Chaotic key generators for data security

BABY H T¹  SUJATHA B R²

¹Associate Professor, Dept. of E&CE, GEC, Hassan, Karnataka, India
²Professor, Dept. of E&CE, MCE, Hassan, Karnataka, India

* Corresponding author’s Email: babygowda@gmail.com

Abstract: The cryptography approach plays a very major role in securing systems by providing authentication, integrity, and confidentiality for the data. In recent decades, the cryptographic systems have provided novel and efficient ways of encryption. Most of these cryptographic systems need unpredictable entities - Keys. Hence Random number generator is an essential component for cryptography. In cryptography, generating random numbers is an important task, not only for generating cryptographic keys, but also for implementing cryptographic algorithms and protocols. This paper presents chaotic analog circuits to generate random numbers that is used as keys in the conventional cipher to protect the image data.

Keywords: Cryptography, Random number generator, Encryption, Decryption, Chaotic circuits

1. Introduction

In public and private networks as data traffic rate is increasing, it is imperative to secure the confidentiality of the information saved on and exchanged between data processing units. Cryptography is one technique which provides security for the data. In recent decades, cryptographic systems have suggested so many new and competent secure methods of encryption. In all these methods the generation of a cryptographic key is extremely important and to ensure security these keys should be highly random i.e., essentially it is a string of random bits. This can only be achieved by generating highly random numbers. As such, random numbers are the foremost requirement for digital signatures, cryptographic algorithms, and communication network protocols. The good random number generator (RNG) should produce numbers that are statistically random and in-deterministic. The chaos theory defines the in-deterministic behavior of the nonlinear dynamic systems which are sensitive to the initial values with specific conditions [1-4]. The chaotic encryption methods are fast, robust, easy to implement and provides high security for the data. The 1D and 2D logistic standard maps are some of the symmetric cipher method which employs substitution-diffusion method. These algorithms include the initial parameters and number of iterations of the chaotic maps and system parameters. But the encrypted cipher text is not fully secure. Only hardware RNG can meet all of these requirements. Therefore, to have a high degree of information protection, a high-quality hardware-based random number generator is absolutely necessary [5-6]. The hardware-based Random Number
Generator strengthens the applications like e-Business, Web browsing and remote access, which currently uses software-based random number generators. The remaining of the paper is organized as follows. In section-2 related works are discussed, section-3 and 4 simulation results of the circuits and randomness test using NIST tool are discussed. In the Section-5 Encryption process and Decryption of the image using Chaos keys are discussed. The section-6 concludes the overall work.

2. Random number generators

Chaotic based circuits have been designed to generate random numbers. The general block diagram of the chaos based RNG system is shown in Fig 2.1, in which output of a chaotic circuit is sampled to obtain digital signal. Then, a binary bit sequence will be extracted by performing the post-processing methods.

![Chaotic Circuit Block Diagram](image)

**Fig. 2.1:** Chaos-based RNG system

2.1 Colpitts Oscillator as a Chaotic Circuit

An oscillator is one of the electronic circuits which exhibit a rich dynamical behavior like many other third-order oscillator configurations available in the literature. In particular, there is a wide-range of statistical and experimental evidence of continuous chaotic behavior for the Colpitts oscillator that can be used in protected communication systems. This system is generic, non-symmetric and possesses an intrinsic non-linearity which can be represented as the exponential characteristic of the active device [9-10].

The Colpitts oscillator shown in Fig 2.2 comprises bipolar junction transistor (BJT) amplifier with common-base configuration. The resonator circuit includes two capacitances (C₁ and C₂) and an inductance (L), and is mainly used to derive the frequency of oscillations. A portion of the voltage of the LC circuit is feed back to the amplifier. The voltage Vcc provides bias to the circuit and the current source I₀ is characterized by a Norton-equivalent conductance G₀. The Colpitts oscillator is normally designed to produce periodic oscillations. However, the oscillator can deliver chaotic waveforms with specific settings of the circuit constraints and appropriate circuitry modifications.
2.2 Amplifier Based Chaotic Autonomous Electronic circuit

This is a simple nonlinear chaotic electronic circuit which comprises Single Amplifier Bi-quad (SAB) which is converted into chaotic oscillator using appropriate passive non-linear element in the form an inductor as shown in Fig 2.3. It is basically an active Band Pass Filter (BPF), which is revised using a passive non-linear p-n junction diode to generate chaotic oscillations, and an inductor as a storage element. The circuit is precisely exhibited using a couple of first-order non-linear differential equations. The circuit shows complex chaotic behavior for a certain set of limit values.

The Autonomous chaotic oscillator has (i) A SAB based active BPF comprises of an Op-amp, four resistors ($R_s, R_b, R_1, R_2$) and two capacitors. (ii) A shunt connection of a P-N junction diode (D) and inductor (L). The diode works as a switch depending on the induced inductor voltage $V_{CD}$ which exists due to the transistance capacitance $C_D$ of the diode. The voltage and current of the autonomous chaotic oscillator are described in equations 1 and 2 respectively.

$$C \frac{dV_0}{dt} = -\frac{2}{R_2} V_0 + \frac{k+1}{R_1} V_1 + \frac{k+1}{R_1} V_{CD}$$
\[
\frac{dV_1}{dt} = \frac{(2k+1)}{(k+1)R_2} V_0 + \frac{k}{R_1} V_1 - \frac{k}{R_1} V_{CD}
\]

\[
\frac{dI_L}{dt} = -\frac{V_{CD}}{L}
\]

\[
C_D \frac{dV_{CD}}{dt} = \frac{1}{R_1} V_1 - I_L - \frac{1}{R_2} V_{CD} - I_D
\]

Here \( k = \frac{R_b}{R_a} \). The diode current \( I_D \) can be represented as a piece-wise function of linear voltage is given by

\[
I_D = \frac{1}{R_D} (V_{CD} - V_T), \text{ if } V_{CD} \geq V_T
\]

\[
= 0 \text{ if } V_{CD} < V_T
\]

\( R_D \) is forward resistance of the diode and \( V_T \) is voltage drop of the forward biased diode. The Multisim circuit simulator has been used to design the circuit. The simulation circuit uses Op-amp- TL02C2 with \( \pm 12V \) power supply and general-purpose diode along with \( R_b=500\Omega, R_a=2k\Omega, C=1nF, L=7.8 \) mH, \( R_2=3.1k\Omega \) and \( R_1=100\Omega \).

3. Simulation and discussion

Multisim has been used for circuit design of oscillator circuits to generate the random numbers. Python language has been used for checking the randomness of the generated random numbers using standard NIST (National Institute of Standards and Technology) test suite and Dieharder battery test. MATLAB has been used for performing encryption process and decryption of the image data. Fig. 3.1 shows the simulated circuit diagram of colpitt’s oscillator that circuit consists Colpitts oscillator, Analog to digital converter (ADC) and Logic analyser. The output of the colpitt’s oscillator is shown in Fig 3.2 has converted into discrete signal using ADC and Logic Analyzer has been used to extract the binary bits from the discrete signal.

Fig. 3.1: Simulated Circuit diagram of the Random number generator
Fig. 3.2: Output waveform of the Colpitts oscillator

Fig. 3.3 shows the simulated circuit of the Amplifier based Autonomous Oscillator and generated waveform. Fig. 3.4 shows the digital waveform from ADC. Binary bits are extracted from the digital waveform using logic analyzer.

Fig. 3.3: Single Amplifier based Autonomous Oscillator output and its waveform

Fig. 3.4: ADC logical waveform
4. Randomness Test

A standard NIST statistical tool and dieharder battery tests are used to analyze the randomness of the binary stream produced by hardware circuits. NIST test focuses on 14 different types of randomness that exists in a sequence and provides percentage of randomness present in it. The 14 tests conducted are described in the table1.

| Statistical Test | Characteristics |
|------------------|-----------------|
| 1. Frequency (Monobit) | Approximately equal number of zeros and ones |
| 2. Cumulative Sums | Equal distribution of zeros or ones at the beginning of the sequence |
| 3. Longest Runs of Ones | Equal distribution of long runs of ones or zeros. |
| 4. Runs | Oscillation between zeros or ones is too fast or too slow |
| 5. Matrix Rank | To check linear dependence among fixed length substrings |
| 6. Spectral (Discrete Fourier Transform) | Periodic features in the bit stream |
| 7. Non-overlapping Template Matchings | Too many occurrences of non-periodic templates |
| 8. Overlapping Template Matchings | Too many occurrences of m-bit run of ones |
| 9. Universal Statistical | Compressibility (regularity) |
| 10. Random Excursions | Deviation from the distribution of the number of visits to a certain state |
| 11. Random Excursion Variant | Deviation from the distribution of the total number of visits (across many random walks) to a certain state |
| 12. Approximate Entropy | Uniform distribution of m-length words |
| 13. Serial | Non-uniform distribution of m-length words. Similar to Approximate Entropy |
| 14. Linear Complexity | Deviation from the distribution of the linear complexity for finite length (sub)strings |

Table 2 shows the random numbers extracted from the ADC Circuit. Fig 4.1 (a) and 4.1 (b) shows the NIST tests result and dieharder battery test results for the generated numbers which is computed using Python language. The p value should be greater than 0.01 and less than 1 for randomness. The p values in the results shows that the generated numbers passed all the tests and numbers are highly random in nature. For ex: for the Monobit test P value is 0.4518 and NIST result indicates test is ‘PASS’, i.e., values generated are random.

Table 2: Generated binary numbers

| SL No | Random number | SL No | Random number | SL No | Random number |
|-------|---------------|-------|---------------|-------|---------------|
| 1     | 11100011      | 16    | 01000011      | 31    | 11000011      |
| 2     | 01010111      | 17    | 01000011      | 32    | 11000011      |
| 3     | 01010111      | 18    | 11000011      | 33    | 11000011      |
| 4     | 10000011      | 19    | 10110011      | 34    | 01100011      |
| 5     | 10000011      | 20    | 01100011      | 35    | 01100011      |
| 6     | 11000011      | 21    | 01010111      | 36    | 11000011      |
| 7     | 11100011      | 22    | 10010111      | 37    | 10010111      |
| 8     | 10110011      | 23    | 10101011      | 38    | 10101011      |
| 9     | 10101011      | 24    | 01010111      | 39    | 11000011      |
| 10    | 00100011      | 25    | 01001011      | 40    | 11000011      |
| 11    | 01000011      | 26    | 11000101      | 41    | 01000011      |
| 12    | 01000011      | 27    | 10010011      | 42    | 01000011      |
| 13    | 00000011      | 28    | 01010111      | 43    | 11010111      |
| 14    | 10010111      | 29    | 01101011      | 44    | 01101011      |
| 15    | 11010111      | 30    | 01101011      |       |               |
Fig. 4.1: a) NIST test results                                                        b) Dieharder battery test results

5. Encryption and Decryption using chaos keys

The lena image shown in Fig 5.1(a) is considered as an input image. By performing XOR operations, the input image is encrypted using the generated random numbers as keys and same has been used to perform the decryption process. Fig. 5.1(b) and Fig. 5.1(c) shows the encrypted and decrypted images respectively. There is a great resemblance between the input image and Decrypted image which represents the input image is recovered correctly.

![Input image](image1.png) ![Encrypted image](image2.png) ![Decrypted image](image3.png)

The Number of pixel change rate (NPCR) is one of the parameters used to analyze the effect of changing one pixel in both plain and cipher images. The NPCR represents the number of pixels differs between the two ciphered images obtained from one-bit differed input image. If C1 and C2 are the two different ciphered images, then the NPCR will be given by,

\[
NPCR = \sum_{k=1}^{M} \sum_{l=1}^{N} \frac{d(k, l)}{MN} \times 100
\]

\[
d(k,l) = 1 \text{ if } C1(k,l) = C2(k,l) \]  

\[
d(k,l) = 0 \text{ if } C1(k,l) \neq C2(k,l)
\]
The NPCR result obtained is average of 98%, shows that encryption method is very sensitive to minor changes in pixel of the input image.

6. Conclusion

This paper presents chaotic colpitt’s oscillator and SAB based chaotic autonomous oscillator circuits to generate binary sequences. The NIST standard tool and Dieharder battery test suite are used to verify the randomness of the generated binary sequences. The results have shown that the binary sequences generated are random in nature and can be used as keys for cryptographic algorithms to secure the data. In this work, image encryption is done using the generated keys and shown that it provides security for the image data. Also, these random sequences can be used for various applications like NONCE generation, One-time pad, password, initialization vectors and parameters of various protocols in crypto systems.

References

[1] Constantin Cehan, Bogdan Cristea, 2002, “Applications of Chaos Theory in cryptography”, 
International Conference on Military Equipment and Technologies Research, Romania, pp: 1-5.
[2] Muhammed Rezal, Kamel Ariffin, 2008, “Chaos Based Cryptography an Alternative to Algebraic Cryptography”, Research Bulletin Institute for Mathematical Research, Vol 2, pp: 41-47.
[3] Dubrova E, Teslenko M and Tenhunen H, 2008, “On Analysis and Synthesis of (n, k)-non- linear Feedback Shift Registers,” Design, Test in Europe, pp: 1286-1291.
[4] Zhu Zhiliang, Chen Dongming, Yang Guangming, 2008, “An improved Image Encryption Algorithm Based on Chaos”, IEEE the 9th International Conference for Young Computer Scientists, pp: 2792-2796.
[5] Cristian-Iulian, Alexandru, 2009, “Chaos-based Cryptography a Possible Solution for Information security”, Bulletin of the Transilvania University of Brasov, vol 2(51), pp: 113-126.
[6] W Jonker and M Petkovic, 2014, “Data Security – Challenges and Research Opportunities”, Springer International Publishing Switzerland, pp: 9–13.
[7] N N Mosola, M.T Dlamini, Jonathan Blackledge, 2017, “Chaos-based Encryption Keys and Neural Keystore for Cloud-hosted Data Confidentiality”, Telecommunication Networks and Applications Conference (SATNAC, 2017), pp.168-173, Southern Africa.
[8] Rim Zahmoul, Ridha Ejbali, Mourad Zaied, 2017, “Image encryption based on new Beta chaotic maps”, Optics and Lasers in Engineering, Elsevier Ltd, pp: 0143-8166.
[9] Tanmoy Banerjee, Bishnu Charan Sarkar, 2010, “Single amplifier biquad based autonomous electronic oscillators for chaos Generation”, Nonlinear Dynamics.
[10] Lahcene Merah, Adda Ali-Pacha, Naima Hadj Saidand , Mustafa Mamat, 2013, “A Pseudo Random Number Generator Based on the Chaotic System of Chua’s Circuit, and its Real Time FPGA Implementation”, Applied Mathematical Sciences, HIKARI Ltd, Vol.7, No. 55, pp: 2719 – 2734.