清華大學 交叉信息研究院

Tsinghua University Institute for Interdisciplinary Information Sciences

Phase-Matching MDI-QKD

Pei Zeng

QCrypt 2018

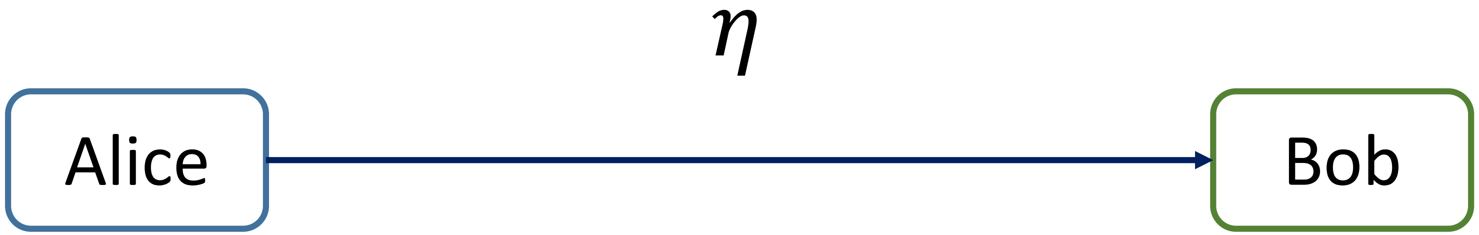
Ma, Zeng and Zhou, PRX.8.031043,(2018)

Outline

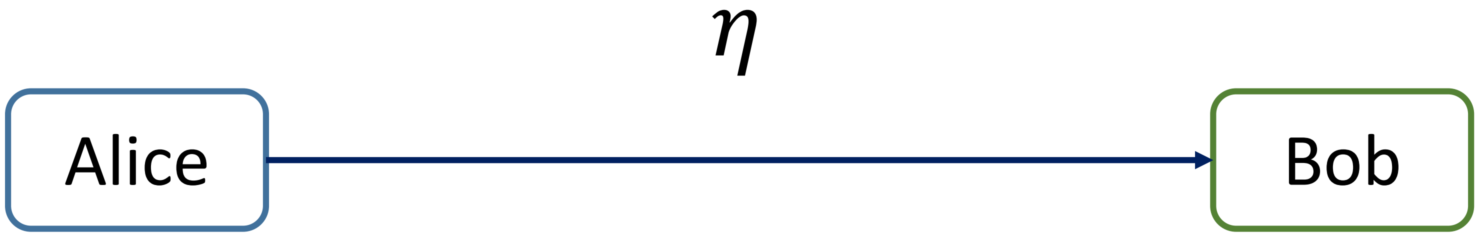
- Motivation & background
- Protocol & security
- Practical issues & simulation
- Summary & outlook

Motivation & Background

$R \quad ? \quad \eta$



$$R = O(\eta^2)$$

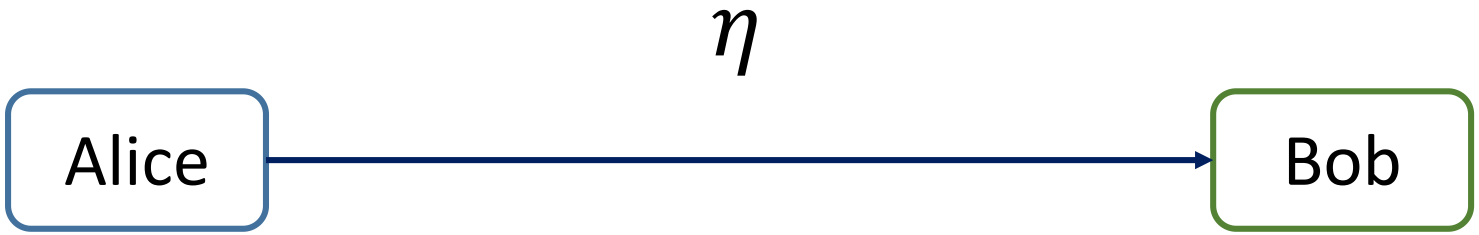


$$|\pm\alpha\rangle, |\pm i\alpha\rangle$$

Huttner, Imoto, Gisin and Mor, PRA 51(3):1863 (1995)
Lo and Preskill, QIC, 7, 431-458 (2007)

$$R = \cancel{O(\eta^2)}$$

$$O(\eta)$$



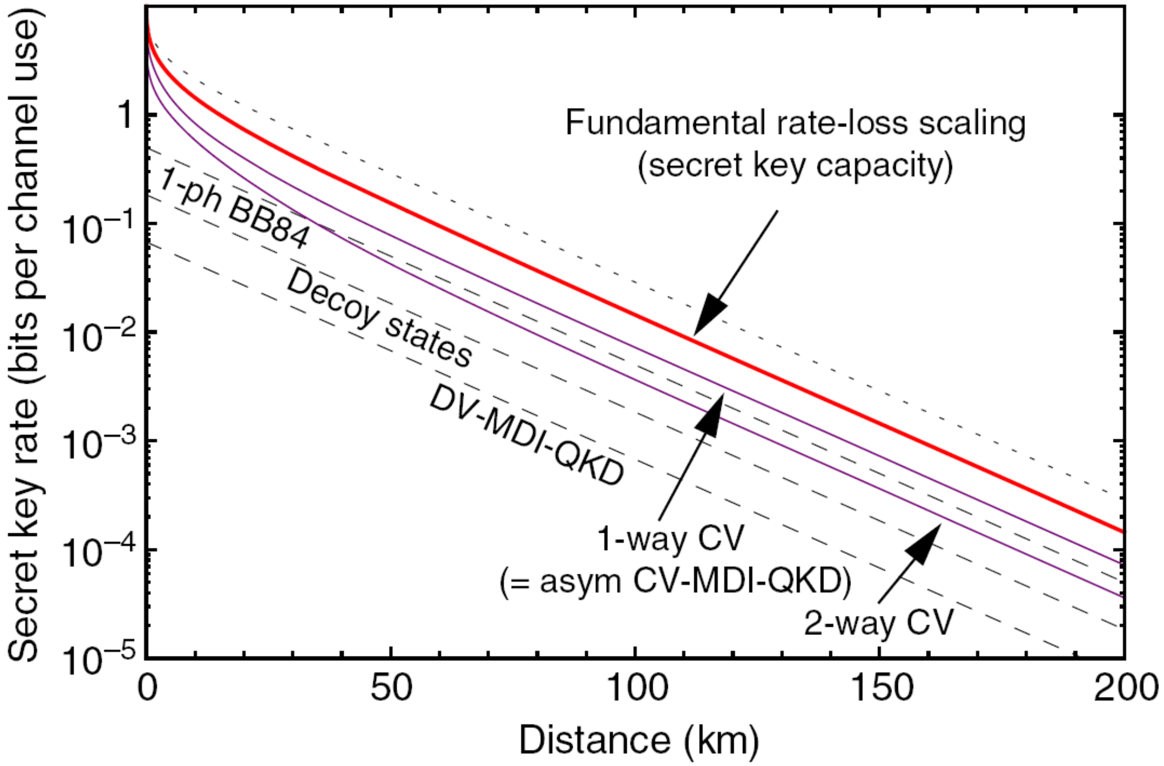
$|\pm\alpha\rangle, |\pm i\alpha\rangle$

Decoy state method

Lo, Ma and Chen, PRL 94, 230504 (2005)

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

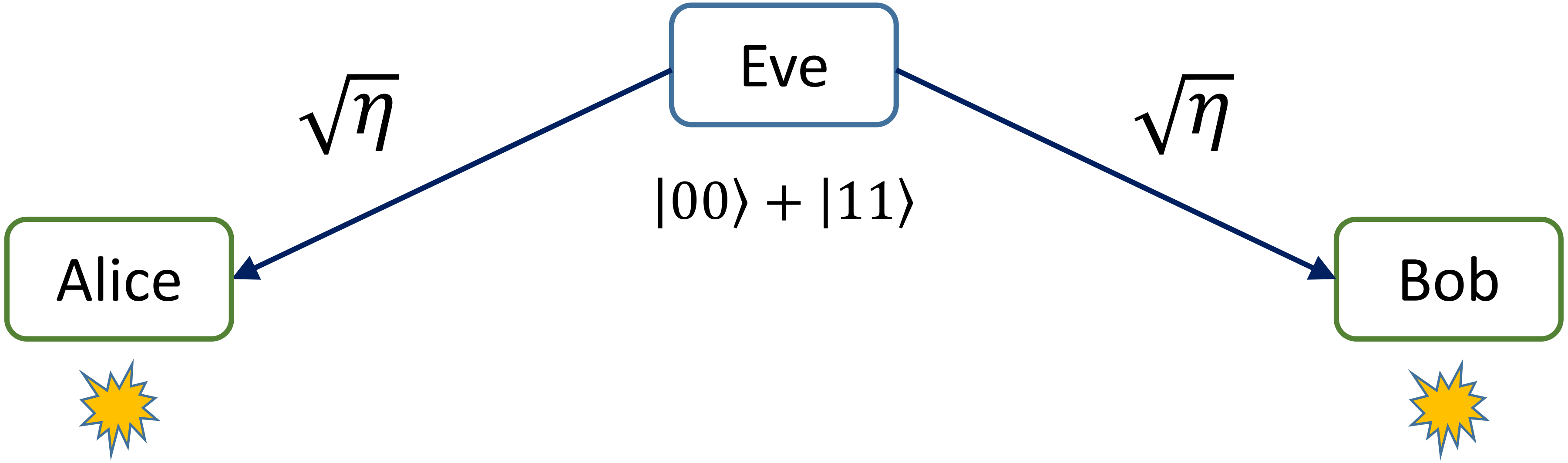
- Secret key capacity (SKC) bound
  - For all point-to-point QKD models
    $R \leq -\log_2(1-\eta)$
- Protocols beyond SKC model?
  - Alice and Bob
    both are sources/detectors



Takeoka, Guha and Wilde, Nat. Comm. 5, 5235 (2014)
Pirandola, Laurenza, Ottaviani, and Banchi, Nat. Comm. 8, 15043 (2017)

$$R = \overline{O(\eta)}?$$

E.g. BBM92 protocol

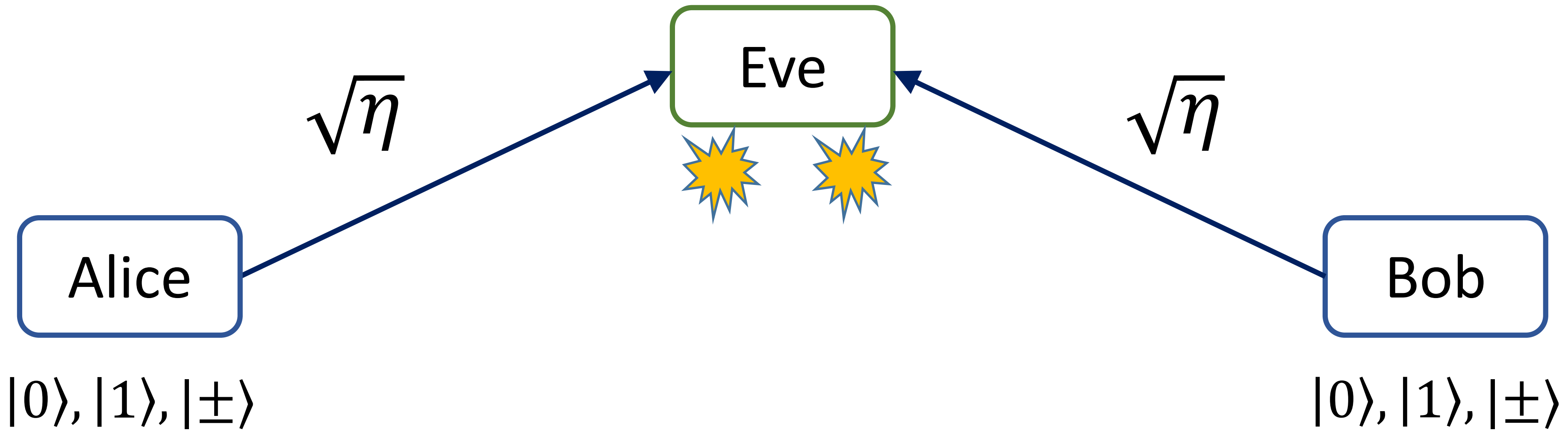


Coincident detection $\Rightarrow$ $R = O\left(\left(\sqrt{\eta}\right)^2\right) = O(\eta)$

Bennett, Brassard, and Mermin, PRL 68, 557 (1992)

$$R = \overline{O(\eta)}?$$

E.g. Polarization encoding MDI-QKD protocol



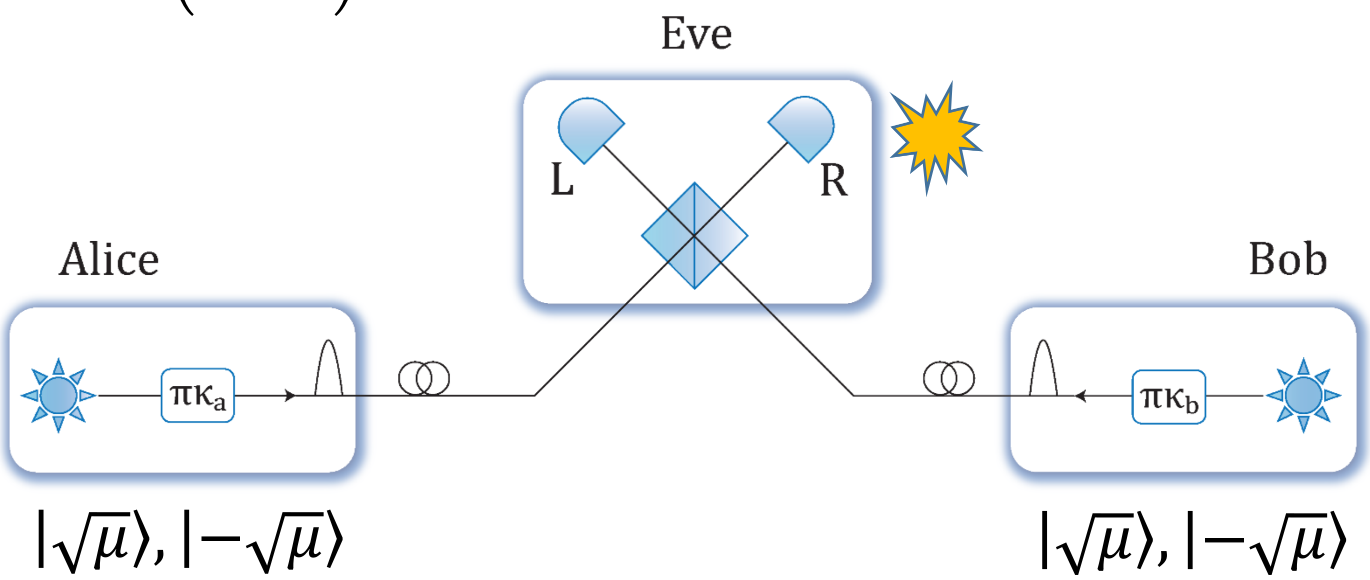
Coincident detection $\Rightarrow$ $R = O\left(\left(\sqrt{\eta}\right)^2\right) = O(\eta)$

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

$R = \overline{O(\eta)}$?

E.g. "MDI-B92" protocol; Phase-matching type protocol

- Unambiguous State Discrimination attack
  - $P_{suc} \sim O(\mu)$
  - $\mu \leq O(\sqrt{\eta}),\ R = O\left(\left(\sqrt{\eta}\right)^2\right) = O(\eta)$

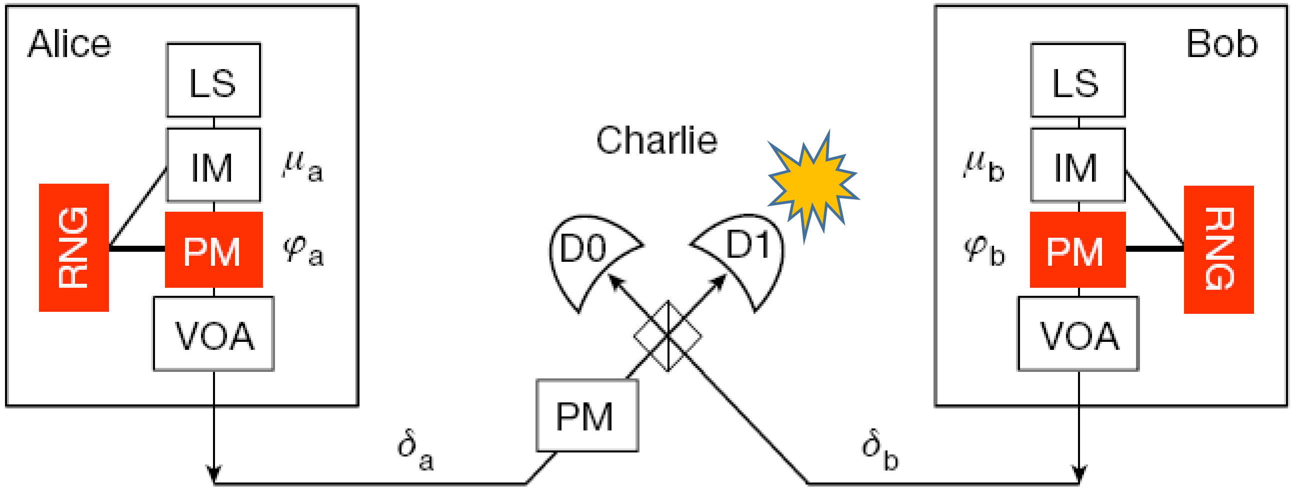


Ferenczi, Ph.D Thesis, Lutkenhaus' group (2013)

$$R > \overline{O(\eta)}!$$

Twin-field QKD

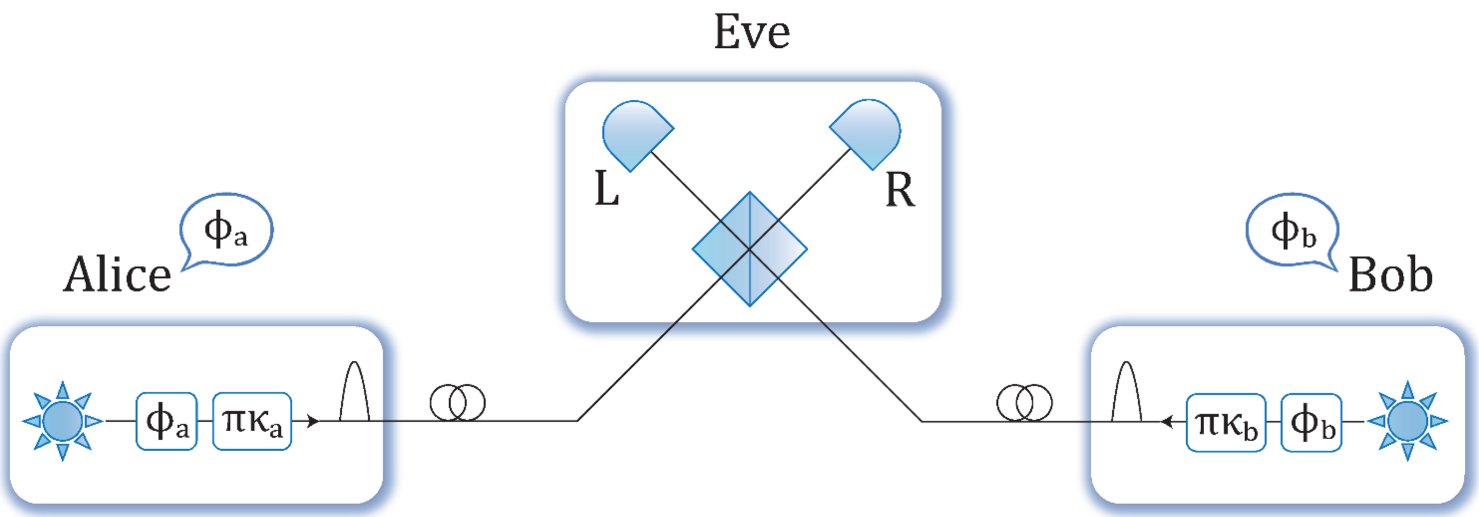
- Point out the potential of $R > O(\eta)$
- BB84 type encoding, $|\pm\alpha\rangle, |\pm i\alpha\rangle$
- Introduce the decoy state method



Lucamarini, Yuan, Dynes and Shields, Nature. 2018, 557(7705):400-403

Protocol & security

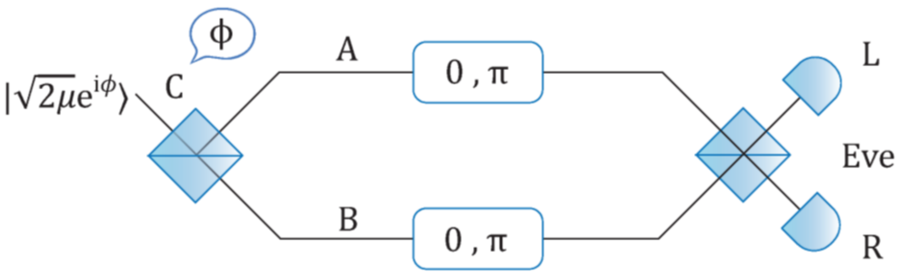
Phase-matching (MDI-)QKD

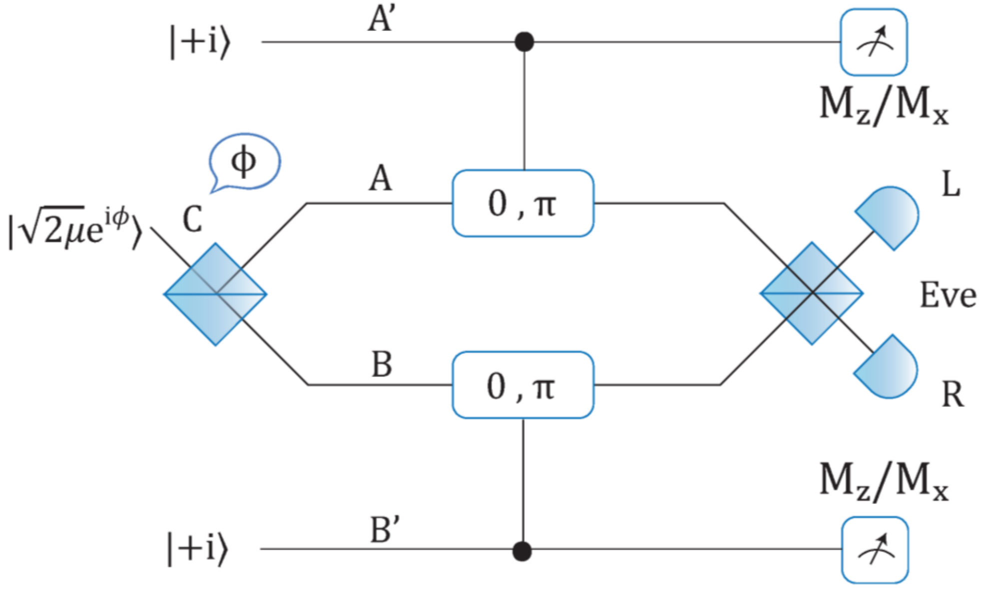


$\left|\sqrt{\mu}e^{i(\phi_a+\pi\kappa_a)}\right\rangle_A$ $\left|\sqrt{\mu}e^{i(\phi_b+\pi\kappa_b)}\right\rangle_B$

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

Random phase PM protocol: Entanglement-based view





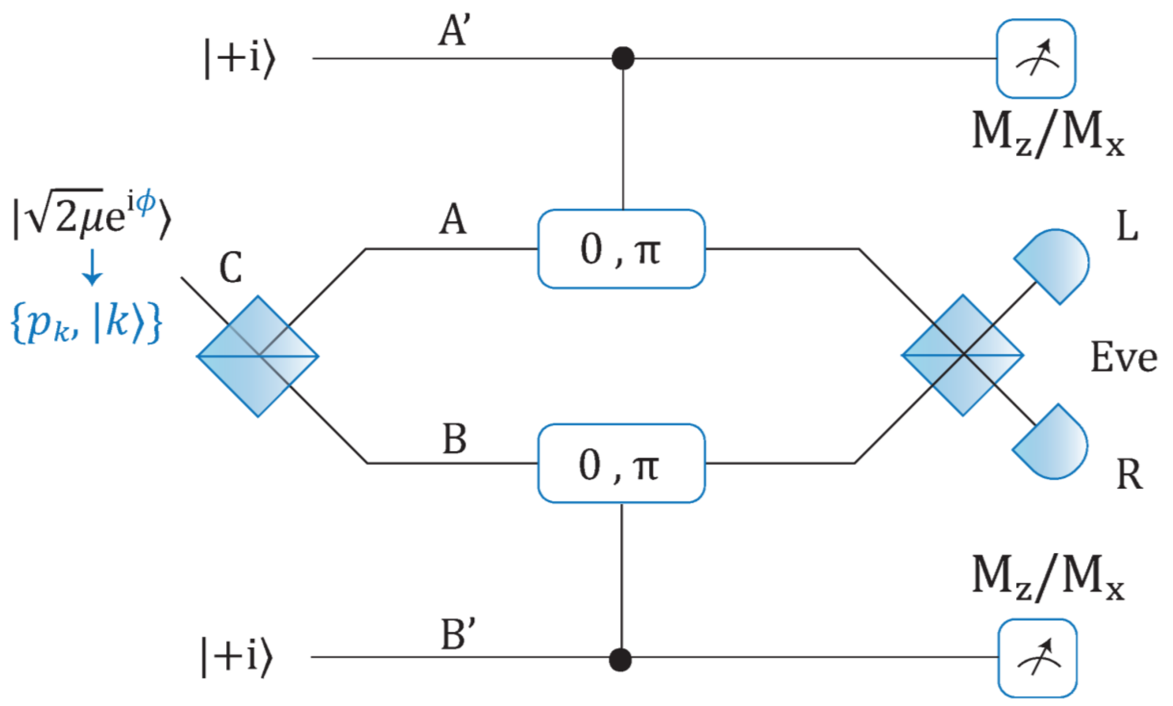
- Consider the post-selected signals with the same phase ϕ
- $K = \left(1 - H(E_\mu^Z) - H(E_\mu^X)\right)$
- Key point: estimate the phase error E_μ^X

Lo and Chau, Science 283, 2050 (1999)
Shor and Preskill, PRL 85, 441 (2000)

Ancillary protocol, decoy state

- For $|k\rangle$ photon number input:
  - $e_k^Z = e_k^X$ if k is odd
  - $e_k^Z = 1 - e_k^X$ if k is even
- Decoy state to estimate $\{e_k^Z, Y_k^Z\}$
- Estimate the overall phase error rate

$$E_\mu^X = \sum_k q_k e_k^X$$



Key rate and parameter estimation

- $K = Q_\mu\left(1 - H\left(E_\mu^Z\right) - H\left(E_\mu^X\right)\right)$
  - $Q_\mu = O(\sqrt{\eta})$
- $E_\mu^X \le q_0 e_0 + q_1 e_1^Z + q_3 e_3^Z + (1 - q_0 - q_1 - q_3)$
  - E_μ^X -- overall phase error rate;

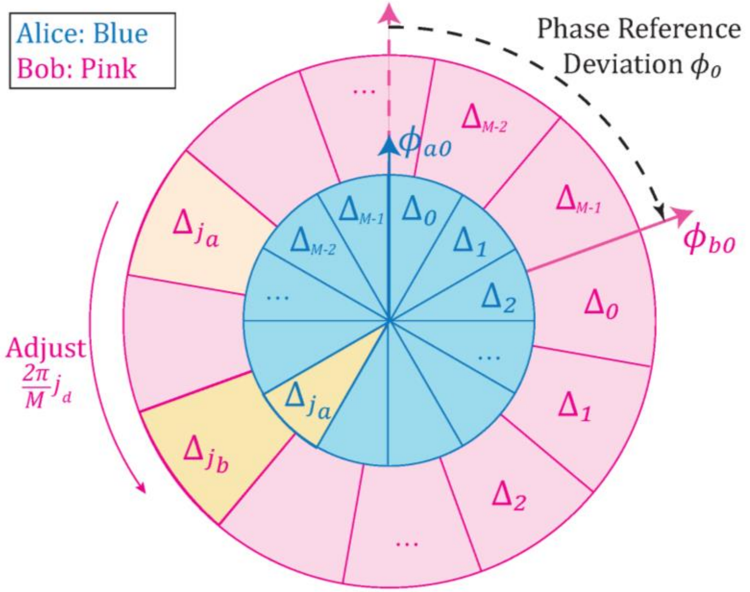
- $Q_\mu = \sum_k p_k Y_k$
- $E_\mu^Z = \sum_k q_k e_k^Z$
- $E_\mu^X = \sum_k q_k e_k^X$

- Phase announcement is critical, not commute with photon number measurement
- Photon number channel model invalid: collective BS attack
- Core observation: overall phase error rate is the same

Practical issues & simulation

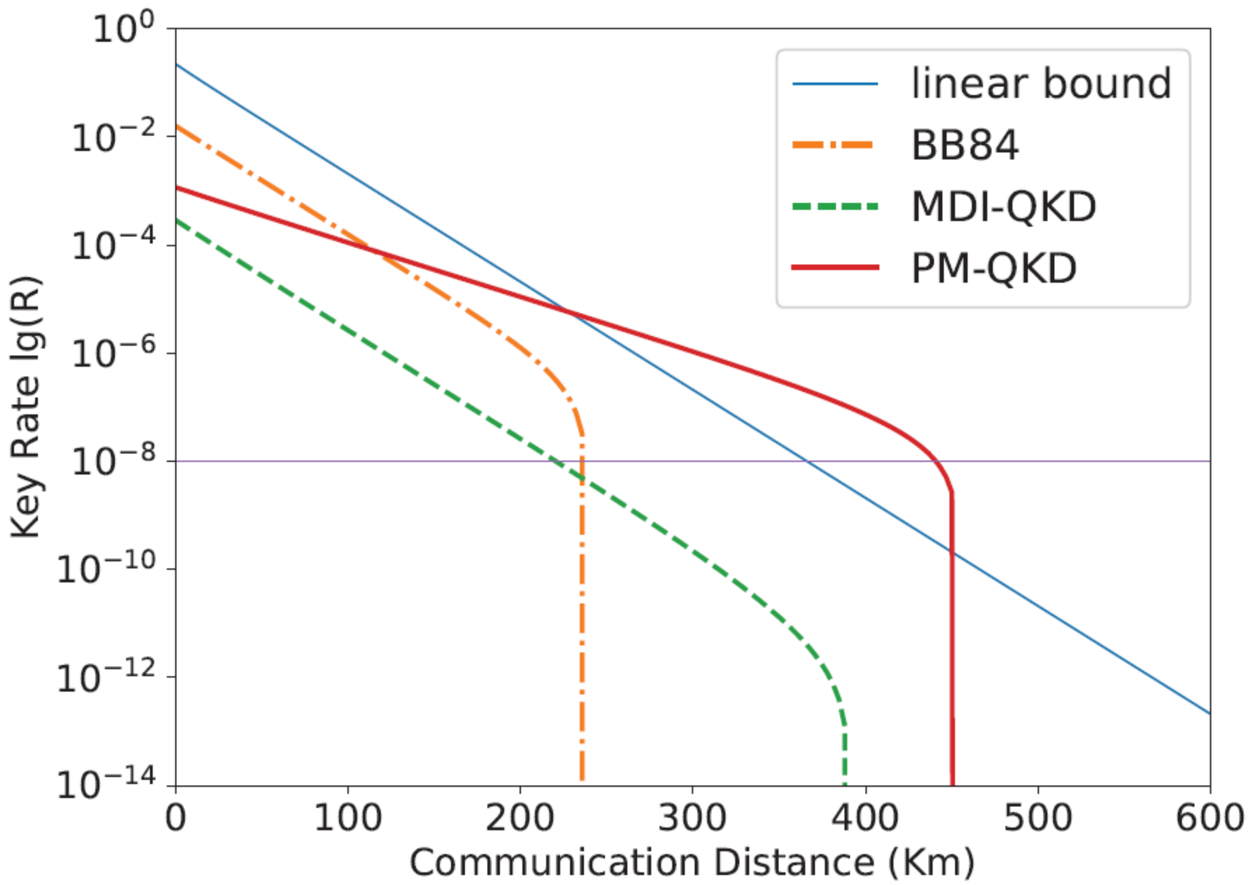
Practical issues

- Infinitesimal post-selection condition
  - Introduce phase slices
  - No effect on the security, just introduce intrinsic errors
- Continuous phase randomization: hard
  - Discrete phase randomization is enough
- Phase locking requirement
  - Alice and Bob can estimate the phase reference deviation of each round
  - Post-selection(Sifting) based on estimated phase difference; no feedback
  - Only requirement: the phase cannot fluctuate too quickly



Performance of PM protocol

- Consider all the practical factor:
  - Dark count: $8 * 10^{-8}$
  - Detection efficiency: 14.5%
  - Sifting factor: 1/8
  - Misalignment: $\sim 1.5\%$
  - Error correction efficiency: 1.15
- $K = \frac{2}{M} Q_\mu \left(1 - fH\left(E_\mu^Z\right) - H\left(E_\mu^X\right)\right)$
- Break the linear bound!



Ma, Zeng and Zhou, PRX.8.031043,(2018)

Summary & outlook

Summary

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

Outlook

$$R = \overline{O\left(\sqrt{\eta}\right)}?$$

Thanks!

清華大學 量子信息中心
Tsinghua University Center for Quantum Information

- Xiongfeng Ma: xma@tsinghua.edu.cn
- Pei Zeng: qubitpei@gmail.com
- Hongyi Zhou: zhouhy14@mails.tsinghua.edu.cn

Xiongfeng Group,
Center for Quantum Information,
Tsinghua University