**Abstract**
Generating keys and keeping them secret is critical in secure communications. Due to the “open-air” nature, key distribution is more susceptible to attacks in wireless communications. An ingenious solution is to generate common secret keys by two communicating parties separately without the need of key exchange or distribution, and regenerate them on needs.

Recently, it is promising to extract keys by measuring the random variation in wireless channels by two most popular channel parameters, i.e., channel state
information and received signal strength. Through results collected from over a hundred tests, this project offers insights to the design of a secure and efficient key generation system and authentication between two communicating parties. The multipath effect in wireless channel and the movement of users/objects is essential and beneficial to key generation as it increases the channel randomness. In this project, we propose
an efficient Secret Key Extraction protocol from the channel state information(CSI), Authentication between two communicating parties and additional encryption using constellation rotation by generated key .
The principles, performance metrics,authentication protocol, encryption using constellation rotation procedure and key generation procedure are comprehensively surveyed.The project concludes with some suggestions for future studies.