A Secure and Efficient Data Transmission Technique Using Quantum Key Distribution

Md. Armanuzzaman[*1], Kazi Md. Rokibul Alam[*2], Md. Mehadi Hassan[*3], and Yasuhiko Morimoto[+4]
[*]*Department of Computer Science and Engineering,*
[*]*Khulna University of Engineering & Technology, Khulna-9203, Bangladesh*
[+]*Graduate School of Engineering, Hiroshima University, Higashi-Hiroshima 739-8521, Japan*
Email: dakumiju@gmail.com[1], rokib@cse.kuet.ac.bd[2], mehadicse38@gmail.com[3], morimoto@mis.hiroshima-u.ac.jp[4]

Abstract—**this paper proposes a new data transmission technique that uses Quantum Key Distribution (QKD) method, One Time Pad (OTP) encryption technique and Huffman encoding compression algorithm to transmit the data more securely and efficiently. While data is transmitted, requirements like secrecy, less overhead through compression etc are crucial issues. QKD is one of the most promising methods which provide unconditional security. It relies upon the immutable laws of quantum physics rather than computational complexity as the basis of its secrecy. To establish the trust between the sender and the receiver, this paper considers a trusted center that distributes and verifies the key. Also it uses Huffman encoding- a lossless compression algorithm to compress the transmitted data over the classical channel that reduces the data transmission overhead. Moreover for data encryption, it applies OTP technique with the key randomly generated by the QKD method that ensures the secrecy of the transmitted data over the classical channel. Thus the overhead of both quantum and classical channels are reduced. Finally the time requirements for encoding-decoding and encryption-decryption for the proposed technique are evaluated.**

Keywords-Quantum Key Distribution; Huffman encoding algorithm; One Time Pad;

I. Introduction

Unlike traditional cryptosystems, Quantum Key Distribution (QKD) method relies on the immutable laws of quantum physics along with cryptosystems to ensure the secrecy of data. Cryptosystems usually rely on keys where at the right time the availability of the correct key to the sender and the receiver is a crucial issue. Nowadays computational power is increasing, and thereby traditional cryptosystems e.g. RSA, DES, AES etc are becoming vulnerable [1]. In QKD, quantum key is used as qubit, and thereby no measurement can determine the state of the qubit absolutely. If any eavesdropper resides in quantum channel, it is easily detectable because the exact quantum state can't be reproduced without first destroying it [2]. This concept has come from two principles. One is 'Heisenberg uncertainty theorem' [3] which states that it is impossible to measure a quantum state without disturbing the system [5]. Another principle is 'no-cloning theorem' [4] which states that exact quantum state can't be copied without first destroying it [5].

Existing QKD methods e.g. [5] uses three quantum channels and two classical channels. Two quantum channels are used to transmit the secret key and one quantum channel is used to transmit the data between the sender and the receiver. Classical channels are used for the verification of qubits. Thus in this case, quantum channel ensures the secrecy between the sender and the receiver. But it is time consuming and expensive. Some QKD method e.g. [6] uses one quantum channel and one classical channel where the quantum channel is used to transmit the key and the classical channel is used to transmit the data. Here the compression of the key reduces the overhead of the quantum channel. But this produces a byproduct which is equal to the length of the data. Although here the data transmission is secure, it increases the transmission overhead of the classical channel.

To overcome these limitations, this paper proposes a new secure and efficient data transmission technique where at first the trust between the sender and the receiver is established by a trusted center that randomly generates the same secret key for the sender and the receiver on the basis of agreement. Instead of quantum channel, classical channel is used herein for data transmission that reduces the time requirement and the transmission cost. Secondly, Huffman encoding algorithm [15] is used to compress the input data that makes the data transmission faster and efficient. Then the secret key is used to encrypt the output of Huffman encoding algorithm employing OTP encryption technique which ensures the secrecy of the transmitted data. In the receiver side, at first OTP decryption technique is applied to decrypt the ciphertext and then Huffman decoding algorithm is applied to decompress and retrieve the transmitted data.

The rest of this paper is organized as follows: Section II discusses the related works. Section III describes the proposed technique. Section IV illustrates the experimental analysis and finally, Section V concludes the paper.

II. Related Works

The QKD technique proposed in [7] known as BB84 is the first cryptography based protocol. It uses two quantum bases namely rectilinear and orthogonal to solve the redundancy of qubits. Another technique proposed in [8] named as B92 measures the qubits where the receiver accepts the measurement while s/he is confident or rejects while s/he is doubtful. Also as discussed in [5], the sender and the receiver can communicate on the classical channel to verify some of their results herein.

The technique proposed in [9] is the first experiment on quantum cryptographic research that showed that quantum cryptography is capable enough to exchange the secret key.

978-1-5386-3288-8/17/$31.00 ©2017 IEEE

The experiment considers two parties who exchange quantum qubits. It also treats that eavesdropper may reside between the communicating parties.

The technique proposed in [10] is a three-party authentication protocol based on time-bound criterion where the trusted center generates the time bound for the clients and the clients themselves generate their session key. It consists of two phases. In the first phase the parties communicate with the trusted center to deliver their time bound, and then use trusted communications to generate and distribute their keys [5]. In the second phase the key generation is performed.

The technique proposed in [11] aims to support several users and ensures their confidentiality and the authentication in applications. It consists of three phases. In the first phase the trusted centre generates the secret key to encrypt the data. The second phase is the authentication process. And the third phase encrypts the data and distributes it to the clients over the network [5].

The technique proposed in [12] is a model that exchanges two bits secret message through partially entangled states which is used to transfer the data securely between two parties. Also as discussed in [5], the technique is comparable with BB84 because it offers a security check over the communication channel using only one qubit. Moreover, it provides a two steps communication security check.

The technique proposed in [13] introduced protocol for QKD. Here the use of two way quantum channel increases its efficiency of key distribution and the classical channel is no more required. It consists of three phases. The first phase generates raw binary data that will be encoded as qubits. In the second phase the sender and the receiver measure their bits and make a comparison between each other to come up with the sifted key. The third phase is generating the secret key based on the measurement and the sifted key.

The QKD technique proposed in [14] is for digital authentication using a hash function. It utilizes quantum principles to perform one way hash function which is considered as an improvement over BB84. It supports authentication by considering programming polarizer. Dual quantum channel is required here and it has a combination of quantum and classical channels that provides high security.

To establish a secure and efficient data transmission technique, this paper combines the concept of QKD along with Huffman encoding compression algorithm and OTP. The advantages of Huffman algorithm is that it is lossless and more efficient when there is redundancy within the input [15]. Besides, the security of OTP technique is unbreakable when randomly generated key is used herein. The proposed technique first generates the secret key using QKD which requires only two quantum channels and three classical channels. Then to reduce the transmission time one classical channel is used to transmit the data. To reduce the overhead of the classical channel, Huffman encoding algorithm is used to compress the data to be transmitted. To ensure the secrecy of the compressed data, OTP encryption technique is applied on it with randomly generated OTP key.

III. PROPOSED TECHNIQUE

The proposed data transmission technique relies on a trusted center that forms an agreement of diagonal and rectilinear basis to establish the trust between the sender and the receiver and to generate the random secret key for them. Here eavesdropper may exist in the quantum channel. Hence the verification of bits and agreement can easily detect the presence of eavesdropper over there. Also the use of Huffman encoding algorithm makes the data compressed and thereby the transmission becomes faster. Moreover, the exploitation of OTP technique ensures the secrecy of the compressed data. As already mentioned, the proposed technique considers two quantum channels and three classical channels. Here two quantum channels are used for secret key generation whereas two classical channels are used for bit verification. Also the use of third classical channel for the purpose of data transmission reduces the cost and time of transmission. The overview of the technique is presented in Fig. 1.

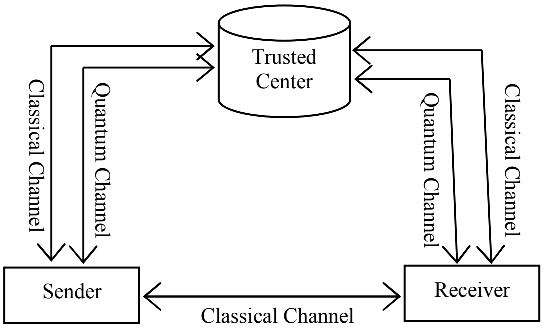

Fig. 1. Overview of data transmission technique.

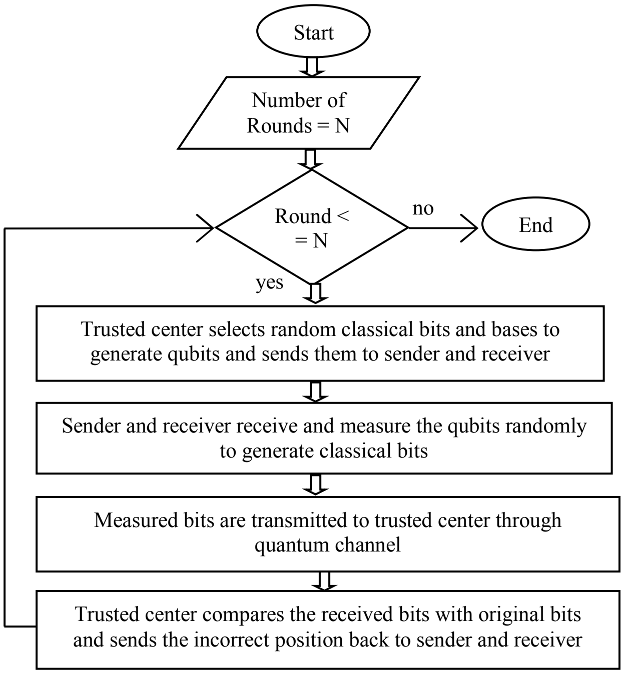
Start
Number of Rounds = N
Round < = N
no
End
yes
Trusted center selects random classical bits and bases to generate qubits and sends them to sender and receiver
Sender and receiver receive and measure the qubits randomly to generate classical bits
Measured bits are transmitted to trusted center through quantum channel
Trusted center compares the received bits with original bits and sends the incorrect position back to sender and receiver

Fig. 2. Flow chart of key generation process.

A. *Secret Key Generation Using QKD*

Fig. 2 presents the key generation process for the proposed technique by the trusted center. Here the sender and the receiver interact *N* times with the trusted center where *N* is a positive integer. At first the trusted center randomly selects bits of qubits as rectilinear and diagonal bases in binary which is represented as 0 and 1 respectively. Now rectilinear bases are 0° and 90° and in binary which are represented as 0 and 1 respectively. Besides diagonal bases are 45° and 135° and in binary which are also represented as 0 and 1 respectively. Depending on the qubit angles, binary classical bits are obtained. For example, the binary value 01 represents rectilinear base where the angle is 90°. Similarly the binary value 10 represents diagonal base where the angle is 45°. The trusted center sends the qubits to the sender and the receiver. They measure the qubits randomly and send back the measured bits to the trusted center. The trusted center then compares them to the original bits and points out the incorrect position if exists and sends them through the classical channels. This process is repeated for finite number of times until satisfactory accuracy is achieved. Thus the random secret OTP key is generated which is used by the sender and the receiver for the purpose of encryption and decryption of the transmitted data respectively.

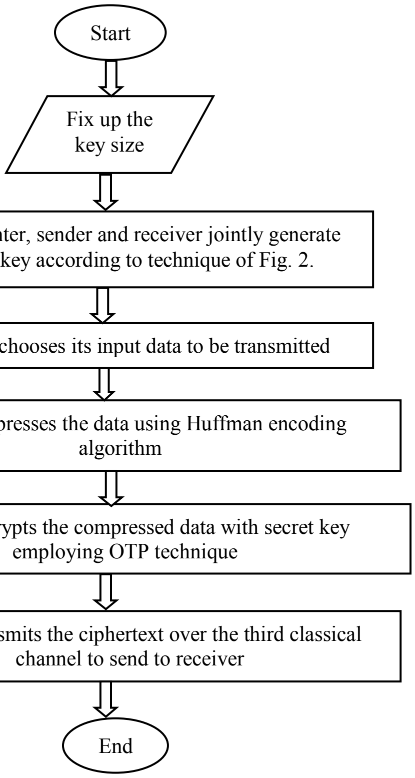
Start
Fix up the key size
The trusted center, sender and receiver jointly generate the random key according to technique of Fig. 2.
Sender chooses its input data to be transmitted
Sender compresses the data using Huffman encoding algorithm
Sender encrypts the compressed data with secret key employing OTP technique
Sender transmits the ciphertext over the third classical channel to send to receiver
End

Fig. 3. Data transmaiison process.

B. *Data Transmission Process*

Fig. 3 depicts the data transmission process of the proposed technique which is as follows.

Step1: At first the trusted center, the sender and the receiver fix up the size of the secret key.

Step 2: Now the trusted center generates the secret key for both the sender and the receiver employing key generation process as discussed in Fig. 2.

Step 3: Then the sender compresses the data using Huffman encoding algorithm [15]. Here it is mention worthy that, the output of compression generates binary values.

Step 4: Prior to transmission, the sender encrypts the compressed data using OTP encryption technique i.e. applies XOR operation. Here using QKD, the random secret key already jointly generated by the trusted center, the sender and the receiver is used as the OTP encryption key where the size of the input data and the key must be equal.

Step 5: Finally the sender sends the ciphertext to the receiver through the third classical channel.

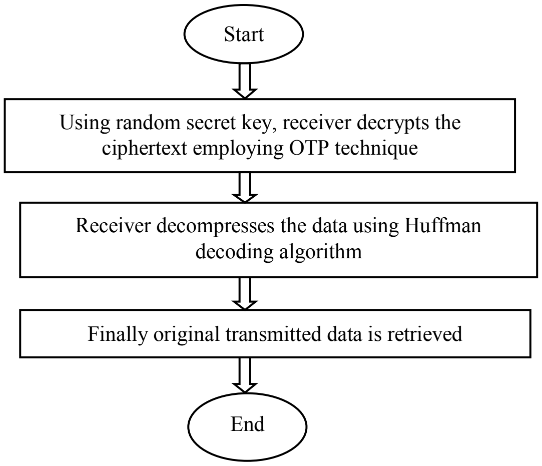
Start
Using random secret key, receiver decrypts the ciphertext employing OTP technique
Receiver decompresses the data using Huffman decoding algorithm
Finally original transmitted data is retrieved
End

Fig. 4. Data receiving process.

C. *Data Receiving Process*

Fig. 4 depicts the data receiving process of the proposed technique which is as follows. Noted that, randomly generated secret key is already possessed by the receiver also.

Step1: At first using the secret key, the receiver decrypts the ciphertext using OTP decryption technique i.e. applies XOR operation which generates the compressed binary data.

Step 2: Now the compressed binary data is decompressed using Huffman decoding algorithm.

Step 3: Thus the receiver retrieves the original transmitted data.

IV. Experimental Analysis

A. *Experimental Setup*

The prototype of the proposed technique is developed under the environment of Intel$^{(R)}$ Core^{TM} i3-2430M 2.50 GHz 64 bit processor with 4 GBytes of RAM running on Windows 8.1 operating system. It is developed in Java employing Eclipse Luna [16] along with jdk1.8.1 as kit where IDE default storage is used for storing data. Also it is assumed that using QKD the trusted center, the sender and the receiver jointly generates the random secret key as: “110010101001001100 1010101110111010110”.

B. *Output of Compression Step*

Step 1: Read the plaintext: “happy hip hop”.

Step 2: Plaintext is converted into compressed text (binary value) using Huffman encoding algorithm as:

“1011100011110110101111100110101111110”.

C. *Output of Encryption Step*

Step 1: Read the compressed text: “101110001111011010 1111100110101111110”

Step 2: Using random secret key, OTP encryption technique (i.e. XOR operation) is performed to convert the compressed text into the ciphertext as:

“00110000011111110001101101110001101111”.

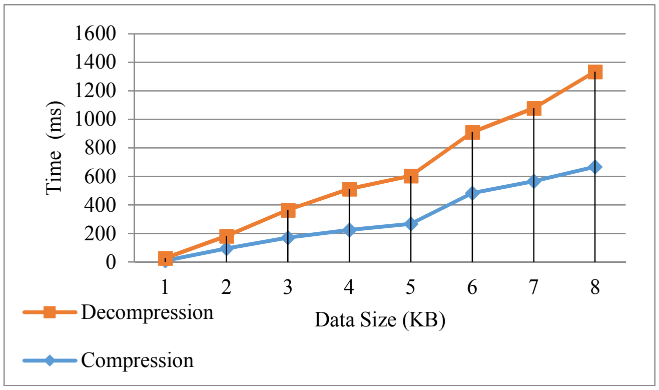

Fig. 5. Time requirement for compression and decompression.

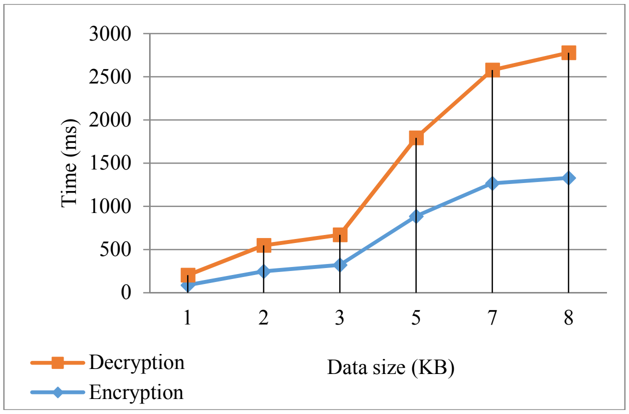

Fig. 6. Time requirement for encryption and decryption.

D. *Output of Decryption Step*

Step 1: To get the compressed text back, consider the ciphertext:

“00110000011111110001101101110001101111”.

Step 2: Using random secret key, OTP decryption technique (i.e. XOR operation) is performed to convert the ciphertext into the compressed plaintext as:

“00110000011111110001101101110001101111”.

E. *Output of Decompression Step*

Step 1: Read the compressed text:

“00110000011111110001101101110001101111”. “

Step 2: Compressed text is converted into original plaintext using Huffman decoding algorithm as:

“happy hip hop”.

F. *Key Size Analysis*

While the key size is fixed up through interactions among the involved parties; the number of rounds influences the accuracy of the key. While the key size increases, the number of rounds also increases to ensure more accuracy. But in the experiment conducted herein, the number of rounds is bounded as shown in Fig. 7.

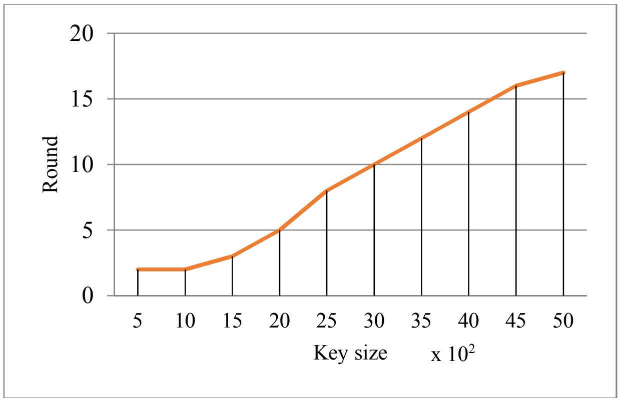

Fig. 7. Relationship between key size and number of rounds.

G. *Compressed Data Analysis*

Huffman algorithm works well when there is huge frequency of the symbols. In contrast when the frequency of the symbols is very few, it does not work well. Also Huffman algorithm needs a mapping table for decompression of data that reduces the overhead. For example while a transmitted data or string “happy hip hop” is considered, there is frequency of symbols. The length of the string is 13. In ASCII encoding, 13*8 = 104 bits is needed. In Huffman encoding the compressed string in binary is “011101010010011” and its length is 15. Additionally, some extra bits are needed to send with the mapping table to the receiver. This is a very efficient compression ratio. Now while a data or string with less frequency e.g. “ABCDEEFFF1234” is considered, the length of the string is also 13. Therefore, the ASCII encoding 13*8 = 104 bits is needed. Herein, Huffman produces the binary compressed data which is 55 bits. This compression is not so efficient.

H. *Ciphertext Analysis*

The OTP technique is a provably secure cryptosystem. The message is represented as a binary string; a sequence of 0’s and 1’s using a coding mechanism such as ASCII coding. The secret key used for both encryption and decryption is a truly random sequence of 0’s and 1’s of the same length as the transmitted data. The encryption is done by adding the secret key to the transmitted data modulo 2, bit by bit. This process is often called exclusive or, and is denoted by XOR. The symbol ⊕ is used.

I. Experimental Results and Discussions

Employing the proposed technique, the time requirement for compression-decompression is presented in Fig. 5. Also the time requirement for encryption-decryption is presented in Fig. 6. Here, plaintexts with different lengths are chosen to depict the result. In both cases, when the size of the data increases, the time requirement also increases and it is easily observable from the figures.

Fig. 5 also shows that for the proposed technique, the time requirement of decompression is larger than that of compression while the size of the plaintext increases. Similarly Fig. 6 also shows that for the proposed technique, the time requirement of decryption is larger than that of encryption.

V. Conclusions

The proposed data transmission technique based on QKD along with Huffman coding compression algorithm and OTP enriches the level secrecy and efficiency of the transmitted data. Here to breach the security of ciphertext, the attacker needs to perform all possible combinations of checking before breaching the secrecy of the data which is expected to be quite difficult. The reason is, the decryption of data of the proposed technique relies on the strength of Huffman algorithm, along with OTP in which the key is generated randomly using QKD. For this reason the proposed technique ensures better secrecy and efficiency than other related techniques, and it is powerful against intruders and eavesdroppers. The main concern of this work is to ensure secrecy and efficiency while data transmission. Over the classical channel, the use of OTP makes the data more secure and the use of Huffman algorithm makes the data transmission faster i.e. efficient.

References

[1] K. S. Kabir, T. Chakraborty, and A.B.M. Alim Al Islam, "SuperCrypt: A Technique for Quantum Cryptography through Simultaneously Improving Both Security Level and Data Rate", Proc. of 2016 Int. Conf. on Networking Systems and Security, pp. 25-33, 2016.

[2] D. Bruss, G. Erdelyi, T. Meyer, T. Riege, and J. Rothe, "Quantum cryptography: A survey," ACM Computing Surveys (CSUR), Vol. 39, No. 2, pp. 1-27, 2007.

[3] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature, Vol. 299, pp. 802-803, 1982.

[4] N. S. Yanofsky and M. A. Mannucci, "Quantum computing for computer scientists," Vol. 20, Cambridge University Press, 2008.

[5] M. Alshowkan, K. Elleithy, A. Odeh, and E. Abdelfattah, "A new algorithm for three-party Quantum key distribution," in 2013 IEEE 3rd Int. Conf. on Innovative Computing Technology (INTECH), pp. 208-212, August, 2013.

[6] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Physical review letters, 67.6, pp. 661-663, 1991.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE Int. Conf. on Computers,Systems and Signal Processing, 1984.

[8] Z. Quan and T. Chaojing, "Simple proof of the unconditional security of the Bennett 1992 quantum key distribution protocol," Physical Review A, Vol. 65, No. 6, p. 062301, 2002.

[9] D. Gottesman and J. Preskill, "Secure quantum key distribution using squeezed states," Physical Review A, vol. 63, p. 022309, 2001.

[10] H.-C. Chen, S.-Z. Lin, and T.-L. Kung, "Three-Party Authenticated Quantum Key Distribution Protocol with Time Constraint," in 2012 Sixth Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 506-511, 2012.

[11] S. Ali, O. Mahmoud, and A. A. Hasan, "Multicast network security using quantum key distribution (QKD)," in 2012 Int. Conf. on Computer and Communication Engineering (ICCCE), pp. 941-947, 2012.

[12] X. Zhang and S. Xie, "Three-party quantum secure direct communication base on partially entangled states," in 2011 Int. Conf. on Mechatronic Science, Electric Engineering and Computer (MEC), pp. 1555-1558, 2011.

[13] F. Zamani and P. K. Verma, "A QKD protocol with a two-way quantum channel," in 2011 IEEE 5th Int. Conf. on Advanced Networks and Telecommunication Systems (ANTS), pp. 1-6, 2011.

[14] R. Sarath, A. S. Nargunam, and R. Sumithra, "Dual channel authentication in cryptography using quantum stratagem," in 2012 Int. Conf. on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1044-1048, 2012.

[15] M. Sharma. "Compression Using Huffman Coding," IJCSNS: Int. Journal of Computer Science and Network Security, Vol.10, No.5, May 2010.

[16] "Eclipse Luna", Software available ahttps://eclipse.org/luna/,on April 2017.