ABSTRACT Key generation from the randomness of wireless channels is a promising alternative to public key cryptography for the establishment of cryptographic keys between any two users. ~~This project reviews the current techniques for wireless key generation~~. The principles, performance metrics and key generation procedure are comprehensively surveyed. ~~Methods for optimizing the performance of key generation are also discussed. Key generation applications in various environments are then introduced along with the challenges of applying the approach in each scenario~~. The project concludes with some suggestions for future studies.

studying two most popular channel parameters, i.e., channel state information and received signal strength. Through results collected from over a hundred tests, this paper offers insights to the design of a secure and efficient key generation system. We show that multipath is essential and beneficial to key generation as it increases the channel randomness. We also find that the movement of users/objects can help introduce temporal variation/randomness and help users reach an agreement on the keys. ~~This paper complements existing research by experiments constructed by a new hardware platform~~

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, e.g., RSS. In this paper, we propose an efficient Secret Key Extraction protocol. It establishes common cryptographic keys for two communicating parties in wireless networks via the real-time measurement of Channel State Information (CSI). It outperforms RSS-based approaches for key generation in terms of multiple subcarriers measurement, perfect symmetry in channel, rapid decorrelation with distance, and high sensitivity towards environments. ~~In this design, we also propose effective mechanisms such as the adaptive key stream generation, leakage-resilient consistence validation, and weighted key recombination, to fully exploit the excellent properties of CSI.~~