Key generation exploiting unpredictable characteristics of wireless channels is information-theoretically secure [1], [2] and has been an active research direction in physical layer security (PLS) [3], [4]. In this technique, two legitimate users, Alice and Bob, measure their common but noisy channel in an alternate manner, through which they can get correlated but not identical observations. Then they will quantize their correlated analog measurements into binary values separately, and their keys are usually not the same. Alice and Bob later reach an agreement on the same key through information reconciliation [5]. Finally, they employ privacy amplification to remove the information revealed during the information reconciliation [6]. Therefore, key generation is able to establish a cryptographic key securely from the noisy observation

Key generation requires the channel to satisfy certain conditions with respect to temporal variation, channel reciprocity, and spatial decorrelation. Temporal variation is the umain random source for key generation, which can be introduced by the movement of any users and/or objects in the wireless environment. It is feasible to exploit channel randomness in the frequency domain [7], [8], [18], [22], [26] and spatial domain [27], [28], but the randomness is limited and cannot be updated in a static environment. Experiments have been carried out in the indoor and outdoor environments and have shown that the mobility of users and/or objects is sufficient to introduce randomness [15], [20], [21].

Channel reciprocity indicates that the signals at each end of the same link have identical statistical features, such as channel gains, phase shift, time delay, etc, which is the basis of key generation systems. Although there is ongoing research effort adopting full-duplex hardware [29]–[31], most of the current commercial wireless devices work in half-duplex mode. Key generation usually works in time-division duplexing (TDD) systems and slow fading channels. Therefore, the received signals are generally asymmetric due to the non-simultaneous measurements and independent noise in different hardware devices, whose effects have been studied theoretically in [26] and experimentally in [32]. Non-simultaneous measurements can be compensated by interpolation to emulate the channel being measured at the same time [19], [21] while noise effect can be suppressed by low pass filtering [26], [33].

The conclusion from applying spatial decorrelation means that any eavesdropper located more than half-wavelength away from legitimate users experiences uncorrelated fading. This property is highly influenced by the channel condition [34]. In a rich multipath environment with uniform scattering, according to the Jakes model, when the number of scatters grows to infinity, the correlation function is the Bessel function of zeroth order and the signal decorrelates when $d = 0.4\lambda$ (approximately half-wavelength) [35], which is the theoretic basis of spatial decorrelation. Some experiments have been carried out to verify this property in UWB systems [10]–[12] and IEEE 802.11g systems [36].

In contrast, spatial decorrelation has also been found to not hold in some channel conditions by simulation [37], [38] and experiments [38]–[40]. In this case, key generation cannot be deemed secure and requires special design consideration to combat eavesdropping when eavesdroppers are close to the legitimate users.

In order to design an effective, workable, and secure key generation system, the above three principles, i.e., temporal variation, channel reciprocity, and spatial decorrelation, should be always satisfied.key generation performance greatly depends on the channel conditions, such as the multipath level and dynamicity, which has not been studied comprehensively yet. In addition, the channel parameter used for key generation also has an impact. For example, it has been reported that RSS-based key generation systems are subject to predictable channel attacks [13], [15] while CSI-based systems are robust to such attacks [7], [13].

In this paper, we study key generation principles comprehensively through experiments with different channel conditions. We implement a testbed using a **customized FPGA-based wireless platform known as wireless open-access research platform (WARP) [41], which supports IEEE 802.11 orthogonal frequency-division multiplexing (OFDM) physical (PHY) layer and distributed coordination function (DCF) MAC layer protocols. This platform** allows us to have full access to the transmission parameters, which are not available in the commercial network interface cards (NICs). A key objective here is to make minimal or even no change to the off-the-shelf wireless protocol, which requires cross-layer design and presents new research challenges. Our contributions are as follows.

- We carry out much more comprehensive experiments than previous research in environments with various multipath and dynamic levels. In particular, we conduct over a hundred tests in an anechoic chamber, a reverberation chamber, and an indoor office environment, which represents little, rich, and moderate multipath, respectively. We consider different dynamic channels, i.e., static, object moving, and mobile scenarios, in these environments. Both CSI and RSS are collected from the testbed and studied with the aim of assessing suitability for key generation when a certain channel conditions satisfy.

- Through the comprehensive experimental results, we are able to offer insights and advices for the design of suitable key generation schemes in different environments and scenarios. We found that in a dynamic environment, (i) the randomness introduced by temporal variation is sufficient for key generation; and (ii) cross-correlation of the channel measurements is high enough to make Alice and Bob reach an agreement, while in a static scenario these properties do not hold and key generation fails. We also conclude that multipath can improve the security performance of key generation. In a multipath environment, spatial decorrelation property holds and eavesdroppers can only get very limited information, while in an environment with little multipath such as an anechoic chamber, eavesdroppers can obtain a highly correlated channel and key generation cannot be deemed secure.

Wireless networks are susceptible to various attacks due to the “open air” nature of the wireless communication [22]. Cryptographic key establishment is a fundamental requirement for secure communication to support confidentiality and authentication services. However, it is difficult to ensure availability of a certificate authority or a key management center in dynamic wireless environments [4]. It is necessary to have alternatives for key agreement between wireless entities in a common channel [12] [14] [2].

One recent trend in this regard is to use physical-layer identification [16]. For example, received signal strength (RSS) becomes a popular statistic of the radio channel and is used as the source of secret information shared between two parties [11]. The variation over time of the RSS, caused by motion multipath fading, can be quantized and used for generating secret keys. Due to presence of noise and manufacturing variations, the generated secret keys might be different, which are corrected by information reconciliation. Finally, privacy amplification is introduced to convert this bit-string into a uniformly distributed string to make it secure enough. However, RSS cannot work well in stationary scenarios due to infrequent and small scale variations in the channel measurements. To address this issue, we propose a secret key extraction based on the inherent randomness of wireless channels. In current widely used IEEE 802.11n networks, data is modulated on multiple Orthogonal Frequency Division Multiplexing (OFDM) subcarriers simultaneously. Each network interface card (NIC) of the device can get a value of Channel State Information (CSI) which describes the current condition of the channel in each subcarrier [1].

Different from RSS, CSI is a fine-grained value derived from the physical layer. It consists of the attenuation and phase shift experienced by each spatial stream on every subcarrier in the frequency domain. In contrast to having only one RSS value per packet, NIC can obtain multiple CSI values at one time. CSI provides other attractive properties. First, it is very sensitive to location such that two closely-placed receivers have very different readings by the same sender. Second, its readings of a pair of sender and receiver have a strong correlation. Third, it presents an excellent quality of randomness. Due to these characteristics, CSI is an ideal resource for secret key extraction.