A Quantum-Assisted Framework for Secure Audio Communication: Integrating Quantum Key Distribution with Steganography and Authenticated Classical Cryptography.

Md. Raisul Islam Rifat[1,3], Md. Mizanur Rahman[2,3], Md. Abdul Kader Nayon[1,3], Md Shawmoon Azad[4] and M.R.C. Mahdy[4]

[1] Department of Electrical and Electronic Engineering, Chittagong University of Engineering and Technology, Raozan, Chattogram, 4349, Bangladesh

[2] Department of Computer Science and Engineering, Rajshahi University of Engineering and Technology, Station Rd, 6204, Rajshahi, Bangladesh

[3] Mahdy's Research Academy, Bashundhara R/A, Dhaka, 1229, Bangladesh

[4] Department of Electrical and Computer Engineering, North South University, Bashundhara R/A, Dhaka, 1229, Bangladesh

E-mail: mahdy.chowdhury@northsouth.edu (M.R.C. Mahdy).

Abstract. The emergence of quantum computing poses a significant security threat to the current classical system since it has the potential to outperform the current classical computer in some specific tasks due to its unique principle of operation. This necessitates finding a method resistant to quantum computers to securely transfer information. This research addresses these challenges by proposing a novel method combining quantum key distribution (QKD), specifically the E91 protocol with the classical encryption-authentication protocol, i.e. ChaCha20-Poly1305 and concealing information within another message through steganography to securely transfer audio messages. A shared secret key is created between the communicating parties using E91 QKD, which exploits the stellar protection of quantum entanglement against eavesdropping. The shared key is hashed through the SHA-3 hash function to generate a fixed-length, high-entropy symmetric key. The audio message is hidden inside another audio signal through steganography. The steganographic signal is encrypted using ChaCha20-Poly1305 AEAD in order to provide another layer of obfuscation as well as a means to verify integrity. Through rigorous experiments, we validated the robustness of the proposed methodology in both classical and quantum attacks. The processing of secret audio signals of varying duration (00:01:32 to 00:01:36) exhibits consistent encryption results. The encrypted stego audios show high randomness, with an average entropy of 7.9999968, an average UACI of 49.999956, and an average NSCR of 99.6107%. We demonstrated the safety of the shared key using the CHSH inequality test, wherein the presence of an eavesdropper, the CHSH value is very less than $2\sqrt{2}$. In addition, the integrity of the secret audios is also validated through the verification of the authentication tag generated during the encryption process. Our research offers a novel framework for secure audio transmission, combining classical encryption and authentication methods with QKD to enhance confidentiality, integrity, and resilience against eavesdropping, ensuring robust end-to-end security.

Keywords: Quantum Key Distribution (QKD),E91 Protocol, Entanglement, CHSH inequality, Steganography, ChaCha20-Poly1305 AEAD, Secure Hash Algorithm (SHA), Encryption, Decryption, Authentication.

1. Introduction

The simplest, as well as the most important, form of exchange for human beings is verbal communications. The invention of the Telephone by Alexander Graham Bell in 1876 transformed the verbal communication demography - making the transmission of human voice, which are essentially audio signals, over long distances possible. In the subsequent centuries, technological improvements has broadened the scope of audio transmission. With the rise of the Internet, the amount of information exchanged through audio signals increased rapidly. This increase number audio transmission resulted in the development of different encryption techniques and cryptographic algorithms. The most popular among these algorithms are the symmetric AES and the asymmetric RSA encryption schemes. AES [1] is a block cipher scheme that utilizes multiple matrix operation to encrypt and decrypt data using the same key. Without any knowledge of the cipher key, it is computationally infeasible to reverse the orations performed during encryption. RSA [2], on the other hand, utilizes prime number factorization to generate public-private key-pairs for each user that are used to encrypt and decrypt data. The security of the RSA scheme relies on the insane amount of computational power required to obtain the private key from a public through prime number factoring.

However, with the advent of Quantum Computers with increasing number of functional qubits, these classical cryptography and encryption schemes face an imposing threat [3]. In 1996, Lov K. Grover proposed an algorithm to search an unordered database of size N using $\sqrt{N}$ quantum queries [4]. Using Grover's algorithm, the number of trials required to brute-force a key of length k reduces from 2^k to $2^{k/2}$. This reduction in number of brute-force trials effectively reduces the security level of symmetric encryption schemes such as AES [5]. For example, the AES-128 encryption scheme with a pre-quantum security level of 128 reduces to a post-quantum security level of 64, which is much easier to brute-force. In 1994, P.W. Shor presented a quantum algorithm that can quickly find the prime factorization of any positive integer N [6]. As the security of the RSA algorithm relies on the arduousness of prime number factorization to derive private key from public key, it is currently facing an existential threat due to the exponential speed of Shor's algorithm. It is estimated that the time complexity for Shor's algorithm is $\mathcal{O}(72(log(N))^3)$, as opposed to $\mathcal{O}(N^3)$ for classical computers.

To address these arising challenges, new research is being done on the field of quantum augmented communication systems. These systems exploits the principles of quantum mechanics to attain secure data transmission. One of the most promising area of research in the field of quantum communications is Quantum Key Distribution (QKD). QKD protocols works by establishing a secure cryptographic key between

two users over an insecure channel [7]. QKD employ properties unique to quantum mechanics, such as the no-cloning theorem [8] and the uncertainty principle [9], that ensures the detection of any eavesdropping attempts and thereby guarantees the security of the key. However, QKD itself does not provide security on its own, rather it facilitates the establishment and secure exchange of secret keys that are subsequently used by other cryptographic algorithms and encryption techniques to secure the transmitted information. In resemblance, the research being done on the field of steganography heralds the emergence of an effective information concealing technique to obscure sensitive information within seemingly harmless transmission. Steganography is the technique of hiding secret massage within another massage in such a manner that it is not discernible that a secret message is embedded [10]. However, the security of any steganographic technique is heavily dependent on the strength of cryptographic technique employed to encrypt the data [11].

This paper introduces a novel approach to reinforce the security of digital audio communication by combining the competency of QKD, classical encryption schemes and steganography. Our system utilizes the E91 QKD protocol proposed by Artur K. Ekert in 1991 [12] to generate a shared key with increased security, which is then hashed to produce a fixed-length (256 bits), high-entropy key that is suitable for symmetric encryption by employing the Secure Hashing Algorithm-3 (SHA3-256) [13]. We inspect the use of ChaCha20-Poly1305 authenticated encryption with associated data (AEAD) algorithm [14] - which combines the stream cipher scheme, ChaCha20 [15] with the message authentication code, Poly1305 [16] - to encrypt the steganographic audio. We performed least significant bit (LSB) substitution steganography to hide an audio signal inside another audio signal [17]. The incorporation of QKD with classical symmetric encryption addresses various security concernment, providing protection against both classical and quantum threats.

The new vulnerabilities in secure data transmission due to quantum computer and the need to oppose them have been the motivation for our research. With the advancement in quantum computing technology, it is imperative to devise innovative cryptographic techniques that can keep the data secure in the prospect of an attack from these powerful computers. It is our aim to develop a vigorous solution for secure data communication by combining the strength of quantum communication with hash function, classical encryption and steganography. Hence, the objective our experimental work is to investigate the viability and credibility of integrating encrypted steganographic techniques with quantum protocols, specifically QKD, to strengthen the security and resilience of audio communication. This innovative amalgamation of steganography and quantum communication embodies a significant furtherance in the field, providing an exceptional and optimistic approach to secure data transmission. Our main contribution can be summarized as follows -

- Proposed an original architecture that successfully combines E91 QKD protocol, ChaCha20-Poly1305 AEAD and audio steganography using LSB.

- Utilized E91 as the key distribution protocol which employs principles of quantum mechanics for secure key exchange.
- Assimilated audio steganography using LSB substitution into the architecture to augment the security and robustness of the overall system.
- Assessed the performance and reliability of the proposed scheme by measuring the security through end-to-end encryption.

Our paper is organized is as follows - Section 2 demonstrates the present sate of the field through the review of existing research and their development, laying the foundation for our our proposed scheme. Section 3 describes the foundational concepts of our proposed schemes. Section **??** describes the proposed methodology, presenting a detailed piecemeal explanation of our proposed architecture. Section **??** delves into the detailed description of our implementation. In section **??**, we present the analysis methods as well as the findings. Section **??** explore deeper into an extensive analysis of the results, construing the findings and excerpting key insights. Finally, section **??** concludes the paper by indicating the direction of future work, highlighting the potential application and extension of our research.

2. Related Works

Post-Quantum cryptography (PQC), also known as Quantum resistant Cryptography, is designed to stave off attacks by both classical and quantum computers. In other words, to design a dependable and future-proof data communication system, a blending of Classical Cryptography and Quantum Cryptography is imperative. One such type of blending could be combining some form of symmetric encryption with quantum key distribution (QKD).

Classical cryptography is based on the hardness of mathematical problems and computer complexity to secure communication for decades. The classical cryptographic techniques, such as Advanced Encryption System(AES), Data Encryption Standard (DES), Asymmetric key algorithms – Rivest-Shamir-Adleman(RSA), Elliptic Curve Cryptography (ECC) and Hash Functions, could be the focus of brute force attack as they are not capable enough to handle quantum attacks. Hence, to solve this problem, the algorithms of Post Quantum Cryptography was proposed which is strong, reliable and secure against quantum attacks.[18]

E91 and BB84 are the methods of Quantum Key Distribution (QKD) based on the completeness of quantum mechanics. BB84 is the first QKD protocol that relies on the Heisenberg uncertainty principle and the no-cloning theorem. On the other hand, E91 is an entanglement based protocol basically generalized from of Bell's theorem. The users (Alice and Bob) can easily detect the eavesdropping attempt checking the Bell's inequality by using this protocol. [19] Among them, E91 is considered safer and more reliable though it faces some technical difficulties.[20]

Hash functions are frequently used in modern cryptography in order to ensure authentication of the digital communication system. It takes an arbitrary length input

and produces a fixed sized hashed value where any small changes in input resulting the complete hashed value. SHA-0, SHA-1, SHA-2, SHA-3 are the dedicated hash functions of the SHA family.[21] Among them, the SHA-3 family is based on permutation having an extendable output function. SHA3-224, SHA3-256, SHA3-384, SHA3-512 are known as cryptographic hash functions. SHA-3 provides resistance to collision, preimage and second preimage attacks which ensures the security attacks such as digital signature generation and verification, key derivation and pseudorandom bit generation. [13]

Steganography is a common practice of hiding information. The main purpose of steganography is to secure the information completely undetectable[22] There are many types of steganography using different types of cover objects such as text [23], audio [24][25][26], video, images (2D and 3D) [27] and information matrices [28].Because of having high quality of redundancy and data transmission rate in signals and audio files, make it suitable for steganographic process.[29] The audio stenographic process are LSB codding, Parity codding, Phase codding, Spread spectrum, Echo hiding. Among them, LSB is the best audio steganography technique as it increases robustness against noise addition and MPEG compression, high capacity and simplicity.[30][24] When the QKD protocols are combined with this, it improves more data security. Using Bernstein-Vazirani algorithm and the BB84 protocol, it generates a secret key to ensure only authorized access to quantum messages. This quantum steganography method increases hidden channel capacity, resists attacks such as intercept-resend, and reduces message detectability by using more Bell states and random information distribution.[31]

ChaCha, a variant of Salsa20, represents the ChaCha family of stream ciphers, which enhances the Salsa20 design. It increases resistance to cryptoanalysis by improving the diffusion per round while maintaining performance. It also achieves better software speed compared to Salsa20 in certain platforms due to its efficient design that allow for SIMD operations.[15] ChaCha is a robust alternative to salsa20, with enhancements that could make it preferable for various cryptographic applications.

The Poly1305 is a specific type of MAC(Message Authentication Protocol) which is a cryptographic tools used to verify the integrity and authenticity of a message.[16] It computes a 16-byte authenticator for variable-length messages using a 32-byte secret key, which includes a 16-byte AES key and a 16-byte addition key which helps in high-speed computations and making it suitable for various applications.[16] The probability of successful attack is also very low due to the uniqueness of nonces and the unpredictability of keys. For all the reasons, it is used widely for network protocols and secure communications.

3. Preliminaries

In this section, we present the primary concepts employed in our methodology. We start with the quantum key distribution (QKD) protocol proposed by Artur Ekert in 1991, commonly known as the E91 key distribution protocol. Protected by Bell's inequality, E91 protocol provides a secure method of sharing generated key pairs. Then we proceed

to the SHA3 family of hashing algorithms, specifically the SHA3-256 function, which can produce a unique 256-bit long hexstream for an input of any length. Next, we introduce the ChaCha20-Poly1305 AEAD, which combines the strong yet simple ChaCha20 stream cipher with Poly1305 MAC. Finally, we discuss the LSB steganography algorithm, which is essentially a technique of hiding an audio signal in the least significant bits of another, larger audio.

References

[1] Rijmen V and Daemen J 2001 *Proceedings of federal information processing standards publications, national institute of standards and technology* **19** 22

[2] Rivest R L, Shamir A and Adleman L 1978 *Communications of the ACM* **21** 120–126

[3] Bernstein D J and Lange T 2017 *Nature* **549** 188–194

[4] Grover L K 1996 A fast quantum mechanical algorithm for database search *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* pp 212–219

[5] Daemen J and Rijmen V 2002 *The Design of Rijndael* (Springer Berlin Heidelberg) ISBN 9783662047224 URL `http://dx.doi.org/10.1007/978-3-662-04722-4`

[6] Shor P W 1997 *SIAM Journal on Computing* **26** 1484–1509 ISSN 1095-7111 URL `http://dx.doi.org/10.1137/s0097539795293172`

[7] Alléaume R, Branciard C, Bouda J, Debuisschert T, Dianati M, Gisin N, Godfrey M, Grangier P, Länger T, Lütkenhaus N *et al.* 2014 *Theoretical Computer Science* **560** 62–81

[8] Bužek V and Hillery M 1996 *Physical Review A* **54** 1844

[9] Sen D 2014 *Current Science* 203–218

[10] Kahn D 1996 *The history of steganography* (Springer Berlin Heidelberg) p 1–5 ISBN 9783540495895 URL `http://dx.doi.org/10.1007/3-540-61996-8_27`

[11] Anderson R J and Petitcolas F A 1998 *IEEE Journal on selected areas in communications* **16** 474–481

[12] Ekert A K 1991 *Physical Review Letters* **67** 661–663 ISSN 0031-9007 URL `http://dx.doi.org/10.1103/PhysRevLett.67.661`

[13] Dworkin M J 2015

[14] Nir Y and Langley A 2015 ChaCha20 and Poly1305 for IETF Protocols RFC 7539 URL `https://www.rfc-editor.org/info/rfc7539`

[15] Bernstein D J *et al.* 2008 Chacha, a variant of salsa20 *Workshop record of SASC* vol 8 (Citeseer) pp 3–5

[16] Bernstein D J 2005 The poly1305-aes message-authentication code *International workshop on fast software encryption* (Springer) pp 32–49

[17] Cvejic N and Seppanen T 2002 Increasing the capacity of lsb-based audio steganography *2002 IEEE Workshop on Multimedia Signal Processing.* (IEEE) pp 336–338

[18] Sharma S, Ramkumar K, Kaur A, Hasija T, Mittal S and Singh B 2023 *Modern Electronics Devices and Communication Systems: Select Proceedings of MEDCOM 2021* 23–38

[19] Ekert A K 1991 *Physical review letters* **67** 661

[20] Alvarez L C and Caiconte P C 2016 *International Journal of Modern Communication Technologies and Research* **4** 265683

[21] Madhuravani B and Murthy D 2013 *Int J Innov Technol Explor Eng* **2** 326–9

[22] Amin M M, Salleh M, Ibrahim S, Katmin M R and Shamsuddin M 2003 Information hiding using steganography *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings.* (IEEE) pp 21–25

[23] Yang Z L, Guo X Q, Chen Z M, Huang Y F and Zhang Y J 2018 *IEEE Transactions on Information Forensics and Security* **14** 1280–1295

[24] Jayaram P, Ranganatha H and Anupama H 2011 *The International Journal of Multimedia & Its Applications (IJMA) Vol* **3** 86–96

[25] Hemeida F, Alexan W and Mamdouh S 2021 *International Journal of Computing and Digital Systems* **10** 555–562

[26] Djebbar F, Ayad B, Meraim K A and Hamam H 2012 *EURASIP Journal on Audio, Speech, and Music Processing* **2012** 1–16

[27] Farrag S and Alexan W 2020 *Multimedia Tools and Applications* **79** 29289–29303

[28] Mashaly M, El Saied A, Alexan W and Khalifa A S 2019 A multiple layer security scheme utilizing information matrices *2019 Signal Processing: Algorithms, Architectures, Arrangements, and*

Applications (SPA) (IEEE) pp 284–289
[29] Singh K U 2014 *International Journal of Computer Applications* **95**
[30] Cvejic N and Seppanen T 2004 Increasing robustness of lsb audio steganography using a novel embedding method *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.* vol 2 (IEEE) pp 533–537
[31] Yalla S P, Hemanth S, Kumar S T, Moulali S and Dileep S 2022 *NeuroQuantology* **20** 923