Quantum Conference Key Agreement Using a Photonic Integrated Circuit Green Machine

Benjamin Fisher[1]*‡, Tyler Stowell[1]†‡, J. Gabriel Richardson[2], Dzianis Saladukha [3], Matthew Hall [3], Robert Bernson[3], Ian Frank, Saikat Guha[2], Peter O'Brien [3], Ryan M. Camacho [1]

[1] *Brigham Young University, Provo, UT 84604*
[2] *University of Maryland, College Park, MD, 20742*
[3] *Tyndall National Institute, Cork, Ireland*

**benja256@byu.edu, †trs66@byu.edu,‡Authors contributed equally*

Abstract: Quantum Conference Key Agreement (QCKA) allows a group of users to establish a shared secret key. We describe the experimental characterization of a "Green Machine" photonic integrated circuit (PIC) and its simulated performance in QCKA.

Quantum Conference Key Agreement (QCKA) allows a group of users to establish a secure shared key and can achieve higher key rates in a quantum network than two-party approaches [1]. QCKA can be implemented using a device which implements a Hadamard unitary known as the "Green Machine" [2], shown in Fig. 1(a). However, realizing this unitary is difficult owing to the low loss and path length stability requirements which reduce key generation efficiency. Here we report the results of fabricating and testing a chip-scale Green Machine that overcomes these limitations. We also report on a novel digital twin simulator that allows for the direct emulation of conference key agreement rates using the fabricated device.

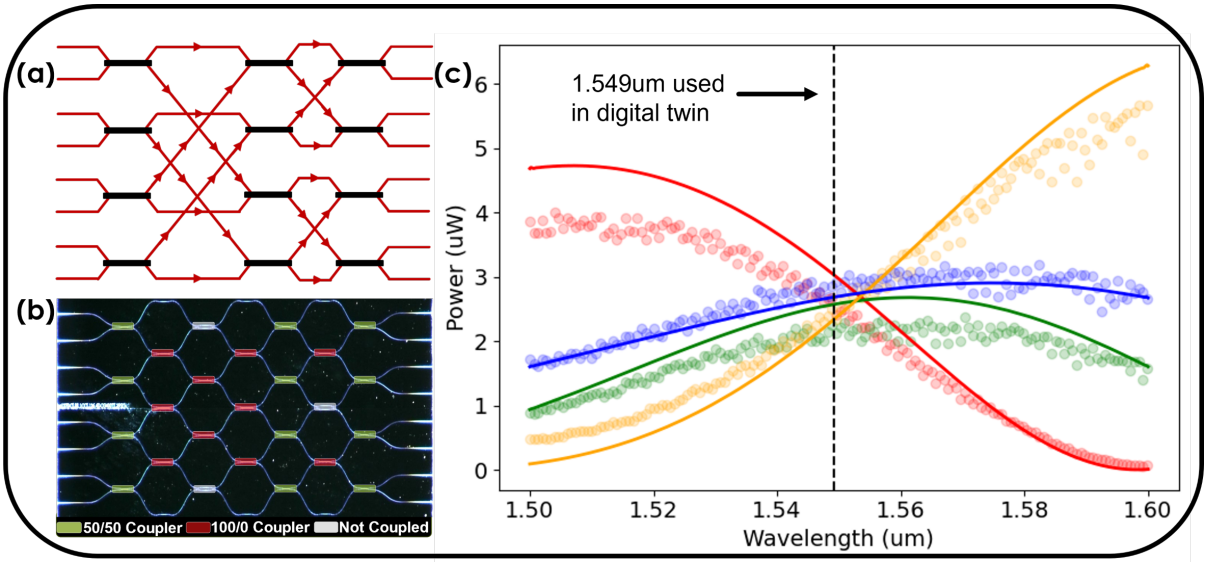


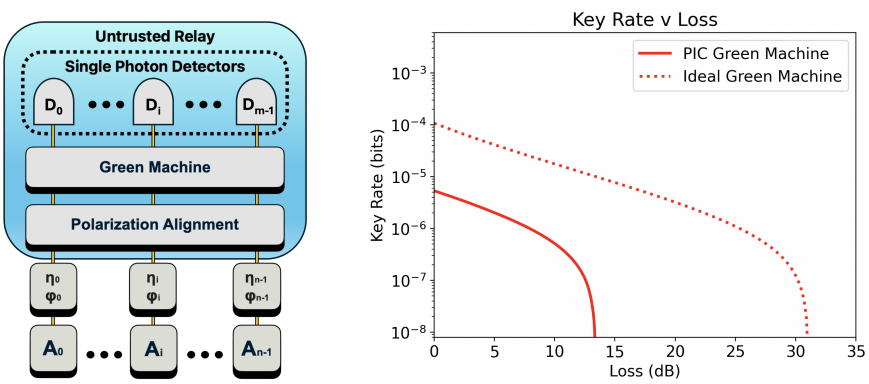
Fig. 1: (a) Layout of the Green Machine comprised of 50/50 directional couplers and 100/0 crossover couplers. (b) Microscope image of a Green Machine fabricated in silicon nitride on silicon dioxide. (c) Theoretical (solid lines) and experimental (data markers) frequency dependent power output from four selected channels when power launched into channel 8. Solid lines represent a full-wave simulation of photonic chip. Markers represent experimental data used to compose the digital twin.

A passive linear optical Green Machine device was fabricated using a silicon nitride on silicon platform. The chip has a 4 μm buried oxide (BOX) layer, close to the available standards in commercial SOI. Green Machine devices optimized for operation at 1550nm and 1585nm were packaged utilizing fiber arrays secured to the PIC with an adaptive curing technique for optimal coupling [3]. The power transmission characteristics of the Green Machine were characterized with a Santec TSL550 laser polarized to TE and measured using Thorlabs DET10C2 detectors. The result of a wavelength sweep on one of the Green Machine ports is shown in Fig 1(c).

We measured the loss of the 1550nm Green Machine to be between 6.7 and 7.8dB loss per channel from input to output. A lower loss of 3.5dB was achieved for a limited number of channels on the 1585nm Green Machine

Package; this represents the current experimental minimum coupling loss for these chips and methods.

In order to utilize our 1550nm Green Machine for QCKA, we implement a protocol developed by Carrara et al [1]. This protocol involves n parties all connected to a central, untrusted relay, as shown in Fig. 2(a). To generate a key, parties switch between key generation (KG) and decoy-state phase estimation (PE) rounds. In a KG round, n parties randomly send coherent state $|\alpha_i\rangle$ or $|-\alpha_i\rangle$ through a quantum channel to a central node. The parties store the state they sent as $x_i \in \{-1, 1\}$. These values are later used to generate a shared key. At the central node, the incoming signals are interfered in an m mode Green Machine, where m is a power of 2 greater than n. Afterwards, threshold detectors obtain and broadcast the detection pattern, and a component of a secret key is generated only when a single detector D_j clicks.



(a) (b)

Fig. 2: (a) QCKA protocol in which n parties connect to a central relay that utilizes an m-mode Green Machine and m single photon detectors to generate a shared key. (b) Key Rates for the Ideal and PIC Green Machines.

In addition to building a PIC Green Machine, our method goes beyond previous work by utilizing a digital twin to produce asymptotic key rates for a general imperfect device characterized by an S-parameter matrix. Our digital twin is composed of three pieces: transmission to the central relay, the Green Machine, and the single photon detectors. Transmission is simulated using parameters such as the loss η_i, the phase error φ_i of each party relative to A_0, and the polarization error θ_i of each party relative to A_0. We created a digital twin of the entire system by combining S-parameters measured from the PIC Green Machine at 1549nm as shown in Fig. 1(c) and simulated S-parameters for the other components using Simphony [4], a quantum photonics simulator for the evolution of Gaussian quantum states. After obtaining our composite quantum state at the single photon detectors, $|\Psi_{spd}\rangle$, we decompose it into the fock basis using The Walrus, a python library for Gaussian quantum state calculations [5]. With this quantum state, we simulate single photon detectors with quantum efficiency η_q and dark count rate p_d.

To simulate key rates, we used the following parameters: $n = 5$, $m = 8$, $\varphi_i = .1745$, $\theta_i = .1745$, $p_d = 10^{-8}$, and $\eta_q = .85$. These values were chosen to represent a configuration that is possible to realize experimentally with current technology. In order to find the maximum key rate for a specific configuration of parameters, α_i must be optimized to increase shared information while minimizing a potential eavesdropper's information. Fig. 2(b) shows the asymptotic key rate per KG round for ideal and PIC Green Machines given the loss between each party and the central relay. As shown, our PIC Green Machine has non-zero key rates up to a loss of 13.4 dB between each party and the central relay.

References

1. G. Carrara, G. Murta, and F. Grasselli, "Overcoming Fundamental Bounds on Quantum Conference Key Agreement," *Phys. Rev. Appl.*, vol. 19, p. 064017, June 2023. Publisher: American Physical Society.
2. S. Guha, "Structured optical receivers to attain superadditive capacity and the holevo limit," *Physical Review Letters*, vol. 106, jun 2011.
3. L. Carroll, J.-S. Lee, C. Scarcella, K. Gradkowski, M. Duperron, H. Lu, Y. Zhao, C. Eason, P. Morrissey, M. Rensing, S. Collins, H. Y. Hwang, and P. O'Brien, "Photonic packaging: Transforming silicon photonic integrated circuits into photonic devices," *Applied Sciences*, vol. 6, no. 12, 2016.
4. C. Carver, A. Probst, B. Arnesen, B. Fisher, T. Stowell, and R. M. Camacho, "Device-aware quantum photonic simulator for gaussian states," in *Frontiers in Optics + Laser Science 2022 (FIO, LS)*, p. JTu4A.32, Optica Publishing Group, 2022.
5. B. Gupt, J. Izaac, and N. Quesada, "The walrus: a library for the calculation of hafnians, hermite polynomials and gaussian boson sampling," *Journal of Open Source Software*, vol. 4, no. 44, p. 1705, 2019.