IOT SECURITY ENHANCEMENT USING PHYSICAL LAYER SIGNATURES

PROJECT GUIDE : MRS. N. VIJAYA

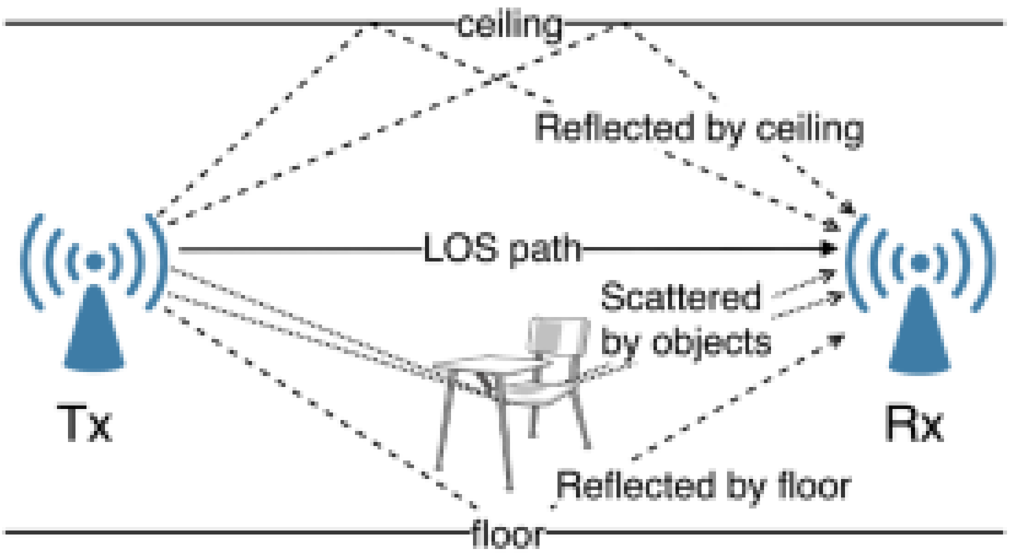
NARAYANAN B - 2016105053

VENKAT KRISHNAN B K J - 2016105077

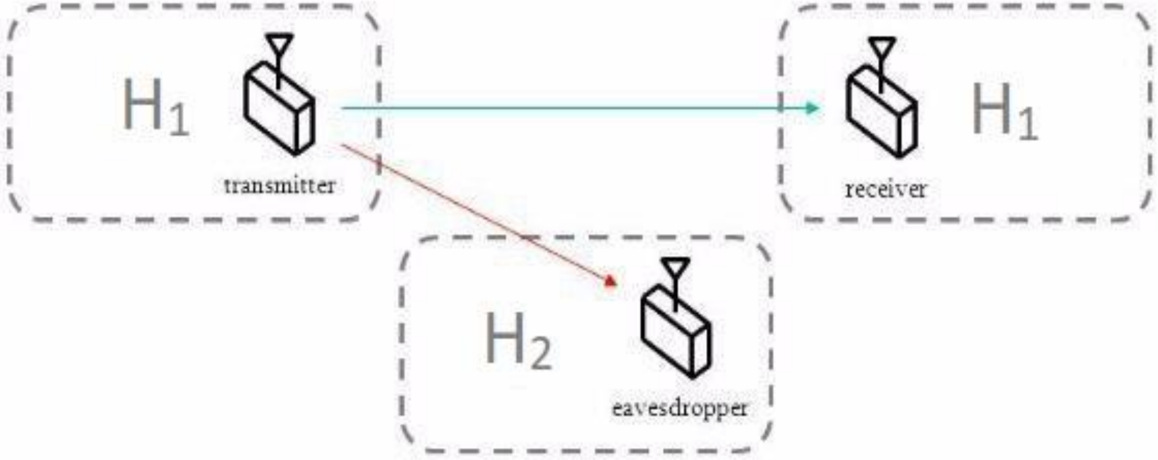
ASHOK KUMAR M - 2016105513

INTRODUCTION

- Wireless networks are susceptible to various attacks due to the “open air” nature of the wireless communication
- A secure wireless communication system involves **authentication and secure transmission**
  - **Authentication** verifies the user identity and prevents malicious users from accessing the network
  - **Secure transmission** protects data integrity and confidentiality using encryption schemes
- **IoT Security**
  - Devices are **low powered** and mostly battery operated
  - Flawed because of the **operational limitations on the computational powe**r
- **Physical layer signatures**
  - Fine-grained values derived from the physical layer, such as **RSS** and **CSI**.
  - **Very sensitive** to location and time
  - Presents an **excellent quality of randomness**



Various factors affecting the signal



Channel Model

MOTIVATION

- **Drawbacks of Conventional Cryptography Techniques**

  Due to the "open-air" nature, key distribution is more susceptible to attacks in wireless communications.

  Mathematically Complex in the case of IoT devices

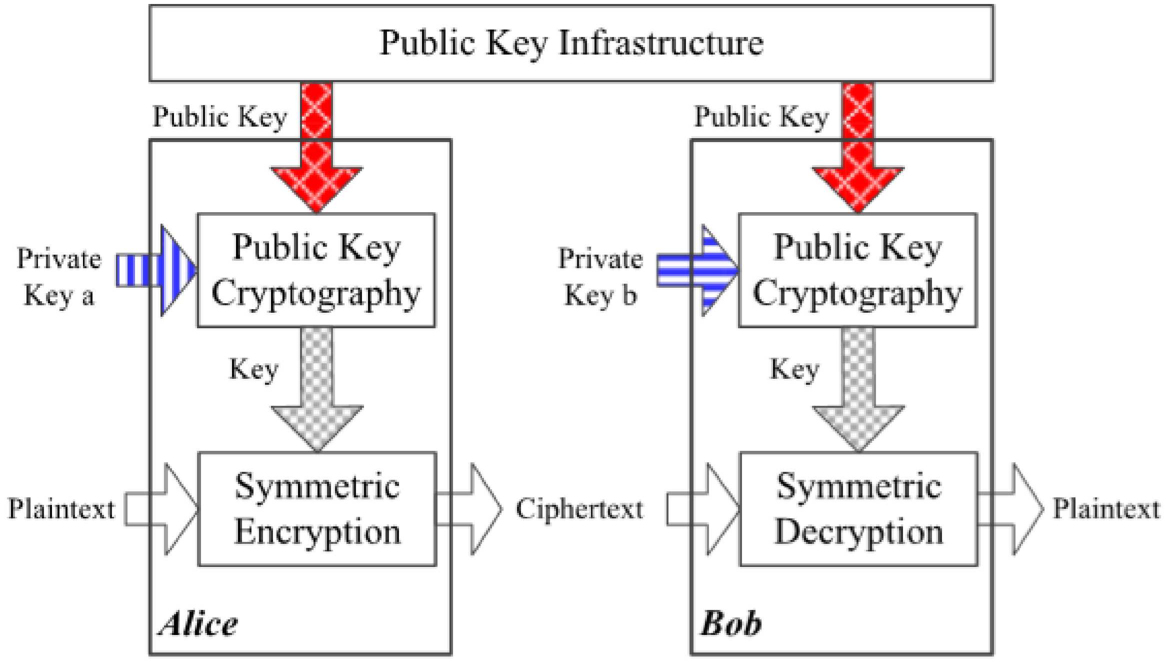
- **Physical Layer Security**

  It involves physical layer signatures which are very random, unique and doesn't involves complex mathematical computations

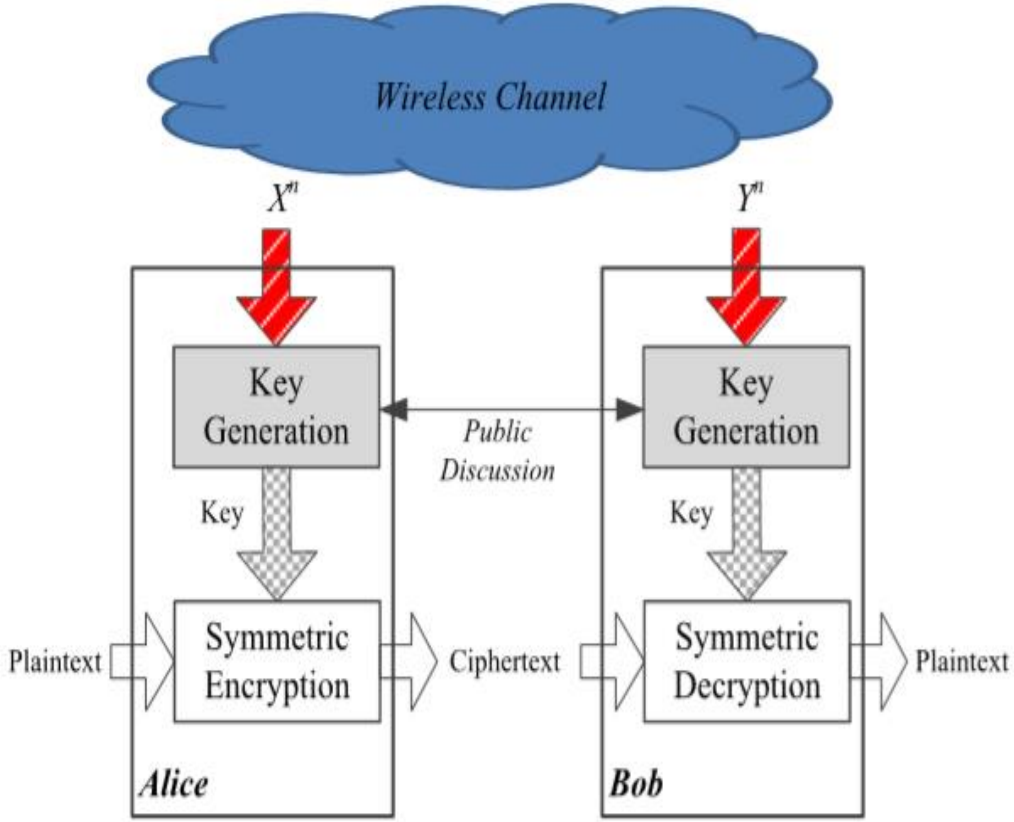
- **Physical Layer Security + Cryptographic Techniques**

  Existing cryptographic securities can be enhanced with the incorporation of physical layer signatures

Existing Method



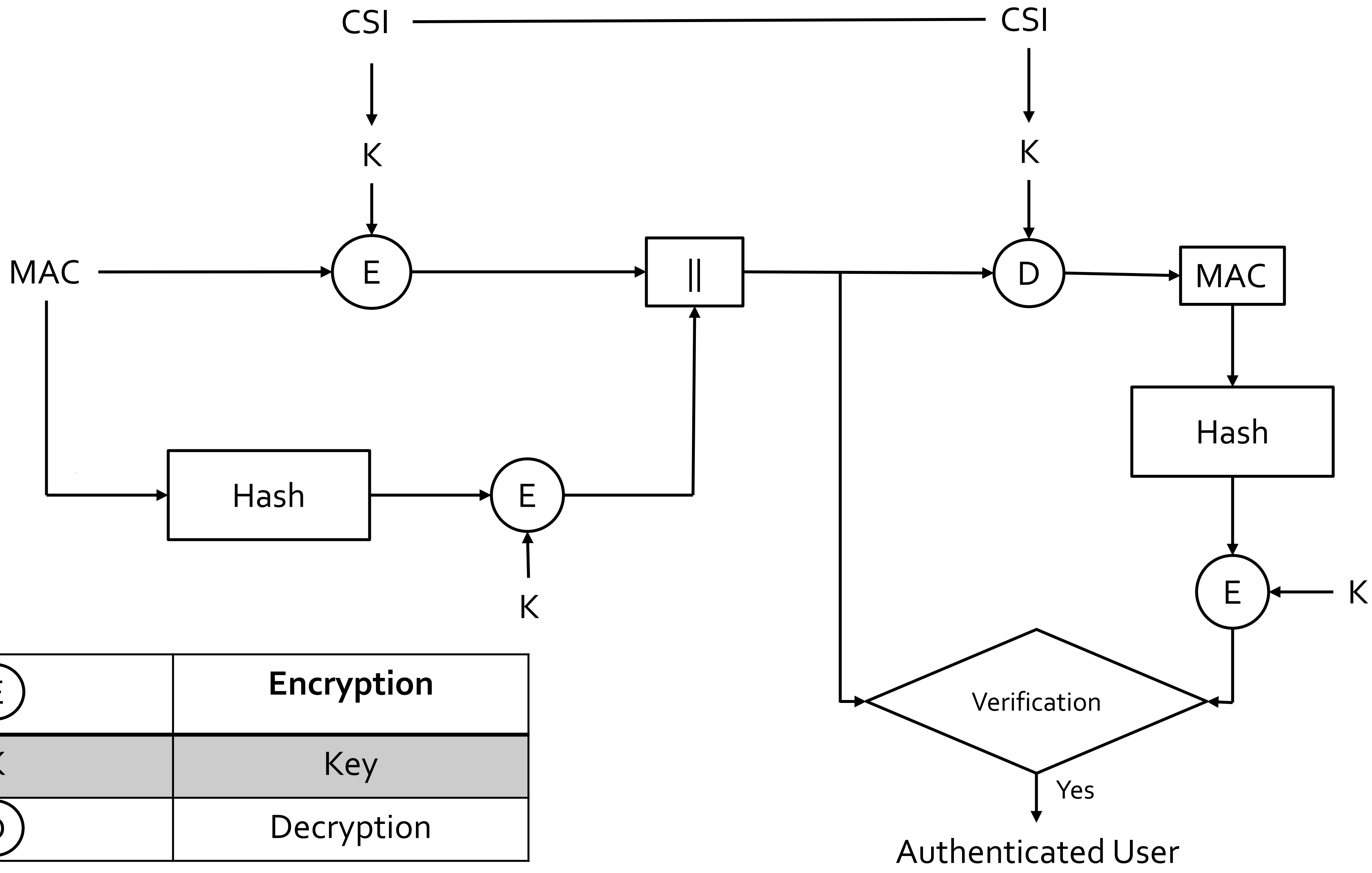
Proposed Method



OBJECTIVE

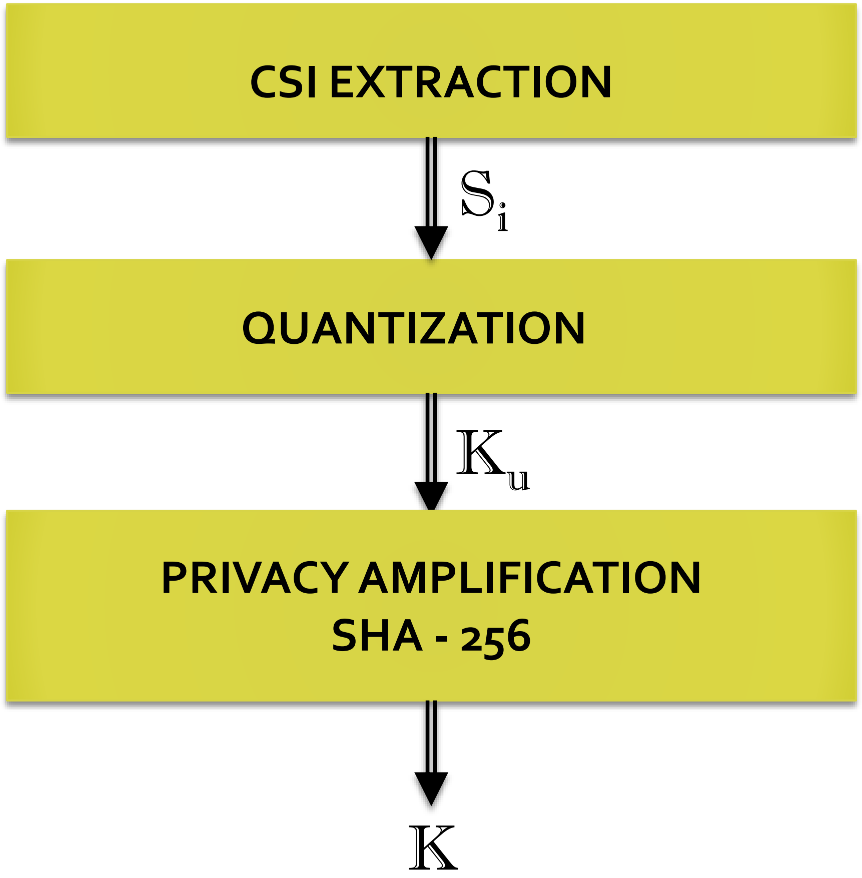
- To develop a new secret key generation algorithm using physical layer signatures (Channel State Information).
- To overcome key exchange, key distribution and key management overhead at legitimate users.
- To provide significant improvement in secrecy.

METHODOLOGY



E	**Encryption**
K	Key
D	Decryption

FLOWCHART


CSI EXTRACTION
S_i
QUANTIZATION
K_u
PRIVACY AMPLIFICATION
SHA - 256
K

QUANTIZATION ALGORITHM

INPUT: Absolute value of CSI, S of length N, $K_d, i = 1 \rightarrow N$

OUTPUT: K_u

Step 1: To find max and min of S

Step 2: To find quantization threshold by using $q_t = \frac{max + min}{2}$

Step 3: Compare S_i with q_t

if $S_i > q_t$ then $K_d i = 1$

else if $S_i < q_t$ then $K_d i = 0$

Step 4: $\Delta = q_t$

Step 5: while($no. of\ zeros\ in\ K_d\ == no.\ of\ ones\ in\ K_d$)

$\Delta = \frac{\Delta}{2}$

if $no. of\ zeros\ in\ Kd\ > \frac{N}{2}$

$q_t = q_t - \Delta$

if $no. of\ ones\ in\ Kd\ > \frac{N}{2}$

$q_t = q_t + \Delta$

Compare S_i with q_t

if $S_i > q_t$ then $K_d i = 1$

else if $S_i < q_t$ then $K_d i = 0$

Step 6: $K_u = K_d$

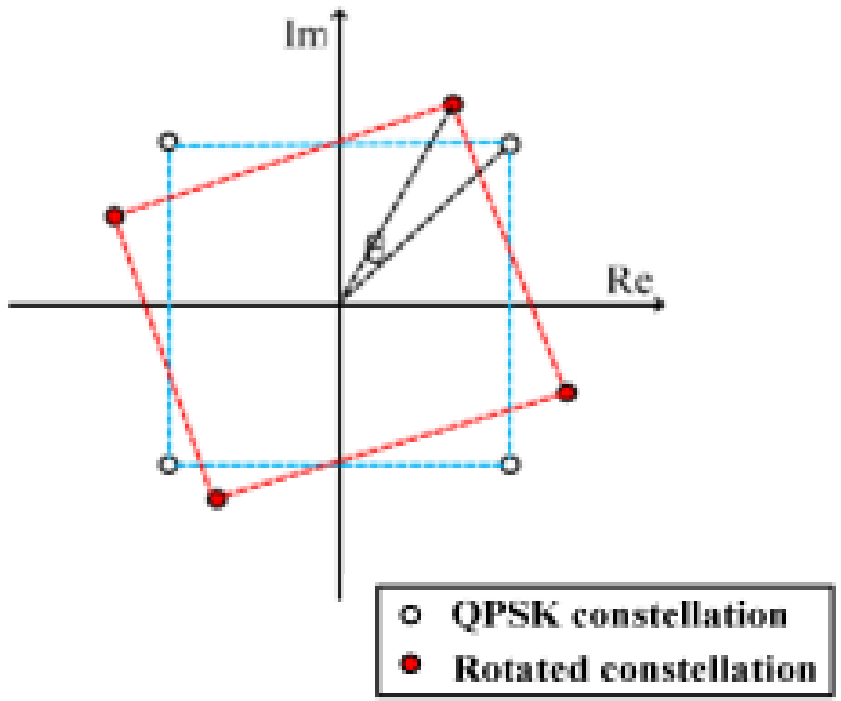
ENCRYPTION

- This encryption technique is based on the constellation rotation in modulation techniques which enhances the security provided in the above layers.
- The constellation rotation requires a phase value to be calculated from the generated key.
- Every constellation symbol S_k is rotated by a unique angle α as

$$S_K^{'} = S_K \cdot e^{j\propto}$$

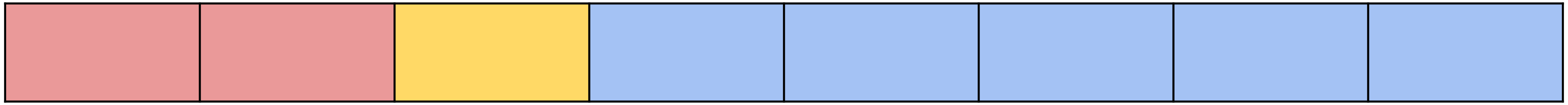
where, S_K - Original constellation symbol

$S_K^{'}$ - Rotated constellation of S_K



PHASE CALCULATION

- To generate an unique angle with respect to the generated key.
- The 256 bit key is split into 8 bit words to find 32 phases.



	Bits used to determine the quadrant of the phase
	Sign Bits
	Magnitude Bits

a_1	a_2

QUADRANT BITS

- The first two bits in the 8 bit word are used to determine the quadrant of the required phase.
- The bits are converted to it's decimal equivalent *i*.
- The base angle is determined by

$$base = i \times 90$$

b

SIGN BIT

- If **b is 0**, the constellation is rotated in the **anticlockwise** direction.
- If **b is 1**, the constellation is rotated in the **clockwise** direction.

MAGNITUDE BITS

C_1	C_2	C_3	C_4	C_5

- These 5 bits are used to determine the position in the respective quadrant.
- The decimal equivalent is determined as n and the required magnitude can be equated as

$$mag = n \times \frac{90}{2^5}$$

Now, the unique angle is determined from the 8-bit word as

$$\propto = (-\mathbf{1})^{\boldsymbol{sign\ bit}} \times (\boldsymbol{base} + \boldsymbol{mag})$$

DECRYPTION

- The original constellation symbol can be recovered as

$$S_K = S_K^{'} \cdot e^{-j\propto}$$

where, S_K - Original constellation symbol

$S_K^{'}$ - Rotated constellation of S_K

- The angle **α** is unique for every user as the CSI is unique. The resulting **α** varies even between the 32 words that makes the constellation rotation more random and more secure.

PERFORMANCE METRICS

MISMATCH RATE

- Mismatch rate is defined to be ratio of mismatched bits between the secret keys independently generated by the user and the provider.
- In the coherence time interval, the mismatch rate is ideally zero between the sender and receiver, but practically due to noise, distortion etc., it is a very low value.

LEAKAGE RATE

- Leakage measures the amount of information learned by the adversary.
- Leakage is defined to be the ratio of matched bits between the sender and the adversary. An encryption scheme with lower leakage is more secure.

PERFORMANCE METRICS

BER PERFORMANCE

- The **bit error ratio** (also **BER**) is the number of bit errors divided by the total number of transferred bits during a time interval.
- The evaluations show that the bit error decreases with an increase in SNR for the intended user but the bit error remains constant even with an increase in SNR for the adversary.

KEY VARIATION WITH TIME

- The CSI is generally very sensitive to variations with time. The key generated by the different users at different time intervals even at the same location are hence unique and random.
- A higher key variation will result in better security.

RESULTS

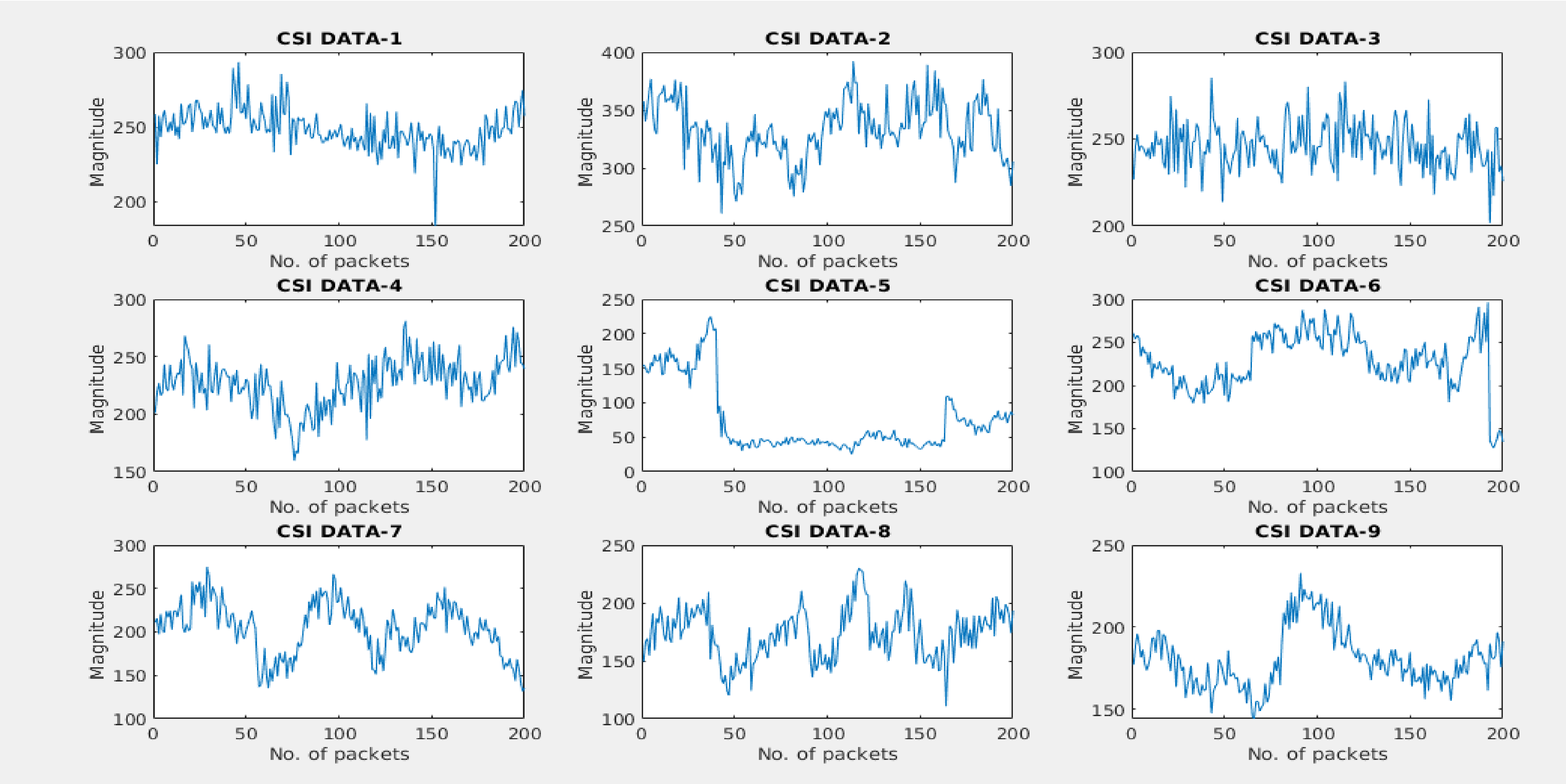
Data extracted from NIC

Field	Value
timestamp	3.3446e+09
csi_len	140
channel	2437
err_info	0
noise_floor	0
Rate	132
bandWidth	0
num_tones	56
nr	1
nc	1
rssi	14
rssi1	14
rssi2	128
rssi3	41
payload_len	1040
csi	*1x1x56 complex...*
payload	*1040x1 uint8*

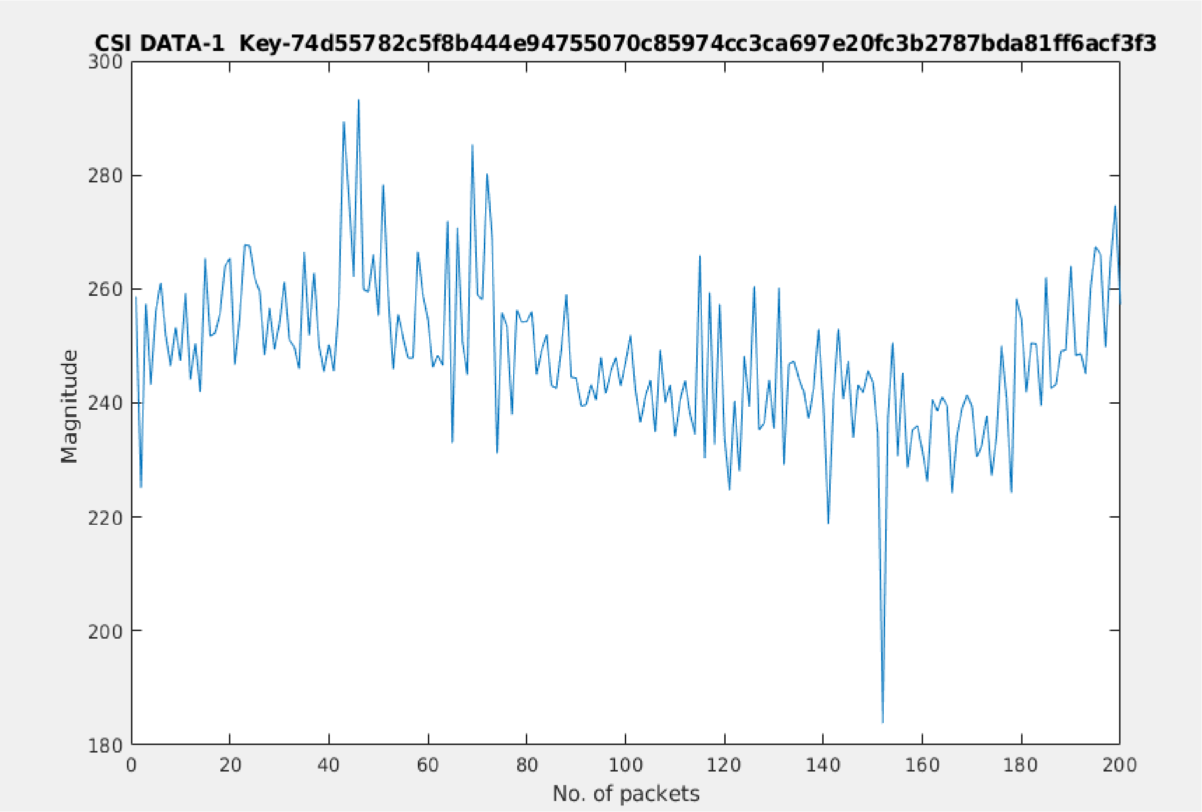
Sample CSI data

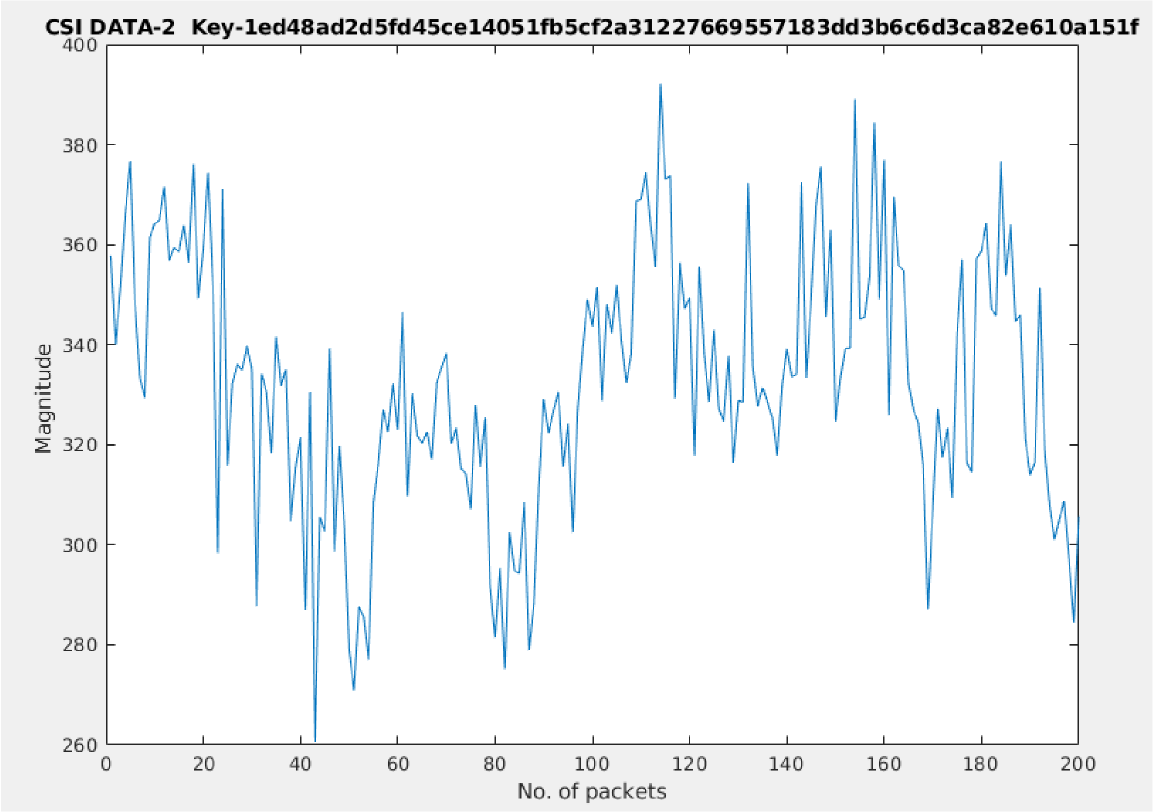
```
val(:,:,1) =

  73.0000 +62.0000i


val(:,:,2) =

  72.0000 +70.0000i


val(:,:,3) =

  91.0000 +65.0000i


val(:,:,4) =

  90.0000 +47.0000i


val(:,:,5) =

  97.0000 +47.0000i
```

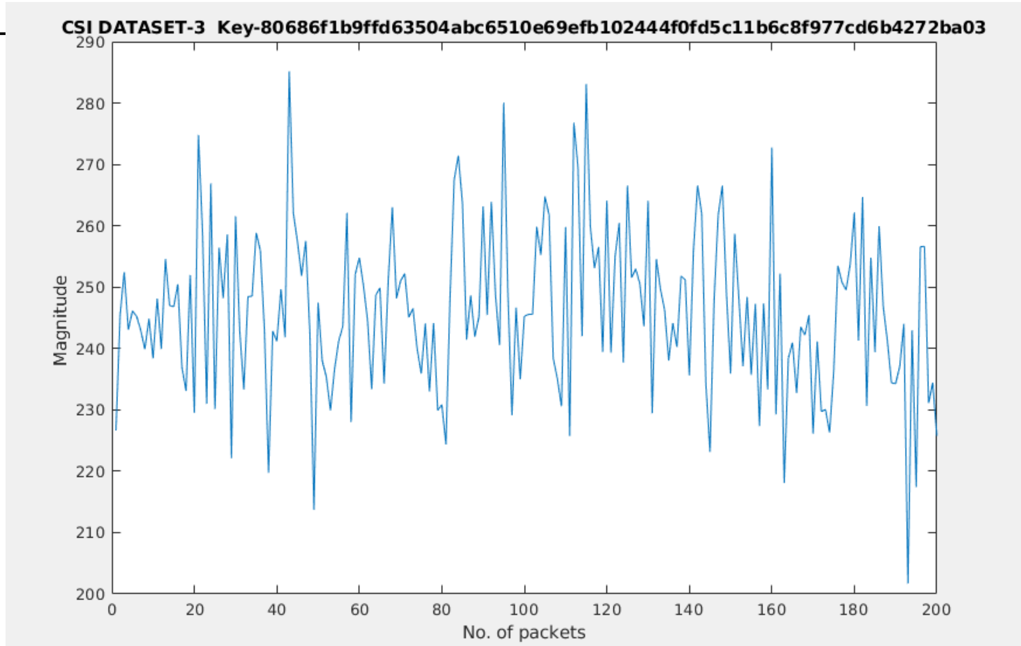
CSI Samples varying with respect to distance and time

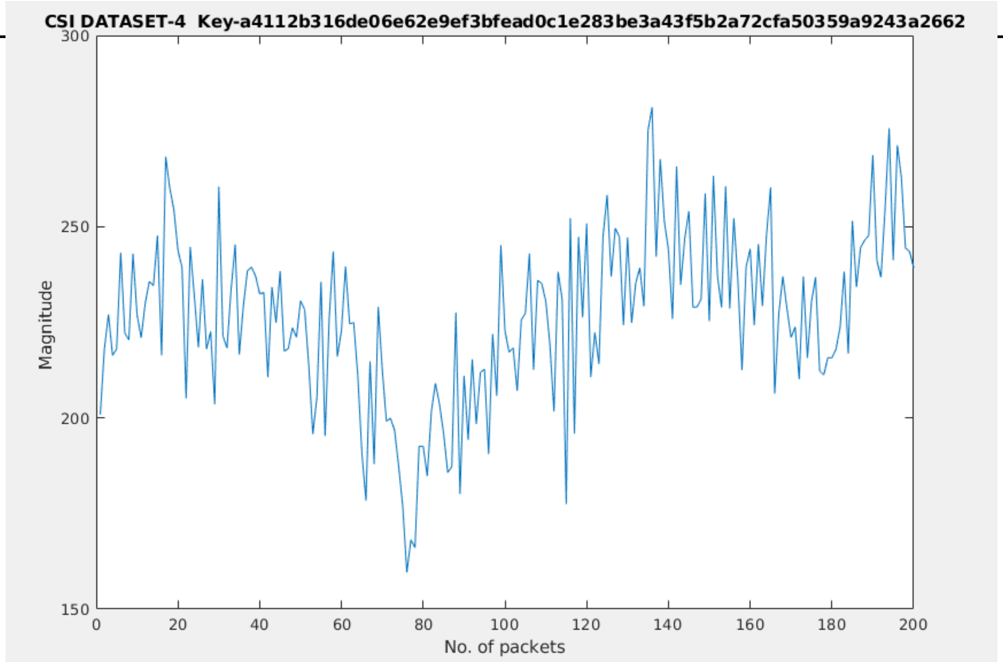


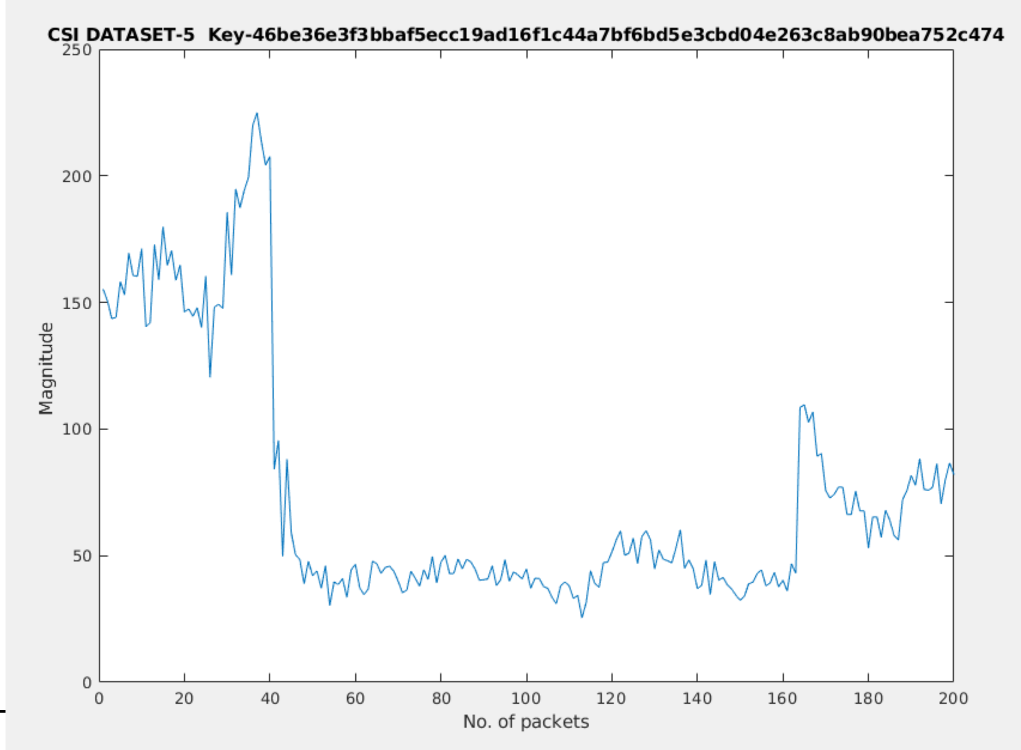
Keys generated for different CSI values

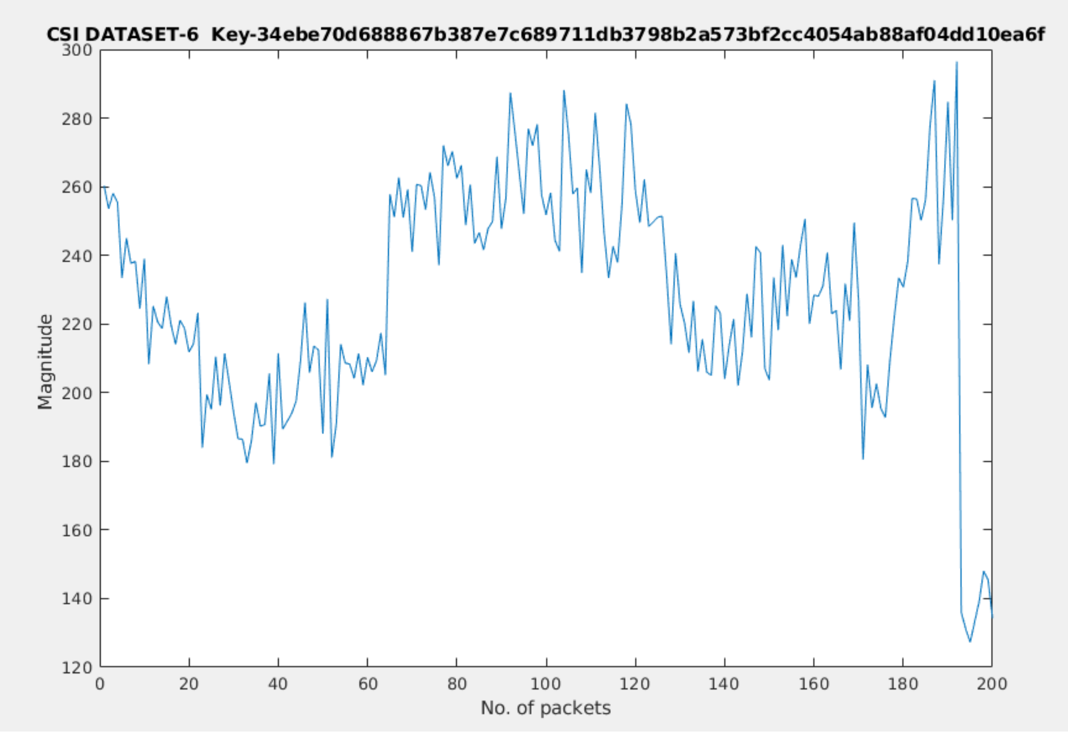


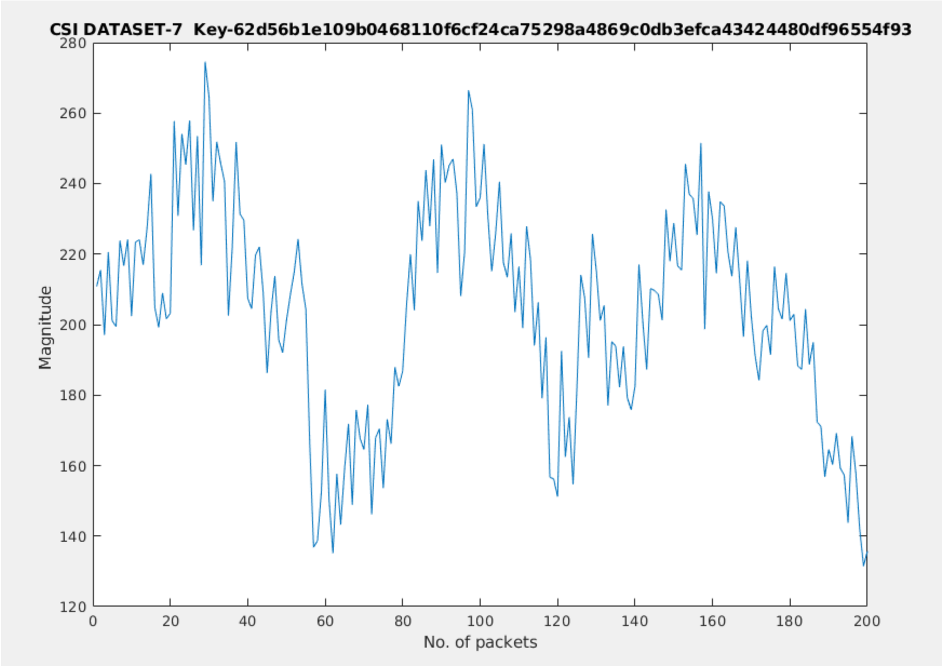


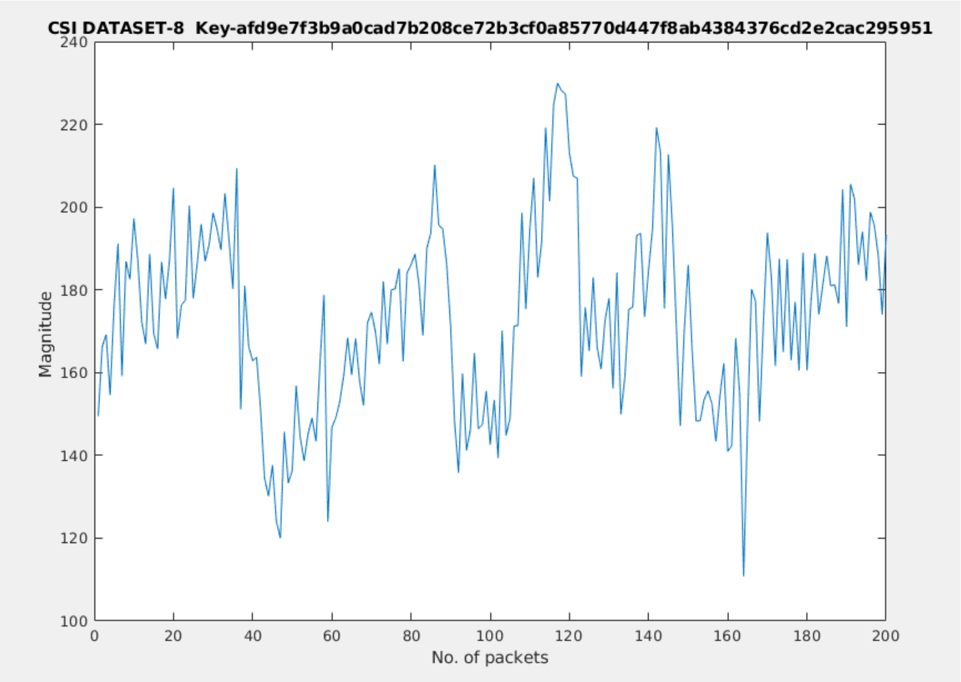

CSI DATASET-3 Key-80686f1b9ffd63504abc6510e69efb102444f0fd5c11b6c8f977cd6b4272ba03
Magnitude
290
280
270
260
250
240
230
220
210
200
0 20 40 60 80 100 120 140 160 180 200
No. of packets

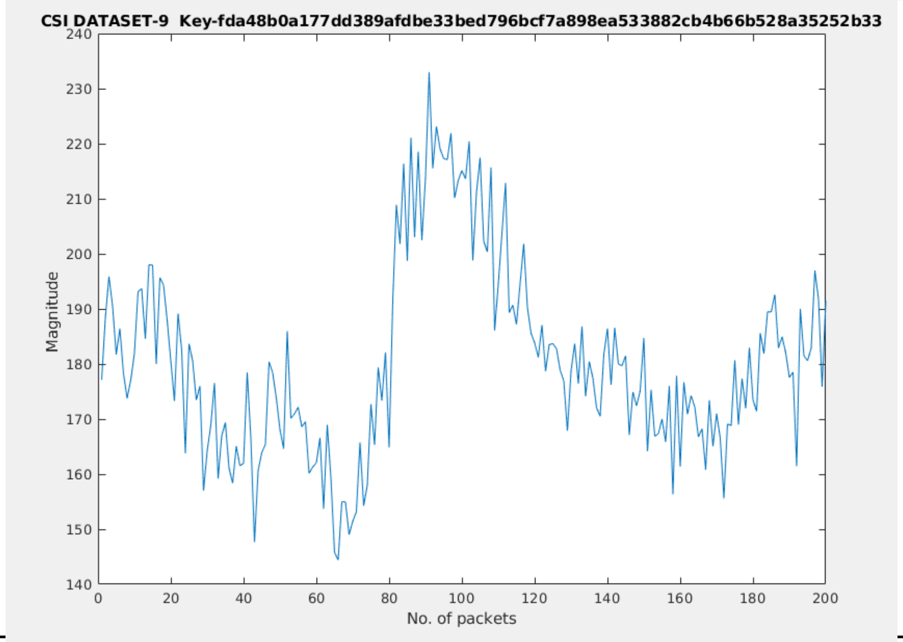

CSI DATASET-4 Key-a4112b316de06e62e9ef3bfead0c1e283be3a43f5b2a72cfa50359a9243a2662
Magnitude
300
250
200
150
0 20 40 60 80 100 120 140 160 180 200
No. of packets


CSI DATASET-5 Key-46be36e3f3bbaf5ecc19ad16f1c44a7bf6bd5e3cbd04e263c8ab90bea752c474
Magnitude
250
200
150
100
50
0
0 20 40 60 80 100 120 140 160 180 200
No. of packets


CSI DATASET-6 Key-34ebe70d688867b387e7c689711db3798b2a573bf2cc4054ab88af04dd10ea6f
Magnitude
300
280
260
240
220
200
180
160
140
120
0 20 40 60 80 100 120 140 160 180 200
No. of packets

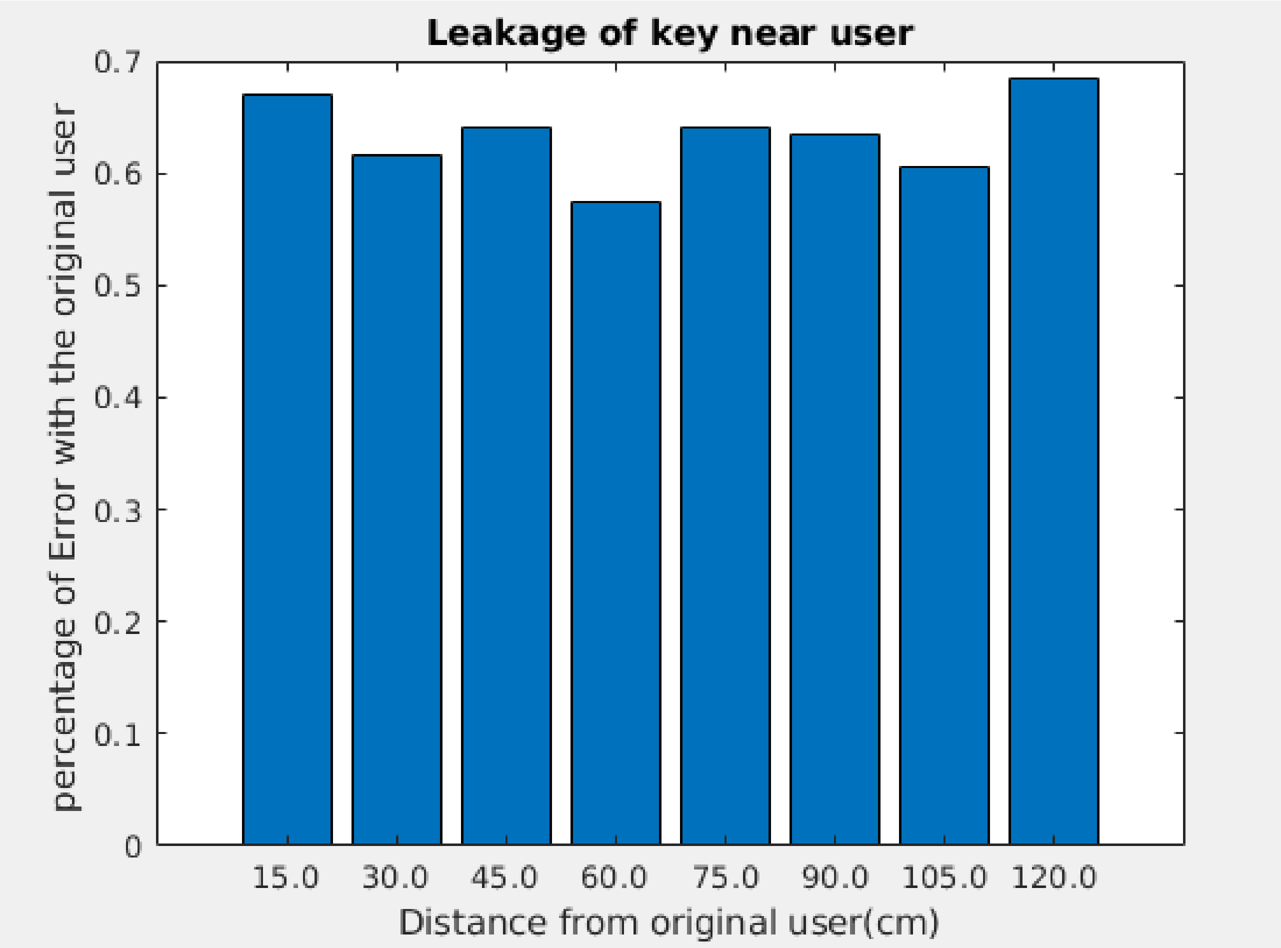

CSI DATASET-7 Key-62d56b1e109b0468110f6cf24ca75298a4869c0db3efca43424480df96554f93
Magnitude
No. of packets


CSI DATASET-8 Key-afd9e7f3b9a0cad7b208ce72b3cf0a85770d447f8ab4384376cd2e2cac295951
Magnitude
No. of packets


CSI DATASET-9 Key-fda48b0a177dd389afdbe33bed796bcf7a898ea533882cb4b66b528a35252b33
Magnitude
No. of packets

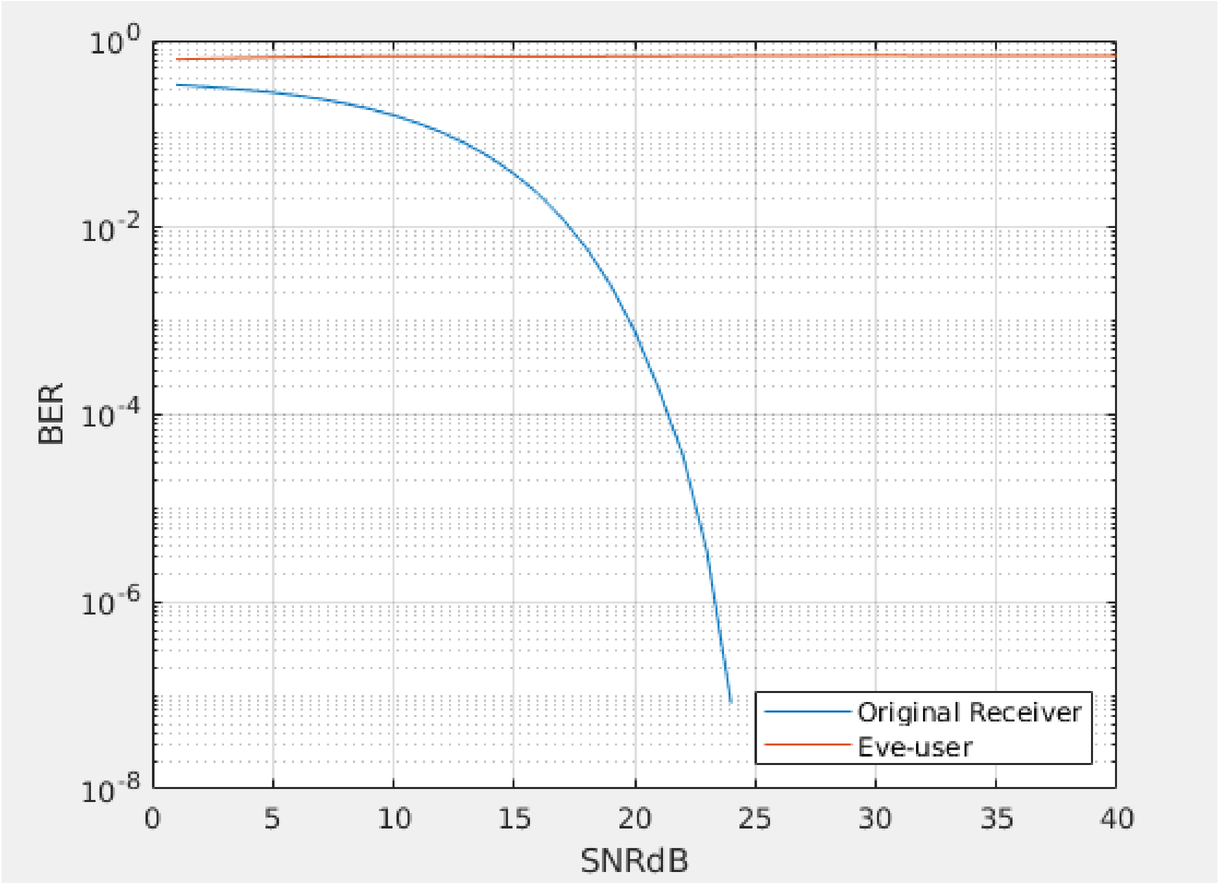
PERFORMANCE METRICS

LEAKAGE RATE



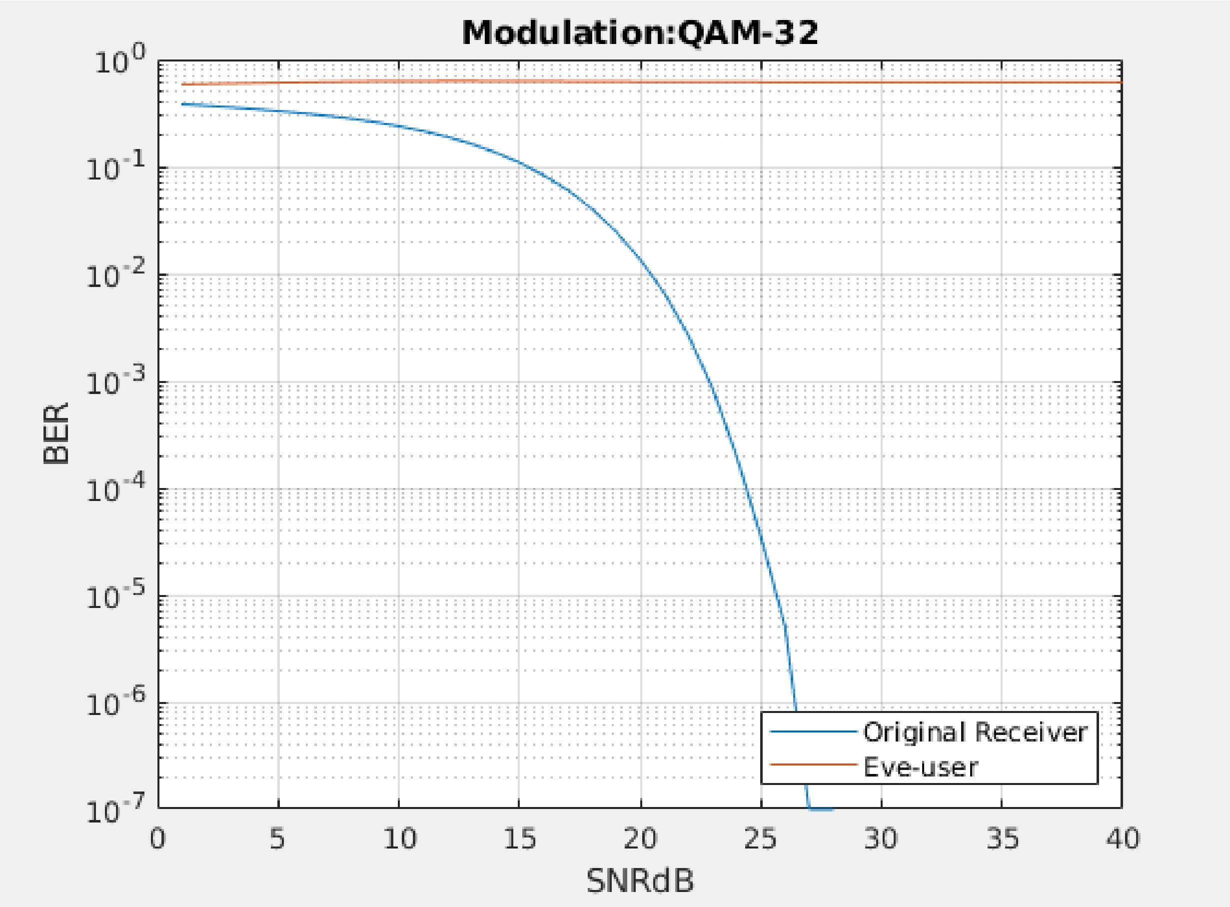
BER PERFORMANCE OF DIFFERENT MODULATION SCHEMES

QAM-16



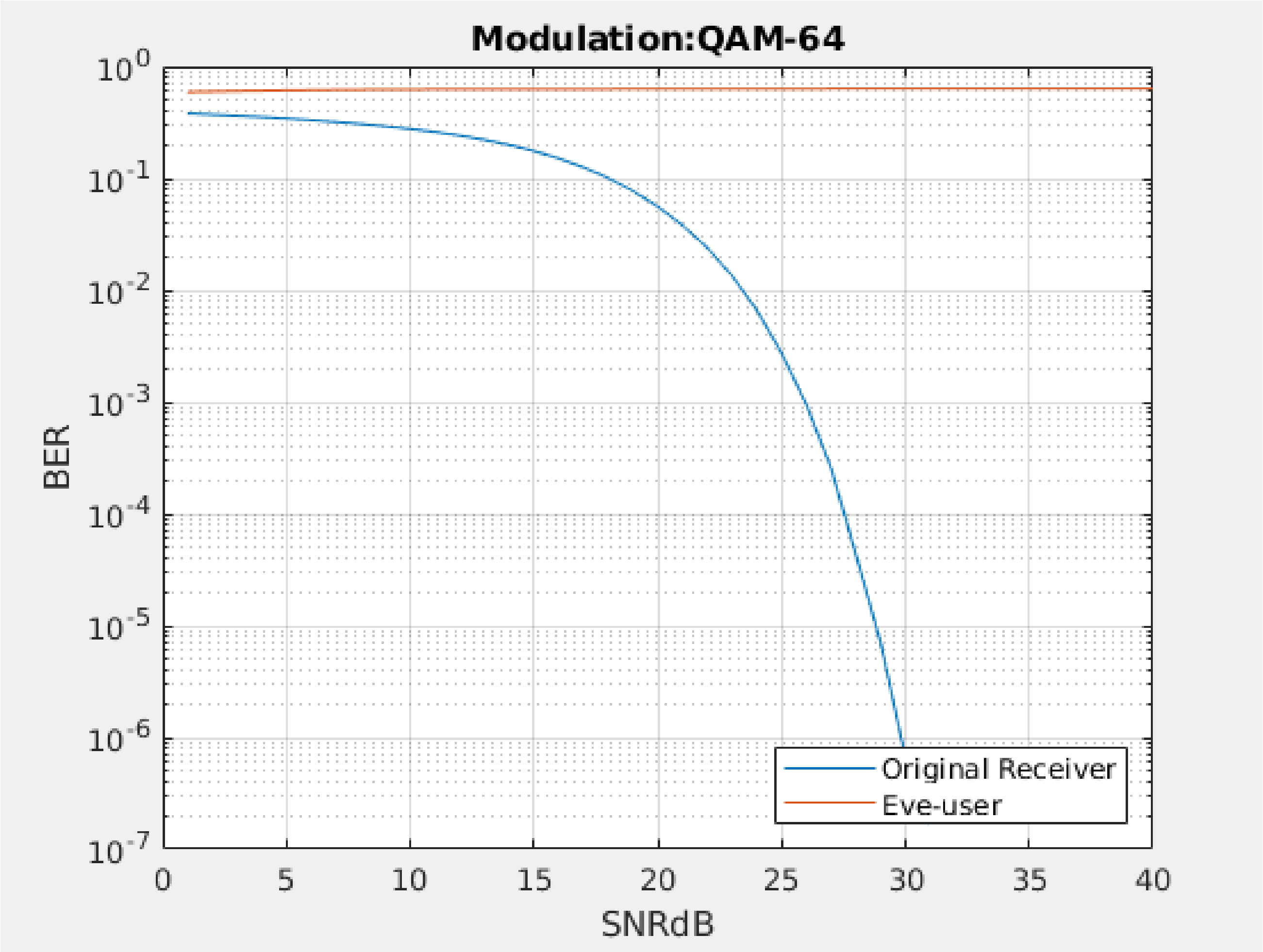
BER PERFORMANCE OF DIFFERENT MODULATION SCHEMES

QAM-32

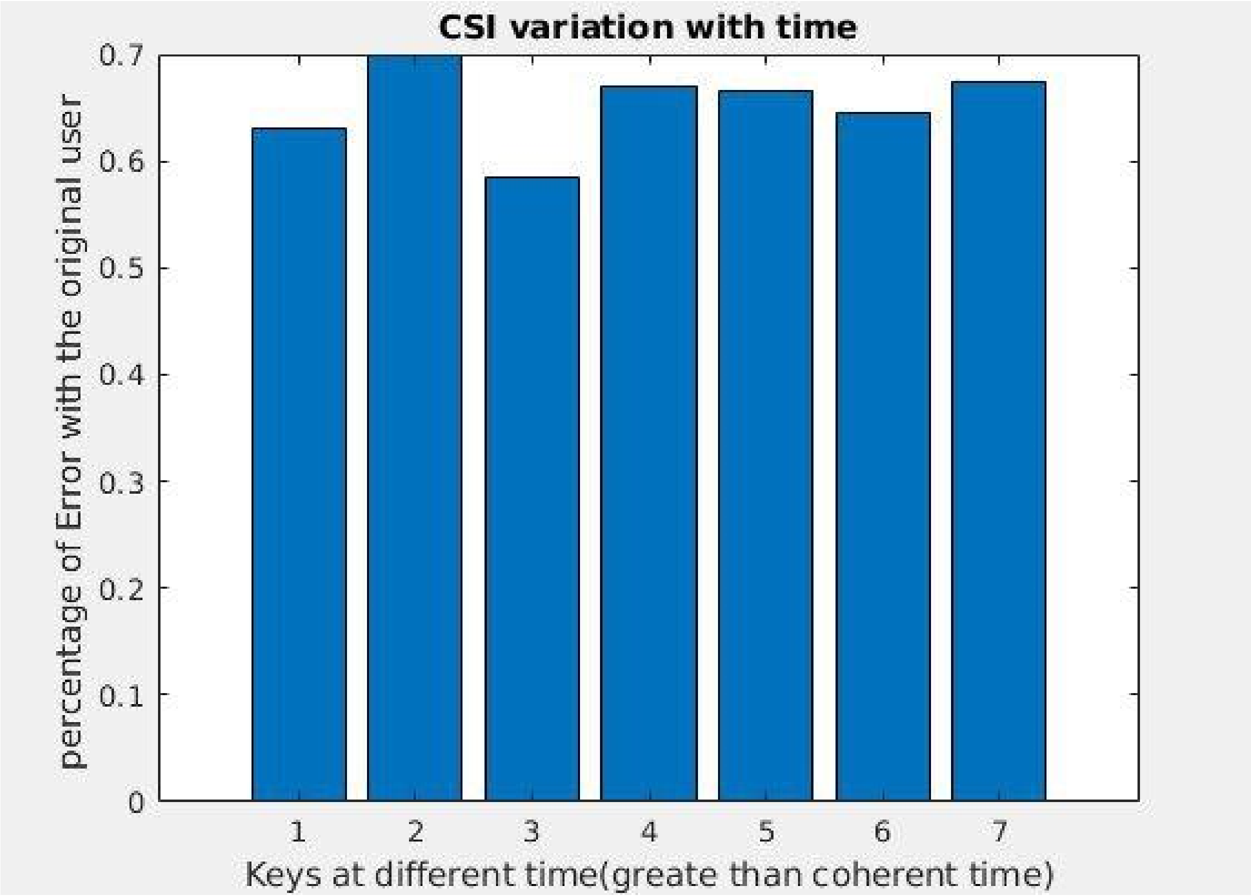


BER PERFORMANCE OF DIFFERENT MODULATION SCHEMES

QAM-64



KEY VARIATION WITH TIME



REFERENCES

- **Physical Layer Security for the Internet of Things** by Junqing Zhang, Sekhar Rajendran, Zhi Sun, Member, IEEE, Roger Woods, Senior Member, IEEE, and Lajos Hanzo, Fellow, IEEE. Published in: IEEE Wireless Communications (Volume:26, Issue: 5, October 2019)
- **Key Generation From Wireless Channels: A Review** by Junqing Zhang, Trung Q. Duong, (Senior Member, IEEE), Alan Marshall, (Senior Member, IEEE), and Roger Woods, (Senior Member, IEEE) 2016. Published in: IEEE Access (Vol. 4)
- **Wireless Physical Layer Identification : Modeling and Validation**, by W.Wang, Z.Sun, S. Piao, B. Zhu, and K. Ren, IEEE Trans. Inf. Forensics Security, vol. 11, no. 9, pp. 2091–2106, 2016
- **Efficient and Secure Key Extraction using CSI without Chasing down Errors**

Jizhong Zhao, Wei Xi, Jinsong Han, Shaojie Tang, Xiangyang Li, Yunhao Liu, Yihong Gong, Zehua Zhou