Contribution ID: **363** Type: **Poster Presentation**

Optimal Attacks on a High-Dimensional QKD System

Thursday, 28 June 2018 15:00 (2 hours)

Quantum Key Distribution (QKD) has received a lot of attention from the cryptographic community since it's inception in the early 1970s, owing to it's ability to be provably secure. Unlike classical key distribution, whose security relies on the inability of current computers to efficiently solve certain difficult mathematical problems, QKD's security is based on the laws of quantum mechanics. With the looming advent of quantum computers (which are capable of solving these difficult math problems in polynomial time) there is raised awareness that we need to start thinking of more secure cryptographic schemes to protect data from ever more powerful adversaries. The study of quantum hacking, which tries to undermine the security of QKD protocols, is thus a necessary pursuit towards making QKD a practical tool for encryption in the future.

Here, we propose a novel attack on a high-dimensional entanglement-based QKD protocol which uses entangled modes of orbital angular momentum (OAM) as qubits. It is well known that propagating OAM modes through turbulence has the effect of spreading the modes into different OAM sub-spaces. We ask whether/how an adversary who has access to these untapped OAM sub-spaces is able to make educated guesses to determine which qubits were sent between communication parties.

Please confirm that you
have carefully read the
abstract submission instructions
under the menu item
"Call for Abstracts"
(Yes / No)

Yes

Consideration for
student awards
Choose one option
from those below.
N/A
Hons
MSc
PhD

MSc

Supervisor details
If not a student, type N/A.
Student abstract submision
requires supervisor permission:
please give their name,
 institution and email address.

Prof. Andrew Forbes, University of the Witwatersrand, andrew.forbes@wits.ac.za

Primary author: Mr PINNELL, Jonathan (University of the Witwatersrand)

Co-authors: Prof. FORBES, Andrew (U. Witwatersrand); Mr NAPE, Isaac (Structured Light Lab, School of Physics, University of Witwatersrand)

Presenter: Mr PINNELL, Jonathan (University of the Witwatersrand)

Session Classification: Poster Session 2

Track Classification: Track C - Photonics