**International Journal of Scientific Research in Computer Science and Engineering** **Research Paper**
Vol.5, Issue.3, pp.42-46, June (2017) **E-ISSN:** 2320-7639

# A Survey on Quantization Schemes for Secure Key Generation

**U.R. Bhatt[1*], R. Sharma[2], A. Soni[3], R. Upadhyay[4]**

[1]Dept. of Electronics and Telecommunication, IET- Devi Ahilya University, Indore, India
[2]Dept. of Electronics and Telecommunication, IET- Devi Ahilya University, Indore, India
[3]Dept. of Electronics and Telecommunication, IET- Devi Ahilya University, Indore, India
[4]Dept. of Electronics and Telecommunication, IET- Devi Ahilya University, Indore, India

*[*]Corresponding Author: umarathore@rediffmaill.com, Tel.: +91 9425333837*

**Available online at: www.isroset.org**

Received 20th May 2017, Revised 30th May 2017, Accepted 24th Jun 2017, Online 30th Jun 2017

***Abstract***— Secure key generation is one of the promising approach to establish secured link between two legitimate nodes for wireless communication. We established a system, which generate the secret key at the both end of the legitimate node. Secure key generation system contain four major block namely channel estimation, quantization, information reconciliation and privacy amplification, in which quantization is one of the important module. In secured key generation, output of the quantizer will affects the bit mismatch rate significantly. The present paper analyses different quantization schemes to make synchronization between two nodes. By applying key generation technique, we analyze effect of quantization bit on the key disagreement rate.

***Keywords***— Secure key generation; Quantization, Key Disagreement Rate (KDR)

## I. INTRODUCTION

Secret key generation is a method in which randomness of wireless channel is used to generate the keys for legitimate pair of nodes (namely Alice and Bob). It insures the key to be secured from illegitimate user or eavesdropper. Since the wireless channel between Alice and Bob is reciprocal and varies randomly over space and time hence these nodes measure the characteristic of the wireless channel and generate the secret keys. But passive eavesdropper, namely Eve, unable to measure same channel so it is not possible to extract same key as that of Alice and Bob. Key generation can be classified into two categories based on: channel model and source model. In the channel model, two nodes Alice and Bob, both transmit common randomness information to each other, and apply reconciliation and privacy amplification to obtain identical keys [1]. In the source model, both users observe and estimate a random process of the wireless channel between them, followed by information reconciliation and privacy amplification over the public channel to generate the same keys. The observation of the random process from the legitimate users is distinct from the eavesdropper's observation, which ensures the secrecy of the shared key. However, compared to source model based key generation, approaches based on channel model have some basic demands from Alice and Bob, that both users should be aware of the channel state information (CSI) of their own channels as well as eavesdropper's channel[2].

The method of generating secret keys consists of four major steps namely Channel estimation, Quantization, Information reconciliation and Privacy amplification. As a first step, the channel is probed at both the nodes to measure the variations of the channel within the coherence time, to obtain a channel profile. The channel profile is then quantized to obtain a preliminary key. Due to variations in the channel profile, the preliminary key constructed at both the ends does not match for all the bits. Hence to synchronize the preliminary keys, error detection and correction methods are used during the information reconciliation stage. During the reconciliation process, the eavesdropper will also have access to the error detection and correction bits. Thus to minimize the possibility of key prediction, the security of the synchronized keys is enhanced in the privacy amplification stage to obtain a final secure key [1,2,3,4].

In this paper we focus more on quantizer which is used to quantize channel profiles and obtain the preliminary key at Alice and Bob side. Based on our literature survey, quantization algorithms can be classified into two categories: lossless and lossy quantization schemes. Lossless quantization [5, 6, 7, 9, 10] maps every sample to an n-bit symbol whereas lossy quantization schemes [4,8] may drop certain samples in favor of a more robust key generation and to maintain high bit entropy. The original intention was that the output stream could be used directly as a shared symmetric key without using posterior information reconciliation and privacy amplification. We also implement conventional quantizer for secret key generation and observe the key disagreement rate (KDR).

The rest of the paper is organized as follows. Section II we summarize the secure key generation method and literature survey on quantization schemes applied for key generation. In section III we describe our practical system setup with data collection, steps of secure key generation and the observations. The paper is then concluded in Section IV.

## II. RELATED WORK

### *A. Physical Layer Key Generation*

The standard method of generating secret keys consists of four major steps as shown in Figure 1 namely channel measurement, quantization, Information reconciliation and Privacy amplification.

*1.Channel Measurement*- There are several channel parameter to estimate the channel like channel state information (CSI) [2], channel gain, phase[1], angle of arrival(AOA)[11], received signal strength (RSS)[12], etc. But we use received signal strength indicator (RSSI) to measure the channel. RSSI is an indicator of the received signal's power strength at the receiver. It is the most popular parameter to measure the channel, because of its availability. RSS based key generation system is applied in IEEE 802.15.4[7. It is usually used by wireless cards in laptops, smart phone and wireless sensor nodes, to measure the strength of the received signal.

*2. Quantization*- Estimated signal is quantized and converted into bits to obtain a preliminary key. Quantization can be done either on the whole block of the estimate signal or on smaller blocks of estimate signal. They can be classified into *lossy* and *lossless* quantization.

In lossless quantization all measurements of the estimate signal are considered. This type of quantization has single or multiple threshold. The threshold is usually the mean or the median of the channel profile [5,6,7,9]. While, in lossy quantization, multiple thresholds are considered. Values above and below the threshold, are usually assigned binary values according to Gray coding. Whereas, values between the threshold are usually discarded [4,8].

*3. Information Reconciliation [1,2]*- The preliminary key obtained at both nodes are usually not identical. This is due to variations in channel parameters, noise variation and hardware component variation. If preliminary key is not synchronized, encryption and decryption of the data is not possible. Hence to detect the error and for correcting it, reconciliation is required. In this process, Alice generates the parity bits of the preliminary key. Then, only parity bits are transmitted to Bob. Using these parity bits, Bob also computes the preliminary key same as Alice and get the key synchronized.

*4. Privacy Amplification*- In the reconciliation process, the eavesdropper can access parity bits and use this leaked information to guess the rest of the secret key. To remove the possibilities of key prediction, the security of the synchronized key is enhanced by privacy amplification. In this process the length of synchronized key can be reduced, by applying universal hash function at the Alice and Bob side. It is also necessary to send hash function by Alice to Bob so both can use same hash function.

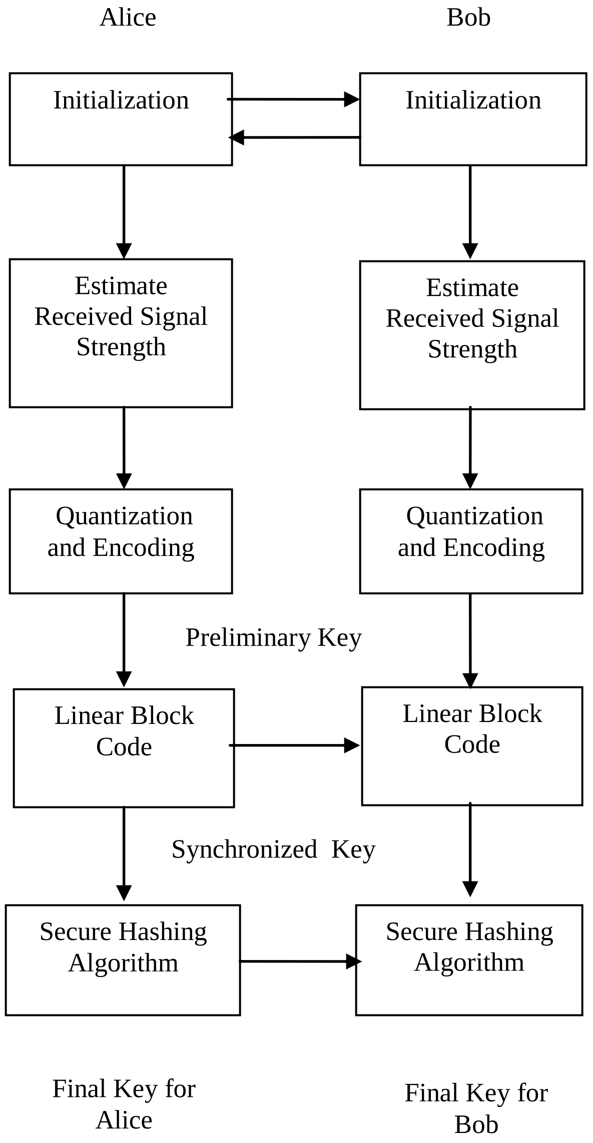

Figure : 1 Illustration for Secret Key Generation

### *B. Quatization Schemes*

Mathur et al.[5] proposed level crossing scheme which is based on a guard band $[x-\alpha*\sigma, x+\alpha*\sigma]$, where x is average of received signal (in form of channel parameter), σ is standard deviation, and α is random number which takes value between (0, 1). In this quantizer threshold is calculated by calculating running window $(\alpha*\sigma)$ and the samples are dropped in the guard band with small absolute values. It also preserve single bit from the m consecutive 1s and 0s and drop the m-1 bits.

Jana et al. [6] have proposed single bit quantizer which is also based on a guard band, similar to the Mathur et al.'s [5] but in this quantizer first RSS measurement is divided into smaller blocks, and then threshold for each block is calculated. The blockwise calculation of threshold is $(\lambda h,\lambda l) = x \pm \alpha*\sigma$ where $\alpha > 0$. In this quantizer extraction of bits is based on upper threshold (for 1) and lower threshold (0) but depend on privacy amplification. Jana et al. [6] also proposed multibit quantizer. It provides N bit extraction per measurement, where N = [log2 range]. The range (RSSmax−RSSmin) is calculated for each block and then divided into $M = 2^N$ equal sized intervals for quantization. Depending on the interval, the RSS measurement is mapped on an N bit assignment (for example use the Gray code sequence).Therefore, the algorithm adapts its output size which depends on the range of RSS measurements. To reduce bit mismatch rate Alice and Bob uses Information reconciliation.

Patwari et al. [7] proposed lossy quantizer. It quantizes the measurement to $K = 4\times2^m$ equally-likely levels and creates Gray code words with m bits. Uniformly distributed preliminary key material can enhance the randomness and makes possible attacks harder. However, by applying unidirectional communication information about the magnitude is revealed. Revealing information of the preliminary key material may result in zeroing the conditional entropy, especially given the fact that additional information reconciliation reveals further entropy.

Ambekar et al. [8] have proposed a two bit quantizer. The three thresholds are chosen blockwise by considering mean and variance of the RSS measurements. This technique cuts off parts of the conditional entropy due to communication.

Zenger et al. [4] extended the work of [7] and presented an empirical quantizer design that can self-organize and aims uniformly distributed output symbols. Therefore, the algorithm divides RSS measurements into smaller blocks and maps the RSS values to uniformly distributed n bit assignment for each block separately. The idea behind that is to generate an output uniform distribution of its symbols. The RSS values are then replaced by the corresponding n bit Gray code sequence. Independent of the initial distribution and without previous knowledge about it, the scheme achieves optimal threshold to map the RSS measurements to equally-likely quantization symbols. This can enhance the randomness of the pre-key material and make possible attacks harder.

Guillaume et al. [9] proposed lossy quantizer in which threshold is decided by the mean value of physical parameter (RSSI). If the sample value is above threshold, it will be considered '1', otherwise '0'.

Wang et al. [10] propose an Entropy-Constrained–like algorithm in which the maximum quantization level, $L \leq 2^{H(h)}$, is decided by estimated entropy H(h) , where h is received signal. Wang et al. [10] also analyze quantization discrepancy occurs due to uncontrolled factor (Non-reciprocity of the channel), and Quantization noise.

## III. PRACTICAL SETUP AND OBSERVATION

### *A. Practical Setup and Data Collection*

In this section, we describe the RSS data sets which were collected using two different transceiver hardware test bed. We collect 120 samples of the RSS over 10 minutes of data collection. Practical setup is shown in Figure 2 and we collect the RSSI (in dBm) shown in the Figure 3 for Alice and Bob.

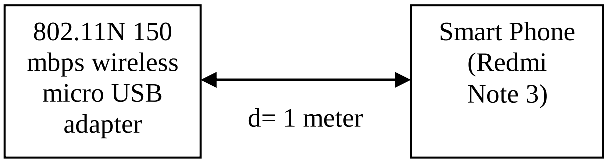
802.11N 150 mbps wireless micro USB adapter
d= 1 meter
Smart Phone (Redmi Note 3)

Figure 2: Practical set up for RSSI collection

### *B. Generation of Secret Key*

In the first Step we collect RSSI by the mentioned practical setup. In the second step, we use n bit-conventional linear quantizers in which the quantization levels were decided by maximum and minimum values of RSSI. The output of the quantizer is passed through encoder which generates the preliminary key, at this stage we compare the encoded output at both nodes and key disagreement rate (KDR) is observed at different signal to noise ratio (SNR) as shown figure 4. In the third step linear block coding is used to improve KDR. In the last step, secure hash algorithm (SHA-1) is employed to find the secret key.

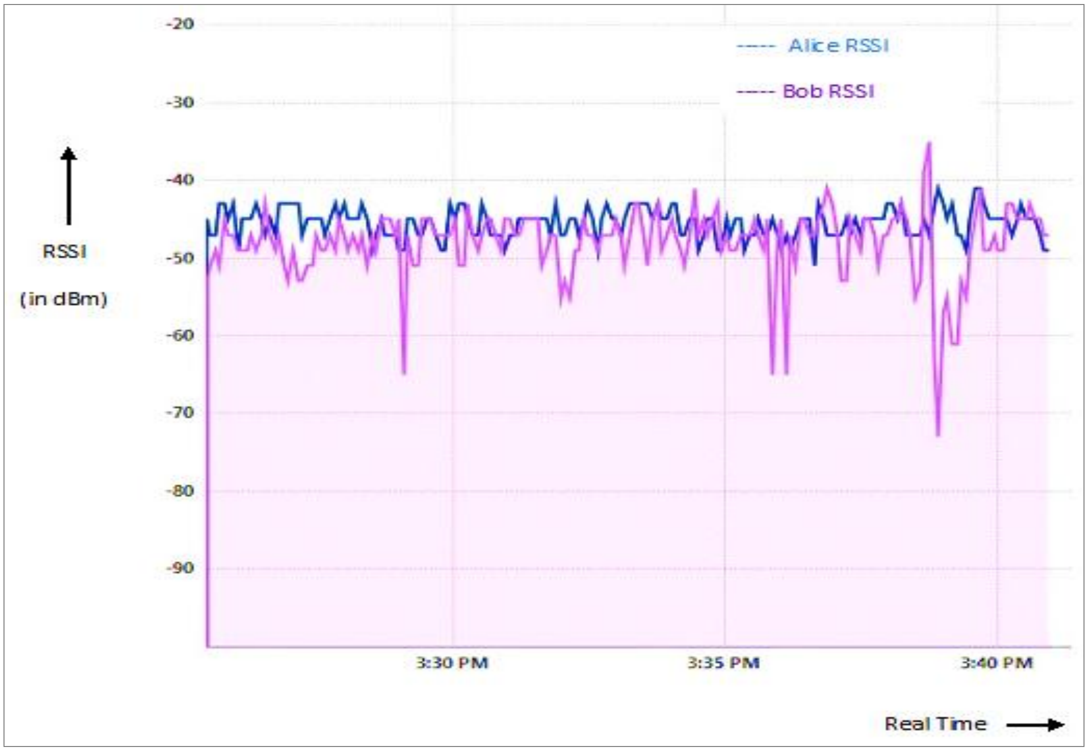

Figure 3 : Received Signal Strength Indicator

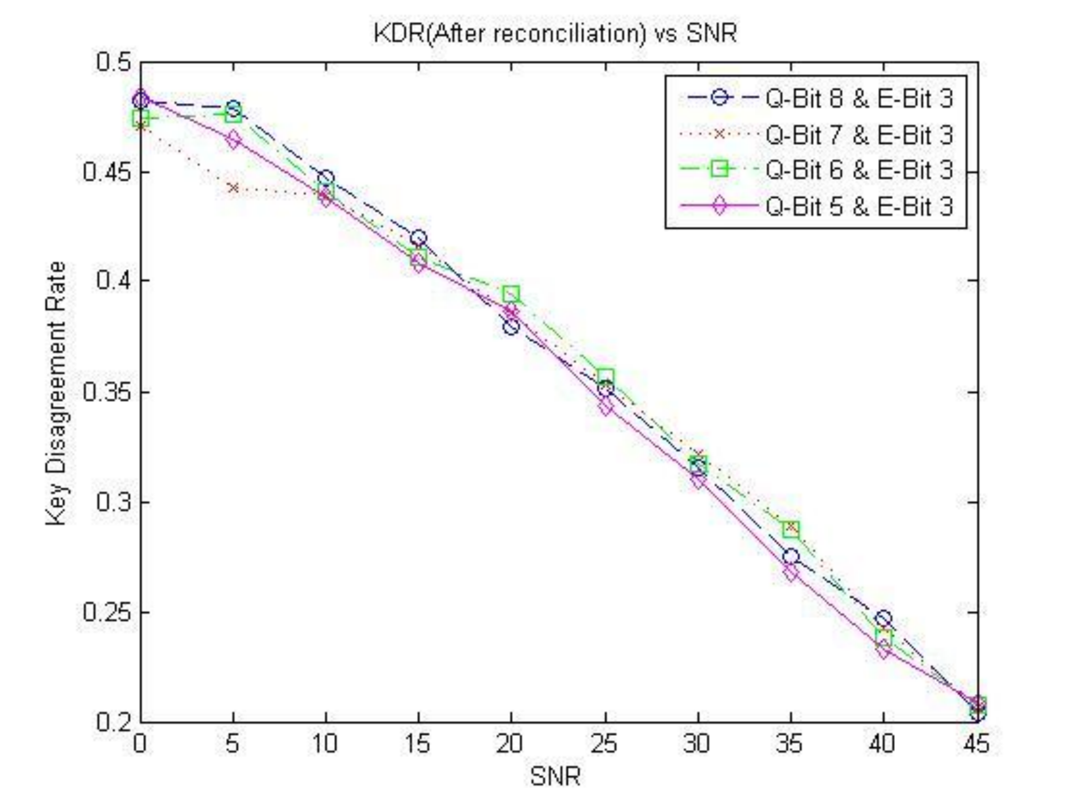

Figure 4 : KDR vs SNR for different Quantization Bits

### *C. Observations*

It is observed from fig. 4 that that during the secret key generation, KDR depends on number of quantization bits (Q-Bit) (number of bits used for one sample). On increasing the Q-Bit the KDR will increase. It happens because, more encoding bits due to more quantization level results in increasing probability of key mismatch.

## IV. CONCLUSION

In this paper, a survey on the most recent quantization schemes for secure key generation is presented. Based on simulation results, it is concluded that KDR will reduce on reducing Q-bit.

## REFERENCES

[1] A. Badawya, T Elfouly, T Khattab, A Mohamedb, M Guizani, "*Unleashing the secure potential of the wireless physical layer: Secret key generation methods*", Physical Communication, Vol. 19, Issue.6, pp. 1-10, 2016.

[2] J. Zhang, T.Q. Duongl, A. marshall, and R. woods, "*Key Generation From Wireless Channels: A Review*", IEEE Access, Vol. 4, Issue.1, pp.614-624, 2016 .

[3] C. T. Zenger, J. Zimmer, C. Paar, "*Security Analysis of Quantization Schemes for Channel-based Key Extraction*", in proc. Workshop wireless commun. Secur. Phys. Layer, portugal, pp.1-7, 2015

[4] C.T. Zenger, M.J. Chur, J.F. Posielek, C. Parr, "*A Novel Key Generating Architecture for Wireless Low-Resource Devices*", International Workshop on Secure Internet of Things, Poland, pp. 26-34, 2014.

[5] S. Mathur, W. Trappe, N.B. Mandayam, C Ye, A. Reznik, "*Radio-telepathy: extracting a secret key from an unauthenticated wireless channel*", 14th Annual International Conference on Mobile Computing and Networking, USA, pp 128–139, 2008.

[6] S. Jana, S. N. Premnath, M. Clark, S.K. Kasera, N. Patwari, S.V. Krishnamurthy, "*On the effectiveness of secret key extraction from wireless signal strength in real environments*", In the presseding of 15th Annual International Conference on Mobile Computing and Networking, China, pp. 321-332, 2009.

[7] N. Patwari, J. Croft, S. Jana, S.K. Kasera, *"High-rate uncorrelated bit extraction for shared secret key generation from channel measurements"*, IEEE Trans. Mob. Comput., Vol 9, Issue1, pp.17-30, 2010.

[8] A. Ambekar, M. Hassan, H.D. Schotten, *"Improving channel reciprocity for effective key management systems"*, 2012 International Symposium on In Signals Systems and Electronics (ISSSE), UK, pp.1-4, Oct 2012.

[9] R. Guillaume, A. Mueller, C.T. Zenger, Christof Paar Andreas Czylwik "*Fair Comparison and Evaluation of Quantization Schemes for PHY-based Key Generation*", 18th International OFDM Workshop,Germany, pp.1-8, 2014.

[10] X. Wang, L. Thiele, T. Haustein, Y. Wang, "*Secret key Generation Using Entropy-Constrained-Like Quantization Scheme* ", 23rd International Conference on Telecommunications (ICT),, China, pp.34-40, 2016

[11] A. Badawy, T. Khattab, T. El-Fouly, A. Mohamed, D. Trinchero, "*Secret key Generation based on AOA estimation for low SNR condition*", IEEE 81st vehicular technology conference, VTC sprint, pp. 1-7, 2015

[12] H. Li, L. Chen, "*RSSI-Aware Energy Saving For Large File Downloading on Smartphones*", IEEE Emebedded System Letters, Vol. 7, Issue 2, pp.63-66, 2015

## Authors Profile

Dr.( *Mrs*.) Uma Rathore Bhatt received his Ph.D. in Electronics and Telecommunication Engineering from DAVV, Indore, India in 2014, M.Tech. in Opto-Elex, SGSITS, Indore, India in 2002 . Dr. Bhatt has been an assistant professor of Electronics and Telecommunication Engineering at IET DAVV since 2003. Her research interests cover Wired and Wireless Access Networks-Specifically Optical Networks, Fiber- Wireless (FiWi) Access Networks, Wireless Sensor Networks Microcontrollers and Microprocessors.

*Mr* Ravindra Sharma received his bachelors in Eelctronics and communication Engineering from the RGPV, university, India in 2010. He is currently pursuing his M.E. at the Department of Electronics and Telecommunications at IET, DAVV Indore, India. His research interests include communication system, physical layer security, internet of things.

Mr. Ankit Soni received his bachelors in Engineering from the Rajiv Ganghi Technical University, Bhopal, India in 2009 and his M.Tech. from Devi Ahilya Vishwavidyalaya, Indore, India in 2012.He is currently pursuing his Ph.D. at the Department of Electronics and Telecommunications at Institute of Engineering & Technology, DAVV, Indore. His research interests include wireless communication, physical layer security, Internet of Things and hardware implementation of communication systems.

*Dr. (Mrs*.) Raksha Upadhyay received his Ph.D. in Electronics and Telecommunication Engineering from DAVV, Indore, India. Dr. Upadhyay has been an assistant professor of Electronics and Telecommunication Engineering at IET DAVV since 2007. Her research interests cover Communication Engineering; Digital Communication,Communication Networks.