UNIVERSITI PUTRA MALAYSIA

DEVELOPMENT OF AUTHENTICATION CODE BASED ON SPECTRAL AMPLITUDE CODING OPTICAL CODE DIVISION MULTIPLEXING FOR MULTI-USER PSEUDO QUANTUM KEY DISTRIBUTION

TAIWO AMBALI ABIOLA

DEVELOPMENT OF AUTHENTICATION CODE BASED ON SPECTRAL AMPLITUDE CODING OPTICAL CODE DIVISION MULTIPLEXING FOR MULTI-USER PSEUDO QUANTUM KEY DISTRIBUTION

By

TAIWO AMBALI ABIOLA

Thesis submitted to the School of Graduate Studies, University Putra Malaysia, in fulfilment of the Requirements for the Degree of Doctor of Philosophy

April 2018

DEDICATION

The work is dedicated to my entire family for their immense contribution and for making the study worthwhile

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

DEVELOPMENT OF AUTHENTICATION CODE BASED ON SPECTRAL AMPLITUDE CODING - OPTICAL CODE DIVISION MULTIPLEXING FOR MULTI-USER PSEUDO QUANTUM KEY DISTRIBUTION

By

TAIWO AMBALI ABIOLA

April 2018

Chairman : **Makhfudzah Mokhtar, PhD**

Faculty : **Engineering**

Quantum Key Distribution (QKD) has remained the provable technique of ensuring secure communication amidst the impending security threat by the emerging quantum computers. Its security guarantee is based on superposition and entanglement, which are fundamental principle of quantum mechanics.

As efforts are currently underway toward actualization of QKD network, researchers have explored a number of techniques though which this could be achieved. Some of the techniques proposed are; subcarrier based QKD network, Orthogonal Frequency Division Multiplexed (OFDM) based QKD network and spectral amplitude coding optical code division multiplexed (SAC-OCDMA) based QKD network. Among the aforementioned technique, SAC-OCDMA based system has history of efficient channel management, asynchronous nature, as well as channel security. Nevertheless, the adopted Optical Orthogonal Code (OOC) which is a family of OCDMA code, has a couple of challenges which include complex architecture, as well as longer code length, both of which are capable of resulting to reduction in the secure key rate and number of simultaneous users.

Thus, this work presents a new one-weight authentication code, which are assigned, uniquely to individual user in SAC-OCDMA based QKD network. The performance of the code was explored in QKD network using simulation, mathematics and laboratory experiment. Firstly, the proof of concept of plug and play (p&p) in QKD network was carried out and the concept of phase reorientation was clearly established using Optisystem simulation tool. This was followed by mathematical modelling of the secure key rate and QBER for different number of users. As observed in the obtained results, at an average mean photon number of 0.48, a 21-user network was achieved at a secure key rate of 24 bps over a distance of 5 km. The result of comparison of the proposed code with a Wavelength Division Multiplexed (WDM) system shows its security capability above the later. The code was further compared with an OOC based network and found to generate key at higher rate when the number of users is below 14. A two-user experimental result shows the real life realization of the proposed system as a transmission distance up to 40 km was achieved with secure key rate of 320 bps. Application of the proposed code in Differential Phase Shift Key – Quantum Key Distribution (DPS-QKD) environment was also established.

The obtained results have shown that aside presenting a secure mechanism, the design flexibility and moderate code length exhibited by the proposed code are excellent factors that could be explored in enhancing the performance of QKD network.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PEMBANGUNAN KOD PENGESAHAN BERASASKAN PENGEKODAN AMPLITUD SPEKTRUM - MULTIPLEKS PEMBAHAGI KOD OPTIK UNTUK RANGKAIAN PENGAGIHAN PSEUDO KUANTUM PELBAGAI PENGGUNA

Oleh

TAIWO AMBALI ABIOLA

April 2018

Pengerusi : Makhfudzah Mokhtar, PhD

Fakulti : Kujuruteraan

Teknik Pengagihan Kunci Kuantum (QKD) masih kekal sebagai teknik yang terbukti dapat menjamin persekitaran komunikasi yang selamat menjelang ancaman keselamatan yang akan berlaku di masa akan datang oleh komputer kuantum. Jaminan keselamatannya didasarkan pada tindihan dan keterlibatan, yang merupakan prinsip asas mekanik kuantum.

Sejajar dengan pelbagai usaha yang sedang giat dijalankan ke arah pelaksanaan rangkaian QKD, para penyelidik telah menerokai beberapa teknik bagi merealisasikan matlamat ini. Beberapa teknik yang dicadangkan adalah; rangkaian QKD berasaskan sub-pembawa, rangkaian QKD Multipleks Pembahagi Frekuensi Ortogon (OFDM) dan Pengekodan Amplitud Spektrum - Multipleks Pembahagi Kod Optik (SAC-OCDMA). Antara teknik yang disebutkan di atas, sistem berasaskan SAC-OCDMA mempunyai sejarah pengurusan saluran yang cekap, sifat tak segerak serta keselamatan saluran. Walau bagaimanapun, Kod Ortogonal Optik (OOC) yang diguna pakai, yang merupakan keluarga kod SAC-OCDMA mempunyai beberapa cabaran yang merangkumi seni bina kompleks, dan juga kod yang panjang, dimana memberi cabaran kepada capaian persekitaran yang selamat dan bilangan pengguna secaraserentak.

Maka, kajian ini mencadangkan satu kod pengesahan yang baru kepada pengguna individu dalam rangkaian QKD berasaskan SAC-OCDMA. Prestasi kod ini diterokai dalam rangkaian QKD menggunakan simulasi, persamaan matematik dan eksperimen makmal. Pertama, konsep pembuktian dalam rangkaian sumbat dan pasang (p&p) QKD dijalankan, dan konsep fasa pengorentasian diperjelaskan dengan menggunakan perisian simulasi Optisystem. Ini diikuti dengan pemodelan matematik bagi kadar kunci yang selamat dan Kuantum Kadar Bit Ralat (QBER) untuk bilangan pengguna yang berbeza. Keputusan eksperimen yang diperolehi menunjukkan, pada purata bilangan foton 0.48, 21-pengguna dalam rangkaian dicapai pada kadar kunci selamat 24 bps sepanjang jarak 5 km. Hasil perbandingan kod yang dicadangkan dengan sistem Multipleks Pembahagi Panjang Gelombang (WDM) menunjukkan keupayaan keselamatannya adalah jauh lebih baik. Kod ini seterusnya diuji dengan rangkaian berasaskan OOC dan didapati mampu menghasilkan kunci pada kadar yang lebih tinggi apabila bilangan pengguna berada di bawah 14. Hasil dari kajian yang dicadangkan menunjukkan ia mampu direalisasi dalam kehidupan seharian dengan mencapai jarak penghantaran sehingga 40 km pada kadar kunci selamat sebanyak 320 bps. Penggunaan kod di dalam persekitaran Anjakan Fasa Kebezaan – Kuantum Pengagihan Kekunci (DPS-QKD) juga telah dilaksanakan.

Hasil yang diperoleh dari teknik kod yang dicadangkan menunjukkan bahawa selain mempunyai mekanisme yang selamat, reka bentuk kod yang fleksibel dan panjang kod sederhana yang dipamerkan menjadi faktor yang sangat baik yang boleh diterokai dalam meningkatkan prestasi rangkaian QKD.

ACKNOWLEDGEMENTS

All praises and adorations are to Almighty Allah, the eternal, who made the study a successful one.

My heartfelt gratitude goes to my supervisor, Dr. Makhfudzha Mokhtar, for the kindhearted relationship she established with me right from the time of my arrival in UPM. The same is extended to the committee members in persons of Prof. Adzir Mahdi, Dr. Abu Bakar Hafiz and Dr. Fared Abu Khir. I pray to Almighty Allah to reward you all in abundance.

I must commend the efforts and sacrifice of my wife and little daughter, Aneesah, towards the success of the program. I appreciate the good spirit demonstrated in the course of the study. May Almighty God let us reap the fruit of the sacrifice.

The unquantifiable contribution of my family members starting from my immediate elder brother, Alhaji Sulaiman, who personally took the responsibility of sponsoring my study in Malaysia deserved an inimitable appreciation. Also the rest of my family who have in one way or the other contributed either financial or through moral words of advice. May Allah grant you your entire requests.

I must commend the support of my colleagues in the study room, friends in Malaysia and in Nigeria for your good relationship. I pray Almighty God will see you through in your various endeavors.

I pray for my late parents for their immeasurable contribution to my life right from my childhood till their demise. May Allah overlook their shortcomings and guide them to the Paradise.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Masters of Science. The members of the Supervisory Committee were as follows:

Makhfudzah Binti Mokhtar, PhD
Senior Lecturer
Faculty of Engineering
University Putra Malaysia
(Chairman)

Mohd Adzir Mahdi, PhD
Professor
Faculty of Engineering
University Putra Malaysia
(Member)

Mohd Hafiz Abu Bakar, PhD
Associate Professor
Faculty of Engineering
University Putra Malaysia
(Member)

Mohd Fared Abu Khir, PhD
Senior Lecturer
Faculty of Science and Technology
Universiti Science Islam Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or currently for any degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-own by Universiti Putra Malaysia, as according to the University Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Dean Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings seminar papers manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated the Universiti Putra Malaysia (Research) rules 2012;
- There is no plagiarism or data falsification/ fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the University Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ______________________________ Date: ____________________

Name and Matric No.: Taiwo Ambali Abiola, GS41445

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012 – 2013) are adhered to.

Signature: ______________________________
Name of Chairman of Supervisory Committee: ______________________________

Signature: ______________________________
Name of Member of Supervisory Committee: ______________________________

Signature: ______________________________
Name of Member of Supervisory Committee: ______________________________

Signature: ______________________________
Name of Member of Supervisory Committee: ______________________________

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advance Encryption Standard
APD	Avalanche Photodiode
AT&T	American Telephone & Telegraph
B92	Bennett (1992)
BB84	Bennett and Brassard (1984)
BBO	Barium Beta-Borate
COW	Coherent One Way protocol
CSA	Cloud Security Alliance
DES	Data Encryption Standard
DFB	Distributed Field back
DPSK	Differential Phase Shift Key
E91	Ekert (1991)
FTTH	Fiber To The Home
FWHM	Full Width at Half Maximum
IBM	International Business Machine
IDQ	ID Quantique
InGaAs	Indium Gallium Arsenate
IR	Intercept Resend
LED	Light Emitting Diode
LM05	Lucamarini M 2005
MAI	Multiple Access Interference
OCDMA	Optical Code Division Multiple Access
OFDM	Orthogonal Frequency Division Multiplexing
OOC	Optical Orthogonal Code
OTBF	Optical Tunable Bandpass Filter
OTP	One-Time Pad
PBS	Polarization Beam Splitter
PDC	Parametric down conversion

PIIN	Phase Induced Intensity Noise
PIN	Positive Intrinsic Negative
PNS	Photon Number Splitting
P&P	Plug and Play
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QSSWG	Quantum-Safe Security Working Group
QuBit	Quantum Bit
RF	Radio Frequency
S09	Serna (2009)
S13	Serna (201)
SAC-OCDMA	Spectral Amplitude Coding Optical Code Division Multiplexing
SAPD	Single Avalanche Photon Diode
SARG04	Scarani, Acin, Ribordy & Gisin (2004)
SMS	Short Message Service
TDM	Time Division Multiplexing
TBF	Tunable bandpass filter
USB	Universal Serial Bus
VOA	Variable Optical Attenuator
WDM	Wavelength Division Multiplexing
XOR	Exclusive OR

CHAPTER 1

INTRODUCTION

1.1 Background Information

Excessive demand for high processing speed and compactness, as the world migrates from paper based to digital age, have been a major driving factor for microprocessor industries to strive for more miniature and high capacity semiconductor devices. According to Gordon Moore, an Intel corporation co-founder, "The number of transistor incorporated in a chip will approximately double every 24 months" [1][2][3]. This miniature in size with high speed become apparent in ever-growing generations of computer from vacuum tube in mid-19th century to artificial intelligence phase in 2010, [4]. Records however have it that between 2020 and 2025, transistor-based microprocessor will have been extremely small and end up generating excessive heat beyond which silicon semiconductor could tolerate. Hence, in quest to further meet up the excessive demand, great effort are being put in place towards development of quantum computers [5][6][7].

Quantum computers are computer systems that perform operations on data using quantum mechanics phenomena of entanglement and superposition [8][9]. As demonstrated by Peter Shor, a computer scientist with AT&T in 1994, a quantum computer will be able to process large amount of information within a very short time compare to the current classical systems that are not capable of factorizing numbers above 512 digits [5], [10], [11].

As efforts are underway towards actual realization of the quantum computers, researchers have identified the impending challenges, which the anticipated computer will pose on the current security system being used. It is a general knowledge that the current states of art in information security absolutely rely on the mathematical complexity involved in their algorithm [12][13], taking advantage of the limited processing capacity of the current computer. However, with the emerging quantum computing, the security system would be vulnerable as the attacker might take advantage of the processing power of the anticipated quantum computer. In view of this, a number of works, including Quantum-Safe Security Working Group (QSSWG) headed by Bruno Huttler, which is a subgroup of Cloud Security Alliance [14], have identified quantum key distribution as a security system for combating the impending security loopholes that would be created by the advent of quantum computer.

Quantum Key Distribution (QKD) is a technology involving sharing of security key between two legitimate parties using fundamental law of physics [12][15]. Concisely, the parties involved can securely disseminate information using cryptography key that are generated by law of quantum mechanics. The protocol has been proven to be secured even in the presence of the most powerful computer system [7], [16]–[20]. The security emanates from the fact that the presence of the eavesdroppers would be easily known as quantum state does not remain the same when a measurement is performed on it. A number of QKD protocols have been proposed with one succeeding others due to emanating loopholes in the later. These include Bennett and Brassard (BB84) [21]–[23], which is often regarded as the backbone of all protocols. Others are Scarani, Acin, Ribordy & Gisin (SARG04) [24]–[26], Ekert 1991 (E91) , Bennett 1992 (B92) [27], Lucamarini M 2005 (LM05), Serna 2009 (S09), Serna 2013 (S13), Coherent One Way protocol (COW), decoy protocol, Differential Phase Shift Key (DPSK-QKD) [14], [28]–[32] and many others.

In spite of the magnificent of its security, researcher have identified a number of ways by which QKD can be vulnerable to attack. Some of the identified challenges are Intercept and Resend (IR) attack and Photon Number Splitting (PNS) attacks, both of which often take place in the channel. PNS attack is a form of attack that is peculiar to BB84 protocols [33]–[36]. Since researchers are still facing difficult time in manufacturing single photon light source, most of the experimental work that have been implemented were achieved using weak coherent laser source. As weak coherent lasers dispense pulses based on established Poisson distribution, there are possibility that the eavesdroppers, in attempt to launch attack on the system, may explore the occasional release of multiple pulse. In an attempt to prevent these, protocols such as SARG04, decoy state protocol, DPSK-QKD protocols and many more, which would be addressed in the next chapter, were proposed.

The latest trends in QKD development are indisputably exploring the multi-user ability of the system. In an establishment with several sections within a certain location, each user requires a distinctive way of identification with minimal resources.

1.2 Problem Statement

Researchers in the past have explored Wavelength Division Multiplexing (WDM) [37] [38] and Time Division Multiplexing (TDM) [39] [40]. These are either challenged with channel insecurity as in the case of the former or low scanning speed, which could hinder transmission speed in the case of later. Subcarrier QKD multiplexing was proposed in [41] and further developed in [42][43]. The technique, which saw bands of frequencies used in modulating the weak pulse laser, was subsequently experimented for two users in [44]. Its low key rate was due to complexity in the system design. Subsequent work include Orthogonal Frequency Division Multiplexing of QKD (OFDM-QKD) [45] proposed in 2015. The system recorded better performance only with activate decoding technique which subsequently add to the cost and complexity of the design. A similar challenges is peculiar to OCDMA based multi-user QKD [46].

In the midst of the aforementioned QKD networks, OCDMA [46] based system has been a center of attraction due to a number of advantages it has over others, including . Records have shown that the technology has history of efficient channel management, asynchronous nature, as well as capability to maintain channel security [47][48][49]. Recently, Razavi proposed a trilling OCDMA based QKD technique [46]. In the work, the researcher established that the system could have optimal performance if implemented with a one-weight code as shown in Figure 1.1. Nevertheless, Optical Orthogonal Code (OOC) was used, which cannot be achieved with one-weight, and has complexity in its derivation [47][50]. Other challenges are excessive long code length which result in high spectral dependency on the light source [51], [52], [48] as well as series of splitting and recombination as shown in Figure 1.2 which, to the best of our knowledge, would increases the power loss and hence, decrease the secure key rate.

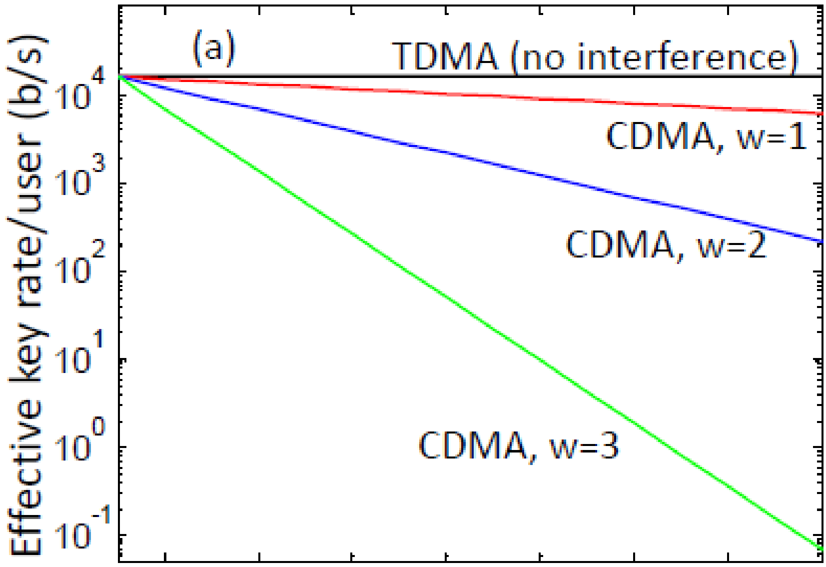

Figure 1. 1: Comparison of OOC code at different weight [46]

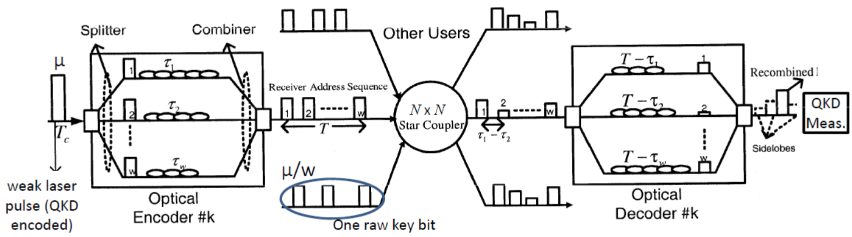

Figure 1. 2: Architecture of Passive OOC code based QKD network

1.3 Significance of the Study

As efforts are being put in place towards development of QKD networks, OCDMA technology has proven to be a promising technique, which does not only focus on getting the signals across to the right receiver but equally put the channel security into consideration. In carrying out this, there is necessity to equally consider viability and achievability of any proposed code in real life scenario. By considering flexibility in design and moderate code length which the proposed one-weight code has to offer over OOC based system, multi-user OCDMA based QKD system could be said to be approaching it final phase of commercialization. Hence, weak coherent pulses sources could be confidently used in QKD network with less security risk.

1.4 Objectives

This work aim at developing an authentication code for SAC-OCDMA based multiple user QKD system.

Specific Objectives

- To design a new authentication code for multi-user Quantum Key Distribution system.
- To implement the proposed code in plug and play QKD system using simulation tool.
- To implement the proposed design using established mathematical equation and compare the performance with the existing technology.
- To experiment the proposed code in test bed in order to explore its real life application.

1.5 Scope of the Work

This work will only focus on development of a new one-weight code for multi-user QKD system. Although the code could be adopted in any QKD system, its performance in multiple plug and play QKD system will be analyzed, based on the available idq 3000 clavis system. The performance will be analyzed using mathematical approach, simulation tool as well as experimental implementation for two users that comprise the commercial id quantic 3000 clavis system and a cloned plug and play system. The performance will be checked based on the number of supported users, the transmission distance, the obtained QBER as shown in figure 1.3 below.

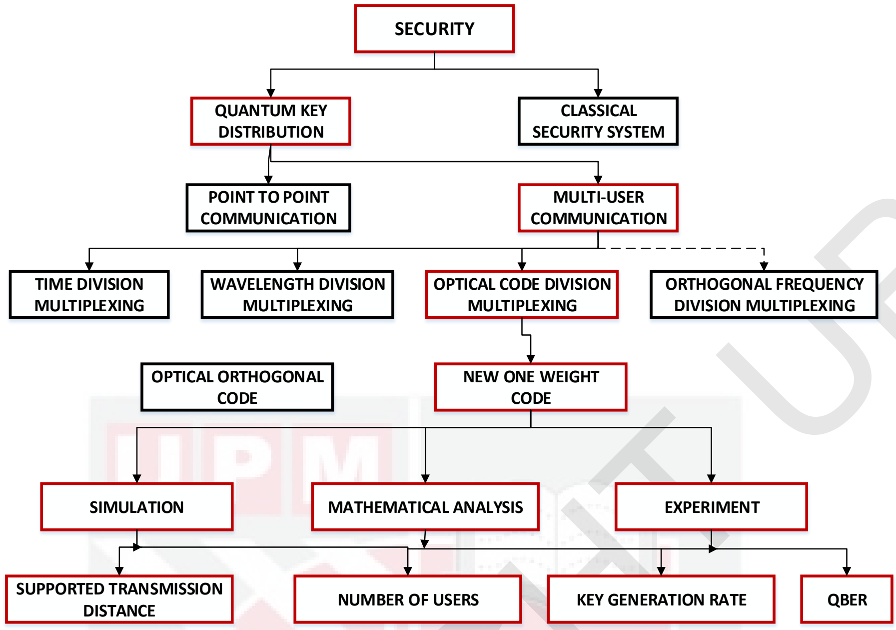

Figure 1. 3: Scope of work

1.6 Work Organization

The presented work begins with introduction, which entails the background of study, the problem statement, objectives, and the significance of the study as contained in chapter 1. This is followed by the review of the literature in chapter 2. Chapter 3 contains the proposed code derivation, and the general concept of plug and play QKD system. The simulation design is vividly explained in chapter 4 while chapter 5 contains the mathematical derivation of the proposed system. This is followed by the experimental work in chapter 6. Application of the proposed code in DPS-QKD system will be explored in chapter 7 while chapter 8 consist of the conclusion and recommendation.

REFERENCES

[1] D. Sadowy, "New microprocessor features for lower power and increased performance: Doing 'Moore's' with less," in *IEEE International Symposium on Electronics and the Environment*, 2005, pp. 146–150.

[2] C. G. Hwang, "New paradigms in the silicon industry," in *Technical Digest - International Electron Devices Meeting, IEDM*, 2006, pp. 1–8.

[3] G. D. Hutcheson, "The Economic Implications of Moore ' s Law," in *Intro to Nano Era*, 1st ed., Berlin, Heidelberg: Springer Series in Materials Science, 1965, pp. 11–14.

[4] D. Burns, "The five generations of computers," *Business to Business*, 2016. [Online]. Available: http://btob.co.nz/business-news/five-generations-computers/. [Accessed: 03-May-2017].

[5] Y. Zhao, X. Chen, Z. Shi, F. Zhou, S. Xiang, and K. Song, "Implementation of One-Way Quantum Computing with a Hybrid Solid-State Quantum System," *Chinese J. Electron.*, vol. 26, no. 1, pp. 27–34, 2017.

[6] J. Singhl and M. Singh, "Evolution in Quantum Computing," in *International conference on System Modeling & Advancement in Reserach Trend*, 2016, pp. 1–4.

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," *Rev. Moden Phys.*, vol. 81, no. 3, pp. 1–52, 2009.

[8] F. Rossi, "The Excitonic Quantum Computer," *IEEE Trans. Nanotechnol.*, vol. 3, no. 1 SPEC. ISS., pp. 165–172, 2004.

[9] H. E. Ruda and B. I. Qiao, "Modeling and prospects for a solid-state quantum computer," *Proc. IEEE*, vol. 91, no. 11, pp. 1874–1883, 2003.

[10] B. Skuse, "The trouble with Quantum Computing," *IET Journal & Magazine*, pp. 54–57, 2016.

[11] M. Knights, "The art of Quantum Computing," *Engineering and Technology*, pp. 30–34, 2007.

[12] L. Mailloux and M. Grimaila, "Performance evaluations of quantum key distribution system architectures," *IEEE Secur. Priv.*, vol. 1, pp. 20–40, 2015.

[13] M. Tomamichel, C. Ci, W. Lim, N. Gisin, and R. Renner, "Tight Finite-Key Analysis for Quantum Cryptography," *Nat. Commun.*, vol. 3, pp. 1–16, 2012.

[14] CSA, *What is Quantum Key Distribution ?* 2016, pp. 1–2.

[15] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Fast and user-friendly quantum key distribution," *J. Mod. Opt.*, vol. 47, no. 2–3, pp. 517–531, 2000.

[16] S. H. Lee, K. H. Jeong, S. H. Kim, and K. H. Kim, "Rayleigh Backscattering-Suppressed Two-Way Quantum Key Distribution," *J. Korean Soc.*, vol. 52, no. 1, pp. 5–10, 2008.

[17] G. Van Assche, *Quantum Cryptography and Secret-Key Distillation*. New York: Cambridge University Press, 2006.

[18] J. Gruska and C. Republik, "Quantum computing," 2004.

[19] N. G. Mcdonald, "Past , Present , and Future of Cryptography."

[20] P. Kumar, "Optical modulation schemes for frequency-coded quantum key distribution," *2010 Natl. Conf. Commun.*, pp. 1–5, Jan. 2010.

[21] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Theoretical Computer Science*, 1984, vol. 560, no. P1, pp. 7–11.

[22] Z. Yan, E. Meyer-Scott, J. P. Bourgoin, B. L. Higgins, N. Gigov, A. MacDonald, H. H??bel, and T. Jennewein, "Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links," *J. Light. Technol.*, vol. 31, no. 9, pp. 1399–1408, 2013.

[23] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, no. 19, pp. 1–3, 2005.

[24] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, p. 57901, Feb. 2004.

[25] A. L. I. Ghazali, A. F. Abas, W. Azizun, W. Adnan, M. Mokhtar, M. A. Mahdi, S. Member, and M. I. Saripan, "Security Proof of Improved-SARG04 Protocol Using the Same Four Qubit States," in *International Conference on Photonic*, 2010, pp. 0–3.

[26] X. Fang-xing and W. Shuang, "Passive decoy state SARG04 quantum-key-distribution with practical photon-number resolving detectors ∗," vol. 100312.

[27] Y.-G. Yang, S.-J. Sun, P. Xu, and J. Tian, "Flexible protocol for

quantum private query based on B92 protocol," *Quantum Inf. Process.*, vol. 13, no. 3, pp. 805–813, Dec. 2013.

[28] L. Moli-Sanchez, A. Rodriguez-Alonso, and G. Seco-Granados, "Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1582–1590, Dec. 2009.

[29] R. Renner, "Security of Quantum Key Distribution," *arXiv:quant-ph/0512258*, vol. 4, 2005.

[30] M. F. Abdul Khir, I. Bahari, M. N. Mohd Zain, and S. Shaari, "Secure communication with one decoy state and two way quantum key distribution scheme," *Malaysian J. Math. Sci.*, vol. 7, no. SUPPL.1, pp. 39–47, 2013.

[31] M. F. Khir, I. Bahari, S. Ali, and S. Shaari, "Weak+ Vacuum and One Decoy State with Two Way Quantum Key Distribution Protocol," *arXiv Prepr. arXiv1108.4756*, no. 4, pp. 11–14, 2011.

[32] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, no. 2, p. 22317, 2003.

[33] T. Nishioka, A. Soujaeff, T. Hasegawa, T. Tsurumaru, J. Abe, and S. Takeuchi, "Single-photon interference experiment over 80 km with a pulse-driven heralded single-photon source," *IEEE Photonics Technol. Lett.*, vol. 20, no. 5, pp. 354–356, 2008.

[34] L. O. Mailloux, M. R. Grimaila, J. M. Colombi, D. D. Hodson, R. D. Engle, C. V. McLaughlin, and G. Baumgartner, "Quantum key distribution: Examination of the decoy state protocol," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 24–31, 2015.

[35] A. Ruiz-Alba, J. Mora, W. Amava, A. Martinez, V. García-Muñoz, D. Calvo, and J. Capmany, "Microwave Photonics Parallel Quantum Key Distribution," *IEEE Photonics J.*, vol. 4, no. 3, pp. 931–942, Jun. 2012.

[36] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Phys. Rev. Lett.*, vol. 91, no. 5, p. 57901, Aug. 2003.

[37] K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V Penty, and A. J. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, p. 51123, 2014.

[38] W. Sun, L.-J. Wang, X.-X. Sun, H.-L. Yin, B.-X. Wang, T.-Y. Chen, and

J.-W. Pan, "Integration of quantum key distribution and gigabit-capable passive optical network based on wavelength-division multiplexing," *Quantum Physics (quant-ph)*, 2016. [Online]. Available: http://arxiv.org/abs/1604.07578.

[39] J. Martinez-mateo, A. Ciurana, and V. Martin, "Quantum Key Distribution Based on Selective Post-Processing in Passive Optical Networks," *IEEE Photonics Technol. Lett.*, vol. 26, no. 9, pp. 881–884, 2014.

[40] F. Garzia, "Comparison of 4 Multi-user Passive Network Topologies for 3 Different Quantum Key Distribution," *Commun. Netw.*, vol. 2, no. 3, pp. 166–182, 2010.

[41] A. Ortigosa-Blanch and J. Capmany, "Subcarrier multiplexing optical quantum key distribution," *Phys. Rev. A*, 2006.

[42] D. Calvo, A. Martinez, W. Amaya, J. G. Rozo, J. Mora, and J. Capmany, "Practical Quantum Key Distribution based on the BB84 protocol," *Waves*, pp. 4–14, 2011.

[43] D. S. Signal, A. Ortigosa-blanch, A. Ruiz-alba, W. Amaya, and A. Mart, "Analysis of Subcarrier Multiplexed Quantum Key Distribution Systems: Signal, Intermodulation, and Quantum Bit Error Rate," *IEEE J. Sel. Top. Quantum Electron.*, vol. 15, no. 6, pp. 1607–1621, 2009.

[44] J. Mora, A. Ruiz-alba, W. Amaya, A. Martínez, V. García-muñoz, D. Calvo, and J. Capmany, "Experimental demonstration of subcarrier multiplexed quantum key distribution system," *Opt. Lett.*, vol. 37, no. 11, pp. 2031–2033, 2012.

[45] S. Bahrani, M. Razavi, and J. A. Salehi, "Orthogonal Frequency Division Multiplexed Quantum Key Distribution Sima," *J. Light. Technol.*, vol. 33, no. 4687–4698, pp. 24–27, 2015.

[46] M. Razavi, "Multiple-Access Quantum Key Distribution Networks," *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 3071–3079, 2012.

[47] M. Moghaddasi, S. Seyedzadeh, and S. B. Ahmad Anas, "Optical Code Division Multiple Access Codes comparison in free space optics and optical fiber transmission medium," *2014 Ieee Reg. 10 Symp.*, pp. 181–184, 2014.

[48] A. Taiwo, S. Seyedzadeh, S. Taiwo, R. K. Z. Sahbudin, M. H. Yaacob, and M. Mokhtar, "Performance and comparison of fiber vibration sensing using SAC-OCDMA with direct decoding techniques," *Opt. - Int. J. Light Electron Opt.*, Jun. 2014.

[49] H. Y. Ahmed, M. Elmaleeh, H. A. Fadhil, and S. Aljunid, "Optical CDMA: Performance of spectral-amplitude coding with new direct recovery scheme using Vector Combinatorial (VC) code," *Int. Arab J. Inf. Technol.*, vol. 10, no. 5, pp. 436–443, 2013.

[50] S. Singhdeo and U. Bhanja, "Design and performance analysis of modified two dimensional Golomb code for optical code division multiple access networks," *Telecommun. Syst.*, 2018.

[51] K. S. Nisar, "Construction Zero Cross Correlation Code using Permutation Matrix for SAC-OCDMA Systems," *Int. J. Open Inf. Technol.*, vol. 4, no. 3, pp. 51–54, 2016.

[52] A. Taiwo, S. Seyedzadeh, R. K. Z. Sahbudin, M. H. Yaacob, M. Mokhtar, and S. Taiwo, "Performance comparison of OCDMA codes for quasi-distributed fiber vibration sensing," *2013 IEEE 4th Int. Conf. Photonics*, no. 3, pp. 111–113, Oct. 2013.

[53] A. Menezes, P. van Oorschot, and S. Vanstone, "Overview of Cryptography," in *Handbook of Applied Cryptography*, CRS Press, Inc., 1997, pp. 1–48.

[54] D. Kahn, *The CodeBreakers*. New York: The Macmillan Company, 1984.

[55] K. Senthil, K. Prasanthi, and R. Rajaram, "A modern avatar of Julius Ceasar and Vigenere cipher," in *2013 IEEE International Conference on Computational Intelligence and Computing Research*, 2013, pp. 1–3.

[56] A. Blair, "Learning the Caesar and Vigenere Cipher by hierarchical evolutionary re-combination," in *2013 IEEE Congress on Evolutionary Computation*, 2013, pp. 605–612.

[57] "Simple Transposition Ciphers - Crypto Corner." [Online]. Available: http://crypto.interactive-maths.com/simple-transposition-ciphers.html. [Accessed: 09-Jul-2015].

[58] M. Hendrych, "Experimental quantum cryptography," Palacky University, 2002.

[59] "McCullough J. - Caution! Wireless Networking: Preventing a Data Disaster." [Online]. Available: http://flylib.com/books/en/2.827.1.70/1/. [Accessed: 08-Jul-2015].

[60] Q. Kester, "A Hybrid Cryptosystem based on Vigenere Cipher and Columnar Transposition Cipher," *Int. J. Adv. Technol. &Engineering Res.*, vol. 3, no. 1, pp. 141–147, 2013.

[61] A. Giordana, L. Saitta, F. Bergadano, F. Brancadori, and D. D. Marchi,

"ENIGMA: a system that learns diagnostic knowledge," *IEEE Trans. Knowl. Data Eng.*, vol. 5, no. 1, pp. 15–28, 1993.

[62] D. Lenton, "Rebuilding the Bombe [Enigma code breaking machine]," *IEE Rev.*, vol. 47, no. 6, pp. 7–10, Nov. 2001.

[63] S. Cass, "A simple enigma," *IEEE Spectr.*, vol. 52, no. 1, pp. 19–20, Jan. 2015.

[64] Neil Sareen (Vanderbilt University), "The Zodiac Ciphers: Messages from a Murderer." [Online]. Available: http://www.wondersandmarvels.com/2013/02/the-zodiac-killer-ciphers.html. [Accessed: 09-Jul-2015].

[65] Patch.com, "Corey Starliper, Massachusetts Man, Claims He Cracked Zodiac Killer's Code," 2011. [Online]. Available: http://www.huffingtonpost.com/2011/07/21/corey-starliper-zodiac-killer-code_n_906092.html. [Accessed: 09-Jul-2015].

[66] D. Rijmenants, "Cipher Machines and Cryptology," *Historical and Technical Information about Crypto Machines*, 2015. [Online]. Available: http://users.telenet.be/d.rijmenants/en/onetimepad.htm. [Accessed: 21-Jul-2015].

[67] G. Zheng, G. Fang, R. Shankaran, and M. A. Orgun, "Encryption for Implantable Medical Devices Using Modified One-Time Pads," *IEEE Access*, vol. 3, pp. 825–836, 2015.

[68] N. Kostinski, K. Kravtsov, and P. R. Prucnal, "Demonstration of an All-Optical OCDMA Encryption and Decryption System With Variable Two-Code Keying," *IEEE Photonics Technol. Lett.*, vol. 20, no. 24, pp. 2045–2047, Dec. 2008.

[69] F. Busching and L. Wolf, "The Rebirth of One-Time Pads—Secure Data Transmission from BAN to Sink," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 63–71, Feb. 2015.

[70] Y.-S. Kim, "Refined Secure Network Coding Scheme with no Restriction on Coding Vectors," *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1907–1910, Nov. 2012.

[71] C. F. Fung, K. Tamaki, and H. Lo, "On the performance of two protocols: SARG04 and BB84," pp. 1–48, 2008.

[72] Y. Jeong, K. Hong, Y. Y. Kim, Y. Y. Kim, Youn-Chang Jeong, Kwan-Young Hong, Yong-Su Kim, and Yoon-Ho Kim, "Weak-pulse implementation of SARG04 quantum cryptography protocol in free space," *2008 Conf. Lasers Electro-Optics*, pp. 1–2, May 2008.

[73] H. Takesue, T. Honjo, K. Tamaki, and Y. Tokura, "Differential phase shift-quantum key distribution," *IEEE Commun. Mag.*, vol. 47, no. 5, pp. 102–106, May 2009.

[74] P. P. Y. I. S. Amiri, A. Nikoukar, A. Shahidinejad, M. Ranjbar, J. Ali, "Generation of Quantum Photon Information Using Extremely Narrow Optical Tweezers for Computer Network Communication," *GSTF J. Comput.*, vol. 2, no. 1, pp. 140–144, 2012.

[75] W. Stallings, "Cryptography and Network Security Chapter 11 Fifth Edition," 1970.

[76] M. A. Mohamed, A. S. Samarah, and M. I. F. Allah, "Optical Encryption Techniques : An Overview," *Int. J. Comput. Sci. Issues*, vol. 11, no. 4, pp. 125–129, 2014.

[77] M. Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols," 2007. [Online]. Available: http://www.cse.wustl.edu/~jain/cse571-07/index.html. [Accessed: 21-Aug-2017].

[78] L. I. Ahmad Ghazali, A. F. Abas, W. A. Wan Adnan, M. Mokhtar, M. A. Mahdi, M. I. Saripan, A. L. I. Ghazali, A. F. Abas, W. Azizun, W. Adnan, M. Mokhtar, M. A. Mahdi, S. Member, and M. I. Saripan, "Security Proof of Improved-SARG04 Protocol Using the Same Four Qubit States," in *International Conference on Photonic*, 2010, pp. 0–3.

[79] A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre," *Europhys. Lett.*, vol. 33, no. 5, pp. 335–340, 2007.

[80] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legre, and V. Makarov, "Attacks exploiting deviation of mean photon number in quantum key distribution and coin-tossing," *Nature*, p. 15, Dec. 2014.

[81] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Performance of Long-Distance Quantum Key Distribution Over 90-km Optical Links Installed in a Field Environment of Tokyo Metropolitan Area," *J. Light. Technol.*, vol. 32, no. 1, pp. 141–151, Jan. 2014.

[82] M. Gabay and S. Arnon, "Quantum Key Distribution by a Free-Space MIMO System," *J. Light. Technol.*, vol. 24, no. 8, pp. 3114–3120, 2006.

[83] S. Ali and O. Mahmoud, "Implementation of SARG04 decoy state quantum key distribution," in *2011 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 2011, pp. 86–90.

[84] D. Gobby, D. Gobby, Z. L. Yuan, Z. L. Yuan, a J. Shields, and a J. Shields, “Quantum key distribution over 122km of standard telecom fiber,” *Appl. Phys. Lett.*, vol. 84, p. 19, 2004.

[85] G. Ribordy, J. Gautier, N. Gisin, and O. Guinnard, “Automated ‘Plug & Play’ Quantum Key Distribution,” *Electron. Lett.*, vol. 34, no. 22, pp. 2116–2117, 1998.

[86] J. Capmany, A. Ortigosa-blanch, J. Mora, A. Ruiz-alba, W. Amaya, and A. Mart, “Analysis of Subcarrier Multiplexed Quantum Key Distribution System: Signal, Intermodulation, and Quantum Bit Error Rate,” *IEEE J. Sel. Top. Quantum Electron.*, vol. 15, no. 6, pp. 1607–1621, 2009.

[87] S. Ali, S. Mohammed, M. S. . Chowdhury, and A. A. Hassan, “Practical SARG04 quantum key distribution,” *Opt Quant Electron*, vol. 44, pp. 471–482, 2012.

[88] D. S. Bethune and W. P. Risk, “Autocompensating quantum cryptography,” *New J. Phys.*, vol. 4, pp. 1–18, 2002.

[89] D. Goddeau, “Quantum Cryptography,” *Read the DOC*, 2015. [Online]. Available: http://rtfm.readthedocs.io/en/latest/cryptography/quantum.html .

[90] W.-Y. Hwang, “Quantum Key Distribution with High Loss: Toward Global Secure Communication,” *Phys. Rev. Lett.*, vol. 5, no. August, pp. 1–4, 2002.

[91] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Phys. Rev. A*, vol. 72, no. 1, p. 12326, 2005.

[92] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, “Experimental Quantum Key Distribution with Decoy States,” vol. 70502, no. February, p. 4, 2005.

[93] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, “Continuous high speed coherent one-way quantum key distribution.,” *Opt. Express*, vol. 17, no. 16, pp. 13326–13334, 2009.

[94] C. Zhou, G. Wu, X. Chen, and H. Zeng, “‘Plug and play’ quantum key distribution system with differential phase shift,” *Appl. Phys. Lett.*, vol. 83, no. 9, pp. 1692–1694, 2003.

[95] K. Wen, K. Tamaki, and Y. Yamamoto, “Unconditional Security of Single-Photon Differential Phase Shift Quantum Key Distribution,” *Opt. Express*, vol. 17, no. 11, pp. 9053–9061, 2008.

[96] M. S. Skolnick, M. Hopkinson, A. Tahraoui, and J. G. Rarity, "CQED-Enhanced Single Photon Sources From InGaAs Quantum Dots," in *CLEOE-IQEC 2007*, 2002, p. 2002.

[97] M. . Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Single-Photon sources and Detectors," *Acta Med. Okayama*, vol. 67, no. 4, pp. 259–263, 2013.

[98] U. Basel, "Ideal single-photon source developed -- ScienceDaily," *sciencedaily*, 2015. [Online]. Available: https://www.sciencedaily.com/releases/2015/09/150907101211.htm. [Accessed: 25-Mar-2016].

[99] A. V. Kuhlmann, J. H. Prechtel, J. Houel, A. Ludwig, D. Reuter, A. D. Wieck, and R. J. Warburton, "Transform-limited single photons from a single quantum dot," *Nat. Commun.*, vol. 6, p. 8204, 2015.

[100] U. Basel, "Ideal single-photon source developed," *sciencedaily*, 2015. [Online]. Available: https://www.sciencedaily.com/releases/2015/09/150907101211.htm. [Accessed: 21-Aug-2017].

[101] X. Ma, C.-H. F. Fung, and H.-K. Lo, "Decoy state protocols for quantum cryptography with parametric down conversion sources Xiongfeng," *Phys. Rev. Lett.*, vol. 99, no. 18, p. 610118, 2007.

[102] T. Aichele, M. Scholz, and O. Benson, "InP/GaInP quantum dots as single-photon sources for quantum information processing," *Proc. IEEE*, vol. 95, no. 9, pp. 1791–1804, 2007.

[103] "Parametric Down-Conversion," *Institute de Fisica*, 2007. [Online]. Available: http://www.if.ufrj.br/~phsr/PHSR/PDC.htm. [Accessed: 24-Apr-2016].

[104] "Single Photon Detection Experiment - Photon Quantum Mechanics," *Photon Quantum Mechanics*, 2009. [Online]. Available: http://singlephoton.wikidot.com/single-photon-detection-experiment. [Accessed: 25-Apr-2016].

[105] P. Walther, A. Nemiroski, A. Gorshkov, A. Zibrov, and M. Lukin, "Quantum memory for long-distance and multiphoton entanglement," *SPIE Newsroom*, pp. 2–5, 2008.

[106] S. Cova, M. Ghioni, a Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection.," *Appl. Opt.*, vol. 35, no. 12, pp. 1956–76, Apr. 1996.

[107] D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J. G. Rarity, and T. Wall, "Photon counting for quantum key distribution with peltier

cooled InGaAs/InP APDs," *J. Mod. Opt.*, vol. 48, no. 13, pp. 1967–1981, 2001.

[108] H. Yuen, "Security Issues Associated With Error Correction And Privacy Amplification In Quantum Key Distribution," *Cornel University Library*, 09-Nov-2014. [Online]. Available: http://arxiv.org/abs/1411.2310. [Accessed: 20-Aug-2017].

[109] N. Gisin, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Moden Phys.*, vol. 74, no. 145, pp. 1–57, 2002.

[110] P. D. Townsend, "Quantum cryptography on multi-user optical fiber networks," *Nature*, vol. 385, p. 47, 1997.

[111] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New J. Phys.*, vol. 13, 2011.

[112] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," *J. Light. Technol.*, vol. 23, no. 1, pp. 268–276, 2005.

[113] L. Zyga, "Physicists take steps toward delivering quantum information to the home," *Physics.org*, 2011. [Online]. Available: https://phys.org/news/2011-07-physicists-quantum-home.html.

[114] T. Nishioka, H. Ishizuka, T. Hasegawa, and J. Abe, "'Circular type' quantum key distribution," *IEEE Photonics Technol. Lett.*, vol. 14, no. 4, pp. 576–578, 2002.

[115] J. Capmany and C. R. Ferna ndez-Pousa, "Analysis of Passive Optical Networks for Subcarrier Multiplexed Quantum Key Distribution," *Microw. Theory Tech. IEEE Trans.*, vol. 58, no. 11, pp. 3220–3228, 2010.

[116] A. Ruiz-Alba, D. Calvo, V. Garcia-Munoz, A. Martinez, W. Amaya, J. G. Rozo, J. Mora, and J. Capmany, "Experimental demonstration of Subcarrier Multiplexed Quantum Key Distribution system feasibility," *Int. Conf. Transparent Opt. Networks*, no. 1, pp. 1–4, 2011.

[117] J. Capmany and C. R. Fernandez-Pousa, "Impact of Third-Order Intermodulation on the Performance of Subcarrier Multiplexed Quantum Key Distribution," *J. Light. Technol.*, vol. 29, no. 20, pp. 3061–3069, Oct. 2011.

[118] J. Bogdanski, N. Rafiei, and M. Bourennane, "Multiuser quantum key distribution over telecom fiber networks," *Opt. Commun.*, vol. 282, no. 2, pp. 258–262, 2009.

[119] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H.

Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, “Field test of a practical secure communication network with decoy-state quantum cryptography,” *Opt. Express*, vol. 17, no. 8, pp. 6540–6549, 2009.

[120] M. Razavi, “Multiple-Access Quantum Key Distribution Networks,” *{IEEE} Trans. Commun.*, vol. 60, no. 10, pp. 3071–3079, 2012.

[121] “What is cryptography? - Definition from WhatIs.com.” [Online]. Available: http://searchsoftwarequality.techtarget.com/definition/cryptography. [Accessed: 05-Jul-2015].

[122] C. H. Bennett, G. Brassard, L. Salvail, and J. Smolin, “Experimental Quantum Cryptography,” 1991.

[123] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental Quantum Cryptography,” *Int. Assoc. Cryptologic Res.*, vol. 5, pp. 3–28, 1992.

[124] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum Cryptography without Bell â€™ s Theorem and Without EPR,” NY, USA, 1992.

[125] B. Korzh, N. Walenta, R. Houlmann, and H. Zbinden, “A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator,” *Opt. Express*, vol. 21, no. 17, pp. 19579–19592, 2013.

[126] C. Liu, S. Zhang, L. Zhao, P. Chen, C.-H. F. Fung, H. F. Chau, M. M. T. Loy, and S. Du, “Differential-phase-shift quantum key distribution using heralded narrow-band single photons,” *Opt. Express*, vol. 21, no. 8, p. 9505, 2013.

[127] H. Takesue, E. Diamanti, C. Honjo T. a nd Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, “Differential phase shift quantum key distribution experiment over 105km fibre,” *New J. Phys.*, vol. 7, p. 232, 2005.

[128] H. Singh, D. L. Gupta, and A. K. Singh, “Quantum Key Distribution Protocols: A Review,” *IOSR J. Comput. Eng.*, vol. 16, no. 2, pp. 1–9, 2014.

[129] M. S. Anuar, S. A. Aljunid, N. M. Saad, and S. M. Hamzah, “New design of spectral amplitude coding in OCDMA with zero cross-correlation,” *Opt. Commun.*, vol. 282, no. 14, pp. 2659–2664, 2009.

[130] T. H. Abd, S. A. Aljunid, H. A. Fadhil, R. A. Ahmad, and N. M. Saad, “Development of a new code family based on SAC-OCDMA system with large cardinality for OCDMA network,” *Opt. Fiber Technol.*, vol. 17, no. 4, pp. 273–280, 2011.

[131] A. M.K, A. S.A., A. S.B.A., S. R.K.Z., and M. M., “A New Optical Spectral

Amplitude Coding Sequence: Khazani-Syed (KS) Code Abdullah," in *International Conference on Information and Communication Technology*, 2007, no. March, pp. 266–278.

[132] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum Key Distribution over 67 km with a plug & play system," *Quantum Phys.*, vol. 4, p. 8, 2002.

[133] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, "Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses," *J. Mod. Opt.*, vol. 48, no. 13, pp. 2009–2021, 2008.

[134] C. H. Bennett, G. Brassard, C. Crkpeau, U. M. Maurer, and S. Member, "Generalized privacy amplification," *Inf. Theory, IEEE Trans.*, vol. 41, no. 6, pp. 1915–1923, 1995.

[135] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in *Advances in Cryptology - EUROCRYPT '93, LNCS 765*, 1994, pp. 410–423.

[136] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, no. 5, p. 52304, 2000.

[137] E. H. Serna, "Quantum Key Distribution From A Random Seed," *Arxiv Prepr*, vol. 2, no. 44, p. 3, 2013.

[138] T. H. Abd, S. A. Aljunid, H. A. Fadhil, I. F. Radhi, R. B. Ahmad, and M. A. Rashid, "Performance improvement of hybrid SCM SAC-OCDMA networks using multi-diagonal csode," *Sci. Res. Essays*, vol. 7, no. 11, pp. 1262–1272, 2012.

[139] H. S. Mohammed, S. A. Aljunid, H. A. Fadhil, H. Abd, R. A. Fayadh, and A. K. Rahman, "Generation of a New Hybrid Subcarrier Multiplexing – Sac-Ocdma System Based on Fso," *J. Theor. Appl. Inf. Technol.*, vol. 58, no. 2, pp. 389–396, 2013.

[140] A. Kumar, A. Dhiman, D. Kumar, and N. Kumar, "Free Space Optical Communication System under Different Weather Conditions," *IOSR J. Eng.*, vol. 3, no. 12, pp. 52–58, 2013.

[141] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, "Optimal Eavesdropping in Quantum Cryptography. I," *Phys. Rev. A*, vol. 56, p. 26, 1997.

[142] M. S. Abdullah, M. Z. Jamaludin, G. Witjaksono, and M. H. H. Mokhtar, "Analysis of pulsed laser diode driver system for multistate quantum key distribution," *Opt. Laser Technol.*, vol. 43, no. 5, pp. 978–983, 2011.

[143] K. Inoue, "Differential phase-shift quantum key distribution systems," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, 2015.