Provably Secure Quantum Key Distribution By Applying Quantum Gate

V. Padmavathi[1], B. Vishnu Vardhan[2], and A. V. N. Krishna[3]
(Corresponding author: V. Padmavathi)

Associate Professor, Department of Computer Science & Engineering, Sreenidhi Institute of Science & Technology[1]
Hyderabad, Telangana, India
Professor, Department of Computer Science & Engineering, JNTUH College of Engineering[2]
Karimnagar, Telangana, India
Professor, Department of Computer Science & Engineering, Christ University[3]
Bengaluru, Karnataka, India
(Email: chpadmareddy1@gmail.com)

(Received Nov. 26, 2016; revised and accepted Feb. 21 & Mar. 31, 2017)

Abstract

The need for Quantum Key Distribution (QKD) is strengthening due to its inalienable principles of quantum mechanics. QKD commences when sender transforms bits into qubits or quantum states by applying photon polarization and sends to the receiver. The qubits are altered when measured in incorrect polarization and cannot be reproduced according to quantum mechanics principles. BB84 protocol is the primary QKD protocol announced in 1984. This paper introduces a new regime of secure QKD using Hadamard quantum gate named as PVK16 QKD protocol. Applying quantum gate to QKD makes tangle to the eavesdroppers to measure the qubits. For a given length of key, it is shown that the error rate is negligible. Also, the authentication procedure using digital certificates prior to QKD is being performed which confers assurance that the communicating entities are legitimate users. It is used as a defensive mechanism on man in the middle attack.

Keywords: Authentication; Quantum Cryptography; Hadamard Gate; QKD; Qubits

1 Introduction

In 1969, Stephen Wiesner identified that quantum mechanics has the prospective to play a vital role in the field of cryptography [26]. This has become a breakthrough idea to recommend a new research field known as Quantum cryptography. It is a promising research area where the secure communications happens by means of principles of quantum mechanics and quantum computing. The central unit of information in quantum computing is quantum bit in short known as qubit. The idea of Quantum cryptography was put forward to project a process for QKD by Wiedemann [25]. In 1984, Bennet and Brassard proposed first QKD and popularly known as BB84 protocol [2]. It requires two communication channels specifically a classical channel and a quantum channel. The classical information is communicated by classical channel and qubits by quantum channel [6].

The two key principles of quantum mechanics are: 1) the principle of Heisenberg Uncertainty; 2) the principle of photon polarization. The Heisenberg Uncertainty principle states that the simultaneous measurement of physical properties which are related, cannot be made [2]. The principle of photon polarization states that the qubits cannot be replicated according to the theorem of no-cloning [27]. Hence, the accomplishment of principles of quantum mechanics is one of the reasons why quantum cryptography is so powerful.

In this paper, a new paradigm of quantum key distribution scheme using one-qubit Hadamard quantum gate named as PVK16 QKD protocol with authentication of two communicating entities prior to key distribution is proposed. Authentication implies secure communication. A noteworthy characteristic of any protocol is that the information is authenticate, if authenticate entities participate in the communication. Without authentication, there is always scope of an eavesdropping attack and the entities are fooled by impersonation.

The quantum gate applied on one-qubit can be illustrated by 2 by 2 matrix [19]. Hence, the time complexity of quantum gates is 2^n which is exponential. It is proved that the exponential complexities are secure. By embodying quantum gate into QKD protocol it becomes cumbersome for an eavesdropper to measure the qubits. Besides QKD, this scheme has also adopted the process of authentication to detect man in the middle attack.

Section 2 will brief about the related work in QKD and authentication. The implementation of proposed protocol is elucidated in section 3. Section 4 explicates the analysis of results. Section 5 highlights on security analysis. Section 6 presents conclusions.

2 Related Work

The last two decades has marked the evolution of Quantum cryptography in productive ways. With various theoretical proposals and demonstrations using experiments, the Quantum cryptography was applied in distributing secret key. Since then, QKD has been used as a solution to the problem of key distribution. A quantum channel was developed using an optical fiber in order to implement QKD in a secure fashion for over different distances like 14 kms, 24 kms [3, 7, 18]. In 2015, a highly secured network switches with QKD systems was developed [5].

In recent years, Quantum cryptography is attracting substantial attention among researchers due to major theoretical and practical research projects related to the implementation of QKD. The QKD was successfully demonstrated to resist eavesdropping attacks, photon number splitting attacks, etc. using diverse protocols like Ekert's entanglement, weak coherent pulses, decoy states and optical fiber [8, 13, 21, 22, 29, 30].

The process of authentication was also carried out to ensure that the communicating entities are alleged users from past years. It was accomplished using several concepts of quantum mechanics namely entanglement, one qubit, Bell states and unitary transformations [1, 14, 28]. Also the authentication process was performed by means of classical XOR operation [4]. In 2009, by using quantum superposition states the authentication protocol was proposed [9]. The public key authentication scheme with trusted server based on discrete logarithms for cryptosystems was also implemented [10, 11].

3 Implementation

PVK16 QKD protocol is introduced to fulfill quantum key distribution using Hadamard gate. It is implemented using MatLab R2014a [15]. The authentication procedure is carried out through digital certificate using OpenSSL tool [20] to detect man in the middle attack.

3.1 Authentication

Authentication avoids Sender and Receiver being fooled from illicit user. In order to provide authentication, we use the notion of digital certificate. It embodies the hashed user's public key which is encrypted with the private key of a trusted certification authority (CA) to form digital signature. The CA issues certificate to the communicating entities upon request. They verify each other's certificate by decrypting signature with CA's public key. With this they will get assurance that each other is communicating with legitimate user. We have implemented authentication using OpenSSL tool which provides X.509 authentication service. X.509 is an important yardstick to grant authentication because the pile of certificate and authentication protocols stated are used in wide range of applications. It is being formed on the use of public key cryptography and digital signatures which entail the use of a hash function [12, 23, 24]. Figure 1 depicts the generation of digital certificate.

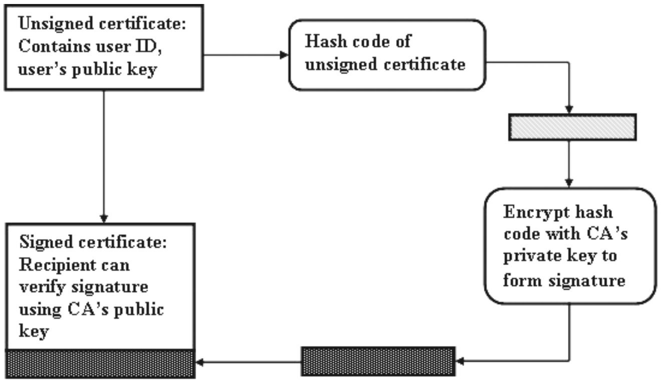
Unsigned certificate: Contains user ID, user's public key
Hash code of unsigned certificate
Encrypt hash code with CA's private key to form signature
Signed certificate: Recipient can verify signature using CA's public key

Figure 1: Digital certificate

The authentication process is carried out as shown in the following steps and described in Figure 2.

Step 1. Sender and Receiver requests digital certificate from Trusted CA before the commencement of communication.

Step 2. CA issues digital certificates to Sender and Receiver.

Step 3. Sender sends certificate to the Receiver for verification.

Step 4. Receiver sends certificate to the Sender for verification.

Step 5. Sender verifies Receiver's certificate whether he/she is alleged user or not by using CA's public key and also Receiver verifies Sender's certificate.

3.2 PVK16 QKD Protocol - Quantum Key Distribution Using Hadamard Gate

Hadamard gate is a one-qubit quantum gate. It takes either qubit $|0\rangle$ or $|1\rangle$ as input and gives $1/\sqrt{2}(|0\rangle + |1\rangle)$ or $1/\sqrt{2}(|0\rangle - |1\rangle)$ as output respectively [2]. The Hadamard gate is denoted as $-\boxed{\text{H}}-$.

The matrix representation of quantum gates is derived using tensor product. The tensor product combines two vector spaces to form a larger one. If U and V are vector spaces of dimensions m and n respectively then $U \otimes V$ is a space on mn. The elements of $U \otimes V$ are linear combinations of tensor products $|u > \otimes |v >$ of elements of $|u >$ of U and $|v >$ of V. Suppose A is a m by m matrix and

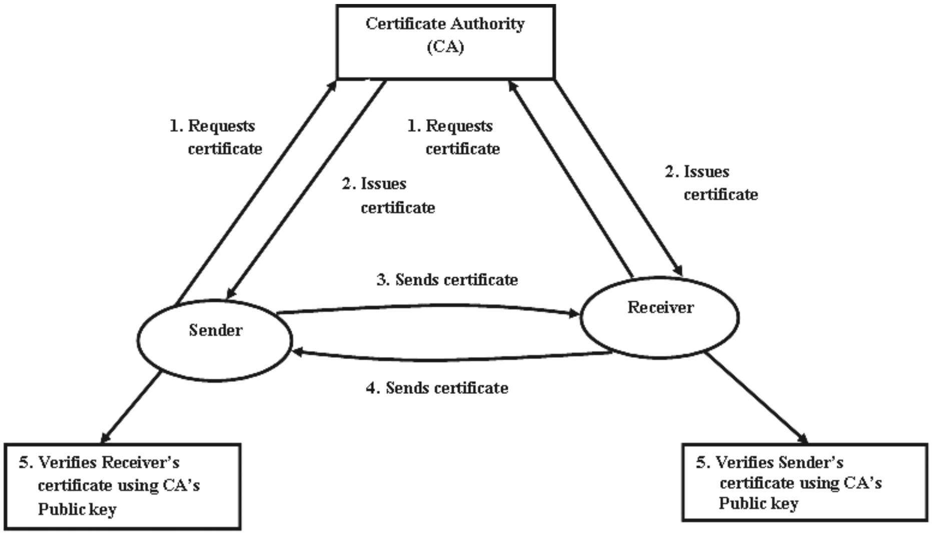

Figure 2: The process of issuing and verifying digital certificate

B is a p by q matrix, then the matrix representation is given as

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}$$

Hence, to represent Hadamard gate which is one-qubit gate, a 2 by 2 matrix is needed as shown below [2, 17].

$$H = 1/\sqrt{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$|0\rangle \rightarrow H = 1/\sqrt{2}(|0\rangle + |1\rangle)$$

$$|1\rangle \rightarrow H = 1/\sqrt{2}(|0\rangle - |1\rangle)$$

The procedure of new protocol of QKD using Hadamard gate namely PVK16 QKD protocol is depicted in Figure 3.

Step 1. Sender's preparation of qubits.
Sender selects random bits 'b' in sequence manner where $b \in (\{0,1\}^n)$, n is the original length of the secret key. Then he/she prepares qubits for those bits individually in one of the four states of BB84 protocol using rectilinear '+' and diagonal 'X' bases shown in Figure 4. The BB84 protocol states are denoted as $|\phi\rangle(0,+)$, $|\phi\rangle(0,X)$, $|\phi\rangle(1,+)$ and $|\phi\rangle(1,X)$ symbolized to photons polarized at 0, 45, 90 and 135 degrees respectively [2, 16] which is depicted in Figure 5. For a given string of random bits $b \in (\{0,1\}^n)$ and string of random bases $\theta \in (\{+,X\}^n)$, $|\phi\rangle(b,\theta)$ is denoted as a state for n photons that encodes the bits $b[x]$ in the bases $\theta[x]$ for every $x \in n$.

To carry out the procedure we acquire the following notation:

- $b(\{0,1\}^n)$: Sender's bit string, n is the original length of the secret key.
- $d(\{0,1\}^m)|m \leq n$: Receiver's bit string.
- $\theta_a(\{+,X\}^n)$: Sender's bases in string.
- $\theta_b(\{+,X\}^m)|m \leq n$: Receiver's bases in string.
- $R\{0,1,\theta_b\}^m|m \leq n$: Receiver's measurement string.
- U: Undetected positions.

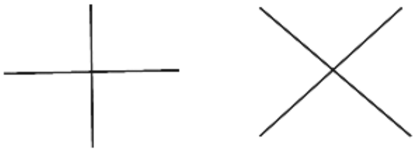

Figure 4: Rectilinear and diagonal bases

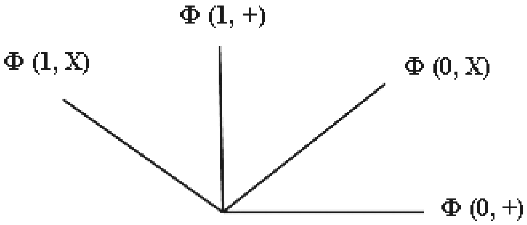

Figure 5: Four states of BB84 protocol

Step 2. Sender applies Hadamard gate.
Sender encodes the qubits $|\phi\rangle(b,\theta_a)$ using Hadamard gate. The outcome is qubits which is denoted as H and sends to Receiver.

Step 3. Receiver's measurement of basis.
Receiver receives H and applies Hadamard gate on

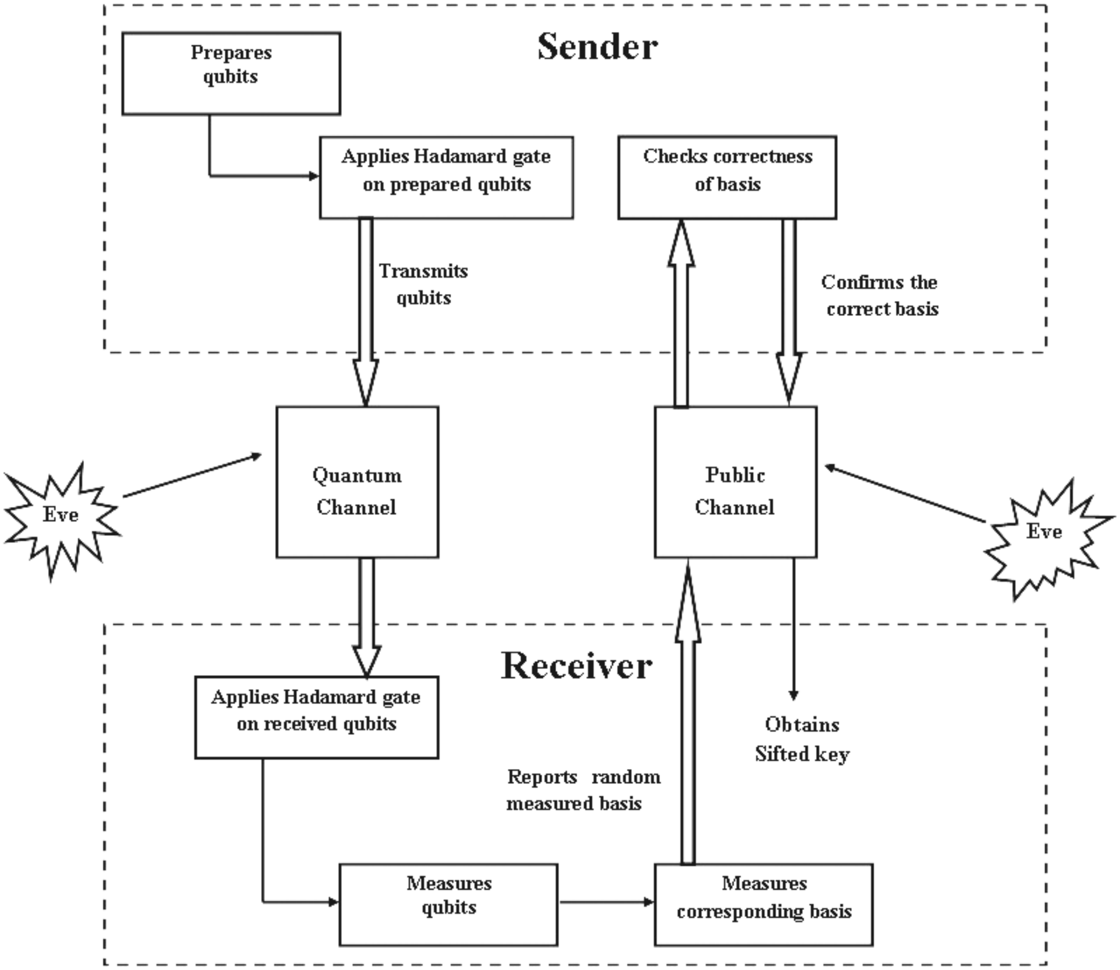
Sender
Prepares qubits
Applies Hadamard gate on prepared qubits
Checks correctness of basis
Transmits qubits
Confirms the correct basis
Eve
Quantum Channel
Public Channel
Eve
Receiver
Applies Hadamard gate on received qubits
Obtains Sifted key
Reports random measured basis
Measures qubits
Measures corresponding basis

Figure 3: PVK16 QKD protocol

H to get qubits. To restore a qubit which is received to its original state, two Hadamard gates in series fashion are applied [17] which is shown in Figure 6. He/she measures each photon $|\phi\rangle(d, \theta_b)$ using either the rectilinear basis $\{|\phi\rangle(0,+),\ |\phi\rangle(1,+)\}$ and diagonal basis $\{|\phi\rangle(0,X),\ |\phi\rangle(1,X)\}$. If Receiver detects a photon i.e. qubit at position x with $|\phi\rangle(d, \theta_b)$ matches with $|\phi\rangle(b, \theta_a)$ i.e. same basis as of Sender's, then the associated outcome is denoted as R, if he/she could able to decode the same Sender's bits for the corresponding basis.

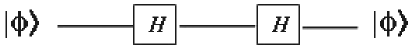

Figure 6: Two Hadamard gates in series restore a quit to its original state

Step 4. Receiver chooses tested basis.
Receiver randomly selects subset of outcome from R and reports to the Sender which is Q i.e. $Q = R \cap U$.

Step 5. Sender says the correctness of basis.
Sender checks $Q[x]$ with $\theta_a[x]$ as well as $b[x]$. If it is correct, gives the confirmation of basis denoted as K otherwise he/she will come to conclusion that eavesdropping/error E has occurred for those basis in position x. $E = U \cup R - k$.

Step 6. Sifted key.
Then both Sender and Receiver shares sifted key $K \in (\{0,1\}^m)|m \leq n$ which is the secret key.

3.3 Error Detection and Calculation

The error is detected when Sender checks $Q[x]$ with $\theta_a[x]$ and $b[x]$. If bits are unmatched, they are discarded. And these bits do not fall under the set of sifted key.

The probability of error is given by $P_e = P_{dx}/P_{bx}$.

- P_e - probability of error.
- P_{dx} - probability of Receiver's measuring bit in x position.
- P_{bx} - probability of Sender's bit position.

Table 1: The comparison of rate of error in key distribution between BB84 and PVK16 QKD protocol

No. of qubits transmitted		**16**	**32**	**64**	**128**
Rate of error (in %)	BB84 QKD Protocol	56	52	46	43
	PVK16 QKD Protocol	37	33	28	26

4 Results

The results are analyzed by carrying out comparison between BB84 QKD protocol and PVK16 QKD protocol which is displayed in Table 1.

The length of qubit is considered as parameter. The error rate is calculated for qubit sizes 16, 32, 64 and 128. From the observation it is noted that the error rate is less in PVK16 QKD protocol. It is less than 40% in all cases. Therefore, with the obtained sifted key, it is sufficient to carry out further communication using proposed protocol. The retransmission of qubits is certainly not necessary. It is plotted in Figure 7.

The basis for less error rate is that PVK16 QKD protocol is being realized with quantum gates. The complexity of quantum gate is 2^n which is exponential. It is determined that the exponential complexities are secure. It becomes tangle for an eavesdropper to know the exact qubit by measuring with random basis and also becomes a challenge to know the sifted key even with high computational resources.

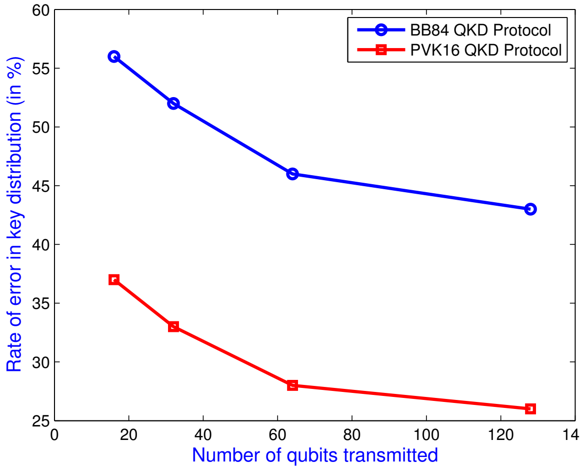

Figure 7: Rate of error in key distribution between BB84 and PVK16 QKD Protocol

5 Security Analysis

The security is analyzed for authentication as well as Quantum key distribution. Authentication is carried out to avoid eavesdropping attack and impersonation. The OpenSSL tool [20] is implemented to ensure that the communicating entities are alleged and both knows that they are communicating with each other, the one whom they have claimed. It was proven that OpenSSL tool [20] is a framework to issue and verify digital certificates. It is used as a defensive mechanism on man in the middle attack and grants trouble free communication.

It is shown that the new regime of protocol that is PVK16 QKD protocol is provably secure in distributing the secret key. The parameter considered is length of qubits. The time complexity of quantum gates is 2^n and which is exponential. Hence, we can convey that PVK16 QKD protocol is more secure. The devised scheme is tailored by reducing few steps from existing. By this the processing period is also reduced as well. It also ensures that it encounters eavesdropping attack. The length of sifted key is more as that of existing scheme which is sufficient to endure further communication. Hence, it avoids retransmission of key.

6 Conclusions

The authentication process through digital certificate is used as a measure for man in the middle attack which is becoming a cumbersome in the path of communication. The fact that the quantum gate has complexity of 2^n assisted in rendering secure communication. It is evidently depicted that PVK16 QKD protocol had essentially encountered man in the middle attack, eavesdropping attack. It is shown that the rate of error is less than 40% and as a result the key size is sufficient to undergo further communication avoiding retransmission of qubits. We thus ascertained the security of using a sifted key distributed by our PVK16 QKD protocol will endow a basis for future systems.

References

[1] H. N. Barnum, "Quantum secure identification using entanglement and catalysis," *arXiv preprint quant-ph/9910072,* 1995.

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

[3] G. Brassard, and C. Crépeau, "25 years of quantum cryptography," *ACM Sigact News,* vol. 27, no. 3, pp. 13–24, 1996.

[4] Y. Chang, C. Xu, and et al., "Quantum secure direct communication and authentication protocol with sin-

gle photons," *Chinese Science Bulletin,* vol. 58, no. 36, pp. 4571–4576, 2013.

[5] M. Fujiwara, T. Domeki, and et al., "Highly secure network switches with quantum key distribution systems," *International Journal Network Security,* vol. 17, no. 1, pp. 34–39, 2015.

[6] L. Gyongyosi and S. Imre, "Quantum informational divergence in quantum channel security analysis," *International Journal of Network Security*, vol. 13, no. 1, pp. 1–12, 2011.

[7] R. J. Hughes, G. Luther, and et al., "Quantum cryptography over underground optical fibers," in *Annual International Cryptology Conference,* pp. 329–342, Springer, 1996.

[8] H. Inamori, L. Rallan, and V. Vedral, "Security of EPR-based quantum cryptography against incoherent symmetric attacks," *Journal of Physics A: Mathematical and General,* vol. 34, no. 35, pp. 6913, 2001.

[9] Y. Kanamori, S. M. Yoo, and et al., "Authentication protocol using quantum superposition states," *International Journal Network Security,* vol. 9, no. 2, pp. 101–108, 2009.

[10] C. C. Lee, M. S . Hwang, and L. H. Li, "A new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation,* vol. 139, no. 2, pp. 343–349, 2003.

[11] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.

[12] C. W. Lin, C. S. Tsai, M. S. Hwang, "A new strong-password authentication scheme using one-way hash functions", *International Journal of Computer and Systems Sciences*, vol. 45, no. 4, pp. 623–626, July 2006.

[13] N. Lütkenhaus, and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New Journal of Physics,* vol. 4, no. 1, pp. 44, 2002.

[14] C. Marcos, and D. J. Santos, "Quantum authentication of classical messages," *Physical Review A,* vol. 64, no. 6, pp. 062309, 2001.

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

[16] D. Mayers, "Unconditional security in quantum cryptography," *Journal of the ACM,* vol. 48, no. 3, pp. 351–406, 2001.

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

[18] A. Muller, H. Zbinden, and N. Gisin, "Underwater quantum coding," *Nature,* vol. 378, no. 6556, pp. 449–449, 1995.

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

[20] OpenSSL, Mar. 31, 2017. (`https://www.openssl.org/source/`)

[21] C. Z. Peng, J. Zhang, and et al., "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Physical Review Letters,* vol. 98, no. 1, pp. 010505, 2007.

[22] D. Rosenberg, J. W. Harrington and P. R. Rice, et al., "Long-distance decoy-state quantum key distribution in optical fiber," *Physical Review Letters,* vol. 98, no. 1, pp. 010503, 2007.

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

[24] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

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

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

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

[28] C. A. Yen, S. J. Horng, and et al., "Quantum direct communication with mutual authentication," *arXiv preprint arXiv:0903.3444,* 2009.

[29] K. I. Yoshino, T. Ochi, and et al., "Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days," *Optics Express,* vol. 21, no. 25, pp. 31395–31401, 2013.

[30] Y. Zhao, B. Qi, and et al., "Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber," *2006 IEEE International Symposium on Information Theory*, pp. 2094–2098, 2006.

Biography

Vurubindi Padmavathi is working as an Associate Professor at Sreenidhi Institute of Science and Technology affiliated to Jawarharlal Nehru Technological University, Hyderabad (JNTUH). She has done her Bachelor of Engineering (CSE), M. Tech. (CSE) and is pursuing Ph.D. in Computer Science and Engineering from JNTUH. Having 14 years of teaching experience, her focus is on the research areas like Cryptography, Information Security and Software Engineering. She has conducted and participated in several workshops, seminars and bridge courses. She has presented and published papers in the International Conferences and in Journals. Mrs. Padmavathi has organized a National conference.

Dr. Bulusu Vishnu Vardhan is working as a Professor in CSE at JNTUH College of Engineering, Nachupally, Karimnagar, Telangana, Inida. He was the Head of the Department of IT, JNTUH College of Engineering, Nachupally from the year 2010 to 2014. He has completed his M. Tech. from Birla Institute of Technology, Mesra, Ranchi in the year 2001 and completed his Ph.D. from JNTUH in the year 2008. Dr. Vishnu Vardhan has 19 years of teaching experience, presently he is guiding 16 research scholars in the area of Cryptography and Information Security, Information Retrieval, Linguistic processing, Data mining and other elite areas. Three scholars are awarded with Ph.D., one from JNTUK and two from JNTUH. He is the member of Board of Studies for Sathavahana University, Karimnagar. He was an active member in Free Software Movement in India. He has completed Government of Andhra Pradesh funded project worth Rs. 5 lakhs from Ministry of IT on localization activity. As a co-investigator completed another UGC funded project worth Rs. 9 lacks. He has evaluated 4 theses for universities like Osmania, Acharya Nagarjuna University. He visited Singapore and presented paper in International Conference ICAEE in 2014. He has more than 35 papers International Journals and Conferences.

Dr. Addepalli V. N Krishna is a Professor in the department of CSE at Christ University, Bengaluru, India. He has completed M. Tech. and Ph.D. in Computer Science and Engineering discipline. He is in the field of teaching and research since 25 years. A. V. N Krishna has participated in various National and International Conferences. He has many publications to his credit. His areas of interests are Cryptography, Mathematical Modeling and Data Mining.