Fully Passive Twin-Field Quantum Key Distribution

Wenyuan Wang[1,*], Rong Wang[1], Hoi-Kwong Lo[1,2,3,4,5,†]

arXiv preprint: 2304.12062

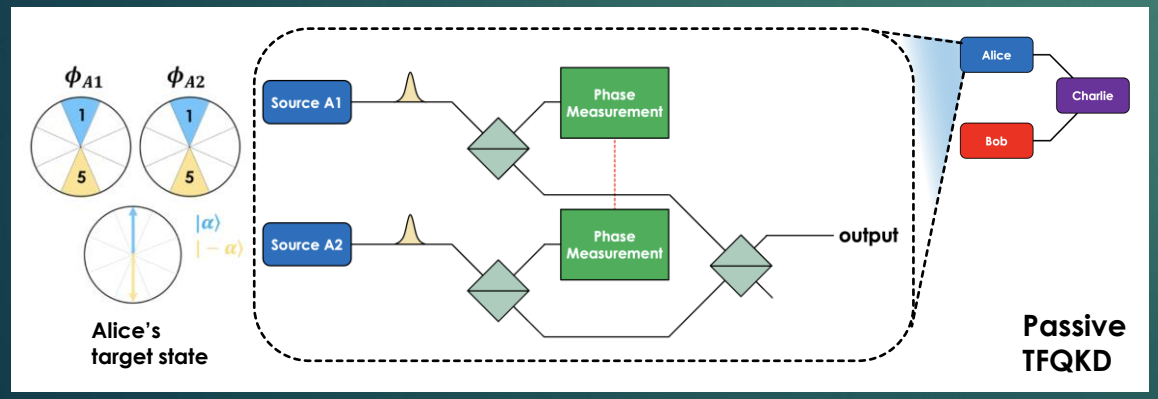
Passive Continuous-Variable Quantum Key Distribution

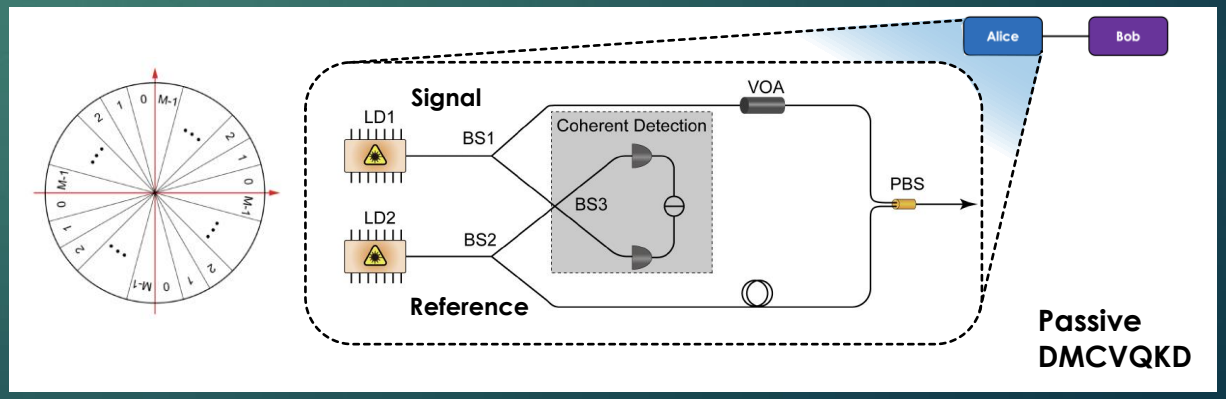
Chenyang Li[1,3,**], Chengqiu Hu[1,‡], Wenyuan Wang[1], Rong Wang[1], Hoi-Kwong Lo[1,2,3,4,5]

arXiv preprint: 2212.01876

[1] Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong
[2] Dept. of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada
[3] Dept. of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario, M5S 1A7, Canada
[4] Centre for Quantum Information and Quantum Control (CQIQC), Toronto, Ontario, M5S 1A7, Canada
[5] Quantum Bridge Technologies, Inc., 100 College Street, Toronto, Ontario, M5S 3G4, Canada

*** wenyuanw@hku.hk** **† hklo@ece.utoronto.ca**
**** licheny@hku.hk** **‡ The author contributes equally as the first author**





Outline

1. Background
    - Motivation for passive QKD
    - Fully Passive BB84
2. Fully Passive Twin-Field (TF) QKD
    - System setup
    - Protocol definition: passively preparing signal and decoy states
        - Security analysis: addressing imperfect source preparation
        - Post-processing strategy: enhancing sifting efficiency
    - Simulation results
    - Discussions: advantages and challenges
3. Passive Discrete Modulated (DM) Continuous-Variable (CV) QKD
    - System setup
    - Protocol definition: phase remapping scheme
    - Source characterization and noise analysis
    - Simulation results

Motivation

Active modulation devices (such as intensity or polarization modulator) might introduce side-channels [1,2] such as intensity correlations, and might be susceptible to hacking attempts like Trojan-horse attacks [3,4].

It would be preferable if we can use only post-selection to obtain the states we'd like to prepare (e.g. decoy intensities, or even the polarization or phase that encodes the key) without using any active modulators.

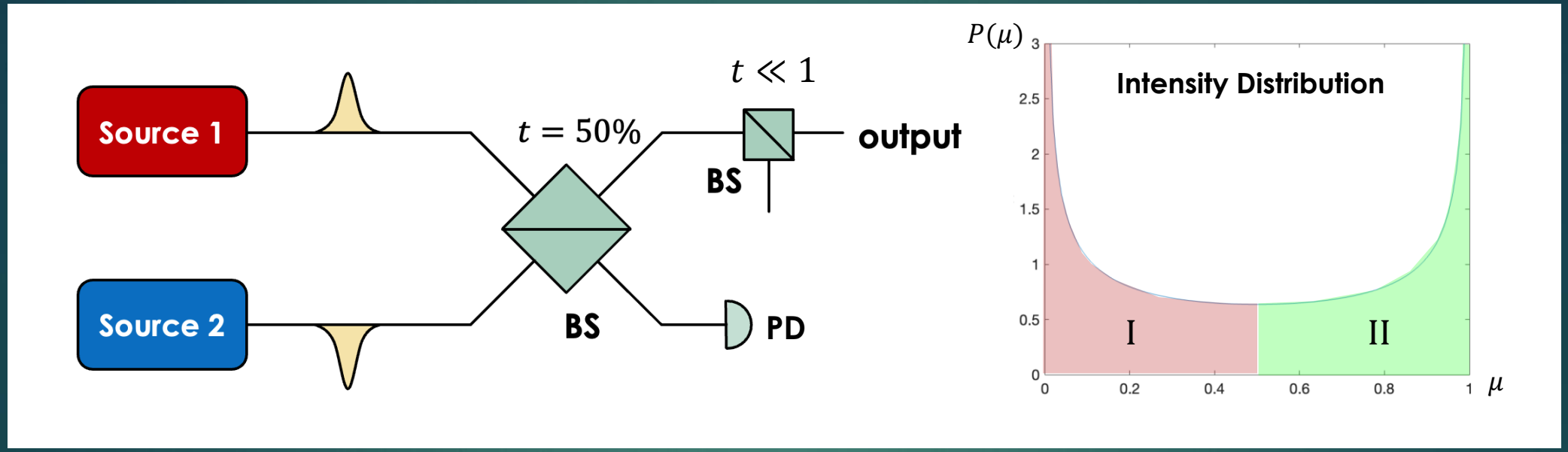
[1] K Yoshino, et al. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses." npj Quantum Information 4.1 (2018): 1-8.

[2] JE Bourassa, A Ganapandithan, L Qian, HK Lo. "Measurement device-independent quantum key distribution with passive, time-dependent source side-channels." arXiv preprint arXiv:2108.08698 (2021).

[3] N Gisin, S Fasel, B Kraus, H Zbinden, G Ribordy, "Trojan-horse attacks on quantum-key-distribution systems." Physical Review A 73.2 (2006): 022320.

[4] K Tamaki, M Curty, and M Lucamarini. "Decoy-state quantum key distribution with a leaky source." New Journal of Physics 18.6 (2016): 065008.

Passive Decoy-State [1,2]



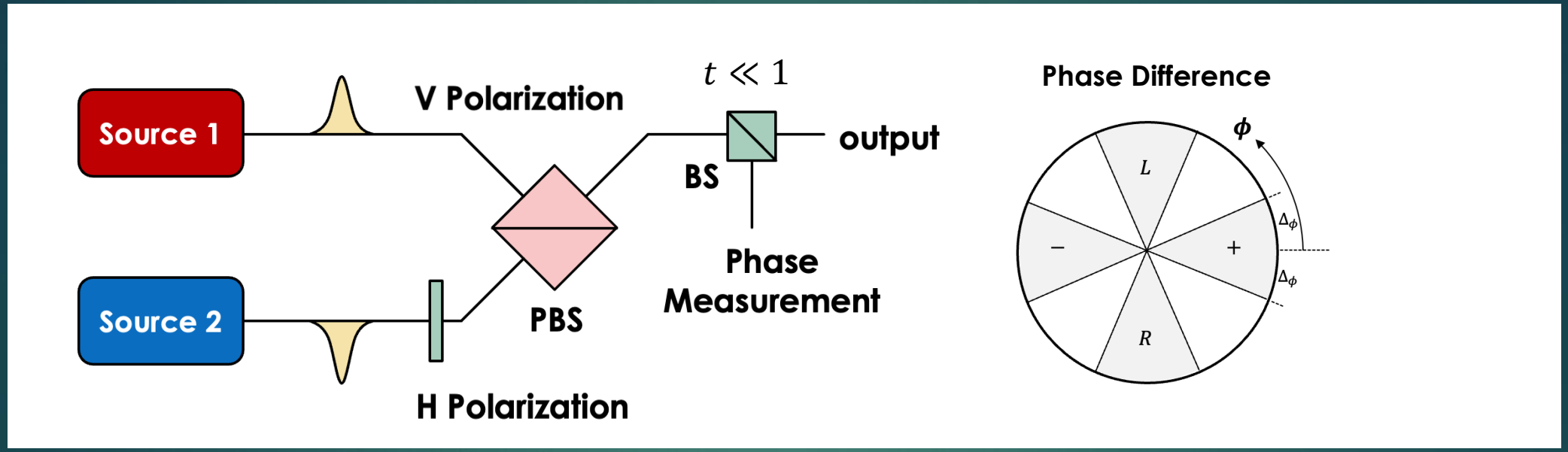
Key idea: interfering two phase-randomized coherent lights, results in correlated output at two ports.

One can observe and post-select based on one output port (with a classical or single-photon detector) to conditionally determine the other port's output state.

[1] M Curty, T Moroder, X Ma, N Lutkenhaus, "Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution" Optics Letters 34.20 (2009): 3238-3240.

[2] M Curty, X Ma, B Qi, T Moroder, "Passive decoy-state quantum key distribution with practical light sources" , Physical Review A 81 (2010): 022310.

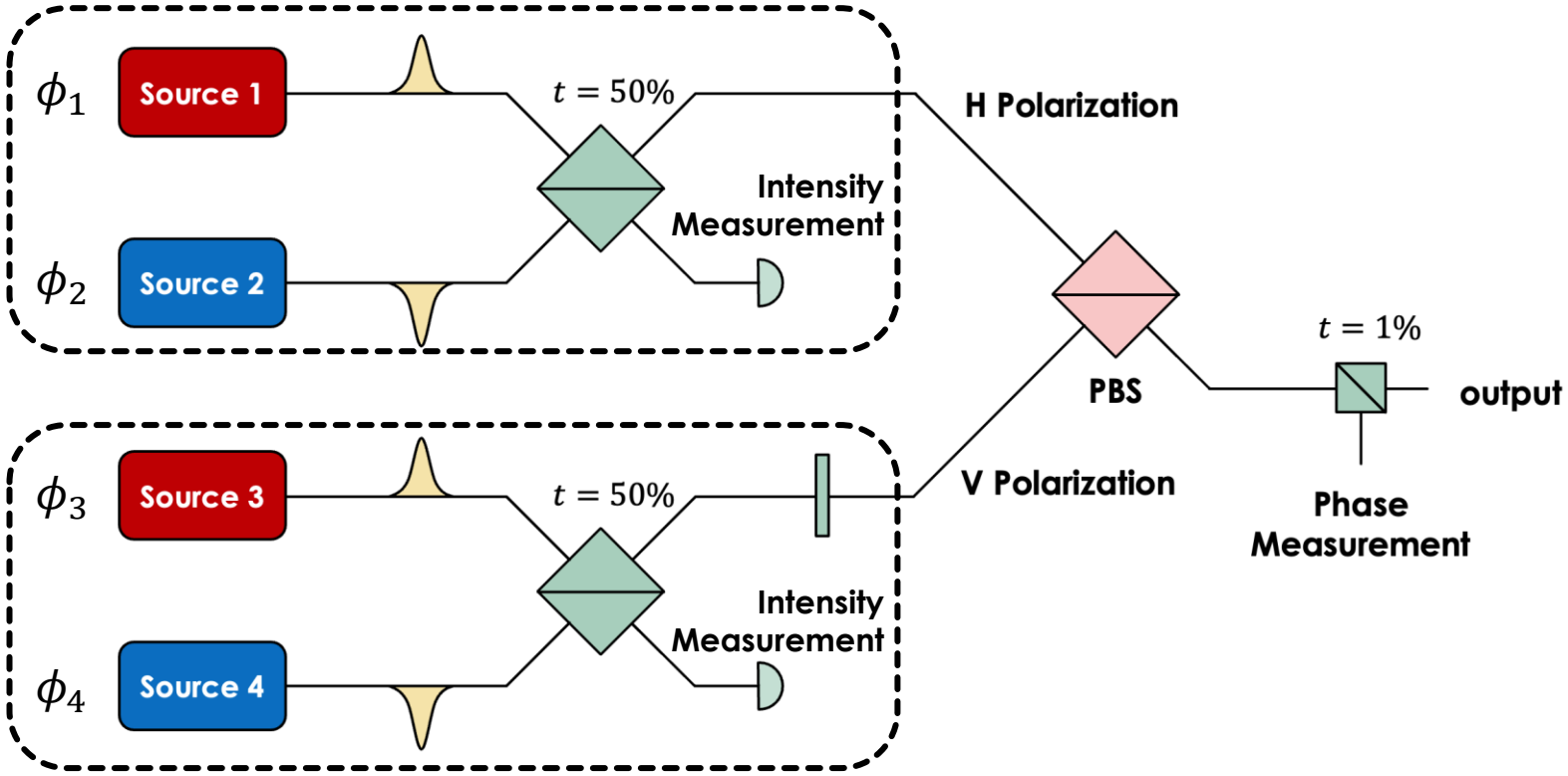
Passive-Encoding BB84 [1]

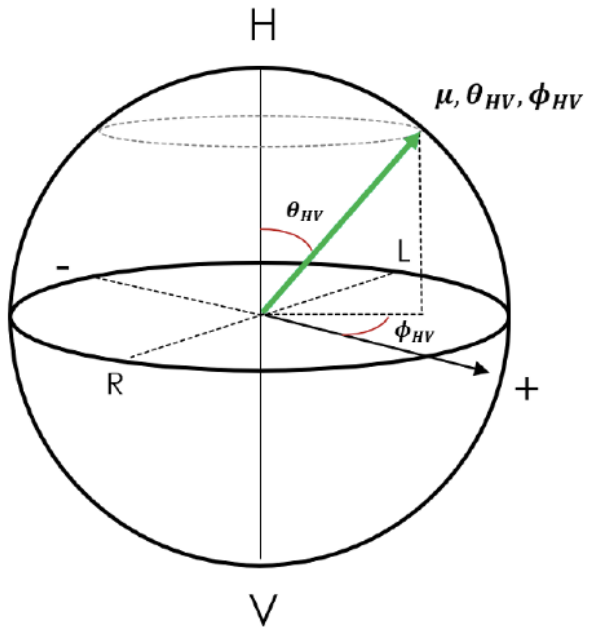


If we replace the beamsplitter with a polarizing beamsplitter and prepare the signals respectively with H and V polarizations, instead of random intensities, we can create random polarization states $(|H\rangle + e^{i\phi}|V\rangle)/\sqrt{2}$ on the equator of Bloch sphere.

[1] M Curty, X Ma, HK Lo, N Lutkenhaus, "Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals." Physical Review A 82.5 (2010): 052325.

Fully Passive BB84





Output: Phase-randomized coherent state with arbitrary polarization on Bloch sphere and arbitrary intensity.

Alice observes and post-selects her local observables $(\mu_H, \mu_V, \phi_{HV})$ to prepare e.g. decoy-state BB84 states.

Fully Passive BB84

Theory:

W Wang, R Wang, C Hu, V Zapatero, L Qian, B Qi, M Curty, HK Lo, "**Fully-Passive Quantum Key Distribution**" Physical Review Letters 130.22 (2023): 220801.

Experimental Demonstration:

C Hu, W Wang, KS Chan, Z Yuan, HK Lo "**Proof-of-Principle Demonstration of Fully-Passive Quantum Key Distribution**", arXiv:2304.10374 (2023).

Concurrent Theory and Experimental Works:

V Zapatero, W Wang, M Curty, "**A Fully Passive Transmitter for Decoy-State Quantum Key Distribution**", Quantum Sci. Technol. 8, 025014 (2023).

FY Lu, ZH Wang, JL Chen, S Wang, ZQ Yin, DY He, R Wang, W Chen, GJ Fan-Yuan, GC Guo, ZF Han, "**Experimental Demonstration of Fully Passive Quantum Key Distribution**", arXiv: 2304.11655 (2023). Accepted by Physical Review Letters.

Fully Passive Twin Field QKD

Motivation

It would be ideal if we can combine passive sources with measurement-device-independent (MDI)-type QKD protocols, to eliminate side-channels from both source modulators and detectors, enabling much better implementation security.

- One approach is combining our passive polarization-encoding source directly with MDI-QKD (however, a major challenge is the sifting efficiency).

- Another different approach is to use phase-encoding and implement twin-field (TF) QKD [1] (which gives us MDI properties, as well as the bonus of better rate-distance tradeoff).

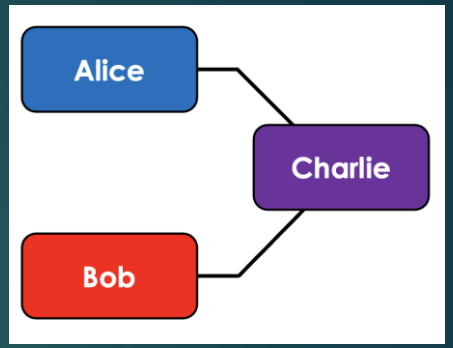
Here we introduce a simple yet effective setup to implement fully passive CAL-TFQKD [2]. Furthermore, we introduce a set of post-processing strategy to greatly improve sifting efficiency.

[1] M Lucamarini, ZL Yuan, JF Dynes, AJ Shields, ``Overcoming the rate–distance limit of quantum key distribution without quantum repeaters." Nature 557.7705:400 (2018).

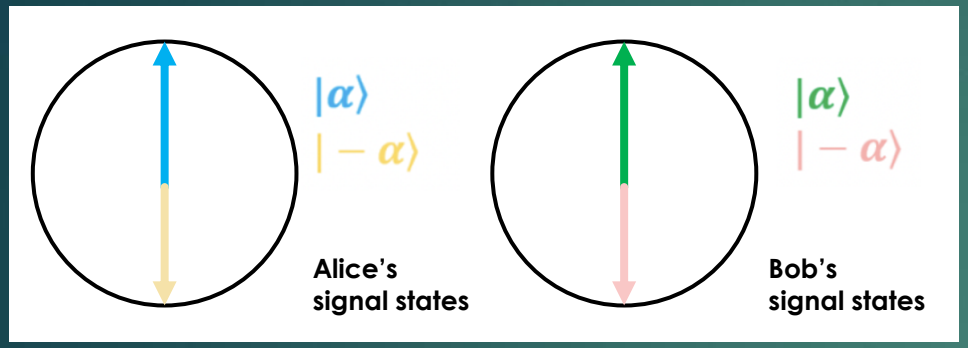
[2] M Curty, K Azuma, HK Lo, ``Simple security proof of twin-field type quantum key distribution protocol." npj Quantum Information 5.1 (2019): 1-6.

CAL-TFQKD Protocol [1]

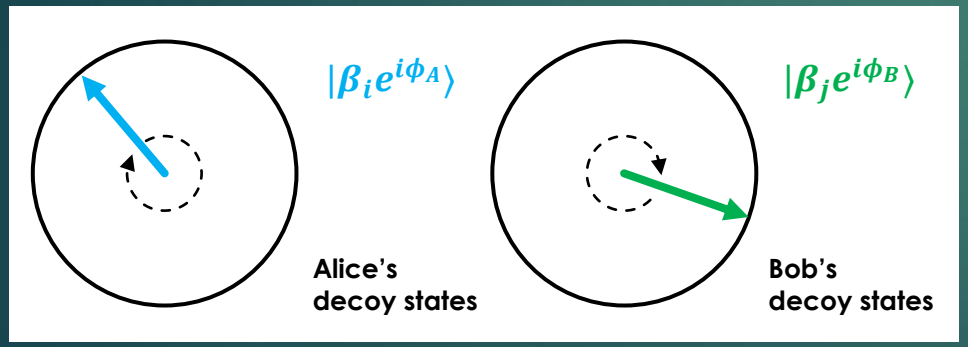
- Basis choice: Alice and Bob each randomly selects the coding X or testing Z basis to prepare corresponding states (which are eventually matched during sifting).



- Coding (signal) X basis: Alice and Bob each prepares and sends coherent states $|\alpha\rangle$ or $|-\alpha\rangle$.

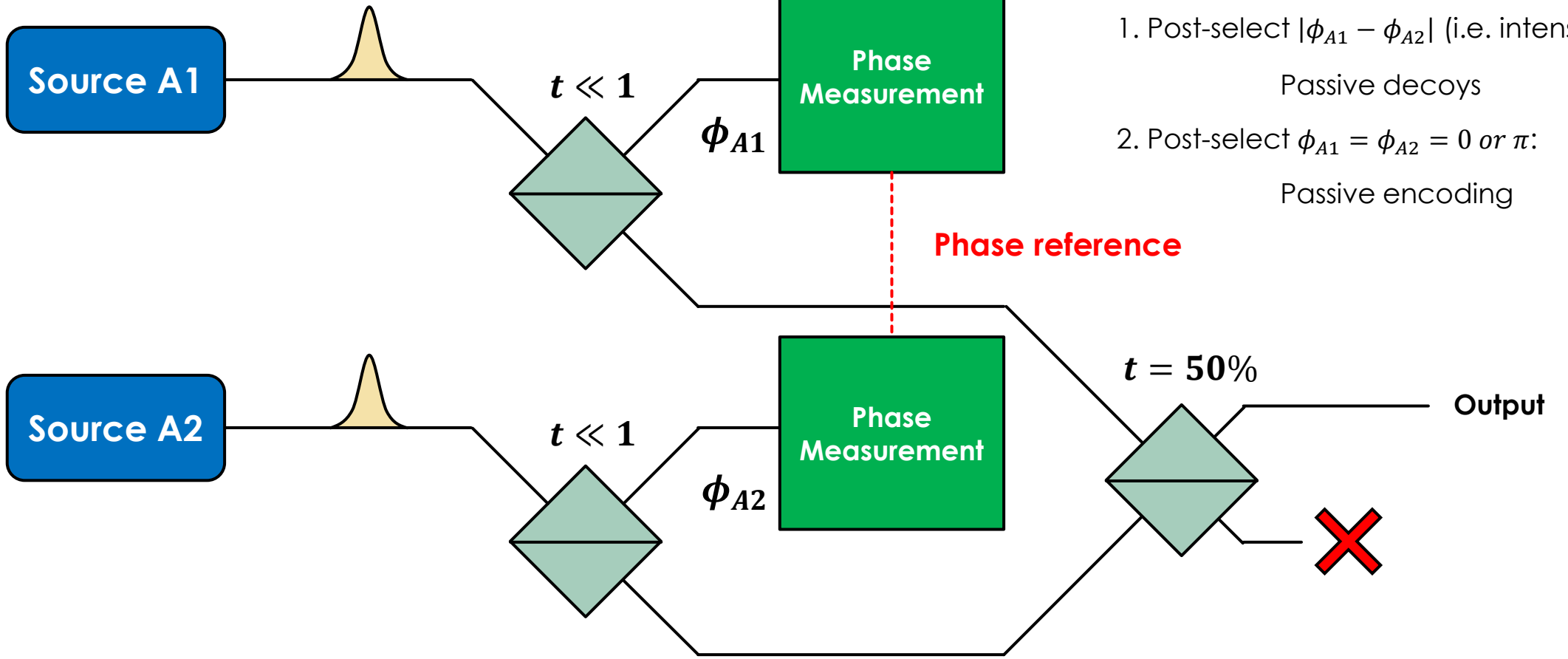


- Testing (decoy) Z basis: Alice and Bob each prepares phase-randomized coherent states with intensities β_i chosen from $\{\mu, \nu, \omega\}$.



[1] M Curty, K Azuma, HK Lo, ``Simple security proof of twin-field type quantum key distribution protocol.'' npj Quantum Information 5.1 (2019): 1-6.

Passive TFQKD Source: Alice



Intuition:

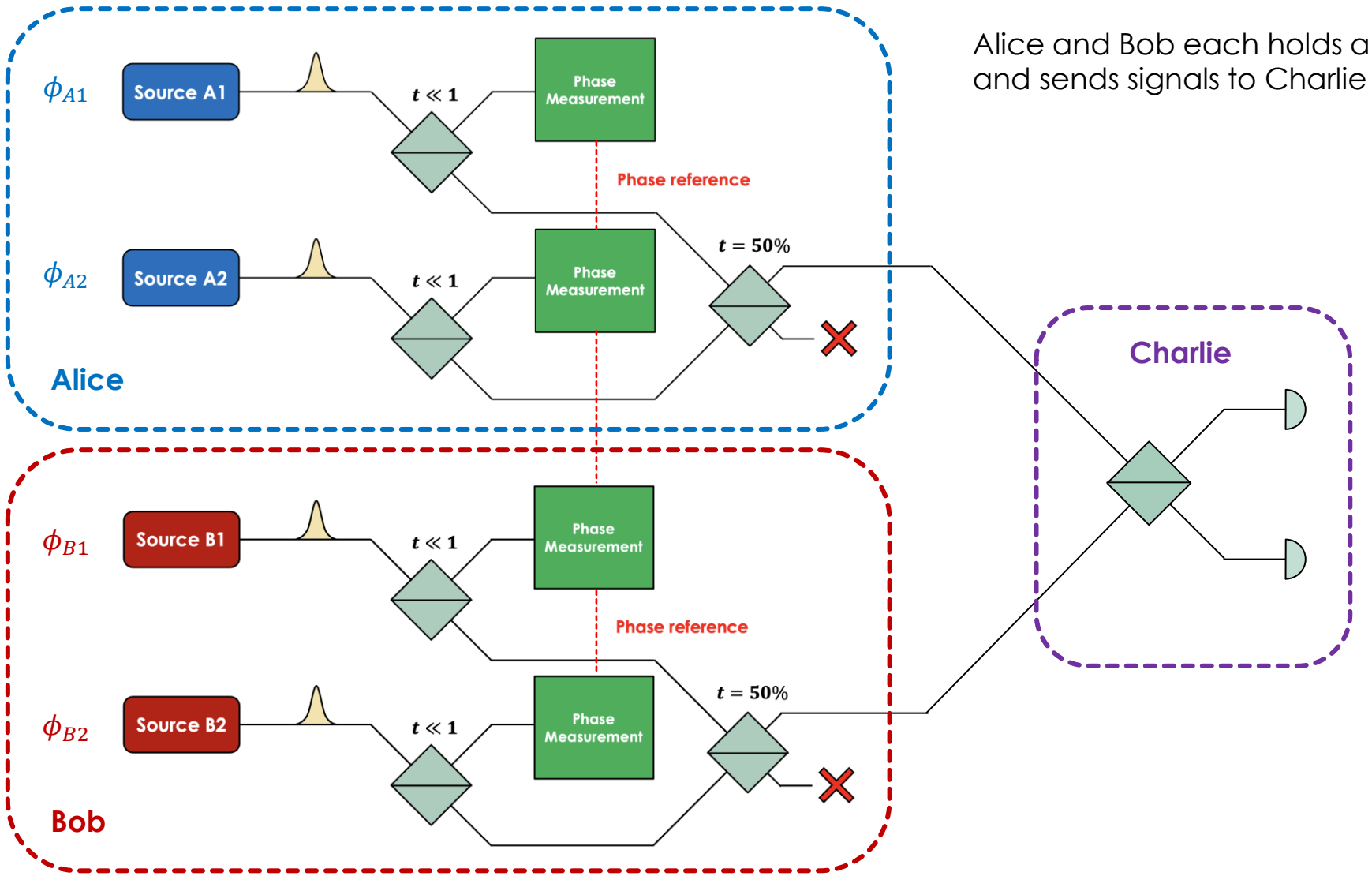
1. Post-select $|\phi_{A1} - \phi_{A2}|$ (i.e. intensity):

   Passive decoys

2. Post-select $\phi_{A1} = \phi_{A2} = 0 \; or \; \pi$:

   Passive encoding

Passive TFQKD Source: Full Setup

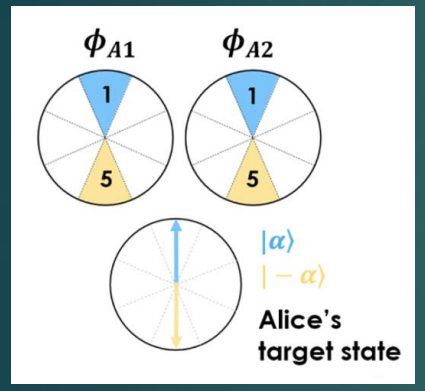


Alice and Bob each holds a fully passive source and sends signals to Charlie for interference

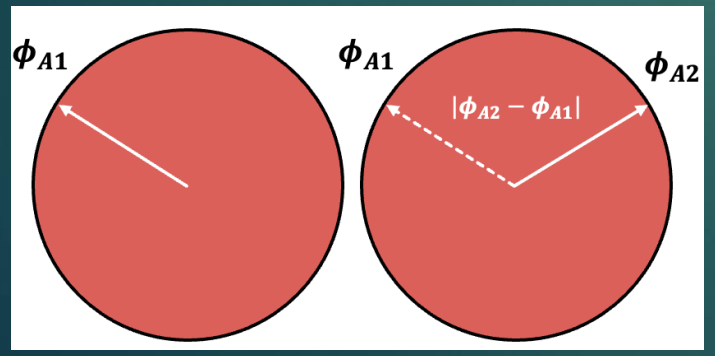
Passive TF-QKD Protocol (Alice as an example)

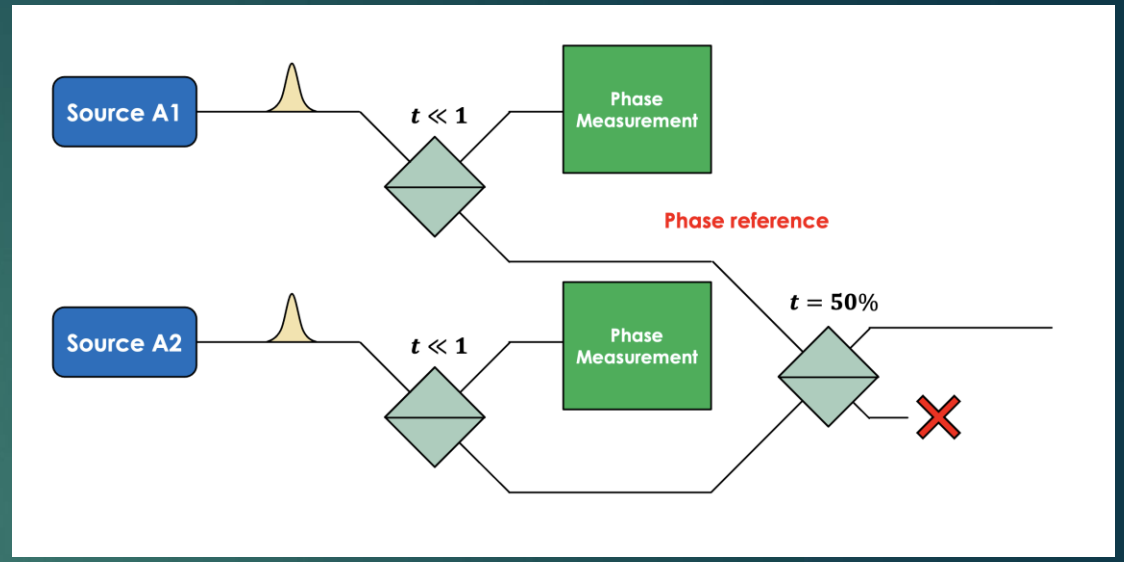
- Basis choice: Alice randomly declares an event is in X or Z basis during post-processing and announces it to Bob.

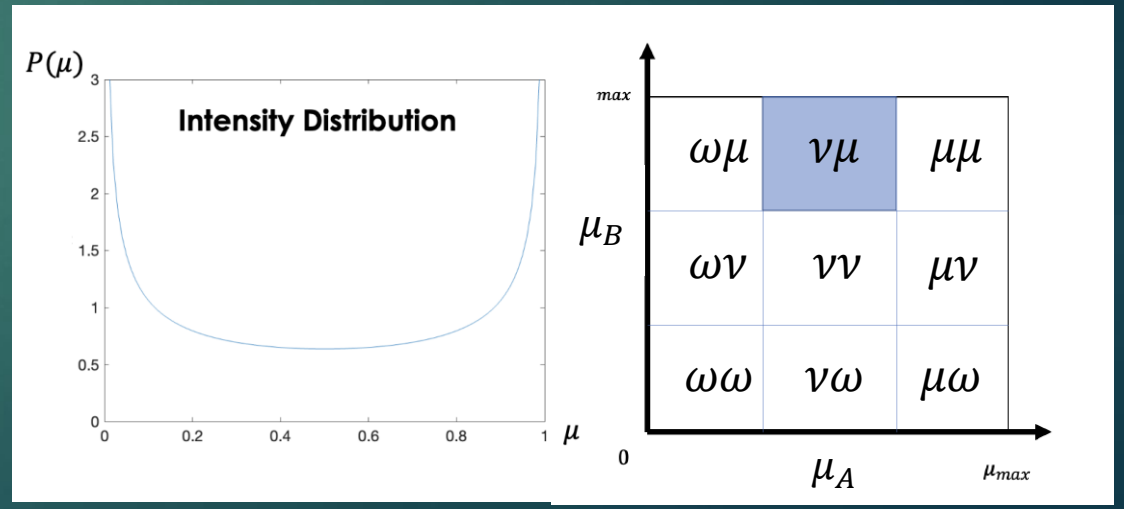
- Coding (signal) X basis: Alice observes the absolute positions of the phase slices that ϕ_{A1} and ϕ_{A2} are in and keeps only cases where ϕ_{A1} and ϕ_{A2} are in the same slice corresponding to 0 or π.



- Test (decoy) Z basis: Alice post-selects phase difference $|\phi_{A1} - \phi_{A2}|$ (equivalent to post-selecting the intensity of a phase randomized state).

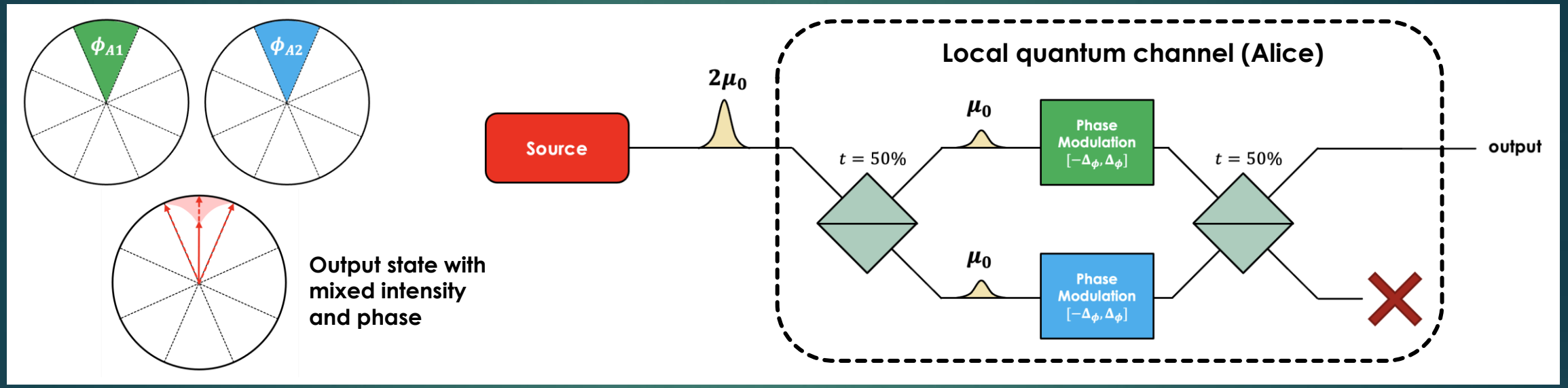






Caveat 1: Security Analysis

Due to the finite size of the phase slices (e.g. for A1 and A2 at Alice's site), the output signals have mixed intensity and phase.

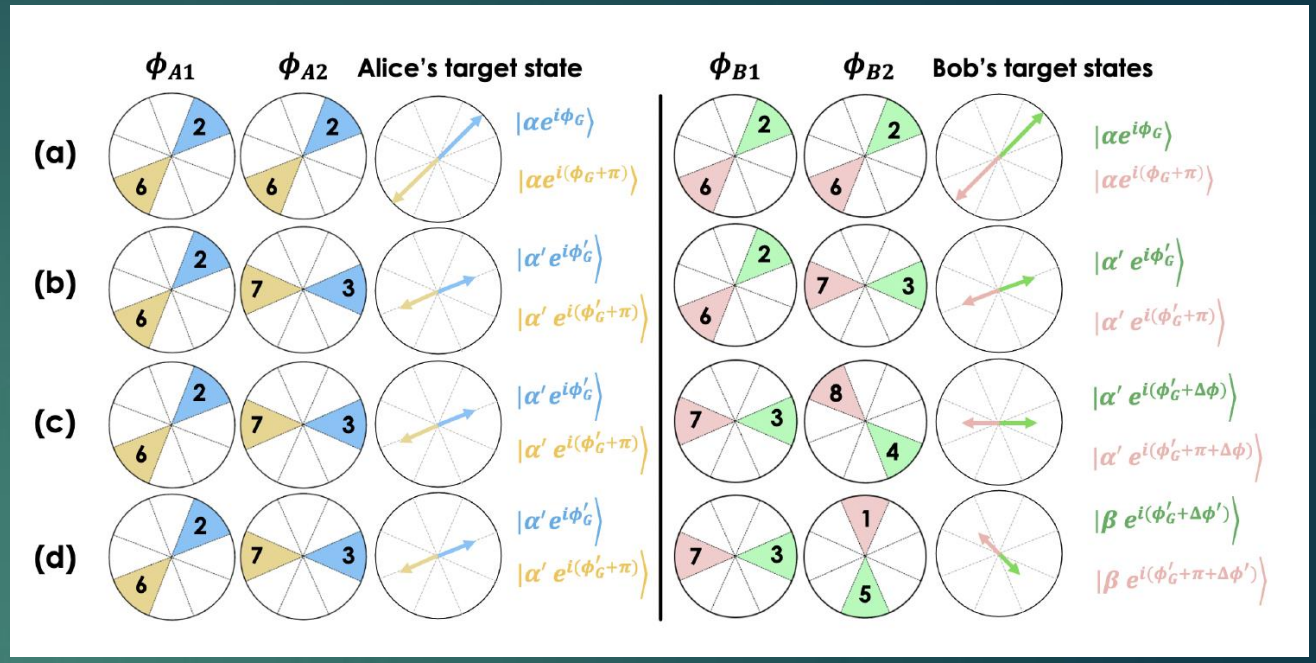


We can equivalently think of this as signals from a "perfect source" passing through a local quantum channel (Alice and Bob each holds one) before exiting into the external physical channel.

The security is not worse if we yield the local channels to Eve, i.e. count them as external loss/error.

Caveat 2: Sifting Efficiency in Coding Basis

$$R = \frac{1}{N^4} \sum_{k_{A1}=1}^{N} \sum_{k_{A2}=1}^{N} \sum_{k_{B1}=1}^{N} \sum_{k_{B2}=1}^{N} [\max(0, R_{0,1}(k_{A1}, k_{A2}, k_{B1}, k_{B2})) + \max(0, R_{1,0}(k_{A1}, k_{A2}, k_{B1}, k_{B2}))]$$

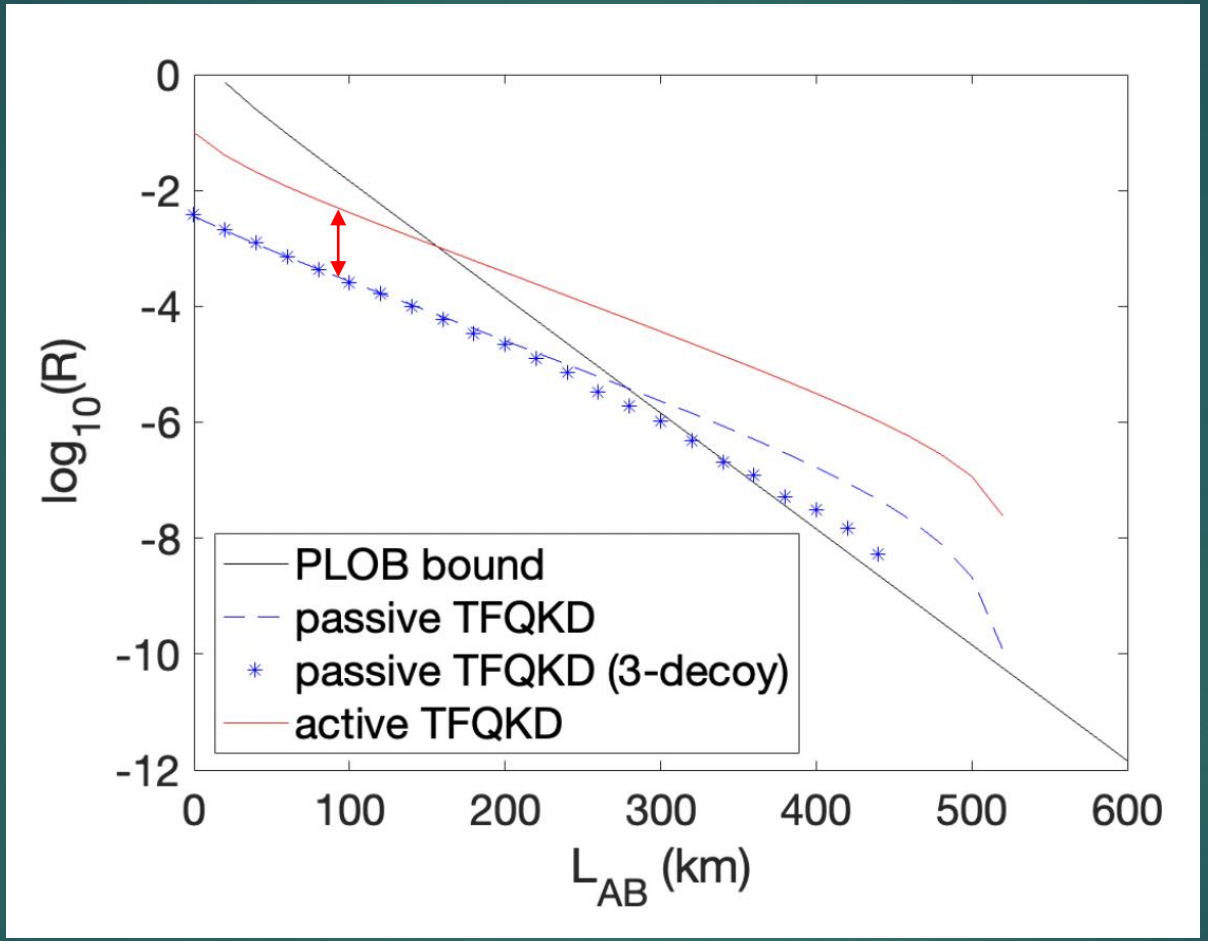


Overall, any combination of A1, A2, B1, B2 slices can be used to attempt key generation (we can simply keep the combinations with nonzero key rate).

Subdividing slices never decreases key rate since we utilize information from all combinations. Therefore, the slice number is only limited by detector resolution, at least in the asymptotic scenario.

Simulation Results

Infinite data size, infinite decoys vs 3 decoys, $e_d = 0, p_d = 10^{-8}$



Thanks for the efficient post-processing strategy, passive TF-QKD only has about 1.2 orders-of-magnitude lower key rate compared to the active case. It can still beat the PLOB bound [1] under the practical 3-decoy scenario.

[1] S Pirandola, R Laurenza, C Ottaviani, L Banchi, "Fundamental limits of repeaterless quantum communications." Nature communications 8:15043 (2017).

Discussions

Our Fully passive TF-QKD protocol allows for much better implementation security (removing side-channels in both source modulators and detectors) while maintaining good key rate.

Our proposed setup also has some additional advantages:

- No basis sifting is needed.

- Resilience against static phase misalignment, like phase-matching (PM) QKD [1].

- Applicability to other TF-QKD protocols, such as no-phase-postselection (NPP) TFQKD [2] and PM-QKD [1], which have similarly structured signals. It is potentially applicable to sending-or-not-sending (SNS) QKD [3], but the vacuum probability may need more optimization.

There are still some remaining challenges:

- A rigorous finite-size analysis will be the subject of future work.

- Experimental implementation is challenging, particularly in terms of addressing frequency drift.

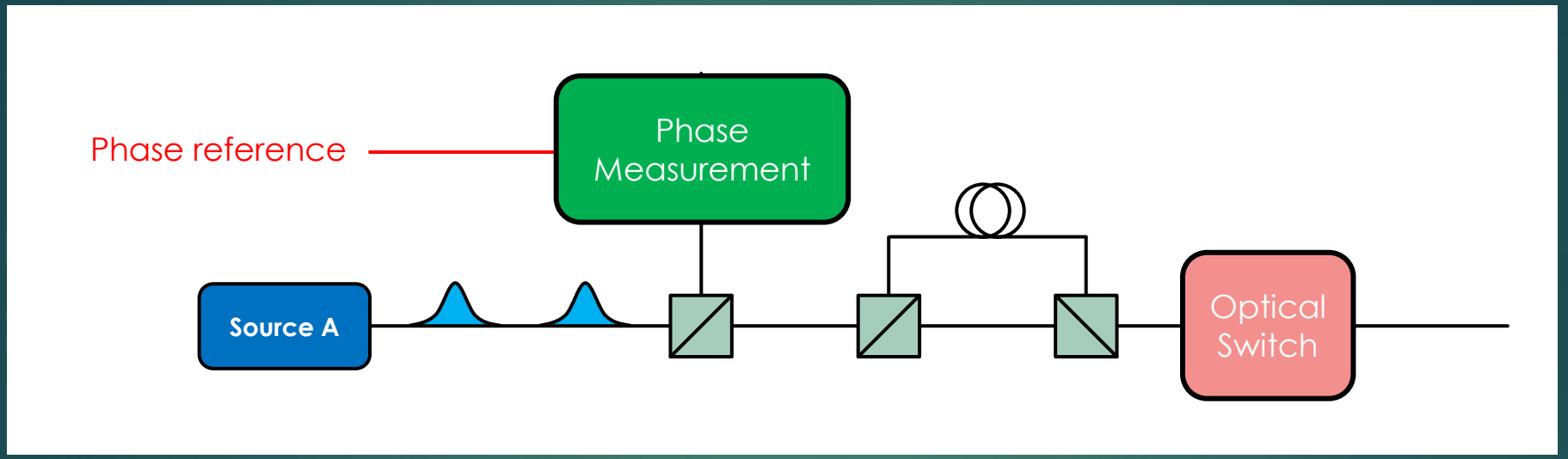
[1] XF Ma, P Zeng, H Zhou, ``Phase-matching quantum key distribution.'' Physical Review X 8.3 (2018): 031043.

[2] C Cui, et al. ``Twin-field quantum key distribution without phase postselection.'' Physical Review Applied 11.3 (2019): 034053.

[3] XB Wang, ZW Yu, XL Hu, ``Twin-field quantum key distribution with large misalignment error.'' Physical Review A 98.6 (2018): 062323.

Compensating Frequency Drift

Frequency drift is a key challenge for implementing passive TF-QKD, since all sources need to have independent phases (e.g. from gain switched lasers) and no phase locking is allowed.



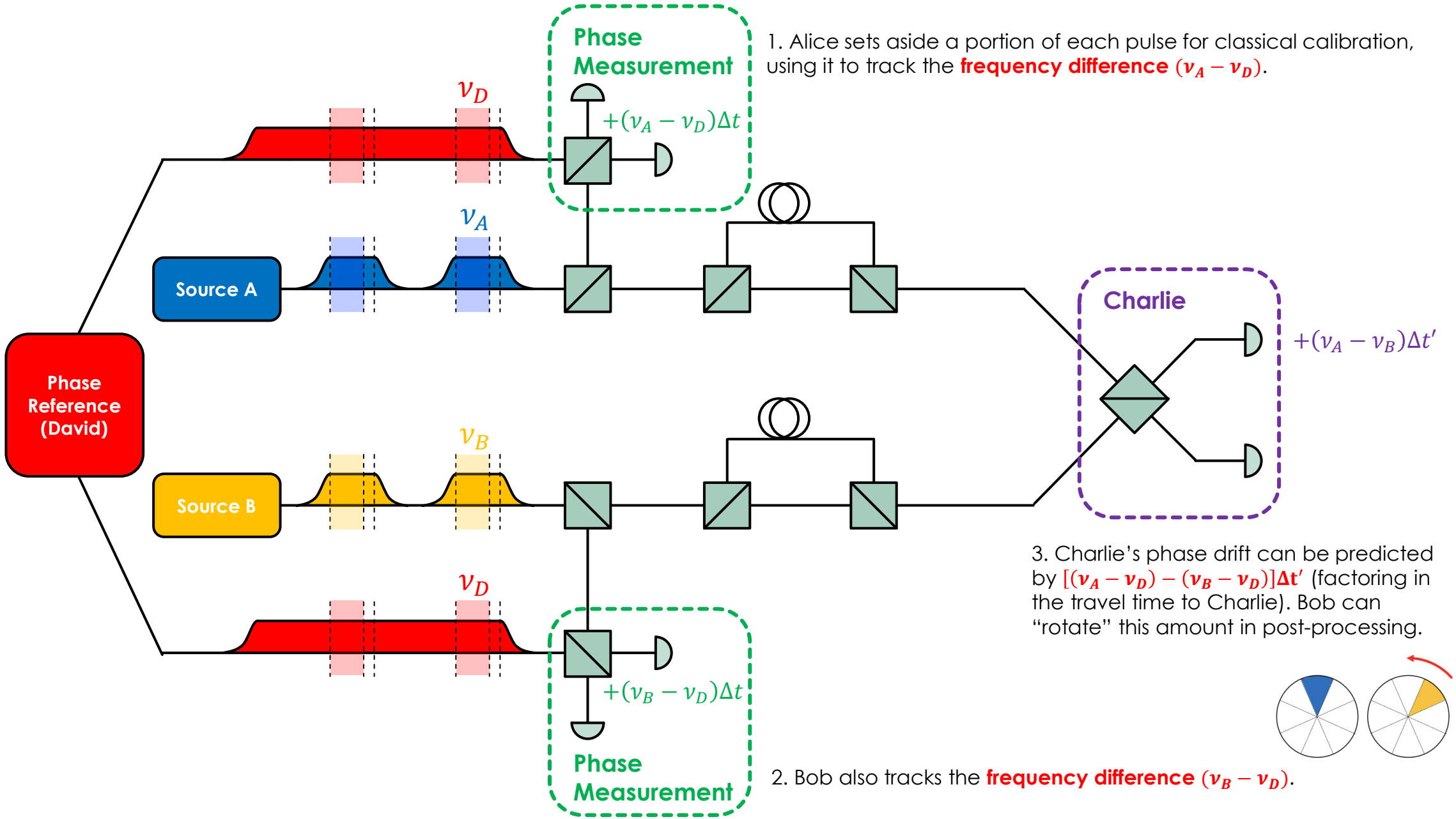
The frequency stability between Alice/Bob's local sources can be guaranteed by using a "single laser" setup and delay line, as proposed in [1] for passive BB84.

The frequency drift between the remote parties Alice and Bob is a more challenging problem. A potential solution would be to use the post-processing technique similar to that of [2] to track frequency difference and compensate for the drift during post-processing.

[1] W Wang, R Wang, C Hu, V Zapatero, L Qian, B Qi, M Curty, HK Lo, "Fully-Passive Quantum Key Distribution" Physical Review Letters 130.22 (2023): 220801.

[2] W Li, et al. "Twin-field quantum key distribution without phase locking." Physical Review Letters 130.25 (2023): 250802.

Compensating Frequency Drift (Remote)



1. Alice sets aside a portion of each pulse for classical calibration, using it to track the **frequency difference** $(\nu_A - \nu_D)$.

2. Bob also tracks the **frequency difference** $(\nu_B - \nu_D)$.

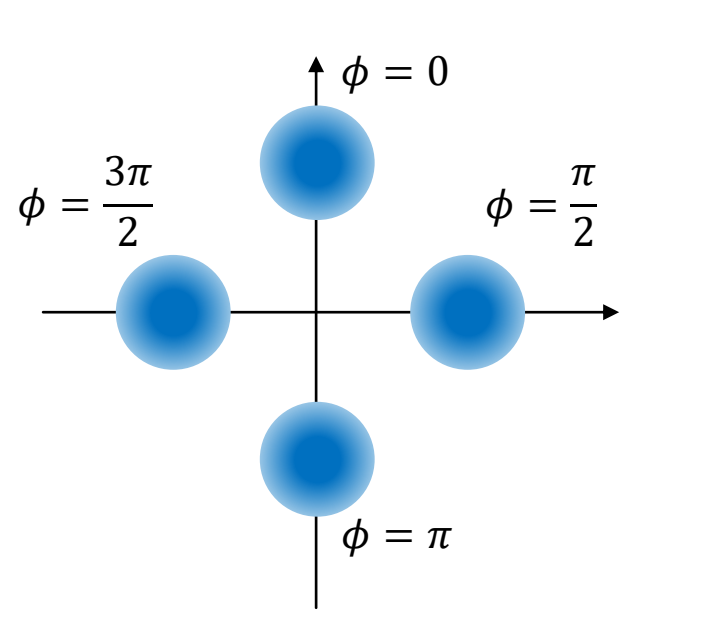
3. Charlie's phase drift can be predicted by $[(\nu_A - \nu_D) - (\nu_B - \nu_D)]\Delta t'$ (factoring in the travel time to Charlie). Bob can "rotate" this amount in post-processing.

Passive Continuous Variable QKD

Protocol: Discrete-Modulated CVQKD

Continuous-Variable (CV) QKD allows for high-rate and low-cost implementation of QKD systems with standard telecom components.

Up so far, passive CVQKD protocols have focused on thermal sources [1-3] which are relatively noisy.

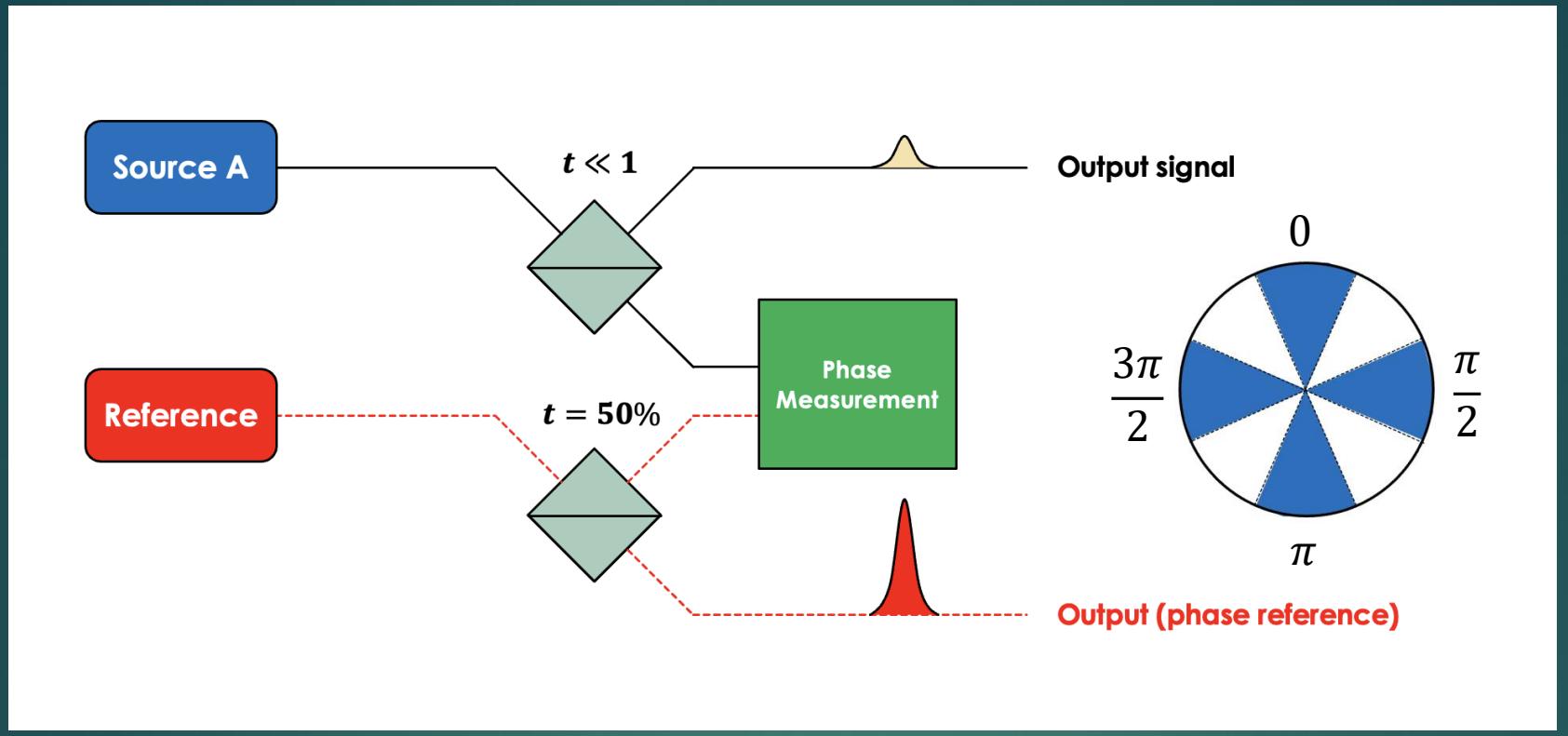


In this work, we focus on the discrete-modulated (DM) CVQKD [4,5] protocol, which directly uses the modulated phases $\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$ of four coherent states to encode key.

We will show that this protocol is in fact highly suitable for a fully passive setup – we can perform passive DMCVQKD without making any compromise to the sifting efficiency and QBER.

[1] B. Qi, P. G. Evans, and W. P. Grice, Physical Review A 97, 012317 (2018).
[2] B. Qi, H. Gunther, P. G. Evans, B. P. Williams, R. M. Camacho, and N. A. Peters, arXiv preprint arXiv:2001.06417 (2020).
[3] P. Huang, T. Wang, R. Chen, P. Wang, Y. Zhou, and G. Zeng, New Journal of Physics 23, 113028 (2021).
[4] J. Lin, T. Upadhyaya, and N. Lutkenhaus, Physical Review X 9, 041064 (2019).
[5] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Physical Review X 9, 021059 (2019).

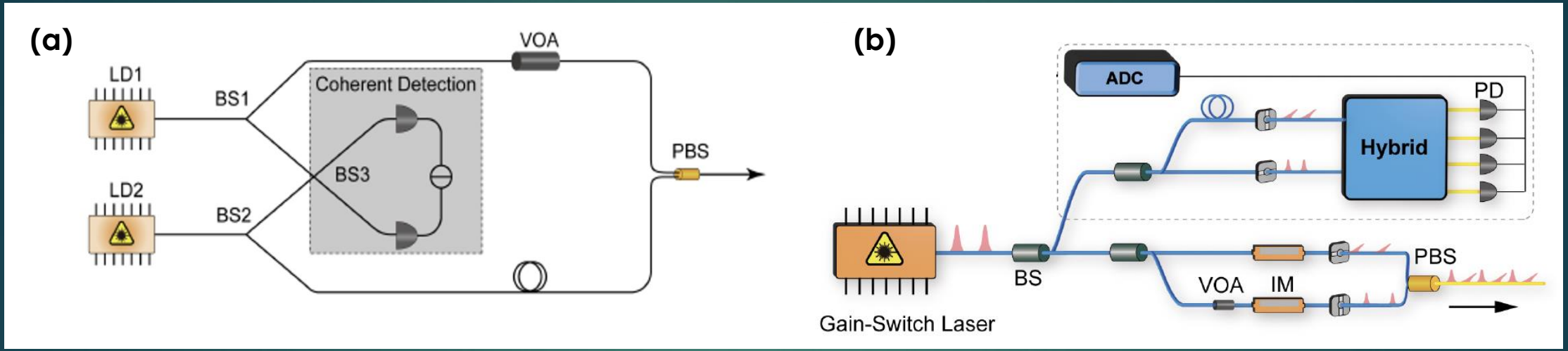
Intuition for Passive DMCVQKD Source



We can split off a part of the signal from a phase-randomized source A, measure it against a phase reference and record it, and send out the signal along with the reference pulse.

We can divide the phase between $[0,2\pi)$ into slices. One intuitive solution is to just select the four slices closest to $\left\{0,\frac{\pi}{2},\pi,\frac{3\pi}{2}\right\}$ (we will discuss how to perform better sifting later).

Setup for Passive DMCVQKD Source



In principle, two gain-switched lasers can be used, sending pulses that respectively correspond to the signals and the phase reference. The "signal" side is attenuated by a VOA to $\mu \ll 1$. Output signals can be time-and-polarization-multiplexed.

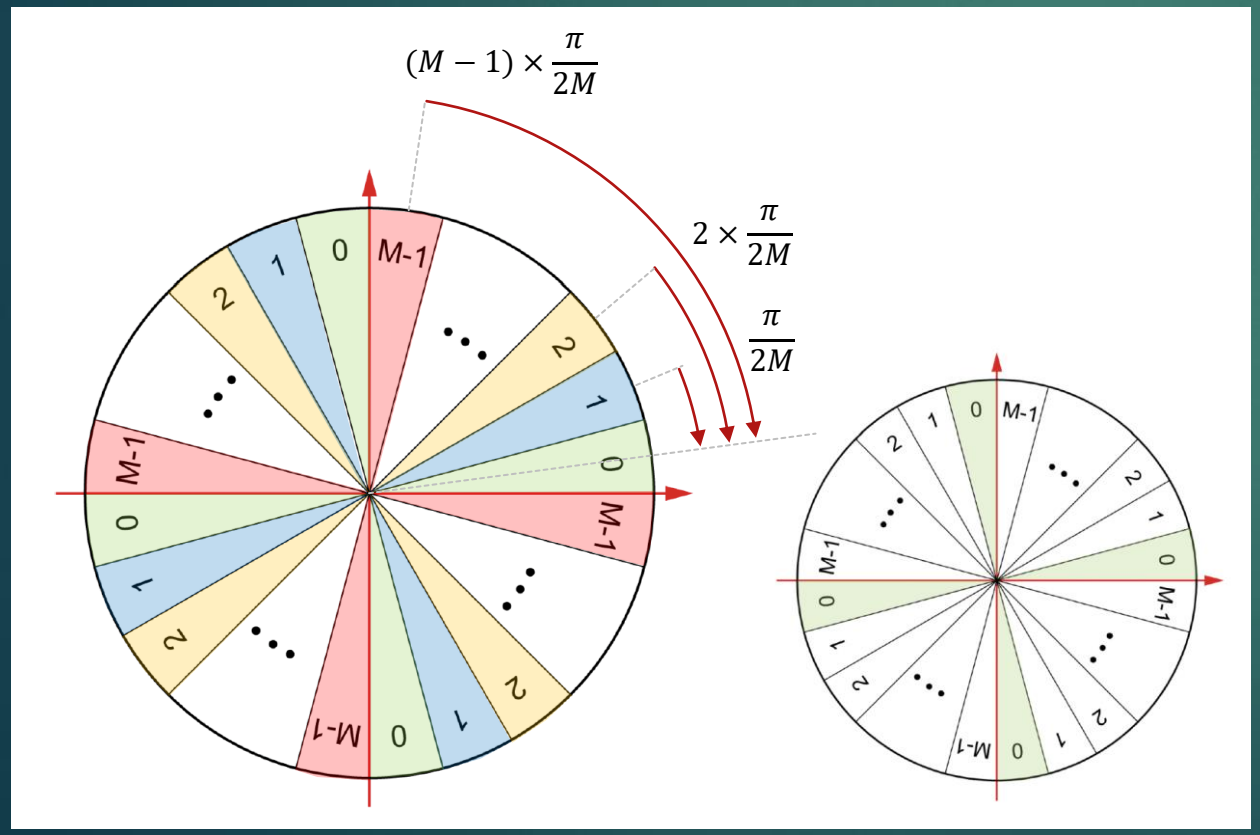
We assume phases are uniformly random and independent between adjacent pulses and between the two lasers. Frequency stability is also required, for which one can again use a "single laser setup" combined with delay.

The coherent detection measures the phase difference. In practice, it can be implemented with a "Hybrid" analyzer as shown in (b) upper right part using four photodiodes.

A perfect solution: phase space remapping scheme

If Alice's measurement outcome is θ, Alice keeps the secret key information $x = \left\lfloor \theta, \frac{\pi}{2} \right\rfloor$ and only announces the $\mathbf{mod}\left(\theta, \frac{\pi}{2}\right)$ global phase basis information to Bob.

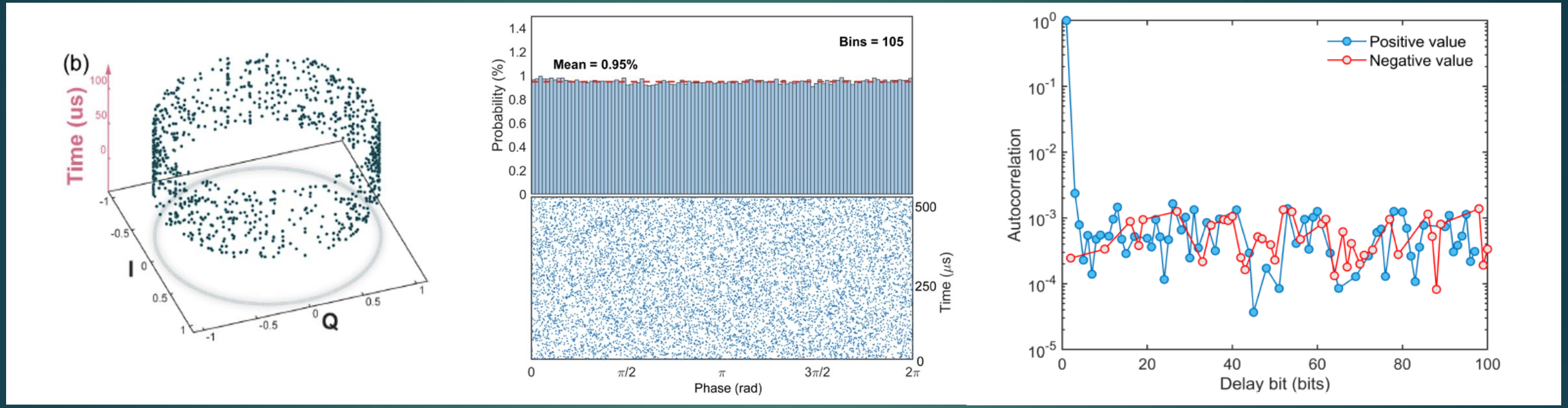
Since Bob performs the heterodyne detection, Bob can realign his phase space based on this global phase basis information $\mathbf{mod}\left(\theta, \frac{\pi}{2}\right)$.



The slice sizes can be infinitesimally small (only limited by detector resolution). Therefore, importantly we suffer from no additional sifting loss or QBER (in contrast to e.g. passive BB84 and TF-QKD).

Assuming ideal sources and detectors, passive DMCVQKD allows for better implementation security while having exactly the same key rate as active DMCVQKD.

Experimental characterization of laser source



We tested and verified the assumptions on uniform randomness and independence (auto-correlation given time shift) of phases among the pulse train.

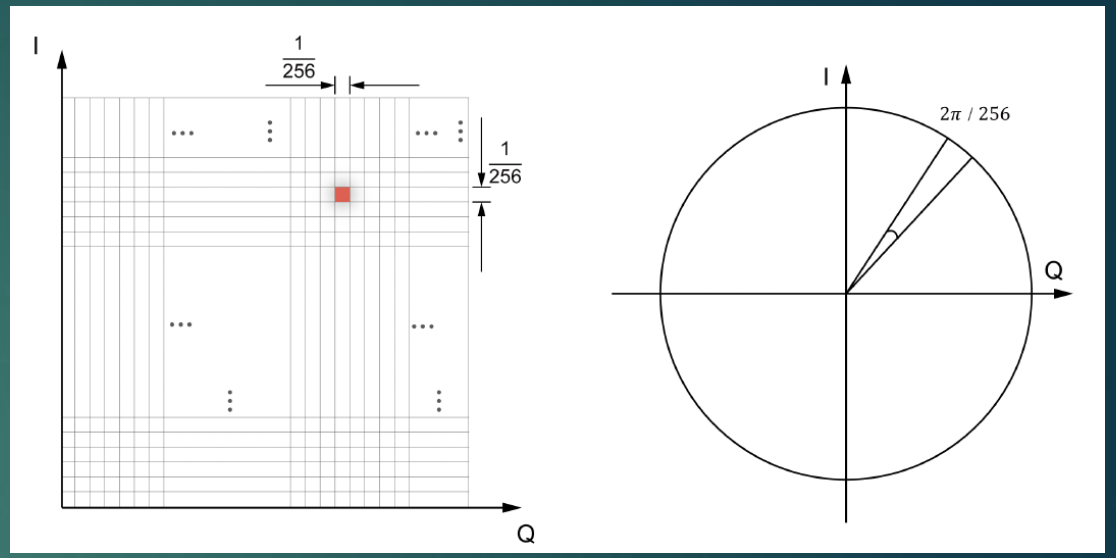
Phase resolution analysis

The slice size is not limited by sifting or QBER, but will be limited by the detection phase resolution.

Consider common 8-bit ADC or DAC:

- Active modulation: resolution is 0.0245 rad

- Passive system: 0.011 rad

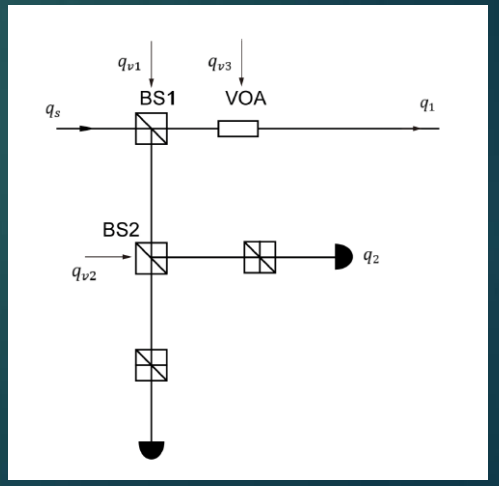


Noise analysis

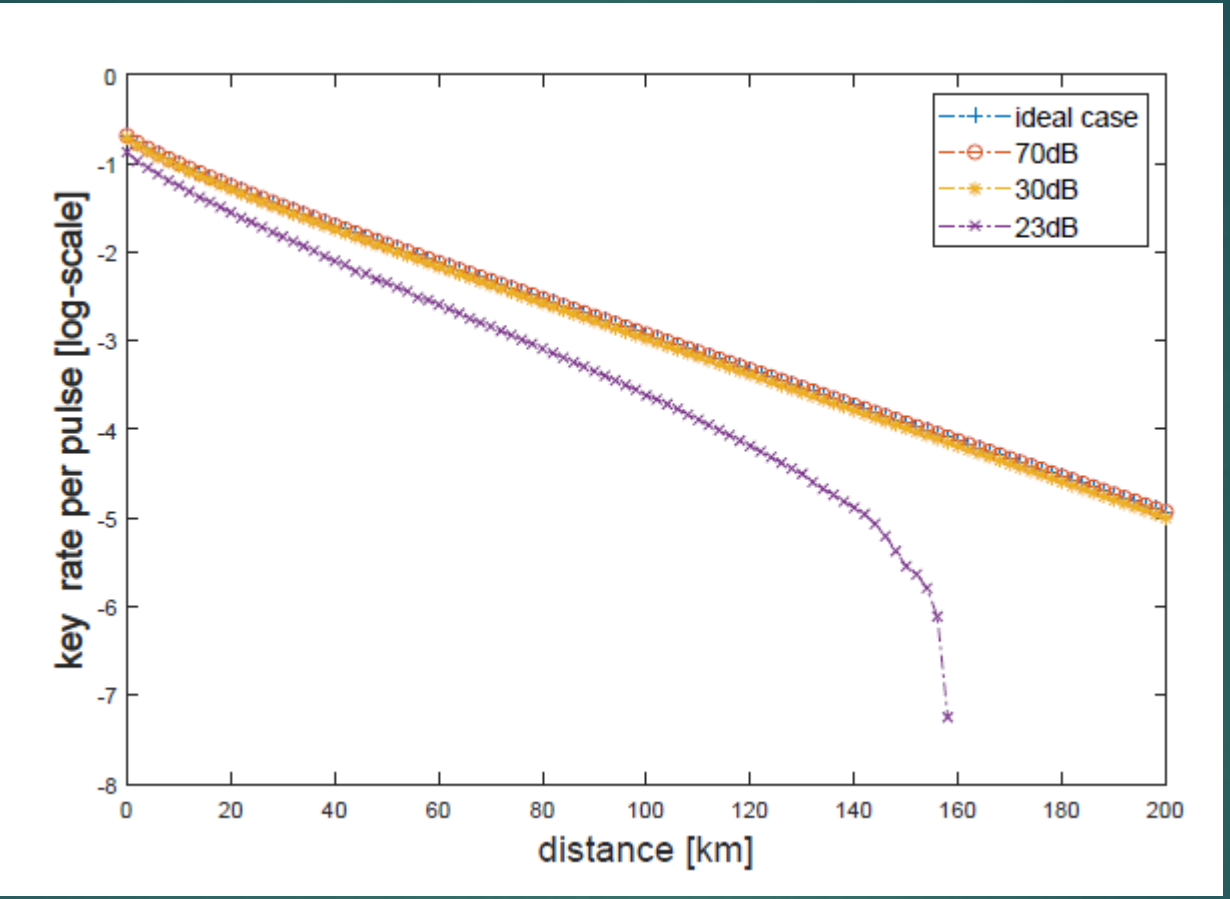
It is expected that the excess noise (due to passive source) approaches zero when the VOA has a large attenuation coefficient.

$$\epsilon = t_0 \frac{2|\mu_s|(1+E_{aq})}{|\mu_s|t_{aq}+4+4E_{aq}} \approx \frac{2t_0(1+E_{aq})}{t_{aq}}$$

E_{aq}: excess noise from detector, t_0: VOA extinction ratio, t_{aq}: Alice's detection efficiency of Q quadrature, $|\mu_s|$: intensity of classical coherent light



Simulation results



When the VOA has an attenuation of more than 30 dB, the excess noise of the passive state preparation scheme can be effectively suppressed, and the key rate will be almost the same as the ideal case.

Thank you very much!

Source Paper/Contact:

Fully Passive Twin-Field Quantum Key Distribution

arXiv preprint: 2304.12062

* wenyuanw@hku.hk † hklo@ece.utoronto.ca

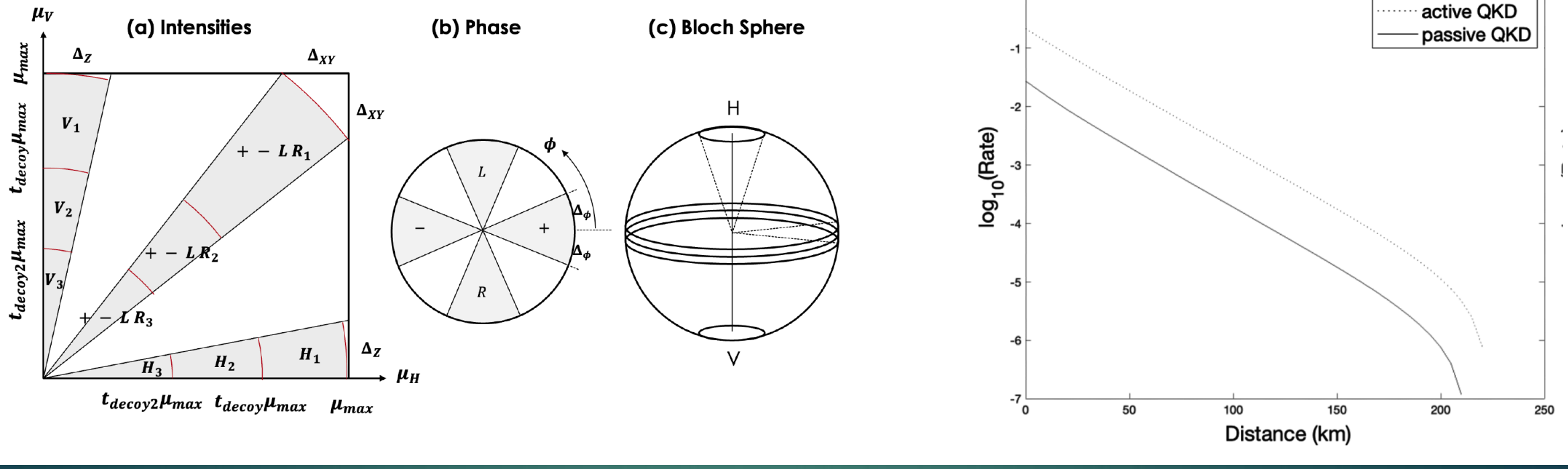
Passive Continuous-Variable Quantum Key Distribution

arXiv preprint: 2212.01876

** licheny@hku.hk

Backup Slides

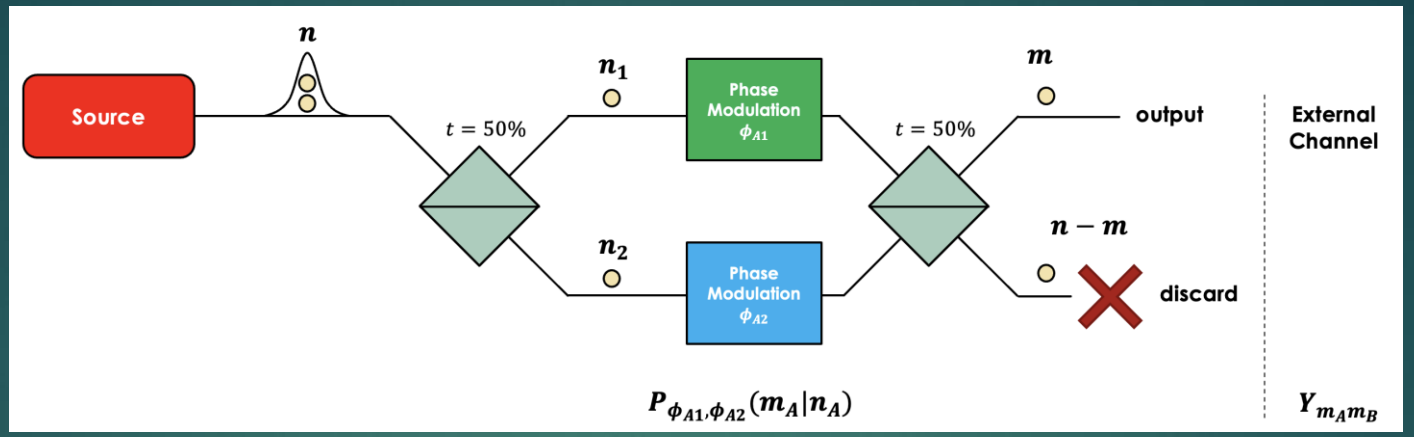
Fully Passive BB84



Alice can prepare BB84 states $\{H, V, +, -\}$ by performing post-selection on her local observables $(\mu_H, \mu_V, \phi_{HV})$.

The key rate is about one order-of-magnitude lower than active BB84 (due to sifting and inherent QBER).

Security Analysis



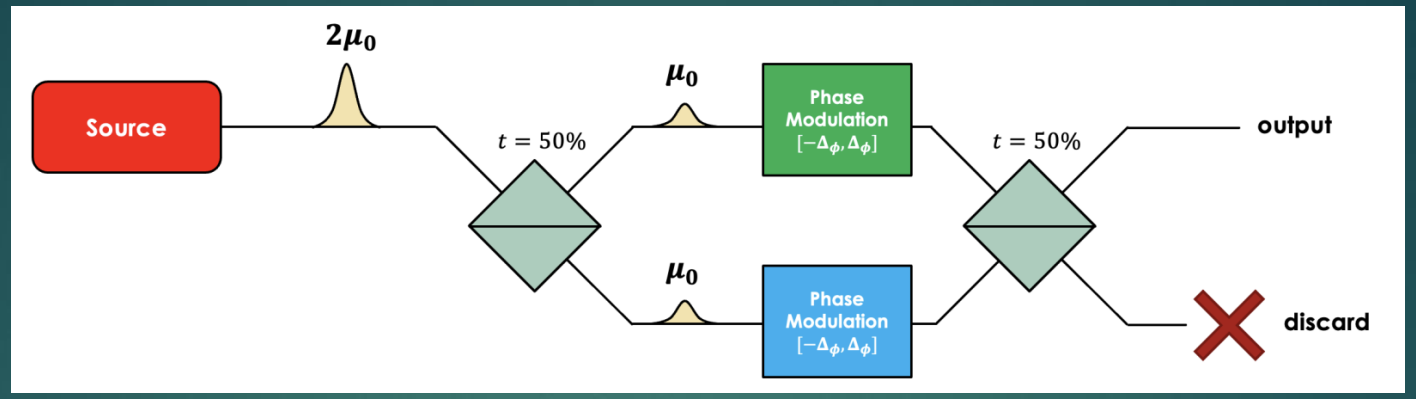
The conjugate basis in virtual protocol involves sending even and odd Cat states.

We can use Cauchy-Schwartz Inequality to first replace the Cat state source with mixed Fock states, and the effect of the local internal channels are simply extra losses $P_{\phi_{A1},\phi_{A2}}(m_A|n_A)$.

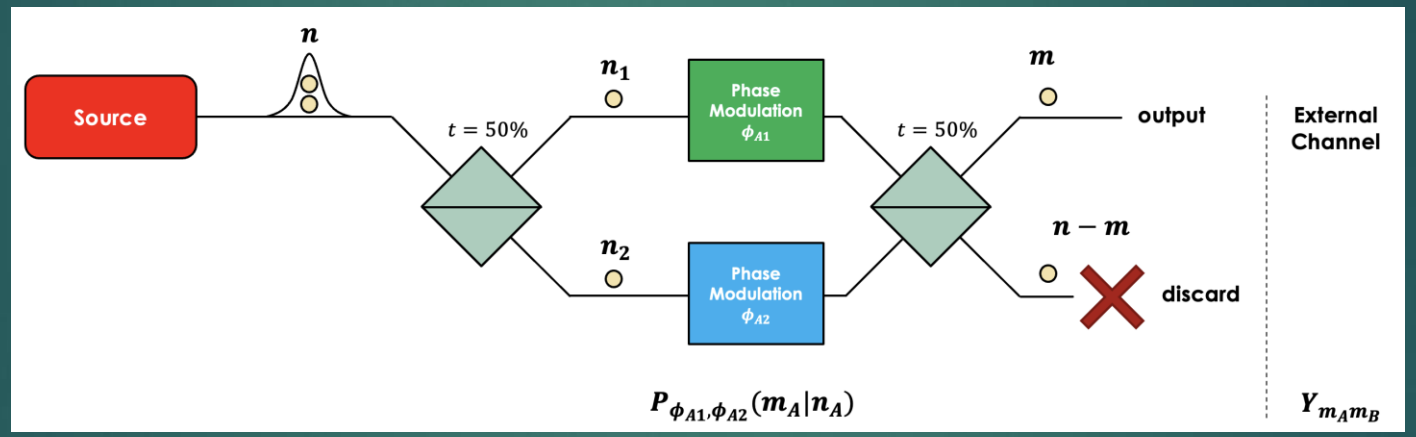
$$Y_{n_A n_B} = \iint \iint_{\phi_{A1},\phi_{A2}\phi_{B1},\phi_{B2}} \left[\sum_{m_A \le n_A} \sum_{m_B \le n_B} P_{\phi_{A1},\phi_{A2}}(m_A|n_A) P_{\phi_{B1},\phi_{B2}}(m_B|n_B) \times Y_{m_A m_B} \right]$$

$$e_{ZZ} = \frac{\Sigma \left(C_{nA} C_{nB} \sqrt{Y_{n_A n_B}} \right)^2}{p_{XX}^{mixed}}$$

Security Analysis



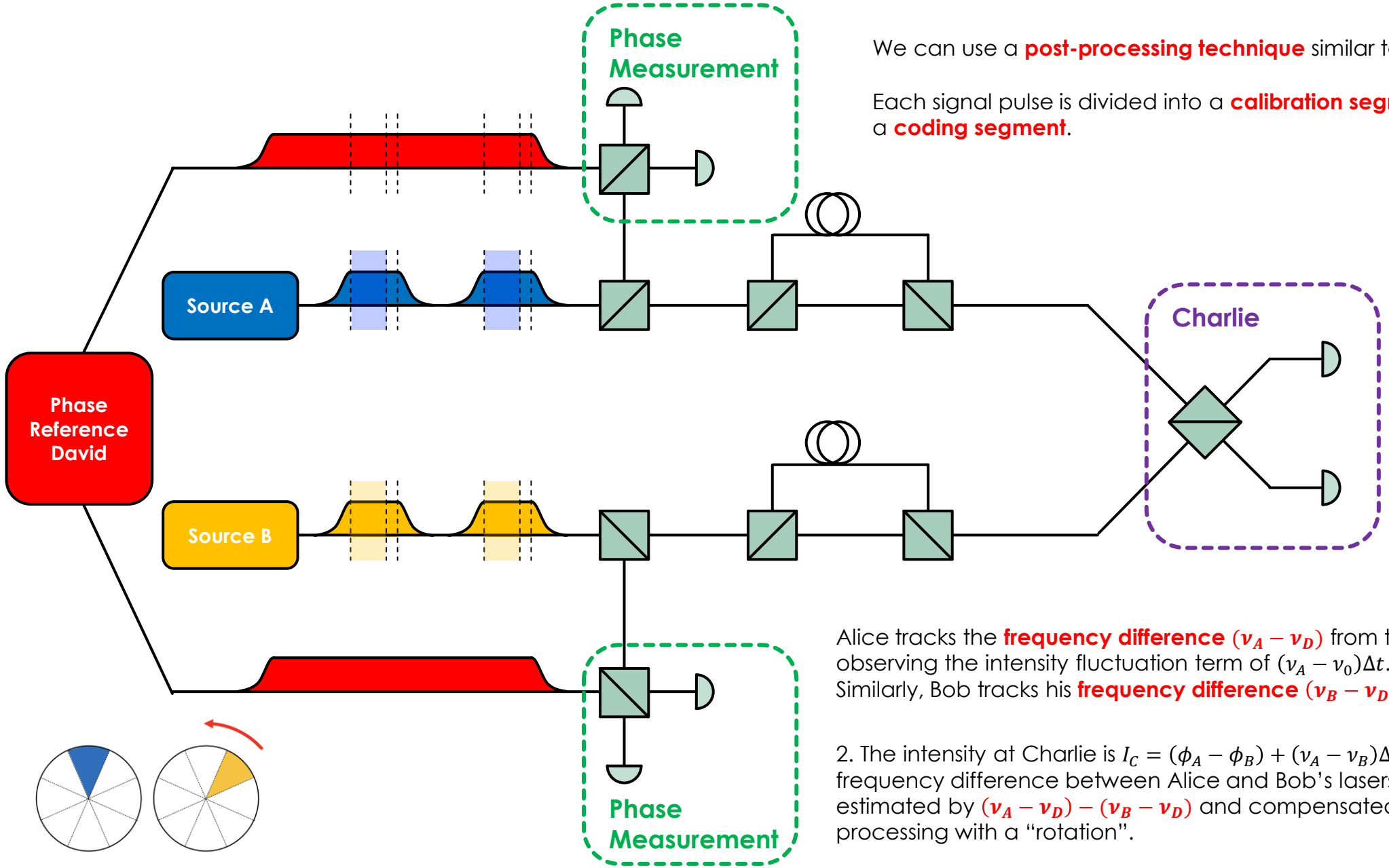
The signal state Gain p_{XX}^{mixed} and QBER e_{XX}^{mixed} already incorporate the effect of such internal channels.



The conjugate basis in virtual protocol involves sending even and odd Cat states.

We can use Cauchy-Schwartz Inequality to first replace the Cat state source with mixed Fock states, and the effect of the local internal channels are simply extra losses $P_{\phi_{A1},\phi_{A2}}(m_A|n_A)$.

Compensating Frequency Drift (Remote)



We can use a **post-processing technique** similar to that of [1].

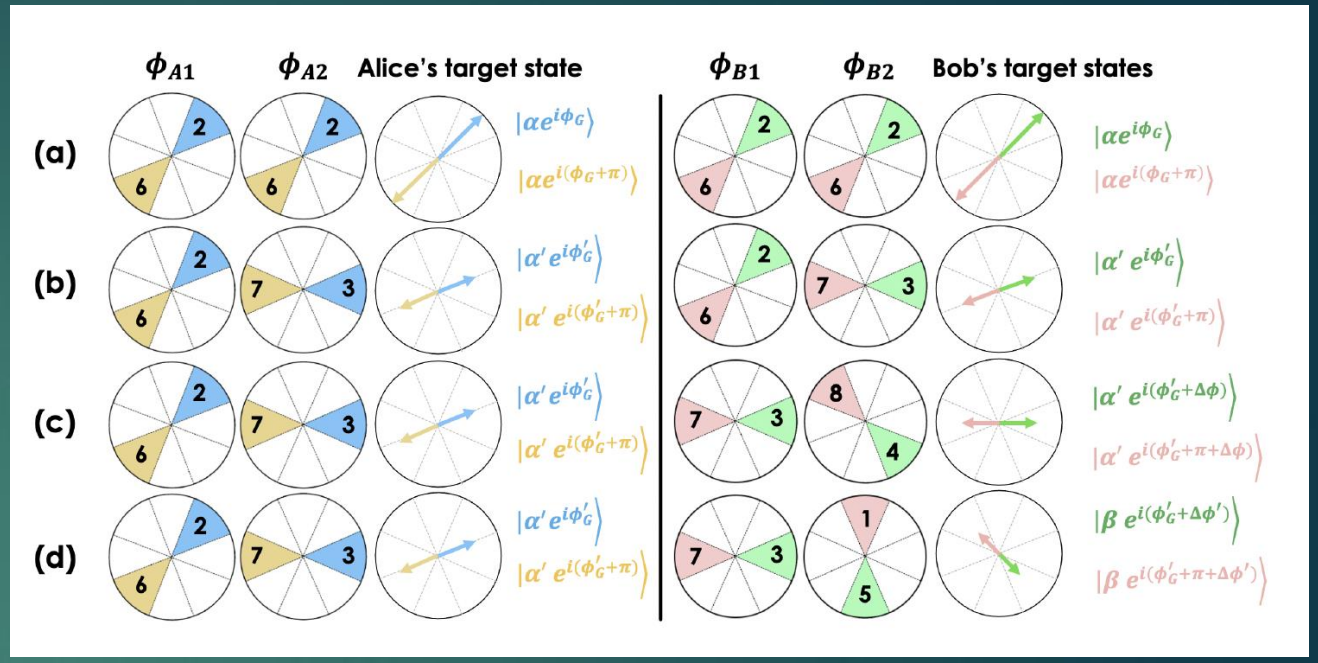
Each signal pulse is divided into a **calibration segment** and a **coding segment**.

Alice tracks the **frequency difference** $(\nu_A - \nu_D)$ from the reference by observing the intensity fluctuation term of $(\nu_A - \nu_0)\Delta t$.
Similarly, Bob tracks his **frequency difference** $(\nu_B - \nu_D)$.

2. The intensity at Charlie is $I_C = (\phi_A - \phi_B) + (\nu_A - \nu_B)\Delta t'$, where the frequency difference between Alice and Bob's lasers can be estimated by $(\nu_A - \nu_D) - (\nu_B - \nu_D)$ and compensated for in post-processing with a "rotation".

Caveat 2: Sifting Efficiency

$$R = \frac{1}{N^4} \sum_{k_{A1}=1}^{N} \sum_{k_{A2}=1}^{N} \sum_{k_{B1}=1}^{N} \sum_{k_{B2}=1}^{N} [\max(0, R_{0,1}(k_{A1}, k_{A2}, k_{B1}, k_{B2})) + \max(0, R_{1,0}(k_{A1}, k_{A2}, k_{B1}, k_{B2}))]$$



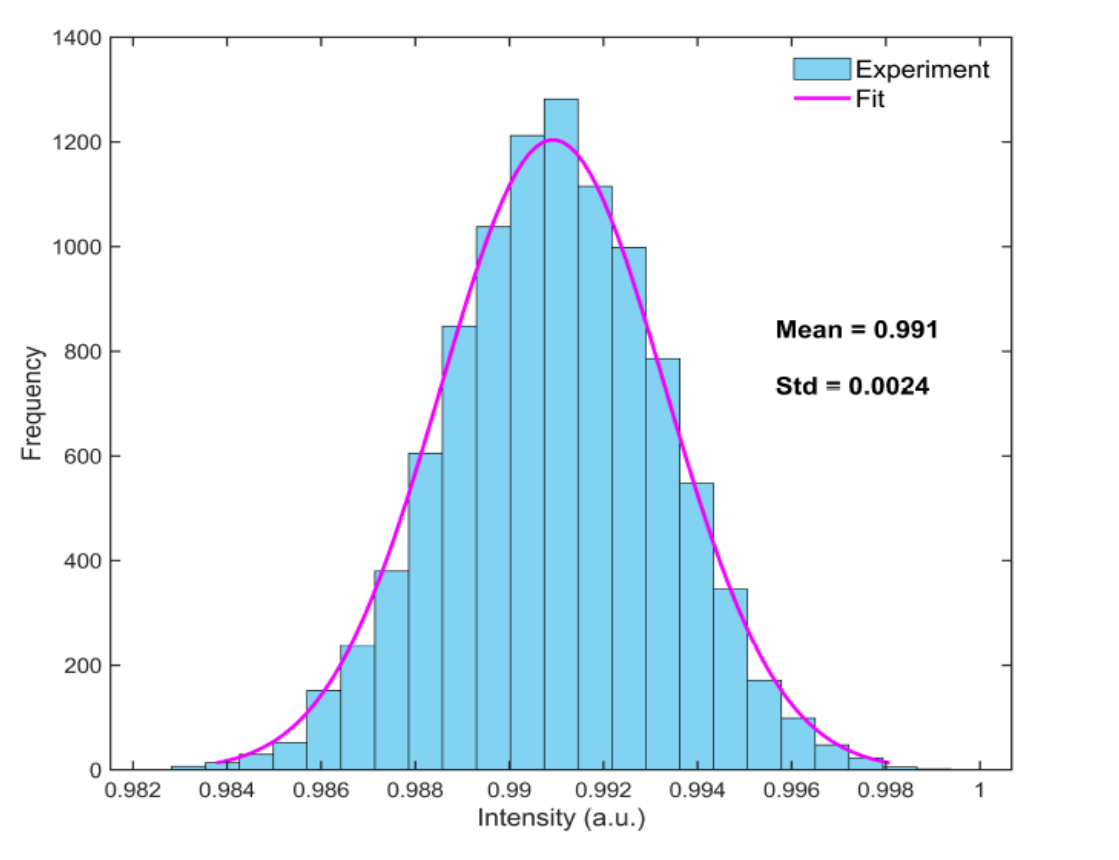
a. Alice and Bob do not need to select $(0, \pi)$ as the signal basis.

b. Local slices at Alice/Bob can be different (resulting in lower signal intensity)

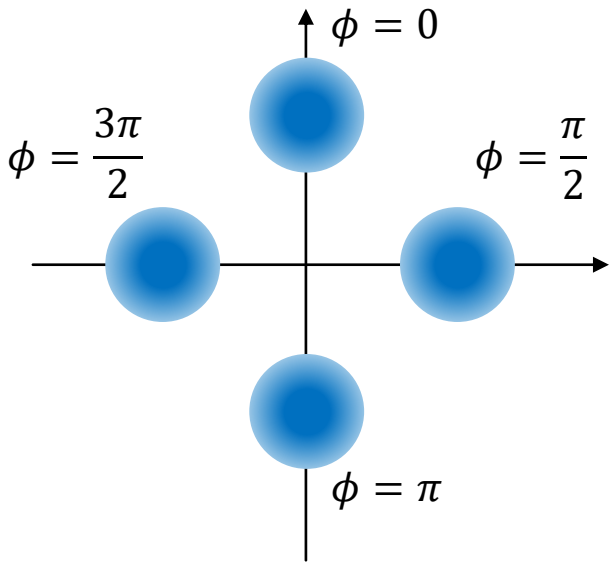
c. Bases for Alice and Bob can be different (resulting in misalignment)

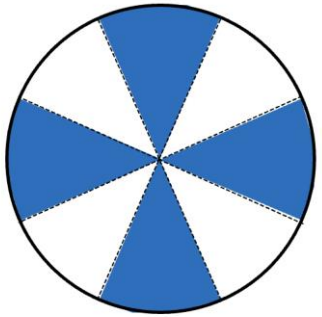
d. Local slice difference, i.e. signal intensities, for Alice and Bob can be different (resulting in intensity asymmetry).

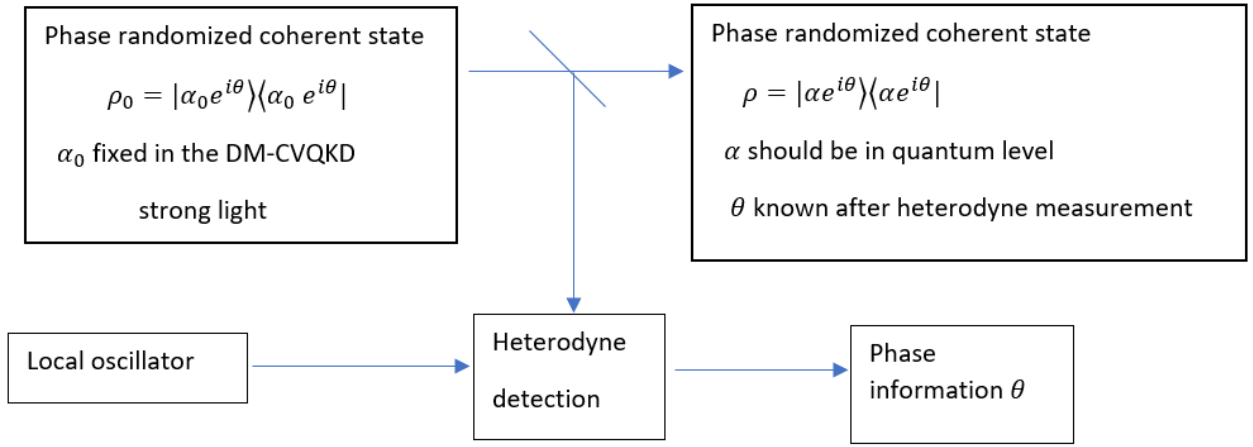
The mismatched slices correspond to various non-optimalities such as lower signal intensity, misalignment, or signal intensity asymmetry, but do not affect the security analysis. Overall, any combination of A1, A2, B1, B2 slices can be used to attempt key generation (we can simply keep the combinations with nonzero key rate).


Experiment
Fit
Mean = 0.991
Std = 0.0024
Frequency
Intensity (a.u.)
0
200
400
600
800
1000
1200
1400
0.982
0.984
0.986
0.988
0.99
0.992
0.994
0.996
0.998
1

Protocol: Discrete-Modulated CVQKD







Passively, θ is not fixed to 0, pi/2, pi, 3pi/2