Secure Multiparty Inner Product Calculation

6.2410 Quantum Engineering Platforms–Final Project

Eugene Jiang
Department of Electrical Engineering and Computer Science
jiange12@mit.edu

Daniel Sanango
Department of Electrical Engineering and Computer Science
danango@mit.edu

Stanley Chen
Department of Electrical Engineering and Computer Science
stanleyc@mit.edu

Executive Summary

As deep learning and machine learning become increasingly central to modern computing, the need for secure computation has become increasingly necessary. In this paper, we propose a quantum-based system designed to perform secure inner product computations. Our approach leverages the principles of Quantum Key Distribution (QKD), channel monitoring, and secret key generation to build a secure computation framework. By alternating pseudorandomly between QKD-based communication and inner product (IP) computation phases, the system ensures that any eavesdropping attempt is both detectable and ineffective. This secure inner product capability enables protected large matrix operations—core to neural networks—within a quantum-secure environment, offering a compact and secure method for quantum-assisted machine learning and confidential data processing.

I. Introduction & Motivation

Modern communication systems allow individuals to exchange critical information rapidly and securely, enabling essential tasks such as financial transactions and password management. As the technological landscape evolves, a growing emphasis on deep learning models and vast databases is prevalent. With this shift, not only is the volume of data increasing, but its value–along with the value of the models trained on it–is becoming more significant. Consequently, data privacy and secure computation are rising in importance, driving the need for robust systems and protocols that prevent third parties from accessing or interpreting sensitive information.

This introduces the motivation for quantum systems designed for secure neural network computing between parties. There are existing theoretical quantum systems that facilitate secure computation between two *non*-trusted parties that can perform inner product operations with incredibly high accuracy and efficiency. However, a central challenge lies in designing a single quantum system capable of performing both inner product (IP) computations and quantum key distribution (QKD), with the flexibility to switch between these tasks securely for use by two trusted parties.

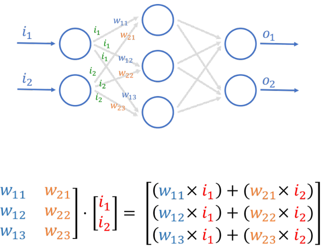
Leveraging the principles of both techniques, we propose a system that enables collaborative computation of machine learning and deep learning models without exposing sensitive data to third parties. This system utilizes motorized polarizers and half-waveplates for light modulation, allowing for the encoding of bases and bits. This system lays foundational work for secure, quantum-enhanced distributed learning, enabling collaboration across institutions without compromising data privacy. For example, organizations in sensitive sectors—such as healthcare, finance, or national security—can jointly train machine learning models without exposing their underlying data, protecting proprietary or confidential information from third-party access.

II. Background

We want to achieve inner product calculations so that we can encode real vectors to be able to compute neural networks. When we take apart a neural network, it all ends up boiling down to a large number of inner product calculations. As you can see in Fig. 1.

Initially we hoped to implement a modified Continuous-Variable Quantum Key Distribution (CV-QKD) system with Gaussian modulation [1], allowing for quick IP calculations. The construction of the system is shown in (Fig 2), which is based on homodyne detection. When performing QKD, Alice encodes the bit and basis by modulating the phase and amplitude of the laser, while Bob selects the measurement basis by introducing different phase shifts randomly on another source of laser. Bob's measurement result is given by the interference of two lasers. Our approach to tailoring the system for IP calculations involves having Bob modulate his laser based on his input vector, rather than applying an arbitrary phase shift, as IPs can also be computed via homodyne detection [2].

While systems like the one described above represent the current state of the art, there has yet to be a fully integrated implementation that combines both QKD and IP computation within a single unified system. We show that with a simple modification to a standard QKD setup, this integration becomes possible. Specifically, instead of performing random-basis measurements, Bob can encode his bit directly into the local oscillator. This change enables the system to produce an output that is proportional to the inner product between Alice's and Bob's data vectors [2].



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

Fig. 1: The usage of IPs in a neural network

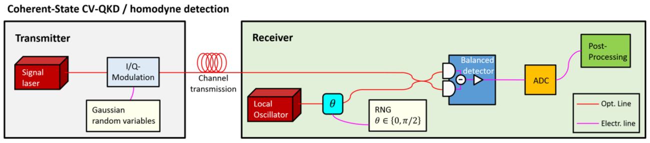


Fig. 2: [1] The scheme of CV-QKD based on homodyne detection. Alice corresponds to the transmitter while Bob is the receiver.

III. Experimental Description

We created a system that is able to provide the same functionality as our initially proposed system. Rather than using phase and amplitude basis, we decided to use polarization bases due to resource and time constraints. Our system relies on key assumptions for optimal security and use. Specifically:

1) There exists a pre-determined schedule for both parties to perform QKD and IP
2) To begin the process, an initial key is already shared
3) To transmit data, generate quantum keys, and perform dot products, Alice and Bob trust each other
4) Motor activity is hidden to prevent third parties from recording motor movement data
5) Information pulses are sent numerous times. This gives us the ability to improve our proposed QKD and IP methods' information accuracy

With these assumptions specified, we now detail our experimental setup in three parts. First, we demonstrate our physical system. Second, we demonstrate our modulation tuning system. Third, we demonstrate our quantum key distribution process. Finally, we demonstrate our inner production calculation process.

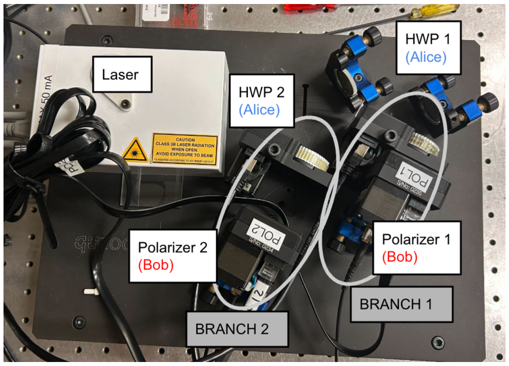


Fig. 3: Physical Setup for QKD-IP System

A. Physical System

For easy laser manipulation (intensity, counts/second) and data extraction methods with a Python interface, we decided to use the qutools quED module in the modern optics lab. While we were able to find phase and intensity modulators in other laboratories, the quED's restrictive design made it impractical to implement a proper CV-QKD system. We thus opted to modulate laser intensity with a motorized half-waveplate and polarizer setup, tools intended for use with the quED.

Our physical system (Fig. 3) utilizes the laser, polarizers, half-waveplates, and motors provided with the qutools quED module. Our setup consists of a laser that sends an optical pulse through two branches. The laser is controlled with the quED's system manager. The laser can be switched to CW or pulsed mode, where features such as laser intensity, pulse frequency, and pulse duration are set.

[In Code: "Automated Motor Tuning"] Because our setup was shared with another group and because of expected motor inconsistencies with maintaining an angle for prolonged periods of time, we first "tune" the motors. To tune the motors, we first set the laser to CW mode and the pulse current to 40.00[mA], giving us a large count rate on both detectors. We then rotate the polarizers and identify the angle where counts are maximized. This angle becomes the offset for our polarizers. We then do the same for the half-waveplates, setting an offset based on maximum counts. With these angle offsets, we guarantee that, at the offset state, the polarizer axis and slow axis are aligned, allowing the system to maintain a self-consistent basis.

In each branch, Alice acts through a half-waveplate, while Bob acts through a polarizer. In both our QKD and IP procedures, Alice and Bob's hardware are manipulated through a python interface with the quED. Information that reaches the end of the branches then travels to the quED system manager, where photon counts from each branch are detected and recorded in 100[ms] bins. Finally, we use our Python interface to extract recorded count data and perform data analyses.

B. Quantum Key Distribution Approach

[In Code: "QKD Functions"] We begin the quantum key distribution process by creating random bases and bits for Alice, and *just* random bits for Bob (as shown in Fig. 4). Setting our laser to pulsed mode, with pulse frequency at 20.00[Hz] and pulse duration at 10.00[μs], we are able to achieve around 1 photon count per 100[ms], with slight jitters to 0 and 2 counts. Alice's half-waveplates are then set to her random basis and bit. Bob encodes his bit guesses in the "+" basis in POL1 and the "x" basis in POL2. The result is then interpreted by the quED, which reports a photon count. This is repeated for n samples. In our approach, we used $n = 300$.

After collecting count data, we begin the sifting phase. Since Bob measures the same bit but in different bases, when doing

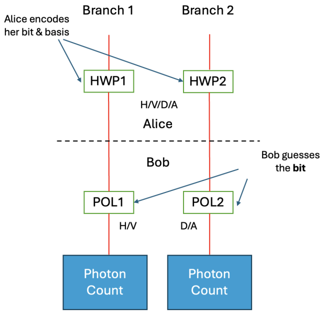


Fig. 4: QKD Approach Diagram

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

TABLE I: Truth table of IP calculation. This is equivalent to logical AND.

the basis-comparison stage, we keep the bit information for the basis that Alice used and throw out the other.

Next, we keep count measures of 1 and throw out the rest. We only keep 1's because this is the least error-prone measurement result. For 0's one would have to also consider the quED's known error rate of 30%, as well as photons failing to arrive at detectors because of absorption in optical fibers.

Finally, we obtain a quantum bit error rate (qBER) by comparing Alice's bits to Bob's bits. Based on this result, if the qBER gets noticeably higher, we can infer that an eavesdropper is present, allowing us to terminate communications.

C. Inner-Product Approach

[In Code: "IP Functions"] We can manipulate the Half Wave plates and Polarizers in both branches change the polarization of the photons to encode both branches in such a way that we are able to achieve the IP truth table (Table I). We demonstrate a photonic system that implements a 2-bit binary inner product operation (equivalent to a logical AND gate) using the polarization states of photons and standard linear optical components. The system is designed such that a coincidence detection event (i.e., simultaneous photon detection in both output arms) occurs if and only if both input bits, held by parties Alice and Bob, are 1. All other input combinations yield no coincidences, thereby reproducing the desired binary truth table for the inner product or AND operation.

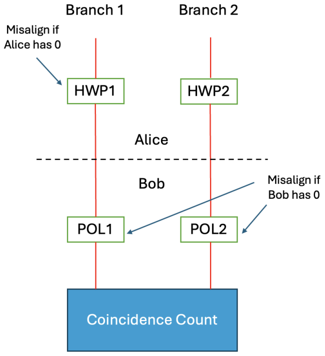


Fig. 5: IP Approach Diagram

In our setup (Fig. 5), Alice's bit is encoded in the polarization state of a pair of single photons, one in each optical arm, prepared using half-wave plates. A bit value of 0 is encoded by preparing one photon in a vertically polarized state and the other in a horizontally polarized state. A bit value of 1 is encoded by preparing both photons in vertically polarized states.

Bob's bit determines the measurement basis and is implemented by placing polarizers in each arm. A bit value of 0 corresponds to setting both polarizers to transmit horizontally polarized light, while a bit value of 1 corresponds to transmitting vertically polarized light.

The behavior of the system under each input configuration is as follows:

- *Alice = 0, Bob = 0 or 1*: At least one of the photons is orthogonal to Bob's chosen measurement basis, resulting in one or both being blocked. Consequently, no coincidences are observed.
- *Alice = 1, Bob = 0*: Both photons are vertically polarized, but Bob's polarizers are set to transmit horizontal polarization, blocking both photons and yielding no coincidences.
- *Alice = 1, Bob = 1*: Both photons are vertically polarized, and both polarizers are aligned to transmit vertical polarization. This results in successful transmission and detection of both photons, producing a coincidence event.

To account for background noise and detector dark counts, we set an intensity threshold above which a detection event is considered a valid coincidence. This threshold ensures that coincidences are only registered in the case of aligned polarization between Alice and Bob (i.e. when both bits are 1). In addition, we averaged the counts during the time interval in which counts were collected. This resulted in a massive boost in accuracy as the number of counts, especially for weak pulses had large fluctuations, so much so that if we too a single sample in a 100 ms integration window, we could easily mistakenly sample a count that appears like background noise.

This method of bit encoding and measurement leverages the fundamental polarization selectivity of linear polarizers, enabling a simple and effective implementation of a logical AND operation using single-photon-level optics. We used a weak pulse to do the experiments as in real applications, we would ideally want very weak pulses. Our settings were set to pulse mode with a pulse duration of 15.00[μs] and a frequency of 150.00[Hz].

IV. Results and Discussion

In QKD mode, we observed a quantum bit error rate (qBER) of approximately 5

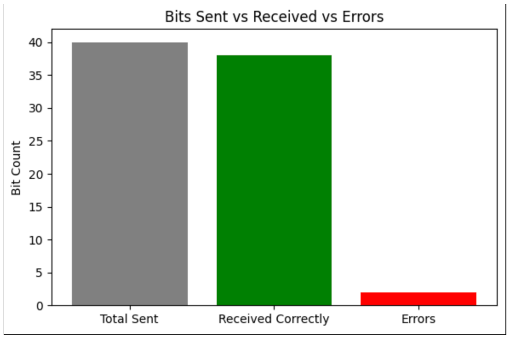


Fig. 6: Bar chart showing the number of bits sent, received, and the number of errors

Although a 5% qBER is within the acceptable range for secure key generation, it is higher than what is achieved in state-of-the-art systems, which often report qBERs below 2% using integrated photonic chips [4]. This gap highlights the limitations of our current setup, especially with respect to manual alignment and relatively noisy components. As for IP mode, we recorded 2 errors out of 900 trial bits, resulting in an estimated bitwise error rate of 0.22%. Using the Clopper-Pearson exact method, we computed a 95% confidence interval of $[0.027\%, 0.801\%]$ for the true error rate. This low error rate suggests that the polarization control and coincidence detection in our setup are functioning reliably under the current configuration. While this level of accuracy is acceptable for basic inference tasks, it is likely insufficient for training machine learning models, which typically require highly precise and repeatable computations to ensure convergence. Training tasks are especially sensitive to noise accumulation over many matrix operations, so even small errors could lead to unstable learning dynamics. These results highlight the need for tighter control over alignment, as well as higher-speed, lower-noise modulation components if the system is to be scaled for more advanced applications like neural network training. A major limitation of our current IP setup is that it is not resilient to eavesdropping. If an eavesdropper intercepts and measures the photons in the wrong basis, the information is irreversibly disturbed and lost, which is a consequence of quantum measurement's destructive nature. This vulnerability reinforces the importance of regularly performing channel monitoring during IP calculations. Although running QKD more frequently enhances the chance of detecting eavesdropping, it also consumes more time and increases overhead. Therefore, there exists a tradeoff between efficiency and security.

Another key challenge lies in the speed and accuracy of both QKD and IP calculations. Our setup operates at a rate of 1 bit/sec in QKD mode and 2 bits/sec in IP mode. Compared to state-of-the-art QKD, which is at GHz speed [4], our system is limited by slow mechanical components and sequential photon-level processing, making it impractical for real-time or large-scale computations. To address this bottleneck, we originally proposed a phase-modulating approach, inspired by techniques used in continuous-variable QKD (CV-QKD) [1]. Phase and amplitude modulation can be implemented using high-speed electro-optic modulators (EOMs), which allow for rapid and precise control of quantum states without moving parts. This would significantly increase the throughput of both key generation and inner product calculations, while also paving the way for more scalable optical computation schemes. As integrated photonics and compact EOM-based systems continue to advance, phase-modulated implementations remain a promising future direction for improving the performance and practicality of dual-purpose quantum systems like ours. Additionally, the accuracy of the inner product calculations is limited by fluctuations in coincidence counts, which introduce noise and variability into the results. The gate-based logic implemented using the quED system is inherently more susceptible to such errors, making it less reliable. In contrast, using modulation-based systems, where two states interfere to perform the inner product, offers a more robust and efficient alternative. This approach not only improves speed but also enhances accuracy, as it eliminates the need to rely on thresholding techniques to infer the inner product value.

V. Conclusion

This project explored a dual-purpose optical system capable of performing both QKD and IP calculation using the same polarization-based setup. Our experiments showed that QKD could be used effectively for channel monitoring, with a qBER of around 5%, while the IP calculation achieved a low error rate of 0.22%. These results support the viability of combining secure communication and computation in a single quantum photonic platform.

Although we initially aimed to use a phase-modulated design, practical constraints led us to adopt a polarization-based approach using familiar equipment from our BB84 lab module. Nevertheless, we remain motivated to pursue the phase-based method in the future, especially given its compatibility with high-speed modulation and scalable photonic integration.

Looking forward, we see several paths for improving and extending this system: integrating faster components like electro-optic modulators, automating QKD/IP switching, expanding the input encoding basis, and applying the system to simple machine learning tasks. These directions are supported by ongoing developments in quantum photonics and suggest that systems like ours may eventually play a role in secure, quantum-assisted computation. Many issues such as accuracy, and computational time can be solved using modulators that would allow us to do computations in the phase and amplitude bases.

References

[1] F. Laudenbach et al., "Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations," Advanced Quantum Technologies, vol. 1, no. 1, p. 1800011, Jun. 2018, doi: https://doi.org/10.1002/qute.201800011.

[2] R. Hamerly, L. Bernstein, A. Sludds, M. Soljačić, and D. Englund, "Large-Scale Optical Neural Networks Based on Photoelectric Multiplication," Physical Review X, vol. 9, no. 2, May 2019, doi: https://doi.org/10.1103/physrevx.9.021032.

[3] K. Sulimany, V. S. Krishna, R. Hamerly, P. Iyengar, and D. Englund, “Quantum-secure multiparty deep learning,” arXiv (Cornell University), Aug. 2024, doi: https://doi.org/10.48550/arxiv.2408.05629.

[4] J. A. Dolphin, T. K. Paraïso, H. Du, R. I. Woodward, D. G. Marangon, and A. J. Shields, “A hybrid integrated quantum key distribution transceiver chip,” npj Quantum Information, vol. 9, no. 1, Sep. 2023, doi: https://doi.org/10.1038/s41534-023-00751-3.