IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) | 978-1-6654-0443-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/INFOCOMWKSHPS51825.2021.9484457

Secret Key Generation Scheme Based on Generative Adversarial Networks in FDD Systems

Zongyue Hou
School of Cyber Science and Engineering
Southeast University
Nanjing, China
zyhou@seu.edu.cn

Xinwei Zhang
School of Cyber Science and Engineering
Southeast University
Nanjing, China
zxw1998@seu.edu.cn

***Abstract*—In frequency division duplexing (FDD) systems, the uplink and downlink transmit information in different frequency bands, so it is difficult to use channel reciprocity to generate secret keys. Existing key generation methods for FDD systems have excessive overhead and security problems. This paper uses deep learning to predict the downlink channel state information (CSI) from the uplink CSI, so that two users can generate highly similar downlink CSI in FDD systems. We propose a key generation scheme based on boundary equilibrium generative adversarial network (BEGAN), including channel estimation, reciprocal channel feature construction, quantization, information reconciliation and privacy amplification. Numerical simulation results are presented to verify the feasibility and effectiveness of the proposed scheme.**

***Index Terms*—Deep learning, boundary equilibrium generative adversarial network, key generation, frequency division duplexing**

I. Introduction

With its mobility and flexibility, wireless networks play an irreplaceable role in all walks of life. Due to the openness of the wireless network, communication is carried out through broadcasting without clear boundaries, making the content transmitted more easily eavesdropped. Traditional security mechanisms require a fixed key management center (KMC) to provide keys for both parties in communication. However, due to the openness of wireless networks, it is difficult to distribute and manage keys through a fixed KMC. In order to mitigate these issues, researchers have proposed a wireless physical layer key generation technology, which uses channel reciprocity to generate keys.

In time division duplexing (TDD) systems, both the uplink and downlink are in the same carrier frequency band. The channel state information (CSI) obtained by Alice and Bob are reciprocal, so we can generate a shared key based on the reciprocity of the channel. However, the uplink (UL) and the downlink (DL) channels are in different frequency bands in frequency division duplexing (FDD) systems, the UL-DL reciprocity no longer exists in terms of the received signal strength, channel gain. Secret key is difficult to generate in FDD systems. There have been several key generation methods developed for FDD systems. In [2], a key generation method based on the Chinese remainder theorem was proposed by utilizing the reciprocity of multipath angle and delay to extract secret key. In fact, [3] constructs reciprocal channel characteristics for key generation in FDD systems. In addition to directly constructing the reciprocal channel parameters, there is also a method of using the channel training stage to establish a combined channel with reciprocal channel gain to generate key [4]. However, these methods exist many limitations, overhead and security problems. Therefore, it is necessary to design a new key generation scheme for FDD systems.

Recently, many scholars have studied downlink channel prediction based on deep learning in FDD systems, and proposed the use of neural networks to predict the downlink CSI from the uplink CSI [5]. Compared with traditional methods, the downlink CSI prediction based on deep learning does not require complex calculations [7]. In [6], it is proposed to use boundary equilibrium generative adversarial networks (BEGANs) to predict downlink CSI from the uplink CSI in an FDD system and treat the CSI matrix as an image. Inspired by these methods, we use the recently popular boundary equilibrium generative adversarial networks (BEGANs) to predict the downlink CSI from the uplink CSI [15]. In this way, two users can obtain highly similar downlink CSI for FDD systems.

In this paper, we predict downlink CSI from uplink CSI by deep learning to construct reciprocal channel features. Based on this method, a key generation scheme is proposed. Our contributions are summarized as follows.

- We use deep learning technology to construct reciprocal channel features, and verify the performance in the simulation. In addition, we artificially add noise to improve the regularization of the network.
- We use information reconciliation based on helper data and propose a complete and detailed key generation scheme.
- Experiment results demonstrate that our proposed scheme outperforms the loopback scheme of [16] in terms of key disagreement ratio.

The rest of the paper is organized as follows. Section II defines the system models for FDD systems, and Section III describes how to use BEGAN to construct reciprocal channel features. Section IV gives the key generation scheme, and

978-1-6654-0443-3/21/$31.00 ©2021 IEEE

Section V performs simulation and verifies the proposed key generation scheme. Section VI concludes the paper.

II. System Model

The key generation involves two legitimate users, namely Alice (base-station) and Bob (user element), and an eavesdropper Eve. We consider an FDD system in which Alice is equipped with M antennas in the form of uniform linear array (ULA) and Bob is equipped with a single antenna. Let h_m denote the channel from user to antenna m at the frequency f. Alice and Bob transmit signals on different carrier frequencies f_2 and f_1 at the same time. The multipath channel model can be expressed as

$$h_m(f,\tau) = \sum_{l=1}^{L} a_l e^{-j2\pi f \tau_l + j\varphi_l} \delta(\tau - \tau_l). \quad (1)$$

Equation (1) is assumed that there are L distinct paths in the environment. a_l is the path gain, which depends on (i) the frequency f, (ii) the distance from Alice to Bob, (iii) the antenna gain. The phase φ_l also depends on the material of the scatterer and the wave incident angle at the scatterer. τ_l is a frequency-independent time delay. In the wideband channel, the coefficient of the n^{th} sub-carrier in an orthogonal frequency-division multiplexing (OFDM) system can be expressed as

$$H_m(f,n) = \sum_{l=1}^{L} a_l e^{-j2\pi f \tau_l + j\varphi_l} e^{-j2\pi \tau_l n/N}, \quad (2)$$

where f_n is the frequency of the n^{th} subcarrier relative to the center frequency f, N is the total number of subcarriers. We define the $M \times N$ channel vector $\mathbf{H}(f) = [\mathbf{H}_1(f), ..., \mathbf{H}_M(f)]$, where $\mathbf{H}_m(f) = [H_m(f,0), ..., H_m(f,N-1)]$. Finally, we define $\mathbf{H}_1 = \mathbf{H}(f_1)$ and $\mathbf{H}_2 = \mathbf{H}(f_2)$.

We designed a key generation scheme based on BEGAN, as shown in Fig. 1. In training stage, Alice trains BEGAN to construct reciprocal channel features, which will be described in detail in Section III. The dataset used for training can be obtained by Alice collecting the CSI obtained by the CSI feedback from Bob [8]. The trained BEGAN model will be used for key generation. In key generation stage, Alice and Bob use channel estimation to obtain $\mathbf{H}_1$ and $\mathbf{H}_2$. Then, Alice and Bob normalize $\mathbf{H}_1$ and $\mathbf{H}_2$ to a number between (0, 1) and obtain channel features $\mathbf{x}_1$ and $\mathbf{x}_2$. Alice will use BEGAN to get $\hat{\mathbf{x}}_2$ from $\mathbf{x}_1$, which enables Alice and Bob to obtain highly correlated channel characteristics $\hat{\mathbf{x}}_2$ and $\mathbf{x}_2$, respectively. They will finally perform quantization, information reconciliation, and privacy amplification to generate the same key. The key generation scheme will be described detailedly in Section IV.

III. BEGAN-Based Reciprocal Channel Features Construction

In order to construct reciprocal channel features for FDD systems to generate a key, we need to transform the CSI matrix into an image. In this section, we first introduced how to turn the CSI matrix into an image, and then introduced the structure of BEGAN.

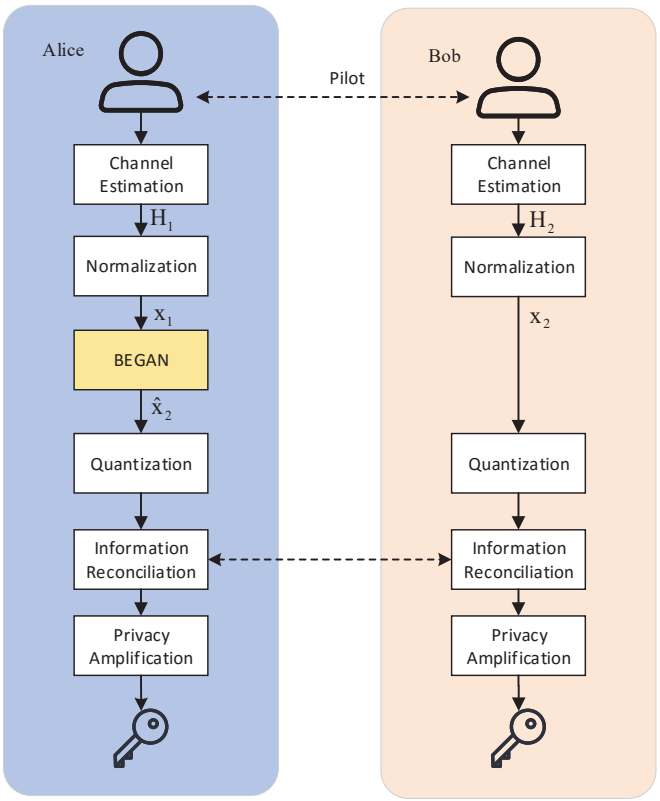

Fig. 1. The Key Generation scheme for FDD systems.

A. CSI as an image

We combine the uplink CSI and the downlink CSI into an image. The size of an image is $2N \times M \times 2$. The first N carriers are the uplink CSI, and the last N carriers are the downlink CSI. In order not to lose the phase information, we set up two channels, using real values in the first channel and imaginary values in the second channel. For example, as shown in Fig. 2, this is a image of first channel. Columns of this image represent $N = 36$ subcarriers. Rows of this image represent $M = 8$ antennas.

B. BEGAN Architecture

After treating the channel matrix as an image, BEGAN can be used to enable Alice and Bob to obtain highly similar downlink CSI. BEGAN consists of two networks: the generator and the discriminator, which are trained at the same time.

Generator is a decoder that has 7 two-dimensional convolutional layers, 2 upsampling layers and a fully connected layer. The purpose of generator is to make it able to fool the discriminator, so as the training progresses, it can gradually generate more and more realistic CSI images. The discriminator is an auto-encoder. The encoder has 7 two-dimensional convolutional layers, 2 subsampling layers and

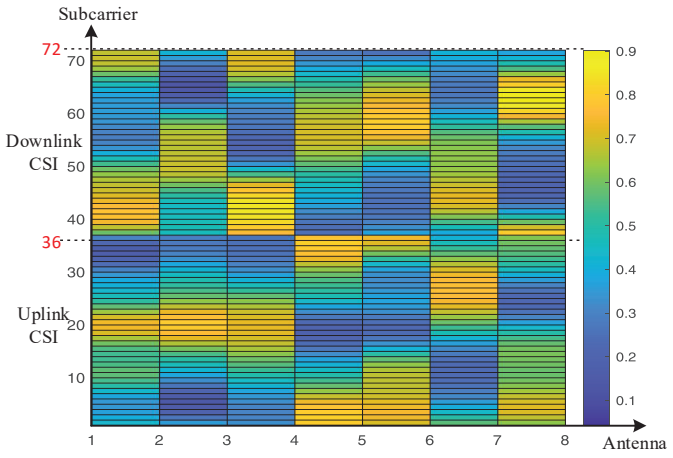

Fig. 2. The CSI image of first channel.

a fully connected layer and same structure is used between the generator and the decoder part of the discriminator in our paper. Discriminator tries to distinguish the generated images from the real images.

C. Training and Prediction

The structure of BEGAN as shown in Fig. 3. In this paper, the steps of constructing reciprocal channel features can be summarized as:

- Training stage: First, we use the complete CSI image (input of the discriminator) to train BEGAN. The generator network can take random vectors z as input and create images after training. By reducing the loss function in the training stage, these images are more and more similar to real CSI images.
- Prediction stage: At this stage, we want to predict the downlink CSI from the uplink CSI to obtain reciprocal channel characteristics. In Fig. 3, the real image is a broken picture with only uplink CSI. Then, we use gradient descent to update z (input of the generator) so that the top half of the generated image becomes more similar to the broken image. After multiple iterations, the lower half of the generated image is the predicted downlink CSI.

After the prediction phase is over, Alice and Bob can obtain similar downlink CSI. Based on this method, we construct reciprocal channel features. As for loss function, we first define $G(z)$ is the generated image and x is the real image. $\hat{x}$ and $\hat{G}(z)$ are the output of discriminator. $L(x)$ and $L(G(z))$ are the reconstruction loss of the auto-encoder when inputting the real image and the generated image, respectively. $L(x)$ can be written as follow:

$$L(x) = \frac{1}{V}\sum_{v=0}^{V-1} ||\hat{x}^{(v)} - x^{(v)}||_2^2, \tag{3}$$

Where $||\cdot||_2$ denotes the L_2 norm, V is the batch size, and the superscript (v) denotes the index of the v-th training sample. The generator loss $L(G(z))$ is given as:

$$L(G(z)) = \frac{1}{V}\sum_{v=0}^{V-1} ||\hat{G}(z)^{(v)} - G(z)^{v}||_2^2, \tag{4}$$

The training stage is trained by minimizing the following loss function.

$$\begin{aligned} L_D &= L(x) - k_t L(G(z)) \\ L_G &= L(G(z)) \\ k_{t+1} &= k_t + \lambda_k(\gamma L(x) - L(G(z))), \end{aligned} \tag{5}$$

Where λ_k is the learning rate, L_G denote the generator loss, L_D is the difference between the reconstruction loss of real images and the reconstruction loss of generated images. It is adjusted by introducing parameter k, which is updated by the last equation in (5). If we define the mask as

$$\text{mask}[i,j] = \begin{cases} 1, & 1 \le i \le N \\ 0, & N < i \le 2N \end{cases} \tag{6}$$

Where i represents the carrier and j represents the antenna. Then the prediction stage is trained by minimizing the following loss function [15].

$$\begin{aligned} \text{contextual loss} &= ||\text{mask} \odot x - \text{mask} \odot G(z)||_2 \\ \text{total loss} &= \text{contextual loss} + \lambda \times L(G(z)) \end{aligned} \tag{7}$$

Where λ is a hyper parameter. Its default value in BEGAN is 0.01. $\odot$ is an element-wise multiplication operator.

We use the Adam method to optimize the parameters. This network has many benefits for our problem. First of all, the discriminator is an auto-encoder, which can learn an efficient representation of the input data through unsupervised learning. In addition, adding noise in training stage can improve the regularization of the network. Second, the input of the generator in GANs is a random vector z, and different z may have different results. But in our network structure, we have constructed a prediction stage, so inputting different z can get the same result.

IV. The BEGAN-Based Key Generation Scheme

In Section III, we propose to use BEGAN to construct reciprocal channel features. In this section, quantization, information reconciliation, and privacy amplification as described in the following subsection.

A. Quantization

Alice and Bob can obtain highly similar $N \times M$ downlink CSI after channel prediction, and then both parties perform quantization. Quantization is a method of converting the measurements into secret key. We use the single threshold method to convert CSI into binary bits and choose the mean value of the CSI as the threshold. The CSI larger than the threshold value will be quantified into bit "1", and the CSI below the threshold value will be quantified to bit "0".

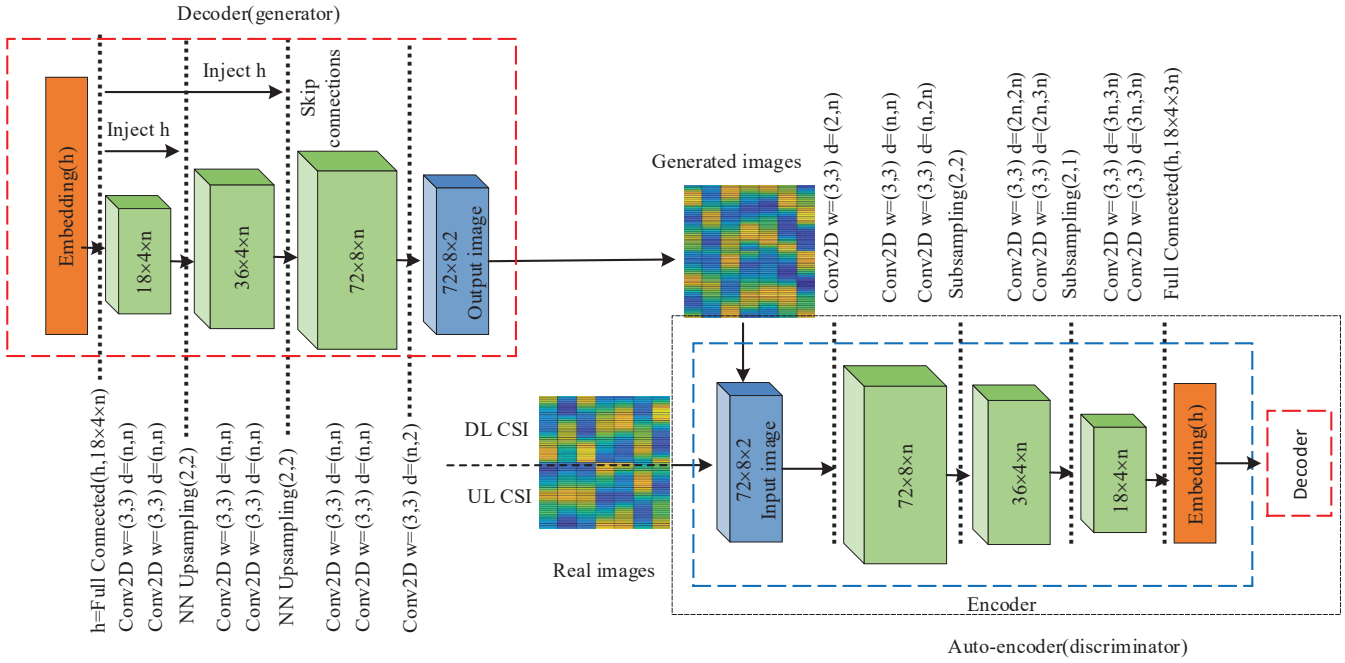

Fig. 3. The network structure of BEGAN(n: a hyperparameter for hidden layers, which we set to n = 64). The discriminator consists of encoder and decoder

B. Information Reconciliation

After the data is quantized, the corresponding bits are slightly different. We need information reconciliation. The information reconciliation enables the sender and the receiver to obtain exactly the same key by exchanging information through the open channel between the two communicating parties. In this process, it is also necessary to ensure that no eavesdropper can obtain information about keys. There are many information reconciliation methods, such as the use of error correction codes to improve the information reconciliation rate. In this paper, we use a helper data based information reconciliation method [10]– [11]. At Bob, Bob calculates helper data according to $\mathbf{x}_2$. Helper data can be given as:

$$w = \begin{cases} (x(i) - x_m)/(x_{max} - x_m), & x(i) > x_m \\ (x(i) - x_m)/(x_m - x_{min}), & x(i) \leq x_m \end{cases} \quad (8)$$

Where $x(i)$ is $x_2(i)_{i=1}^{L}$ or $\hat{x}_2(i)_{i=1}^{L}$, L is the length of helper data, and x_m is the median of $\mathbf{x}_2$. Then the helper data w, x_m, x_{max}, and x_{min} is transmitted to the Alice through the common channel. Next, at Alice, Alice uses $\hat{\mathbf{x}}_2$, x_m, x_{max}, and x_{min} to calculate helper data w_p. Index where w and w_p are not approximately equal are recorded in Loc, which is then sent to Bob to generate secret keys. Finally, Bob deletes the corresponding data to generate keys according to the received index information Loc. The concrete steps of the information reconciliation algorithm are given in the Algorithm 1.

Algorithm 1 Information reconciliation algorithm

Input: Length of helper data: $L = M \times N$, Downlink CSI: $x_2(i)_{i=1}^{L}$, Median of $\mathbf{x}_2$: x_m, Maximum value of $\mathbf{x}_2$: x_{max}, Minimum value of $\mathbf{x}_2$: x_{min}, Predicted downlink CSI: $\hat{x}_2(i)_{i=1}^{L}$

Output: Helper data: w, w_p, The index of the data point that does not meet the requirements: Loc

At Bob
for $i < L$ **do**
  Compute helper data using (8)
  $i = i + 1$
end for
return w
Bob transmit helper data w and x_m, x_{max}, x_{min} to Alice
At Alice
Use $\hat{\mathbf{x}}_2$ to calculate helper data w_p
if $w_p - w < 0.001$ **then**
  Generate secret keys
else
  Discard it and store the index of it in Loc
end if
return Loc
Alice transmit Loc to Bob
At Bob
Delete the value with index Loc to generate secret keys

C. Privacy Amplification

In addition, privacy amplification is also required. The purpose of it is to prevent data transmitted in public channels from being stolen by eavesdroppers. Privacy amplification is achieved by using the hash function.

TABLE I
THE ADOPTED DEEPMIMO DATASET PARAMETERS

Parameter	Value
Frequency	2.4GHz and 2.5GHz
Number of BSs	1
Active users	40000
Number of BS antennas	8
System BW	0.5GHz
Number of selected sub-carriers	36
Number of paths	5

V. Implementation and Simulation Results

In the following, we discuss the details of the implementation and the simulation results.

A. Simulation Setup

In the simulations, we consider the indoor scenario 'I1' that is offered by the DeepMIMO dataset [12] and is generated based on the accurate 3D ray-tracing simulator Wireless Insite [13]. The frequency of the uplink channel is 2.4GHz, and the frequency of the downlink channel is 2.5GHz.

As depicted in Fig. 4, the "I1" scene includes a 10m$\times$10m room with two tables in it and 8 antennas tiling up part of the ceiling. The users are distributed in two different x-y grids, and each user location is on the floor [14]. In this 3D ray-tracing situation, we generate the DeepMIMO dataset based on the parameters in Table I. There are a total of 64 carriers in the scene. We choose the first 36 carriers. In order to form training and testing datasets, we shuffle the elements of the generated DeepMIMO datasets. The number of training samples that were created independently was 40,000 (35,000 for training, 2,000 for validation and 3,000 for test).

We initialize the random vector z to a uniform distribution between 0 and 1. The initial learning rate is 0.0001. TensorFlow 2.1.0 is employed as the deep learning framework. The parameters of the BEGAN are initialized as random vector z. The batch size is 32, and the number of epochs is 20. To avoid mode collapse, a shared weight is used between the generator and the decoder part of the discriminator in our paper.

B. Simulation Results

We first simulated the data without adding noise, and got good performance in the generation stage. However, we could not get the correct downlink CSI in the prediction stage. The variance of the CSI generated by the generator was too small to restore the correct CSI. We added Gaussian noise with a mean of 0 and a variance of 0.2 to improve its regularization.

At the same time, we added Gaussian noise with different SNR to study the ability of the BEGAN to cope with different noises. As for the comparison metric, we have used normalized mean squared error (NMSE), which is defined as:

$$NMSE = E\left[\frac{||\mathbf{x}_2 - \hat{\mathbf{x}}_2||_2^2}{||\mathbf{x}_2||_2^2}\right], \tag{9}$$

where $E[\cdot]$ represents the expectation operation.

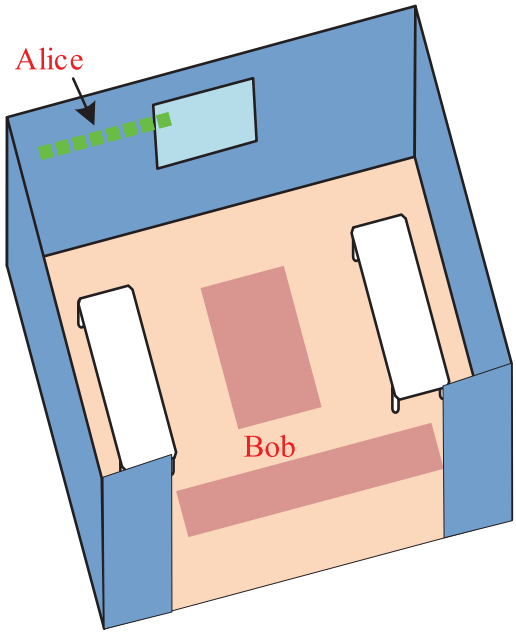

Fig. 4. An approximate depiction of the considered environment (scenario). The green little boxes on the ceiling represent the distributed antennas of the base station. The two red brown rectangles are two grids representing possible user locations. This ray-tracing scenario is constructed using the Wireless InSite by Remcom [13].

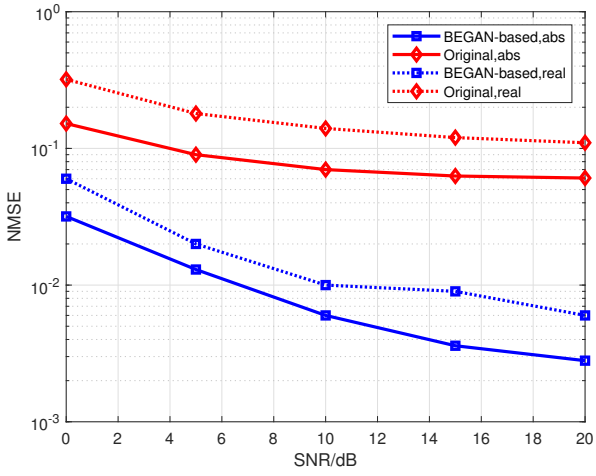

Fig. 5. NMSE performance of BEGAN with different SNR.

The results of prediction are shown in Fig. 5, as the SNR increases, the NMSE of the network decreased. Fig. 5 also shows that the NMSE of the absolute value is lower than the real value. As for the comparison metric, we have used key disagreement ratio (KDR) and key generation efficiency (KGE). 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. KGE is defined as the number of key bits generated divided by the number of original measurements used to generate keys. The number of original measurement

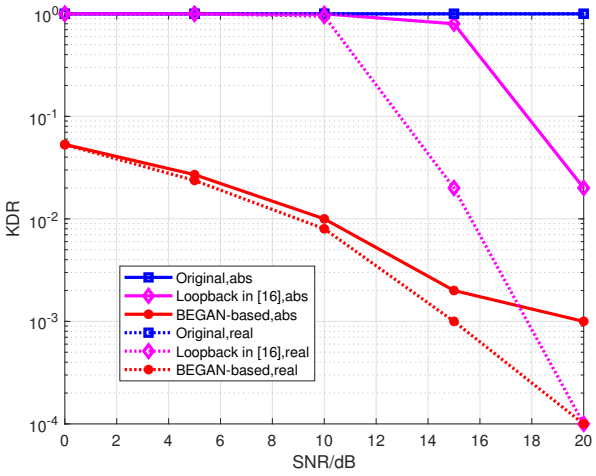

Fig. 6. KDR performance of BEGAN with different SNR.

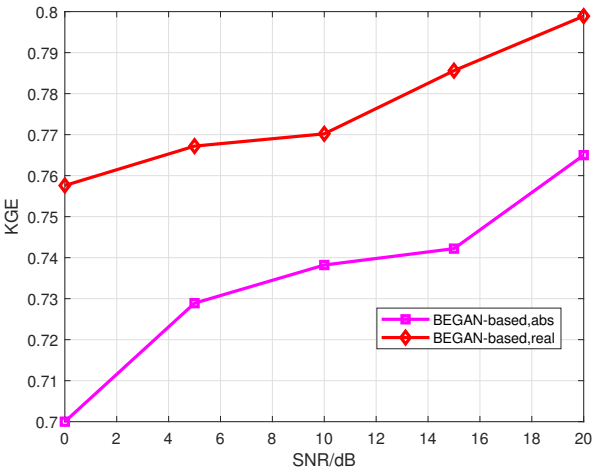

Fig. 7. KGE performance of BEGAN with different SNR.

values required to generate a 128-bit key is different in the information reconciliation algorithm, so it is the average of multiple experiments.

Fig. 6 compares our scheme with the loopback scheme in [16] in terms of the KDR. Compared with the original channel, when the SNR is 10dB, we can improve the performance to 10^{-2} using the channel predicted by BEGAN. Fig. 7 compare the performance of KGE under different SNR. With the continuous improvement of SNR, KGE is also improving.

VI. Conclusion

The reciprocity of short-time channel properties no longer exists between UL and DL in FDD systems. In this paper, we use BEGAN to predict the downlink CSI from the uplink CSI and propose a new secret key generation method for FDD systems. In addition, a complete and detailed key generation scheme is proposed, including channel estimation, reciprocal channel features construction, quantization, information reconciliation, and privacy amplification. Numerical results demonstrate that our proposed scheme is effective and enable key generation applied in FDD systems.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 61801115, in part by the Zhishan Youth Scholar Program of SEU (3209012002A3). (Corresponding author: Xinwei Zhang)

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, 2016.

[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," *Sci. China Inf. Sci.*, vol. 55, no. 7, pp. 1605–1616, 2012.

[3] G. Li, A. Hu, C. Sun, and J. Zhang, "Constructing reciprocal channel coefficients for secret key generation in FDD systems," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2487–2490, Dec. 2018.

[4] 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 (GC Wkshps)*, Atlanta, GA, USA, Dec. 2014, pp. 1297–1302.

[5] M. Arnold and S., "Enabling FDD Massive MIMO through Deep Learning-based Channel Prediction," *arXiv preprint arXiv:1901. 03664*, 2019.

[6] M. Safari and V., "Deep UL2DL: Channel knowledge transfer from uplink to downlink," *arXiv preprint arXiv:1812.07518*, 2018.

[7] Y. Yang, F. Gao, G. Y. Li, and M. Jian, "Deep learning based downlink channel prediction for FDD massive MIMO system," *IEEE Commun. Lett.*, pp. 1–1, 2019.

[8] C. Wen, W. Shih, and S. Jin, "Deep learning for massive MIMO CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 748–751, Oct. 2018.

[9] T. Wang, C. Wen, S. Jin, and G. Y. Li, "Deep learning-based CSI feedback approach for time-varying massive MIMO channels," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 416–419, Apr. 2019.

[10] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Mar. 2008.

[11] J. de Groot, B. Škori´c, N. de Vreede, and J.-P. Linnartz, "Quantization in zero leakage helper data schemes," *EURASIP J. Adv. Signal Process.*, vol. 2016, p. 54, Dec. 2016.

[12] A. Alkhateeb, "DeepMIMO: A generic deep learning dataset for millimeter wave and massive MIMO applications," in *Proc. Inf. Theory and Applications Workshop (ITA),* San Diego, CA, Feb. 2019, pp. 1–8.

[13] "Remcom wireless insite," https://www.remcom.com/ wireless-insite-em-propagation-software.

[14] M. Alrabeiah and A. Alkhateeb, "Deep learning for TDD and FDD massive MIMO: Mapping channels in space and frequency," *arXiv preprint arXiv:1905.03761,* 2019.

[15] D. Berthelot, T. Schumm, and L. Metz, "BEGAN: boundary equilibrium generative adversarial networks," *arXiv preprint arXiv:1703.10717,* 2017.

[16] S. J. Goldberg, Y. C. Shah, and A. Reznik, "Method and apparatus for performing JRNSO in FDD, TDD and MIMO communications," U.S. Patent, 8 401 196 B2, Mar. 19, 2013.