On the Key Generation from Correlated Wireless Channels

Zhang, J., He, B., Duong, T. Q., & Woods, R. (2017). On the Key Generation from Correlated Wireless Channels. *IEEE Communications Letters*, *21*(4), 961-964. https://doi.org/10.1109/LCOMM.2017.2649496

Published in:
IEEE Communications Letters

Document Version:
Peer reviewed version

On the Key Generation from Correlated Wireless Channels

Junqing Zhang, Biao He, *Member, IEEE,* Trung Q. Duong, *Senior Member, IEEE,* and Roger Woods, *Senior Member, IEEE*

***Abstract*—This letter investigates the secret key capacity of key generation from correlated wireless channels in a source model. We systematically study a practical scenario by taking into account all relevant parameters including sampling delay, eavesdroppers' location, qualities of legitimate and eavesdropping channels, Doppler spread, and pilot length. Our findings indicate that secret key capacity is determined by the cross correlation of the channel measurements, and a better legitimate channel is not necessary when the correlation between legitimate channels is higher than correlation between legitimate and eavesdropping channels. We also find that it is possible to tune the secret key capacity by carefully designing the sampling delay, pilot length, and channel qualities. This letter offers practical design guidelines on secure key generation systems.**

***Index Terms*—Physical layer security, key generation, secret key capacity**

I. Introduction

Key generation extracts common randomness of the unpredictable features residing in wireless channels between users [1]. By alternately and separately measuring their common channel, the legitimate users, namely Alice and Bob, can obtain highly correlated channel measurements. With a key generation protocol including quantization, information reconciliation, and privacy amplification, the users can establish a common cryptographic key through the noisy channel measurements [1].

The security performance of key generation is characterized by the secret key capacity, which was first derived and formalized in [2], [3]. The scenario that Alice and Bob are observing the same Gaussian random source and the mutual information between their noisy and correlated observation was studied in [4]. The work in [5] investigated key generation over temporally correlated fading channels and derived the secret key capacity between two legitimate users. By taking into account the effects of channel qualities and channel estimation, a more practical implementation and setup was considered in [6]. Spatial decorrelation was experimentally studied in [7]–[9].

This work was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, by the Royal Society Research Grant under Grant ID RG160302, and by the Newton Institutional Link under Grant ID 172719890.

J. Zhang and T. Q. Duong are with the Institute of Electronics, Communications and Information Technology in Queen's University Belfast, Belfast, U.K. (email: {jzhang20, trung.q.duong}@qub.ac.uk)

R. Woods is with the Electronics and Computer Engineering Cluster in Queen's University Belfast, Belfast, U.K. (email: r.woods@qub.ac.uk)

B. He is with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong. (email: eebiaohe@ust.hk)

However, a general analysis of the secret key capacity is missing. Many commercial wireless transceivers are half-duplex, and the sampling delay will impact the mutual information between Alice and Bob. In addition, the information leaked to eavesdroppers will decrease the secret key capacity, or even render an insecure key generation system when eavesdroppers have a better correlation such as when they are very close to the legitimate users. These effects are essential for the design of secure key generation systems, however, they have not been considered in previous work.

In this letter, we carry out a complete and rigorous analysis on the secret key capacity by considering a more general and practical scenario and taking into account sampling delay and eavesdropping. We first derive the analytical expression of secret key capacity and then validate it by Monte Carlo simulations. We find that the secret key capacity is determined by the cross correlation of the channel measurements and a better legitimate channel is not required in order to achieve a positive secret key capacity, as long as the correlation between the measurements of legitimate users are higher than the correlation between measurements of legitimate user and eavesdropper. We analyze the effects of all the relevant parameters including correlation relationship of legitimate and eavesdropping channels, channel estimation, sampling delay, and provide guidelines on the design of a practical and secure key generation system.

Notation: Lower case letters and bold lower case letters denote scalar and vector, respectively. $(\cdot)^\dagger$ denotes the conjugate transpose, and $E\{\cdot\}$ is the expectation operation.

II. System Model

A key generation source model[1] is shown in Fig. 1, which includes Alice and Bob, and an eavesdropper, Eve, located d meters away from Bob. Without loss of generality, only the scenario that Eve observes Alice's transmission is considered. In the source model, the users measure their common channel, and will get noisy but correlated observations. Key generation usually works in time-division duplex (TDD) mode and all the users run at the same frequency, therefore, the uplink and downlink channels are reciprocal. As shown in Fig. 2, at time $t_a(i) = iT_s$, where T_s is the sampling period and $i = 0, 1, ..., M-1$, Alice sends out a packet, through which Bob and Eve can measure the channel. At time $t_b(i) = iT_s + \tau$, where τ is the sampling delay, Bob also sends out a packet and Alice can carry out the channel measurement.

[1]Key generation channel model is not considered in this letter.

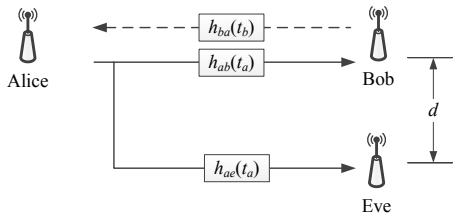


Fig. 1. Key generation source model

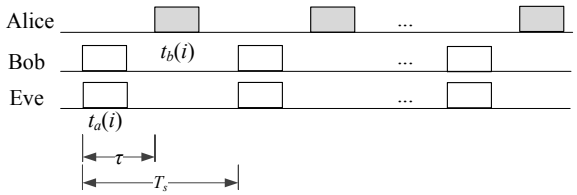


Fig. 2. Timing of the measurements

In this letter, we consider a time-varying Rayleigh fading channel with a Jakes Doppler spectrum, $h_{ab} \sim \mathcal{CN}(0, \sigma_h^2)$ and the autocorrelation function of the channel gain is given as

$$\begin{aligned}\rho(h_{ab}(t_a), h_{ab}(t_b)) &= \frac{E\{h_{ab}(t_a)^\dagger h_{ab}(t_a+\tau)\}}{\sigma_h^2} \\ &= J_0(2\pi f_d \tau) = r_1(\tau), \end{aligned} \tag{1}$$

where $J_0(\cdot)$ is a zeroth-order Bessel function of the first kind, f_d is the maximum Doppler shift. The eavesdropping channel is also a Rayleigh fading channel, $h_{ae} \sim \mathcal{CN}(0, \sigma_{h_{ae}}^2)$. It is related to h_{ab} as [10]

$$h_{ae} = \frac{1}{\sqrt{\beta}}(r_2(\Delta d) h_{ab} + \sqrt{1 - r_2(\Delta d)^2}\omega), \tag{2}$$

where $\beta = \sigma_h^2/\sigma_{h_{ae}}^2$, $r_2(\Delta d) = J_0(2\pi\Delta d)$, $\Delta d = \frac{d}{\lambda}$, λ is the length of waveform, and $\omega \sim \mathcal{CN}(0, \sigma_h^2)$. The correlation between h_{ab} and h_{ae} can be calculated as

$$\rho(h_{ab}(t), h_{ae}(t)) = \frac{E\{h_{ab}(t)^\dagger h_{ae}(t)\}}{\sigma_h \sigma_{h_{ae}}} = r_2(\Delta d), \tag{3}$$

which allows us to model the spatial decorrelation and analyze its effect on the secret key capacity.

The channel can be measured by sending pilot sequence $\mathbf{s}$ from the transmitter u to the receiver v, $\{u, v\} = \{a, b, e\}$. In a block fading channel, channel gains remain the same during the pilot transmission. The received signal can be written as

$$\mathbf{y}_v = h_{uv}\mathbf{s} + \mathbf{n}_v, \tag{4}$$

where $\mathbf{n}_v$ is additive white Gaussian noise (AWGN) at the receiver v with variance $\sigma_{n_v}^2$, and h_{uv} is the channel gain. The receiver can then estimate the channel using least square (LS) method as

$$\widehat{h}_{uv} = \frac{\mathbf{s}^\dagger}{||\mathbf{s}||^2}\mathbf{y}_v = h_{uv} + \frac{\mathbf{s}^\dagger}{||\mathbf{s}||^2}\mathbf{n}_v, \tag{5}$$

and

$$\sigma_{\widehat{h}_{uv}}^2 = \sigma_{h_{uv}}^2 + \frac{\sigma_{n_v}^2}{||\mathbf{s}||^2} = \sigma_{h_{uv}}^2 + \frac{\sigma_{n_v}^2}{P l_p}, \tag{6}$$

where P is the instantaneous transmission power and l_p is the length of $\mathbf{s}$. The signal-to-noise ratio (SNR) of the channel is

$$\gamma_{uv} = \frac{P\sigma_{h_{uv}}^2}{\sigma_{n_v}^2}. \tag{7}$$

Assuming all the users have the same noise power σ_n^2, so that $\gamma_{ab} = \beta\gamma_{ae}$. The mean-square error (MSE) of LS estimation can be given as

$$\eta_{uv} = \frac{1}{\gamma_{uv} l_p}. \tag{8}$$

III. Security Analysis

The secret key capacity, $C_{SK}^{\widehat{h}}$ [11], is

$$C_{SK}^{\widehat{h}} = I(\widehat{h}_{ab}, \widehat{h}_{ba}) - I(\widehat{h}_{ab}, \widehat{h}_{ae}). \tag{9}$$

In this section, we derive the secret key capacity of the key generation source model and analyze all the relevant parameters.

As the users are running at the same carrier frequency, according to the channel reciprocity, $h_{ba}(t) = h_{ab}(t)$, then $\rho(h_{ab}(t_a), h_{ba}(t_b)) = \rho(h_{ab}(t_a), h_{ab}(t_b)) = r_1(\tau)$.

The cross correlation coefficient between $\widehat{h}_{uv}$ and $\widehat{h}_{tr}$ can be given as

$$\rho(\widehat{h}_{uv}, \widehat{h}_{tr}) = \frac{1}{\sqrt{1+\eta_{uv}}\sqrt{1+\eta_{tr}}}\rho(h_{uv}, h_{tr}), \tag{10}$$

where $\{t, r\} = \{a, b, e\}$.

Because h_{uv}, h_{tr}, $\widehat{h}_{uv}$ and $\widehat{h}_{tr}$ follow Gaussian distribution, their mutual information [12] can be calculated as

$$I(h_{uv}, h_{tr}) = -\frac{1}{2}\log_2(1 - \rho(h_{uv}, h_{tr})^2), \tag{11}$$

$$I(\widehat{h}_{uv}, \widehat{h}_{tr}) = -\frac{1}{2}\log_2(1 - \rho(\widehat{h}_{uv}, \widehat{h}_{tr})^2). \tag{12}$$

The secret key capacity can be derived as

$$\begin{aligned} C_{SK}^{\widehat{h}} &= \frac{1}{2}\log_2\left(1 - \rho(\widehat{h}_{ab}, \widehat{h}_{ae})^2\right) - \frac{1}{2}\log_2\left(1 - \rho(\widehat{h}_{ab}, \widehat{h}_{ba})^2\right) \\ &= \frac{1}{2}\log_2\left(\frac{1 + \eta_{ab} - \frac{r_2(\Delta d)^2}{1+\beta\eta_{ab}}}{1 + \eta_{ab} - \frac{r_1(\tau)^2}{1+\eta_{ab}}}\right). \end{aligned} \tag{13}$$

$C_{SK}^{\widehat{h}}$ is affected by parameters including η_{ab} (equivalently γ_{ab} and l_p), $r_1(\tau)$ (equivalently τ and f_d), $r_2(\Delta d)$ (equivalently Δd), and β.

In order to obtain a positive $C_{SK}^{\widehat{h}}$, the variable of the logarithm function $\log(x)$ should be larger than one and the condition can be written as

$$\alpha = \left(\frac{r_2(\Delta d)^2}{1+\beta\eta_{ab}}\right) / \left(\frac{r_1(\tau)^2}{1+\eta_{ab}}\right) < 1. \tag{14}$$

$$\Rightarrow \beta > \underbrace{\left[\frac{r_2(\Delta d)^2}{r_1(\tau)^2} - 1\right]\gamma_{ab} l_p}_{\beta_1} + \underbrace{\frac{r_2(\Delta d)^2}{r_1(\tau)^2}}_{\beta_2} = \beta'. \tag{15}$$

- When $r_2(\Delta d) < r_1(\tau)$, $\beta_1 < 0$, $\beta_2 < 1$, then $\beta' < 1$. There always exists values $\beta' < \beta < 1$.
- When $r_2(\Delta d) \geq r_1(\tau)$, $\beta_1 \geq 0$, $\beta_2 \geq 1$, then $\beta' \geq 1$. Therefore $\beta > \beta' \geq 1$.

When $r_2(\Delta d) < r_1(\tau)$, even eavesdroppers have a higher SNR than the legitimate users, as long as they do not have a better channel correlation, the system can still generate keys securely. Even when $r_2(\Delta d) \geq r_1(\tau)$, legitimate users can still achieve a positive secret key capacity by improving their channel quality, or deteriorating the eavesdropping channels such as introducing artificial noise.

IV. Simulation Results and Design Guidelines

In this section, we analyze effects of all the parameters through simulation and offered insights to design a secure key generation system. $I(\widehat{h}_{uv}, \widehat{h}_{tr})$ and $C_{SK}^{\widehat{h}}$ can be calculated by (12) and (13), respectively. Besides the results of the noisy channel measurements, we showed the results of the noiseless channel as a comparison, where $I(h_{uv}, h_{tr})$ can be calculated by (11) and C_{SK}^{h} is given as

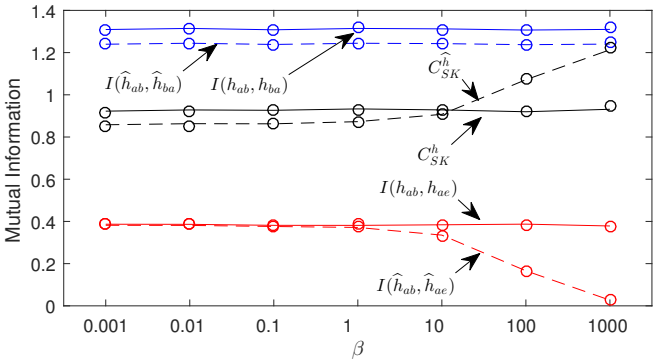
$$C_{SK}^{h} = I(h_{ab}, h_{ba}) - I(h_{ab}, h_{ae}). \tag{16}$$

We also carried out the Monte Carlo simulations to validate our analytical analysis. For each simulation, we ran $M = 100,000$ times. We then used a method based on k-nearest neighbor (knn) distances [13] to numerically compute the mutual information. In all the figures below, lines represent the analytical results and markers (o) represent the numerical results calculated by knn method. As observed from the figures, the numerical and analytical results matched very well.

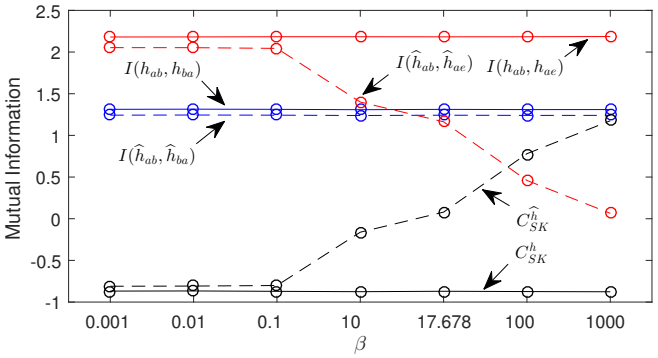
The mutual information are affected by the channel qualities between Alice, Bob, and Eve. The effect of β, i.e., the ratio of legitimate channel's SNR and eavesdropping channel's SNR, is evaluated by applying two examples and the results are shown in Fig. 3. In the setting of Fig. 3a, $\beta' = -48.947$, therefore $\beta > \beta'$ always holds, which can be seen from the figure. When $0 < \beta < 1$, the legitimate channel quality is not as good as the eavesdropping channel, but the system is still secure. However, when the eavesdropper is much closer to Bob, as shown in Fig. 3b, $\beta' = 17.678$, the legitimate channel's SNR should be at least 17.678 times higher than the eavesdropping channels' SNR, in order to obtain a better correlation between the channel measurements and thereof a positive $C_{SK}^{\widehat{h}}$. In a slow fading channel with $f_d = 10$ Hz and a sampling delay $\tau = 0.01$ s, only when $\Delta d < f_d\tau = 0.1$, the system may not be secure. In a 2.4 GHz system, this distance is $d = 0.1 \times c/f_c = 0.1 \times 3 \times 10^8/(2.4 \times 10^9) = 1.25$ cm, which is quite short and the legitimate users will be aware whenever the eavesdroppers are so close to them.

As shown in (8), the channel estimation performance is affected by the SNR and pilot. Their effects on the key generation performance are shown in Fig. 4 and Fig. 5, respectively. In a low SNR environment, the channel estimation performance is affected by the noise and the mutual information $I(\widehat{h}_{ab}, \widehat{h}_{ba})$ is very small. A longer pilot performs better in suppressing the noise effect and improving the key generation performance.

The mutual information is also affected by the sampling delay and channel variations. The sampling delay, τ, will affect the measurements correlation between Alice and Bob. As shown in Fig. 6, a τ that is too small does not help to get a high secret key capacity. When the values of $\rho(\widehat{h}_{ab}, \widehat{h}_{ba})$ and $\rho(h_{ab}, h_{ba})$ are very close to one, although $\rho(\widehat{h}_{ab}, \widehat{h}_{ba})$ is only slightly smaller than $\rho(h_{ab}, h_{ba})$, $I(\widehat{h}_{ab}, \widehat{h}_{ba})$ is much smaller than $I(h_{ab}, h_{ba})$. This is because the logarithm function $\log(x)$ decreases quickly when x is close to zero. Most of the published key generation systems are applied in slow fading channels and the analysis in a fast fading channel has never been discussed. As shown in Fig. 6b, when τ is smaller than 0.001 s, the system can still get a positive secret key capacity. This requirement is relatively easy to meet. It has been reported in [9] that a key generation system with $\tau = 60 \times 10^{-6}$ s is designed. The mutual information change versus Doppler spread, f_d, is shown in Fig. 7. The value, $f_d = 100$ Hz, is the typical Doppler spread in vehicular



(a) $r_2(\Delta d) < r_1(\tau)$. $\Delta d = 0.2$, $r_2(\Delta d) = 0.6425$.



(b) $r_2(\Delta d) \geq r_1(\tau)$. $\Delta d = 0.05$, $r_2(\Delta d) = 0.9755$.

Fig. 3. Mutual information change versus β. $r_1(\tau) = 0.9037$, $f_d = 10$ Hz, $\tau = 0.01$ s, $\gamma_{ab} = 10$ dB, and $l_p = 10$.

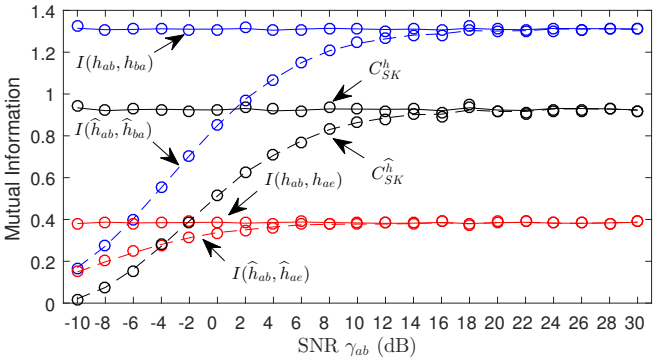


Fig. 4. Mutual information change versus SNR γ_{ab}. $l_p = 10$, $f_d = 10$ Hz, $\tau = 0.01$ s, $\beta = 0.1$, and $\Delta d = 0.2$.

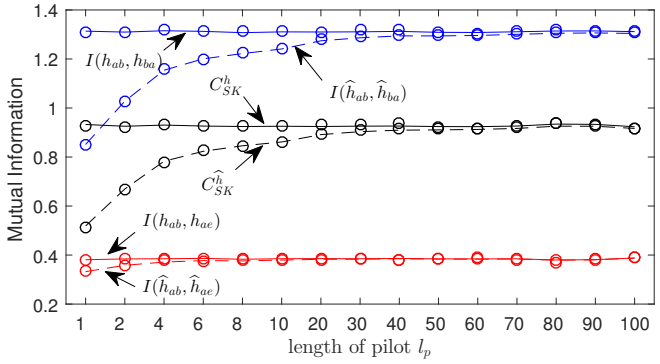


Fig. 5. Mutual information change versus pilot length l_p. $\gamma_{ab} = 10$ dB, $f_d = 10$ Hz, $\beta = 0.1$, $\tau = 0.01$ s, and $\Delta d = 0.2$.

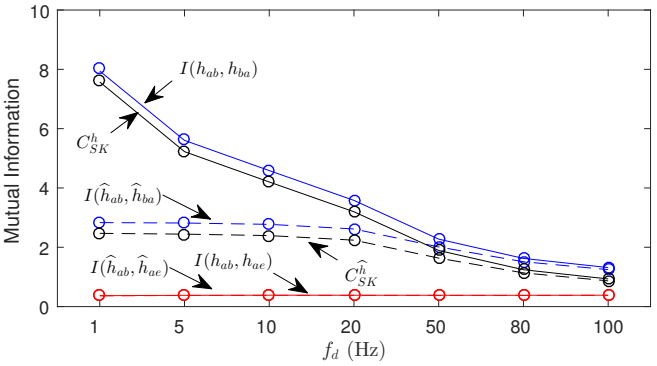
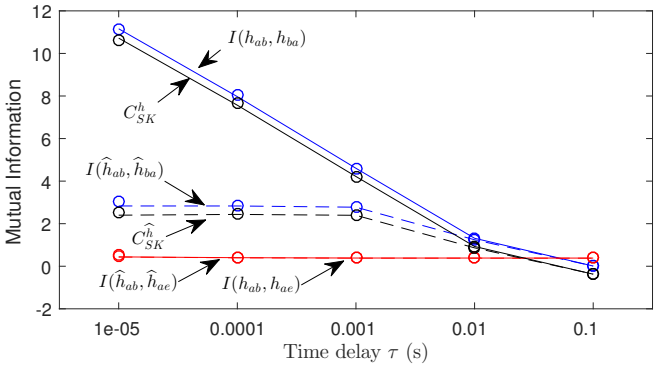
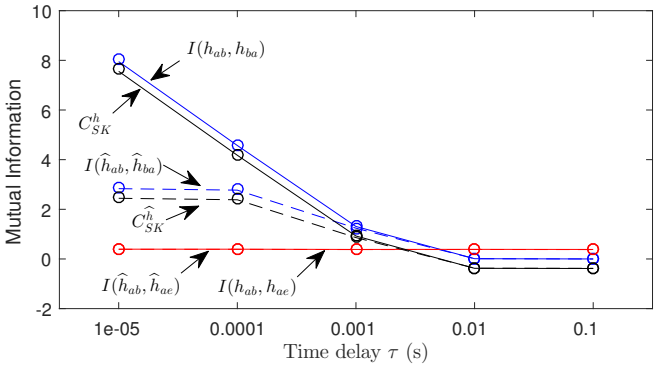


Fig. 7. Mutual information change versus Doppler shift f_d. $\gamma_{ab} = 10$ dB, $l_p = 10$, $\tau = 0.001$ s, $\beta = 0.1$, and $\Delta d = 0.2$.



(a) Slow fading channel with $f_d = 10$ Hz.



(b) Fast fading channel with $f_d = 100$ Hz.

Fig. 6. Mutual information change versus time delay τ. $\gamma_{ab} = 10$ dB, $l_p = 10$, $\beta = 0.1$, and $\Delta d = 0.2$.

communications and therefore key generation is workable in most of the application scenarios with a less dynamic channel. Secret key capacity characterizes the information amount that can be extracted in one realization and is not affected by the sampling period, T_s.

V. Conclusion

This letter systematically investigated the secret key capacity of key generation from wireless channels by considering effects of sampling delay and eavesdropping in a source model. We found that secret key capacity is determined by the cross correlation coefficients of the channel measurements and a better legitimate channel is not required. We analyzed the effects of all the relevant parameters, including sampling delay, eavesdroppers' location, qualities of legitimate and eavesdropping channels, Doppler spread, and pilot length. Key generation design guidelines were provided to achieve a high and positive secret key capacity.

References

[1] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, Mar. 2016.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography – Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[4] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE Int. Symp. Inform. Theory*, Seattle, WA, USA, Jul. 2006, pp. 2593 – 2597.

[5] X. Wu, Y. Song, C. Zhao, and X. You, "Secrecy extraction from correlated fading channels: An upper bound," in *Proc. Int. Conf. Wireless Commun. & Signal Processing*, Nanjing, China, Dec. 2009, pp. 1–3.

[6] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[7] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th Annu. Int. Conf. Mobile Computing and Networking (MobiCom)*, San Francisco, California, USA, Sep. 2008, pp. 128–139.

[8] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, 2010.

[9] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, Aug. 2016.

[10] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis, and R. Schober, "Amplify-and-forward relay selection with outdated channel estimates," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1278–1290, 2012.

[11] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011, p. 121.

[12] T. M. Cover and J. A. Thomas, *Elements of information theory*, 2nd ed. John Wiley & Sons, 2006, p. 252.

[13] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Physical Review E*, vol. 69, no. 6, p. 066138, 2004.