Modeling Entanglement-Based Quantum Key Distribution for the NASA Quantum Communications Analysis Suite

Michael J. P. Kuban, Ian R. Nemitz, Yousef K. Chahine
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

***Abstract* – One of the most practical, and sought after, applications of quantum mechanics in the field of information science is the use of entanglement distribution to communicate quantum information effectively. Similar to the continued improvements of functional quantum computers over the past decade, advances in demonstrations of entanglement distribution over long distances may enable new applications in aeronautics and space communications. The existing NASA Quantum Communications Analysis Suite (NQCAS) software models such applications, but limited experimental data exists to verify the model's theoretical results. There is, however, a large body of experimental data in the relevant literature for entanglement-based quantum key distribution (QKD). This paper details a Monte Carlo-based QKD model that uses NQCAS input parameters to generate an estimated QKD link budget for verification of NQCAS. The model generates link budget statistics like key rates, error rates, and S values that can then be compared to the experimental values in the literature. Preliminary comparisons show many similarities between the simulated and experimental data, supporting the model's validity. A verified NQCAS model will inform experimental work conducted in Glenn Research Center's (GRC) NASA Quantum Metrology Laboratory (NQML), supporting the United States Quantum Initiative and potential NASA missions.**

Nomenclature –
NQCAS- NASA Quantum Communications Analysis Suite
QKD- Quantum Key Distribution
NQML- NASA Quantum Metrology Laboratory
QISE- Quantum Information Science and Engineering
RF- Radio Frequency
FSO- Free Space Optical
SPDC- Spontaneous Parametric Down-Conversion
EPR- Einstein-Podolsky-Rosen
CHSH- Clauser-Horne-Shimony-Holt
QBER- Quantum Bit Error Rate
PNR- Photon Number Resolution
POVM- Positive Operator-Valued Measure
CW- Continuous-Wave

Roadmap – This paper begins with a brief introduction to QKD and the model's justification in Section I. This is followed by a thorough description of the model's implementation in Section II. Preliminary data gathered from the simulation and the associated analysis can be found in Section III. Concluding remarks and future work can be found in Section IV. Finally, specific calculations mentioned in the paper can be found in Section V.

I. INTRODUCTION

Section I is meant to provide a pedagogical overview of quantum key distribution (QKD), as well as justification for the associated NASA Quantum Communications Analysis Suite (NQCAS) verification model. It begins by describing the theory behind QKD and the reasons for its popularity, then it moves on to a description of a common entanglement-based QKD protocol known as E91. Finally, it concludes with a description of why modeling this process is important for both NQCAS and for NASA as a whole.

A. QKD Background

The field of quantum information science and engineering (QISE) has become a priority for governmental, academic, and commercial research, with work in associated fields increasing rapidly [1], [2]. The National Quantum Initiative Act, signed into law in late 2018, provides a framework "to accelerate quantum research and development for the economic and national security of the United States" [2], encouraging universities to accelerate their efforts to increase the nation's QISE capabilities through a grand unification of quantum computing algorithms [3] and deeper dives into quantum networking [4]. Meanwhile, commercial entities are focusing more and more on the development of fault-tolerant quantum computers [5] and quantum AI [6].

The rise of viable quantum computers brings into question the sustainability of classical encryption methods. Most classical encryption methods rely on the mathematical complexity of large integer factorization to ensure security [7]; a complexity that may well become trivial with novel quantum phase estimation algorithms [8].

To resolve this issue, quantum cryptography was first introduced by Stephen Wiesner in 1983 [9], and then it was popularized about a year later with the first specific QKD protocol [10]. The main advantage of QKD is that it encodes information in properties of the individual quanta used for transmission instead of distributing classical information through radio frequency (RF) or free-space optical (FSO) signal modulation [11]. These quantum properties protect the encoded information from eavesdropper attacks via the Heisenberg Uncertainty Principle [12] and the No-Cloning Theorem [13], both of which are foundational principles in quantum mechanics. While there are a number of potentially "quantum resistant" algorithms [14] [15], the fact that QKD attributes its security to fundamental physical principles instead of computational complexity allows the QKD-based