PROGRESS AFTER FIRST REVIEW

METHODOLOGY

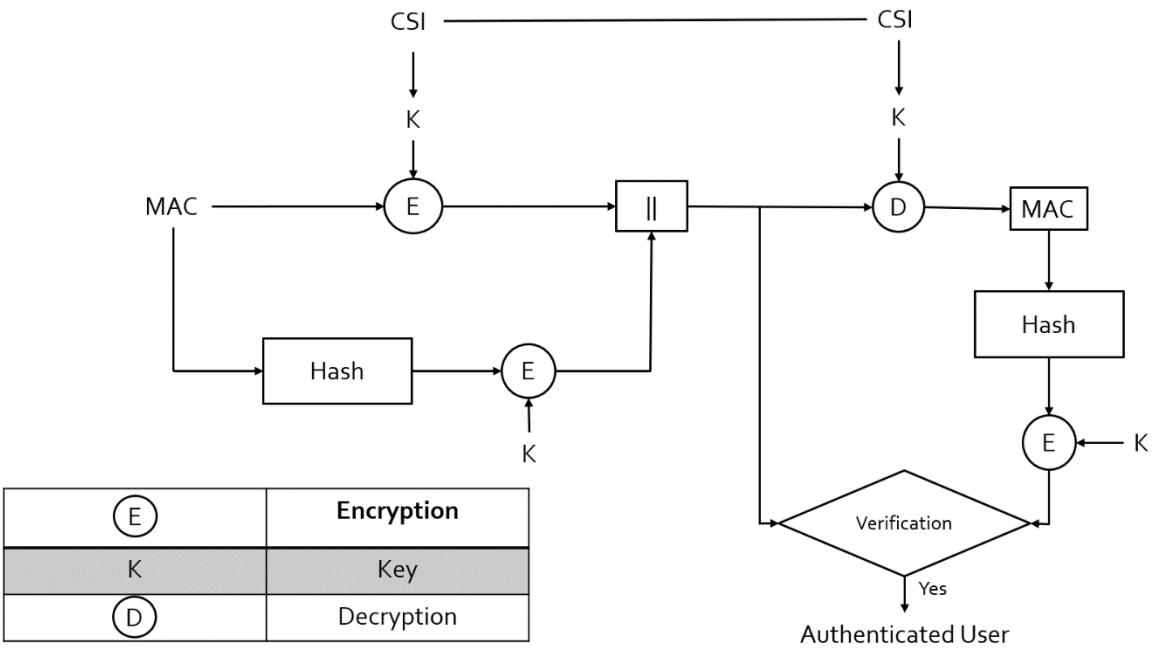


Figure 1 : Proposed methodology of authentication protocol

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

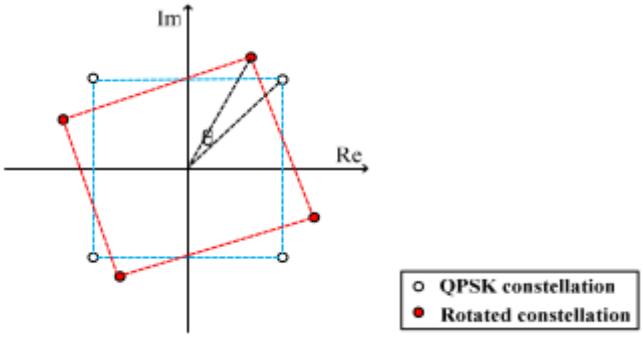


Figure 2 : QPSK Constellation and possible rotation

PHASE CALCULATION

The phase calculation is used to generate an unique angle α with respect to the generated key. The 256 bit key is split into 8 bit words to find 32 phases α.

Figure 3: Representation of the 8-bit word from the 256-bit key

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

QUADRANT BITS

a_1	a_2

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

$$base = i \times 90$$

SIGN BIT

b

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, called the **magnitude 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.

BER PERFORMANCE

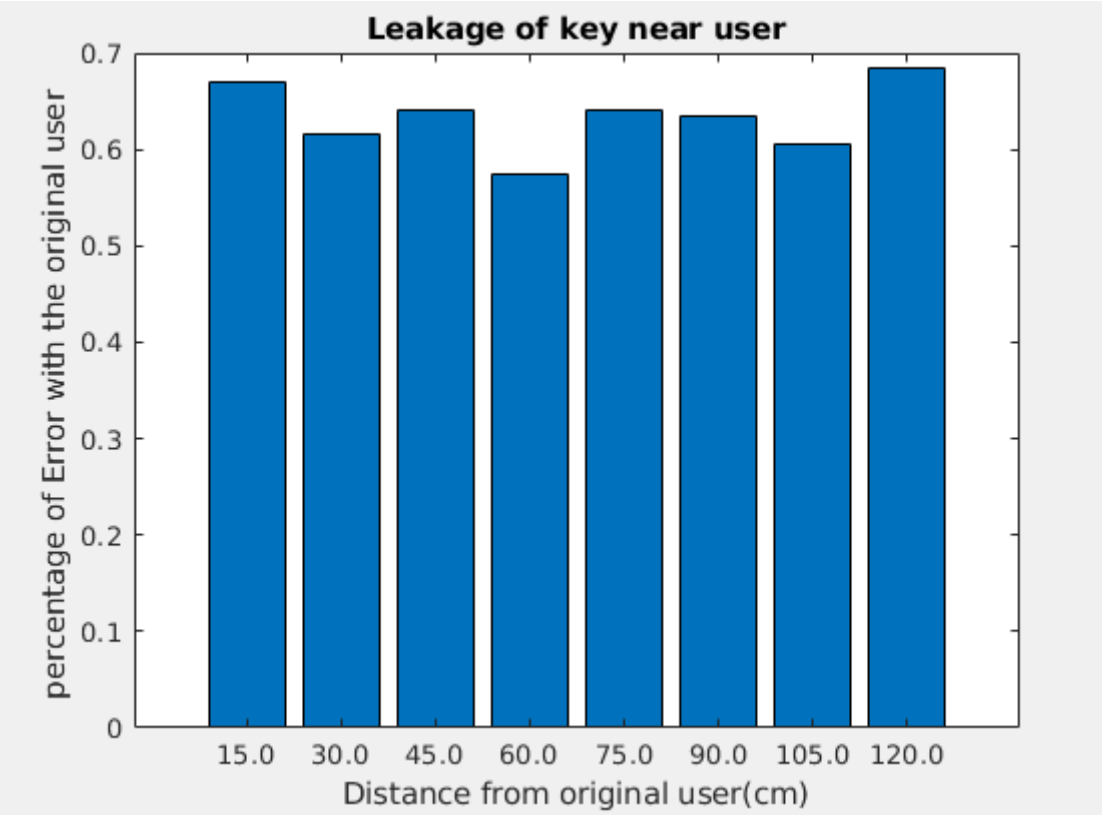
The **bit error ratio** (also **BER**) is the number of bit errors divided by the total number of transferred bits during a time interval. The evaluations show that the bit error decreases with an increase in SNR for the intended user but the bit error remains constant even with an increase in SNR for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

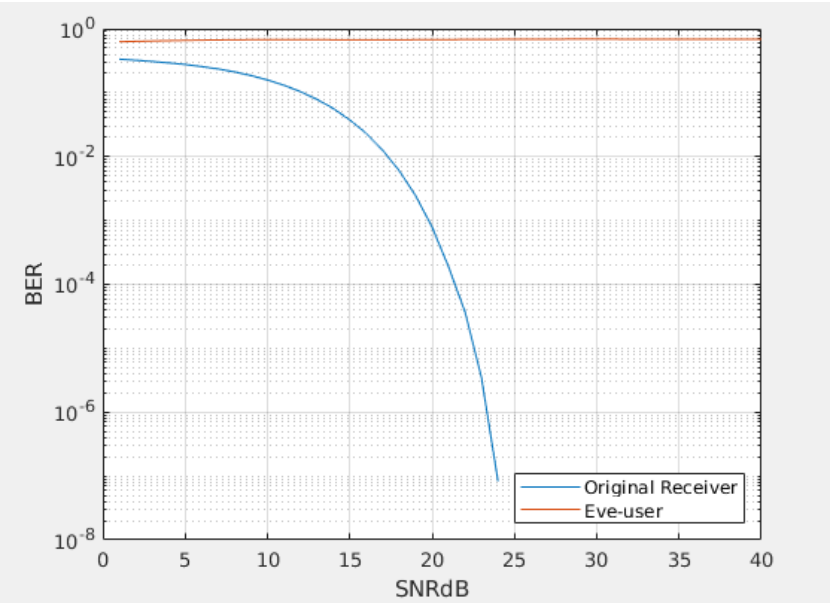
RESULTS

LEAKAGE RATE

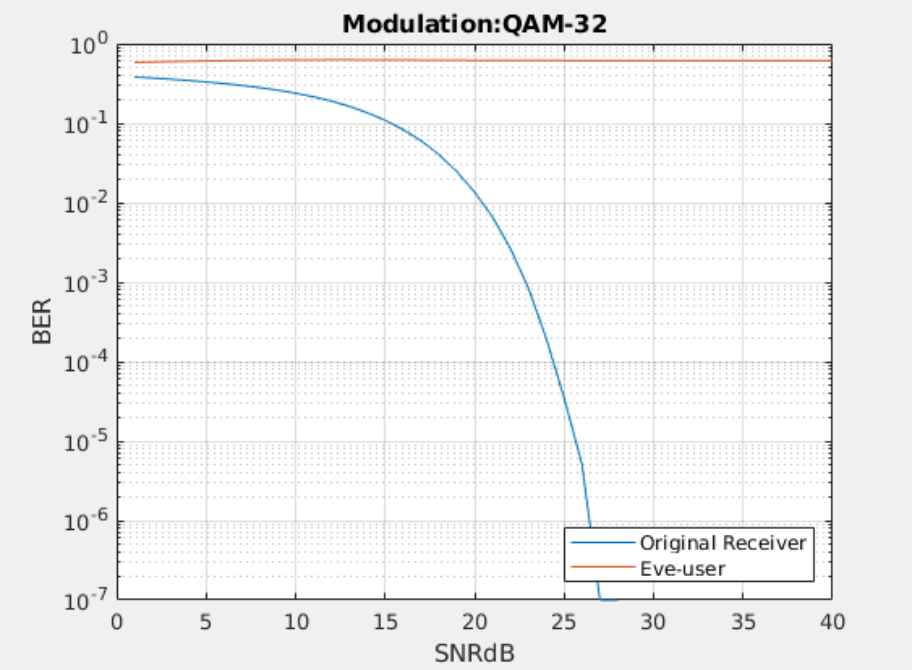


BER PERFORMANCE OF VARIOUS MODULATION TECHNIQUES

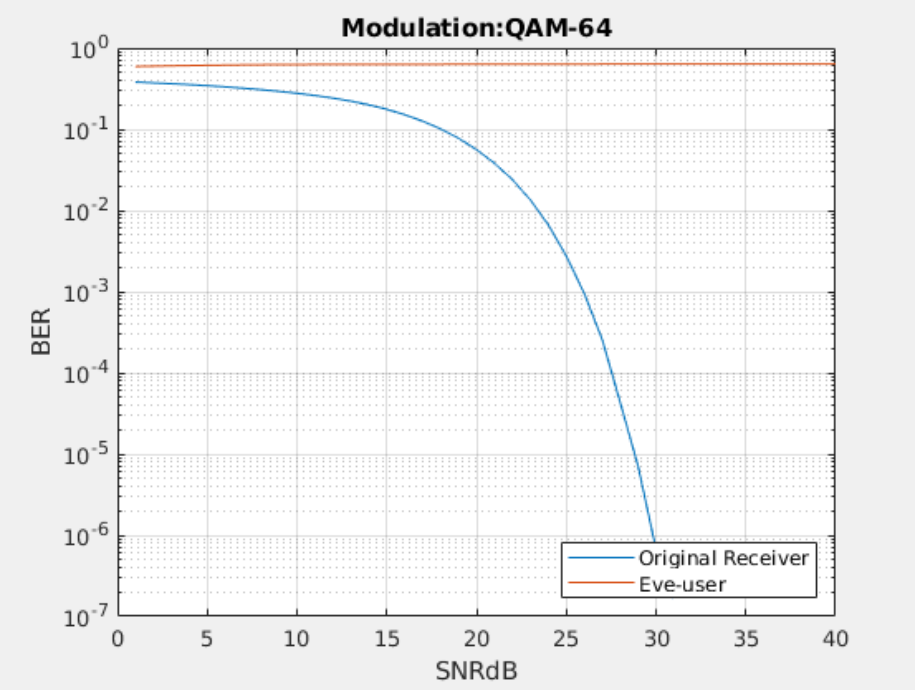
QAM-16



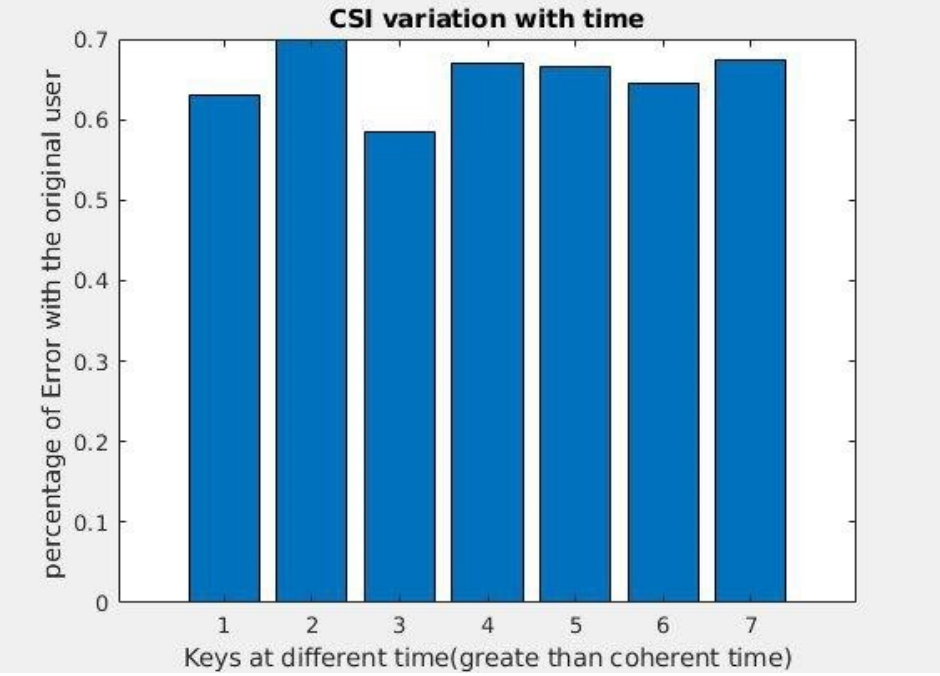
QAM-32



QAM-64



KEY VARIATION WITH TIME



.