation:* An entanglement source generates EPR pairs $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

(2) *Transmission:* Alice and Bob each receive and store one qubit of an EPR pair. Any pair lost or failing storage is discarded.

(3) *Parameter Estimation:* By measuring a random sample of EPR pairs in the Z and X bases, Alice and Bob estimate the quantum bit and phase error rates, e_b and e_p, respectively.

(4) *Quantum Error Correction:* They correct quantum errors in the remaining stored qubit pairs, resulting in nearly perfect EPR pairs.

(5) *Key Measurement:* They measure the EPR pairs in the local Z basis and generate the final key.



Entanglement-measurement-based

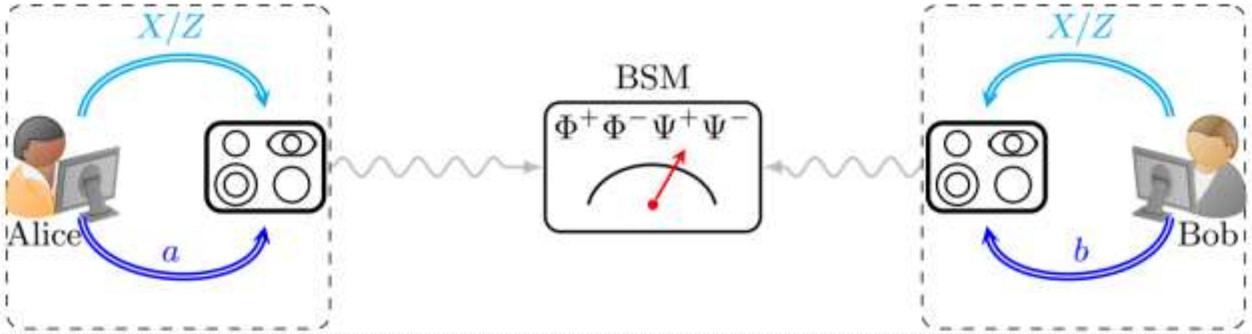
(1) *State Preparation:* Alice and Bob each prepare qubits randomly in states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, and sends to the measurement site.

(2) *Bell-State Measurement:* At the measurement site, the two qubits will be projected into one of the four Bell states.

(3) *Key Mapping:* Bob flips the bit value in the Z basis if the measurement outcome is $|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$ or $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. Bob flips the bit value in the X basis if the measurement outcome is $|\Phi^+\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ or $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$.

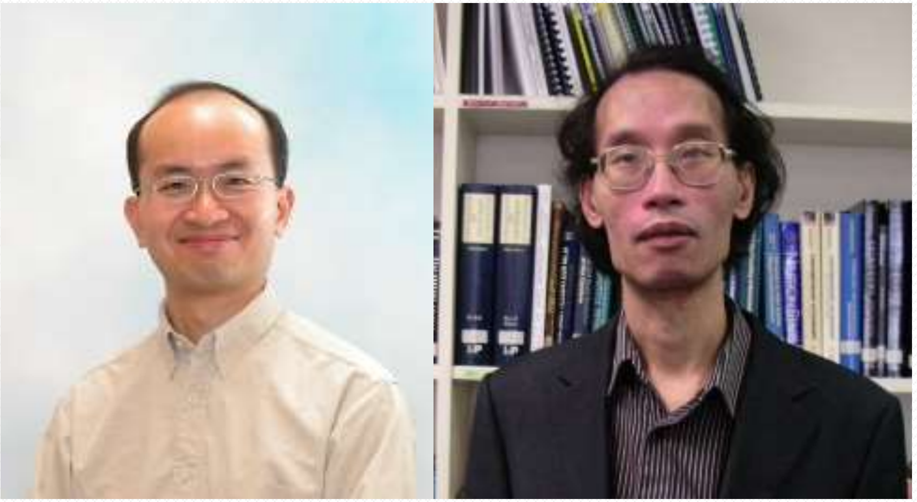
(4) *Sifting:* Alice and Bob announce their basis choices publicly and keep the bits where bases match.

(5) *Key Distillation:* Alice and Bob perform classical postprocessing, including information reconciliation and privacy amplification, to generate a secret key.



Lo-Chau security proof: BBM92

- Entanglement distillation
  - Distill perfect EPR pairs from imperfect ones
  - Bell basis: $|00\rangle \pm |11\rangle, |10\rangle \pm |01\rangle$
  - Objective: $|00\rangle + |11\rangle$
- Bit errors (Z)
  - $|01\rangle + |10\rangle$
- Phase errors (X)
  - $|00\rangle - |11\rangle$
- Both bit and phase errors (Y)
  - $|01\rangle - |10\rangle$



Lo and Chau, Science 283, 2050 (1999)

Security based on entanglement distillation

- Bit error correction (Z: 0,1)
  - Bit errors: |01>+|10> and |01>-|10>
  - After bit error correction: |00>+|11> or |00>-|11>
- Phase error correction (X: +,-)
  - Phase errors: |00>-|11> or |01>-|10>
  - After phase error correction: |00>+|11> or |01>+|10>
- Share (almost) pure EPR pairs: |00>+|11>
- Measure in Z basis to get final key
  - Almost perfect privacy (randomness)

$$(|00\rangle + |11\rangle)^n$$

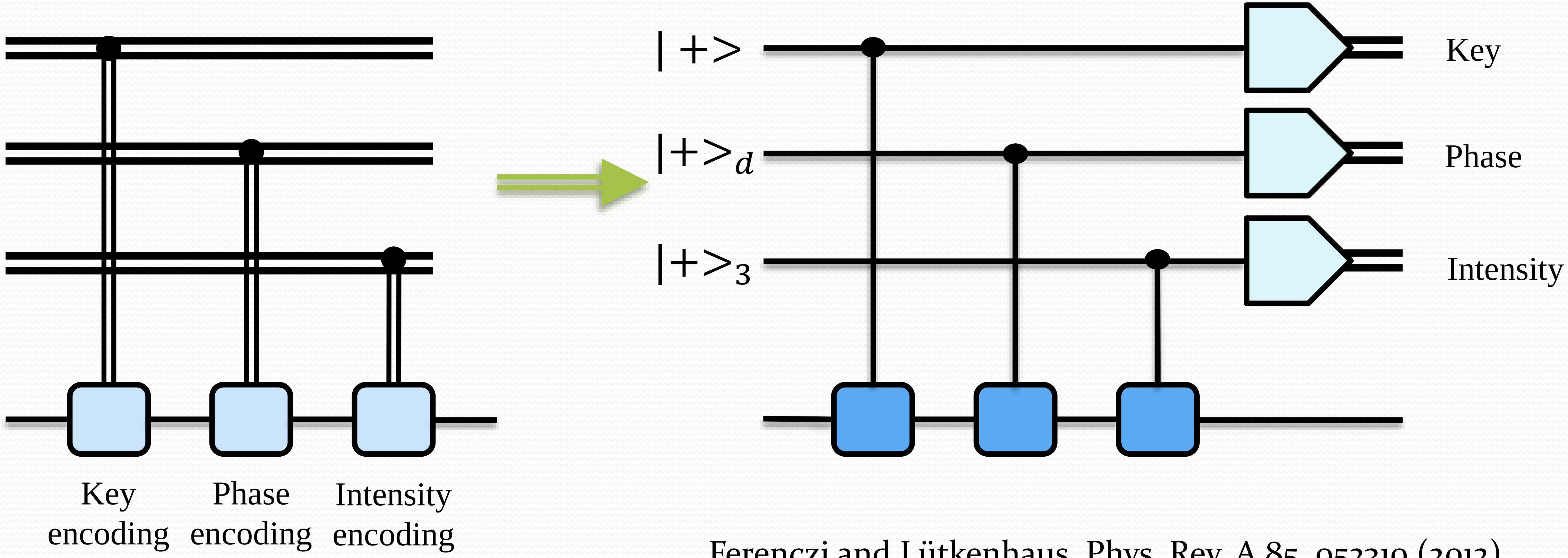
Local Z measurement

$$\sum_k |kk\rangle\langle kk| \otimes \rho_E$$

Secure key definition:
Ben-Or, Horodecki, Leung, Mayers, and Oppenheim, TCC 2005
Renner and König, TCC 2005

Source replacement

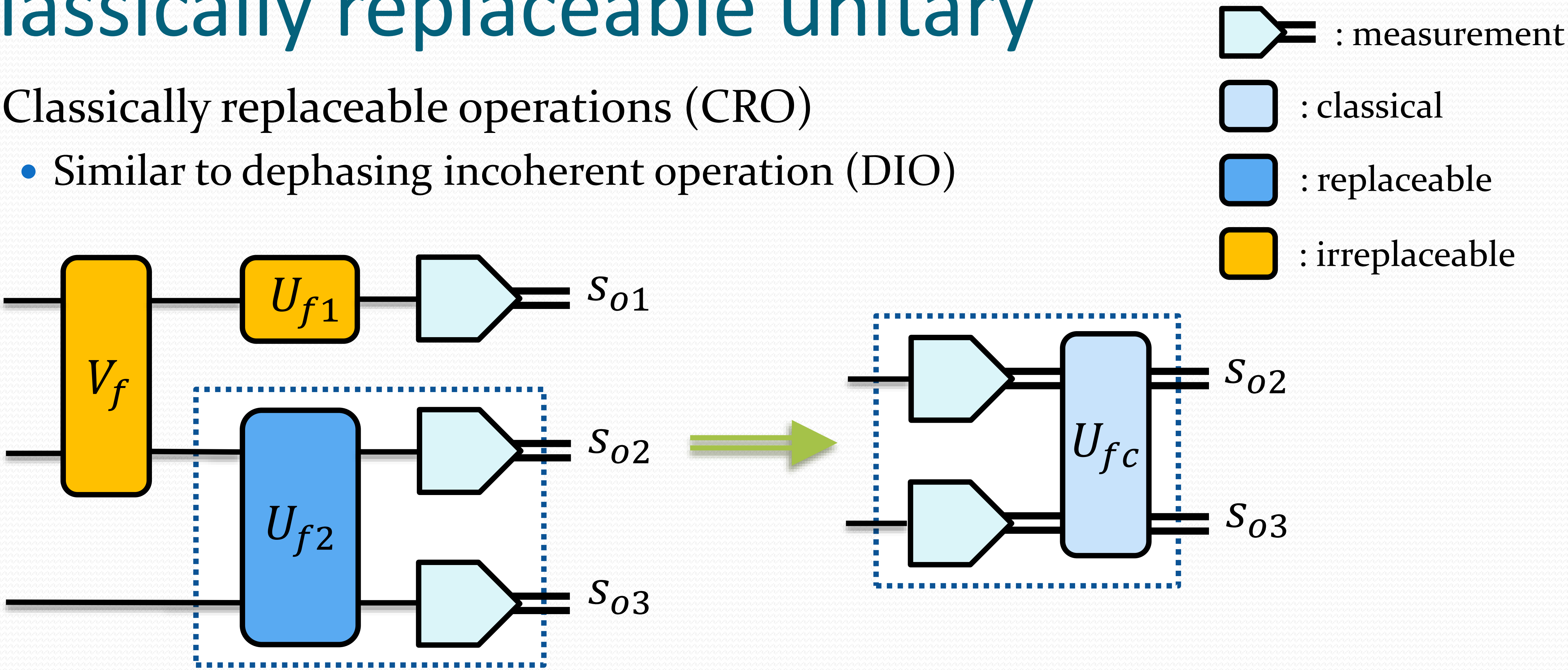
- Classical encoding ⇒ ancilla qubits + control-unitary



Ferenczi and Lütkenhaus, Phys. Rev. A 85, 052310 (2012)

Classically replaceable unitary

- Classically replaceable operations (CRO)
  - Similar to dephasing incoherent operation (DIO)



Liu, Zhang, and Ma Quantum 6, 845, (2022)

Shor-Preskill security proof

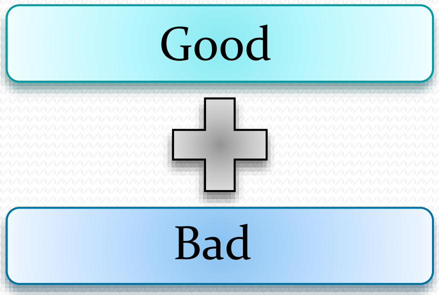
- Problem with the Lo-Chau proof
  - Requires quantum computers
- Reduce to prepare-and-measure schemes
  - Commuting operations in quantum mechanics
  - Put the final key measurement ahead before error correc
- Bit error correction becomes key reconciliation
  - Enables Alice and Bob shares identical keys
- Phase error correction becomes privacy amplification
  - Enables Alice and Bob shares private keys

Shor and Preskill, PRL 85, 441 (2000)

$$R = 1 - H(e_{bit}) - H(e_{phase})$$

Gottesman-Lo-Lütkenhaus-Preskill 2004

- Two types of raw key bits
  - Good ones: secure (e.g. single photon states)
  - Bad ones: insecure (e.g. multi photon states)

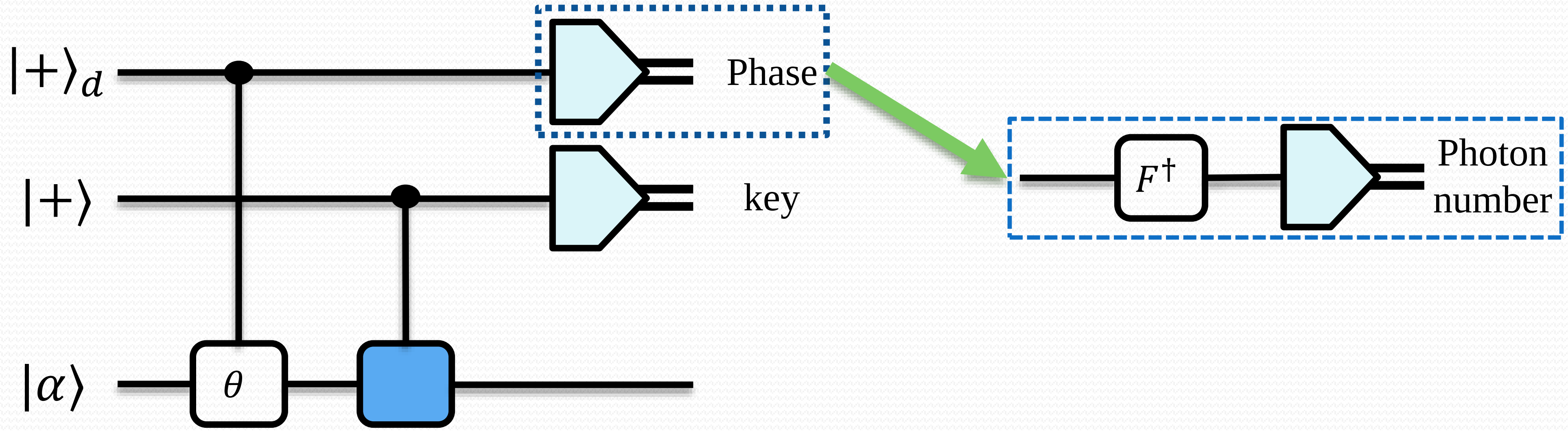


- Tagging idea
  - Raw key contains good key bits and bad key bits
  - Good key $\oplus$ Bad key = Good key
  - Only need to know the amount of good key, and then "randomly" XOR all the key bits
  - Privacy amplification can be only performed on good ones

$$R \geq -Q_\mu h(E_\mu) + Q_1[1 - h(e_1)]$$

Phase randomization vs. Fock state

- Input coherent state
- Phase randomization



Optic encoding

Qubit encoding with photons

- Polarization encoding
  - $|0\rangle$: horizontal; $|1\rangle$: vertical; $|+\rangle$: 45^o diagonal; $|-\rangle$: -45^o diagonal;
  - Essentially relative phase between two circular polarizations
- Phase encoding
  - Find any two orthogonal modes
  - Time-bin
  - Spectrum; space
- Find a qubit subspace
  - Encoding and detection

State	Polarization	Relative phase
$\|0\rangle$	*horizontal*	0
$\|1\rangle$	*vertical*	π
$\|+\rangle$ $\|0\rangle + \|1\rangle$	45^o *diagonal*	$\frac{\pi}{2}$
$\|-\rangle$ $\|0\rangle - \|1\rangle$	-45^o *diagonal*	$\frac{3\pi}{2}$

Optical modes

$$|0,1,2,\ldots\rangle_s \otimes |0,1,2,\ldots\rangle_r$$

- For quantum cryptography, we often assume the modes are orthogonal
  - Photons in orthogonal modes are perfectly distinguishable
- Qubit subspace of a single photon state

$$|0\rangle_s|1\rangle_r + e^{i\theta}|1\rangle_s\,|0\rangle_r$$

- In practice: coherent state

$$|\alpha\rangle = e^{|\alpha|^2/2}\sum_{k=0}\frac{\alpha^k}{\sqrt{k!}}|k\rangle$$

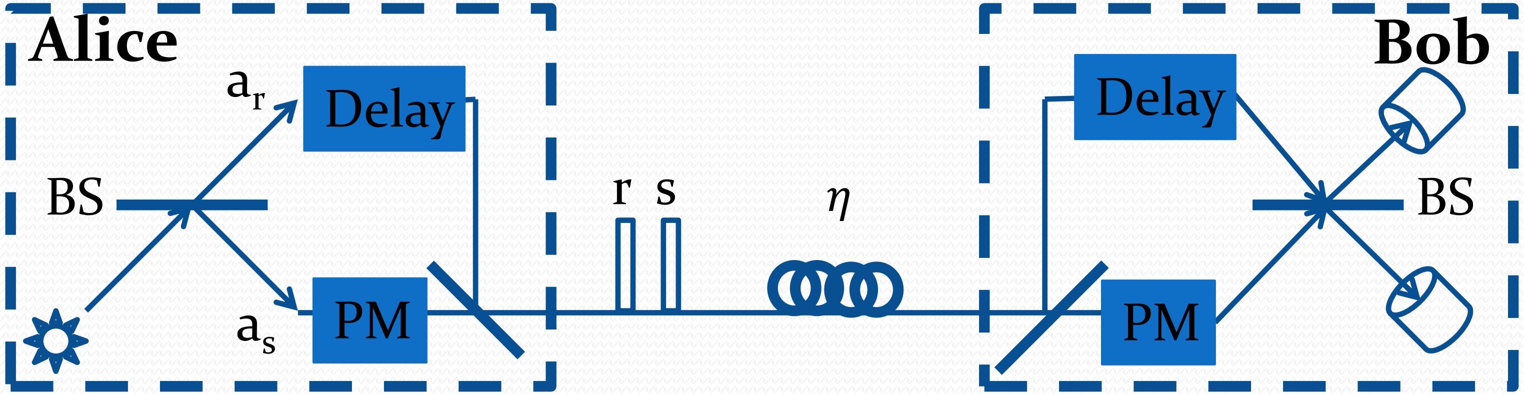
- Here α is a complex number, we can separate intensity μ and phase θ

$$\alpha = \sqrt{\mu}e^{i\theta}$$

Time-bin encoding

- Photon in mode r/s

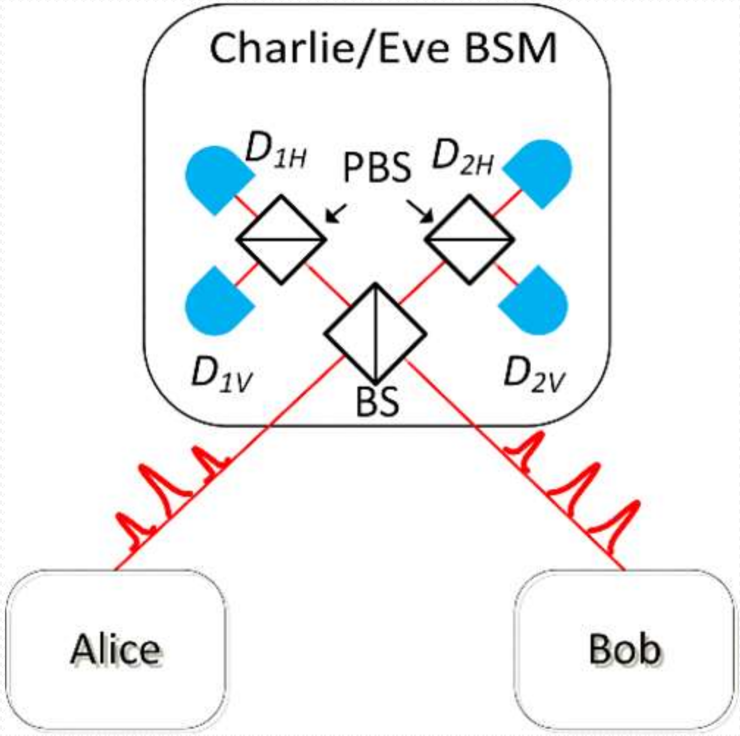
- Advantage: low bit error rate
  - Determined by the vacuum preparation
  - Detection rate: $O(\eta)$, single-click



Measurement-device-independent

MDI-QKD

- Alice and Bob are symmetric
  - Alice (same as Bob) randomly chooses bit {0,1} and basis {X, Z} and sends the state to an untrusted party, could be Eve
  - Source is the same as BB84
- Eve projects the two qubits into one of four Bell states
  - Bell state measurement (BSM)
- "Time-reversed" EPR distribution QKD (BBM92)

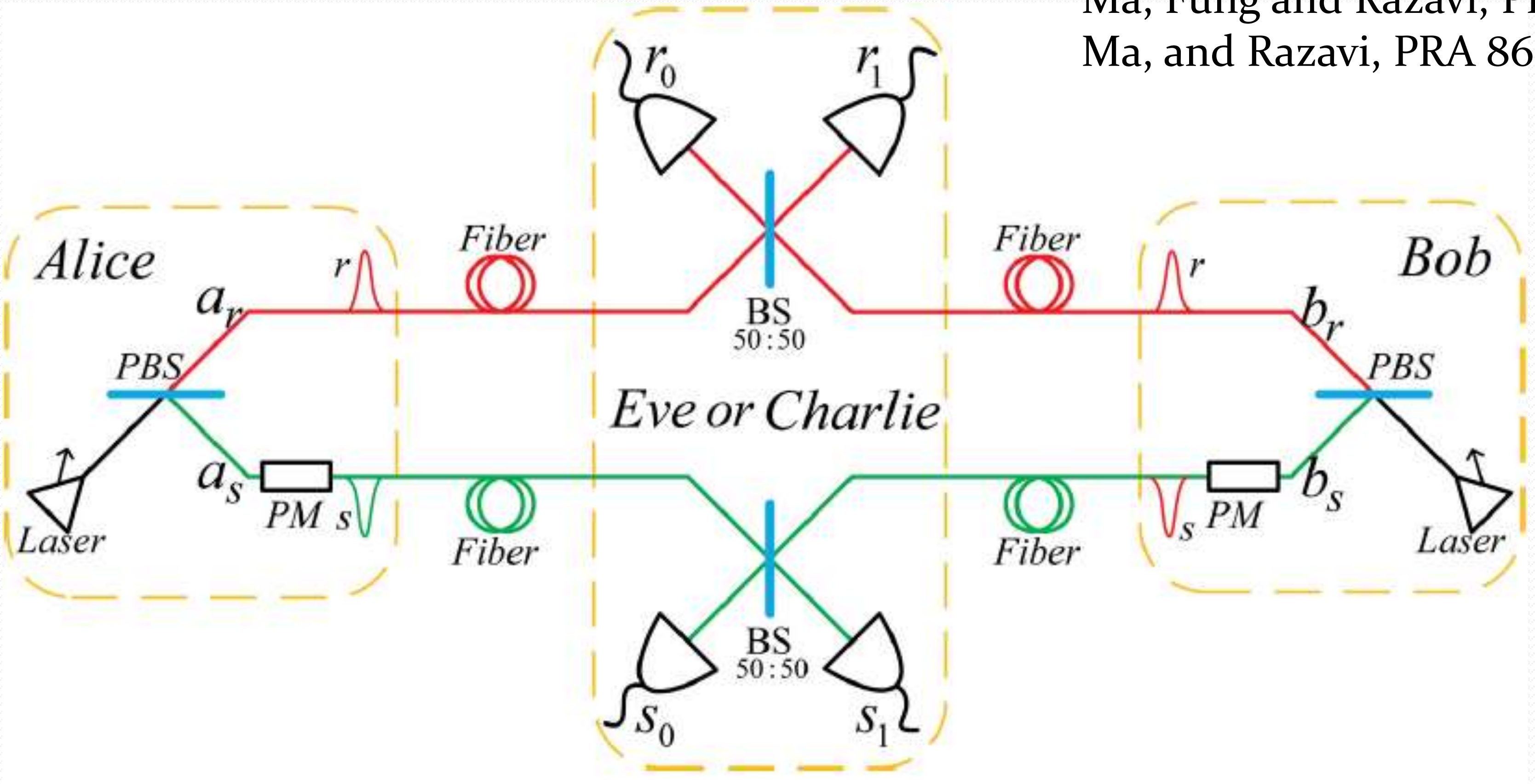


Lo, Curty, and Qi, PRL 108, 130503 (2012)

Time-bin phase-encoding MDI-QKD

- Relative phase of two modes: $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$

Tamaki, Lo, Fung, and Qi, PRA 85, 042307 (2012)
Ma, Fung and Razavi, PRA 86, 052305 (2012)
Ma, and Razavi, PRA 86, 062319 (2012)



Features of MDIQKD

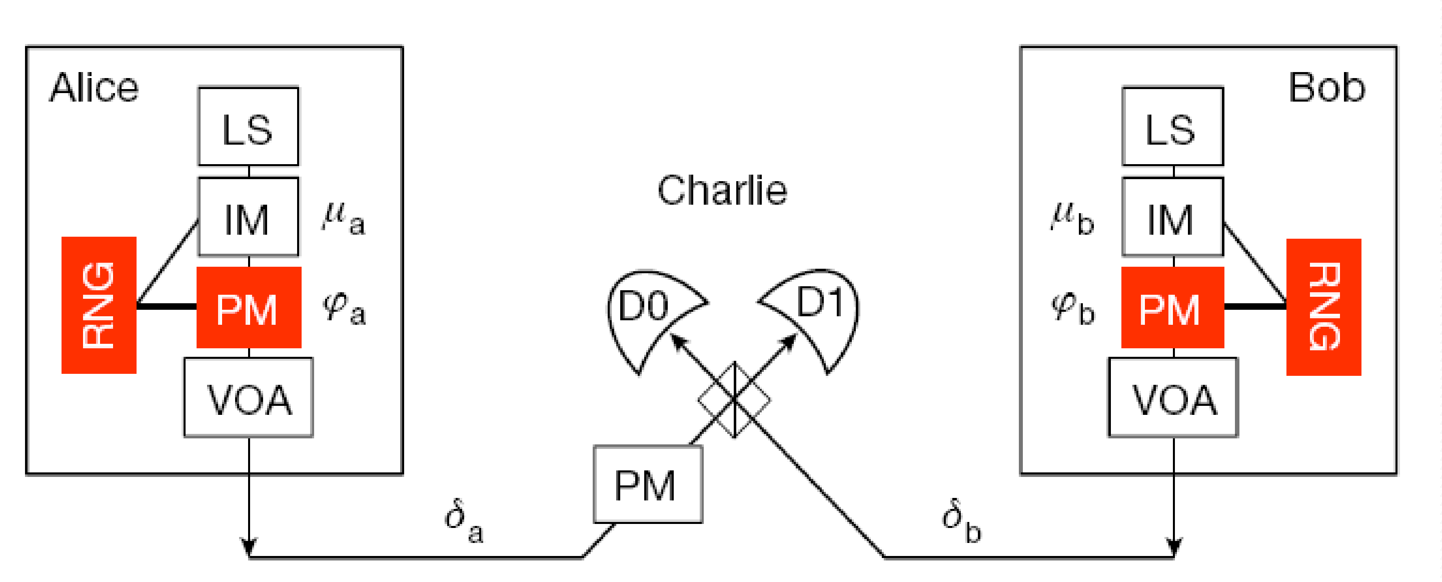
- Measurement device independent
  - The measurement devices are assumed to be held by an untrusted party
  - Immune to all detection attacks
- Two quantum channels
  - Like entanglement based protocol, the effects of background counts can be reduced
  - Need coincident detection

$$R = O(\eta)$$

- Performance: same as the decoy-state QKD, under the linear bound

Twin-field QKD

- Key rate of $R = O(\sqrt{\eta})$!
  - BB84 type encoding, $|01\rangle \pm |10\rangle, |01\rangle \pm i|10\rangle$ as the X,Y basis
  - Introduce the decoy state method

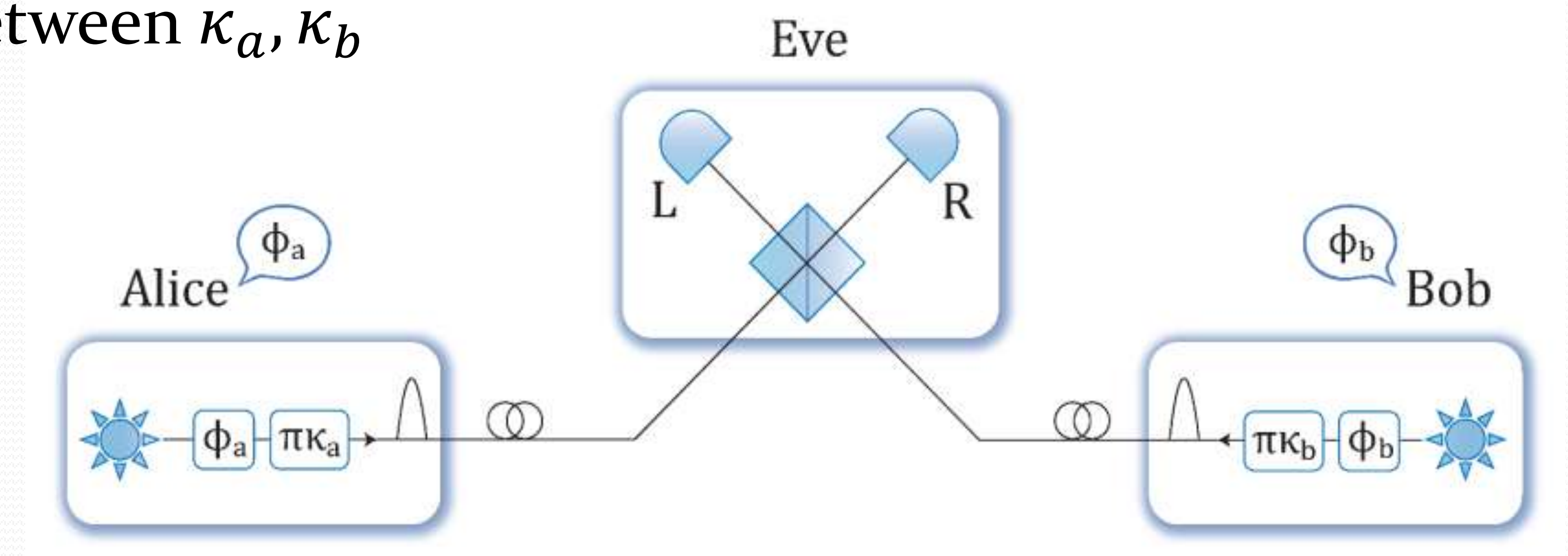


Lucamarini, Yuan, Dynes and Shields, Nature 557(7705): 400 (2018)

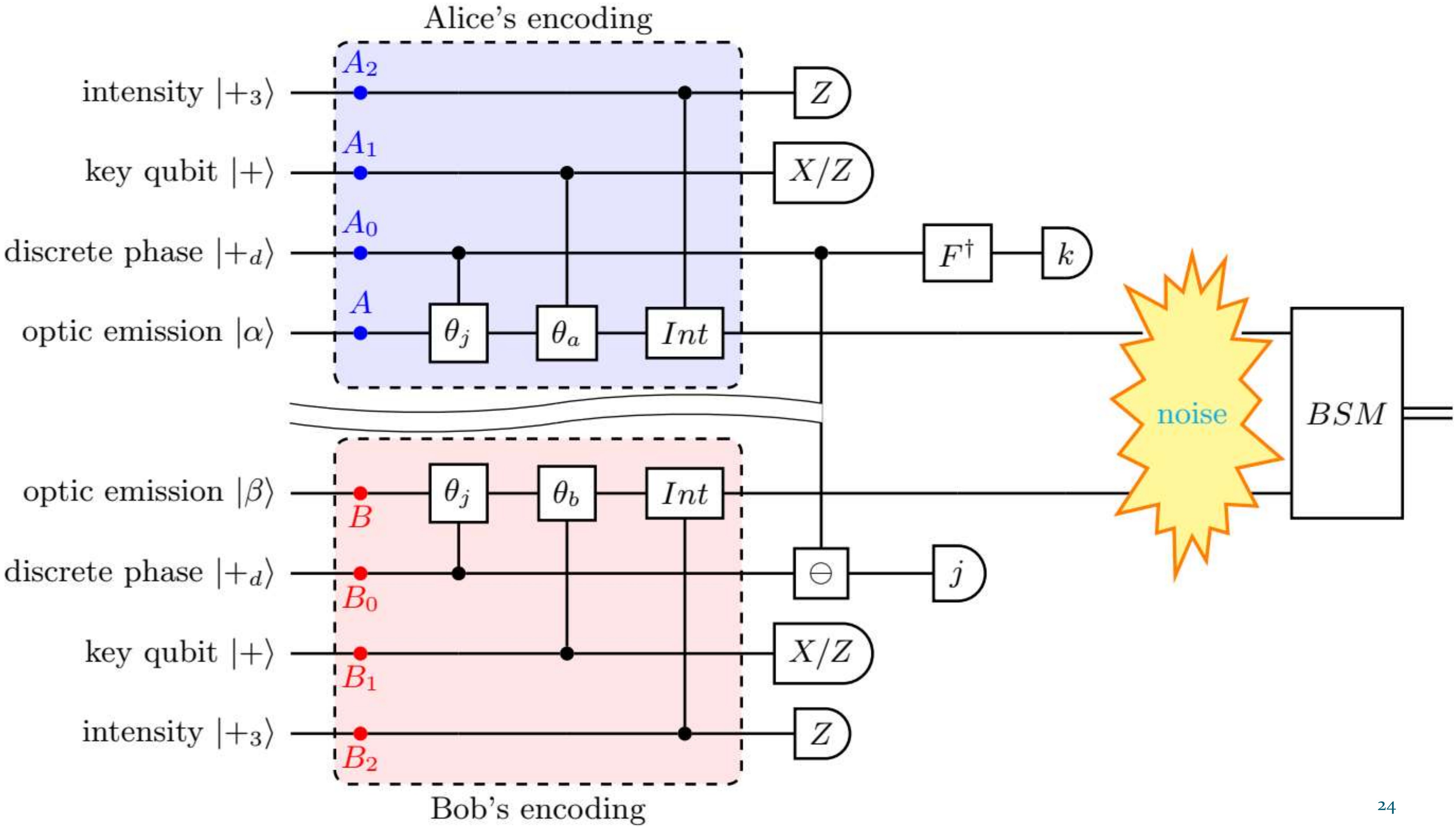
Phase-matching (MDI) QKD

Ferenczi, Chapter 7, Ph.D. thesis (2013)
Ma, Zeng and Zhou, PRX.8.031043, (2018)
Lin and Lütkenhaus, PRA, 98(4), 042332, (2018)

- Extension of “MDI-B92” protocol
- Detection matches the phases: Eve’s detection create a correlation between κ_a, κ_b



$\left|\sqrt{\mu}e^{i(\phi_a+\pi\kappa_a)}\right\rangle_A$ $\left|\sqrt{\mu}e^{i(\phi_b+\pi\kappa_b)}\right\rangle_B$



Alice's encoding
intensity $|+_3\rangle$
key qubit $|+\rangle$
discrete phase $|+_d\rangle$
optic emission $|\alpha\rangle$
A_2
A_1
A_0
A
θ_j
θ_a
Int
Z
X/Z
$F^\dagger$
k
noise
BSM
optic emission $|\beta\rangle$
discrete phase $|+_d\rangle$
key qubit $|+\rangle$
intensity $|+_3\rangle$
B
B_0
B_1
B_2
θ_j
θ_b
Int
$\ominus$
j
X/Z
Z
Bob's encoding

Key rate

- Phase announcement is critical, and does not commute with photon number measurement
- Photon number channel model invalid: collective BS attacks
- Key observation: even parity state = phase error

$$R = Q_\mu\left(1 - H\left(E_\mu^Z\right) - H(q_{even})\right)$$

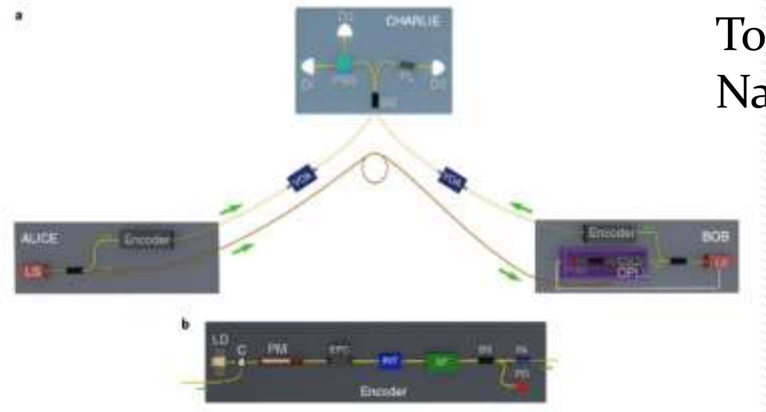
  - $Q_\mu = \sum_k p_k Y_k = O(\sqrt{\eta})$
  - $q_{even} = 1 - \sum_k q_{2k+1} \leq 1 - q_1$
  - $q_k = \frac{p_k Y_k}{Q_\mu}$; $E_\mu^Z = \sum_k q_k e_k^Z$

$$R = O(\sqrt{\eta})$$

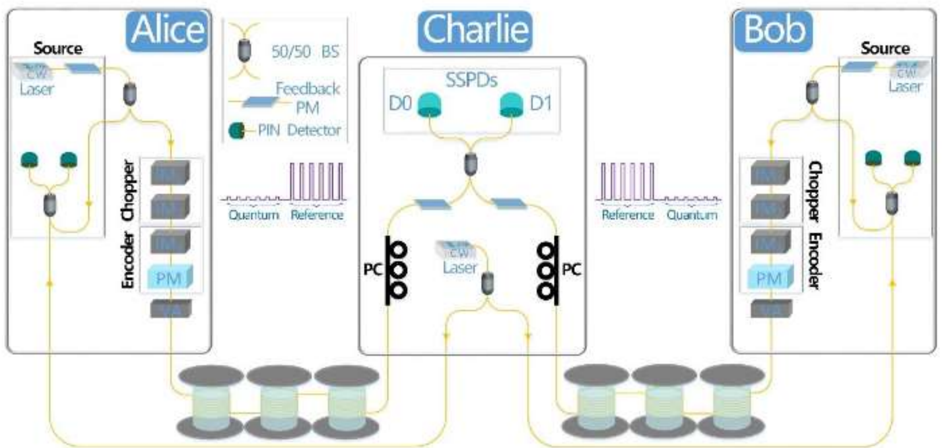
Maeda, Sasaki, and Koashi, Nat. Comm. **10**, 3140 (2019)

Zeng, Wu, and Ma, Phys. Rev. Applied 13, 064013, (2020)

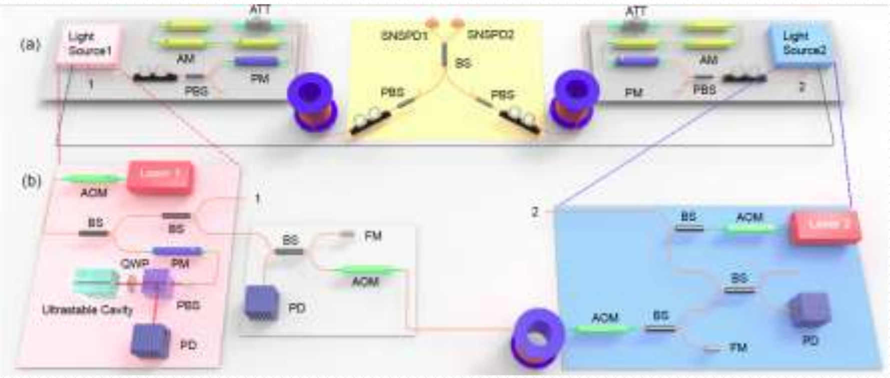
Experimental realizations



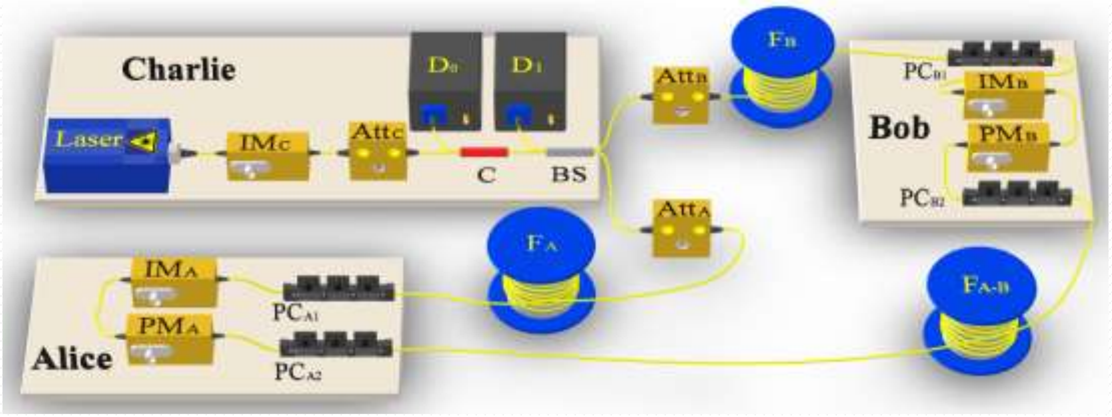
Toshiba group
Nat. Photon. 13, 334–338 (2019)



USTC Han's group
PRX 9, 021046 (2019)



USTC Pan's group: PRL 123, 100505 (2019)



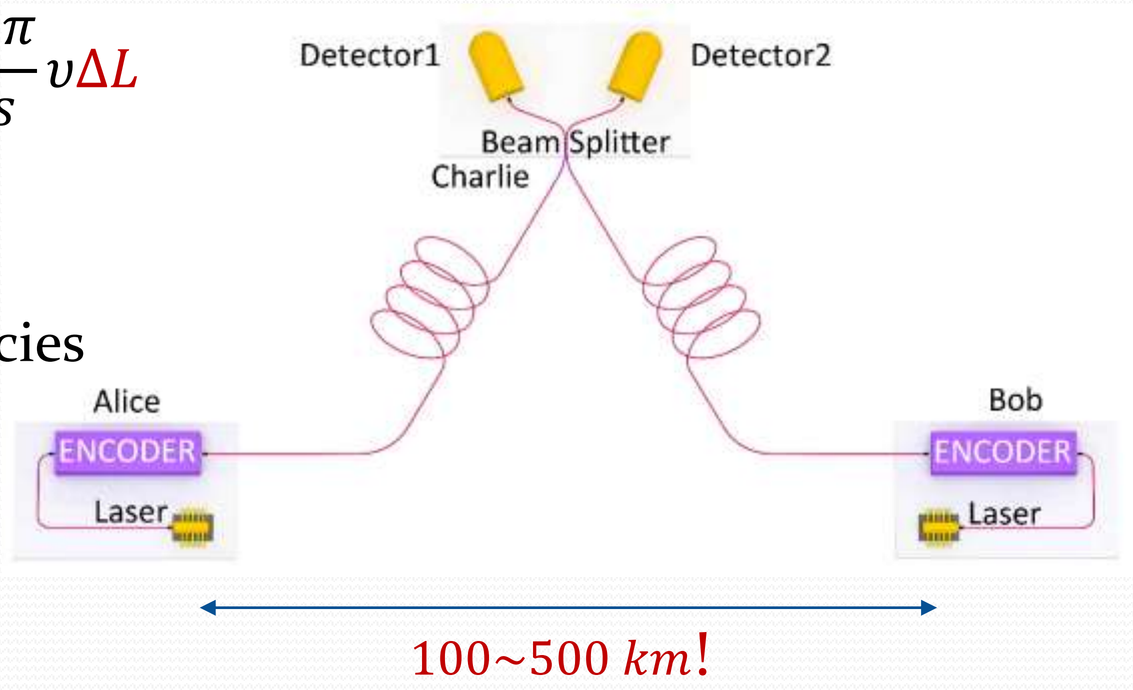
Toronto Lo's group: PRL 123, 100506 (2019)

Challenges in experiment

- Core issue: a long-arm single-photon interferometer
- Phase stabilization: major challenge

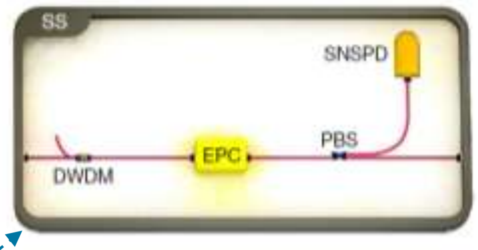
$$\delta_{ba} = \phi_b(t) - \phi_a(t) = \Delta\phi^0 \; + \; \frac{2\pi}{s}L\Delta\upsilon \; + \; \frac{2\pi}{s}\upsilon\Delta L$$

- $\Delta\phi^0$: fluctuation of the initial phase
  - Long coherence time >> pulse interval time
- $\Delta\upsilon$: deviation and fluctuation of laser frequencies
  - Cannot be larger than 1kHz
- ΔL: drift of fiber optical length
  - Cannot be longer than 200 nm

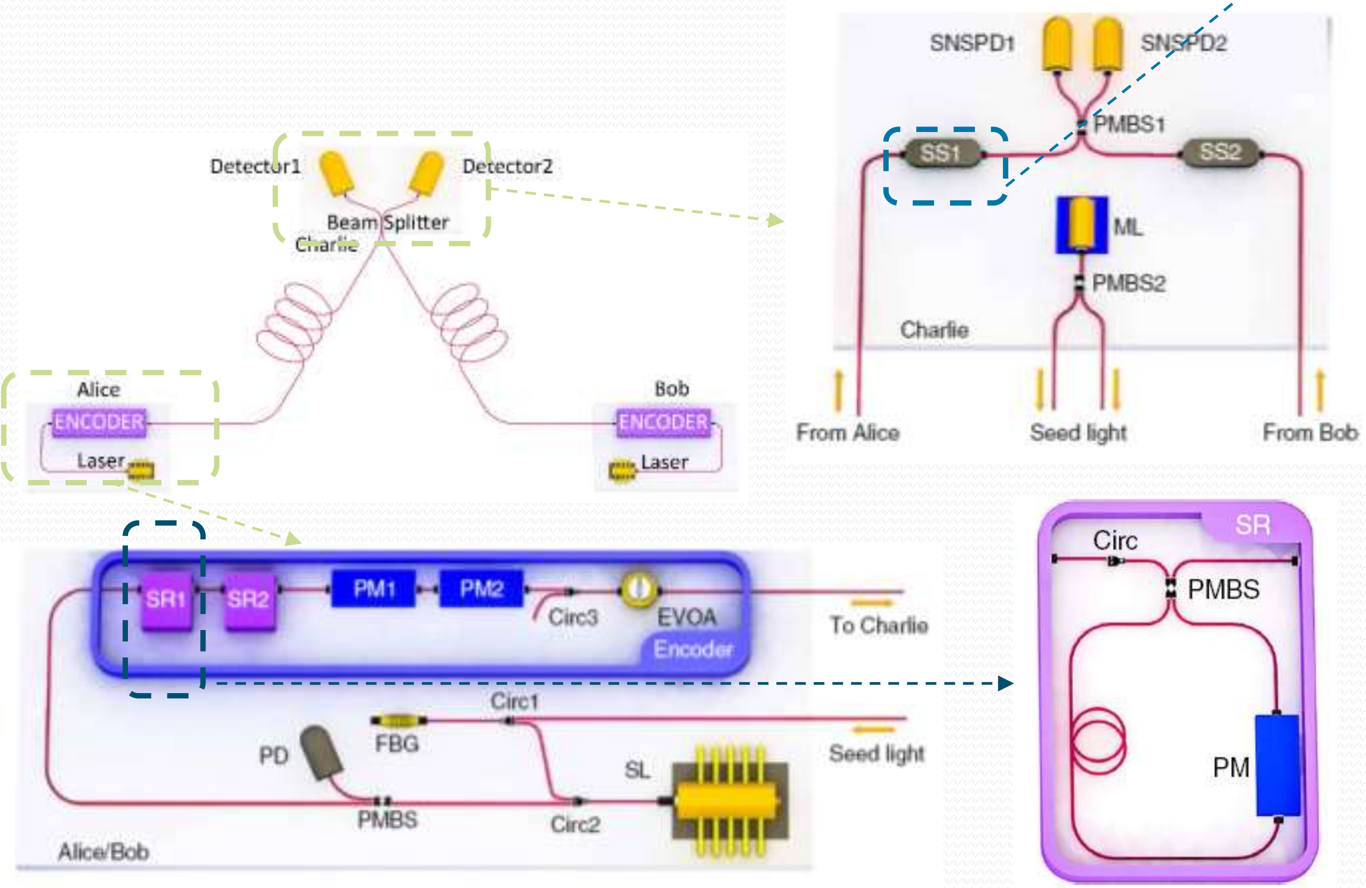


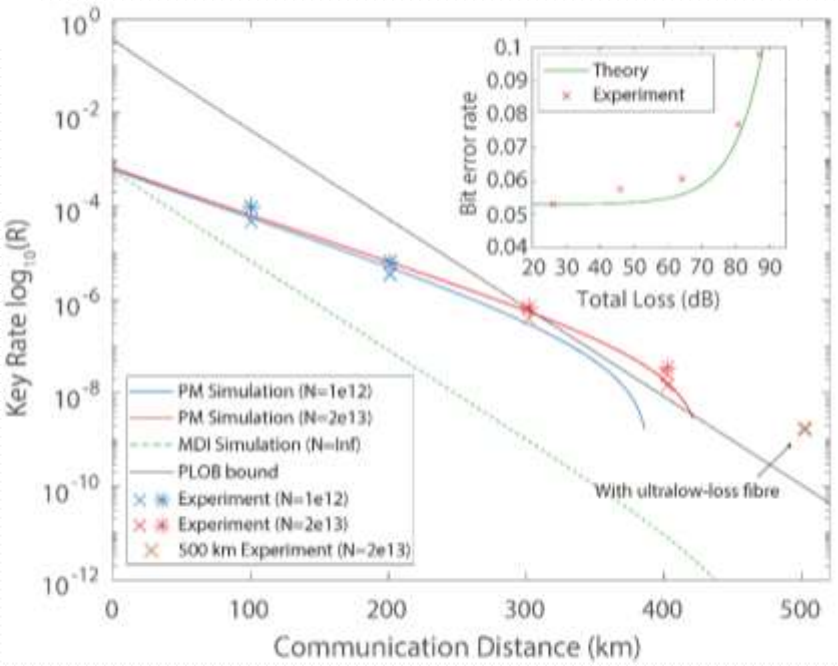
Exp implementation

- Laser injection + phase post-selection



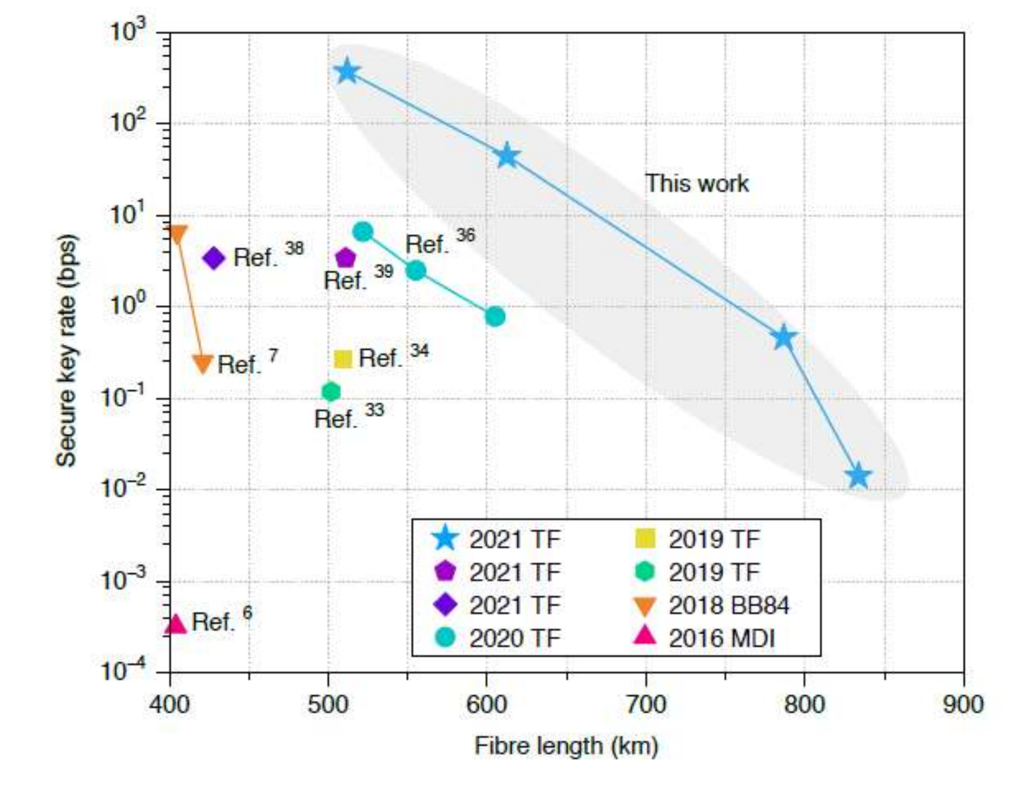
Parameters	Values
Slice number, D	16
Error correction efficiency, f	1.1
Background count rate, p_d	1.2×10^{-8}
Detection efficiency, η_d	23%
PM misalignment error, e_d^{pm}	5.3%
MDI misalignment error, e_d	1.5%
Fibre loss	0.19 dB km^{-1}

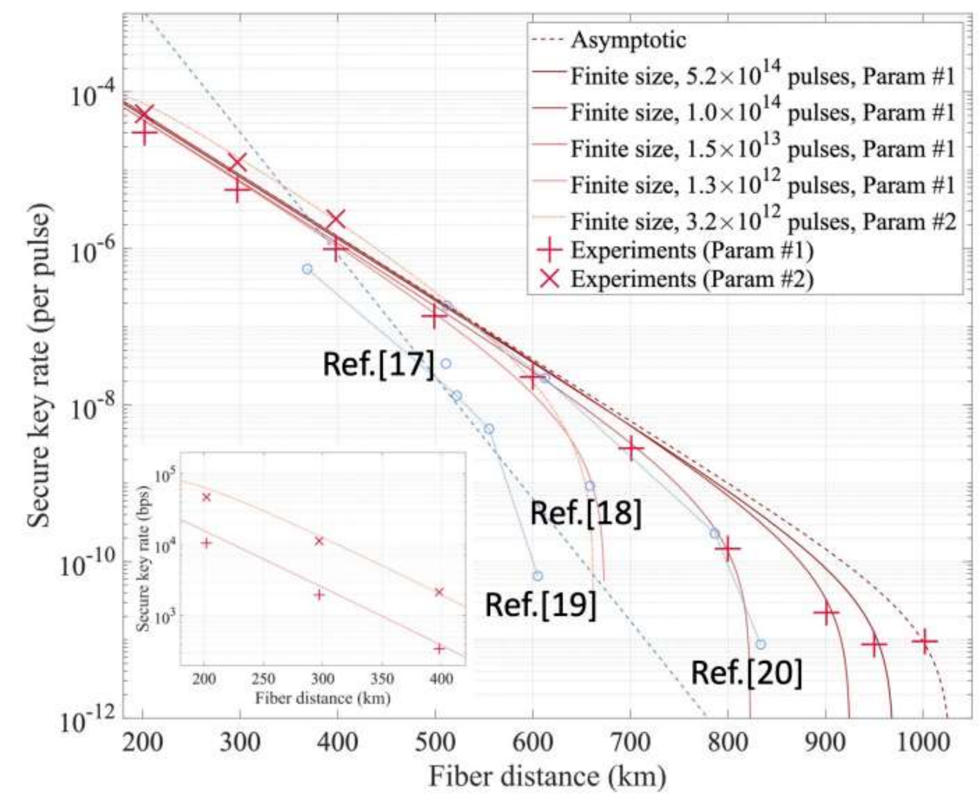




USTC group: Fang et al. Nat. Photon. 14, 422-425, (2020)

Extreme experimental distance





Wang et al., Nature Photonics 16, 154–161 (2022)
833 km

Liu et al., PRL 130, 210801 (2023)
Over 1000 km

Mode-pairing scheme

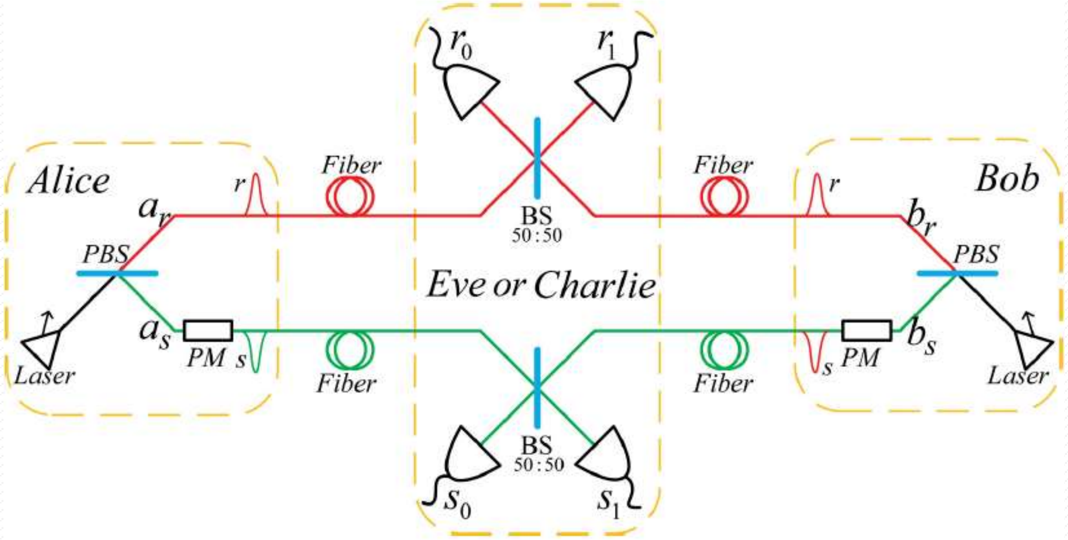
Trade-off in practicality and performance

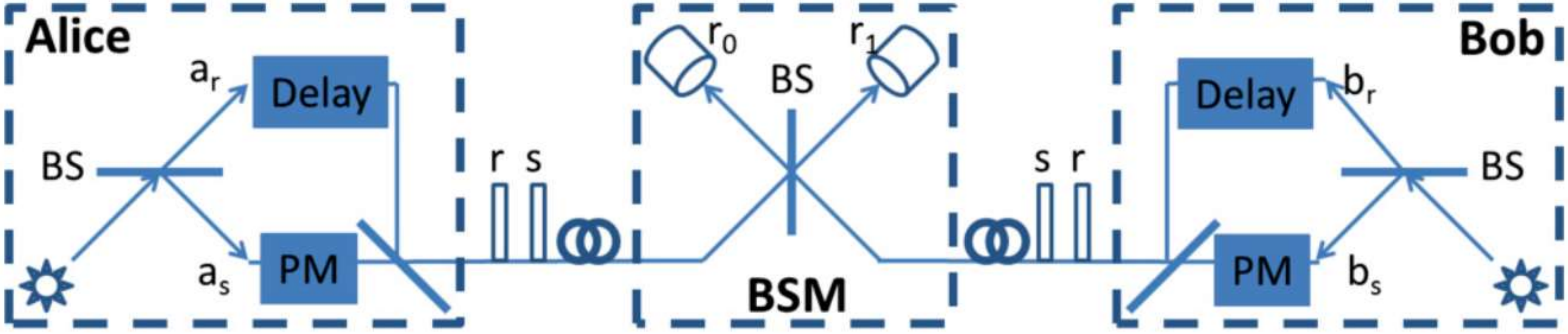
- Key challenge in phase-matching scheme: global phase locking
  - Independent lasers
- Quadratic key improvement
- Time-bin encoding MDI-QKD
  - Relative phase is easy to stabilize
  - Key rate linearly depends on transmittance
- Can we have both advantages?
- Yes! With mode-pairing scheme

Zeng, Zhou, Wu, Ma, Nat. Comm. 13, no. 1, 3903, (2022)
Discussions with Norbert Lutkenhaus

Time-bin MDIQKD

- Two orthogonal optical modes
  - Space -> time
- Robust against phase fluctuation

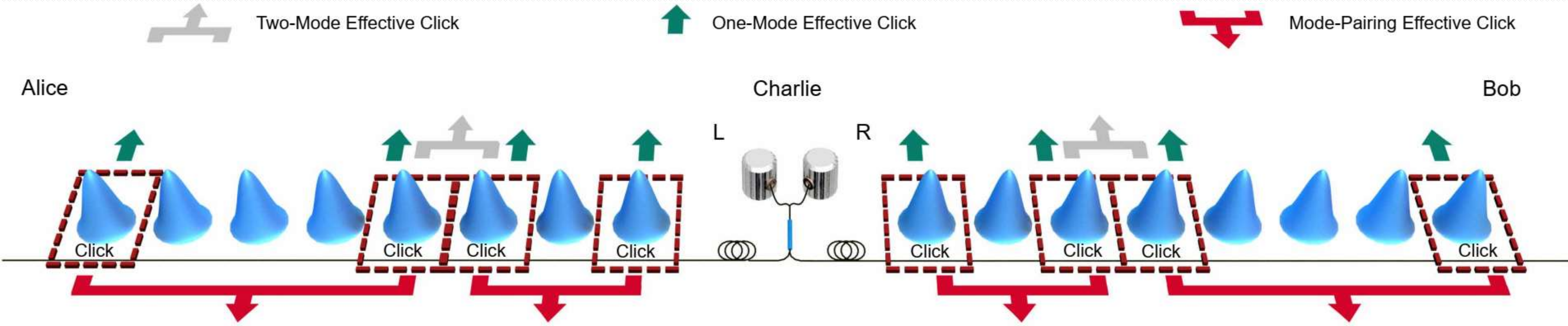




Ma and Razavi, PRA 86, 062319 (2012)

Mode-pairing scheme

- Schematic setup

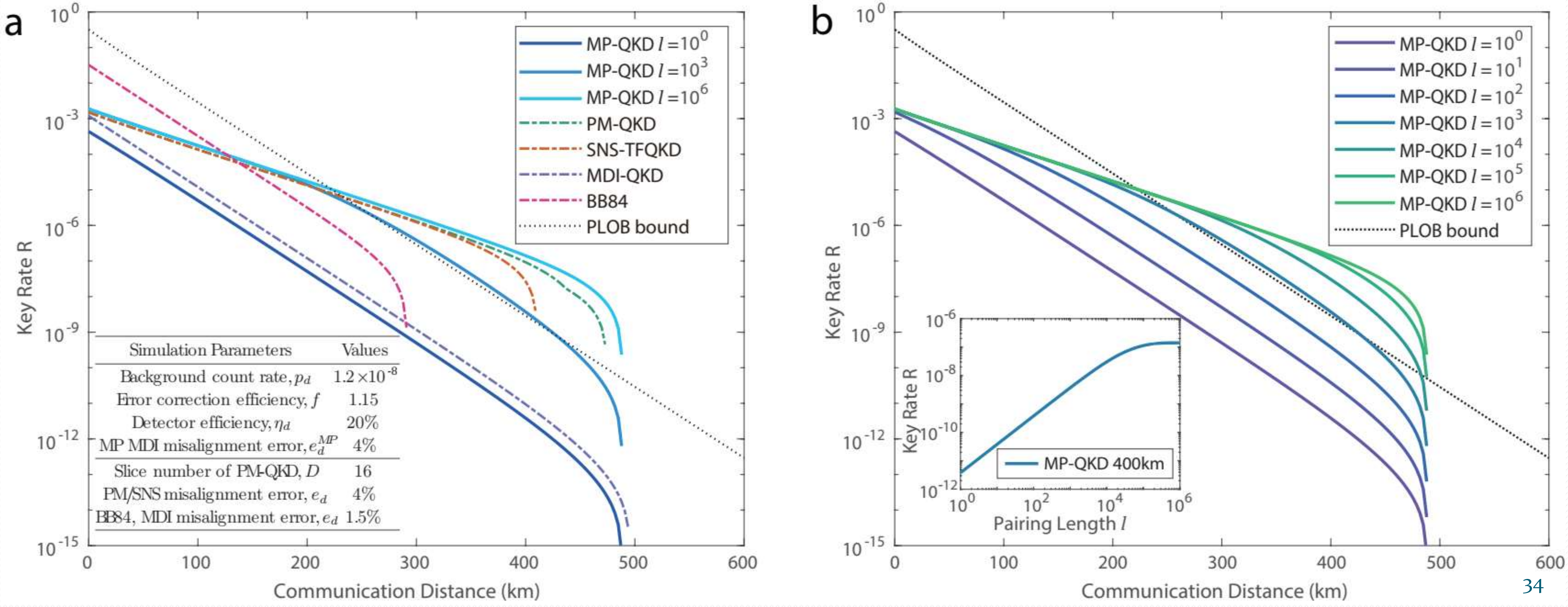


- Key bits are determined after Charlie announces detection results
- Alice and Bob pairs the successfully clicks

Zeng, Zhou, Wu, Ma, Nat. Comm. 13, no. 1, 3903, (2022)
Discussions with Norbert Lutkenhaus

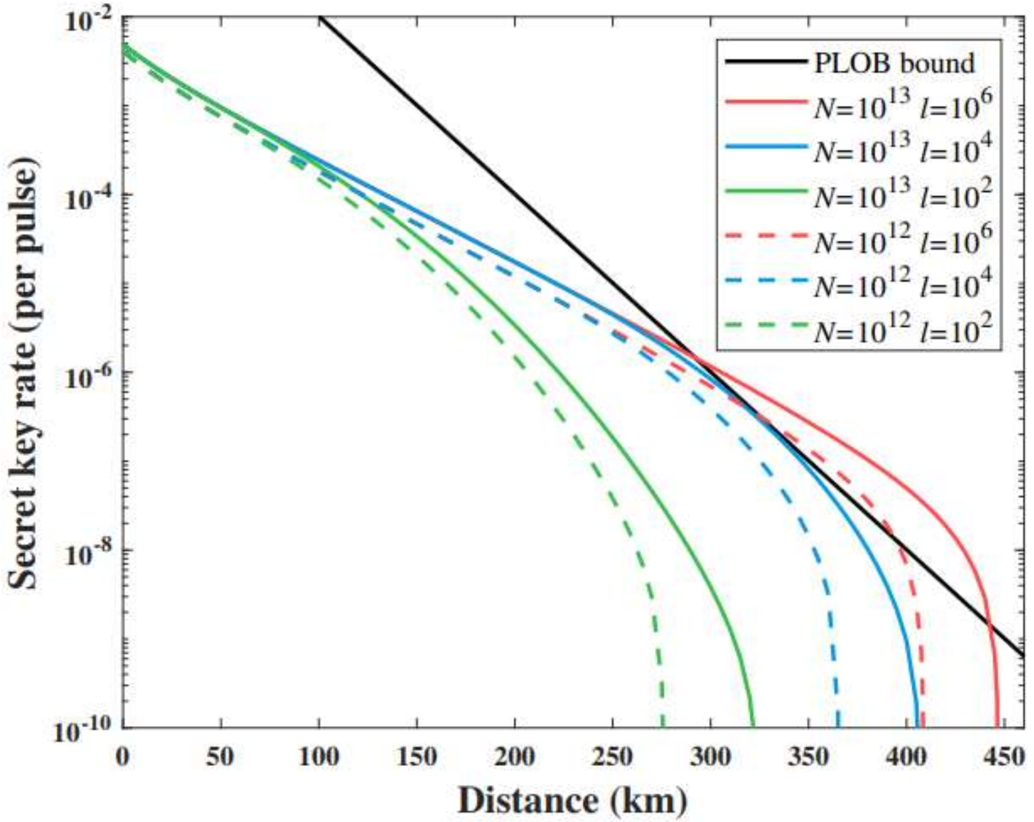
Quadratically key rate improvement

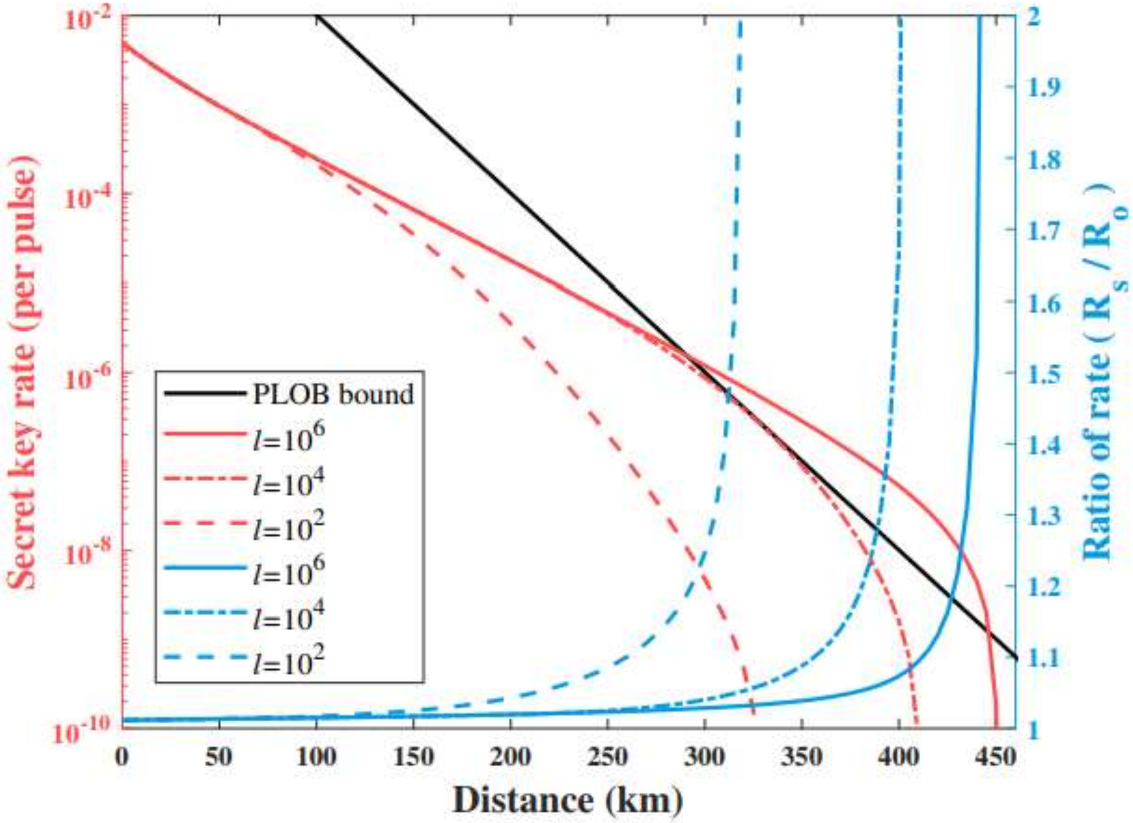
- Performance: $R = O\left(\sqrt{\eta}\right)$



Simulation Parameters	Values
Background count rate, p_d	1.2×10^{-8}
Error correction efficiency, f	1.15
Detector efficiency, η_d	20%
MP MDI misalignment error, e_d^{MP}	4%
Slice number of PM-QKD, D	16
PM/SNS misalignment error, e_d	4%
BB84, MDI misalignment error, e_d	1.5%

Other security analysis

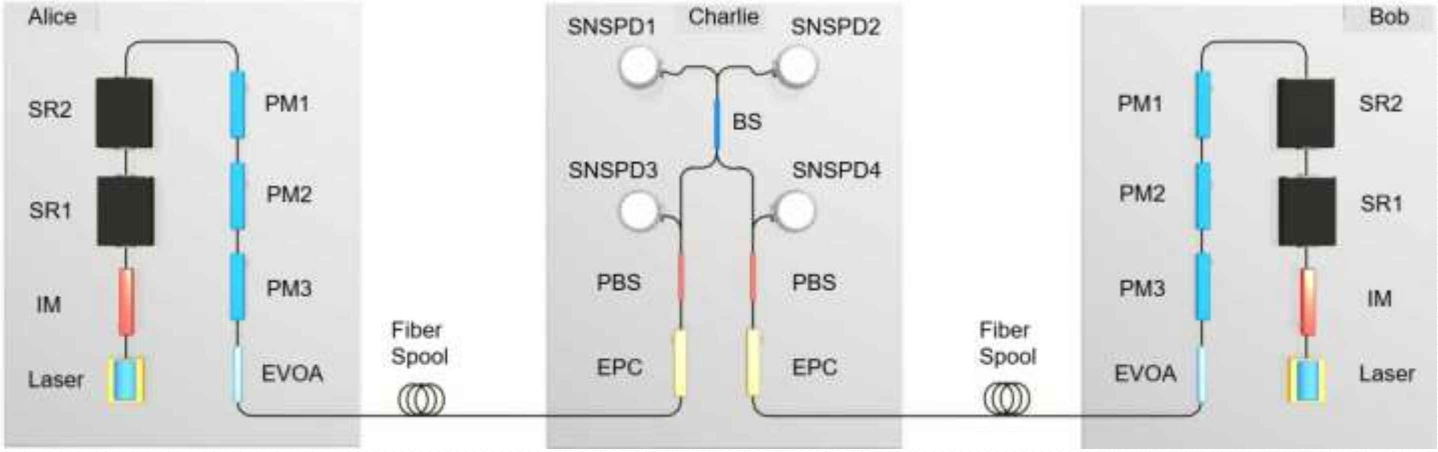


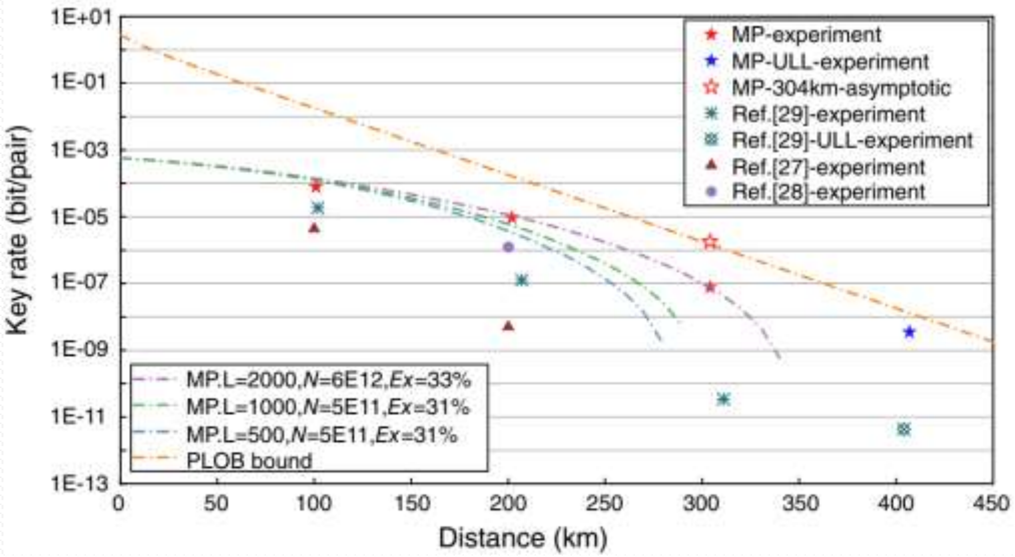


Wang, Yin, et al., arXiv:2302.13481 (2023)

Experimental implementation

- USTC group



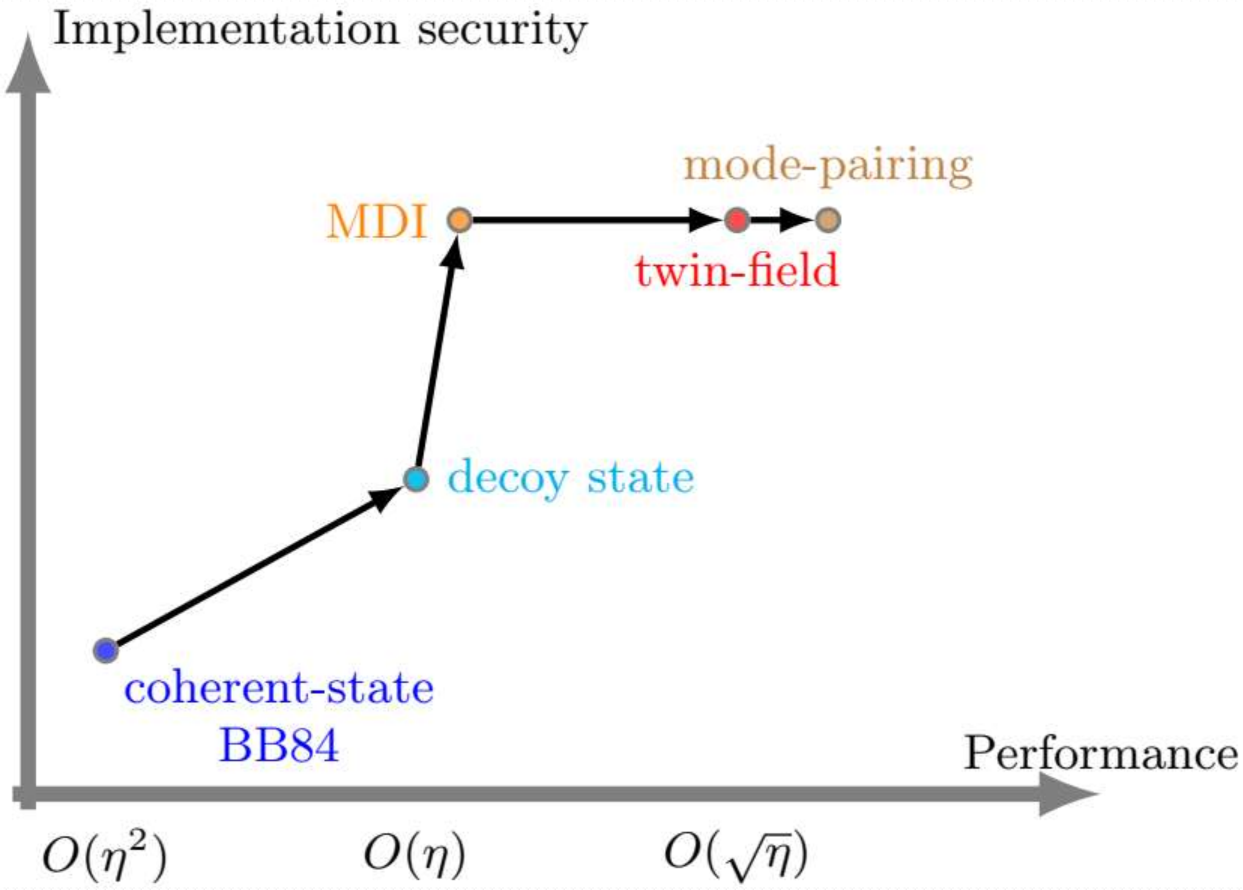


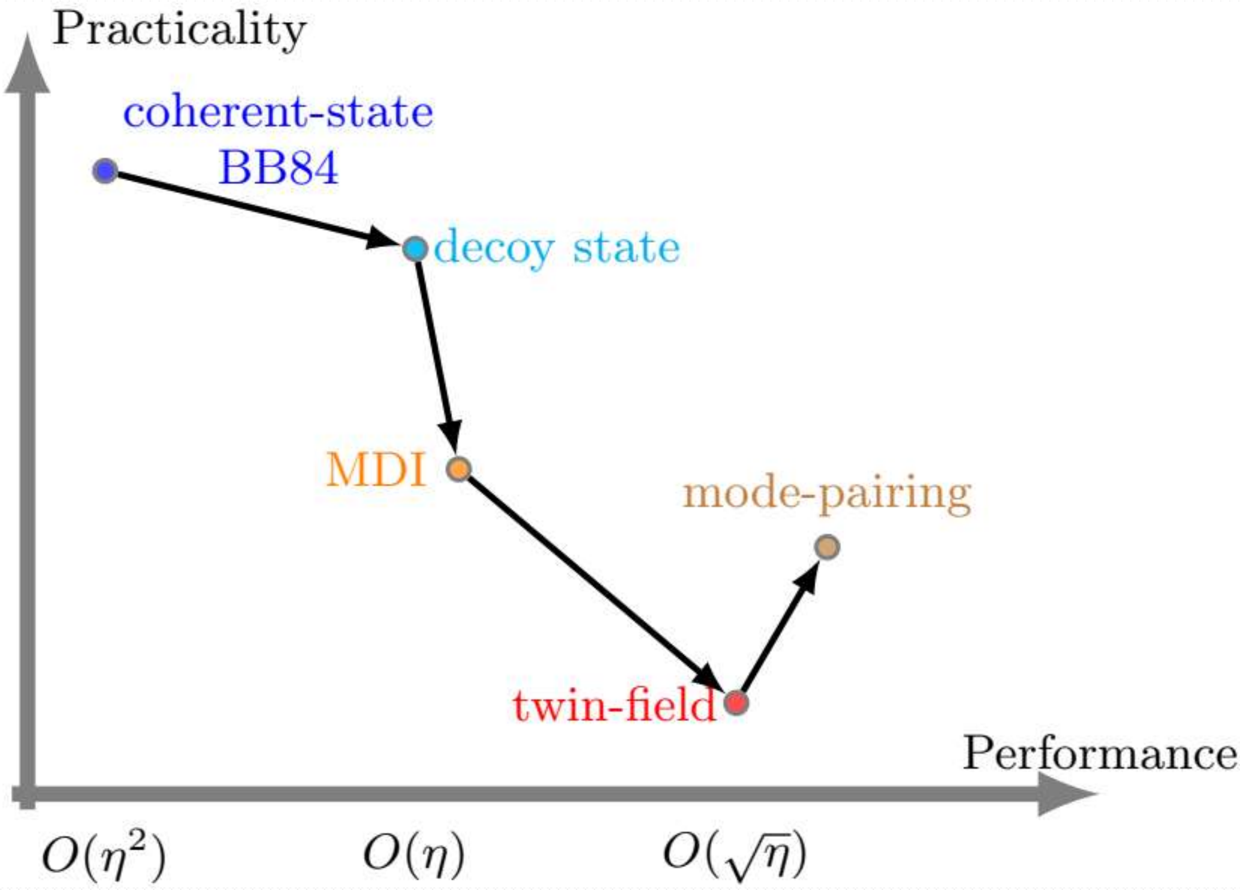
Zhu, Huang, et al., PRL 130, 030801, (2023)
Another demo: Zhou, Lin, Xie, et al., PRL 130, 250801, (2023)

Features of mode-pairing scheme

- Optimal intensity is higher
  - Higher key rate comparing to the phase-matching scheme
- Sifting factor is worse
  - Suffer from large statistical fluctuation
- Key bit and basis value are determined in postprocessing
  - Challenge for security proof

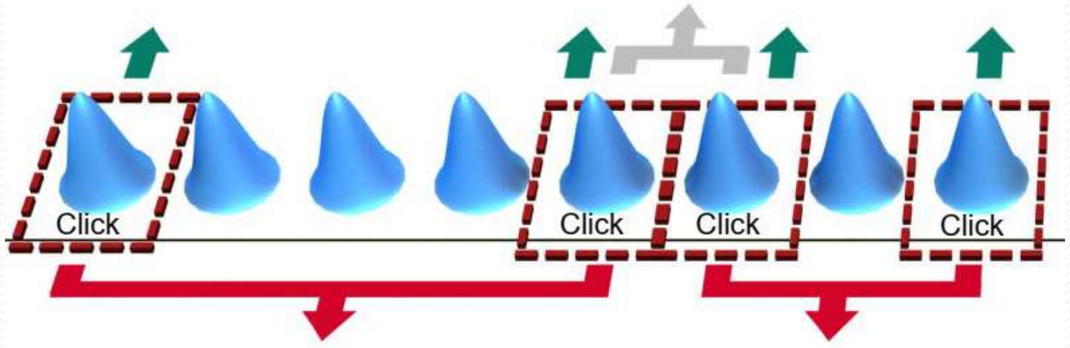
Development of QKD





Open questions: better pairing strategy

- Statistical fluctuation on X-basis data is bad
- Check out a few clicks to determine better pairing
  - Current simple scheme: pair two adjacent clicks
- Depending on some phases and intensities
  - Do not expose key information
- Separate key generation and test bits
  - Better sifting factor
- Regular MDIQKD + mode-pairing



Open questions

- Beyond time-bin mode
  - Paring among different degrees of freedom: frequency, spatial, orbital angular momentum
  - How to encode phases efficiently
- Coherent detection
  - High-dimensional / continuous-variable
- Add more (untrusted) nodes: $R > O(\sqrt{\eta})$?
  - Further enhance the performance
  - Practical repeaters

Conclusion and outlook

- Measurement-device-independent property
- Quadratic key rate

$$R = O(\sqrt{\eta})$$

- Feasible implementation
  - *Remove the global phase-locking requirement!*
- Further enhance implementation security
  - *Reduce the theoretical assumptions on the sources*
- Higher performance
  - High-dimensional/CV encoding
  - Add quantum nodes in the channel

Cheap,
high security-level,
high performance
QKD / Quantum
Internet

electronics

an Open Access Journal by MDPI

IMPACT FACTOR 2.9

CITESCORE 4.7

Electronics (ISSN 2079-9292) is an international, peer-reviewed, open access journal on the science of electronics and its applications.

- **2022 Impact Factor: 2. 90 (*Journal Citation Reports* - Clarivate)**
  71/159 (Q2) in "PHYSICS, APPLIED" (SCIE)
  131/275 (Q2) in "ENGINEERING, ELECTRICAL & ELECTRONIC" (SCIE),
  99/158 (Q3) in "COMPUTER SCIENCE, INFORMATION SYSTEMS" (SCIE)
- **Coverage by Leading Indexing Services** Scopus, SCIE (Web of Science), CAPlus / SciFinder, Inspec, and many other databases.

Editor-in-Chief

Prof. Dr. Flavio Canavero
Department of Electronics and Telecommunications, Politecnico di Torino, 10129 Torino, Italy

Article Processing Time

(data from the second half of 2022**)**

14.4 Days
Submission to First Decision
3.3 Days
Acceptance to publication

Section Quantum Electronics:

This section publishes original and significant contributions to the theory and experimental implementations on the topic of quantum electronics. More specifically, articles will be considered on superconducting circuits, semiconductor qubits, NV centers, and electron qubits in general. Connections to atomic, molecular, and optical physics, as well as to mechatronic systems (i.e., robots and drones) when combined with quantum science, are also welcome. We will consider as well the relation to quantum artificial intelligence and quantum machine learning of electronic quantum systems.

MDPI

Electronics Editorial Office
St. Alban-Anlage 66
4052, Basel, Switzerland

electronics@mdpi.com
www.mdpi.com/journal/electronics
@ElectronicsMDPI

Invitation to submit

Recent Advances in Quantum Communication with Realistic Devices
Guest Editor: Hongyi Zhou
Deadline: 15 October 2023

Quantum Information, Computation and Cryptography
Guest Editors: He-Liang Huang, Chu Guo, Zu-En Su and Shi-Lei Su
Deadline: 15 November 2023

Quantum Computation and Its Applications
Guest Editors: Ilias K. Savvas and Apostolos Xenakis
Deadline: 15 December 2023

Quantum Computing System Design and Architecture
Guest Editors: Koen Bertels and Shaukat Ali
Deadline: 31 December 2023

Advances in Silicon Quantum Electronics
Guest Editors: Prof. Dr. Xihua Wang and Dr. Lingju Meng
Deadline: 31 March 2024

Thank you!

- Welcome to visit!