Constructing Reciprocal Channel Coefficients for Secret Key Generation in FDD Systems

Guyue Li, Aiqun Hu, Chen Sun, and Junqing Zhang

***Abstract*—Physical layer-based key generation encounters the reciprocity bottleneck when applied in frequency-division duplexing (FDD) systems. This letter constructs reciprocal channel characteristics of the uplink and downlink transmissions for key generation in FDD systems. The frequency dependency of propagation characteristics in both large-scale fading and small-scale fading is investigated. A general channel model is then established by considering frequency impact. A reciprocal channel construction framework is finally created. Numerical results demonstrate that our algorithm can construct bidirectional channel coefficients with high correlation, and thus enable key generation technology to be used in FDD systems.**

***Index Terms*—Physical layer security, secret key generation, reciprocal channel coefficient, frequency-division duplexing.**

I. Introduction

Inspired by the random nature and reciprocal electromagnetic propagation of wireless communication, two legitimate users, namely Alice and Bob, can independently establish the common key based on their channel observations [1]. The security of the generated key is based on the spatial diversity of wireless channel that a third party will observe an independent wireless channel when she is not within the vicinity of Alice and Bob, e.g., beyond 6.25 cm in 2.4 GHz [1]. Since key generation simplifies the secret key sharing process, it has great practical appeal, especially in resource-constrained large-scale wireless networks. This technique thus provides an alternative solution for key sharing and distribution, which can overcome some weaknesses of traditional key exchanges, e.g., requiring a secured infrastructure.

Time-division duplexing (TDD) and frequency-division duplexing (FDD) are the two duplexing methods used in wireless communications. Key generation requires a highly correlated channel measurements between Alice and Bob to agree on the same key. The uplink and downlink transmissions operate at the same carrier frequency in TDD systems, and their channel responses are reciprocal, which satisfies the key generation requirement. Therefore, many key generation applications and prototypes have been reported in TDD systems [1], e.g., by employing WiFi, ZigBee, and Bluetooth.

FDD is dominant in the cellular connections, e.g., LTE, NB-IoT, but has received little investigation for key generation. The uplink and downlink transmissions run at two different carrier frequencies and the channel reciprocity does not hold any more. Most of the reciprocal channel parameters used in TDD systems, such as received signal strength, channel gains, envelope and phase, can be quite different in FDD systems. The multipath angle and delay are the only two channel parameters supposed to hold the reciprocity in FDD systems [2]. Unfortunately, angle and delay can hardly be estimated accurately without massive multiple antennas or wide bandwidth. It is thus difficult to explore frequency-invariant channel parameters in FDD systems [3]. Apart from directly extracting reciprocal channel parameters, combinatorial channels with reciprocal channel gains can be established with the aid of an additional reverse channel training phase, termed as loopback-based protocols [4–6]. However, these protocols complicate the channel sounding process and their security performance cannot be guaranteed because a passive eavesdropper can capture the entire transmissions [7].

To the best knowledge of the authors, this letter is the first work that constructs reciprocal channel characteristics for key generation in FDD systems without additional reverse channel training phase. The main contributions are as follows.

- The frequency dependency of propagation characteristics in both large-scale fading and small-scale fading is investigated. This analysis contributes a better understanding of bidirectional reciprocity in FDD systems.
- A general channel model for FDD systems is established by taking into account the frequency impact.
- We propose a novel reciprocal channel coefficients construction framework which is able to achieve highly correlated bidirectional channel coefficients.

It greatly expands the application scope of key generation to FDD systems.

II. Channel Model for FDD Key Generation

Alice and Bob send pilots to each other at different dedicated frequency bands with centering frequency f_1 and f_2, respectively. The up-down link frequency separation, $\Delta f = |f_1 - f_2|$, satisfies that $\Delta f \ll f_1$. For example, $\Delta f / f_1$ is generally smaller than 10% in FDD-LTE systems [8]. Literature and field measurements have shown that when $\Delta f \ll f_1$, the uplink and downlink transmissions travel the same propagation paths and suffer the same clusters [3, 9]. This inspires us to explore reciprocal characteristics for Alice and Bob to generate common keys. This section will investigate the bidirectional reciprocity of propagation characteristics in both large-scale and small-scale fading for FDD systems.

Manuscript received xx, 2018; revised xx, 2018; accepted xx, 2018. Date of publication xx, 2018; date of current version xx 2018. This work was supported in part by National Natural Science Youth Foundation of China under Grant 61801115. The associate editor coordinating the review of this letter and approving it for publication was xxx. (*Corresponding author: Guyue Li*)

G. Li and A. Hu are with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. (e-mail: {guyuelee, aqhu}@seu.edu.cn.)

C. Sun is the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China. (e-mail: sunchen@seu.edu.cn.)

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (email: junqing.zhang@liverpool.ac.uk)

Digital Object Identifier

A. Large-Scale Fading Parameters

1) Path Loss: Alpha-beta-gamma (ABG) free space reference distance model is a common multi-frequency path loss model for 5G cellular communications [10, 11], given as

$$\mathrm{PL}^{\mathrm{ABG}}(f,d) = 10\alpha\log(d) + \beta + 10\gamma\log(f), \tag{1}$$

where f is the carrier frequency in GHz and d is the distance in meters between transmitter and receiver, α and γ are coefficients showing the dependence of path loss on distance and frequency, respectively, β is the optimized offset. The pass loss is dependent on the carrier frequency.

2) Shadow Fading: Shadowing is the effect that the received signal power fluctuates due to objects obstructing the propagation path between the transmitter and receiver. The relationship between the shadow fading magnitude and the i^{th} object of depth η_i is modeled as [10]

$$\sigma_{\mathrm{SF}}(\eta_i) = \exp(-A_i\eta_i), \tag{2}$$

where A_i reflects the i^{th} changing rate of shadow fading over η_i. When A_i is the same for all blocking objects, the shadow fading can be expressed as

$$\sigma_{\mathrm{SF}}\Big(\sum\nolimits_i \eta_i\Big) = \exp\Big(-A\sum\nolimits_i \eta_i\Big). \tag{3}$$

According to the central limit theorem, when there are a large number of objects, $\sum_i \eta_i$ is Gaussian distributed. The shadow fading σ_{SF} can thus be modeled as a log-normal distributed random variable [10, 12].

In FDD systems, because $\Delta f \ll f_1$, the changing rate A_i is approximately the same. Moreover, as the uplink and downlink transmissions travel the same path, the depth of all block objects, η_i, is identical. Thus, the shadow fading of uplink and downlink transmission can be deemed reciprocal [12, 13].

B. Small-Scale Fading and Multipath Parameters

Small-scale variations of the channel result from constructive and destructive additions of multipath radio wave components. Since uplink and downlink transmissions travel the same propagation path, the numbers of paths, N, are identical.

1) Delay: The propagation time of the n^{th} path is $T_n = \frac{d_n}{c}$, where d_n is the distance of the n^{th} path and c is the speed of light. Then, the delay of the n^{th} path is given by $\tau_n = T_n - T_1$. As delay only depends on the path distance, it is reciprocal in the uplink and downlink transmissions [9].

2) Per-path Power: The power delay profile (PDP) describes the received signal power as a function of propagation delays, which can be modeled as

$$P(\tau_n) = a\exp(-b\tau_n), \tag{4}$$

where a and b are frequency dependent coefficients. According to [14], $a = 0.4715, b = 0.0123$ and $a = 0.2605, b = 0.0108$ for the 700 MHz and 4.9 GHz band, respectively. Although a varies greatly versus frequency, it is a constant factor which can be eliminated through power normalization. It is observed that b varies only by about 10% for a large frequency separation of 4.2 GHz. Hence, it is reasonable to treat b reciprocal in FDD systems with a small frequency separation.

Moreover, some measurement results have shown that the average delay profiles are still similar among three largely separated frequency bands of 3 GHz, 8 GHz and 15 GHz for urban mobile communications [15]. Therefore, the PDP is considered to be reciprocal.

3) Phase: The phase is caused by both wave propagation and user mobility. The phase of the n^{th} path caused by propagation can be modeled as [3]

$$\phi_{0,n}(f) = 2\pi f d_n/c - \psi_n, \tag{5}$$

where ψ_n is a frequency-independent phase that captures whether the path is direct or reflected. Unfortunately, the first term of (5) can be very different because of the frequency separation in FDD systems. For example, when $\Delta f = 30$ MHz and $d_n = 1$ m, the phase difference in $\phi_{0,n}(f)$ is 0.2π.

When Alice is moving with angle θ_v and velocity v, the offset phase caused by the mobility is given by

$$\phi_{v,n}(t,f) = 2\pi f v\cos(\theta_n - \theta_v)t/c, \tag{6}$$

where θ_n is the angle of departure (AoD) for the n^{th} path at Alice, defined as the mean angle with which a departing path's power is transmitted, It is observed that channel phase is a frequency dependent propagation characteristics.

4) Angle: The angle of arrival (AoA) is defined as the mean of angles of an incident path's power at the receiver. As the propagation paths of the uplink and downlink are reciprocal, the AoA in the uplink is equal to the AoD in the downlink, and vice versa.

The angle spread represents the root mean square of angles with which a departure/arrival path's power is transmitted/received. Measurements have shown that angle spread does not significantly deviate with the channel frequency [9, 13].

C. Channel Modeling for FDD Systems

Based on the above analysis and the 3GPP spatial channel model [16], the channel coefficient of the n^{th} path can be expressed as

$$h_n(t,f) = g_n(f)\exp\big(-j\phi_n(t,f)\big). \tag{7}$$

Since the path amplitude varies in a larger time scale than that of path phase, $g_n(f)$ is not considered as an explicit function of time, t, in this paper. The path amplitude $g_n(f)$ is given by

$$g_n(f) = \sqrt{\sigma_{\mathrm{PL}}(f)\sigma_{\mathrm{SF}}P(\tau_n)}, \tag{8}$$

where $\sigma_{\mathrm{PL}}(f)$ is the path loss gains. According to the ABG model, $\sigma_{\mathrm{PL}}(f)$ can be given as

$$\sigma_{\mathrm{PL}}(f) = 10^{\beta/10}d^{\alpha}f^{\gamma}. \tag{9}$$

The path phase $\phi_n(t,f)$ is given as

$$\phi_n(t,f) = \phi_{0,n}(f) + \phi_{v,n}(t,f). \tag{10}$$

Considering the frequency impact on path amplitude and phase, the overall FDD channel model is established as (11).

In the wideband channel, the coefficient of the ℓ^{th} sub-carrier in an orthogonal frequency-division multiplexing (OFDM) system is given by

$$H(t,f,\ell) = \sum\nolimits_{n=1}^{N} h_n(t,f)\exp(-j2\pi\tau_n\ell/L), \tag{12}$$

where L is the number of sub-carriers.

$$h(t,f,\tau)=\sum\nolimits_{n=1}^{N}\sqrt{10^{\beta/10}d^{\alpha}\sigma_{\mathrm{SF}}P(\tau_n)}f^{\gamma/2}\exp\Big(-j(2\pi f d_n/c-\psi_n+2\pi f v\cos(\theta_n-\theta_v)t/c)\Big)\delta(\tau-\tau_n). \tag{11}$$

III. Reciprocal Channel Construction

According to the channel model established in Section II-C, the channel coefficient is frequency dependent and its relationship with frequency is not straightforward. To facilitate key generation in FDD systems, we propose a novel reciprocal channel construction framework named SAR, which is consisted of three steps: path Separation, Adjustment and Reconstruction.

A. Path Separation

Due to the frequency-dependent phase of each channel path, radio waves that reinforce each other on one frequency may cancel each other on another one. As a result, the bidirectional wireless channels may be quite different in FDD systems due to the superposition effects of multipath. The OFDM systems will get the estimation of frequency response, $\widehat{H}(t,f,\ell)$. We then perform multipath separation to map the $\widehat{H}(t,f,\ell)$ to individual paths $\{\widehat{h}_n(t,f)\}$, which can be obtained by

$$\widehat{h}_n(t,f)=\frac{1}{\sqrt{L}}\sum\nolimits_{\ell=1}^{L}\widehat{H}(t,f,\ell)\exp(j2\pi n\ell/L). \tag{13}$$

We use the same definition of the signal to noise ratio (SNR) as in [17], which is defined in the frequency domain as

$$\mathrm{SNR}=\frac{\mathbb{E}_{t,\ell}\{|H(t,f,\ell)|^2\}}{\sigma^2} \tag{14}$$

where $\mathbb{E}_{t,\ell}\{|H(t,f,\ell)|^2\}$ represents the average channel gains in the frequency domain and σ^2 is the noise variance. In OFDM systems, the length of cyclic prefix is designed longer than the maximum delay. In addition, the length of cyclic prefix is less than that of half OFDM sub-carriers. Thus, the path gains in the time domain are concentrated in the region $n<L/2$, and we can use the second half signals in the time domain ($n\geq L/2$) to estimate the noise variance σ^2. When the power of $\widehat{h}_n(t,f)$ is more than 10 times σ^2, the n^{th} is considered as a valid propagation path in this paper.

B. Adjustment

Both amplitude and phase of each path are frequency dependent, and thus need to be adjusted after the path separation. A novel amplitude and phase adjustment algorithm for the n^{th} path is shown in Algorithm 1. $\widehat{x}$ and $\widetilde{x}$ represent the estimated and adjusted variables, respectively.

The amplitude adjustment is straightforward. A frequency independent channel amplitude is achieved by dividing $f^{\gamma/2}$, as shown in step 1 of the Algorithm 1. The adjusted amplitude then becomes $\widetilde{g}_n=\sqrt{10^{\beta/10}d^{\alpha}\sigma_{\mathrm{SF}}P(\tau_n)}$.

Phase adjustment is a little complicated. According to (10), the phase difference between two adjacent channel coefficients can be given as $\Delta\phi_n(t,f)=2\pi v\cos(\theta_n-\theta_v)\Delta t f/c$, where Δt is the sampling interval and usually very short in practical systems, e.g., 0.5 ms. Step 2 eliminates the initial phase $\phi_{0,n}(f)$ by time-domain differential. $\Delta\widehat{\phi}_n(t,f)$ usually falls to $[-\pi,\pi]$, e.g., when $v=10$ m/s, $\Delta t=0.5$ ms, $f=2$ GHz. Next, Step 3 compensates $\Delta\widehat{\phi}_n(t,f)$ in case of a sudden change. Since $\exp\big(-j\phi_n(t,f)\big)$ in (11) is a periodic function with period 2π, the estimated path phase $\widehat{\phi}_n(t,f)$ is actually $\bmod\ (\phi_n(t,f),2\pi)$, where $\bmod\ (\cdot,\cdot)$ represents the modulus operator. There is a possibility that $\Big|\Delta\hat{\phi}_n(t,f)\Big|$ is larger than π. For example, $\phi_n(t+\Delta t,f)$ is a little bit less than 2π while $\phi_n(t,f)$ is slightly larger than 2π. Hence, $\widehat{\phi}_n(t+\Delta t,f)$ is close to 2π while $\widehat{\phi}_n(t,f)$ is close to 0. Finally, Step 4 divides the frequency value and we obtain a frequency-invariant differential phase $\widetilde{\phi}_n(t)$.

Algorithm 1 Amplitude and phase modification algorithm.

```
Require: The $n^{th}$ path channel $\widehat{h}_n(t,f)=\widehat{g}_n(f)\exp(-j\widehat{\phi}_n(t,f))$ sampled by time interval $\Delta t$;
Ensure: The $n^{th}$ adjusted path channel $\widetilde{h}_n(t)=\widetilde{g}_n\exp(-j\widetilde{\phi}_n(t))$;
1: Adjust the channel amplitude by $\widetilde{g}_n=\widehat{g}_n(f)/f^{\gamma/2}$.
2: Calculate the phase difference between the adjacent time as $\Delta\widehat{\phi}_n(t,f)=\widehat{\phi}_n(t+\Delta t,f)-\widehat{\phi}_n(t,f)$.
3: Compensate phase difference by
       $\Delta\bar{\phi}_n(t,f)=\Delta\widehat{\phi}_n(t,f)+2k\pi,\ k\in\{0,\pm 1\}$
   satisfying $|\Delta\bar{\phi}_n(t,f)|\leq\pi$;
4: Construct the reciprocal phase $\widetilde{\phi}_n(t)=\Delta\bar{\phi}_n(t,f)c/f$.
5: return $\widetilde{h}_n(t)$;
```

Please note that the adjusted amplitude and phase are not the estimation of the real amplitude and phase, but constructed for the key generation purpose to get reciprocal characteristics.

C. Reconstruction

At last, the channel is reconstructed by superimposing the adjusted paths and its frequency response can be given as

$$\widetilde{H}\left(t,\ell\right)=\sum\nolimits_{n=1}^{N}\widetilde{h}_n(t)\exp(-j2\pi\tau_n\ell/L), \tag{15}$$

The reconstructed channel is invariant of carrier frequency.

IV. Simulation Results

This section evaluated the reciprocity performance of the proposed SAR approach by numerical simulations. An FDD OFDM system was considered with the centering frequency $f_1=2.4$ GHz and $f_2=2.64$ GHz. The channel coefficients in the frequency domain are generated according to (12) and the multipath number is set as $N=6$. We used the same quantization algorithm as in [17], which is a two-level quantization with 10% guardband.

Fig. 1 compares the coefficients of the original and constructed channels of Alice and Bob, respectively. The SNR is 10 dB. The left two sub-figures are the amplitude and real

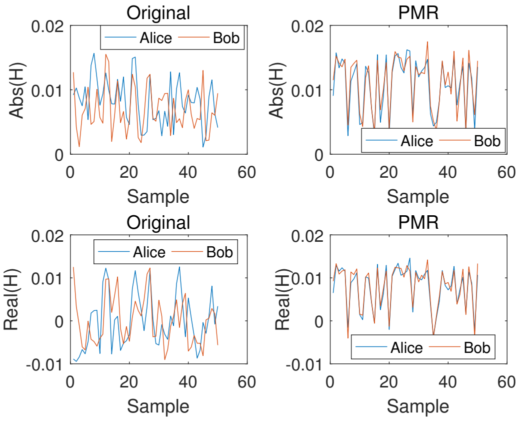
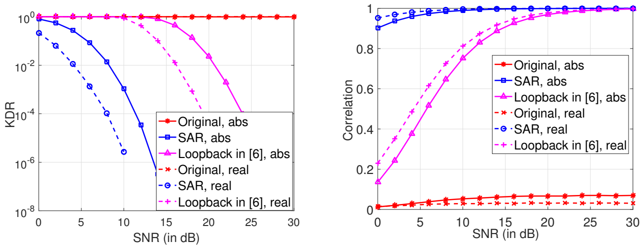


Fig. 1. Channel coefficients of one sub-carrier. SNR is 10 dB.



(a) (b)

Fig. 2. The comparison of (a) KDR and (b) cross-correlation versus SNR.

part of the original channel, while the right two sub-figures are those in the constructed channel. From the results, the original channel coefficients have very large differences, while constructed channel coefficients are strongly matched.

The key disagreement ratio (KDR) is defined as the number of failed groups divided by the number of the entire groups, where the length of secret key is 128-bit. Let y_1/y_2 denote the amplitude or real part of the channel estimation at Alice/Bob. The cross-correlation between y_1 and y_2 is defined as

$$\rho = \frac{1}{\sigma_{y_1}\sigma_{y_2}}\mathbb{E}\{(y_1-\mu_{y_1})(y_2-\mu_{y_2})\}, \tag{16}$$

where μ_{y_1} and σ_{y_1} are the mean and standard deviation of y_1.

These two metrics are commonly used to evaluate key generation reciprocity [17] and are also used in this paper.

Fig. 2 compares our scheme with the loopback scheme in [6] in terms of the KDR and cross-correlation. Both amplitudes and real parts of the original channel are quite different, and their correlation coefficients are low and the KDRs approach 1. Compared with the loopback scheme, when the KDR is 10^{-4}, our scheme using modified channel can improve the performance about 10 dB. The cross-correlation of our proposed scheme was also much better than the loopback scheme. As the adjusted channel coefficients are reciprocal and noise has a greater influence on amplitudes than real parts, the performance of real parts is better than that of amplitudes.

V. Conclusion

This letter for the first time designed a FDD-based key generation scheme by employing a general reciprocal channel construction framework. A detailed analysis of propagation characteristics in both large-scale fading and small-scale fading was carried out and both amplitude and phase of the channel coefficients are found not reciprocal in FDD systems. In order to construct reciprocal characteristics for key generation, we proposed an SAR protocol, by first separating the channel paths, then adjusting them according to the carrier frequency, and finally reconstructing the path amplitude and phase. Numerical results demonstrated that our SAR protocol can construct bidirectional channel coefficients with high reciprocity, and enable key generation applied in FDD systems.

References

[1] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, no. 3, pp. 614–626, 2017.

[2] W. J. Wang, H. Y. Jiang, X. G. Xia, P. C. Mu, and Q. Y. Yin, "A wireless secret key generation method based on chinese remainder theorem in FDD systems," *Science China (Information Sciences)*, vol. 55, no. 7, pp. 1605–1616, 2012.

[3] D. Vasisht, S. Kumar, H. Rahul, and D. Katabi, "Eliminating channel feedback in next-generation cellular networks," in *Proc. ACM SIGCOMM Conf*, Florianopolis, Brazil, Aug. 2016, pp. 398–411.

[4] A. M. Allam, "Channel-based secret key establishment for FDD wireless communication systems," *Communications on Applied Electronics*, vol. 7, no. 9, pp. 2394–4714, 2017.

[5] X. Wu, Y. Peng, C. Hu, H. Zhao, and L. Shu, "A secret key generation method based on CSI in OFDM-FDD system," in *Proc. IEEE GLOBECOM Workshops*, Atlanta, GA, USA, Dec. 2014, pp. 1297–1302.

[6] S. J. Goldberg, Y. C. Shah, and A. Reznik, "Method and apparatus for performing JRNSO in FDD, TDD and MIMO communications," *US Patent, US8401196*, 2013.

[7] L. Peng, G. Li, J. Zhang, R. Woods, M. Liu, and A. Hu, "An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation," *IEEE Trans. Mobile Comput.*, pp. 1–1, 2018.

[8] G. LTE, "Evolved universal terrestrial radio access (E-UTRA); User equipment (UE) radio transmission and reception," *Technical Specification 36.101 Release 10*.

[9] D. S. Baum, J. Hansen, and J. Salo, "An interim channel model for beyond-3G systems: extending the 3GPP spatial channel model (SCM)," in *Proc. IEEE VTC*, Stockholm, Sweden, May 2005, pp. 3132–3136.

[10] S. Sun, T. A. Thomas, T. S. Rappaport, H. Nguyen, I. Z. Kovacs, and I. Rodriguez, "Path loss, shadow fading, and line-of-sight probability models for 5G urban macro-cellular scenarios," in *Proc. IEEE Globecom Workshops*, San Diego, CA, USA, Dec. 2015, pp. 1–7.

[11] S. Sun, T. S. Rappaport, S. Rangan, T. A. Thomas, A. Ghosh, I. Z. Kovacs, I. Rodriguez, O. Koymen, A. Partyka, and J. Jarvelainen, "Propagation path loss models for 5G urban micro- and macro-cellular scenarios," in *Proc. IEEE VTC*, Nanjing, China, Jul. 2016, pp. 1–6.

[12] W. Kim, H. Lee, J. J. Park, M. D. Kim, and H. K. Chung, "Carrier frequency effects on propagation characteristics in rural macro environments," in *Proc. Fourth Int. Conf. Communications and Networking in China*, Xian, China, Aug. 2009, pp. 1–5.

[13] IST-WINNER, "Deliverable 1.1. 2 v. 1.2,"WINNER II Channel Models", ist-winner2," Tech. Rep., 2008 (http://projects. celtic-initiative. org/winner+/deliverables. html), Tech. Rep., 2007.

[14] D. W. Matolak, K. A. Remley, C. Holloway, and C. Gentile, "Outdoor-to-indoor channel dispersion and power-delay profile models for the 700-MHz and 4.9-GHz bands," *IEEE Antennas Wireless Propag. Lett.*, vol. 15, pp. 441–443, 2015.

[15] Y. Oda, R. Tsuchihashi, K. Tsunekawa, and M. Hata, "Measured path loss and multipath propagation characteristics in uhf and microwave frequency bands for urban mobile communications," in *Proc. IEEE VTC Spring*, Rhodes, Greece, 2001, pp. 337–341.

[16] 3GPP, "Spatial channel model for MIMO simulations," *TR 25.996 V14.0.0*, Mar 2017.

[17] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, 2018.