International Journal of Innovative
Computing, Information and Control
Volume **14**, Number **1**, February **2018**

 ISSN 1349-4198
pp. 371–377

SIGNIFICANCE OF KEY DISTRIBUTION USING QUANTUM CRYPTOGRAPHY

Vurubindi Padmavathi[1], Bulusu Vishnu Vardhan[2]
and Addepalli V. N. Krishna[3]

[1]Department of Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Yamnampet, Ghatkesar, Hyderabad 501301, Telangana, India
chpadmareddy1@gmail.com

[2]Department of Computer Science and Engineering
JNTUH College of Engineering, Jagitial
Karimnagar 505327, Telangana, India
mailvishnu@yahoo.com

[3]Department of Computer Science and Engineering
Christ University
Hosur Road, Bengaluru 560029, Karnataka, India
hari_avn@rediffmail.com

Received May 2017; revised September 2017

Abstract. *The main challenge to the cryptosystems is providing secrecy in distributing key. This challenge is explained through key distribution problem. The key distribution in classical cryptosystems is based on classical information or bits. As bits can be replicable, there will be scope for an eavesdropper to make copies of information. The classical key distribution methods rely on computational assumptions which are not potential to offer anticipated results. Consequently, it is solved using laws of quantum mechanics, and the solution is Quantum Key Distribution (QKD). In QKD, the bits are encoded into quantum states or qubits using photon polarization. The qubits cannot be replicated as per the laws of quantum mechanics. An attempt to replication will introduce errors. Thus an eavesdropping will inevitably lead to detectable traces and then the legitimate entities will decide upon discarding a particular qubit. BB84 protocol is the first QKD protocol evolved in 1984. This paper notifies the significance of QKD over key distribution performed using classical methods. It is evidently shown that the time taken to distribute a secret key through BB84 QKD protocol is comparatively less than the classical methods of key distribution.*

Keywords: Classical key distribution, Photon polarization, QKD, Quantum cryptography, Quantum mechanics, Quantum key distribution, Qubits

1. **Introduction.** In classical cryptography, the communication is carried out between two entities using classical information. As it is known that classical information can be replicated, it is trouble-free for an eavesdropper to make copies of it and to read. Therefore, it is necessary to provide secure communication using the concepts of quantum cryptography. In 1969, Wiesner proposed that the uncertainty principle of quantum mechanics could be used for cryptography [1]. Thus, this proposal hatched into quantum cryptography which is a promising field for cryptographers. Quantum cryptography is a well thought research area where two entities can have secure communications by implementing laws of quantum mechanics. This thought was extended to put forward a process for QKD which is verifiably secure under the laws of quantum mechanics by

Wiedemann [2]. The basis of QKD is the photons which are the predominant elements in the distribution of secret keys whose transmission is fast and secure.

Bennet and Brassard had association with Stephen Wiesner and contributed to projecting the QKD first in 1984, named as BB84 protocol [3]. It uses two communication channels namely a classical channel and a quantum channel. The classical information is transmitted on classical channel and qubits through the quantum channel.

It is easy to store, transmit and process classical information or bit (0s and 1s). It is easy to make copies of classical information in terms of bit. One can measure classical bit without disturbing it. In quantum computer it is difficult to store, transmit and process. There is no method to copy quantum bit as per no-cloning theorem [6]. Quantum bit can be destroyed when measured in incorrect photon polarization.

In a classical computer the memory stores a bit and can execute computations on only one set of numbers. However, a quantum computer stores a quantum state or a quantum bit popularly known as qubit. It exists in the state $|0\rangle$ or $|1\rangle$ and can also exist in a superposition state. The superposition state is represented as $|\Phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, where α, β are complex numbers. It can store superposition of 2^n n-bit strings. Consequently, on a quantum computer one can compute in a single step with 2^n values. This enormous massive parallelism is one reason why quantum computing is so powerful [4,7]. The D-Wave 2X processor, with 1000 qubits, can evaluate at once all 2^{1000} possible solutions [5].

The communication through quantum channel is secure since the transmissions depend on the unchallengeable quantum mechanics laws. The two prime components of quantum mechanics are, namely the principle of Heisenberg uncertainty and the principle of photon polarization. The Heisenberg uncertainty principle states that the two related physical properties cannot be measured simultaneously. The principle of photon polarization states that the replication of qubits is not possible by means of theorem of no-cloning [3].

In 2017, a method for chip based QKD is introduced to demonstrate BB84, differential phase shift, coherent one way protocols [12]. The BB84 protocol can offer keys for distances 200 km and 240 km, with and without multiplexing respectively [13] is established in 2017. QKD was built over 307 km using optical fiber [14]. In 2015, QKD systems with GHz-clocked were presented to manage keys [15].

In 2011, Los Alamos National Laboratory had developed a hub and spoke network to route messages [16]. In Tokyo, a star network named as Tokyo QKD network was established, which connects a range of centers. It incorporates three layers; they are quantum layer, the key management layer, the communication layer [17]. A project to build QKD network was implemented by Europe which is SEcure COmmunication based on Quantum Cryptography (SECOQC). It was a collective research achievement by 41 industrial and research organizations [18,19]. The DARPA team had set up a quantum network which is a quantum key distribution network with ten nodes in Massachusetts, USA and is in operation since 2004 [20].

This paper is organized as follows. Section 2 presents problem statement. Section 3 elucidates about BB84 QKD protocol. Section 4 describes about classical key distribution algorithms. Section 5 explicates the implementation and results of significance of QKD through comparisons made between QKD and classical methods of key distribution and finally Section 6 presents conclusions and future directions.

2. **Problem Statement.**

The noteworthy features of key distribution are security and the time required in distributing the key. However, the classical information is replicable; consequently it becomes easy for an eavesdropper to know the information. The classical methods rely on computational assumptions which are not potential to offer anticipated

results. Hence, an elegant concept of quantum key distribution is employed to distribute the key. This paper confirms that distribution of key is secure due to two laws of quantum mechanics. The replication of qubits is not possible and the act of measuring a qubit disturbs the information. Thus an eavesdropping will inevitably lead to detectable traces and then the legitimate entities will decide upon discarding a particular qubit.

Also, it is evidently shown that the time taken to distribute a key using QKD is less than the key distribution done using classical approach. Apparently, it should be less in order to have fast and effective communication. The observations are made for time taken to distribute a secret key between BB84 QKD protocol and classical key distribution protocols that is RSA and AES.

3. **BB84 QKD Protocol.** Bennet and Brassard put forward the well known BB84 QKD protocol for the first time in 1984. The two constituents of BB84 protocol are namely rectilinear basis (+) and diagonal basis (X) and four states of photons which are polarized. Using photon polarization the bits are encoded into qubits. A binary 0 is a photon polarization of 0° in the rectilinear basis or 45° in the diagonal basis. A binary 1 is a photon polarization of 90° in the rectilinear basis or 135° in diagonal basis [3]. The two basis and photon polarization are shown in Figures 1 and 2 respectively [8].

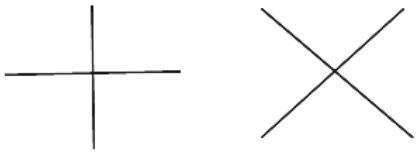

FIGURE 1. Rectilinear and diagonal basis

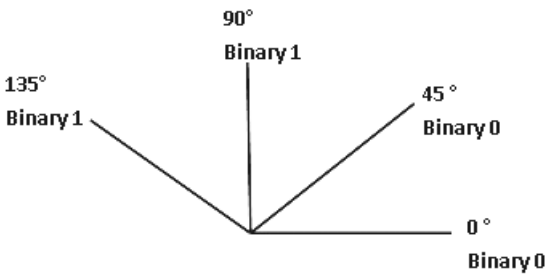

FIGURE 2. Photon polarization to represent bits

BB84 protocol requires two communication channels, one is classical channel and the other is quantum channel which is established between sender and receiver in order to distribute a secret key. They transmit qubits through quantum channel and the conventional messages through classical channel. The subsequent steps will elucidate the process to distribute a secret key. Steps 1 and 2 require quantum channel. Steps 3 to 5 require classical channel. The following notations are used to carry out BB84 QKD protocol.

- $b \in \{0,1\}^n$: Sender's bit string b, n is the original length of the secret key.
- $d \in \{0,1\}^m | m \leq n$: Receiver's bit string d.
- $\theta_a \in \{+, X\}^n$: Sender's basis in string.
- $\theta_b \in \{+, X\}^m | m \leq n$: Receiver's basis in string.

- *Step 1: Sender preparation of qubits.* Sender prepares qubits in sequence manner by choosing random bits $b \in \{0,1\}^n$ and representing those using corresponding random basis $\theta_a \in \{+, X\}^n$, where '+' and 'X' are rectilinear and diagonal basis respectively.

$|\Phi\rangle\,(b, \theta_a)$ is denoted as a state for n photons that encodes the bits $b[x]$ in the basis $\theta[x]$ for every $x \in n$ and transmits to the receiver through quantum channel.

- *Step 2: Receiver measurement of qubits.* Receiver measures each of received qubits $|\Phi\rangle\,(d, \theta_b)$ using either the rectilinear basis $\{|\Phi\rangle\,(0, +), |\Phi\rangle\,(1, +)\}$ and diagonal basis $\{|\Phi\rangle\,(0, X)$ and $|\Phi\rangle\,(1, X)\}$. If receiver's measurement, i.e., $|\Phi\rangle\,(d, \theta_b)$ matches with sender's $|\Phi\rangle\,(b, \theta_a)$, then they will share the same bits.
- *Step 3: Receiver reports basis.* Receiver reports his basis randomly through the classical channel denoted as S.
- *Step 4: Sender confirms the qubits.* Sender confirms the correctness of basis to receiver.
- *Step 5: Sifted key.* Both discard the bits for which the measurement is incorrect and the correct bits is the secret key known as sifted key represented as k [3].

4. **Classical Key Distribution Algorithms.** The significance of QKD is shown by comparing the time taken for secret key distribution with symmetric and asymmetric classical key distribution algorithms. RSA public key algorithm and Advanced Encryption Standard (AES) are taken as examples for asymmetric and symmetric algorithm respectively to illustrate the defined problem.

4.1. **Asymmetric algorithm.** The RSA is an asymmetric algorithm in which the plaintext and ciphertext are integers between 0 and $n - 1$. Preferably, the numbers should be large in order to avoid attacks. The encryption key or public key $\mathrm{K_U}$ is a pair of positive integers (e, n) and the decryption key or private key of $\mathrm{K_R}$ is a pair of positive integers (d, n). The values of n and e are known to both sender and receiver and the value of d is known only to the receiver.

For plaintext M and ciphertext C, the encryption and decryption processes are of the following forms, for some n [9].

Plaintext $\mathrm{M} = \mathrm{C}^d \pmod n$

Ciphertext $\mathrm{C} = \mathrm{M}^e \pmod n$

4.1.1. *Key generation.* The following steps will explain the key generation process of RSA algorithm.

- *Step 1:* Select p, q where p and q are both prime numbers
- *Step 2:* Calculate $n = p \times q$
- *Step 3:* Calculate $\phi(n) = (p - 1) \times (q - 1)$ where $\phi(n)$ is Euler totient function
- *Step 4:* Select integer e where GCD $(\phi(n), e) = 1$ and $1 < e < \phi(n)$
- *Step 5:* Calculate d where $d = e - 1 \bmod(\phi(n))$
- *Step 6:* Public key $\mathrm{K_U} = (e, n)$
- *Step 7:* Private key $\mathrm{K_R} = (d, n)$

4.1.2. *Primality test.* Primality test is a practical probabilistic algorithm for testing large numbers in random fashion, for testing whether a number is prime or not. The inputs to RSA algorithm are two large prime numbers; hence the numbers have to be tested for primality. There are several primality test algorithms [21,22]. The complexity of algorithms for testing will vary.

4.2. **Symmetric algorithm.** The Advanced Encryption Standard (AES) is a symmetric encryption algorithm. It operates on data block of 128 bits called as State. The State is organized as a four by four byte matrix. The key lengths are 128, 192 or 256 bits implemented on 10, 12 or 16 rounds respectively. AES encrypts an input block by applying the same round function. The iterations of round function alter the State by applying non-linear, linear, and key-dependent transformations. Each round transforms 128-bit

State into a modified 128-bit State. Every byte of the State matrix is affected by four transformations [10].

5. **Implementation and Results.** The comparison of time taken for secret key distribution between classical (asymmetric and symmetric) key distribution and quantum key distribution is implemented.

5.1. **Comparison of time taken for key distribution between asymmetric and quantum key distribution.** The implementation is shown using MatLab R2014a [11]. Two parameters are taken into consideration: 1) key generation time and 2) key distribution time. Assuming both the channels (classical and quantum) are secure, the implementation is carried out between RSA public key algorithm [9,10] vs. BB84 QKD protocol. The time is measured in seconds. The unit for key size is bits and qubits for classical key distribution and QKD respectively.

Table 1 shows the comparison of time taken for RSA public key distribution and BB84 QKD protocol for 128, 256, 512, 1024 and 2048 length of key. It is observed that BB84 takes less time to distribute key. There are differences of 15s, 17s, 21s, 25s and 29s for 128, 256, 512, 1024 and 2048 key sizes respectively. It is plotted in Figure 3.

TABLE 1. Comparison of time taken between asymmetric key distribution and quantum key distribution algorithms

Key size (in bits/qubits)		**128**	**256**	**512**	**1024**	**2048**
Time taken for key distribution (in s)	**RSA algorithm**	0.063	0.096	0.135	0.172	0.218
	BB84 QKD protocol	0.048	0.079	0.114	0.147	0.189

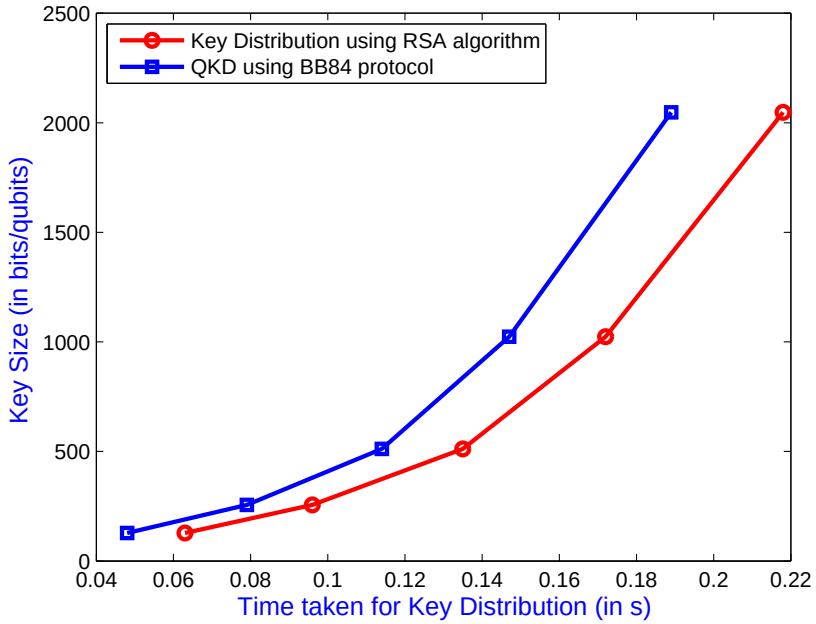

FIGURE 3. Comparison of key distribution between RSA algorithm and BB84 protocol

5.2. **Comparison of time taken for key distribution between symmetric and quantum key distribution.** Table 2 exhibits the comparison of time taken for AES symmetric key distribution and BB84 QKD protocol. The length of the key is 128, 192 and 256 (bits/qubits). There are differences of 11s, 13s and 17s for 128, 192 and 256 key sizes respectively which is plotted in Figure 4.

It has been explored that the time taken to distribute key with BB84 QKD protocol is less when compared to classical key distribution algorithms. The basis for the difference in time is, in the classical key distribution algorithms the preprocessing (choosing numbers, testing for primality of a number, etc.) should be fulfilled in order to generate and distribute the key.

TABLE 2. Comparison of time taken between symmetric key distribution and quantum key distribution algorithms

Key size (in bits/qubits)		**128**	**192**	**256**
Time taken for key distribution (in s)	**AES algorithm**	0.059	0.071	0.096
	BB84 QKD protocol	0.048	0.058	0.079

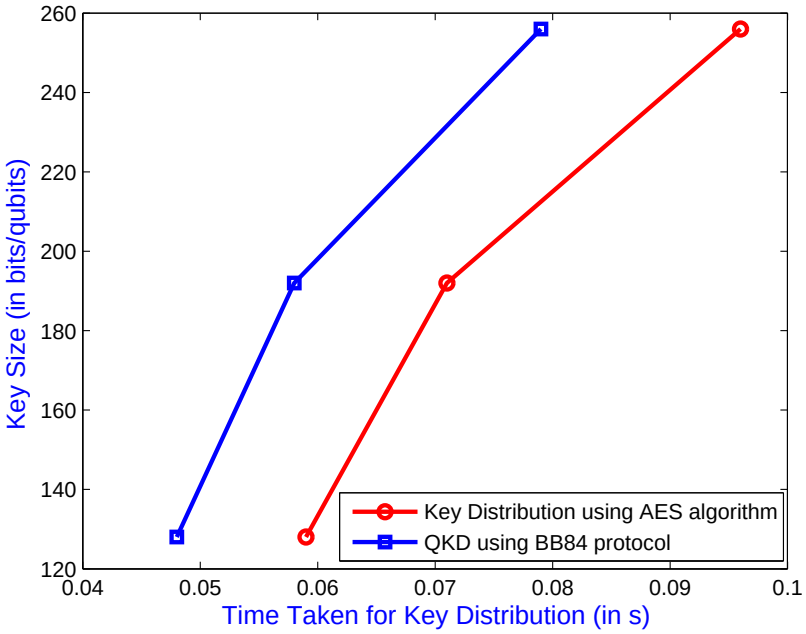

FIGURE 4. Comparison of key distribution between AES algorithm and BB84 protocol

6. **Conclusions and Future Directions.** By means of laws of quantum mechanics, the requirement of quantum cryptography in solving key distribution problem is proven. The laws of quantum mechanics are the reason to raise the fact that quantum cryptography is so effective. The photons are the predominant elements in QKD; hence the transmission is fast and provably secure. The qubits cannot be replicated and when measured in incorrect basis leads to detectable traces of eavesdropping attack. It is clearly exhibited the significance of distributing key using quantum cryptography over classical key distribution methods. Thus, this paper marks the significance of QKD. Further, the quantum gates can be embodied into QKD protocol to make even more tangle for the eavesdroppers to deduce the key. Also a method for authentication is included to the protocol and can be

implemented in security applications. Hence, we determine the security of using a sifted key distributed through QKD protocol will afford potential for the systems.

REFERENCES

[1] S. Wiesner, Conjugate coding, *ACM Sigact News*, vol.15, no.1, pp.78-88, 1983.

[2] D. Wiedemann, Quantum cryptography, *ACM Sigact News*, vol.18, no.2, pp.48-51, 1986.

[3] C. H. Bennet and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proc. of IEEE International Conference on Computers, Systems and Signal Processing*, pp.175-179, 1984.

[4] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press, 2002.

[5] *The D-Wave 2000Q^{TM} System – The Most Advanced Quantum Computer in the World*, https://www.dwavesys.com/d-wave-two-system, 2017.

[6] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature*, vol.299, no.5886, pp.802-803, 1982.

[7] D. McMahon, *Quantum Computing Explained*, John Wiley & Sons, 2007.

[8] V. Padamvathi, B. Vishnu Vardhan and A. V. N. Krishna, Quantum cryptography and quantum key distribution protocols: A survey, *IEEE the 6th International Conference on Advanced Computing (IACC)*, pp.556-562, 2016.

[9] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol.21, no.2, pp.120-126, 1978.

[10] W. Stallings, *Cryptography and Network Security: Principles and Practices*, Pearson Education India, 2006.

[11] *MATLAB and Statistics Toolbox Release 2014a*, The MathWorks, Inc., Natick, MA, United States, 2014.

[12] P. Sibson, C. Erven, M. Godfrey et al., Chip-based quantum key distribution, *Nature Communications*, vol.8, 2017.

[13] B. Fröhlich, M. Lucamarini, J. F. Dynes et al., Long-distance quantum key distribution secure against coherent attacks, *Optica*, vol.4, no.1, pp.163-167, 2017.

[14] B. Korzh, C. C. W. Lim, R. Houlmann et al., Provably secure and practical quantum key distribution over 307 km of optical fibre, *Nature Photonics*, vol.9, no.3, pp.163-168, 2015.

[15] M. Sasaki, M. Fujiwara, R.-B. Jin et al., Quantum photonic network: Concept, basic tools, and future issues, *IEEE Journal of Selected Topics in Quantum Electronics*, vol.21, no.3, pp.49-61, 2015.

[16] R. J. Hughes, J. E. Nordholt, K. P. McCabe et al., *Network-Centric Quantum Communications with Application to Critical Infrastructure Protection*, arXiv preprint arXiv: 1305.0305, 2013.

[17] *Tokyo QKD Network – The Project UQCC (Updating Quantum Cryptography and Communications)*, www.uqcc.org/QKDnetwork/, 2017.

[18] M. Dianati, R. Alléaume, M. Gagnaire, X. Shen and X. Sherman, Architecture and protocols of the future European quantum key distribution network, *Security and Communication Networks*, vol.1, no.1, pp.57-74, 2008.

[19] A. Poppe, M. Peev and O. Maurhart, Outline of the SECOQC quantum-key-distribution network in Vienna, *International Journal of Quantum Information*, vol.6, no.2, pp.209-218, 2008.

[20] C. Elliott, The DARPA quantum network, *Quantum Communications and Cryptography*, Boca Raton, FL, USA, pp.83-102, 2006.

[21] M. O. Rabin, Probabilistic algorithm for testing primality, *Journal of Number Theory*, vol.12, no.1, pp.128-138, 1980.

[22] G. L. Miller, Riemann's hypothesis and tests for primality, *Proc. of the 7th Annual ACM Symposium on Theory of Computing*, pp.234-239, 1975.