A Novel Encrypted High Frequency FSK Modulation Technique Powered by Microwave Gunn Oscillator

Prashnatita Pal

October 23, 2024

A Novel Encrypted High Frequency FSK Modulation Technique Powered by Microwave Gunn Oscillator

Prashnatita Pal[1]*,
[1],[2]Electronics & Communication Engineering, STCET
*Corresponding Author & Email: prashnatitap@gmail.com

Abstract: **The use of frequency shift keying (FSK) is a popular digital modulation method in contemporary communication systems for effectively transferring digital data across microwave frequencies. The abstract goes through the procedures needed in creating asymmetric cryptosystem like Modified and Optimized RSA (MORSA) encrypted FSK employing the Gunn oscillator, emphasizing the importance of putting the oscillation device in a waveguide. The waveguide serves as a guided transmission medium for appropriately directing and transporting the produced microwaves, enabling efficient data transmission. Second, the main challenge for all data transmission infrastructure types is providing a secure connection. For safeguarded communication, many data encryption methods are used. The selection of a suitable combination of encryption and modulation algorithms may enhance simultaneously the confidentiality level. The suggested Gunn-based FSK modulation technology, along with the MORSA encryption algorithm, offers a high degree of security as well as signal quality. The suggested technique's performance has been experimentally validated.**

Keywords — High Frequency, MORSA algorithm, FSK modulation, Gunn Oscillator

1. INTRODUCTION

In the digital age, secure communication is a critical requirement to safeguard sensitive information from unauthorized access and potential cyber threats. Encryption techniques play a pivotal role in ensuring data confidentiality and integrity during transmission. Among various encryption methods, the RSA (Rivest–Shamir–Adleman) algorithm stands out as a widely used and robust public-key cryptographic system. However, the computational complexity of RSA encryption can

lead to significant processing overhead, especially in resource-constrained environments. This paper presents a novel approach to address the challenges posed by traditional RSA encryption in microwave communication systems. We propose a modified and optimized RSA encryption scheme, specifically. tailored for FSK (Frequency Shift Keying) generation using a Gunn oscillator. The Gunn oscillator, based on the Gunn Effect in semiconductor materials, is a versatile and efficient source of microwave signals, ideal for data transmission in various communication applications. The introduction begins by emphasizing the importance of secure communication and the increasing demand for efficient encryption methods in the face of emerging cyber threats. We highlight the limitations of conventional RSA encryption and its potential impact on microwave communication systems, especially in scenarios where real-time processing and low-latency transmission are critical. Next, we provide an overview of FSK modulation and the principles of the Gunn oscillator, demonstrating their suitability for microwave data transmission. We then introduce the modified and optimized RSA encryption scheme, which aims to mitigate the computational burden while maintaining the desired level of security.

In conclusion, the proposed modified and optimized RSA encrypted FSK generation using the Gunn oscillator offers a compelling solution for secure microwave data transmission. By leveraging the efficiency of the Gunn oscillator and the streamlined RSA encryption, our approach enables secure communication in resource-constrained environments without compromising data integrity and privacy. This study opens new avenues for advanced microwave communication systems that strike the right balance between security and performance, making it suitable for applications such as military communications, secure IoT networks, and other confidential data exchanges.

The presentation of a unique methodology of FSK modulation for encrypted data in binary format using a Gunn Oscillator is the paper's innovation.

The remainder of the work is structured as follows. A literature review was conducted in the second phase. The third part introduces the MORSA algorithm. The fourth part discusses the theoretical ideas of the FSK generator, which employs a Gunn oscillator. The fifth part describes the experimental setup. Finally, the study finishes with several key remarks about confidential interaction and opportunities in the future.

2. LITERATURE SURVEY

Despite producing a single spectrum output as expected, waveguide-mounted Gunn oscillating devices have been the subject of much investigation throughout the years [1]. Naturally, the Vander Pol [2] oscillators concept was employed to analyze the behavior of the Gunn oscillator, resulting in the device being modeled with a nonlinear negative conductivity. Later, it was revealed that frequency had an impact on the I-V characteristics. Most studies concentrate on the oscillator's fundamental mode, however, other works [3,4] emphasize the second harmonic generation of a Gunn oscillating device. However, the various anharmonic spectrum patterns of oscillations at the fundamental frequency have not been recorded, nor have the reasons for this oscillator activity.

3. OVERVIEW OF MORSA

3.1 Origin of MORSA

Modified and Optimized RSA Cryptosystem (MORSA) designed [5] to bolster the encryption process and protect sensitive information from sophisticated cyber threats. The proposed MORSA integrates several advancements that address the weaknesses inherent in the original RSA algorithm. Firstly, the MORSA algorithm incorporates an enhanced key generation process, ensuring that the generated keys are significantly larger and resistant to modern cryptographic attacks, such as brute force and factoring methods. Additionally, the new key generation technique reduces the overhead associated with key size, making it more feasible for resource-constrained devices to utilize strong encryption. This optimization mitigates the performance bottlenecks observed in traditional RSA due to the high computational complexity involved in prime number generation.

4. FSK GENERATION USING MICROWAVE GUNN OSCILLATOR

a. Frequency-shift keying (FSK)

Frequency-shift keying (FSK) is a digital modulation method that communicates dual information by shifting the discrete frequency that serves as the carrier signal [5]. FSK modulation technique is employed in a variety of current communication systems such as cell phone communication, emergency broadcasts, and so on. The BFSK system is the most basic variant of the FSK technology. Binary data (0s and 1s) is communicated as a discrete frequency model in the BFSK system. The binary digits '0' represent space frequency and '1' represent mark frequency.

b. Microwave Gunn Ocillator

The Gunn oscillator is a type of semiconductor microwave oscillator that generates microwaves in the frequency range of about 1 to 100 GHz. It operates based on the Gunn Effect, which was discovered by physicist J.B. Gunn in 1963. The frequency versus output power characteristics of a Gunn oscillator (shown in fig 2) can be understood by considering the device's operating regions and limitations. The key aspects influencing these characteristics are the Gunn Effect, domain formation, and the device's resonant cavity.

In the domain formation region, the electron domains move through the semiconductor material, leading to the generation of microwave power. The output power increases with the bias voltage applied across the device, reaching a peak at a specific voltage level. Beyond this point, the output power starts to decrease due to various effects, such as domain instabilities and heating. It's essential to avoid operating the Gunn oscillator at voltages beyond the peak output power to prevent device failure and thermal damage. Additionally, output power can be influenced by the device's thermal characteristics, as excessive heating can reduce the efficiency and reliability of the oscillator. A D.C. voltage can be supplied to the diode through a further Gunn biased voltage (of exceptionally high value). Consequently, we arrange for an average voltage across the Gunn diode V_{bias} to be shown in Figure 3. It is claimed that the diode is biased towards the negative resistivity region. Because voltages (about comparable to V_{bias}) have an elevated dynamic resistance, even tiny variations in the oscillation frequency tend to rise. Because of the oscillation, the diode voltage swings back and forth. As this swing expands, it will ultimately reach the areas were. While inside the area, resistive dissipation tends to diminish the power of any oscillation. The oscillation power tends to rise inside the area. Therefore, the degree of the oscillation typically settles at a level where the amount of energy 'produced' per cycle within the area equals the amount of energy wasted each cycle within the region.

This paper investigated the possibility of synchronous oscillation at anharmonic frequencies within the waveguide-mounted Gunn oscillator based on the experimental results given in Fig. 4. The spectrum demonstrates that oscillations are happening at three frequencies at the same time: 10.400 GHz, 10.407 GHz, and 10.414 GHz.

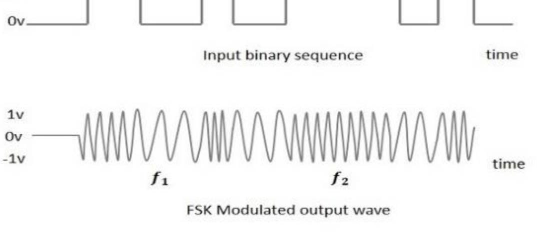

Figure:1. The pattern of the Frequency shift key

5. ALGORITHM OF MORSA ENCRYPTED FSK MODULATION

1. Start
2. Speech samples are recorded using the mobile recorder.
3. Conversion into.wav format for ease.
4. Plotting the amplitude vs. time graph for each of the speech samples in Python.
5. Uploading it into Python for ste13c1t further analysis
6. Voice recognition is done by matching with a reference stored speech keyword database.
7. After a match is found, the spectrograph of the corresponding speech sample is plotted in Python.
8. Speech samples are recorded using the mobile recorder.
9. An MORSA algorithm is applied on noise eliminated signal for encryption of speech signal.
10. Digital signal was then passed through Gunn Oscillator to convert this digital signal into FSK (Frequency Shift Keying) and transmitted to the receiver. [Explain at Section 6]
11. At the receiver, to identify f_1 and f_2, the FSK signal is passed through a coupler which divides the corresponding signal into two parts. These two parts contain frequencies both frequencies f_1 and f_2 in the same phase. [7]
12. The resulting two signals are passed through two different resonating cavities of frequencies of f_1 and f_2 to identify them and then summed up using a circuit to get the original speech signal.
13. MORSA decryption algorithm or any other decryption algorithm (whichever is applied in Step 8) is applied on analog signal for decryption and get back original speech signal which is authenticated in Step 6.
14. Stop

6. THE RELEVANCE OF THE RESEARCH:

The Gunn oscillator, like any other oscillator, is a regenerative system with a limiter-type nonlinear element. A bias choke is used to supply the required bias to the Gunn diode once it has been properly placed in the waveguide cavity, allowing that diode's negative resistance to decrease from -12 to -8 plus the remaining resistance to a value of around -3 at the desired frequency of oscillation. This helps to avoid oscillations in the biassed circuit along with other sorts of oscillation. The diode has a high mechanical tuning range and an oscillation frequency that is 9.64 GHz. The proposed Gunn oscillator's frequency of oscillation can additionally be adjusted using the bias voltage of the Gunn diode. The three distinct frequencies for oscillations were seen through experimentation with frequencies of 10.400 GHz, 10.407 GHz, and 10.414 GHz after proper mechanical tuning and a little change to the biassed voltage of the Gunn diode positioned in the cavity. The details of the experimental results using the spectrum analyzer outputs are reported in Table I. The two nearby peaks are separated by a distance of 61 MHz.The following are the technical requirements for the components and devices. The figure demonstrates that the oscillator's frequency changes practically linearly from 10.425 to 10.400 GHz as the bias voltage varies from 8 to 13 V. As a result, the bias voltage sensitivity of the linear frequency of the employed Microwave Gunn Oscillator is 0.00498 GHz/V in the linear range of operation. Also within the aforementioned range, the Gunn Ocillator strength varies from a minimum of 18.12 dBm to a high of 20.53 dBm. The waveguide's physical dimensions were 2.3 cm in width and 1 cm in height. As a result, its critical wavelength (c=2b) is 4.6 cm. And the guided wavelength (g) in the waveguide for a 0 cm signal would be.

The frequency of a Gunn oscillator can be varied by varying the bias voltage V_B of the diode. Experimental results indicate that the Gunn oscillator frequency, ω_g, can be written as

$$\omega_g = \omega_{go} + k_{\omega b}\,\Delta V_b$$

where ω_{go} indicates the frequency of the Gunn oscillator when $V_B=V_{BO}$, V_{BO} is a fixed bias voltage ΔV_b is the change in bias voltage about V_{BO} and kωb is bias voltage sensitivity of the Gunn oscillator angular frequency.

a. *High-Frequency Shift Keying*

Figure 5 depicts the technique for producing two different frequencies using the Gunn Oscillator for FSK modulation. The Gunn bias voltage of the Gunn Oscillator is adjusted to a certain level and overlaid with the encrypted information in a binary bit in our FSK generating process. It is caused by two separate microwaves frequencies. As with FSK modulation, the negative side reflects binary 'one' while the other alternate side represents 'zeros'. The digital information can be modulated employing the Gunn Oscillator, and the modulation process is shown in Figure 5. The following figure depicts an acceptable form of oscillation in the Biased voltage (8.412v) versus the power output characteristics of a Gunn Oscillator.

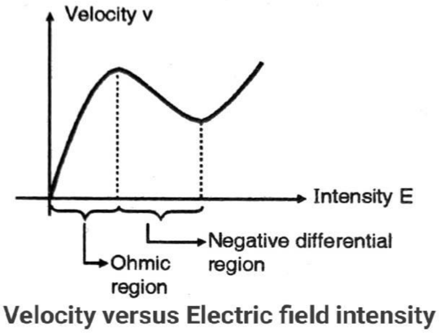

Fig 2. Microwave Gunn Charactaristic

The peak power is determined to be 21 dBm, and the associated frequency is 10.407GHz (Fc). Normally, Fc is the cavity's resonant frequency as well as the frequency of the oscillation created by Gunn

Oscillator. The power output is split into two halves to its 3dB points to have a bigger frequency variation 10.414GHz- 10.400GHz = 14MHz. Corresponding frequencies at 3dB points are f2 and f1, and the frequency deviation is f1 - f2 = fc. The bias voltage is set at Va for the bottom half of the power point and Vb for the top half. The encrypted digital data signal is coupled to the Gunn Oscillator power supply's external modulation mode, thus this digital signal, represented here as a train of periodic rectangular pulses only, is superimposed over the biased voltage-clamped at its negative levels at Va. The digital signal's amplitude is then adjusted to the biased voltage level Vb.

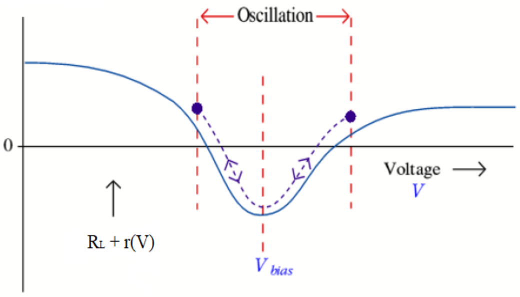

Figure:3. Dynamic resistance of Gunn Diode

The data signal "one" s will be broadcast at f_1 frequency levels, while the data signal "zero" s will be delivered at f_2 frequency levels. It may be helpful to understand the Gunn Oscillator's electrical tuning sensitivity, which is defined as the rate of change in oscillator frequency per volt change in biased voltage. The encryption process of digital data is already explained in our previous article [8].

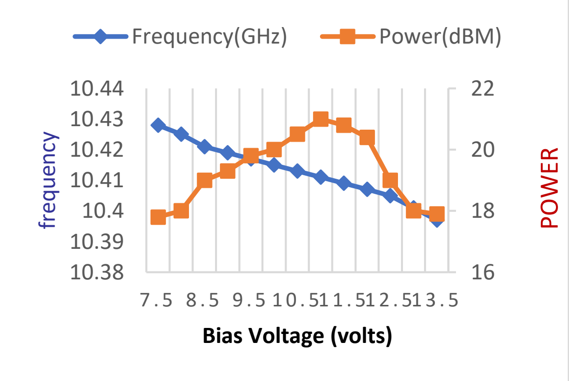

Fig4 The results of the experiments indicate the bias tuning characteristics of the Gunn Oscillator that were used in the investigation (Gunn diode model no. MA49104-111 (25 mW))

CONCLUSION

The primary goal of this article is to secure an information signal modulation in the microwave range using the suggested FSK which is not achievable with traditional FSK. The MORSA technique was used to encrypt the data. In this case, an experimental configuration has been created by combining security with modulation. The potential of safe communication for high-frequency applications is highlighted in this research. We may go to the millimeter and sub-millimeter levels with a few adjustments to the Gunn Oscillator construction. As a result, the frequency for this revolutionary design may be raised to sub-millimeter and millimeter-wave levels. We know that the amplitude and frequency changes caused by the Gunn bias voltage at the Gunn Oscillator cannot be separated. Using this pulse waveform, the security level is increased while the resolution for audio and video transmission is improved. These are the two most significant benefits of high-frequency shift keying modulation over standard FSK modulation.

Table 1

Bias Voltage of the Gunn diode. (V)	Position of the peak	frequency of oscillation (GHz)	Power in dBm
8.412	Center	10.407	16
	Left	10.400	18
	Right	10.414	14

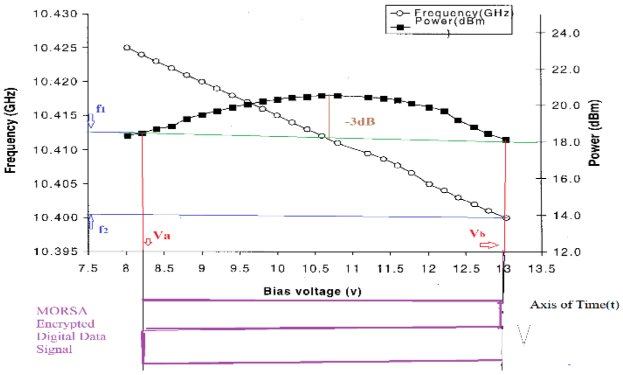

Fig:5 Marked frequency and space-frequency generation using a reflex klystron.

REFERENCES

1. R N Bates & S Feency, "Novel varacter-tuned millimeter wave Gunn oscillator"s, Electron Lett, 23, 714-715 (1987).
2. Vander Pol. B, "The nonlinear theory of electric oscillation". Proc. IRE, 22, 1051-1086 (1934).
3. B N Biswas, P Pal & D Mondal, "A new model for fundamental mode operated Gunn oscillator", JIETE (India), 37, 321-322 (1991).
4. I Stanchev & R Kozhuharov, "Characterization of second harmonic effects in Gunn diode microwave Oscillators", Proc of 8th Colloquium on microwave communication, Budapest, Hungery, 109-110, 25-26 Aug. 1988.
5. Pal P, Sahana B C and Poray J - Secured Information Transfer Power by Modified and Optimized RSA Cryptosystem, Easy Chair Preprint no. 10635,2023.
6. Kennedy, G.; Davis, B. (1992). Electronic Communication Systems (4th ed.). McGraw-Hill International. ISBN 978-0-07-112672-4., p 509.
7. Pal P, Chandra Sahana B, Poray J. RSA encrypted FSK RF transmission powered by an innovative microwave technique for invulnerable security. *The Journal of Defense Modeling and Simulation*. 2022;19(4):839-854. doi:10.1177/15485129211031670
8. Pal, P., Sahana, B.C., Poray, J., Mallick, A.K. (2021). Voice Password-Based Secured Communication Using RSA and ElGamal Algorithm Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 1299. Springer, Singapore. https://doi.org/10.1007/978-981-33-4299-6_32