Security at the Speed of Light: Countering Cyberattacks via Novel On-Chip Photonic Protocols

Pate, Jeremiah

Last year, over 556 million people were victims of cyberattacks, equating to a socioeconomic impact topping $1 trillion. Malicious data breaches pose peril to national security, medical devices, power grids and nuclear stockpiles. Quantum photonic protocols transmit information with provable security, allowing the data to be its own defense; however, practicality issues have plagued this emergent photonic technology. This project explores continuous variable quantum protocols that are aligned with current data communication and do not rely upon expensive devices. Squeezed-light allows for the reduction of noise, enabling attempted breaches to be detected through an increase in noise/error rate. Finite-Difference Time-Domain (FDTD) simulations were used to design a four-wave mixing system for generation of squeezed-states of light; computer simulations measured my protocol's resilience against collective attacks, the strongest attacks against any quantum protocol. An iterative engineering approach was used between numerical and physical testing. A tabletop device, centered upon an Acousto-Optic Modulator and Mach-Zehnder interferometer, was designed for physical implementation. A genetic algorithm multi-objective optimization improved the protocol. Physical experimentation concurred with numerical analysis. This protocol was robust against attacks, even when detector imperfections and realistic fiber optic channels were taken into account. This protocol can be transmitted over 100 kilometers and included into existing fiber optic infrastructure. The resulting system will be integrated onto a photonic chip which performs real-time analysis through post-processing. This novel, six-state protocol is a viable solution to the current cyber-security impasse.

Awards Won:

SPIE, the international society for optics and photonics: Third Award of $1,000