QUANTUM CRYPTOGRAPHY: THE FUTURE OF SECURITY

[1]Venkatesh Prasad. G, [2]Rohit A S Nair, [3]Nagamani S , [4] Madhavi Giridhar D

[1] Student, School of Computational Sciences and IT, Garden City University, Bangalore, India.

[2] Student ,School of Computational Sciences and IT, Garden City University, Bangalore, India.

[3]Assistant Professor, School of Computational Sciences & IT, Garden City University, Bangalore, India.

[4]Assistant Professor, School of Computational Sciences & IT, Garden City University, Bangalore, India.

Abstract:
As technology leaps forward and is continuously growing on a fast pace and billions of terabytes of data being stored everyday the urge to data more and more secure swings into action, the data could contain from simple text documents which are publicly available to personal messages and super secret files, we never know! But as the privacy worm bugs people its on security researchers to calm them down, but how? Thats where cryptography swings into actions and shows how the transfer of data from location A to location B be secured by encrypting it. But the problem doesn't end here with the introduction to cryptography and encryption methods there is a new urge to make it "better", but why? Why not? So in this paper we're going to take a look at a cryptographic method called Quantum Cryptography which is he science of exploiting quantum mechanics for cryptographic tasks where the phenomenon of single-photon interference is used to perform quantum cryptography over an fibre optic cable from one end to another as a communication link.

Index Terms: Cryptography, Encryption, Communication, Quantum, Data.

I-INTRODUCTION

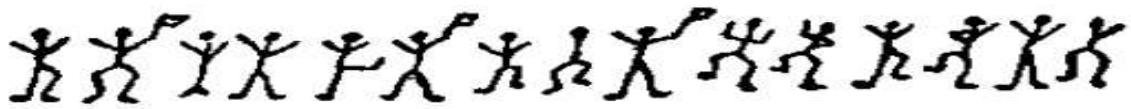
As mentioned in the abstract as things tend to grow we tend to make them better and better but now here before we get into the topic of quantum cryptography and more, lets first have a look at cryptography. So then what is cryptography? Cryptography or cryptology is a process in which the plain text in converted into an unreadable or secret form called the cipher text which would make it very difficult for a "man-in-the-middle" to understand what the message/data that was being shared from (let's use the typical ancient words) Alice to Bob. In today's world the need for data privacy/secrecy is vital as ever, but as always the urge to make things better is what is driving cryptography and data privacy. Even with encryptions algorithm like the RSA algorithm etc., the need for better cryptographic methods would never stop. Well for now the 2 seemingly unrelated philosophical foundations of quantum mechanics are now being brought to bear directly on the problem of communications security in the potentially practical emerging technology of quantum cryptography.

In this paper we shall discuss about quantum cryptography and its potential applications. Well then the question arises again, what is quantum cryptography, will we ever need it? What is wrong with the cryptographic methods we already have? What are its limitations and what are the prospects for future improvements? The two main goals of cryptography are sender and a receiver to have a receipt or identity to be able to communicate without the "man-in-the-middle" knowing it so the its proven that there was no tampering of data during the transfer both these goals can be achieved by providing a secret key for both sender and the receiver as a form of receipt whilst irrespective of the same key for both or not hence generating a key truly random to its origin would make it tougher but there is a problem, (well there is always a problem) it's known as the "key distribution problem", the problem states that how does the sender and receiver be sure that the man in the middle or the eavesdropper has partial information or full information while on its way to its destination? Well the key distribution has be relying on the establishment of a physically secure channel or in other words a trusted courier or a conditional security of difficult mathematical equations on a the public key, hence making quantum key distribution (QKD) the most obvious solution for this problem where it is impossible to "tap" single quantum signal with common methods that

are being used in the modern day. In remainder of this paper we move on further by understanding cryptography, the importance of QKD and more

II-CRYPTOGRAPHY

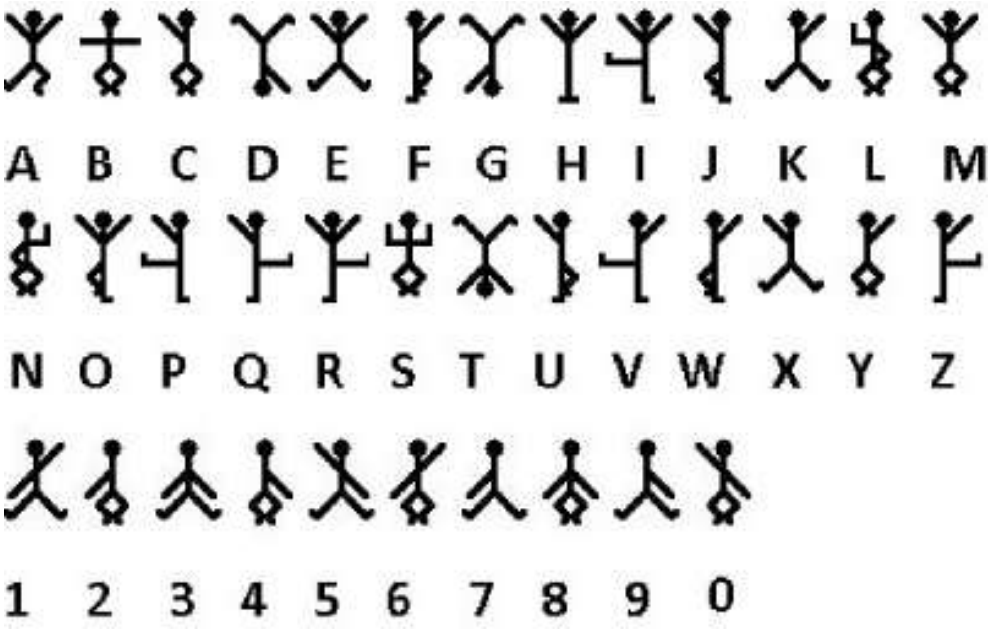
To explain to significance of quantum cryptography it is important to explain some of the features of cryptography in common. These features can easily be explained with real life examples for easier understanding. In this example of



Sherlock Holmes' "Dancing Men" which spell out the message "AM HERE ABE

pher we take a look at Sir Arthur Conan Doyle's "The Adventure of the Dancing Men." In this story, Elsie, the American wife of an English gentleman, Hilton Cubbitt, is terrorized by the appearance of chalked stick-figures outside her house. Sherlock Holmes is called in and quickly realizes that the figures are not the scribbling of children, but rather are a form of cryptography, in which each letter of the alphabet as been substituted with a stick figure, known only to the sender which seem to look like this : and the intended recipient, Elsie. This cryptosystem yields to the crypt analytical powers of Sherlock Holmes, who breaks the cipher after collecting only 62 characters, by observing the relative frequencies of the different characters, identifying the most frequent with the letter "E" and using intuition.2 with this information the master detective is able to compose his own cryptogram summoning Abe Slaney to Elsie's 5 house. The criminal, believing that only Elsie could have composed a "Dancing Men" message, is promptly arrested by the police on his arrival. The deciphering text or the receiver's key looking like this: this story explains several cryptographic issues, it shows that the two aspects of cryptography can be accomplished if the sender and the receiver share the knowledge of the secret key.

we take a look at Sir Arthur Conan Doyle's "The Adventure of the Dancing Men." In this story, Elsie, the American wife of an English gentleman, Hilton Cubbitt, is terrorized by the appearance of chalked stick-figures outside her house. Sherlock Holmes is called in and quickly realizes that the figures are not the scribbling of children, but rather are a form of cryptography, in which each letter of the alphabet as been substituted with a stick figure, known only to the sender which seem to look like this : and the intended recipient, Elsie. This cryptosystem yields to the crypt analytical powers of Sherlock Holmes, who breaks the cipher

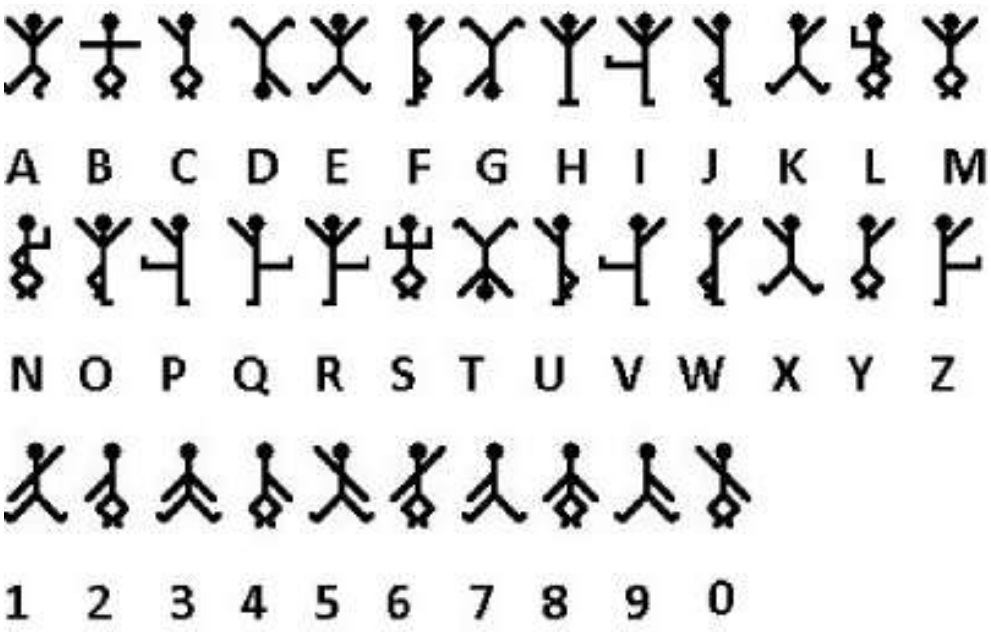


Sherlock Holmes' "Dancing Men" which spell out the message "AM HERE ABE SLANEY." Decoded

after collecting only 62 characters, by observing the relative frequencies of the different characters, identifying the most frequent with the letter "E" and using intuition.2 with this information the master detective is able to compose his own cryptogram summoning Abe Slaney to Elsie's 5 house. The criminal, believing that only Elsie could have composed a "Dancing Men" message, is promptly arrested by the police on his arrival. The deciphering text or the receiver's key looking like this: this story explains several cryptographic issues, it shows that the two aspects of cryptography can be accomplished if the sender and the receiver share the knowledge of the secret key.

$$P = E_K^{-1}(C) \quad ,$$

1) **Key material, key distribution & one-time pad** As mentioned there are many modern cryptographic methods, in the modern-day secret key or symmetric encryption algorithms, the plain text is converted into a cipher or cryptogram which is commonly known, as any particular communication it all the encryption is dependent on the key which is secretly shared only b/w the sender and the receiver generally known as Alice and bob. Moving forward the second most important assumption of cryptography or in other words known as kirchoff's view the secrecy must not completely depend on the algorithm hence generating a cryptogram and sending it to bob or the receiver:and hence recovering the plain text, the process slips under the radar of the eavesdropper which indicates that the attacker was not able to get hold of the key and hence proving that the message sent from Alice to bob was unread or not tampered. Many cryptographic systems have been made using this concept DES System which uses a 56-bit key bring one of the them, but there is a more secure and unbreakable method which is known as the one-time was in which the sender and the receiver acquire a quantity of secrecy keys which are truly random which is as large as the message that would be transmitted, in this method the senders plain text let's call it "P" are created in a sequence P={p1 , ... , pn }and then encrypts with the key let's call it "K" which is in a sequence K={k 1 , ... , k n } to give a result of the cryptography let's call it "C" which is formed in a sequence C = {c1 , ... , cn }, where using modular arithmetic in the base, N, of the message characters, and when the receiver the encrypted message or the cryptogram, the receiver subtracts his/her key using modular arithmetic hence getting the desired plain text back. But if the on-time pad truly unbreakable then why is it not exclusively used? Well because the key generation involves a distribution and management problem. The necessity for generating, distributing and storing the key material in advance renders the one-time pad system vulnerable to the "insider threat." In theory the one-time pad is unbreakable, but in practice, it has been very difficult to use. This is one reason for the popularity of public key cryptography systems which are "difficult," but not impossible, to break, and easy to use



Sherlock Holmes' "Dancing Men" which spell out the message "AM HERE ABE SLANEY." Decoded

$$C = E_K(P) \qquad c_i = p_i + k_i \pmod N$$

$$\| \Phi \rangle \| \equiv |\langle \Phi | \Phi \rangle|^{1/2} \quad .$$

2) Quantum Key Distribution or QKD To know what QKD is we should ignore the commonly used key distribution where the sender sending a particular key to the receiver instead we use a a more symmetrical starting point in which the sender and the receiver generate their own key, unique random number sets contains more numbers than required and then compare the generated set of number to refine the share subset which becomes a key material. The only necessity for the key material is that the number should be random and secretive. This can be accomplished by distillation of the sequence of the senders token, one type of 0 and a different type of 1 and sent to the receiver by the sender and then the receiver moves forward with his/her set with bit-by-bit synchronization with the sender and then compares it with the senders token bit and replies the sender by telling if the token/key is the same or not with the receivers information both the sender and receiver can identify the bits in common and hence keeping the bits and forming the key and discarding the others. If one of the senders token fails to reach the receiver it doesn't stop the process because it is the tokens that arrive which are used in the distillation process the most obvious problem with this method is that if the token are classical objects they carry the bit value before they're observed by the sender hence this could mean it could passively be sniffer by an attacker, now lets take a look if its possible to generate a secure key if the tokens are quantum objects.We will use the B92 QKD protocol in terms of the preparation and measurement of states in a two-dimensional Hilbert space such as that of a spin-1/2 particle. The spin operators σ1 , σ2 , σ3 , obey the algebra and then introduce a ba the z-axis satisfying the orthonormality relations

$$[\sigma_i, \sigma \qquad \sigma_3 \begin{cases} |\uparrow\rangle \\ |\downarrow\rangle \end{cases} = \begin{cases} +|\uparrow\rangle \\ -|\downarrow\rangle \end{cases}, \qquad j,k = 1,2,3$$

$$\langle\uparrow|\uparrow\rangle = \langle\downarrow|\downarrow\rangle = 1$$

$$\langle\uparrow|\downarrow\rangle = 0$$

3) From these states we can also make eigenstates with spin-up or spin-down along the x-axis where

$$|\rightarrow\rangle = 2^{-1/2}\left(|\uparrow\rangle + |\downarrow\rangle\right) \text{ and } |\leftarrow\rangle = 2^{-1/2}\left(|\uparrow\rangle - |\downarrow\rangle\right).$$

$$\sigma_1 \begin{cases} |\rightarrow\rangle \\ |\leftarrow\rangle \end{cases} = \begin{cases} +|\rightarrow\rangle \\ -|\leftarrow\rangle \end{cases},$$

4) A (von Neumann) measurement in quantum theory is a projection operator in Hilbert space.For example, a measurement for spin-down along the z-axis is represented by the projection operatorand similarly a measurement for spin-down along the x-axis is represented byThe result of a measurement P on a state ψ is given by the "collapse of the wavefunction" where its describe the first outcome as a "pass" and the second as "fail." Here we have defined the norm as

$$|\psi\rangle \rightarrow \begin{cases} \dfrac{P|\psi\rangle}{\|P|\psi\rangle\|} & \text{with probability } \langle\psi|P|\psi\rangle \\ \dfrac{(1-P)|\psi\rangle}{\|(1-P)|\psi\rangle\|} & \text{with probability } \langle\psi|(1-P)|\psi\rangle \end{cases},$$

5) Thus, the outcome of a measurement in quantum mechanics is, in general, only predictable with some probability.

For the B92 protocol the sender has two non-orthogonal state preparations: A or → ; and the receiver can make two non-orthogonal measurements: PB or P← . The "pass" probabilities of the various preparation-measurement combinations are given in Table 1.

	$\|\uparrow\rangle$	$\|\rightarrow\rangle$
$P_{\|\downarrow\rangle}$	0	0.5
$P_{\|\leftarrow\rangle}$	0.5	0

In the first step of the B92 protocol the sender and the receiver generate their own independent sets of random numbers. In Step 2 they proceed through their sets bit-by-bit in synchronization, with Alice preparing a state for each of her bits according to Table 2. the sender sends each state over a "quantum channel" to the receiver. The receiver makes a measurement of each state he receives, according to the value of his bit as given by Table 3,and records the result ("pass" = Y, "fail" = N).

bit	state
0	$\|\uparrow\rangle$
1	$\|\rightarrow\rangle$

Table 2

bit	measurement
0	$P_{\|\leftarrow\rangle}$
1	$P_{\|\downarrow\rangle}$

Table 3

6)Practical implementation of QKD The most apparent way to execute the QDK quantum channel is with a single- photon polarization state, like preparation of vertical and right-handed-circular polarizations, and then measuring of the horizontal linear and left-handed-circular polarizations, another set of single-photon states lets call it phase state having the properties required for quantum cryptography and be constructed by allowing a photon to impinge on a simple beam splitter. We can see the action of a lossless beamsplitter in terms of photon creation and annihilation operators as a transformation from the two "in" modes to the two "out" modes as :

where we have implemented an adjustable phase shift, φA, in the second output. Here

$$\left[a_{in}^{(1)}, a_{in}^{(2)}\right] = \left[a_{in}^{(1)}, a_{in}^{(2)\dagger}\right] = \left[a_{in}^{(1)\dagger}, a_{in}^{(2)}\right] = 0$$

$$\left[a_{in}^{(1)}, a_{in}^{(1)\dagger}\right] = \left[a_{in}^{(2)}, a_{in}^{(2)\dagger}\right] = 1 \quad ,$$

$$a_{in}^{(1)}|0\rangle = a_{in}^{(2)}|0\rangle = 0$$

$$a_{out}^{(2)} \qquad |\downarrow\rangle \equiv 2^{-1/2}\left[a_{out}^{(2)\dagger} + ia_{out}^{(1)\dagger}\right]|0\rangle \quad \text{for} \quad \phi_B = \pi$$

$$\text{or}$$

$$|\leftarrow\rangle \equiv 2^{-1/2}\left[ia_{out}^{(1)\dagger} + ia_{out}^{(2)\dagger}\right]|0\rangle \quad \text{for} \quad \phi_B = 3\pi/2 \quad .$$

$$a_{out}^{(3)} = 2^{-1/2}\left[ie^{i\phi_B}a_{out}^{(1)} + a_{out}^{(2)}\right]$$

$$a_{out}^{(4)} = 2^{-1/2}\left[e^{i\phi_B}a_{out}^{(1)} + ia_{out}^{(2)}\right] \quad .$$

where 0 is the "vacuum" (no photon) state, and similarly for the "out" operators. Thus, if we equip Alice with this beamsplitter and she introduces a single photon state at the "in"-port "this amounts to a preparation of the non-orthogonal "out" states the receiver may now introduce the above "out" modes into the "in" ports of a second beamsplitter and add an additional phase, φB , to Alice's "out" "1" mode, giving final "out" state destruction operators

$$\left|in^{(1)}\right\rangle = a_{in}^{(1)\dagger}|0\rangle \quad ,$$

$$|\uparrow\rangle \equiv 2^{-1/2}\left[a_{out}^{(1)\dagger} + ia_{out}^{(2)\dagger}\right]|0\rangle \quad \text{for} \quad \phi_A = 0$$

$$\text{or}$$

$$|\rightarrow\rangle \equiv 2^{-1/2}\left[a_{out}^{(1)\dagger} - a_{out}^{(2)\dagger}\right]|0\rangle \quad \text{for} \quad \phi_A = \pi/2 \quad .$$

If a detector is placed in the receivers "3" output port, the detection of a photon corresponds to a projection onto the non-orthogonal states

The four states constructed above have the necessary orthogonality properties for B92 QKD. Thus, by combining the two beamsplitters of the sender and the receiver may construct an interferometric version of QKD where the probability that a photon injected by the laser source is detected is given byThus, if the sender and the receiver use the phase angles (φA , φB) = (0, 3π/2) for their "0" bits and (φA , φB) = (π/2, π) for their "1" bits they have an exact representation of B92.

To make a working quantum cryptography device using either polarization or phase states we should consider the making, prorate and identification of single photons. An approximation to use a highly attenuated pulsed laser source, with a convenient choice being a probability of 10% that the pulse contains one photon, which means that 8 ~ 90% of the pulses contain no photon, but this is the price that must be paid (in data rate) for having < 1% of pulses containing two or more photons, which are the ones susceptible to a beamsplitting attack.

$$P_D = \cos^2\left(\frac{\phi_A - \phi_B}{2}\right) \quad .$$

REFERENCES:

[1] C. Bennett and G. Brassard, "Quantum Cryptography:Public Key Distribution and Coin Tossing," International Conference on Computers, Systems, and Signal Processing,Bangalore, India, 1984.

[2] A. Ekert, "Quantum Cryptography Based on Bell'sTheorem," Phys. Rev. Lett. 67, 661 (5 August 1991).

[3] Ekert, Artur. "What is Quantum Cryptography?" Centre forQuantum Computation –Oxford University.Conger., S., and Loch, K.D. (eds.). Ethics and computer use. Commun. ACM 38, 12 (entire issue).

[**4**] Johnson, R. Colin. "MagiQ employs quantum technology forsecure encryption." EE Times. 6 Nov. 2002..

[5] Mullins, Justin. "Quantum Cryptography's Reach Extended."IEEE Spectrum Online. 1 Aug. 2003.

[6] Petschinka, Julia. "European Scientists againstEavesdropping and Espionage." 1 April 2004. 7. Salkever,Alex. "A Quantum Leap in Cryptography." BusinessWeekOnline. 15 July 2003.

[7] Schenker, Jennifer L. "A quantum leap in codes for securetransmissions." The IHT Online. 28 January 2004..

[8] MagiQ Technologies Press Release. 23 November 2003.

[9] Schenker, Jennifer L. "A quantum leap in codes for securetransmissions." The IHT Online. 28 January 2004.

[10] C. Elliott, "Building the quantum network," New J. Phys. 4(July 2002) 46.

[11] Pearson, David. "High!speed QKD Reconciliation using Forward Error Correction." Quantum Communication,Measurement and Computing. Vol. 734. No. 1. AIP Publishing, 2004.

[12] Curcic, Tatjana, et al. "Quantum networks: from quantumcryptography to quantum architecture." ACM SIGCOMM Computer Communication Review 34.5 (2004): 3-8.

[13] Shor, Peter W., and John Preskill. "Simple proof of securityof the BB84 quantum key distribution protocol." PhysicalReview Letters 85.2 (2000): 441.

[14] Bienfang, J., et al. "Quantum key distribution with 1.25Gbps clock synchronization." Optics Express 12.9 (2004):2011-2016.

[15] Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto."Differential phase-shift quantum key distribution." Photonics Asia 2002. International Society forOptics and Photonics, 2002.

[16] Barnum, Howard, et al. "Authentication of quantummessages." Foundations of Computer Science, 2002.Proceedings. The 43rd Annual IEEE Symposium on. IEEE,2002.

[17] Elliott, Chip, David Pearson, and Gregory Troxel. "Quantumcryptography in practice." Proceedings of the 2003conference on Applications, technologies, architectures, andprotocols for computer communications. ACM, 2003.

[18] Buttler, W. T., et al. "Fast, efficient error reconciliation forquantum cryptography." Physical Review A 67.5 (2003):052303