Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC)

Shafiqul Abidin [a,*], Amit Swami [b], Edwin Ramirez-Asís [c], Joseph Alvarado-Tolentino [d], Rajesh Kumar Maurya [e], Naziya Hussain [f]

[a] Department of Computer Science, Aligarh Muslim University, Aligarh, Uttar Pradesh, India
[b] Emirates College of Technology, United Arab Emirates
[c] Department of Administration and Tourism, Santiago Antúnez de Mayolo National University, USA
[d] Department of Systems and Informatics Engineering, Santiago Antúnez de Mayolo National University, USA
[e] Master of Computer Application, ABES Engineering College, Ghaziabad, India
[f] Department of Computer Science and Engineering, School of Computers, IPS Academy Indore, India

ARTICLE INFO

Article history:
Received 4 May 2021
Received in revised form 15 May 2021
Accepted 28 May 2021
Available online xxxx

Keywords:
Quantum cryptography
DARPA
IPSEC
Twisted light
Mobile cloud computing

ABSTRACT

Quantum cryptography concentrates on the solution of cryptography that is imperishable due to the reason of fortification of secrecy which is applied to the public key distribution of quantum. It is a very prominent technology in which 2 beings can securely communicate along with the sights belongings to quantum physics. However, on basis of classical level cryptography, the used encodes were bits for data. As quantum utilizes the photons or particles polarize ones for encoding the quantized property. This is presented in qubits as a unit. Transmissions depend directly on the inalienable mechanic's law of quantum for security. This paper includes detailed insight into the three most used and appreciated quantum cryptography applications that are providing its domain-wide service in the field of mobile cloud computing. These services are (it) DARPA Network, (ii) IPSEC implementation, and (iii) the twisted light HD implementation along with quantum elements, key distribution, and protocols.
© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the 1st International Conference on Computations in Materials and Applied Engineering – 2021.

1. Introduction

Einstein writes, "IT can't believe God plays the cosmos dice,"! However, quantum mechanics showed him to be mistaken and an amazing crop for new in's encryption schemes benefits from the dices that Einstein found so worrying. While most people assume that they are science fiction, quantum encryption systems now operate, with experiments shielding internet traffic in urban areas. These structures are so modern that they should take a quantum cryptography distribution (QKD) or best as its third and last insight into shaping cryptography in the 20th century [1]. To achieve perfect secrecy, it should be using Vernam ciphers, often know as one-time pads," for at least as long as this message would not repeat. In fact, sadly, it was impossible for Vernam ciphers to transmit one-time pads which would be totally confidential, completely uncommon, and one-off pads, so it was not commonly accepted. The most popular techniques today are Diffie-Hellman key exchangers and RSA prime factor algorithms. These key public techniques are omnipresent. Unlike Shannon, who thought that opponents had infinite mathematical abilities, public-key tactics presume that such mathematical functions are a way in which to do one thing, but are too hard to reverse in an adversary's time [2]. Specialized cryptographic instruments will elicit ever-fluid streams of random bits whose values are invisible to third parties. By using these parts as key material for Vernam ciphers, it can quickly and cheaply attain the ideal of Shannon's complete secrecy [3]. In comparison, QKD offers information-theoretical confidentiality, which is strongly founded on physics law, on the unproved basis of core public technology. The quantum key dissemination (QKD), first proposed in 1984 by Bennett and Brassard, is a technique for sending a concealed key. On account of a fundamental trademark in quantum mechanics known as the no-cloning hypothesis, any exertion by an outsider to snoop constantly brings about mix-ups that the sender and beneficiary may distinguish. Customarily, current QKD frameworks utilize a qubit framework

* Corresponding author.
E-mail address: abidinshafiqul72@gmail.com (S. Abidin).

https://doi.org/10.1016/j.matpr.2021.05.593
2214-7853/© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the 1st International Conference on Computations in Materials and Applied Engineering – 2021.

Please cite this article as: S. Abidin, A. Swami, E. Ramirez-Asís et al., Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC), Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2021.05.593

to encode data, for example, photon polarization. These gadgets are immediately sent, and today innovation is promptly accessible to scramble and unravel data in the qubit state, permitting framework clock speeds under the GHz system. The spatial level of photon opportunity has as of late been set up as a significant wellspring of data move [4].

While such encoding plans offer a simple answer for expanding data ability, as a result of the cross-talk instigated by diffraction they are inadmissible for long-range optical associations. Diffraction incites a mind-boggling absence of spread for numerous spatial frequencies, which brings about spatial modular combination. Cross-talking raises the SER rate and essentially decreases the ensured key pace of a QKD gadget. The utilization of OAM modes will limit this unfavorable impact. OAM modes have the alluring property of being symmetrical when spreading in a gadget with roundabout gaps due to their rotational symmetry [5].

The occurrence of MCC has created a significant kind of turnaround on computer science technology including on to the developers of the phone. MCC is vital technology nowadays, as it is applicable in diverse services likewise: electronic mobile commerce (EMC), electronic mobile learning (EML), electronic mobile banking (EMB), electronic mobile healthcare (EMH), and electronic mobile game (EMG). However, mobile devices (MDs) are now becoming very sophisticated; the reason behind it is the larger development and application complexity. This offloading task onto the cloud deals with many issues, including security, mobile application development and quality of service.

2. Literature review

Integrity, availability and confidentiality problems are required to get address as the task gets offloaded by means of the cloud. Privacy, end-to-end security, and authentication requirements to get integrated by offloading the architecture kind of framework. It is essential to be sure about the reliability and security of the task for transmission of MDs to the cloud, the reason behind it is the information. Data can get stored and also be moved into the cloud by means of a wireless kind of connection. Because of the wireless connection, transferring is now vulnerable for both zones including the external and internal attacks. Quality of the service (QoS) is very vital for the relaxation of effective transferring of the task in the area of the cloud system.

2.1. Quantum key distribution

Modern networks typically rely on one of the two foundational encryption strategies to ensure that traffic through the grid is confidential and integral: symmetrical key and asymmetric key. In particular, the best systems of today usually use both public key signals and hidden "session" keys and then secure all or part of the traffic flow with these session keys. Any other systems bring hidden keys "out of the channel," as in the case of traditional cryptography, for instance by courier. Basically speaking, the unitary dimensions of quantum mechanics theory of uncertainty and a breach of Bell's inequality by Einstein-Podolsky-Rosen – now proposes a third model for key distribution: quantum encryption. The efficacy of this paradigm seems demonstrated by initial studies [6]. In order to ensure the secrecy of transmitted records, basic regulations of design may also be applied if the theoretical models are verified in the use of the real equipment. QKD consists of a dim light pulse transmitted from Alice to Bob via the quantum medium, e.g. as dim light pulses, plus the sorting of the real main content. This method includes public contact with the advanced QKD algorithms (key agreement protocols) between Alice and Bob on the public network. The key results can then be used to secure user traffic, for example, for cryptographic purposes. According to the laws of quantity physics, any Eva (Eve), which induces snoops on the quantum canal, causes the flux of individual photons to be troubling. It can be observed by Alice and Bob, taking suitable reactions and thus the eavesdropping effort by Eve [7]. This creates a hypothesis that for resisting quantum computer order, new systems which would not be based on discrete logarithms issues have to be explored. This is the only way through which data security can get a guarantee for the future internet in the zone of cyberspace [8].

Bennett and Brassard, who likewise portrayed the primary QKD convention called BB84, proposed in 1984 quantum cryptography. A couple of examination groups the world over had the option to create and run quantum cryptographic gadgets during the creative cycle. Apparently, there is also the interest in cryptograms based on a very different physical phenomenon - intertwining between pairs of photons produced by spontaneous parametric downgrading - which is weak, coherent quantum cryptography (SPDC). This is what it is talking about. Geneva has shown and explored cryptography in many important papers. An excellent summary of QKD's present state of the art was presented by the Geneva team [9]. It highly encourages anybody who wants to get to know more about this fascinating area.

Quantum data properties: The concept of the whole uncertainty principle was the position of a particle in the world of micro which is not possible at all to get determined, thus it does exist in diverse spaces along with diverse chances [10]. It's proposed that when a copy of any arbitrary gets deletes in a quantum state isn't allowed through the linearity of theory by quantum.

3. Methodologies

Alice sends to Bob an arbitrarily module set of single photons (a double-sided card here with a random number. Alice picks one card side by chance and sends the card to Bob by writing random 0 or 1 on that side. Bob also picks a random side and reads the value of this side. Bob reads exactly what Alice wrote as Alice and Bob take the same hand. If not, he reads a 0 or 1 at random overall [11]. Since Bob has read all the photons, Alice is performing a scanning transaction to discard any situations in which he reads wrong (basis). It sends Alice the random basis settings list and informs him which settings are correct. Alice and Bob then deny any value on which they differ and retain the remaining raw material values. Now, what about a ruminant, who is it going to name Eve? In the first place, Eve is like Bob. She would imagine what side of the card she'll be able to read, and the other half will be of random importance for the half of the time she reads what Alice sent. But a little bit of a single photon she cannot surreptitiously sift so she demolishes it as she reads it. But if this photon is not obtained, it does not lose; this method of sifting will discard the photon, and Alice and Bob will not include it in their main stuff [12]. The no-cloning theorem of Quantum Mechanics states it cannot clone values on both sides of the card — only the side on which it reads. A random value may be on the other hand. In actual systems, however, some channel noise is still present and even though they require wiping out operations, the cryptographic device may work with some level of sound. In order to resolve this problem, it uses reasonably robust error detecting and correction protocols in order to identify and correct bit errors and the effect is compounded by anonymity, such that Eve knows just a little bit about the resulting Alice and Bob values [31,13].

3.1. QKD in systems

In 1992 Bennet and Brassard designed the first rudimentary QKD apparatus; since then, many systems, including systems built by Los Alamos, British Telecom, Johns Hopkins University, and IBM Almaden Research Center, have followed. QKD can run via telecom fiber or the atmosphere. While their technological specifics vary considerably, researchers have seen both methods. At a rate of about 5,000 bits/s at a distance of up to 50 km via telecom or 10–20 km through the atmosphere, today's devices produce very high-end main content [14,32]. Although these speeds are not high enough to secure valuable single pad traffic, they permit the fast re-encryption of traditional cryptographic algorithms, such as the Advanced Encryption Standard (AES). Each device uses a typical wavelength (1550.12 nm) highly attenuated "single-photon" telecommunications laser with phase modulation through Mach Zehnder unbalanced interferometers and APDs, which detect single photons [33,15]. An additional Mach-Zehnder interferometer is contained in the Receiver at Bob, arbitrarily set in one of two phases for demodulation. Alice often transmits a light pulse, a standard amount of power for telecommunications that is multiplied by the same fiber [16]. Fig. 1 illustrate the complete functioning.

3.2. Protocols and algorithms

During the production of its systems, it found that QKD optics is probably the easiest part; electronics are harder than optics and software is harder than electronics for a practical device. Fig. 4 demonstrates how QKD protocols could integrate into a UNIX operating system, providing key material for use in cryptography protecting Internet traffic through standard IPsec protocols and algorithms for its Indigenous Internet Key Exchange (IKE). BBN QKD protocol stack is written in C for portability to real-time devices that are embedded. David Pearson, Gregory Troxel (BBN Technologies) and IT will explore this deployment more in-depth, and how QKD communicates elsewhere with IKE and IPsec 8.

Fig. 2 shows the complete functionality. This process happens by some form of one-way function, such as the digital signatures implemented using key-public techniques in most modern cryptographic schemes. Authentication is based on mutual secret keys in classical QKD literature, such as universal hash functionality [17,34].

3.3. QKD DARPA networks

The DARPA Quantum Network comprises two Alice and Anna transmitters and two viable receptors, Bob and Boris, with quantum channels associated straightforwardly through the fiber by means of a two-stage optical switch. For one or the other collector, either sender may arrange a common key. The switch is optically aloof: as such, no photons that move through it is distinguished or enhanced so the quantum condition of the photons that encode fundamental pieces can't be disturbed. Where two QKD endpoints don't share a direct or exchanged channel, yet are cross-canalized by confided in transfers, its systems administration conventions permit them to concur on a mutual key by choosing an organization course, creating another R-number and sending a one-time R cushion scrambled on every association [18]. The following flow of QKD will be a lot more bizarre than it is today since it will get important material from sets of many-sided photons. This is in certain regards the most acceptable of all methods of QKD since it uses the intrinsic inconsistency and marvel of the universe [19,35]. Fig. 3 shows the complete functionality.

3.4. QKD architectures

As observed, Alice's transmitter communicates singular photons with a laser heartbeat of 1550 nm that is unequivocally constricted. Any of them goes through an arbitrarily regulated Mach-Zehnder interferometer in Alice in one of four focuses, encoding both a premise and an incentive for the self-obstruction of the photon. Another Mach Zehnder interferometer is utilized in the Bob beneficiary, arbitrarily regulated in one of the two stages to pick a base. The photons gathered travel through the Bob interferometer for one of the two thermoelectrically cooled single-photon indicators to show worth. Alice is likewise communicating light heartbeats duplicated by a similar fiber, at 1300 nm to give Bob data about planning and outlining.

Figs. 4-6 exhibit the crucial instrument of its progression encoding framework.

Fig. 5 represents how a genuine photon functions with its heartbeat from Alice's 1550 nm QKD source into the Bob locator pair. Here you can see the photon rather than a molecule as a wave. Hence the interferometer is taking the two headings as opposed to choosing a solitary bearing.

Fig. 6 demonstrates the blend of the resultant twofold beat of the Bob 50/50 coupler before the finders. The beat in the upper train is pretty much precisely coordinated with that in the lower train when the interferometers were changed right, which implies that the two amplitudes are added together. The correct part of the graph shows a composite waveform before the 50/50 sets of QKD finders from Bob. At last, it is presently ready to exhibit decisively how estimations of ' and '1' are sent among Alice and Bob utilizing QKD beats. As it portrayed, it was the blend of twofold heartbeat that made the focal pinnacle, expecting that interferometers Alice and Bob are pretty much definitely coordinated.

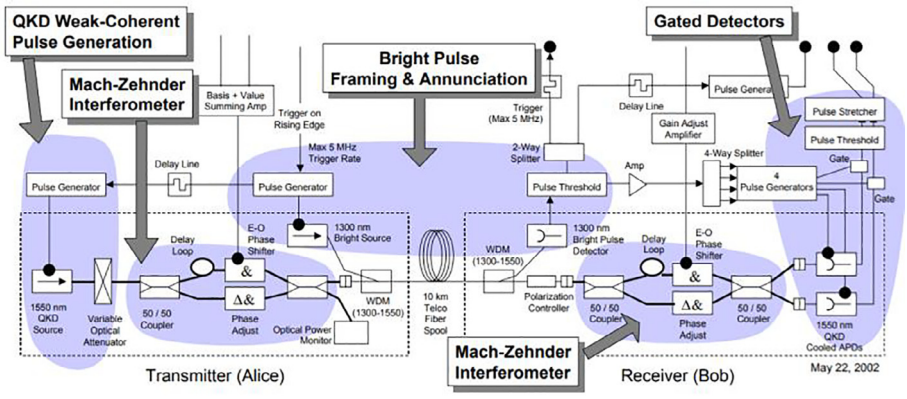

Fig. 1. BBN quantum cryptography (FD).

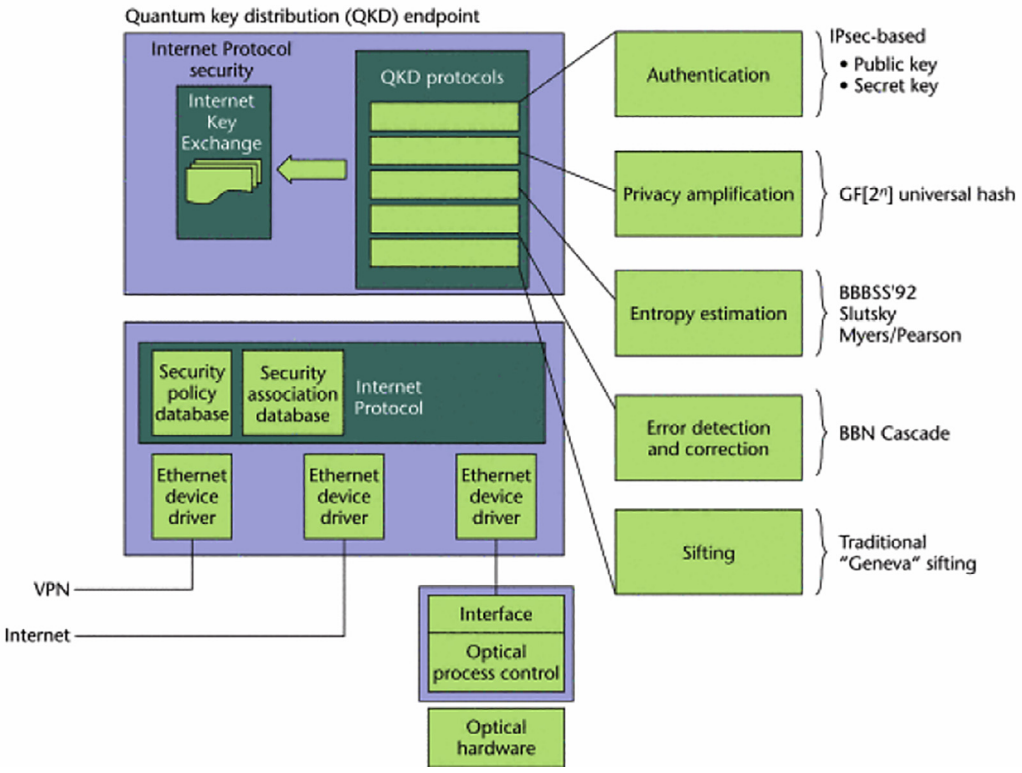

Fig. 2. BBN QC protocols.

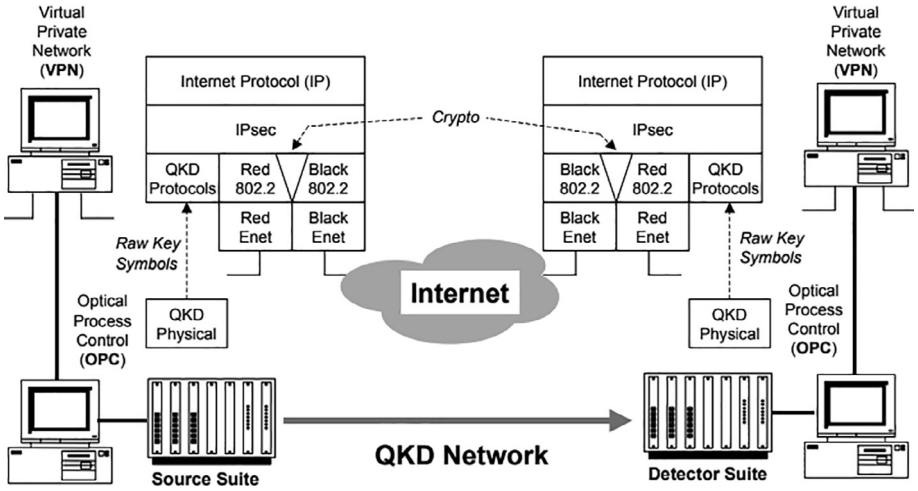

Fig. 3. QKD Networks.

3.5. IPSEC implementation

On the off chance that a cryptographic quantic key substance has been finished, it tends to be utilized as keys for at least one application. Its first utilization of these key substances is for IPsec-based virtual private organizations as standard encryption keys. As needs are, both the preparing way of IPsec and its fundamental arrangement convention (IKE) have been extended to utilize basic material acquired with quantum cryptography. Since both Alice and Bob persistently stream new data, the two of them can change the key uses pretty much consistently in their cryptographic calculations [36,20]. One of its components, the IKE convention, requires two endpoints to concur on the cryptographic conventions and calculations that they might want to use for a given security affiliation, and the other on the keys they use to encode as well as confirm the accompanying message traffic in this security affiliation [21]. Inside the IETF, RFC 2409, Internet Key Exchange, IKE is determined as a standard record (IKE). While IKE is a generally intricate convention, its essential standards are clear. Figure 10 uncovers the critical components of the current kinship between two IKE peers. The utilization of IKE for quantum encryption is of specific importance for a modest bunch of novel IKE configuration pieces, which can impact its general gadget plan [22]. This can without much of a stretch occurs in quantum cryptography since clamor must be noticed and probabilistically revised in a solitary photon channel. IKE doesn't have any

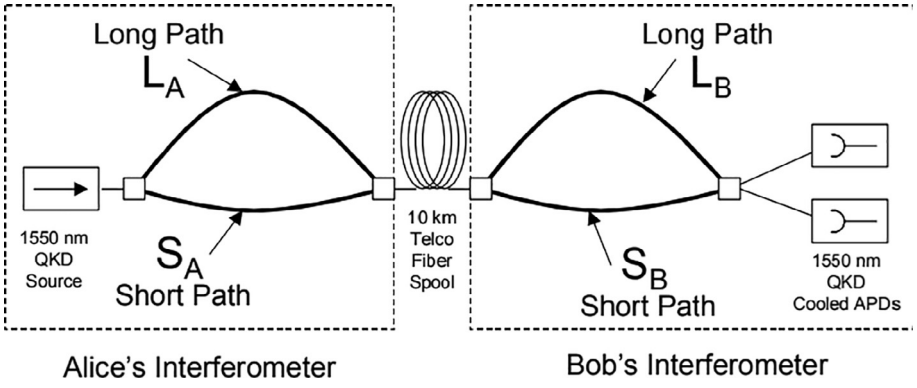

Fig. 4. Paths through unbalanced Mach-Zehnder interferometers.

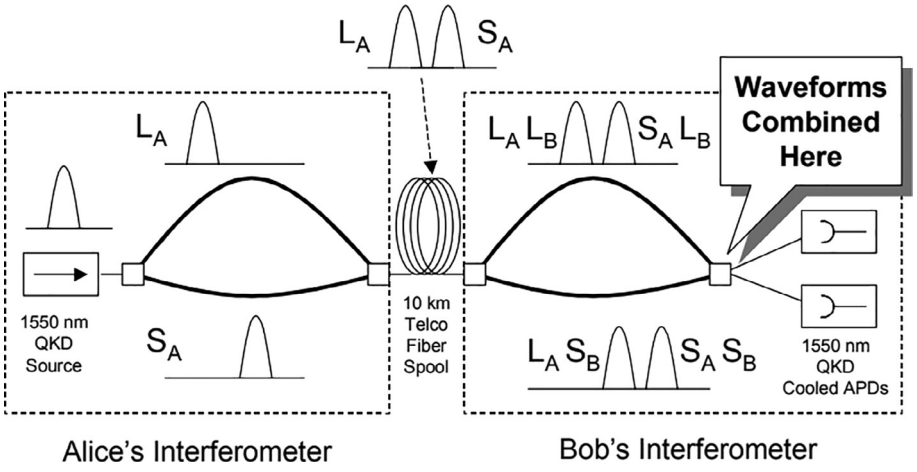

Fig. 5. Effects of an unbalanced interferometer on a photon.

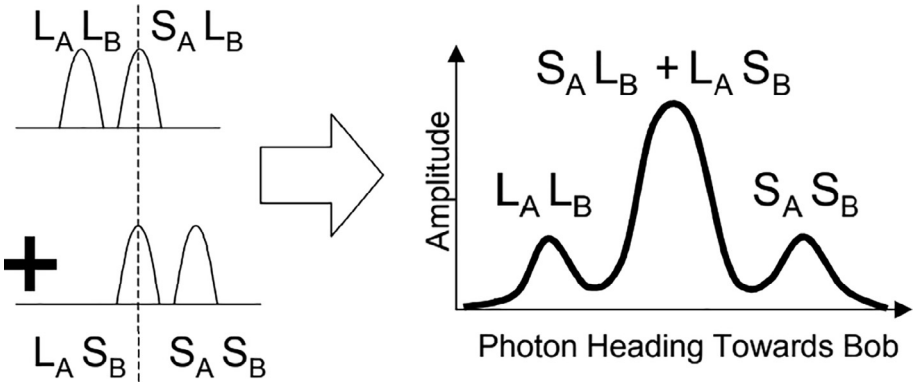

Fig. 6. Recombined photon at 50 / 50 coupler just before Bob's QKD detectors. The central peak is self-interfering.

frameworks to notice or treat certain circumstances. The outcome appears to have not been appropriately encoding/interpreted for all security affiliations utilizing key pieces extricated from this bad data. It will appear to be that this condition will continue until the security affiliation is reestablished, for example, another security affiliation is moved [35,23].

3.6. QKD with twisted light technology

Alice has subjectively chosen two extra bases for her photons in its framework. A determination of OAM vortex modes is the essential coding source. The two modes have a setup of extreme focus and a helical advance profile as follows:

$$\varphi^{l}OAM = e^{il\varphi} \tag{1}$$

A straight blend of OAM record modes with equal amplitudes is utilized to make the commonly fair-minded premise set as:

$$\varphi^{n}_{ANG} = \frac{1}{\sqrt{d}} \sum_{l=-N}^{N} \varphi^{l}_{OAM} \exp\left(\frac{i2\pi nl}{d}\right) \tag{2}$$

Whereas, in its test the measurements are (D = 2 N + 1 = 7). Because of their restricted adequacy varieties, it alludes to such modes as

precise (ANG) modes. As opposed to OAM modes, ANG modes are commonly lopsided, given as:

$$\left|\langle\varphi^{n}_{ANG}|\varphi^{l}_{OAM}\rangle\right|^{2}=\frac{1}{d}\forall\{n,l\} \quad (3)$$

Through a 4f telescope, which frames a lossless 2 m long contact connect, arrangements are then imaged at Bob's getting opening [24,34]. The means made in different bases were then disposed of by Alice and Bob. Now, the key created is known as the screwed key [25,33]. This is achieved by using a universal hash function to make the error-corrected key a short random key.

4. Results and analysis

Performance of transport and identification: The efficiency of the refractive components of the modal sorter is estimated by 85%. For holograms and the corresponding phase correction feature, two Holoeye PLUTO phase-only SLM's are used. Moreover, the SLMs are fitted with two cylindrical lenses to adapt the look ratio of the transformed straps. Per SLM is measured at a diffraction efficiency of about 45 percent. The efficiency of connections between the converted modes and the fiber spectrum has been estimated at about 18%.

Classical ability for knowledge: This scheme avoids the timeless changeover between various spatial modes and makes it possible to calculate the error rate even more accurately using a large range of symbols sent and received. But a uniform lack of coordination and detection does not modify the shared knowledge between the sifted keys of Alice and Bob as the time-frames are excluded in the reconciliation protocol without a photon-detection occurrence [26,32].

IKE security: The Eavesdropper (Eve) tests the status of the caught photon on an arbitrarily picked premise in a capture resend assault and afterward sends a photon back that will be in a similar condition. Eve reliably studies few audits to acquire data about the fundamentals in a precise attack. From this chart, it is obvious that its trial SER is far beneath the essential wellbeing limits against block attempts and reliable assaults [27,31].

High efficiency: When losses rise, the main generation rate decreases. The protocol also becomes vulnerable to PNS attacks due to high contact losses. With high-efficiency sLMs or with AR-coated custom refractive elements the performance of its detection system can be easily improved. This would mean that the propagation quality of its experiment would be improved six times. Furthermore, the amount of damage induced by the air dispersion can be decreased by activity in the near-infrared device.

Mitigation of turbulence: The spatial profile of modes can degrade as atmospheric turbulence arises. As a result, the nearby OAM and ANG models are merged. Turbulence has been a target of detailed studies in OAM modes. The use of all other approaches to encrypt and use adaptive optics Technologies are standard strategies for mitigating the detrimental effects of atmospheric turbulence. Long-range open-space dissemination of OAM modes with new detection schemes has recently been carried out [28,36].

Longer dimension: More modes improve the amount of information that each photon carries which results in a higher protected bit rate. It previously showed that its Mode Sorter would filter 25 OAM and ANG modes per observed photons with an average mutual knowledge of 4.17 bits. Consequently, the number of APDs in this experiment will easily increase the encoded information per photon [29,30]. Finally, through sizing and receiving apertures, the amount of modes that the optical communication supports is reduced.

5. Conclusion

The DARPA Quantum Network uncovers that quantum encryption can be utilized truth be told, on a fundamental level, to furnish virtual private web networks with a ceaseless key dispersion. Any significant components of the quantum cryptography hypothesis are still exceptionally bewildering. On the basis of classical cryptography and quantum mechanics, quantum cryptography is a fresh and new system in the line of cryptography. As compared to classical cryptography, it has ultimate benefits are in the zone of an unconditional sniffing detection system along with security. The characteristics can aid in resolving the security of cyberspace on the basis of critical issues for the internet. As being specific, it generates the security for diverse applications, likewise: smart cities, internet, and future internet as cyberspace. The analysis on the basis of experiments has shown the conclusion of unconditional security along with the detection of sniffing on behalf of quantum cryptography that makes it very suitable for the usage of the internet in the future. The various assaults and the definite quantum–mechanical hypothesis behind photon yield, engendering, identification, and so on to put it plainly, it is currently evident that quantum cryptography is in fact conceivable.

CRediT authorship contribution statement

Shafiqul Abidin: Investigation, Supervision. **Amit Swami:** Writing - review & editing. **Edwin Ramirez-Asís:** Writing - review & editing. **Joseph Alvarado-Tolentino:** Investigation. **Rajesh Kumar Maurya:** Supervision. **Naziya Hussain:** Investigation, Writing - original draft.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H.B. AbdulWahab, A.M.S. Rahma, July). Proposed new quantum cryptography system using quantum description techniques for generated curves, In The 2009 International conference on security and management, 2009.
[2] G. Alagic, G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, R. Perlner. Status report on the first round of the NIST post-quantum cryptography standardization process. US Department of Commerce, National Institute of Standards and Technology. 2019.
[3] S.M. Barnett, S.J. Phoenix, Information-theoretic limits to quantum cryptography, Phys. Rev. A 48 (1) (1993) R5.
[4] C.H. Bennett, Experimental quantum cryptography, J. Cryptol. 5 (1) (1992) 3–28.
[5] C.H. Bennet, G. Brassard. Quantum cryptography: public key distribution and coin tossing, Proc. Int'l Conf. Computers Systems & Signal Processing, pp. 175-179 1984.
[6] C.H. Bennett, G. Brassard, A.K. Ekert, Quantum cryptography, Sci. Am. 267 (4) (1992) 50–57.
[7] D.J. Bernstein, Introduction to Post-Quantum Cryptography. In Post-Quantum Cryptography, Springer, Berlin, Heidelberg, 2009, pp. 1–14.
[8] P. Bhatia, R. Sumbaly. Framework for wireless network security using quantum cryptography. arXiv preprint arXiv:1412.2495. 2014.
[9] D. Bouwmeester, Experimental quantum teleportation, Nature 390 (1997) 577–579.
[10] A. Broadbent, C. Schaffner, Quantum cryptography beyond quantum key distribution, Des. Codes Crypt. 78 (1) (2016) 351–382.
[11] Y. Chen, P.K. Verma, S. Kak, Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks, Security Commun. Netw. 2 (6) (2009) 546–554.
[12] M. Christandl, R. König, R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, Phys. Rev. Lett. 102 (2) (2009) 020504.
[13] C. Elliott, D. Pearson, G. Troxel, August). Quantum cryptography in practice, in: In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, 2003, pp. 227–238.

[14] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74 (1) (2002) 145.
[15] A. Goyal, S. Aggarwal, A. Jain, Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper, In 5th IEEE International Conference on Advanced Computing & Communication Technologies [ICACCT-2011], 2011.
[16] H.J. Hughes, Practical Free-space quantum key distribution over 10 km in daylight and at night, New J. Phys. (2002) 43–51.
[17] B.C. Jacobs, J.D. Franson, Quantum cryptography in free space, Opt. Lett. 21 (22) (1996) 1854–1856.
[18] H.K. Lo, N. Lütkenhaus. Quantum cryptography: from theory to practice. arXiv preprint quant-ph/0702202. 2007.
[19] N. Lütkenhaus, Estimates for practical quantum cryptography, Phys. Rev. A 59 (5) (1999) 3301.
[20] T.M.T. Nguyen, M.A. Sfaxi, S. Ghernaouti-Hélie. Integration of quantum cryptography in 802.11 networks. In First International Conference on Availability, Reliability and Security (ARES'06) (pp. 8-pp). IEEE.
[21] M. Niemiec, Error correction in quantum cryptography based on artificial neural networks, Quantum Inf. Process. 18 (6) (2019) 174.
[22] H.R. Pawar, D.G. Harkut. Classical and Quantum Cryptography for Image Encryption & Decryption. In 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE) (pp. 1-4). IEEE. 2018.
[23] C. Peng, J. Chen, S. Zeadally, D. He, Isogeny-based cryptography: a promising post-quantum technique, IT Prof. 21 (6) (2019) 27–32.
[24] S.J. Phoenix, S.M. Barnett, P.D. Townsend, K.J. Blow, Multi-user quantum cryptography on optical networks, J. Mod. Opt. 42 (6) (1995) 1155–1163.
[25] S.J. Phoenix, S.M. Barnett, A. Chefles, Three-state quantum cryptography, J. Mod. Opt. 47 (2–3) (2000) 507–516.
[26] T.C. Ralph, Security of continuous-variable quantum cryptography, Phys. Rev. A 62 (6) (2000) 062306.
[27] J.G. Rarity, P.R. Tapster, P.M. Gorman, P. Knight, Ground to satellite secure key exchange using quantum cryptography, New J. Phys. 4 (1) (2002) 82.
[28] M.S. Sharbaf. Quantum cryptography: An emerging technology in network security. In 2011 IEEE International Conference on Technologies for Homeland Security (HST) (pp. 13-19). IEEE. 2011.
[29] M. Tomamichel, C.C.W. Lim, N. Gisin, R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. 3 (1) (2012) 1–6.
[30] D. Chauhan, C. Singh. Sentimental Analysis on Impact of COVID-19 Outbreak. In: Agrawal S., Kumar Gupta K., H. Chan J., Agrawal J., Gupta M. (eds) Machine Intelligence and Smart Systems. Algorithms for Intelligent Systems. Springer, Singapore. 2021 https://doi.org/10.1007/978-981-33-4893-6_21.
[31] Deepika Chauhan, Ashok Kumar, Pradeep Bedi, Vijay Anant Athavale, D. Veeraiah, Boppuru Rudra Pratap, An effective face recognition system based on Cloud based IoT with a deep learning model, Microprocessors Microsyst. 81 2021 103726,ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2020.103726.
[32] Pradeep Bedi, Shivlal Mewada, Rasmbabu Arjunarao Vatti, Chaitanya Singh, Kanwalvir Singh Dhindsa, Muruganantham Ponnusamy, Ranjana Sikarwar, Detection of attacks in IoT sensors networks using machine learning algorithm, Microprocessors Microsyst. 82 2021,103814,ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2020.103814.
[33] Z. Qureshi, N. Agrawal, D. Chouhan, Cloud based IOT: Architecture, application, challenges and future, Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. 3 (2018) 359–368.
[34] , IoT–Blockchain Integration-Based Applications Challenges and Opportunities vol 140 (2021), https://doi.org/10.1007/978-981-15-7130-5_7.
[35] M. S. T. M. C. S. M. S. Survey of Protocol for Provisioning of QOS in MANETS. Int. J. Recent Innov. Trends Comput. Commun. 3(5) 2015 2587-2590. https://doi.org/10.17762/ijritcc.v3i5.4289.
[36] C. Singh, M.R. Aloney, Comparative Study of LEACH Routing Protocol for WSN, Int. J. Adv. Res. Comput. Sci. Manage. Stud. 3 (3) (2015) 322–327.