International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | Jun 2022 www.irjet.net p-ISSN: 2395-0072

ENCRYPTION KEY GENERATION FOR DIGITAL CIRCUITS USING ANALOG CIRCUITS

MR. A Y PRABHAKAR, ANKIT PATHAK, AVANISH PAL, AYUSH MAHESHWARI

Professor, Department of E&TC Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India.
Department of E&TC Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India.
Department of E&TC Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India.
Department of E&TC Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India.

Abstract - *Previously, encryption keys for digital systems had been generated using hardware and software techniques. However, these techniques can be duplicated because they are pseudo-random. Because of this, a hacker can readily duplicate and enhance the method that produces the encryption key in software.*

This problem can be resolved by creating a random encryption key that doesn't adhere to any algorithm or pattern. To generate this kind of key, a hybrid methodology is suggested in this research. The digital and analogue components are combined in the suggested circuit.

The analogue domain is represented by Chua's circuit with a random noise source. Two capacitors, a resistor, and an inductor make up Chua's circuit, which may generate an oscillating waveform with a distinct output.

The Chua's circuit is fueled by a randomized input thanks to the addition of noise in the circuits, which produces a much more random output.

The key is generated, and then the data is stored on a digital storage medium. Sd card is used to store the digital bits, and Proteus8 is used to simulate the analogue component. RXD TXD Virtual Terminal may display the circuit's 8-bit digital output signals. The system makes use of an analogue circuit diagram, a digital circuit diagram, a virtual terminal, and an SD card to represent the key kept on a memory block.

The project's final output is a randomly generated 8-bit encryption key for digital systems

Key Words: **Chua's circuit, Noise generator, Multisim, Proteus 8.**

1. INTRODUCTION

Numerous techniques have been developed by humans to protect sensitive data from unauthorized access. People in ancient Greece wrote messages on wood that had been covered with wax to send a secret letter. In the same way, we must hide important information in the digital age. To accomplish this, we also work to create it "cover" for our private data. The technical word for this process is encryption. Digital systems frequently encrypt data using hardware or software techniques that generate an encryption key. In these tactics, algorithms that generate random keys are frequently employed.

But any algorithm can contain a small amount of randomness. After a predetermined number of repetitions, the process will be repeated, enabling a hacker to obtain the encryption key and steal sensitive data.

Pseudo-randomness is used in the vast majority of encryption key generation techniques. Since they are based on a particular algorithm, it is possible to generate the encryption key by deciphering its pattern or using reverse engineering methods.

Making an encryption key that defies algorithmic analysis and cannot be reverse-engineered is the solution to this problem. How to achieve this goal is explained in this project. Since no algorithm will be used in the method for generating encryption keys outlined in this project, the encryption key will not contain any repetitions.

This study will present a novel approach to producing encryption keys for digital systems. The keys will be generated using a hybrid strategy that connects an analogue circuit to a digital circuit. The analogue circuit will incorporate Chua's circuit as well as a short chain of inverters. Chua's circuit, which is only a straightforward configuration of electrical parts, generates oscillations with no recurring output. The Chua's circuit has various requirements. two capacitors, one nonlinear component, and one resistor.

The circuit will be given a noise signal to make the encryption key more random. A voltage device that simulates the noise signals found in digital systems is used to represent the noise signal. This technique will provide unpredictability in the encryption key, making tracing it back extremely difficult because there is no precise mechanism for producing the encryption key. As the weather circumstances vary, such as temperature and cross signals, the noise signal will shift. Regenerating the encryption key is nearly hard, even by the same manufacturer.

The encryption key must be transformed into a digital format after it has been generated. The encryption key will be used in digital circuits even if it is generated in the analogue domain. For this reason, the analogue signal is transformed into a digital signal. A converter from analogue to digital can be used for this. The speed and voltage requirements of digital and analogue circuits were taken into consideration when designing this digital convenor.

This hybrid approach will help create a highly random encryption key that is impossible to duplicate using any algorithm or reverse engineering.

2.IMPLEMENTATION

In this project, a novel method for creating the encryption key for digital systems will be presented. An analogue circuit will be connected to a digital circuit as part of a hybrid method for key generation. Chua's circuit and a short chain of inverters will also be present in the analogue circuit.

A straightforward arrangement of electrical parts, Chua's circuit will oscillate such that the output is never repeated. The analogue circuit is connected to the ADC converter, which produces a binary or numeric output.

The produced 8-bit binary output will always be distinct. In order to decrypt the message signal, the output is then placed into the memory card along with the encrypted key.

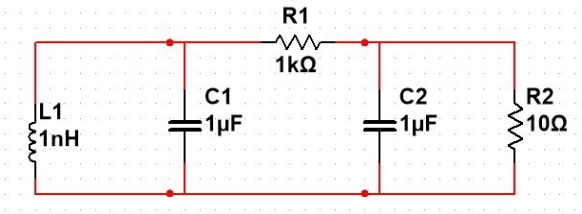
3.WORKING

- When a circuit is a built-in combination with Chua's oscillator and a Noise Generator, the output always generates a random waveform.
- Suppose we input a sine waveform into the circuit and change the resistance value of the combined circuit, we get the randomized waveform of a sine wave.
- These random signals are then converted into digital signals using an Analog-Digital Converter (A-D converter).
- Now, these digital signals are then converted into binary, finally, a test bench is written in Verilog to simulate the circuit and the expected output 8-bit encryption key is generated.

4.RESULTS

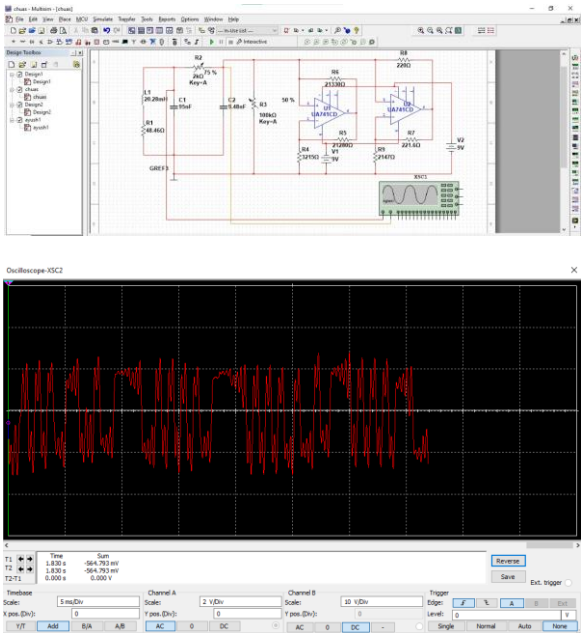
Step 1:

Initially, we created Chua's circuit which consists of inductors, capacitors, and resistors.

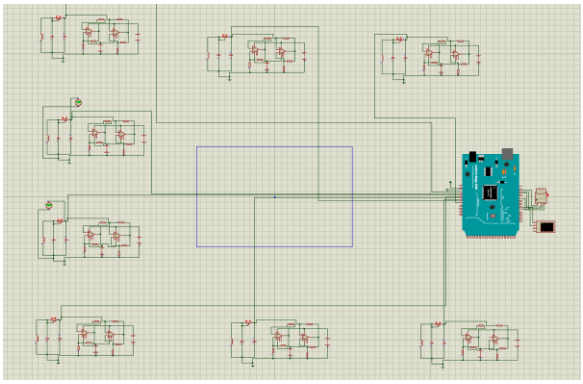


Step 2:

As we move forward, we have generated a random signal by combing Chua's circuit with a noise generator.

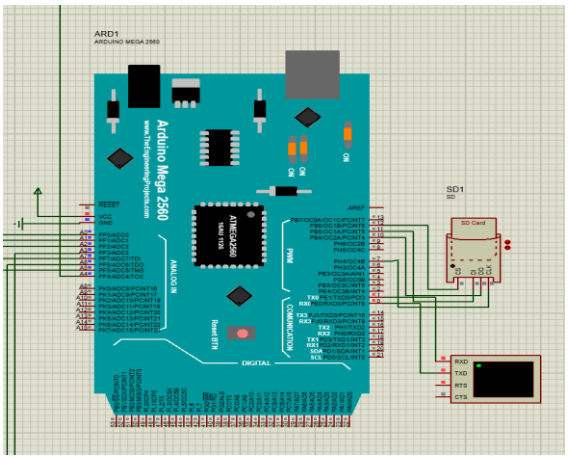


Step 3:



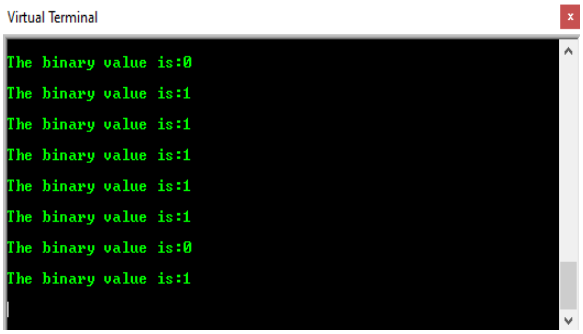
Now we have connected all 8 Chua's circuits in parallel to generate an 8-bit random binary signal.

Step 4:



Now the 8-bit random key is stored in the memory card to forward on the decryption side to encrypt the message signal.

Step 5:



This is the final output in Virtual Terminal, this 8-bit random output changes after every interval.

5. CONCLUSION

This work put up a fresh idea for digital system encryption key generation using a mixed-signal approach. The study also underlines the significance of noise and fluctuating signals in digital systems.

Using a mixed-signal approach, the model circuit for the encryption key generator was constructed.

Phase 1 involves designing and simulating Chua's circuit. It was challenging to determine the ideal values for the circuit's properties to achieve the Chua effect. By utilizing Kirchhoff's rules, numerous equations were developed to get around this obstacle. The components of the circuit were selected to increase the circuit's overall efficiency. The design is appropriate for low power applications because of this feature. In addition to the power advantage, the circuit has a parallel bit generating approach that makes it extremely efficient.

The second phase entails creating a noise generator that can simulate actual noise. Numerous noise equations, random number generators, and software were employed to accomplish this.

The Arduino, which includes an integrated ADC converter, is the focus of phase three. We have coded the analogue signal in Arduino to produce digital output. This program compiles analogue values and outputs binary values, 0 and 1, as a result. The memory card that is connected to Arduino is then given these binary values. The binary values are kept on the memory card here. We can see the output on the terminal display with the aid of Rxd and Txd terminals.

6. FUTURE SCOPE

- The key's length can be changed to make a significant difference. Another aspect that the hacker will research is the length of the encryption key. The length of the data that has to be encrypted can set a range for the key's potential length. The encryption key will gain a new level of robustness thanks to this functionality.

- Another element that might make an encryption key particularly unpredictable is varying sample time. By using a variety of random sampling rates with respect to the oscillation frequency of the Chua's circuit, the implementation can be carried out. The time it takes to produce the key will be highly variable due to the fluctuating sample rate. The encryption key may be more secure and random thanks to this function.

7. REFERENCES

- https://www.scribd.com/document/141906870/Chua-s-Circuit-Implementations
- https://en.wikipedia.org/wiki/The_Codebreakers
- https://www.researchgate.net/publication/261126433_Sampling_Circuits_That_Break_the_kTC_Thermal_Noise_Limit
- https://store.arduino.cc/products/arduino-mega-2560-rev3
- https://ieeexplore.ieee.org/document/9278996
- https://en.wikipedia.org/wiki/History_of_cryptography
- https://randomnerdtutorials.com/guide-to-sd-card-module-with-arduino/