Survey on Quantum Cryptography

Sneha shree K[1], Umme Hani J[2],Varshitha S[3], Usha K Patil[4]

[123]*UG Students, Department of Computer science & Engineering, ,Mysuru Royal Institute of Technology, Mandya*

[4]*Assistant Professor ,Department of Computer science &engineering,Mysuru Royal Institute of Technology, Mandya*

Abstract- Quantum cryptography is one of the most resplendent applications of quantum information theory. Quantum cryptography is science of exploiting quantum mechanical properties to perform cryptographic tasks. The development of quantum cryptography assures in addressing some of the uncertainty that influx classical encryption technique such as the key distribution problem and the predicated breakdown of public/private key system. It operates on the ―Heisenberg uncertainty and arbitrary polarisation of light. If one endeavours to read the encoded data, the quantum state will be transmuted. This could be acclimated to detect eavesdropping in ―Quantum key distribution‖. Quantum cryptography, which uses photon and relies on the law of Quantum physics in lien of ―profoundly and immensely colossal number‖ is the cutting edges of revelation which seems to ensure privacy even when postulating eavesdroppers with un-circumscribed computing potency.

Keywords- Quantum cryptography, Quantum Key Distribution,message encryption, communication, Encoding, Decoding, Entanglement.

I. INTRODUCTION

Cryptography is the art of devising codes and cipher. Quantum cryptography is an effort to sanction two users of a prevalent communication channel to engender a body of shared and secret information. Quantum cryptography has a different ways of sending the key to the receiver. It uses ―photons‖ to send a key. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed (no-cloning theorem). This could be used to detect eavesdropping in quantum key distribution. The word ―quantum*"* itself refers to the most fundamental behaviour of the smallest particles of matter and energy.

Quantum theory explains everything that exists and nothing can be in violation of it. Quantum cryptography is different from traditional cryptographic systems in that it relies more on physics, rather than mathematics, as a key aspect of its security model. This information, which generally takes the form of a random string of bits, can then be used as a conventional secret key for secure communication. It is possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at a point when it is measured. This principle plays a critical role in the attempts of eavesdropper in cryptosystem based on quantum cryptography. Secondly, photon polarization principle describe how light photons can be oriented or polarized in specific directions.

Heisenberg's uncertainty Principle states that there is intrinsically dubiousness in the act of quantifying a variable of a particle. Commonly applied to the position and momentum of a particle, the principle states that the more precisely the position is kenned the more uncertain the momentum is and vice versa (18).

Heisenberg's uncertainty Principle and Quantum entanglement can be exploited in as system of secure communication often referred as ‖Quantum cryptography.Most security breaches involve accessing unauthorized data or illicit network access (4). For the recent years, the intruders have demonstrated incremented technical cognizance, developed incipient ways to exploit network susceptibilities, and engendered advanced software implements to automate attacks (5).By sending the key encoded at the single photon level on a photon-by photon substructure, quantum cryptography guarantees that the act of an eavesdropper intercepting a photon, even if it just to observe or to read it, irretrievable transmutes the information encoded on that photon (1), (2), (3).The security of quantum key distribution relies on the inviolable laws of quantum mechanics, and the infeasibility of perfect cloning of non-orthogonal states implicatively insinuates the security of this protocol (2). Additionally, quantum cryptography technology makes extensive utilization of the Heisenberg dubiousness principle for ascertaining secure cryptography. The propose of this research paper is to explore the quantum cryptography technology in network security.

II. FEATURES

- High speed full duplex encryption.
- Automated key management secret key exchanged via quantum physics ‖set of forget‖ operation.
- No impact on network performance
- Point to point, layer to layer encryption for LAN/WAN/SAN networks.

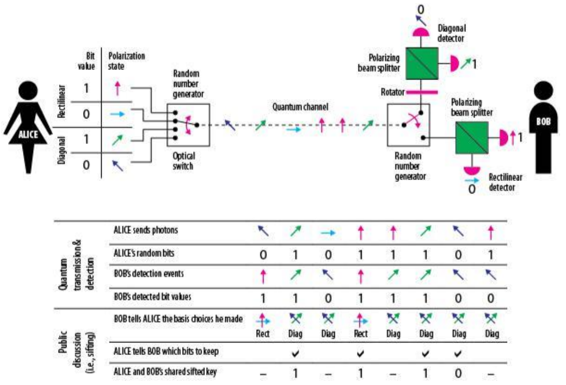
III. WORKING

Quantum cryptography uses photon to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can takes place. This is where binary code comes into play. Each type of a photon's spin represents one piece of information-usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. For example, 11100100110 could correspond with h-e-l-l-o.

So a binary code can be assigned to each- for example, a photon that has a vertical spin [1] can be assigned as 1 (19).

The miniature transmitter communicates with a trusted authority to generates random cryptographic keys to encode and decode information (6).How are the steps that shows how quantum cryptographic works(10).

- Alice uses a light source to create a photon.
- The photon is sent through a polarizer and randomly given one of four possible polarization and bit designations Vertical (One bit), Horizontal (Zero bit), 45 degree right (One bit), or 45 degree left (Zero bit).
- The photon travels to Bob's location.
- Bob has two beam splitters — a diagonal and vertical/horizontal - and two photon detectors.
- Bob randomly chooses one of the two beam splitters and checks the photon detectors.
- The process is repeated until the entire key has been transmitted to Bob.
- Bob then tells Alice in sequence which beam splitter he used.
- Alice compares this information with the sequence of polarizers she used to send the key.
- Alice tells Bob where in the sequence of sent photons he used the right beam splitter.
- Now both Alice and Bob have a sequence of bits (sifted key) they both know.



ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
ALICE's random bits	0	1	0	1	1	1	0	1
BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
BOB's detected bit values	1	1	0	1	1	1	0	0
BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
ALICE tells BOB which bits to keep		✓		✓		✓	✓	
ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

Fig.1: working of Quantum cryptography

IV. QUANTUM KEY DISTRIBUTION

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography is Quantum key Distribution which offers an information-theoretically secure solution to the key exchange problem. The most well-kenned and developed application of quantum cryptography is quantum key distribution (QKD),which is the process of utilizing quantum communication to establish a shared key between two parties(Alice and Bob) without a third party(Eve)learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob(8). If eve endeavours to learn information about the key is established, it is then typically utilized for encrypted communication utilizing classical techniques.

The security of quantum key distribution can be proven mathematically without imposing any restrictions on the facilities of an eavesdropper, something not possible with classical key distribution. This is conventionally described as "unconditional security", albeit there are some minimal postulations required, including that the laws of quantum mechanics apply and that Alice and Bob are able to authenticate each other, i.e. Eve should not be able to impersonate Alice or Bob as otherwise a man in the middle assailment would be possible.

While quantum key distribution is ostensibly secure, its applications face the challenge of practicality. This is due to transmission distance and key generation rate inhibitions. In 2018 Lucamariniet. al. proposed a scheme that can possibly overcome the "rate-distance limit". The Twin-Field Quantum Key Distribution Scheme suggests that optimal key rates are achievable on "550 km of standardoptical fibre", which is already commonly utilized in communications today.(7) Examples for Quantum key distribution are ElGamal.

A. ElGamal

determine if the session is secure. If the session is secure, a felicitous number of photons can be culled as the bits of the cryptographic key that both the sender and receiver will utilize.

The ElGamal encryption system is an asymmetric key encryption algorithm for public key cryptography which is based on the Diffie-Hellman key exchange. The system provides and additional layer of security by asymmetrically encrypting keys previously used for symmetric message encryption. ElGamal encryption can be defined over any cyclic group. Its security depends upon the difficulty of a certain problem related to computing discrete logarithms.(20).

V. WORKING OF QKD

Quantum key distribution (QKD) uses individual photons for the exchange of cryptographic key data between two users, where each photon represents a single bit of data. The value of the bit, a 1 or a 0, is tenacious by states of the photon such as polarization or spin(9).

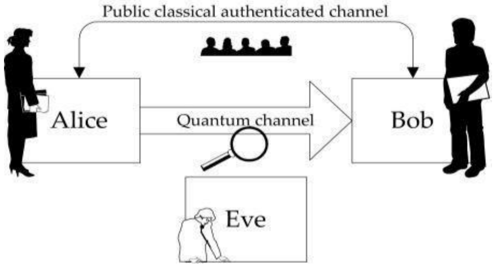


Fig.2: Quantum key distribution comprises a quantum channel and a public classical authenticated channel. [11].

At the sender’s end, a laser engenders a series of single photons, each in one of two polarizations: horizontal or vertical. The polarization of the photon is quantified at the receiver’s end. If an eavesdropper intercepts the photon to determine its polarization, the photon is ravaged in the process, and the eavesdropper would have to engender an incipient, duplicate photon to pass on to the receiver.

The uncertainty of quantum physics makes it infeasible for the eavesdropper to determine both properties of the photon, so it would be infeasible for him to send along a precise duplicate. because of this, the receiver would descry a high error rate in the photons being received, which would denote someone was intercepting the data.

To determine the error rate, the states of a diminutive percentage of photons are compared over a separate channel by the receiver and the sender. Because the comparison process ravages the photons these cannot be utilized in engendering a key. But the error rate can be acclimated to

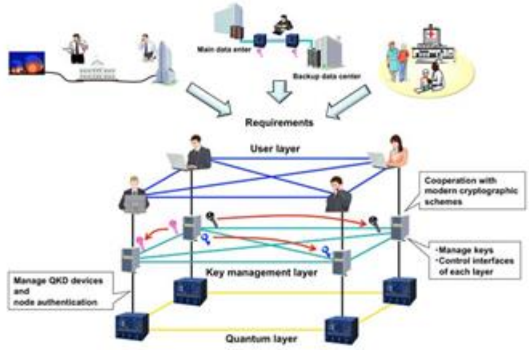

Main data enter
Backup data center
Requirements
User layer
Cooperation with modern cryptographic schemes
·Manage keys
·Control interfaces of each layer
Manage QKD devices and node authentication
Key management layer
Quantum layer

Fig 3: functioning of Quantum key distribution

VI. SECURITY

As there exits many different solutions to perform secret key accidence, but QKD is the only subsisting and virtually implementable scheme that can offer information-theoretic security.one advantages of utilizing QKD as the instauration mechanism for link encryption is the long-term security guarantee for the keys. This is to be compared with the conventional mode of operation for VPN encrypts, where the establishment of an encryption key relies on asymmetric cryptography and thus implicatively insinuate a susceptibility to potential subsisting computational attacks on public-key scheme [12].

Another consequential operational interest of OKD, when used sequentially to engender successive encryption keys, is the property called ―forward-secrecy‖ of the establishment keys. The successive keys established over a QKD link are independent from one another. Consequently, the potential compromise of a single key cannot lead to the compromise of other keys. We can descry that the forward-secrecy of QKD is a natural consequence than the perpetual. As a matter of fact, In the sequential engenderment of QKD keys, the secret material needed at each QKD round to authenticate the classical channel stems from an antecedent QKD round. Forward-secrecy in key establishment is a consequential property and additionally be obtained with public key cryptography under computational postulations[13] while it cannot be obtained at all with computational symmetric cryptography since the successive keys are not independent from one another.

VII. CLASSIFICATION

A. Position based Quantum cryptography

In this work, we study position-predicated cryptography in the quantum setting. The aim is to utilize the geographical position of a party as its only credential. On the negative side, we show that if adversaries are sanctioned to apportion an arbitrarily immensely colossal entangled quantum state, no secure position-verification is possible at all. We show a distributed protocol for computing any unitary operation on a state shared between the different users, utilizing local operations and one round of classical communication. Utilizing this surprising result, we break any position-verification scheme of a very general form. On the positive side, we show that if adversaries do not apportion any entangled quantum state but can compute arbitrary quantum operations, secure position-verification is achievable. Jointly, [17] these results suggest the fascinating question whether secure position-verification is possible in case of a bounded amount of entanglement. Our positive result can be interpreted as resolving this question in the simplest case, where the bound is set to zero. In models where secure situating is achievable, it has a number of intriguing applications. For example, it enables secure communication over an insecure channel without having any pre-shared key, with the assurance that only a party at a categorical location can learn the content of the conversation. More generally, we show that in settings where secure position-verification is achievable, other position-predicated cryptographic schemes are possible as well, such as secure position-predicated authentication and position-predicated key acquiescent.

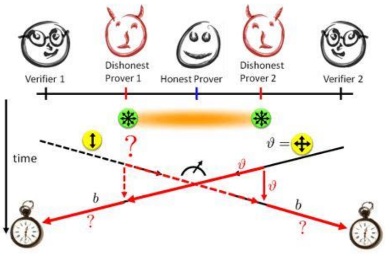


Fig.4: Working of Position based on Quantum cryptography

B. Device Independent Quantum cryptography

A first area of focus is to closing the gap between theory and experiments. Present security analyses make very inductively authorizing experimental requisites, such as the essentiality to manipulate entangled states with high efficiency and fidelity; little noise is abode on the communication channels. Among the results presented in this issue, [25] study a 'semi-contrivance-independent' (SDI) model in which one of the contrivances is trusted; in this scenario they provide ameliorated quantitative bounds for the quandary of self-testing an EPR pair, with an analysis predicated on the phenomenon of EPR steering.[26] considers another SDI model, one in which only the dimension of the system is kenned but not the quantifications, and provides implements to quantify entanglement and security proofs for QKD.[27] studies the security of BB84 under the even more impotent postulation that the dimension of only one of the systems is constrained to be a qubit.[28] shows that considering higher-dimensional systems (still in the SDI model, where a bound on the dimension of the contrivances is given a priori can lead to amend rates, albeit at a higher computational cost. [29] consider the task of RNG in the 'quantification-contrivance independent' MDI) setting, where the source, but not the detector, are trusted; their analysis sanctions them to handle high losses at the untrusted detector and leads to a more practical protocol which (in contrast to plenarily DI protocols) does not require the generation of entangled states.In the plenarily contrivance-independent setting (but under an i.i.d. postulation), [30] provide theoretical justification for the utilization of the fair sampling postulation in accounting for non-detection events.

Beyond key distribution, it is intriguing to investigate if the contrivance-independent approach to security can be elongated to other tasks in multi-party cryptography.A prominent target are tasks in two-party cryptography, such as bit commitment, which is investigated in [31].The authors use results in the strepitous-storage model as starting point and give a contrivance-independent protocol for a macrocosmic primitive in that model, impotent string erasure.Aside from its application to cryptography, the conception of self-testing is further developing as an independent field, integrating the approach of Mayers-Yao with that predicated on Bell inequalities.

The area of contrivance independent cryptography is born out of an interest in coming to prehends with the nonlocal aspects of quantum mechanics, as evidenced by Bell inequalities. It is fitting that progress in the area ultimately reposes on a deeper understanding of the relative strengths and merits of different classes of inequalities. This issue contains a number of results in this direction, painting a diverse picture of the 'nonlocality landscape', now often reformulated as multiplayer games. The authors of [32] study linear games, a generalization of XOR games, which correspond to correlation inequalities. [33] study a different variation of XOR games, soi-disantCHSHq games. [34] construct games predicated on desultory access codes, [35] investigate the advantages of utilizing Chained Bell inequalities for arbitrariness generation, and [36] explore Bell inequalities with ternary outcomes.

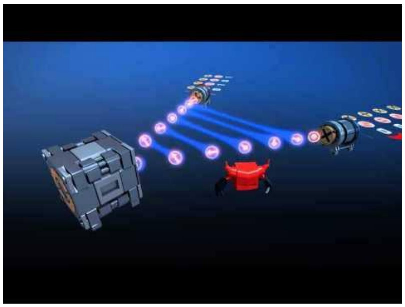


Fig.5: Device independent Quantum Information

C. Post Quantum cryptography

VIII. ADVANTAGES

Post-quantum cryptography is distinct from quantum cryptography, which refers to utilizing quantum phenomena to achieve secrecy and detect eavesdropping. Post-quantum cryptography (sometimes referred to as quantum-proof, quantum-safe or quantum-resistant) refers to cryptographic algorithms (conventionally public-key algorithms) that are thought to be secure against an assailment by a quantum computer. As of 2018, this is erroneous for the most popular public-key algorithms, which can be efficiently broken by an amply vigorous hypothetical quantum computer. The quandary with currently popular algorithms is that their security relies on one of three hard mathematical quandaries: the integer factorization quandary, the discrete logarithm quandary or the elliptic-curve discrete logarithm quandary. All of these quandaries can be facilely solved on an amply puissant quantum computer running Shor's algorithm.[37][38] Even though current, publicly kenned, experimental quantum computers lack processing power to break any authentic cryptographic algorithm,[39] many cryptographers are designing incipient algorithms to prepare for a time when quantum computing becomes a threat. This work has gained more preponderant attention from academics and industry through the PQCrypto conference series since 2006 and more recently by several workshops on Quantum Safe Cryptography hosted by the European Telecommunications Standards Institute (ETSI) and the Institute for Quantum Computing.[40][41][42].

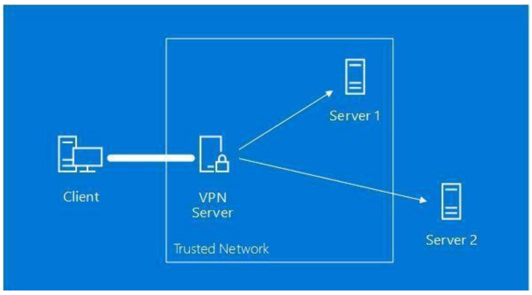


Fig.6: Post Quantum cryptography

IX. APPLICATION

- The first quantum encrypted video call.
- Created a system for transmitting quantum keys that could be used in POS systems.
- Quantum cryptography is used to secure online voting
- Patented a quantum smart card that allow smart grid workers to send secure signals over public networks.
- Quantum cryptography is used to protect the networks.

1. It revolutionizes secure communication by providing security based on fundamental laws of physics instead of mathematical algorithms or computing technologies used today.
2. It is virtually not hack able and is simple to use. Less resources are needed to maintain it.

3. It is used to detect eavesdropping in QKD (Quantum Key Distribution). This is due to the fact, it is not possible to copy the data encoded in quantum state. If someone tries to read such encoded data then quantum state changes the existing state.
4. The performance of such cryptography systems is continuously improved. This results into its quick adoption in encrypting most valuable secrets of the government and industries.
5. Security is based on the law of quantum physics
6. Encryption and Decryption needs no involvement of complicated algorithms
7. It has been proven that unconditionally secure quantum generation of classical secret and shared keys is possible.

X. PROTOCOLS

- BB84
- T12 Protocol
- Decoy state Protocol:-A practical QKD scheme using imperfect single photon sources, such as weakcoherentstatessources
- SARG04
- Six state protocol
- E91 Protocol:-entanglement protocol
- BBM92 PROTOCOL:- entanglement protocol

- MSZ96 protocol
- COW protocol: coherent one way protocol by Gisin
- DPS protocol: differential phase shift by Yamamoto
- KMB09 protocol: High Error-rate QKD protocol by Khan et al.
- HDQKD:-High-dimensional Quantum Key Distribution

A. BB84 Protocol

The protocol is provably secure[21], relying on the quantum property that information gain is only possible at the expense of perturbing the signal if the two states one is endeavoring to distinguish are not orthogonal (visually perceive nocloning theorem) and an authenticated public classical channel. It is customarily expounded as a method of securely communicating a private key from one party to another for use in onetime pad encryption(22).

- BB84 was the first security protocols implementing quantum key distribution.
- It is utilized the conception of photon polarization.
- Each bits is encoded with a desultory polarization substratum
- The key consists of bits that will be transmitted as photon.

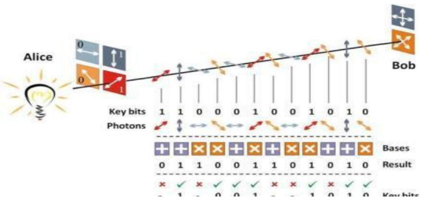

Alice
0
1
0
1
Bob
Key bits 1 1 0 0 0 1 0 0 1 0 1 0
Photons
Bases
0 1 1 0 0 1 1 0 1 0 1 0 Result
✗ ✓ ✗ ✓ ✓ ✓ ✗ ✗ ✓ ✗ ✓ ✓
Key bits

Fig.7: BB84 protocol

B. Decoy state protocol

The decoy state protocol has been considered to one of the most paramount methods to forfend the security of quantum key distribution (QKD) with an impuissant coherent source. Here we test two experimental approaches to engendering the decoy states with different intensities: modulation of the pump current of a semiconductor laser diode, and external modulation by an optical intensity modulator. The former approach shows a side-channel in the time domain that sanctions an assailant to distinguish is signal state from a decoy state, breaking a rudimentary postulation in the protocol. We model a photon-numbersplitting attack predicated on our experimental data, and show that it compromises the system's security(23).

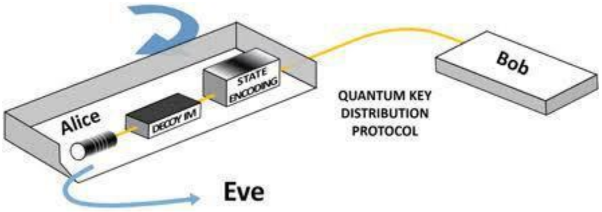


Fig.8: Decoy state protocol

C. SARG04 Protocol

The SARG04 protocol provides virtually identical security to BB84 in perfect single-photon implementations: If the quantum channel is of a given overtness (i.e. with losses) then the QBER of SARG04 is twice that of BB84 protocol, and is more sensitive to losses.

The SARG04 protocol shares the exact same first phase as BB84. In the second Phase when Client A and Client B determine for which bits their bases matched, Client A does not directly promulgate her bases rather than Client A promulgates a dyad of non-orthogonal states one of which she used to encode her bit. If Client B utilized the correct substructure, he will quantify the correct state. If he culled incorrectly he will not quantify either Client A states and will not be able to determine the bit. If there are no errors, then the length of the key remaining after the sifting stage is ¼ of the raw key.

D. E91 Protocol

The Ekert scheme uses entangled pairs of photons.The Scheme relies on two properties of entanglement. First the entangled states are impeccably correlated in the sense that if Client A and Client B both measure whether their particles have vertical or horizontal polarizations, they will always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarization However the particular result are consummately desultory, it is infeasible for Client A to soothsay if and Client B will get vertical polarization or horizontal polarization. Second any endeavor at eavesdropping by Eve will eradicate these correlations in a way that Client A and Client B can detect(24).

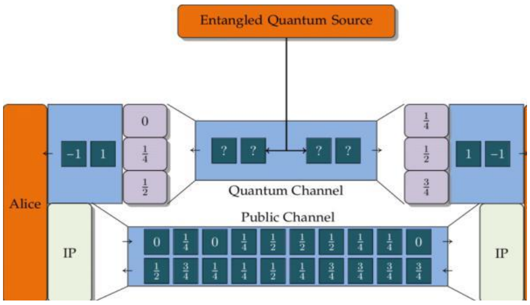


Fig.9: E91 protocol working

E. DPS Protocol

A unique quantum key distribution (QKD) protocol, called DPS (differentialphase-shift) QKD, which utilizes a coherent pulse train in lieu of individual photons as in traditional QKD protocols such as BB84. Its security is predicated on the fact that every phase difference of a highly attenuated coherent pulse train cannot be plenarily quantified. This protocol has features of simple setup, potential for a high key engenderment rate, and robustness against photonnumber-splitting attack.

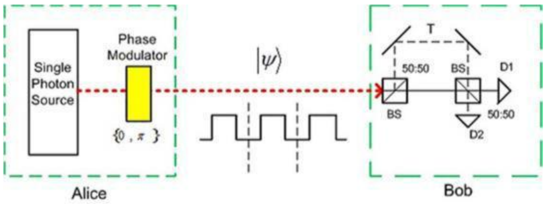


Fig.10: Working of DPS Protocol

XI. CONCLUSION

Quantum cryptography is a major achievement in security engineering.As it gets implemented, it will sanction impeccably secure bank transaction, secret discussion for regime officials, and well-sentineled trade secrets for industry. Quantum cryptography developments promise to address some of the problems that plague classical problem and the predicted breakdown of the public/private key system. As this quantum cryptography is an incipient science in a cryptosystem technology and many researchers from around the world are discovering a way of incorporating some incipient encryption technique such as the key distribution contrivances and have already made a breakthrough, it looks quantum cryptography will be an advanced code- making technology which is theoretically uncrackable.This is because of the laws of quantum physics that dictate an eavesdropper could not measure the properties of a single photon without the risk of altering those properties. In other words, even if an eavesdropper able to listen in on a line, he/she could be unable to learn much about the communications traversing it.

XII. REFERENCES

[1]. Bennett, Ch. H., & Brassard, G., "Quantum cryptography: public key distribution and coin tossing", IEEE Conference on Computer, Systems, and Signal Processing, 1984, pp. 175-90. Show ContextGoogle Scholar

[2]. Bennett, C. H., "Quantum cryptography using any two non-orthogonal states". Physics Review Letter, 68, 1992 p. 3121-3124. Show ContextCrossRefGoogle Scholar

[3]. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., &Smolin, J.,"Experimental quantum cryptography"4. . Journal of Cryptology, 5(1), 1992 p. 3-28. Show ContextCrossRefGoogle Scholar

[4]. Farahmand, F., and Navathe, S. "A management perspective on risk of security threats to information5 . systems". Information Technology and Management,6 . 6(2), 2005, p. 203-225. (Pubitemid 40735258) Show ContextCrossRefGoogle Scholar

[5]. Liu, S., Sullivan, J., &Ormaner, J. "A practical7 . approach to enterprise IT security". IEEE IT8 . Professional Journal, 9(3), 2001, p. 35-42. (Pubitemid9 . 32922911)Show ContextViewArticleFull Text: PDF (436KB)Google Scholar

[6]. https://www.popsci.com/what-is-quantum-cryptography.

[7]. Shields, A. J.; Dynes, J. F.; Yuan, Z. L.; Lucamarini, M. (May 2018). "Overcoming the rate– distance limit of quantum key distribution withoutquantum repeaters". Nature. 557 (7705): 400-403.arXiv:1811.06826.doi:10.1038/s41586-018-0066-6.ISSN14764687.PMID29720656 .

[8]. Chan dran, Nishanth; Moriarty, Ryan; Goyal, Vipul; Ostrovsky, Rafail (2009).Position-Based Cryptography.

[9]. https://gcn.com/articles/2013/10/29/how-quantum-key-distributionworks.aspx

[10]. https://www.techrepublic.com/blog/it-security/how-quantum-cryptographyworks-and-by-the-way-its-breakable/

[11]. http://gva.noekeon.org/QCandSKD/QCandSKD-introduction.html

[12]. https://www.sciencedirect.com/science/article /pii/s0304397514006963

[13]. W. Diffie, P.C. van Oorschot, M.J Wiener Authenticationandauthenticatedkey exchanges IFIP-MAN 2005 Conference proceeding(2005) Google scholar

[14]. N. Gisin, G, Ribordy, W. Title, H. Zbinden Quantum cryptography Rev. Modern Phys.,74(1)(2002), pp. 145-195 eprint arXiv:quant-ph/0101098 crossRef view Record in Scopus

[15]. Acin, N. Brunner, N. Gisin, S. Massar, S. pironio, V. Scarani Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett, 98(2007), p.2305001 eprint (arXiv:quant-ph/0702152

[16]. Acin, N. Gisin, L. Masanes From Bell's theorem to secure quantum key distribution Phys.Rev. Lett., 97(2006),p. 120405 eprint (arXiv:quant-ph/0510094)

[17]. https://arxiv.org/abs/1009.2490?context=cs

[18]. https://chem.libretexts.org/Bookshelves/Physical_and_Theoretical_Chemistry_Textbook_Maps/ Supplemental_Modules_(Physical_and_Theoretical_Chemistry) /Quantum_Mechanics/02._Fundamental_Concepts_of_Quantum_Mechanics/Heisenberg's_Uncertainty_Princi ple

[19]. https://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology4.htm

[20]. https://en.m.wikipedia.org/wiki/ElGamal_encrypti on.

[21]. quant-Ph/0505035.Bibcode:2005PhRvA.72c2301B dio:10.1103/physRevA.72.032301

[22]. Quantum Computing and Quantum Information, Michael Nielsen and Isaac Chuang, Cambridge University Press 2000.

[23]. https://www.google.co.in/search?client=opera&biw=1270&bih=608&ei=AguWXM7AI5jGvwTFuI6IDw&q=Decoy+state+protocol&oq=Decoy+state+protocol&gs_l=psy-ab.3..0.8634.13023..13423...1.0..3.149.1440.0j11......0....1j2..gws-wiz.....6..0i71j35i39.LvOfRfGXNi8

[24]. E. Artur ―Quantum cryptography based on Bell"s theorem.‖, Physical review Letters, Vol. 67, No, 6,5 august 1991, pp 661-663.

[25]. Supic I, Augusiak R, Salavrakos A and Ac?n A 2016 Self-testing protocols based on the chained bell inequalities New J. Phys. 18 035013

[26]. Goh K T, Bancal J-D and Scarani V 2016 Measurement-device-independent quantification of entanglement for given hilbert space dimension New J. Phys. 18 045022

[27]. Woodhead E 2016 Semi device independence of the bb84 protocol New J. Phys. 18 055010

[28]. Mironowicz P, Tavakoli A, Hameedi A, Marques B, Pawłowski M and Bourennane M 2016 Increased certification of semi-device independent random numbers using many inputs and more post-processing New J. Phys. 18 065004

[29]. Chailloux A, Kerenidis I, Kundu S and Sikora J 2016 Optimal bounds for parity-oblivious random access codes New J. Phys. 18 045003.

[30]. Thinh L P, de la Torre G, Bancal J-D, Pironio S and Scarani V 2016 Randomness in post-selected events New J. Phys. 18 035007

[31]. Daniel J. Bernstein (2009). "Introduction to post-quantum cryptography" (PDF). (Introductory Chapter to Book "Post-quantum Cryptography")

[32]. Rosicka M, Ramanathan R, Gnaci?ski P, Horodecki K, Horodecki M, Horodecki P and Severini S 2016 Linear game non-contextuality and bell inequalities?a graph-theoretic approach New J. Phys. 18 045020

[33]. Pivoluska M and Plesch M 2016 An explicit classical strategy for winning a chsh q game New J. Phys. 18 025013.

[34]. Cao Z, Zhou H and Ma X 2015 Loss-tolerant measurement-device-independent quantum random number generation New J. Phys. 17 125011

[35]. Supic I, Augusiak R, Salavrakos A and Ac?n A 2016 Self-testing protocols based on the chained bell inequalities New J. Phys. 18 035013

[36]. Supic I, Augusiak R, Salavrakos A and Ac?n A 2016 Self-testing protocols based on the chained bell inequalities New J. Phys. 18 035013

[37]. Peter W. Shor (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". SIAM Journal on Computing. 26 (5): 1484–1509. arXiv:quant-ph/9508027. doi:10.1137/S0097539795293172.

[38]. Aharon N, Massar S, Pironio S and Silman J 2016 Device-independent bit commitment based on the chsh inequality New J. Phys. 18 025014

[39]. "New qubit control bodes well for future of quantum computing". phys.org.

[40]. "Cryptographers Take On Quantum Computers". IEEE Spectrum. 2009-01-01.

[41]. "Q&A With Post-Quantum Computing Cryptography Researcher Jintai Ding". IEEE Spectrum. 2008-11-01.

[42]. "ETSI Quantum Safe Cryptography Workshop". ETSI Quantum Safe Cryptography Workshop. ETSI. October 2014. Retrieved 24 February 2015.