Advances in Chip-Based Quantum Key Distribution

By

HENRY SEMENENKO

Department of Physics
UNIVERSITY OF BRISTOL

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of DOCTOR OF PHILOSOPHY in the Faculty of Science.

SEPTEMBER 2019

Word count: ten thousand and four

Abstract

Here goes the abstract

Acknowledgements

Here goes the dedication.

AUTHOR'S DECLARATION

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: ..... DATE: .....

Table of Contents

LIST OF TABLES

TABLE **Page**

List of Figures

Figure **Page**

Chapter 1

Introduction

CHAPTER 2

BACKGROUND

2.1 Cryptography

The idea of obscuring messages from third-party onlookers dates back (as far as we can tell) to ancient Egypt. With the convenience of being able to share thoughts through written methods came with an immediate compromise to security.

2.1.1 Symmetric Key Encryption

2.1.2 Public Key Cryptography

A more practical method of encrypting data is to

2.2 Quantum Theory

2.2.1 Quantum Information

2.2.2 Quantum Photonics

2.3 Quantum Key Distribution

BB84 [1]. Shor [2].

2.3.1 Protocols

Point-to-Point

Device Independence

2.3.2 Hacking

2.4 Integrated Photonics Devices

2.4.1 Requirements

2.4.2 Indium Phosphide

2.4.3 Silicon on Insulator

2.4.4 Integrated Detectors

2.5 Summary

CHAPTER 3

HONG-OU-MANDEL INTERFERENCE BETWEEN INTEGRATED DEVICES

Hong-Ou-Mandel (HOM) interference is a fundamental tool in any quantum engineering toolbox. It underpins a range of processes ranging from computing to communication. While it is well understood, generating states for quantum interference at the GHz speeds required for modern telecommunication remains practically challenging.

3.1 Sources and Requirements

Several methods can be conceived to generate weak coherent pulses (WCPs)

3.2 Experiment

3.3 Results

3.3.1 Hong-Ou-Mandel Interference Between GHZ Coherent States

3.3.2 Phase Coherence

3.4 Outlook

CHAPTER 4

CHIP-BASED MEASUREMENT-DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

4.1 MDI-QKD Protocol

4.2 Integrated Transmitters

4.3 Results

4.4 Outlook

CHAPTER 5

FULLY INTEGRATED QUANTUM KEY DISTRIBUTION

5.1 QKD Metropolitan Network Requirements

5.2 Receiver Device

5.3 Experimental Setup

5.4 Results

5.5 Outlook

CHAPTER 6

LASER SEEDING

6.1 QKD Transmitters Requirements

6.2 Test Device

6.3 Results

6.4 Outlook

CHAPTER 7

CONCLUSION

BIBLIOGRAPHY

[1] C. H. BENNETT AND G. BRASSARD, *Quantum cryptography: Public key distribution and coin tossing*, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, New York, 1985, IEEE, pp. 175–179.

3

[2] P. W. SHOR, *Algorithms for quantum computation: Discrete logarithms and factoring*, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, SFCS '94, Washington, DC, USA, 1994, IEEE Computer Society, pp. 124–134.

3