Abstract

In this thesis, a Recurrent Neural Network based Tree Parity Machine is proposed with the aim of high security. The communicating partners use the technique of mutual synchronization for secret key generation. The generated neural key is used for encryption and decryption by using Autoencoder. To check the strenght of our proposed model, we have applied Man in the Middle Attack which shows that it is impossible for an attacker to synchronize with the communicating partners. We also implemented the simulation of 1000 attackers which proves that the generated key is completly secure. The model also provide sufficient accuracy for encryption and decryption process. It is also evaluated in terms of encryption and decryption time and also compared with other algorithms and model. It shows that this model take less time than other previously explained models.