IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, March 2024

Encryption using True Random Number

Kavitha I[1], HarimadavS[2], Karthigeyan P[3], Kirubanithi R[4], Kreshanth S V[5]

M.E Assistant Professor (O G)[1]

SRM Valliammai Engineering College, Kattankulathur, Kanchipuram, Tamil Nadu, India

kavithai.it@srmvalliammai.ac.in, harimadhav6181@gmail.com, karthigeyenparthi12@gmail.com,

kirubaramesh2002@gmail.com, kreshkatana29@gmail.com

Abstract*:* *In moment's connected digital geography, data security and sequestration have come consummate enterprises. Traditional encryption ways frequently calculate on mock arbitrary number creators (PRNGs) to induce encryption keys, which are deterministic and vulnerable to attacks. This design proposes a new approach to enhance data encryption by exercising true arbitrary number creators (TRNGs) for generating encryption keys. In this work, a secure optic ultrafast arbitrary number creator grounded on arbitrary ray gamut's was demonstrated. Unlike the usual system of recording ray intensity over time, the arbitrary ray diapason under each pump palpitation was recorded and converted into arbitrary figures through post-processing. Approaches in three different confines — space, diapason and time were used to increase the rate of arbitrary number generation. The randomness of performing arbitrary bit aqueducts was vindicated by the NIST statistics tests.*

Keywords: encryption

I. INTRODUCTION

True arbitrary figures are deduced from changeable physical processes, icing an advanced degree of randomness compared to PRNGs. The main ideal of this design is to probe, design, and apply an encryption system that harnesses the power of true arbitrary figures for generating robust and unbreakable encryption keys. The system will involve the integration of a tackle- grounded TRNG, able of rooting entropy from changeable sources, similar as electronic noise or radioactive decay. Kimetal. lately demonstrated a presto, 250 Tb/ s arbitrary number creator (RNG) grounded on a chip-scale ray. The RNG achieved largely resemblant ultrafast arbitrary bit generation by introducing spatiotemporal hindrance of numerous lasing modes in a especially designed depression. In addition, arbitrary fibre spotlights have entered great attention in recent times due to their fairly broad bandwidth, which is analogous to that of semiconductor spotlights, and their temporal intensity shown arbitrary oscillations without depression convinced time- detention which are essential forultra-speed arbitrary bit. Approaches in three different confines- spaces, diapason and time were used to increase the rate of arbitrary number generation. The randomness of performing arbitrary bit streams was vindicated by the NIST statistic tests. The design proposes new approach for True number Generations TRNG).

II. RELATED WORKS

An arbitrary ray is a type of ray that relies on multiple light scattering and gain to give the feedback medium and light modification, independently. Unlike a regular ray, a arbitrary ray doesn't bear a depression for the feedback medium. Random spotlights have low fabrication costs and special optic parcels similar as broad emigration angle and low spatial consonance, which make them promise in numerous fields. Over the once many times, arbitrary spotlights have been applied in patch-free imaging, super-resolution spectroscopy, and secure communication. According to the intensity of the optic feedback, arbitrary spotlights are generally divided into two administrations. When the optic feedback intensity isn't strong enough, all the arbitrary ray modes reaching the threshold will be amplified together, leading to a smooth incoherent arbitrary ray peak with a line range of a many nanometres. When the optic feedback intensity is strong enough, a strong competition will live between the individual arbitrary ray modes. Randomness is ubiquitous in the macrocosm and can be used to induce arbitrary bits for IoT device security. currently, a variety of detectors similar as LDR detectors, sound detectors, accelerometers, bars, and gyroscopes are used in IoT bias for colourful operations Secure communication, data transfer, and processing have been major areas of development and

DOI: 10.48175/IJARSCT-15617

exploration over the last decade. Cryptographic algorithms and colourful communication protocols calculate on dependable and secure transfer of information grounded on data encryption or authentication. The source of randomness can be computational or physical. Random number creators RNGs) are essential for numerous operations in everyday computing, especially in the areas of computer security and cybersecurity where encryption and crucial generation are necessary. An arbitrary bit creator is a system by which a string of changeable figures or symbols is created. There are two orders of RNGs (1) Pseudo Random Number creators (PRNGs), also called software grounded RNGs, and True Random Number creators (TRNGs) PRNGs use fine algorithms to induce arbitrary figures that appear to be arbitrary but are actually deterministic. TRNGs, on the other hand, induce arbitrary figures using physical processes similar as atmospheric noise, radioactive decay, and thermal noise. TRNGs are more secure than PRNGs because they're not grounded on fine algorithms and are thus less predictable.

III. METHODOLOGIES

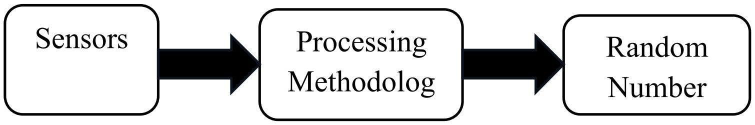


Figure 1TRNG Generalist Diagram

Everyday life is filled with random numbers, and generators of random numbers (RNGs) are frequently used in cryptography, Monte-Carlo computational simulations, information security, and stochastic modelling in contrast to numbers that are pseudo-random numbers. Given that random numbers are based on non-deterministic physical processes, they are more promising for information security applications. Wenming Tian and Shengye Jin are with the State Key Laboratory of Molecular Reaction Dynamics and Dynamics Research Centre for Energy Digital Object Identifier. True RNGs have been implemented after decades of development through physical entropy sources like Raman scattering, random fiber lasers, chaotic semiconductor lasers, amplified spontaneous emissions frequency jitter of oscillators, quantum photoelectric effect, and thermal noise in electronic circuits. Due to the high bandwidth and enormous amplitude signals of the light source, optical Random number generators utilizing stochastic silicon lasers as typical entropy sources have attracted a great deal of attention since the groundbreaking discovery in 2008. recently showed out a quick, chip-scale laser-based RNG that can handle 250 Tb/s. By introducing spatiotemporal interference of many laser modes in a specially designed cavity, massively parallel fast random bit generation was achieved. Furthermore, in recent years, random fiber laser has drawn a lot of interest. Similar to semiconductor lasers, random Fiber lasers also have a reasonably wide bandwidth. Importantly, for ultra-high speed random bit production, the temporal intensity of the laser exhibits random fluctuations free from cavity-induced time-delay fingerprints. Optical RNGs have a greater potential for use due to their ultrafast random number production rate. There are currently two primary methods to increase the rate of optical RNGs: (1) increasing the optical source's bandwidth, and (2) increasing the number of spatial channels. When these two techniques reach a certain stage of growth, hardware limitations will come into play. Therefore, investigating a new topic is particularly essential for raising the rate of optical RNG. The random number generator (RNG) is an essential component of many prevalent computing processes, particularly those related to computer and cyber security, where encryption and key generation are required. A method for creating a string of erratic numbers or symbols is called a random bit generator. Two types of random number generators (RNG) exist. Pseudo generators of random numbers, or software based random number generators, are the first type. True random number generators (TRNG) are non-deterministic in nature, making them non-repetitive and non-predictable, whereas PRNG is deterministic in nature, making it repeatable and predictable. This work demonstrated an encrypted visual ultrahigh-speed random number generator (RNG) based on coherent random laser spectra that are "concealed." Unlike earlier techniques for producing random numbers, which were applicable to RFLs and chaotic semiconductor lasers, our approach involved storing the random laser spectrum under each pulse and transforming it into a random number. The production of random numbers is now far more effective thanks to this technique. High-order finite difference was used to solve the statistical bias issue. We also investigated ways to boost the rate of random number generation by expanding the channels for random number generation and enhancing the spectral resolution. In addition, the use of a streak camera increased the rate at which random numbers were generated in the temporal domain. In order to design quicker TRNG, four LDR (Light Dependent Resistor) sensors—also known as photo-resistor sensors or photo-cell sensors—as well as a sound sensor are used in this work. These are inexpensive sensors that are beneficial to many IoT applications' security. The LDRs are used to extract randomness from light intensity. The relationship between light intensity and LDR resistance is inverse. The sound sensor functions similarly to an ear. It works by detecting the volume of noise or the sound intensity in the immediate area and sending an Analog output voltage signal to a micro controller. The addition of the spectral dimension, as opposed to the present global generation of random numbers of methods, is primarily responsible for the quick speed. All the National Institute of Standards and Technology's (NIST) statistical tests were passed by the generated random bit streams, confirming the suitability of our approach for generating random numbers. Additionally, compared to RNGs operating in CW mode, the short pulse mode of operation offers improved anti-electromagnetic interference ability and increased communication security.

TRNG General Schematic Diagram

The block design in Figure 1 is made up of sensors (LDR, Sound, Temperature) that pick up noise from the environment as light and sound. These signals are then sent to a processing algorithm, which creates random bits. To create a more reliable and impenetrable data protection system, this project aims to harness the power of real randomness by incorporating hardware-based true random number generators (TRNGs) into encryption algorithms. On comparison with the common random number generation techniques used today. The outcomes random bit streams verified the suitability of our approach for random number generation by completing every National Institute of Standards and Technology (NIST) statistics test.

IV. FRAMEWORK PROPOSED

This section builds the hardware basis of the proposed TRNG by using the unpredictability of the sound and LDR sensors as a source of randomness.

Components Used:

a) Arduino UNO

The Arduino Uno is a microcontroller board that is used to process the data obtained from the sensors.

Fig 2 Arduino UNO

It consists of:

- 14 Digital Pins.
- Among digital pins D3 to D11 excluding D4, D7and D8, are used for pulse width modulation.
- PWM: it converts digital output to Analog input.
- UART: D0 and D1.
- A0 to A7: Analog pins

DOI: 10.48175/IJARSCT-15617

- D0 to D13: digital pins
- D2 and D3 are external interrupt pins
- SCK: D13.
- SCK is serial clock which synchronize the data generated by a controller.
- MISO: D12 and MOSI: D11.
- In MOSI data is sent from controller to peripheral.
- Master work as controller and slaves work as peripheral.
- Slave Select (SS): D10.

b) Light Dependent Resistors

Light Dependent Resistors, or LDR sensors for short, are also known as photoresistors. It is very light-sensitive, meaning that as light intensity rises, the LDR sensor's resistance falls and vice versa.

Fig 3 Light Dependent Resistor

c) Sound Sensor

It is a sound detection module that produces electrical signals from sound waves. It is crucial to the security of Internet of Things devices and is extremely sensitive to noise.

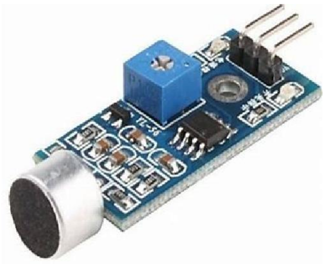


Fig 4 Sound sensor

d) Temperature Sensor

A pre-assembled device with all the parts required for temperature detection is called a thermistor temperature sensor module. A microcontroller, an analog-to-digital converter (ADC), and a thermistor are usually its constituent parts.In essence, thermos-resistors are resistors whose resistance varies in response to temperature. The term "Negative Temperature Coefficient," or NTC, describes how a temperature increase will cause a decrease in sensor resistance.

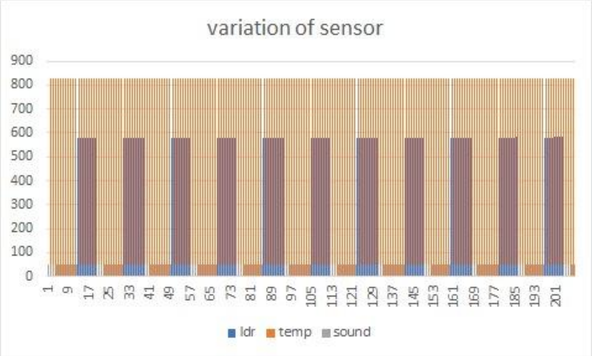
Fig 5 Thermistor Temperature sensor

DOI: 10.48175/IJARSCT-15617

V. ESTIMATION OF RANDOMNESS IN LDR AND SOUND SENSOR

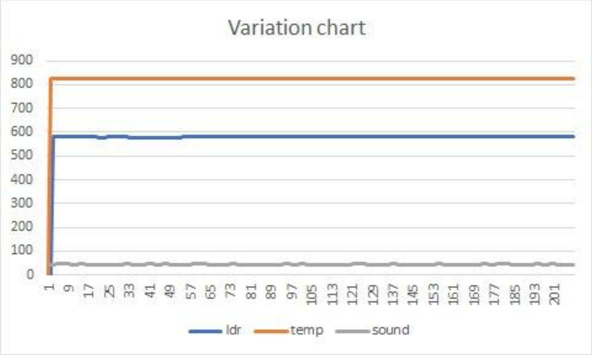
```
Procedure GETRANDOMNESS (Grand)
    Segment the long Grand input into vectors: W(j)
    for each W(j) data chunk: do
    Split W(j)into two matrices: W1 and W2
    Extract Entropy:
    $R (i, j) = (W1(i, j) \oplus ((W1(i, j) < (j \bmod 8))$
    $\oplus W2(i, j)$
    Split R into two matrices: R1 and R2
    Final output:
    $(i, j) = (R1(i, j) \oplus ((R1(i, j) < (j \bmod 8))$
    $\oplus R2(i, j)$
    Convert the matrix (O) into a vector and
    Output the values.
```

The software uses the modular arithmetic concept and EX-OR operation between sensors to generate more unpredictable random numbers. Every type of environment will be compatible with the suggested design. By using a microcontroller to connect the hardware to the PC, random sample sizes of at least one million are gathered. These samples were later approved for the NIST STS test.



According to the graph, the light sensor reading (ldr) is highest at the start of the time period and progressively drops after that. At the start of the time interval, the temperature sensor reading (temp) is at its lowest and then progressively rises. Midway during the duration, the sound sensor reading (sound) is at its lowest, then it rises toward the end.

The image above is a bar graph called "variation of sensor," which shows data throughout a range of measurements for three distinct types of sensors: sound, temperature, and ldr. The top label on the bar graph reads "variation of sensor." Three sets of bars—yellow for sound, red for temperature, and blue for light—represent various sensor types. The measurement values are indicated by the numbered y-axis, which runs from 0 to 900.



Numerical labels ranging from 0 to 201 are spaced apart on the x-axis, and they may indicate different measurement units or instances. Every "ldr" bar extends to the maximum (900) value on the y-axis. in contrast to others. The heights

ISSN
2581-9429
IJARSCT

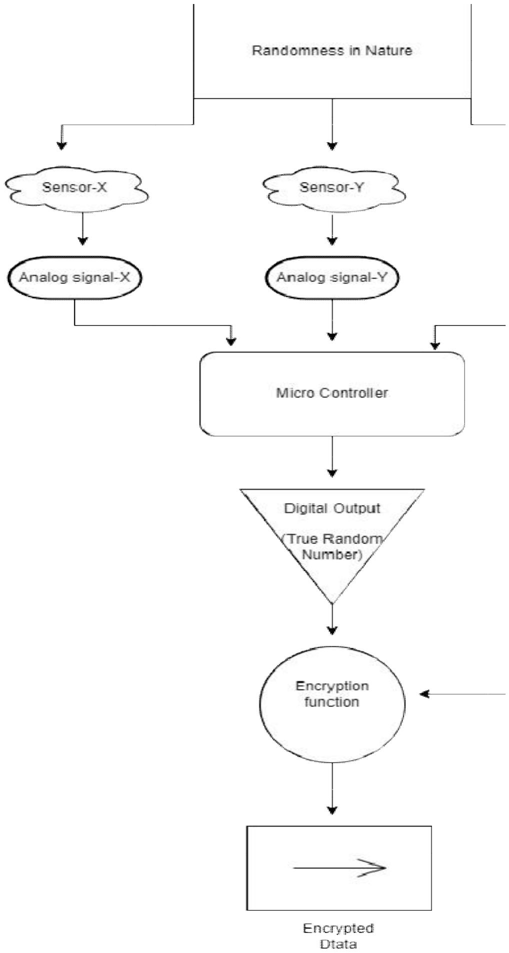
DOI: 10.48175/IJARSCT-15617

of the "temp" bars vary, but they are substantially lower than the "ldr" bars. Since there are no bars displayed for "sound," it is possible that its values are zero or very low when compared to others.

The graph that supplied is called a "Variation chart" and it shows data from three different kinds of sensors: sound, temperature, and ldr. Numerical values on the x-axis span from 0 to 201, while those on the y-axis go from 0 to 900. The orange "temp" line doesn't change from its high value around 800. The blue "ldr" line moves somewhat but remains in the middle of the graph, close to a value of about 500. The gray "sound" line on the graph stays stationary at a low point, indicating that its values may be zero or insignificant in relation to other values.

Architecture Diagram

The flowchart in the image illustrates how randomness in nature may be used to generate encrypted data. The first line of the flowchart, "Randomness in Nature," feeds into three distinct sensors, designated "Sensor-X," "Sensor-Y," and "Sensor-Z." The randomness is transformed into an analog signal by each sensor, which is designated as "Analog signal-X," "Analog signal-Y," and "Analog signal-Z" accordingly. A "Micro Controller" is then fed these analog signals and given the task of processing them. "Digital Output (True Random Number)" is the output of the Micro Controller. The "Encryption function" creates" Encrypted Data" by using this true random number and the “DataTo Be Encrypted."

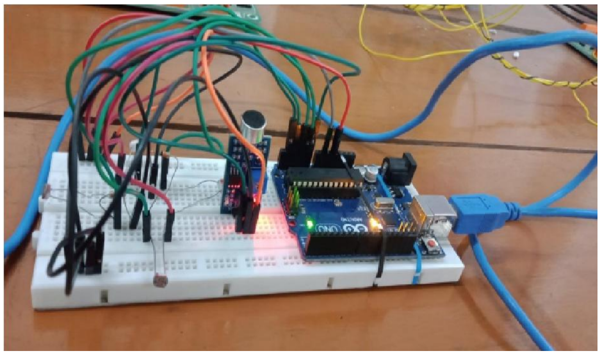


ALGORITHM OF PROPOSED TRNG
Input: Ldr (n), S1 // n = 1 to 4
Output: Y (random output)
Step 1: Ldr (n) = Ln; sound sensor = S1;

```
Step 2: Condition 1,
if (S1<0)
S1=-S1
Z1= (L1*L2) %S1; // Modular Arithmetic
Z2= (L2*L3) %S1;
Z3= (L3*L4) %S1;
Z4= (L4*L1) %S1;
Step 3: Condition 2,
if (Z1 > Z2)
Y1 = 1;
else
Y1 = 0;
if (Z3 > Z4)
Y2 = 1;
else
Y2 = 0;
Step 4: Y = Y1 ^ Y2 // EXOR operation
Output: Y // Generated True Random Output
```

VI. EXPERIMENTAL SETUP AND RESULTS

A sound sensor is positioned typically in the experimental setup, but four distinct LDR placements are made to maximize light collection. This heightens uncertainty and may help achieve quick and safe randomized number strings at a higher rate of production. The suggested design produces unpredictable output and functions well in a range of light and noise levels.



REFERENCES

[1] [1] M. H. Kalos and P. A. Whitlock, Monte Carlo Methods. Hoboken, NJ, USA: Wiley, 2009.

[2] D. R. Stinson, Cryptography: Theory and Practice. London, U.K.: Chapman and Hall/CRC, 2005.

[3] J. D. Hart, Y. Terashima, A. Uchida, G. B. Baumgartner, T. E. Murphy,and R. Roy, “Recommendations and illustrations for the evaluation of photonic random number generators,” APL Photon., vol. 2, no. 9, 2017,Art. no. 090901.

[4] M. Herrero-Collantes and J. C. Garcia-Escartin, “Quantum random number generators,” Rev. Mod. Phys., vol. 89, no. 1, 2017, Art. no. 015004.

[5] S. Asmussen and P. W. Glynn, Stochastic Simulation: Algorithm and Analysis, vol. 57, Berlin, Germany: Springer, 2007, pp. 487 488.

[6] N. Jiang, C. Xue, D. Liu, Y. Lv, and K. Qiu, “Secure key distribution based on chaos synchronization of VCSELs subject to symmetric randompolarization optical injection,” Opt. Lett., vol. 42, no. 6, pp. 1055–1058, 2017