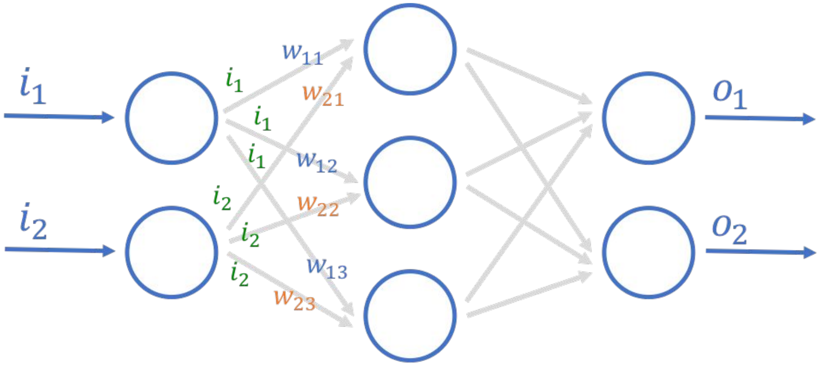
Secure Multiparty Inner Product Calculation

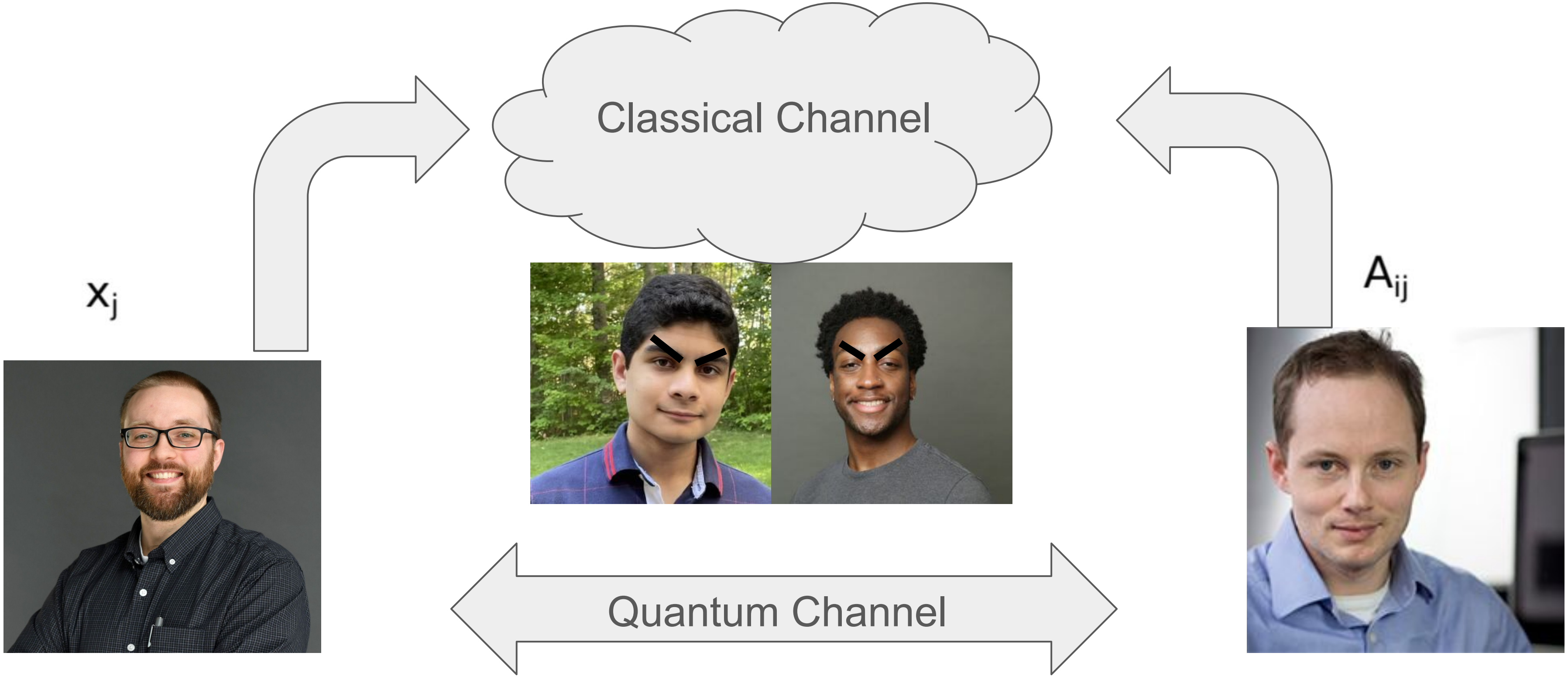
MIT 6.2410 Final Project
Daniel Sanango, Eugene Jiang, Stanley Chen

Motivations

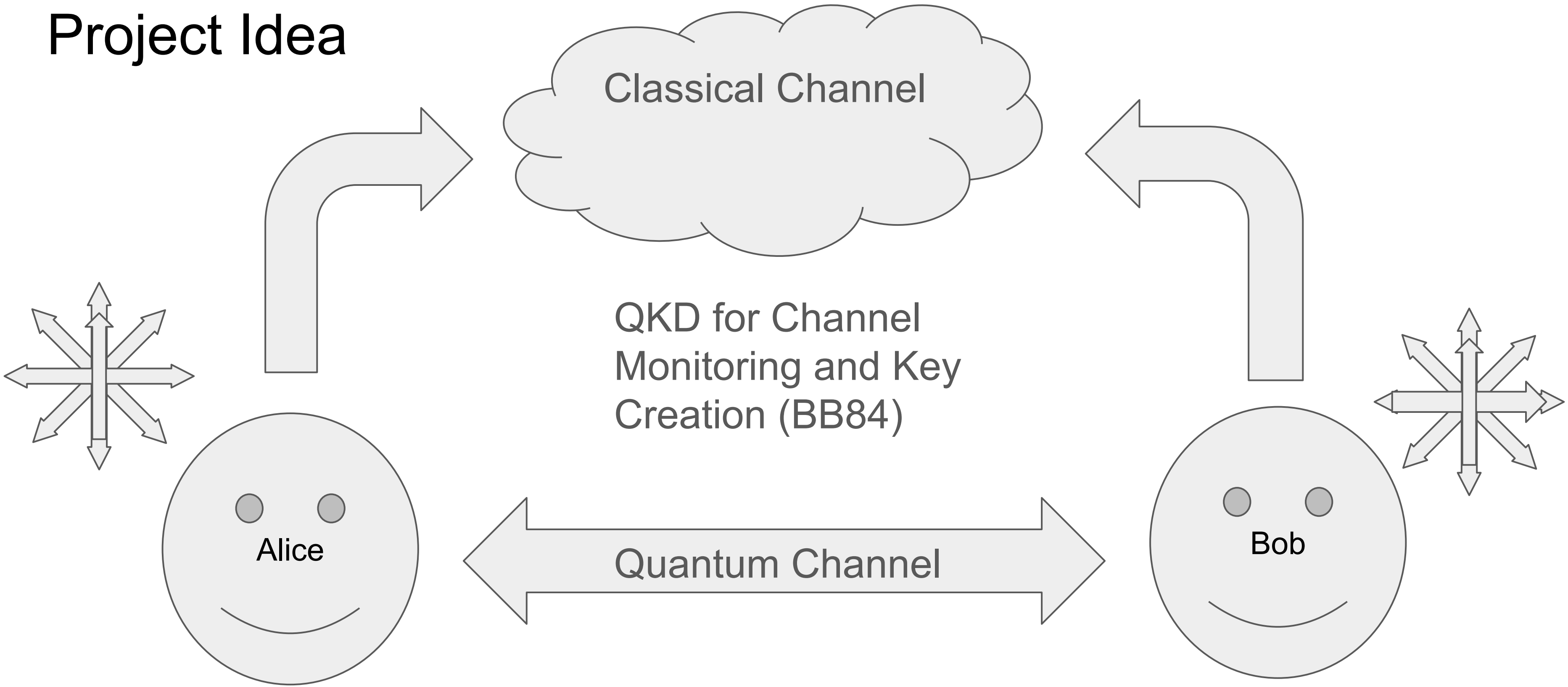
- The purposes of Quantum Key Distribution (QKD)
  - Channel monitoring → detects eavesdroppers
  - Secret key generation → denotes the working basis of each bit during IP
- The purposes of Inner Product Calculations (IP)
  - Inner Product → Matrix multiplication → Neural Networks
- Novelty: Same hardware, dual role
  - Enables efficient task switching between IP and QKD
  - Eavesdroppers cannot deliberately avoid eavesdropping during QKD by observing the hardware setup
  - Secure, compact



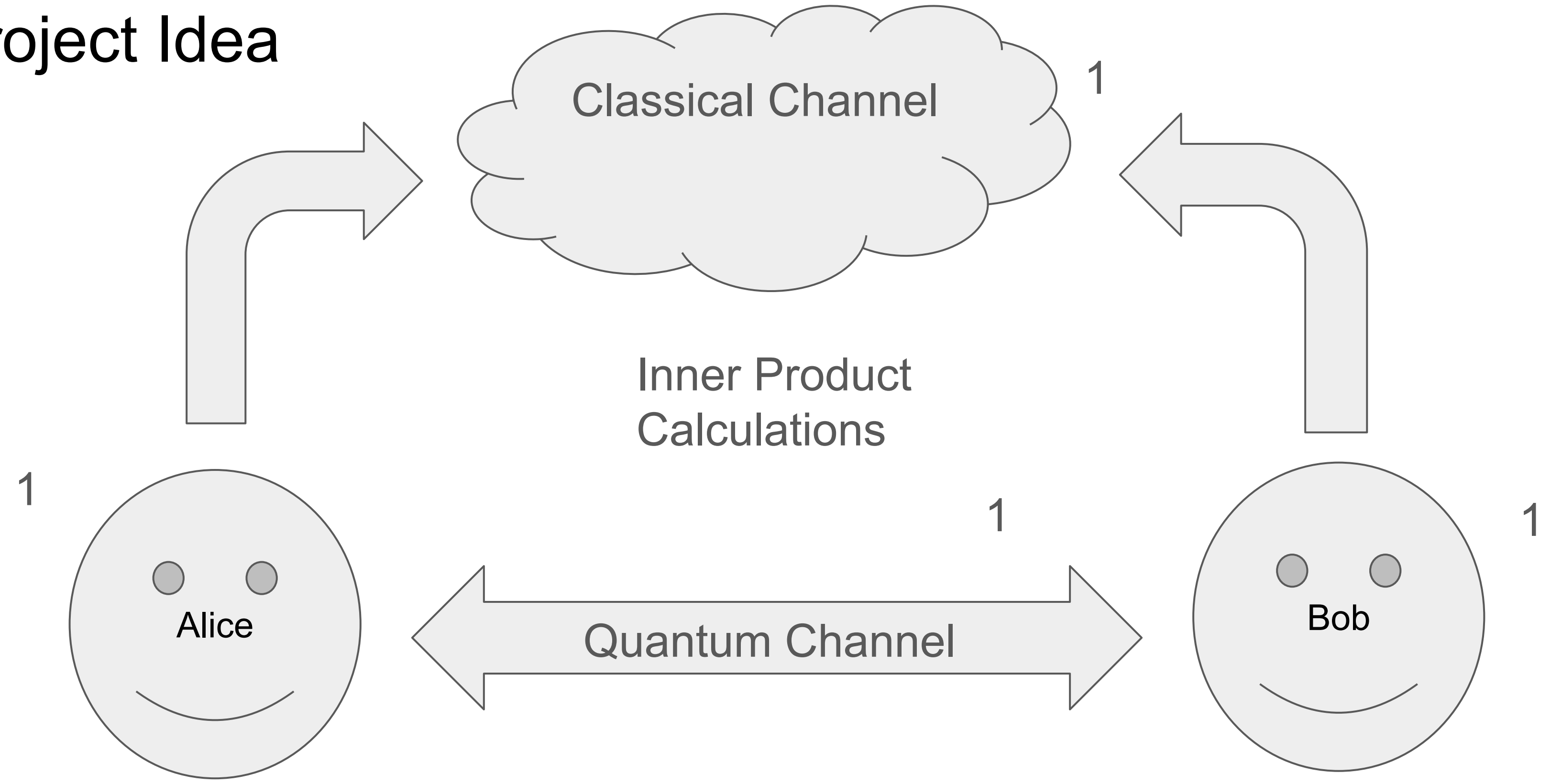
$$\begin{bmatrix} w_{11} & w_{21} \\ w_{12} & w_{22} \\ w_{13} & w_{23} \end{bmatrix} \cdot \begin{bmatrix} i_1 \\ i_2 \end{bmatrix} = \begin{bmatrix} (w_{11} \times i_1) + (w_{21} \times i_2) \\ (w_{12} \times i_1) + (w_{22} \times i_2) \\ (w_{13} \times i_1) + (w_{23} \times i_2) \end{bmatrix}$$


Classical Channel
x_j
A_{ij}
Quantum Channel

Project Idea

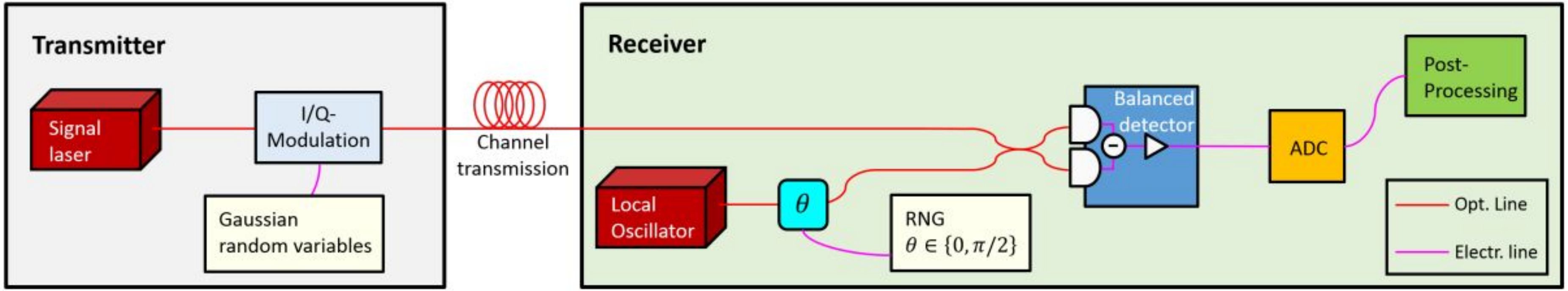


Project Idea

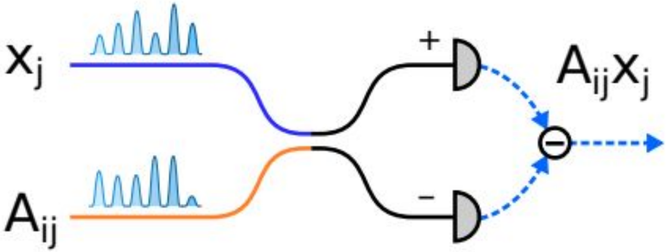


Proposed Approach

Coherent-State CV-QKD / homodyne detection



Advanced Quantum Technologies



arXiv

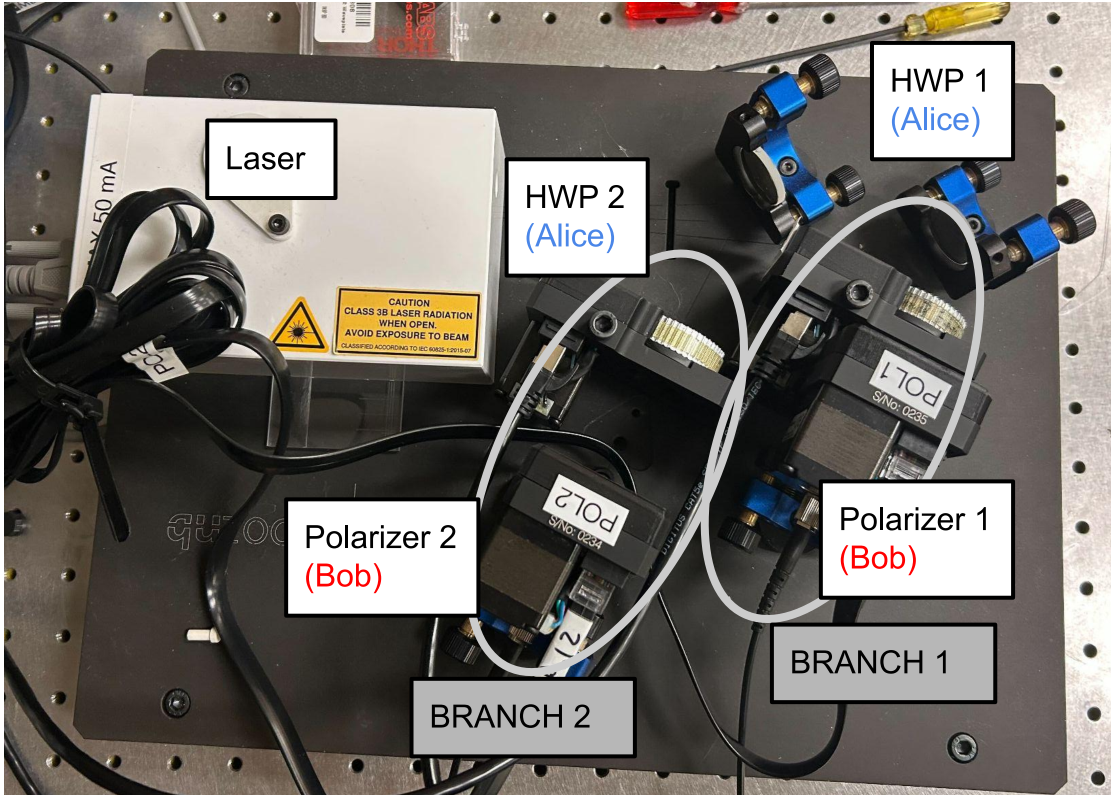
Current Setup

IP

- Weak Coherent Pulse (WCP) and truth table

QKD

- Single photon pulsed mode with modified BB84

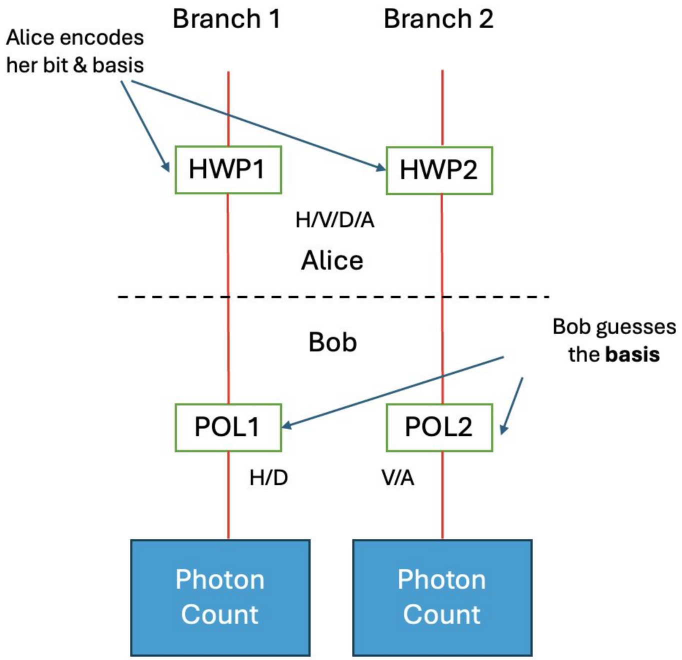


System Assumptions

- Pre-determined schedule for IP+QKD
- Initial key already shared
- Alice and Bob trust each other
- Hide motor activity (eavesdropping protection)
- Pulse sent numerous times (QKD and IP methods use this to improve accuracy)

Quantum Key Distribution (QKD)

- Pulsed mode, single-photon behavior
- Alice encodes her bit & basis by rotating HWPs (randomly selected)
- Bob guesses the basis, then measures two bits simultaneously (one in each branch)
- Keep matching bases and “1”s
    - “1” less error-prone (photon absorption, quCR error rate of 30%)
- Expecting 5%-10% qBER

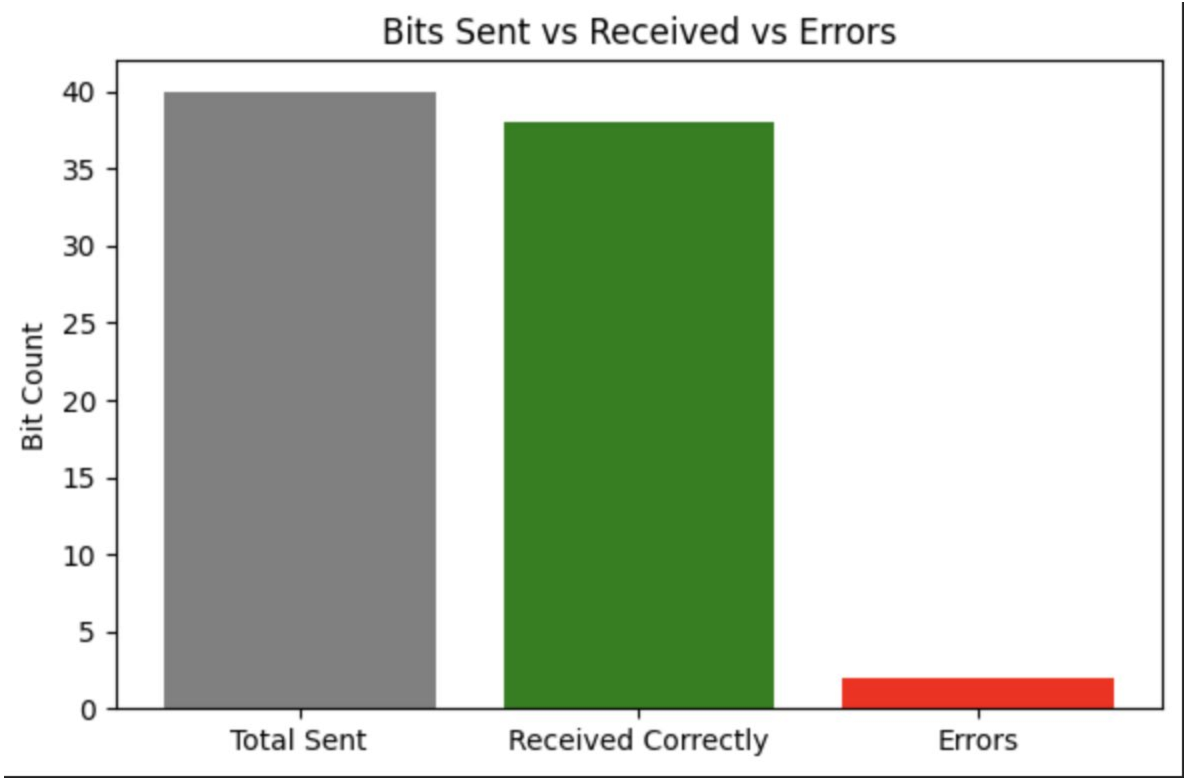


QKD Result & Analysis

Expected: 5%-10%

Obtained: 5% qBER

Eavesdropper → measured qBER greater



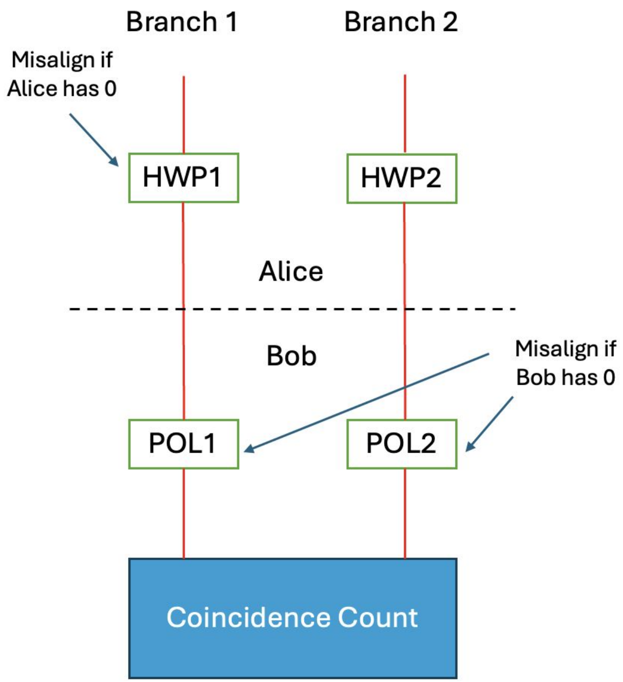
Inner Product Calculation

- Alice and Bob encodes their bits by rotating their HWPs (polarizers)
- The result is given by the coincidence count
- Using weak coherent pulse (WCP)
  - More consistent product results
  - Easier to set up

IP Truth Table		Alice	
		0	1
Bob	0	0	0
	1	0	1

Default (11): HWP and polarizer in the same branch are aligned

At least one of the two branches will be shutted down if there's a 0, which ideally gives rise to no coincidence count



IP Result & Analysis

- 2 errors in 900 trials
- 0.22% estimated error rate
- 95% Confidence interval: [0.027, 0.801]% Clopper-Pearson Exact CI
- Acceptable for Inference but not training

Discussion

- Our IP calculation is not resilient to eavesdropping
    - Information is lost if eavesdropper has measured the photons in the wrong basis
- Tradeoff between efficiency & security
    - Performing channel monitoring more frequently increases the security but takes more time

Conclusion & Prospects

- Expanded applications
  - Can be generalized to calculate inner products of any base (not just binary)
  - Can be scaled up to do matrix multiplication (useful in neural networks, ML, etc)
- Remaining Challenges
  - Optimize efficiency, motors slow (potentially use electro-optic modulator)
  - Improve accuracy of IP calculation
- Project extensions
  - Test if the system is able to detect eavesdroppers experimentally
  - Program the system to automatically schedule itself to run QKD and IP
  - Use a system with phase and amplitude basis
  - Use the system to train a small neural network

Thanks For Listening

Any questions?