Beam-Based Secure Physical Layer Key Generation for mmWave Massive MIMO System

Hao Gao, Yanling Huang, and Danpu Liu(✉)

Beijing Laboratory of Advanced Information Networks,
Beijing Key Laboratory of Network System Architecture and Convergence,
Beijing University of Posts and Telecommunications, Beijing
People's Republic of China
dpliu@bupt.edu.cn

Abstract. Massive MIMO system greatly enriches the randomness of the secret keys in the physical layer and increases the rate of key generation. However, it is not practical to obtain full channel state information for key generation in actual communication scenarios due to a large number of additional signaling overhead. In this paper, we proposed a feasible physical layer key generation scheme by using the beam information as a random source. The procedure for key generation is designed based on the current beam management mechanism in 5G NR. Therefore, the secret key is synchronously generated in the process of two-stage beam search between the gNB and the UE before data transmission, and the additional signaling overhead for key generation is little. Furthermore, to cope with the non-uniform distributed characteristics of the beams, we adopt Huffman code in the encoding of the beam index, thereby improving the efficiency of the key generation. Simulation results show that the proposed scheme can achieve mutual information per bit as high as 0.97, which is 2% to 3% better than that of equal length coding. Furthermore, the bit disagreement rate can be less than 1% in a harsh communication environment with a signal-to-noise ratio of −10 dB.

Keywords: Physical layer security · Beam management · MIMO · Secret key generation · Huffman coding

1 Introduction

The Fifth Generation mobile communication (5G) is based on heterogeneous networking and new wireless technologies, providing support for access to massive devices, diverse wireless services, and rapid data traffic growth. Due to the extremely high data transmission rate of 5G mobile communication, people will use it to transmit a large amount of key information, including some private information. If the transmission process is stolen, it is likely to bring hidden dangers to the user security. Therefore, the development of 5G puts forward higher requirements for the performance of wireless communication security such as reliable transmission and privacy protection.

H. Gao et al. (Eds.): ChinaCom 2020, LNICST 352, pp. 37–51, 2021.
https://doi.org/10.1007/978-3-030-67720-6_3

Generating keys based on wireless channel characteristics is a method to ensure information security in the physical layer. During the key generation process, legitimate users can measure dynamic channel parameter information separately, which can effectively avoid the exchange of keys between legitimate users, thereby improving key security. Moreover, the spatial variability and time variability of wireless channels can increase the randomness of secret keys. Owing to low complexity and ease of operation, the key-based physical layer security technology has become a research hotspot for physical layer security.

Many kinds of channel characteristics can be used to generate the secret key, including received signal strength (RSS) [1], channel impulse response (CIR) [2]/ channel state information (CSI) [3], and phases [4]. We note the work in [5], which uses multi-level quantization of MIMO channel measurements to generate secret key bits, as well as [6, 7], which quantize noisy channel measurements at transmitter and receiver to generate secret key bits in conjunction with Slepian-Wolf coding. Other well-known references that study the use of CSI to generate encryption keys are [8–12], which also include information-theoretical analysis of the proposed method.

In recent years, researches on physical layer key generation for large-scale antenna systems have been initially carried out. In [13], for the millimeter-wave(mmWave) Massive MIMO communication system, Long Jiao, Jie Tang et al. proposed to use two new channel characteristics that can reflect the sparsity of the mmWave channel, namely the virtual angle of arrival (AoA) and the angle of departure (AoD) as a random source to generate keys. Besides, the work in [14] proposed a method that uses AoA with a random perturbation angle as a random source for feature extraction. This method has a high key generation rate and key consistency, and to a certain extent can prevent co-eavesdropping. However, the above methods need to work under the condition that the high-dimension full CSI including AoA/AoD is known, and is not compatible with 5G New Radio (NR) protocol where only the equivalent baseband channel with low-dimension is estimated.

In summary, the physical layer secret key generation in the massive MIMO communication system faces the following new challenges due to its unique channel characteristics and the huge number of antennas: 1) The existing key generation algorithms need to obtain full Channel State Information (CSI). High-dimensional channel estimation is challenging as the number of antennas increases. 2) The existing algorithms are not compatible with the two-stage synchronization process in the 5G NR protocol. If designing a key generation mechanism that is independent of the synchronization process, the additional signaling overhead will be introduced.

To address the above issues, we proposed a key generation scheme based on the existing 5G NR protocol framework in this paper. The beam representing the spatial characteristics of the mmWave channel is used to generate secure keys. Choosing the beam instead of AoA/AoD as a random source has the following advantages: 1) The beam information can be obtained by beam sweeping and does not rely on the acquisition of full CSI. 2) The quantized beam index can be directly used as the generated secret keys, thereby avoiding errors caused by the quantization process. Furthermore, the proposed scheme combines the key generation and the two-stage beam search procedure defined in 5G NR protocol, so that the legitimate users simultaneously complete the generation of the physical layer secret key during the existing initial access and beam refinement process, and little extra signaling overhead is required. Finally, considering that the actual beam direction distribution is not uniform, we use Huffman code when encoding the beam index, so that the number of generated secret key bits is as close as possible to the theoretical information entropy, achieving higher coding efficiency than equal length coding. The simulation results show that the mutual information per bit reaches above 0.97 and the key agreement rate reached 99% for the harsh environment with a signal-to-noise ratio (SNR) of −10 dB.

Notation: $\|\mathbf{a}\|_2$ denotes the l_2 norm of vector a. $(\cdot)^H$ means the conjugate transpose of the matrix. $\mathcal{CN}(0, \sigma^2)$ denotes a complex Gaussian distribution with zero mean and variance σ^2. $\cup$ denotes cascade operation.

2 System Model

This paper focuses on a downlink single-user MIMO system. As shown in Fig. 1, Alice and Bob are legitimate users in communication, and Eve is a potential eavesdropper.

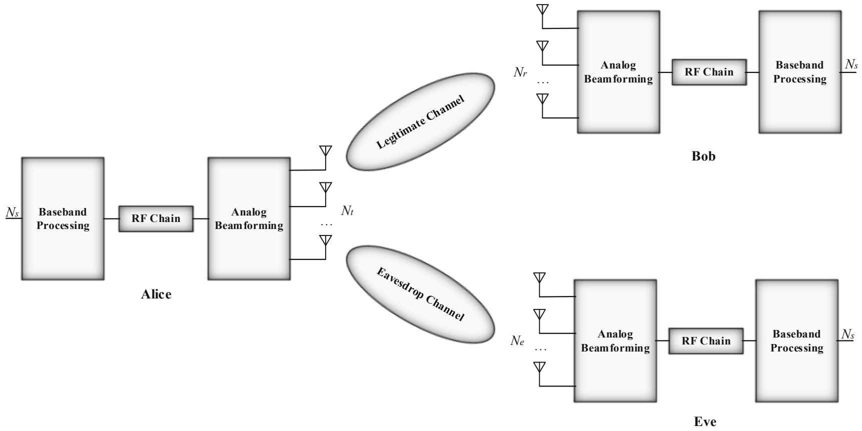

Fig. 1. Key generation system model in massive MIMO.

Alice and Bob can also represent generation node base station (gNB) and user equipment (UE) in the 5G NR protocol. The Alice is mainly composed of a baseband processing unit, N_{RF} Radio Frequency (RF) links, and an analog precoding unit; the Bob or Eve has a similar structure. Assume that N_t antennas deployed on the Alice and N_r antennas deployed on the Bob are connected to one RF link in a fully connected manner, respectively. N_e antennas are deployed on Eve in the same way. The system supports single-stream transmission during communication, which means $N_s = 1$. Generally, the hybrid beamforming system model is as follows:

$$y = \mathbf{w}^H \mathbf{H} \mathbf{f} s + \mathbf{w}^H \mathbf{n} \tag{1}$$

where s is the pilot sequence of symbol, given that $|s|^2 = P_t$, and P_t denotes the transmit power of all antennas. $\mathbf{n} \in \mathbb{C}^{N_r \times N_t}$ is the noise matrix with independent and identically distributed components $\sim \mathcal{CN}(0, \sigma^2)$. Define that $\mathbf{f} \in \mathbb{C}^{N_t \times 1}$ and $\mathbf{w} \in \mathbb{C}^{N_r \times 1}$ are beamforming vectors for analog beamforming (ABF). $\mathbf{H}$ is a wideband geometric mmWave channel that can be modeled as an Extended Saleh-Valenzuela (ESV) channel, and its expression in the time domain is given by

$$\mathbf{h}[d] = \sqrt{\frac{N_t N_r}{\rho}} \sum\nolimits_{c=1}^{C} \sum\nolimits_{r_l}^{R_l} \alpha_{r_l} p_{rc}(dT_s - \tau_c - \tau_{r_l}) \boldsymbol{\alpha}_R(\theta_c - \vartheta_{r_l}) \boldsymbol{\alpha}_T^H(\phi_c - \phi_{r_l}) \tag{2}$$

where $\mathbf{h}[d]$ denotes the MIMO channel response when the delay is d. Define that ρ is the path loss, and C denotes the number of clusters. Let the variables θ_c,$\phi_c \in (0, 2\pi)$ be the physical AoA and AoD respectively. There are R_l paths in each cluster and each path has a relative delay τ_{r_l} and an AOA/AOD offset $\vartheta_{r_l}, \phi_{r_l}$. The variable α_{r_l} denotes the path gain and p_{rc} represents the pulse shaping function corresponding to a sampling interval of T_s at τ second. The vector $\boldsymbol{\alpha}_R \in \mathbb{C}^{N_r \times 1}$ and $\boldsymbol{\alpha}_T \in \mathbb{C}^{N_t \times 1}$ as follows are the antenna array response vectors at Bob and Alice respectively, where uniform linear arrays (ULA) are used.

$$\boldsymbol{a}_R(\theta) = \frac{1}{\sqrt{N_r}} \left[1, e^{j\frac{2\pi}{\lambda} d_s \sin(\theta)}, \ldots, e^{j(N_r - 1)\frac{2\pi}{\lambda} d_s \sin(\theta)}\right]^T \tag{3}$$

$$\boldsymbol{a}_T(\emptyset) = \frac{1}{\sqrt{N_t}} \left[1, e^{j\frac{2\pi}{\lambda} d_s \sin(\phi)}, \ldots, e^{j(N_t - 1)\frac{2\pi}{\lambda} d_s \sin(\phi)}\right]^T \tag{4}$$

λ denotes the wavelength and d_s denotes the distance between the antenna elements, which is generally taken as half the wavelength.

The design of the beamforming vectors is usually implemented via codebook-based beam sweeping. Each codeword in the codebook corresponds to a beam index and beam direction. The simplest method for legitimate users is to traverse the predetermined beamforming codewords set, and select the best codeword pair that can maximize spectral efficiency to construct beamforming vectors $\mathbf{f}$ and $\mathbf{w}$. The set of beamforming codewords used in this paper is the DFT codebook, where the weighting coefficient of the n-th antenna in the m-th codeword can be expressed as

$$Q_{m,n} = e^{j\frac{2\pi mn}{M}}, m = 0, 1, \cdots, M - 1; n = 0, 1, \cdots, N - 1 \tag{5}$$

where m denotes the number of codewords, and n denotes the number of antennas.

3 Beam-Based Secret Key Generation

In this section, we proposed a key generation scheme for the mmWave massive MIMO system, which will be compatible with the existing NR protocol.

Massive MIMO improves the spectral efficiency of the system while also providing beams as new channel characteristics in spatial dimensions. Unlike the other channel characteristics such as RSS, CIR, and phase, the beam information is discrete and quantified so the error caused by quantization can be avoided in the secret key generation process. Besides, the estimation of the channel matrix will be more challenging as the number of antennas increases, but high-dimensional channel estimation is not required in our scheme because beam information can be obtained through a two-stage synchronization process in 5G NR protocol. Therefore the proposed scheme focuses on beam information and is compatible with the existing beam management framework, devoting to a feasible key generation solution.

3.1 Beam Management in 5G NR

The 5G NR synchronization procedure is based on the two-stage beam management operations to reduce the complexity of beam sweeping:

- **Initial access:** A pair of coarse beams for uplink and downlink communication will be initially established between UE and gNB after coarse beam sweeping. But the beam gain at this time is not high due to its wide width. Therefore, further beam management is required to determine a finer beam pair, thereby obtaining a higher communication rate.
- **Beam refinement:** The best pair of fine beams for communication will be determined in this stage. At first, subdivide the coarse beam determined in the previous stage into several fine beams. Subsequently, UE and gNB perform a fine beam search to ensure accurate beam alignment. Finally, a pair of fine beams having better ABF gain for communication will be determined.

The above two stages constitute beam management. In each stage, beam management is based on four different operations: beam sweeping, beam measurement, beam determination, and beam reporting [15].

The current key generation scheme [13, 14] is independent of the 5G NR beam management framework, which will undoubtedly increase additional signaling overhead. To ensure that the synchronization process and the key generation process are completed at the same time, we redesigned and expanded the existing beam management framework as follows.

3.2 The Beam-Based Secret Keys Generation Procedure

The specific implementation steps can be divided into an initial access stage, a beam refinement stage, and a coding stage, as shown in Fig. 2.

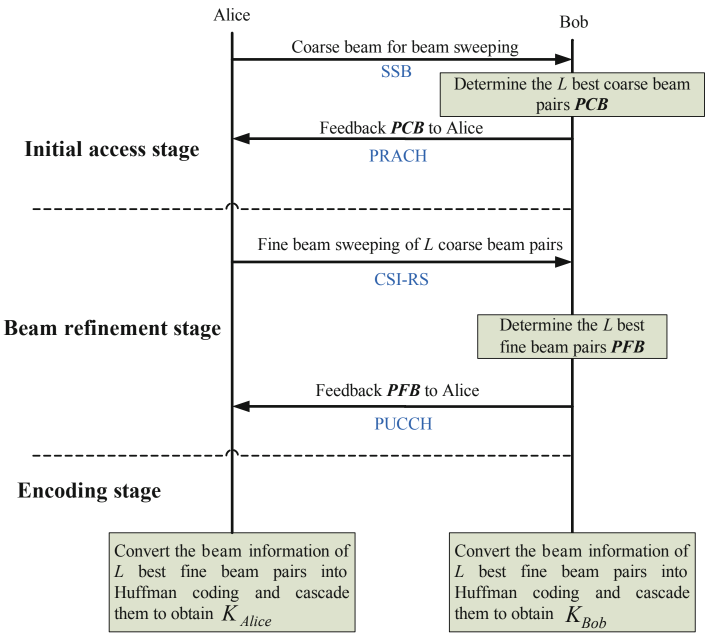
Alice
Bob
Coarse beam for beam sweeping
SSB
Determine the *L* best coarse beam pairs ***PCB***
Feedback ***PCB*** to Alice
PRACH
Initial access stage
Fine beam sweeping of *L* coarse beam pairs
CSI-RS
Beam refinement stage
Determine the *L* best fine beam pairs ***PFB***
Feedback ***PFB*** to Alice
PUCCH
Encoding stage
Convert the beam information of *L* best fine beam pairs into Huffman coding and cascade them to obtain K_{Alice}
Convert the beam information of *L* best fine beam pairs into Huffman coding and cascade them to obtain K_{Bob}

Fig. 2. Beam-based key generation procedure.

- **Initial access stage:** Alice and Bob perform coarse beam sweeping to determine the best coarse beam in this stage. As Bob is not connected to the system, Alice traverses the codewords, using coarse beams to periodically send the reference signal Synchronization Signal Block (SSB), and Bob uses coarse beams to receive and determine the L best coarse beam pairs that maximize the Reference Signal Receiving Power (RSRP), given by

$$\text{RSRP} = \|\boldsymbol{y}\|_2 \tag{6}$$

  Define that $PCB = [TCB_1, RCB_1, TCB_2, RCB_2, \ldots, TCB_L, RCB_L]$ is the L pairs of coarse beam information, where TCB_i and RCB_i are the best transmit and receive coarse beam respectively. One of the best pairs of the coarse beam is used for Bob to access the system, and the remaining $L-1$ pairs of coarse beam index are recorded and used for increasing secret key rate. Subsequently, Bob accesses the system through a physical random access channel (PRACH) and feedbacks PCB to Alice;
- **Beam refinement stage:** Bob can communicate with Alice after the initial access stage. Next, the coarse beam needs to be refined to further align the beam direction to improve communication quality. Alice first traverses the relevant fine beam codewords in TCB_i, and sends the channel state information reference signal (Channel State Information-Reference Signal, CSI-RS) to Bob. Then Bob traverses the relevant fine beam codewords in RCB_i to receive, and selects the pair of beams that maximizes RSRP as the best fine beam pair. After cycling the above steps for

the L pairs of coarse beams, Bob gets the L best fine beam pair information $PFB = [TFB_1, RFB_1, TFB_2, RFB_2, \ldots, TFB_L, RFB_L]$, where TFB_i and RFB_i are the best transmit and receive fine beam index respectively. Finally, Bob sends PFB to Alice through the physical uplink control channel (PUCCH);

- **Encoding stage:** Alice and Bob encode the fine beam information PFB into a binary sequence respectively. Due to the different probability of each beam being selected, we will use Huffman coding to convert PFB into binary bits. The specific reasons will be discussed in the next section. Alice and Bob encode each pair of fine beams in PFB, and then concatenate the converted code groups to obtain their respective secret keys as follows:

$$K_{Alice} = \bigcup\nolimits_{1 \leq i \leq L} \left(THm_i^{Alice} \cup RHm_i^{Alice}\right) \tag{7}$$

$$K_{Bob} = \bigcup\nolimits_{1 \leq i \leq L} \left(THm_i^{Bob} \cup RHm_i^{Bob}\right) \tag{8}$$

where THm_i and RHm_i are the Huffman code group of the transmitting beam index and the receiving beam index corresponding to the i-th pair of beams.

3.3 Variable Length Coding of Beam Indexes

In [13, 14], the physical AoA and AoD are set to a uniform distribution of $(0, 2\pi)$, and the probability of each beam being selected is equal. However, the codebook-based beam distribution in actual scenarios is not uniform due to the different beam width as shown in Fig. 3. The wider the beam, the higher the probability of being selected. Given that AoA and AoD is uniformly distributed, the probability of being selected for each beam can be expressed by

$$Pb_i = \frac{bw_i}{\sum_{i=1}^{N} bw_i}, \quad i \epsilon 1, 2, \ldots, N \tag{9}$$

where N denotes the number of beams, bw_i is the width of the i-th beam, and Pb_i is the probability of the i-th beam being selected.

According to the above analysis, the actual beam index is a non-uniformly distributed discrete random variable, so it is not appropriate to convert them to binary bits with equal length coding. Huffman coding is a type of variable word length coding that constructs the code group with the shortest average length based on the occurrence probability of characters, which means that the number of codewords is as close as possible to information entropy, thereby improving secret key generation efficiency. From the perspective of information security, even if the beam information has eavesdropped on, Eve cannot get the Huffman code group corresponding to the beam index. In a word, the introduction of Huffman coding can both improve the efficiency of the secret key generation and reduce the risk of eavesdropping.

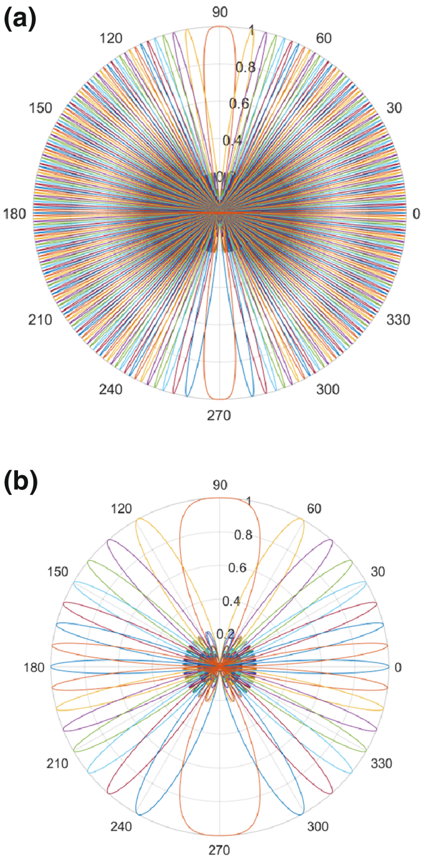

Fig. 3. (a) Beam direction on Alice, $N_t = 128$, (b) Beam direction on Bob, $N_r = 16$

4 Information-Theoretic Analysis

4.1 Mutual Information Analysis

In this section, we discuss the information entropy of random sources under the mmWave channel. Since the selected random source is the beam index that has been quantified to Huffman encoding, the analysis of information entropy can be regarded as the calculation of the information entropy of discrete random variables. Mutual information of beam number can be written as

$$I_k = (\rho_A; \rho_B) \tag{10}$$

where ρ_A and ρ_B are the fine beam indexes at Alice and Bob, respectively, and both of them are discrete random variables. ρ_B can be obtained by two-stage beam sweeping at Bob, ρ_A can be uploaded to Alice by Bob. According to the definition of mutual information, it can be written as

$$I_k = H(\rho_A) + H(\rho_B) - H(\rho_A, \rho_B) \tag{11}$$

As the beam information obtained by Alice depends on the upload process, the joint entropy of ρ_A and ρ_B is

$$H(\rho_A, \rho_B) = H(\rho_B) \tag{12}$$

Combining (11) and (12), mutual information I_k depends on the information entropy of ρ_A. The loss of information entropy between ρ_A and ρ_B mainly results from the transmission errors during the upload process, which can be shown as

$$H(\rho_A) = \sum_{k=0}^{N_{\rho_B}} b\left(k; N_{\rho_B}, ber_{up}\right)[H(\rho_B) - k] \tag{13}$$

where $b\left(k; N_{\rho B}, ber_{up}\right)$ is the binomial distribution, and variable k is the number of error bits. N_{ρ_B} is the length of ρ_B and ber_{up} denotes upload bit error rate. Next we discuss the information entropy of ρ_B in two cases.

Case 1: The distribution of fine beams is uniform, that is, the probability of each fine beam being selected is the same. According to the definition of discrete variable information entropy, we can get

$$H(\rho_B) = log_2 N_B \tag{14}$$

where N_B is the number of values that the random variable ρ_B can take. According to [13],

$$N_B \approx 2^L \cdot N_r \cdot N_t \tag{15}$$

Case 2: The distribution of fine beams is uneven, and that's the case in actual scenarios. The information entropy of ρ_B can be expressed as

$$H(\rho_B) = -\sum\nolimits_{i=1}^{N_B} p_{Bi}\, log_2\, p_{Bi} \tag{16}$$

where p_{Bi} denotes the possibility of the i-th fine beam combination.

4.2 Security Mutual Information Analysis

In our work, security mutual information can be written as $I_{sk} = (\rho_A, \rho_B | \rho_E)$. Eve has two methods to eavesdrop on secret keys.

One method is that Eve can get the same beam indexes as Bob during the fine beam sweeping process. However, the premise of this method must be that Eve knows the index of candidate beam pairs L and have the same configuration as Bob. Only if the eavesdropping channel must be highly correlated with the legal channel, Eve can get the same scan results as Bob. In the mmWave system, two channels become independent if they are separated by several wavelengths [16]. As is known, the millimeter wavelength is on the scale of the millimeter and the distance between two antenna elements in the Massive MIMO transceiver can be very small (0.5 wavelengths or 5.35 mm) [17]. It is almost impossible to keep Eve within half a wavelength around Bob. So it is very difficult for Eve to eavesdrop on the secret keys through the first method.

The other method for Eve to eavesdrop on the secret keys is to intercept the uploaded information from Bob. However, Bob uploads the beam indexes instead of the secret keys themselves. After receiving the beam indexes, Alice needs to use Huffman encoding to convert them into the final secret key. Even if Eve intercepts the uploaded beam index information, Eve does not know the Huffman code corresponding to each beam number and cannot generate the secret key as the same as a legitimate user. Thus our work guarantees the security of the secret key. We can get $I_{sk} \approx I_k$.

5 Simulation Results

In this section, we will demonstrate the performance of the proposed scheme through simulation. There are three main evaluation indicators: key generation rate, bit disagreement rate, and mutual information per bit. 1) The key generation rate measures the number of bits generated during user access. 2) Bit disagreement rate measures the inconsistent bit rate between legitimate users. Obtaining a lower Bit disagreement rate can effectively reduce the subsequent coordination overhead. 3) Mutual information per bit: the normalized mutual information between Alice and Bob which is the mutual information over the number of generated bits [13]. This metric measures the key generation efficiency.

In our simulation, Alice is equipped with N_t antennas, and Bob is equipped with N_r antennas. Define that $N_\mathrm{t} - N_\mathrm{r}$ is the antenna configuration and $N_{RF} = 1$. The antenna array structure is ULA. We model a wideband geometric ESV channel, and its AOA and AOD denoted as $\vartheta_{r_l}, \phi_{r_l}$ are evenly distributed in $(0, 2\pi)$. Set that each coarse beam contains 4 fine beams. In order to reduce the impact of beam sweeping on fine beam selection, Bob searches for three more fine beams when performing fine beam search. The 7 fine beams near the center angle of the coarse beam are searched in fine beam search. The number of simulations is set to 500.

Figure 4 shows the fine beam distribution at Alice and Bob under $N_t = 256$, $N_r = 32$, $L = 3$. The probability of each fine beam being selected is equal under ideal conditions, however because of the different width of each fine beam, the wider beam is more likely to be selected. Although AOA and AOD denoted as $\vartheta_{r_l}, \phi_{r_l}$ are evenly distributed in $(0, 2\pi)$, the fine beam distribution in the actual scene is uneven.

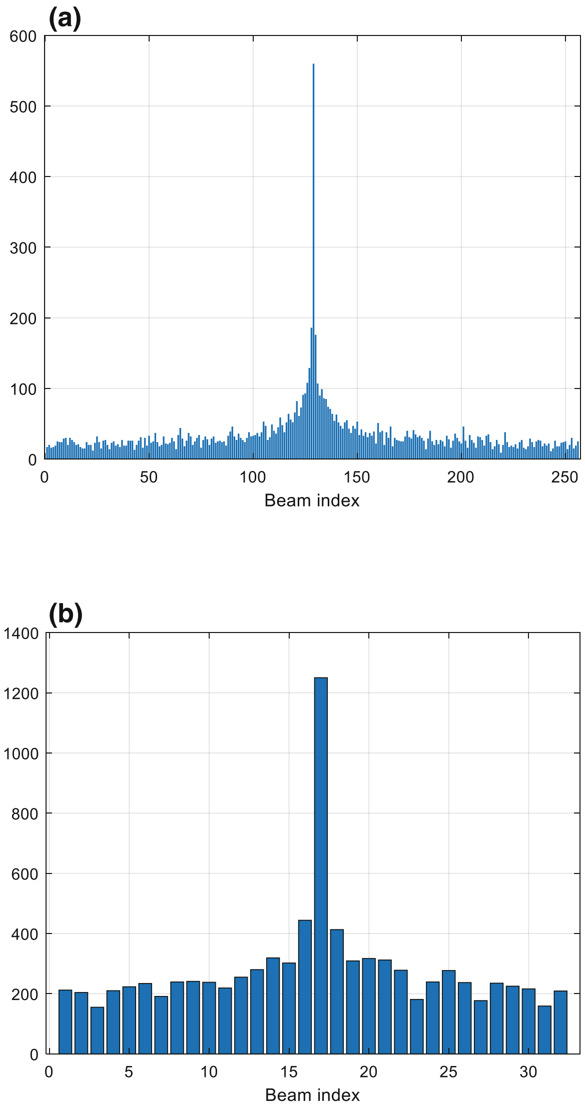

Fig. 4. (a) Fine beam distribution at Alice under $N_t = 256$, $L = 3$, (b) Fine beam distribution at Bob under $N_r = 32$, $L = 3$

Figure 5 shows the comparison of the number of secret key bits in the two antenna configurations. The baseline is the scheme proposed in [13], where full CSI is required and equal length code is used in the encoding of beam indexes. Set that the transmit and receive antenna numbers as $N_t = 128$, $N_r = 16$ and $N_t = 256$, $N_r = 32$ with selected beam pairs number $L = 3$, respectively. It can be seen that more antennas can effectively increase the number of secret key generation. The random variables selected in this paper

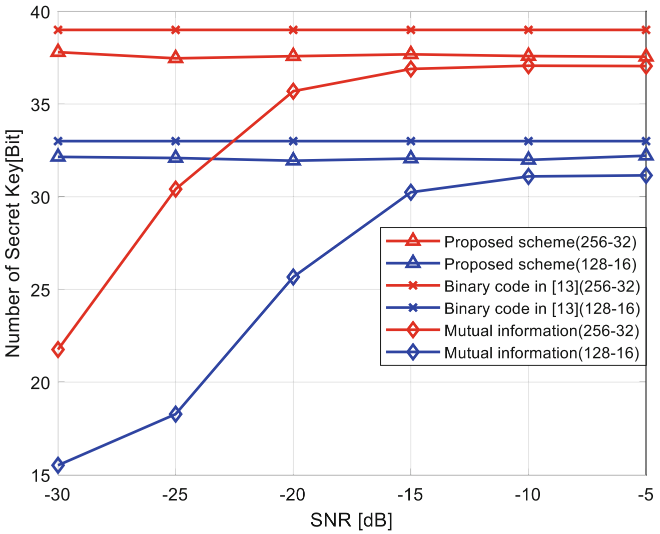

Fig. 5. Secret key bits at different SNRs and antenna configurations

are unequal probability distribution, so the Huffman coding used in our scheme can obtain the minimum code length closer to the mutual information entropy. In other words, we use fewer bits to represent the same amount of information compared with [13].

Figure 6 shows the mutual Information per bit in the two antenna configurations. It can be seen that the mutual information per bit rises with the increase of the signal-to-noise ratio, and the average bit mutual information of the two configurations reaches more than 0.9 at a low SNR = −15 dB; when the SNR is greater than −10 dB, the

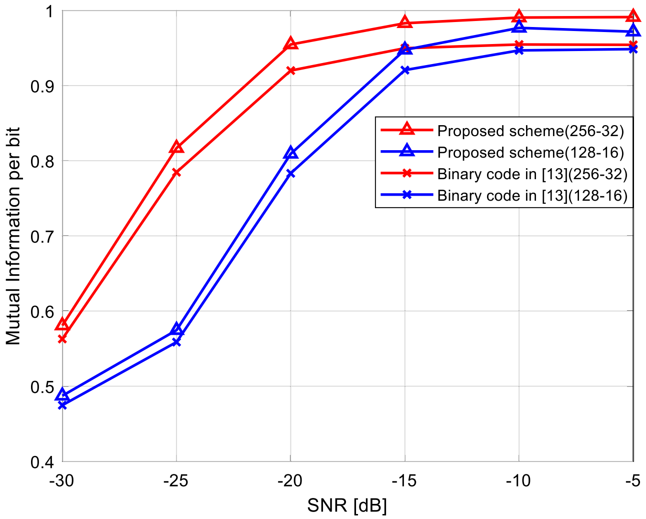

Fig. 6. Mutual Information per bit at different SNRs and antenna configurations

mutual Information per bit tends to be saturated. The increase in the number of antennas is helpful to improve the mutual information per bit. A large number of antennas can obtain a higher beam gain, thereby reducing the bit error rate during the upload process. The encoding method does not affect the mutual information of random variables, therefore the Huffman coding used in this paper can obtain the shortest code length of the secret key, obtaining higher mutual information per bit compared with [13].

Figure 7 shows the bit disagreement rate in the two antenna configurations. It can be seen from the figure that the bit disagreement rate does not perform well at low SNRs. The decrease of bit disagreement rate is obvious with the increase of the SNR. At SNR = −10 dB, the bit disagreement rate drops below 1% under the configuration of 256-32 and 128-16, which shows good robustness of the proposed scheme in a harsh communication environment.

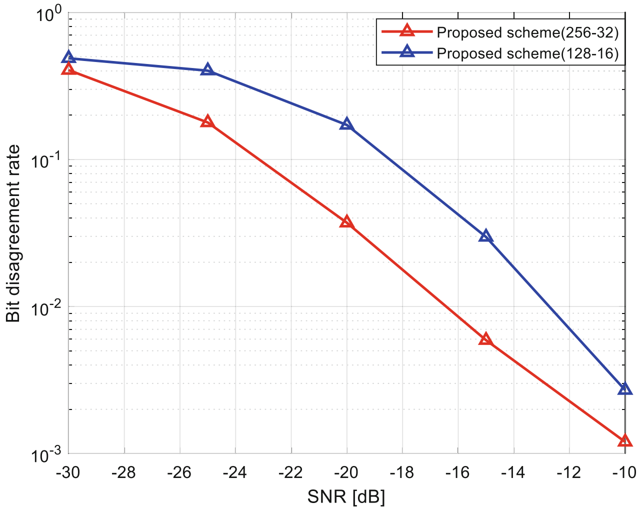

Fig. 7. Bit disagreement rate at different SNRs and antenna number

6 Conclusion

In this paper, we studied the beam-based secure key generation assisted by the two-stage beam sweeping in the massive MIMO system and proposed a key generation scheme compatible with the 5G NR beam management mechanism. In this scheme, we select the beam as the random source to generate the secret key. Bob determines the fine beam information through a two-stage beam sweeping and feedback them to Alice. Considering that the selected random source is unevenly distributed under the ESV channel, we use Huffman variable-length coding to encode the random source to obtain higher key generation efficiency. Even if Eve intercepts the beam index information, Eve cannot generate the secret key as a legitimate user. In the information theory analysis, we discussed the information entropy of our scheme and the two methods for

Eve to obtain the secret keys and put forward reasonable solutions to these two methods. The indicators to measure the effectiveness of the proposed scheme are the key generation rate, the average bit of mutual information, and the key disagreement rate. Simulation results show that Our scheme has higher coding efficiency than equal length coding. When the SNR is –10 dB, the bit disagreement rate is less than 0.01 and the mutual information per bit is greater than 0.97.

Acknowledgement. This work is supported by the Open Project of A Laboratory under Grant No. 2017XXAQ08, the National Natural Science Foundation of China under Grant No.61971069 and 61801051.

References

1. Liu, H., Yang, J., Wang, Y., Chen, Y.J., Koksal, C.E.: Group secret key generation via received signal strength: protocols, achievable rates, and implementation. IEEE Trans. Mob. Comput. **13**(12), 2820–2835 (2014)
2. Mathur, S., Trappe, W., Mandayam, N., Ye, C., Reznik, A.: Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, Series MobiCom 2008, New York, NY, USA, pp. 128–139. ACM (2008)
3. Wang, Q., Su, H., Ren, K., Kim, K.: Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In: 2011 Proceedings IEEE INFOCOM, pp. 1422–1430, April 2011
4. Bakşi, S., Popescu, D.C.: Secret key generation with precoding and role reversal in mimo wireless systems. IEEE Trans. Wirel. Commun. **18**(6), 3104–3112 (2019)
5. Furqan, H.M., Hamamreh, J.M., Arslan, H.: Secret key generation using channel quantization with SVD for reciprocal MIMO channels. In: Proceedings International Symposium Wireless Communication System (ISWCS), pp. 597–602, September 2016
6. Etesami, J., Henkel, W.: LDPC code construction for wireless physical-layer key reconciliation. In: Proceedings 1st IEEE Int. Conference Communication China (ICCC), Beijing, China, pp. 208–213, August 2012
7. Graur, O., Islam, N., Filip, A., Henkel, W.: Quantization aspects in LDPC key reconciliation for physical layer security. In: Proceedings 10th IEEE International ITG Conference System, Communication Coding, Hamburg, Germany, pp. 1–6, February 2015
8. Sun, X., Wu, X., Zhao, C., Jiang, M., Xu, W.: Slepian-wolf coding for reconciliation of physical layer secret keys. In: Proceedings IEEE Wireless Communication Networking Conference, Sydney, Australia, pp. 1–6, April 2010
9. Wallace, J.: Secure physical layer key generation schemes: performance and information theoretic limits. In: Proceedings IEEE International Conference Communication (ICC), Dresden, Germany, pp. 1–5, June 2009
10. Lai, L., Liang, Y., Poor, H.V., Du, W.: Key generation from wireless channels: a review. In: Physical Layer Security Wireless Communication, FL, USA: CRC Press, p. 47C92 (2013)
11. Yaacoub, E.: On secret key generation with massive MIMO antennas using time-frequency-space dimensions. In: 2016 IEEE Middle East Conference on Antennas and Propagation (MECAP), Beirut, pp. 1–4 (2016). https://doi.org/10.1109/mecap.2016.7790086
12. Patwari, N., Croft, J., Jana, S., Kasera, S.K.: High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE Trans. Mobile Comput. **9**(1), 17–30 (2010)

13. Jiao, L., Tang, J., Zeng, K.: Physical layer key generation using virtual AoA and AoD of mmWave massive MIMO channel. In: IEEE Conference on Communications and Network Security (2018)
14. Jiao, L., Wang, N., Zeng, K.: Secret Beam: robust secret key agreement for mmWave massive MIMO 5G communication. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 9–13, December 2018
15. Onggosanusi, E., et al.: Modular and high-resolution channel state information and beam management for 5G new radio. IEEE Commun. Mag. **56**(3), 48–55 (2018)
16. Chen, C., Jensen, M.A.: Secret key establishment using temporally and spatially correlated wireless channel coefficients. IEEE Trans. Mobile Comput. **10**(2), 205–215 (2011)
17. Güvenkaya, E., Hamamreh, J.M., Arslan, H.: On physical-layer concepts and metrics in secure signal transmission. Phys. Commun. **25**, 14–25 (2017)