Channel covariance matrix based secret key generation for low-power terminals in frequency division duplex systems

Zheng Wan, Kaizhi Huang, Yangming Lou, and Yajun Chen
Information Engineering University, Zhengzhou, People’s Republic of China
✉Email: huangkaizhi@tsinghua.org.cn

Abstract

The existing secret key generation (SKG) techniques are not applicable for frequency division duplex (FDD) Internet of Things networks due to the low power constraints and limited computing resources. This letter proposes a SKG scheme based on the channel covariance matrix in FDD systems. First of all, a novel algorithm is proposed for inferring the downlink channel covariance matrix from the observed uplink channel covariance matrix with the aid of the transformation matrix. Then, a complete SKG scheme for low-power terminals in FDD systems is designed to generate keys from the downlink channel covariance matrix. Finally, simulation results show that this scheme can generate high-agreement secret keys in FDD systems. Compared with the loopback mechanism-based SKG scheme, this scheme is suitable for low-power terminals and can achieve significant performance improvement in terms of the key disagreement ratio.

Introduction:
Physical layer secret key generation (SKG) techniques based on wireless channels have been widely studied in recent years, which can provide lightweight cryptographic protocols for wireless communication systems. Based on the reciprocity, spatial decorrelation and temporal variation of wireless channels, two legitimate users can obtain real-time updated secret keys through the steps of channel estimation, quantization, information reconciliation and privacy amplification [1]. However, the reciprocity of wireless channels is no longer hold since the uplink channel and the downlink channel experience different fading in frequency division duplex (FDD) systems. As a result, most reciprocal shared random sources used in time division duplex (TDD) systems, such as received signal strength, channel impulse response and channel frequency response, are completely different between the uplink and downlink channel in FDD systems.

Several research works have attempted to address the above problems. Based on the spatial reciprocity, some works have explored frequency-independent parameters to generate secret keys. In [2], the angle and delay of each path were extracted to generate shared keys. In [3], considering the slow variability of the channel covariance matrix, a SKG scheme based on the channel covariance matrix eigenvectors was proposed. However, the complexity of path extraction algorithms and special restrictions on the antenna configuration in [2, 3] was not suitable for low-power terminals. Besides spatial reciprocity-based schemes, a loopback mechanism-based SKG scheme was proposed in [4]. Nevertheless, this method was insecure and can be attacked by a passive eavesdropper [5].

In this letter, we propose a secret key generation scheme based on the channel covariance matrix in FDD systems. We design a novel algorithm to infer the downlink channel covariance matrix (DCCM) from the observed uplink channel covariance matrix (UCCM). Hereafter, a complete key generation scheme is proposed to generate keys from the downlink channel covariance matrix. Compared with the existing SKG schemes, this scheme does not require high computational operations and is suitable for low-power terminals. Simulation results show that this scheme can achieve significant performance improvement in terms of the key disagreement ratio.

System model:
Consider the FDD IoT network, where Alice is equipped with $M$ antennas and Bob is a low-power terminal equipped with a single antenna due to the device cost. Alice and Bob wish to agree on secret keys from wireless channels. Meanwhile, there exists a potential passive eavesdropper Eve who is more than several wavelengths away from Bob. Assuming that Eve knows the complete SKG process and tries to eavesdrop, as shown in Figure 1.

We consider a frequency-flat fading channel, where the spatially correlated Rayleigh fading channel [6] between Alice and Bob can be expressed as

$$ h = \int g(\theta) a(\theta) d\theta = \int_{-\Delta/2}^{\Delta/2} g(\theta) a(\theta) d\theta, $$

where $g(\theta) = |g(\theta)|e^{j\phi}$ is complex-valued channel gain whose amplitude and random phase are $|g(\theta)|$ and $\phi$, respectively. Signal power received at Alice is limited within the angle interval $A = [\theta - \Delta/2, \theta + \Delta/2]$, where $\theta$ and $\Delta$ are mean angle of arrival (AoA) and angle spread (AS), respectively. This assumption is reasonable when Alice is located at an elevated position and Bob is surrounded by limited local scatters in realistic outdoor wireless propagation environments [7]. $a(\theta)$ is an array manifold vector for signals arriving from $\theta$. When a uniform linear array (ULA) is deployed, $a(\theta)$ is given as

$$ a(\theta) = \frac{1}{\sqrt{M}} \left[ 1, e^{j2\pi \frac{d}{\lambda} \cos \theta}, \ldots, e^{j2\pi \frac{d}{\lambda} (M-1) \cos \theta} \right]^T, $$

where $\lambda$ and $d$ denote the signal wavelength and antenna spacing, respectively.

It is noted that Bob is only equipped a single antenna, the channel from Alice to Bob is a scalar. To construct a vector of channels at Bob, Alice sends pilots by different antennas in different slots during a coherence time. The specific time slots allocation is shown in Figure 2.

**Statistical channel reciprocity based on channel covariance matrix:** The wireless channel is well modelled as a non-stationary process. In practice, considering an outdoor urban environment, for instance, massive IoT devices are deployed for smart cities and environment monitoring. The statistical information of wireless channels varies over time due to the movement of vehicles and people. That is to say, the covariance matrix varies over time. Therefore, the channel covariance matrix can be used to generate real-time updated secret keys. The channel covariance matrix $R$ can be expressed as

$$ R = \mathbb{E}[hh^H] = \int_{A} \mathbb{E}[|g(\theta)|^2] a(\theta) a^T(\theta) d\theta = \int_{-\Delta/2}^{\Delta/2} p(\theta) a(\theta) a^T(\theta) d\theta, $$

**Fig. 1 Secret key generation system in FDD**

**Fig. 2 The specific time slots allocation of channel estimation**
where $p(\theta) = \mathbb{E}[|g(\theta)|^2]$ denotes the angular power spectrum (APS) characterizing the channel power distribution per unit angle. Since the downlink and uplink channel share the same propagation environment, the angle of departure (AoD) in the downlink channel is the same as the AoA in the uplink channel, i.e., $A_\alpha = A_\lambda$. Moreover, the reciprocity of the electromagnetic propagation ensures that uplink and downlink ray power densities are approximately the same [8], i.e., $p_\alpha(\theta) = \alpha p_\lambda(\theta)$, where $\alpha$ is a frequency-dependent scalar. Hence, channel covariance matrix based statistical channel reciprocity is available for FDD systems. The UCCM $\mathbf{R}_e$ and DCCM $\mathbf{R}_d$ can be represented as

$$
\mathbf{R}_e = \int_{\theta = -\Delta/2}^{\theta = +\Delta/2} p_e(\theta) \mathbf{a}_u(\theta) \mathbf{a}_u^H(\theta) d\theta,
$$

(4)

where $\mathbf{a}_u(\theta)$ is the $u$th element of the $m$th column can be calculated by the average variance changes much more slowly than the coherence time, the channel covariance matrix is a constant over a certain window of time, which is called the coherent time of channel covariance in this letter. Therefore, Alice and Bob can measure the channel covariance through the numerical averaging during a coherent time of channel covariance. For $N$ channel estimations during a coherent time of channel covariance, the channel covariance matrix can be computed through the numerical averaging method as

$$
\hat{\mathbf{R}}_{m} = \frac{1}{N} \sum_{n=1}^{N} \mathbf{h}_m[n] \mathbf{h}_m[n]^H.
$$

(11)

Since only a limited number samples are available, the calculated $\hat{\mathbf{R}}_{m}$ may be a non-Toeplitz matrix. We can artificially generate a Toeplitz matrix, whose $m$th element of the first column can be calculated by the average value of $m$th diagonal elements of $\hat{\mathbf{R}}_{m}$, there is

$$
\hat{\mathbf{R}}(m, 1) = \frac{1}{M - m + 1} \sum_{i=1}^{M-m+1} \hat{\mathbf{R}}(m + i - 1, 1).
$$

(12)

Then Alice estimates the mean angle $\hat{\theta}$ and AS $\hat{\theta}$ using the fast iterative shrinkage-thresholding algorithm (FISTA) to compute the transformation matrix $\mathbf{F}$. As a result, Alice can infer $\mathbf{R}_d$ from the observed $\hat{\mathbf{R}}_d$ with the aid of $\mathbf{F}$. Notably, we adopt the truncated Fourier representation to approximate $p(\theta)$, thus it is crucial for the selection of $\Delta$. It is

\begin{align}
\mathbf{R}_e &= \int_{\theta = -\Delta/2}^{\theta = +\Delta/2} p_e(\theta) \mathbf{a}_u(\theta) \mathbf{a}_u^H(\theta) d\theta, \\
\mathbf{R}_d &= \int_{\theta = -\Delta/2}^{\theta = +\Delta/2} p_d(\theta) \mathbf{a}_u(\theta) \mathbf{a}_u^H(\theta) d\theta.
\end{align}

(5)

Since the distribution of $p(\theta)$ is unknown, it is difficult to derive the closed-form solution of $\mathbf{R}$ and obtain the transformation relationship between $\mathbf{R}_e$ and $\mathbf{R}_d$. We try to approximate the continuous integral of Equation (4) and (5) via truncated Fourier series. Here we replace $p(\theta)$ by a $\Delta$-periodic function $p'(\theta)$ with $p(\theta)$ as the base function. The Fourier series $c(k)$ of $p'(\theta)$ is denoted by

$$
c(k) = \frac{1}{\Delta} \int_{\theta = -\Delta/2}^{\theta = +\Delta/2} p'(\theta) e^{-j2\pi k \theta / \Delta} d\theta.
$$

(6)

We take the main $K$th harmonic component to approximate $p'(\theta)$, then there is $p'(\theta) \approx \sum_{k=-K}^{K} c(k) e^{j2\pi k \theta / \Delta}$. As a result, the continuous PAS function can be approximated by discrete expansion coefficients. Further, $\mathbf{R}_e$ and $\mathbf{R}_d$ can be approximated as

$$
\mathbf{R}_e \approx \sum_{k=-K}^{K} c(k) \mathbf{S}_m(k),
$$

(7)

$$
\mathbf{R}_d \approx \sum_{k=-K}^{K} c(k) \mathbf{S}_n(k),
$$

(8)

where $\mathbf{S}_m(k)$ and $\mathbf{S}_n(k)$ are written as

$$
\mathbf{S}_m(k) = \int_{\theta = -\Delta/2}^{\theta = +\Delta/2} \mathbf{a}_m(\theta) \mathbf{a}_m^H(\theta) e^{-j2\pi k \theta / \Delta} d\theta,
$$

(9)

$$
\mathbf{S}_n(k) = \int_{\theta = -\Delta/2}^{\theta = +\Delta/2} \mathbf{a}_n(\theta) \mathbf{a}_n^H(\theta) e^{-j2\pi k \theta / \Delta} d\theta,
$$

(10)

respectively. Let $m$ and $n$ be the $m$th and $n$th elements of the ULA, respectively, $(m,n)$th element of $\mathbf{S}(k)$ is given as

$$
\mathbf{S}_{m,n}(k) = \int_{\theta = -\Delta/2}^{\theta = +\Delta/2} \mathbf{a}_m(\theta) \mathbf{a}_n^H(\theta) e^{-j2\pi k \theta / \Delta} d\theta.
$$

(11)

Since $\Delta$ is usually small in realistic outdoor wireless propagation environments, we can approximate the integral of Equation (11) using the Taylor expansion of $\cos(\theta)$, where $\cos \theta \approx \cos \hat{\theta} - (\theta - \hat{\theta}) \sin \hat{\theta}$. Hereafter, $\mathbf{S}_{m,n}(k)$ is computed as

$$
\mathbf{S}_{m,n}(k) = \begin{cases} 
\Delta, & k = 0, m = n, \\
\frac{\sin(k \hat{\theta})}{k \hat{\theta}} \sin\left(\frac{k \Delta}{2}\right) \left(1 + \frac{\Delta}{2} \sin\left(\frac{k \Delta}{2}\right) \sin\left(\frac{k \Delta}{2} \sin\left(\frac{k \Delta}{2} \cdots \sin\left(\frac{k \Delta}{2} \cos\hat{\theta}\right) \right) \right), & \text{others},
\end{cases}
$$

(12)

where $\Delta = 2\pi / (m - n)$. For the ULA with antennas placed at equal intervals, the channel covariance matrix is a positive semi-definite Hermitian Toeplitz [9]. Therefore, $\mathbf{R}$ can be completely represented by the first column. Assuming that $\mathbf{r} = \mathbf{R}(:, 1)$, $\mathbf{S} = [\mathbf{S}^k(\cdot, 1), \mathbf{S}^{k+1}(\cdot, 1), \ldots, \mathbf{S}^{K}(\cdot, 1)]$ and $\mathbf{e} = [c(\hat{\theta}), c(-\hat{\theta} + K + 1), \ldots, c(K + 1)]^T$, where $\mathbf{e}(\cdot)$ denotes the vector formed by all the elements in the first column of the $m \times m$ matrix $\mathbf{X}$, it can be easily derived that $\mathbf{r}_s = \mathbf{S} \mathbf{e}$ and $\mathbf{r}_d = \alpha \mathbf{S} \mathbf{e}$. Therefore, the transformation matrix $\mathbf{F}$ between $\mathbf{R}_e$ and $\mathbf{R}_d$ can be calculated by $\mathbf{F} = \alpha \mathbf{S}(\mathbf{S}^T)^{-1}$. As a result, based on the statistical channel reciprocity, Alice can infer downlink channel covariance matrix $\mathbf{R}_d$ from the observed uplink channel covariance matrix $\mathbf{R}_e$ with the aid of the transformation matrix $\mathbf{F}$. Channel covariance matrix based secret key generation scheme: Our proposed channel covariance matrix based secret key generation scheme for low-power terminals in FDD systems mainly consists of two steps: Channel covariance matrix estimation and Key generation from the channel covariance matrix, as shown in Figure 3.

Fig. 3 Channel covariance matrix based secret key generation scheme

1. Channel covariance matrix estimation: Alice and Bob send public pilots to estimate the channel response $\hat{\mathbf{h}} \in \mathbb{C}^M$. Since the channel covariance changes much more slowly than the coherence time, the channel covariance matrix is a constant over a certain window of time, which is called the coherent time of channel covariance in this letter. Therefore, Alice and Bob can measure the channel covariance through the numerical averaging during a coherent time of channel covariance. For $N$ channel estimations during a coherent time of channel covariance, the channel covariance matrix can be computed through the numerical averaging method as

$$
\hat{\mathbf{R}} = \frac{1}{N} \sum_{n=1}^{N} \mathbf{h}_m[n] \mathbf{h}_m[n]^H.
$$

(13)

Since only a limited number samples are available, the calculated $\hat{\mathbf{R}}$ may be a non-Toeplitz matrix. We can artificially generate a Toeplitz matrix, whose $m$th element of the first column can be calculated by the average value of $m$th diagonal elements of $\hat{\mathbf{R}}$, there is

$$
\hat{\mathbf{R}}(m, 1) = \frac{1}{M - m + 1} \sum_{i=1}^{M-m+1} \hat{\mathbf{R}}(m + i - 1, 1).
$$

(14)
Table 1. Simulation parameters

| Parameter                        | Value                      |
|----------------------------------|----------------------------|
| Channel model                    | Spatially correlated       |
| Rayleigh fading channel          |                            |
| Duplex method                    | FDD                        |
| Uplink carrier frequency         | 2 GHz                      |
| Downlink carrier frequency       | 1.9 GHz                    |
| Antenna configuration of Alice   | ULA, separated with half wavelength |
| Antenna configuration of Bob     | Single antenna             |
| Monte Carlo times                | $10^4$                     |

Fig. 4 KDR comparisons versus SNR with different AS.

Table 2. NIST statistical test results

| Test                   | P          |
|------------------------|------------|
| Frequency              | 0.437274   |
| Block Frequency        | 0.275709   |
| Cumulative Sums        | 0.834308   |
| Runs                   | 0.350485   |
| Longest Run of ONES    | 0.534146   |
| FFT                    | 0.162606   |
| Approximate Entropy    | 0.834308   |
| Serial                 | 0.213309   |

Hermitian Toeplitz matrix which is confined to $(2M - 1)$-dimensional real linear spaces and the symmetries of $c(k)$, we choose $K = M - 1$ in this scheme to reduce the computational complexity.

(2) Key generation from the channel covariance matrix: Considering that the channel covariance matrix has a certain auto-correlation due to closely spaced antennas array, the quantized keys will have serious redundancy if we extract secret keys directly from the channel covariance matrix. Eve can easily crack the ciphertext encrypted using non-random keys via dictionary attack. Therefore, we extract eigenvalues of the channel covariance matrix to generate uncorrelated secret keys. Specifically, the channel covariance matrix $\tilde{R}_d$ and $\tilde{R}_e$ are decomposed as

$$\tilde{R}_d = U_dA_dU_d^H,$$  \hspace{1cm} (15)

$$\tilde{R}_e = U_eA_eU_e^H,$$ \hspace{1cm} (16)

where $U$ is the eigenvector matrices of size $M \times M$, and $A$ is the eigenvalue matrices of size $M_i \times M_i$, here $M_i \triangleq \text{rank}(R)$. For $T_e$ times of sampling at the different coherent time of channel covariance, Alice and Bob can obtain a set of symmetric eigenvalues $Q^e = \{A_{11}^e, \ldots, A_{n1}^e\}$ and $Q^d = \{A_{12}^d, \ldots, A_{n2}^d\}$, which are quantized via uniform quantization algorithm [1]. It is worth noting that although there is a frequency-dependent scalar $\alpha$ between the eigenvalues of the UCCM and DCCM, its effect will be eliminated by the quantization because $\alpha$ is a constant and does not affect the shape of the eigenvalue matrix. Then, we use error correction code-based information reconciliation scheme [1] to correct mismatch bits. Finally, SHA-256 universal hash function is used for privacy amplification to eliminate leaked information.

Simulation results: In this section, we verify the performance of the proposed SKG scheme through Monte Carlo simulation. Alice is equipped ULA with eight antennas whose antenna spacing is separated with half wavelength. Bob is equipped with a single antenna. The uplink and the downlink carrier frequency are 2 and 1.9 GHz, respectively. The channel responses based on the spatially correlated Rayleigh fading channel model are randomly generated according to Equation (1), where the main angle $\theta$ is assumed to be uniformly distributed over an interval $[\pi / 6, \pi / 3]$. We set $N = 100$ to compute channel covariance matrix through numerical averaging method. Simulation parameters are listed in Table 1.

Figure 4 plots key disagreement ratio (KDR) against signal to noise ratio (SNR) with different schemes. It is noted that the complexity of path extraction algorithms and special restrictions on the antenna configuration in [2, 3] was not suitable for the low-power terminals. Therefore, we only compare with the method proposed in [4]. It is obviously that KDR of the channel covariance matrix-based SKG scheme is much lower than that in [4]. The reason lies in that our scheme takes advantage of the statistical channel reciprocity, where Alice can accurately infer the DCCM from the observed UCCM. However, the algorithm proposed in [4] introduces more noise due to two rounds of channel sounding. We also compare the performance of KDR at different AS $\Delta$. It can be seen that KDR increases as $\Delta$ increases. There are two main reasons for the performance loss. First, the FISTA algorithm relies on the approximative representation of channel in the angular domain. It provides a worse estimation accuracy when $\Delta$ becomes wider. More importantly, the channel covariance matrix which is approximated by Taylor expansion is no longer accurate when $\Delta$ is large. Note that the KDR between Eve and Bob always remains at 0.5 with the increase of the SNR, indicating that Eve cannot steal useful information from shared keys regardless of the signal strength. This is because the eavesdropping channel is independent of the legitimate channel so that the channel covariance matrix of Eve is not correlated with that of Bob.

To verify the secret key randomness, a National Institute of Standards and Technology (NIST) randomness test is performed on quantized sequences. Considering that some tests require extremely long sequences, we only run eight typical tests out of 16 different test. For each subtest, if the test result is not less than 0.01, i.e. $P \geq 0.01$, it can be considered as random. Table 2 shows that the key bits generated from channel covariance matrix eigenvectors pass the NIST tests, indicating that this scheme can generate secret keys with strong randomness.

Conclusion: In this paper, we propose a secret key generation scheme based on the channel covariance matrix in FDD systems. With the aid of the transformation matrix, the downlink channel covariance matrix can be inferred from the observed uplink channel covariance matrix. The proposed algorithm greatly relaxes the requirement on the angle estimation and antenna configuration, which is suitable for low-power terminals. Simulation results show that our proposed SKG scheme can generate high-agreement uncorrelated secret keys, which can satisfy the security requirements of FDD communication systems. Furthermore, due to the slow variability of the channel covariance matrix, the secret key generation rate will be limited. Therefore, it is worthwhile to improve the key generation rate for FDD systems in the future.

Acknowledgment: This work has been supported by National Natural Science Foundation of China (Nos.61801435, 61871404, 61701538).
References

1. Zhang, J., et al.: Key Generation from Wireless Channels: A Review. IEEE Access 4, 614–626 (2016)
2. Wang, W., et al.: A Wireless Secret Key Generation Method Based on Chinese Remainder Theorem in Fdd Systems. Sci. China Inf. Sci. 55(7), 1605–1616 (2012)
3. Liu, B., Hu, A., Li, G.: Secret Key Generation Scheme Based on the Channel Covariance Matrix Eigenvalues in Fdd Systems. IEEE Commun. Lett. 23(9), 1493–1496 (2019)
4. Wu, X., et al.: A Secret Key Generation Method Based on Csi in Ofdm-Fdd System. 2013 IEEE Globecom Workshops (GC Wkshps), pp. 1297–1302.IEEE, Piscataway, NJ (2013)
5. Peng, L., et al.: An Investigation of Using Loop-Back Mechanism for Channel Reciprocity Enhancement in Secret Key Generation. IEEE Trans. Mob. Comput. 18(3), 507–519 (2019)
6. You, L., et al.: Pilot Reuse for Massive Mimo Transmission over Spatially Correlated Rayleigh Fading Channels. IEEE Trans. Wirel. Commun. 14(6), 3352–3366 (2015)
7. Fang, J., et al.: Low-Rank Covariance-Assisted Downlink Training and Channel Estimation for Fdd Massive Mimo Systems. IEEE Trans. Wirel. Commun. 16(3), 1935–1947 (2017)
8. Xu, G., Liu, H.: An Effective Transmission Beamforming Scheme for Frequency-Division-Duplex Digital Wireless Communication Systems. 1995 International Conference on Acoustics, Speech, and Signal Processing, pp. 1729–1732.IEEE, Piscataway, NJ (1995)
9. Miretti, L., Cavalcante, R.L.G., Stanczak, S.: Fdd Massive Mimo Channel Spatial Covariance Conversion Using Projection Methods. 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 3609–3613.IEEE, Piscataway, NJ (2018)