

Effectiveness of enhanced tight finite scheme in quantum key distribution protocol for network communication

ABSTRACT

Classical cryptography is mainly about the challenge to compute the secret key using current computing system. We tend to hide our information from being stealing by others. In order to do so, in this research paper we are proposing a method that use the law of physics in communication in terms of cryptography and key distribution by applying quantum theorems and principle. Using BB84 protocol as a base in quantum key distribution together with the implementation of tight finite key that compress the Shannon entropy and Von Neumann theory. Our multiparty system would be a new area of authentication. Throughout this paper, we are going to prove that our method will give a small error rate between the initial key rates with the final key rate then will impact the attack resilient. Yet the key cannot be formed and transferred simply.

Keyword: Quantum key distribution; Secure authentication; Multi party; Tight finite key