SECURITY IMPROVISATION USING MODIFIED CRYPTOGRAPHIC ALGORITHMS FOR NON-ORTHOGONAL MULTIPLE ACCESS(NOMA) TECHNIQUES

Praseetha S[1], Velmurugan R[2], Vengadesh K[3], Vigneshwaran S[4], Surya V[5]

[1]Assistant Professor
Department of Electronics and Communication Engineering
Sri Krishna College of Engineering & Technology, Coimbatore
praseethas@skcet.ac.in

[2]U.G Scholar
Department of Electronics and Communication Engineering
Sri Krishna College of Engineering and Technology, Coimbatore
19euec171@skcet.ac.in

[3]U.G Scholar
Department of Electronics and Communication Engineering
Sri Krishna College of Engineering and Technology, Coimbatore
19euec172@skcet.ac.in

[4]U.G Scholar
Department of Electronics and Communication Engineering
Sri Krishna College of Engineering and Technology, Coimbatore
19euec175@skcet.ac.in

[5]U.G Scholar
Department of Electronics and Communication Engineering
Sri Krishna College of Engineering and Technology, Coimbatore
19euec156@skcet.ac.in

Abstract

The attention of researchers is getting drifted toward NOMA, due to its efficiency in spectral usage, low latency, etc. Many believe that OMA cannot be further relied on. With the increased number of users, we need a better system- better than OMA. Although active development is done in the development of NOMA, security in the PLS remains an issue. The proposed work explains how this situation can be tackled using cryptographic algorithms.

Keywords: *OMA, OFDMA, NOMA, Security, Communication*

1. Introduction

It is expected that more than 29 billion devices will be accessing the internet by the year 2030. [8] Data traffic, latency, etc., will become a great issue with that many devices. The current OMA can't do the job. Despite the advantages like better SNR, it does have some disadvantages (which are discussed later in this paper). Thus, a better scheme is required that can handle large traffic. NOMA is one of the promising candidates for this job. This paper discusses how NOMA is preferable to OMA and further advancements that can be done to improve the former.

2. NOMA's Predecessor:

To understand NOMA, one must first understand its predecessor i.e., OFDMA. In OFDMA, users are allocated by both time and frequency. The OFDM stands for Orthogonal Frequency Division Multiplexing (A is for Access). In the process of FDM, the entire bandwidth is divided into a set of frequency bands. To avoid Inter Symbol Interference, they use Guard bands- a range of frequencies that separate the subcarriers. These subcarriers are multiplexed at the transmission end and transmitted over a single channel thus allowing multiple users' information to be sent simultaneously.

Though this process seems fair, they have many disadvantages. One of them is the inefficient usage of bandwidth. Guard bands might not seem like a lot but when the number of users increases, so does the guard band. Since guard bands don't carry any information, this ends up wasting the bandwidth. To avoid this Orthogonal scheme was introduced. This scheme divides the bandwidth among the users into several parts. The division is such that the frequencies are orthogonal to each other. Two frequencies are said to be orthogonal if their inner product is zero.

$$\int_{t1}^{t2} x_i(t)x_j(t)dt = 0 \ \ where\ i \ \neq j \qquad (1)$$

This would mean that no signal could interfere with each other. This would mean the ISI is theoretically zero. This eliminates the need for guard bands. Thus, the overall bandwidth is conserved by exploiting the orthogonality principle.

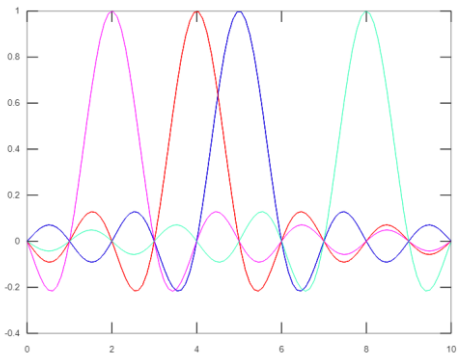

Fig1: Multiple Orthogonal Signals in a lossless typical OFDM System

As seen, even though many signals overlap when at the maximum value of a particular sinc, no other signal is maximum.

2.1. Disadvantages of OFDM:

The following are some of the major disadvantages of OFDM:

a) The PAPR (Peak to Average Power Ratio) is high in the case of OFDM. Hence large amplitude variations can create high noise. The lower the PAPR, the better the system.[10][11].
b) Sensitive to Doppler shift, and frequency sync problems [9].
c) High sensitivity to Carrier Frequency Offsets (CFO) [12].

3. NOMA (SIC)- Working:

Although orthogonality almost reduces the ISI and has much more advantages, when the number of users increases, OFDMA cannot be used. This is why the researchers are on the lookout for a good modulation technique. Next to OFDMA, NOMA seems to be the best [13]. Let's discuss how NOMA works in brief.

Say there are two users in the cell. These two users might be one of the following categories:

a) A is a video streaming device while B is just a normal device
b) Vice versa of (a)
c) A is farther away from the signal tower than B (i.e.) a cell edge user.
d) Vice versa of (c).

Now in normal system, all users are treated the same. But NOMA picks the user and treats it specially. Say we are in a situation (d)/(b). In the chosen situation user B can be prioritized. Under OMA, user A and user B would receive the following signals:

$$y_1 = c_1 p r_1 + w_1 \quad (2)$$

$$y_2 = c_2 p r_2 + w_2 \quad (3)$$

$(c_i - channel, r_i - received\ signal, p - power, w - noise)$

Respectively.

They would be transmitted with the same power. In NOMA though, the signals are superposed on each other. This means, all the signals are modulated and added at the transmitter end. At the receiver end, B is given more power (as per our assumption above). So $p_2 > p_1$. B now receives the following:

$$y_2 = c_2(p_1 r_1 + p_2 r_2) + w_2 \quad (4)$$

(c_2 because the message traveled through the channel corresponding to user 2).

$$y_2 = c_2 p_1 r_1 + c_2 p_2 r_2 + w_2 \quad (5)$$

since $p_2 > p_1$, the two terms viz. $(c_2 p_1 r_2)$ and (w_2) can be considered as noise. The equation is now modified as:

$$y_2 = c_2 p_2 r_1 + w_2' \quad (6)$$

where w_2' is the noise to be removed.
But for user A, the equation is as follows:

$$y_1 = c_1(p_1 r_1 + p_2 r_2) + w_1 \quad (7)$$
$$y_1 = c_1 p_1 r_1 + c_1 p_2 r_2 + w_1 \quad (8)$$

Since $p_2 > p_1$, $c_1 p_2 r_2$ cannot be considered as noise.
Hence, user A has to decode what subscript base, c sub 1 , p , end base , sub 2 , r sub 2 is. It now estimates what this value is and subtracts it from the received signal:

$$y_1 = c_1 p_1 r_1 + c_1 p_2 r_2 + w_1 - c_1 p_2 \hat{r}_2 \quad (9)$$

where $\hat{r}_2$ is the estimate of the r_2.
This process is called Successive Interference Cancellation (SIC). If the estimation is good, then the equation will now become:

$$y_1 = c_1 p_1 r_1 + w_1 \quad (10)$$

Shannon's Capacity equation tells that:

$$R < log_2\left(1 + \frac{P}{N_0}\right) \quad (11)$$

$$R - rate, P - power, N_0 - noise$$

Extending this to NOMA,

$$R_2 < log_2\left(\frac{P_2}{N_0 + P_1}\right) \text{ and } R_1 < log_2\left(\frac{P_1}{N_0 + P_2}\right) \quad (12)$$

If the detection and decoding is successful, then from the user's point of view, there's only one person transmitting. Thus, an increased rate pair than the one obtained in OMA is observed. This is how SIC works and how NOMA can be superior to OMA.

3.1. Limitations of SIC:

SIC works in the following way:
Step1: The signal is received from the signal tower.
Step2: The strongest signal is first decoded.

Step3: After decoding, the result of the step2 is subtracted from the received signal.
Step4: Repeat steps 2 and 3 until the desired signal is obtained.

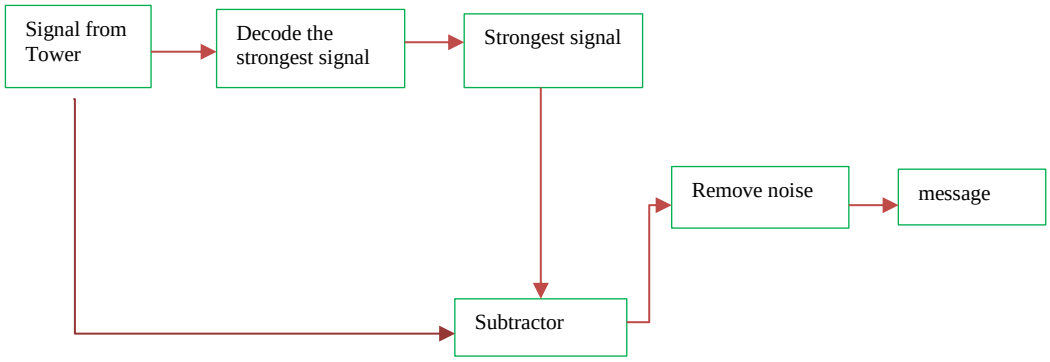

Fig 2: Block Diagram of SIC in a hypothetical 2-user NOMA system

The signals are detected and decoded successively one after another; which is why it is named Successive Interference Cancellation.

The following conclusions can be arrived at from the above explanations:
a) Say there are n users in a network. Now user k is performing SIC in his system. The algorithm successfully decoded the first m signals and while doing so k made a small error in m^{th} signal. Now all the $m - n$ decoding k does will be faulty.
b) The process is complicated and time-consuming.
c) Higher complexity implies higher computation. Higher computation implies higher power consumption.
d) Each time while decoding a stronger signal, it is nothing but another user's message. This leads to a violation of privacy. (Overcoming this is dealt with in the next section).

4.Enhancing the PLS of NOMA:

As seen in the previous section, if a near user wishes, he can decode not one, but most of the far users' messages sequentially by tweaking the algorithm a little bit.

4.1. MAC and IMEI as crypto keys:

An encryption key is meant to be a secret. In [2], the author proposes that the MAC and IMEI can be used as keys to encrypt the message. Using this scheme is simple, and would work for most of the cases. In this paper, the author handled the security issue quite well.

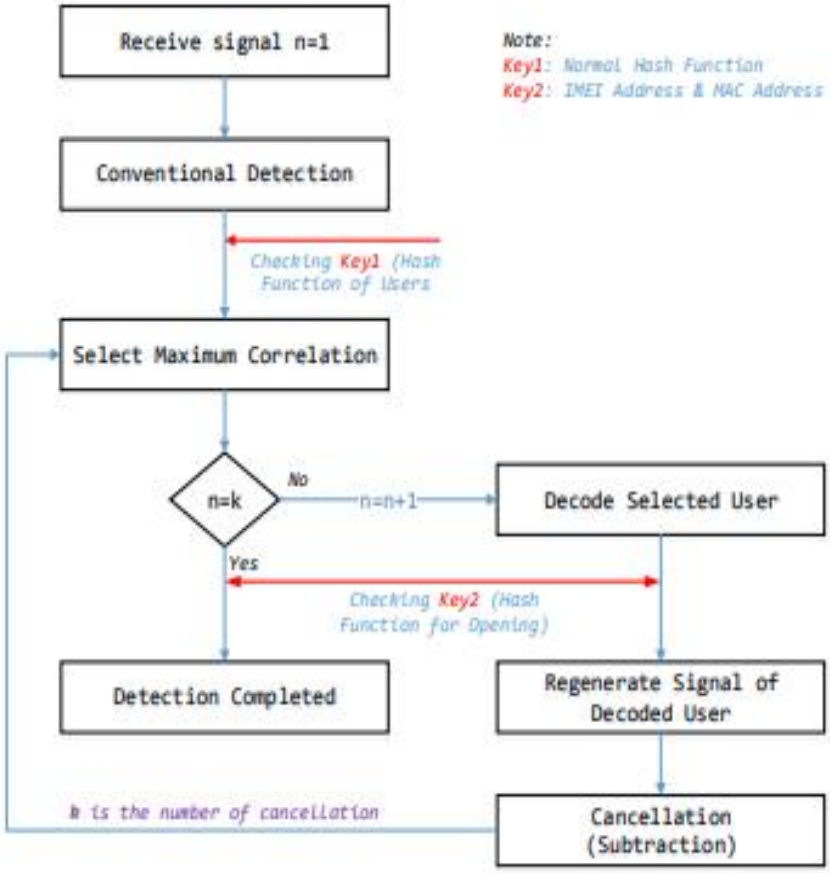

Fig3: Proposed Scheme using MAC and IMEI as keys

After the signal is received, the normal detection is done (decoding strongest signal and such process). Here, the first generated key is applied and checked. If it returns a true response, then the sequential iteration begins and SIC is done until the desired signal is obtained.

Using MAC as a secret crypto key is not good because it is well known that for two devices be it direct device to device or device to the router, the MAC should be shared between them. Hence MAC address of a device cannot be kept as personal.

4.2. Modified AES as an encryption standard:

In [1] the author uses a modified lightweight AES algorithm for voice encryption. In this work, the author removes the usage of the mix column operation and the output is directly taken from the shift-rows operation. This reduces the computation time.

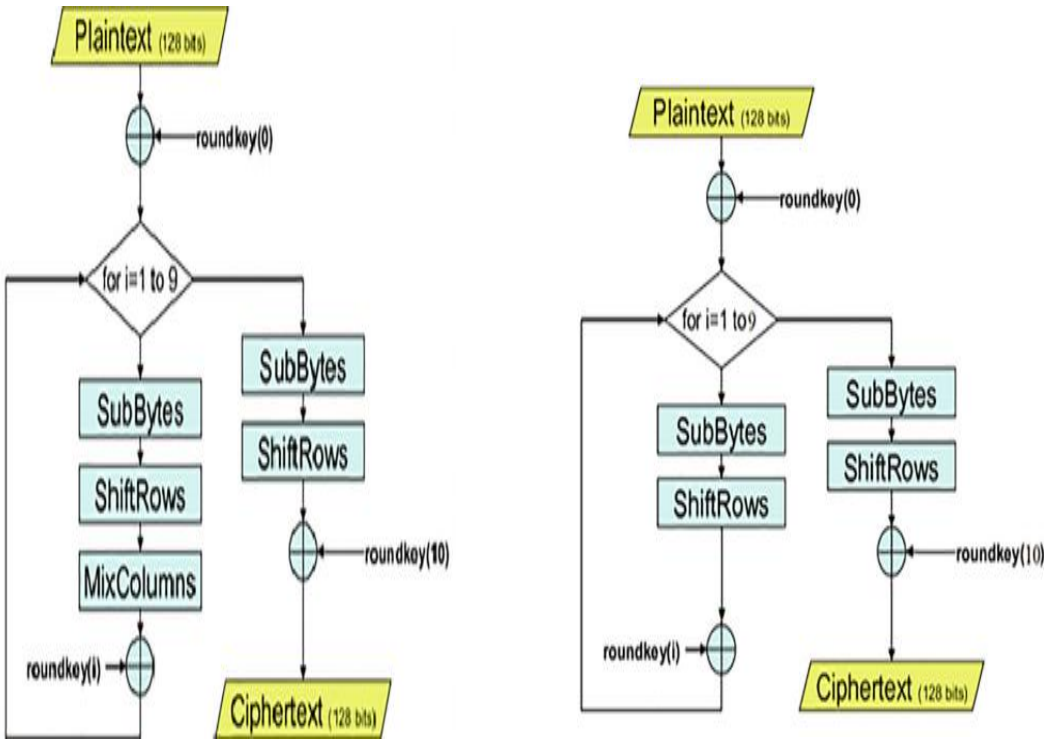

Fig4a: Typical AES **4b: Modified AES**

Upon simulating this modified AES using the VIVADO tool, and analyzation using Artix-7 and Kintex-7 FPGAs, the following features are observed while compared to the traditional AES:

A decrease of

1. 10.67%in setup delay time.
2. 17.34% in hold time (for Artix-7).
3. 58.51% in setup delay time.
4. 64.20% in hold time (for Kintex-7).

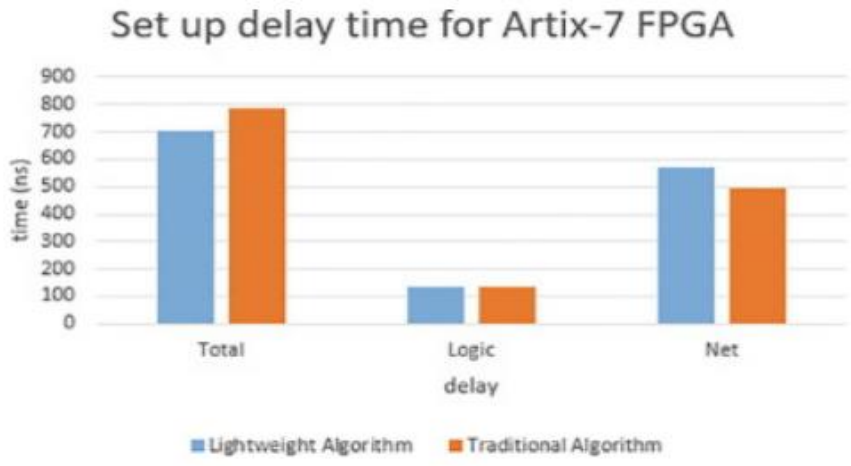

Fig 5: Delay time in the modified AES

This lightweight AES can be used for encrypting the modulated signal. A portion of the safety is traded off in order to achieve fast encryption of voice signals. As said the mix-column feature is removed due to the removal of this feature, one cannot expect the same encryption level as in AES.

4.3. Improved Twofish Algorithm:

The Twofish algorithm is mainly used for encrypting highly confidential data. The key length of this algorithm varies which makes it even harder to crack. But the downside is that Twofish takes up more time to run.

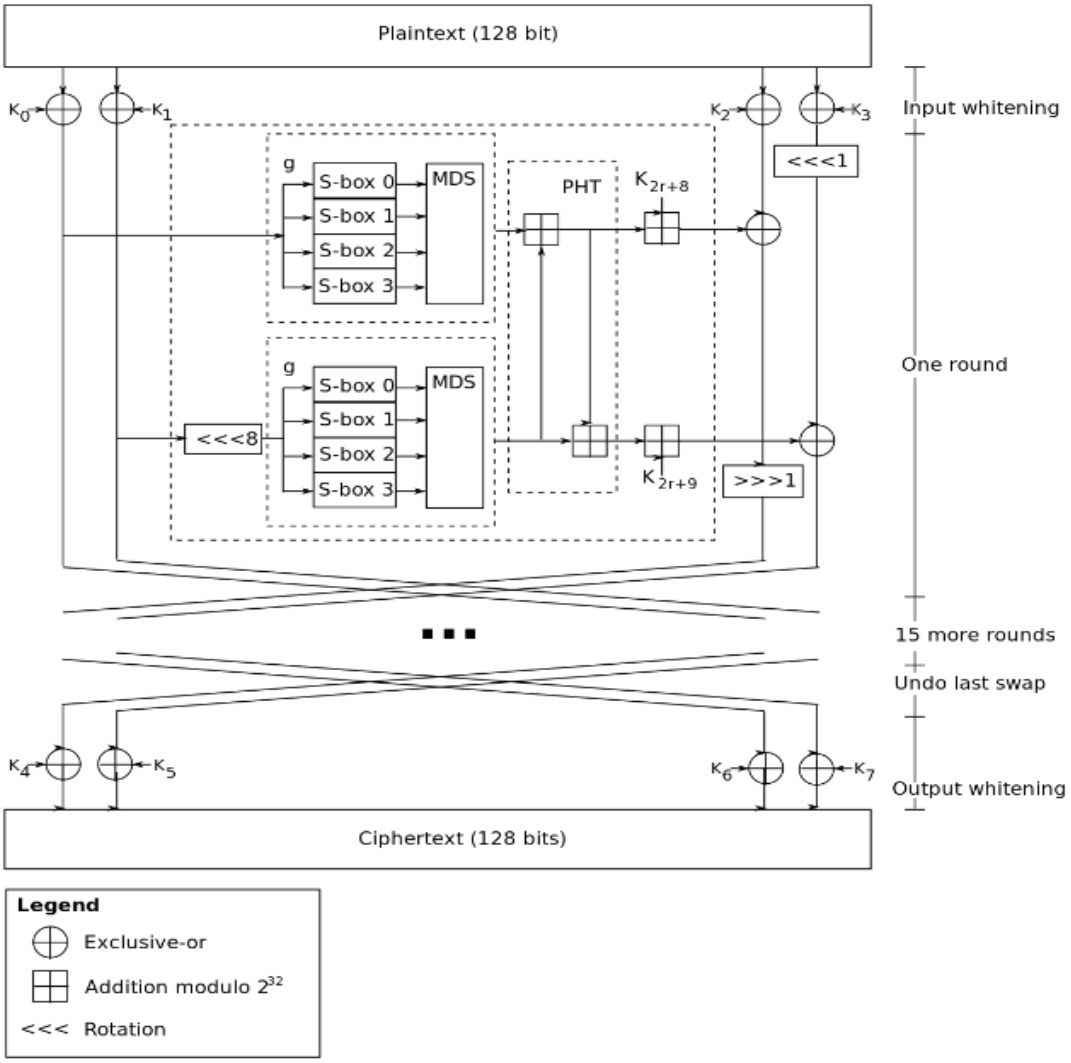

Fig6: Block Diagram of Twofish algorithm

In [15], the author proposes two lightweight versions of the Twofish algorithm. This lightweight version based on NIST training is faster than the original algorithm. In this work ([15]), the authors modify the F-Function using the tech of Present algorithm. This is used to make the former faster, securer and memory efficient.

A complex hash function can be generated for this purpose and a secret key could be randomly generated and shared. Like AES the key could be long and complex and can be run multiple times to increase the strength.

4.4. Proposed System:

At the transmitter side, encryption has to be done at two stages:

a) One for identifying the signal during the SIC process,
b) Another for encrypting the actual signal.

The flow is as follows:

1. The message signal is as usual modulated using suitable scheme say QAM.
2. The conventional processing is done.
3. An algorithm of choice (as mentioned in the former sections) with suitable parameters (low run-time, better security, etc) is used to generate first key.
4. The key is xor-ed with the signal while second key is generated.
5. Like step 4, the second key is also xor-ed. The signal is power amplified and aired.
6. The superposed signal is received and strongest signal is decoded first. The appropriate signal is chosen using the first generated key.
7. Using the second key, the message is decoded.

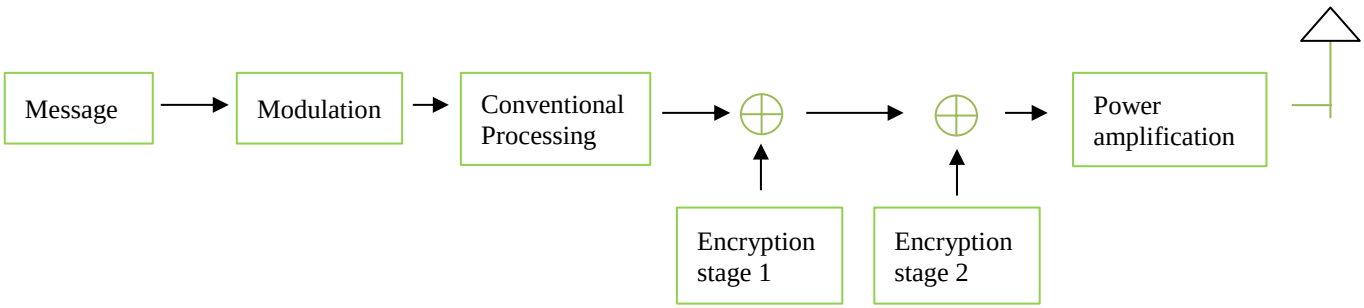

Fig7: Improved uplink side

The stage one encryption is solely for the faster identification of the signal and play little to no part in the security. Hence it can be one to few rounds. This trade off can reduce the delay time.

Conclusion:

In this paper, an introduction to the OFDM is given to understand the process of NOMA and why it is needed. Furthermore, the SIC is also explained and its disadvantages were briefed. Security and privacy being one of the most important concerns is elaborated and solutions to overcome them were also discussed.

Acknowledgement:

We thank the supervisor who guided us all along this work. We also thank our college who was the driving force for this work.

References

The following papers were referred for this work and were of great help.

[1]. *Keshav Kumar, K.R. Ramkumar, Amanpreet Kaur, "A lightweight AES algorithm implementation for encrypting voice messages using field programmable gate arrays" https://DOI.org/10.1016/j.jksuci.2020.08.005.*

[2]. *G. B. Satrya and S. Y. Shin, "Security enhancement to successive interference cancellation algorithm for non-orthogonal multiple access (NOMA)," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017, pp. 1-5, DOI: 10.1109/PIMRC.2017.8292165.*

[3]. *Melki, R., Noura, H.N. & Chehab, A. Physical layer security for NOMA: limitations, issues, and recommendations. Ann. Telecommun. **76**, 375–397 (2021).*

[4]. *B. M. ElHalawany and K. Wu, "Physical-Layer Security of NOMA Systems Under Untrusted Users," 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1-6, DOI: 10.1109/GLOCOM.2018.8647889.*

[5]. *W. Kabir, "Orthogonal Frequency Division Multiplexing (OFDM)," 2008 China-Japan Joint Microwave Conference, 2008, pp. 178-184, DOI: 10.1109/CJMW.2008.4772401.*

[6]. *Yong Soo Cho; Jaekwon Kim; Won Young Yang; Chung G. Kang, "Introduction to OFDM," in MIMO-OFDM Wireless Communications with MATLAB®, IEEE, 2010, pp.111-151, DOI: 10.1002/9780470825631.ch4.*

[7]. *Furqan, Muhammad & Hamamreh, J. M. & Arslan, Huseyin. (2019). Physical Layer Security for NOMA: Requirements, Merits, Challenges, and Recommendations.*

[8]. *S. S. Prasad, C. K. Shukla, and R. F. Chisab, "Performance analysis of OFDMA in LTE,"* 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), *2012, pp. 1-7, DOI: 10.1109/ICCCNT.2012.6395933.*

[9]. *Y. Zhao and S. . -G. Haggman, "Sensitivity to Doppler shift and carrier frequency errors in OFDM systems-the consequences and solutions," Proceedings of Vehicular Technology Conference - VTC, 1996, pp. 1564-1568 vol.3, DOI: 10.1109/VETEC.1996.504021.*

[10]. *N. Dinur and D. Wulich, "Peak-to-average power ratio in high-order OFDM," in IEEE Transactions on Communications, vol. 49, no. 6, pp. 1063-1072, June 2001, DOI: 10.1109/26.930636.*

[11]. *B. S. Krongold, "PAR Reduction in the Uplink for OFDMA Systems," 2006 IEEE 7th Workshop on Signal Processing Advances in Wireless Communications, 2006, pp. 1-5, DOI: 10.1109/SPAWC.2006.346393.*

[12]. *W. Zhang and J. Lindner, "SINR Analysis for OFDMA Systems with Carrier Frequency Offset," 2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007, pp. 1-5, DOI: 10.1109/PIMRC.2007.4394105.*

[13]. *H. Haci, H. Zhu and J. Wang, "Performance of Non-orthogonal Multiple Access With a Novel Asynchronous Interference Cancellation Technique," in IEEE Transactions on Communications, vol. 65, no. 3, pp. 1319-1335, March 2017, DOI: 10.1109/TCOMM.2016.2640307.*

[14]. *K. T. Augustine and U. Purushotham, "Implementation of AES To Encrypt and Decrypt Speech Using LUT With Mux Gates," 2021 International Conference on Advances in Computing and Communications (ICACC), 2021, pp. 1-6, DOI: 10.1109/ICACC-202152719.2021.9708165.*

[15]. *E. A. Al-Kareem and R. S. Mohammed, "Modify Twofish Algorithm to Lightweight using Present Techniques for Data Protection," 2021 International Conference on Advanced Computer Applications (ACA), 2021, pp. 122-127, DOI: 10.1109/ACA52198.2021.9626819.*

[16]. *Nurdin, A.A., Djuniadi, D. (2022). Securing Audio Chat With Cryptool-Based Twofish Algorithm. In journal of Soft Computing Exploration (Vol. 3, Issue 1, pp. 37-43). Surya Hijau Manfaat. https://doi.org/10.52465/joscex.v3i1.65.*