

Implementation of a secure wireless communication system using true random number generator for internet of things

Huirem Bharat Meitei, Manoj Kumar

Department of Electronics and Communication Engineering, National Institute of Technology Manipur, Imphal, India

Article Info

Article history:

Received Sep 13, 2022

Revised Jan 12, 2023

Accepted Jan 15, 2022

Keywords:

All digital phase locked loop

ESP8266

Field programmable gate array

Internet of thing

True random number generator

ABSTRACT

This paper describes the design and implementation of an internet of thing (IoT)-based application that uses a true random number generator (TRNG) with an all digital phase locked loop (ADPLL) for secure wireless communication. Field programmable gate array (FPGA) boards were used on the transmitter and receiver sides and were interfaced with Esp8266 chips to wirelessly send and receive encrypted sensor data. The MQ-2 gas sensor and tracking sensor were connected to the FPGA board on the transmitter side, where data from the sensors was encrypted using the exclusive-OR (XOR) function and the TRNG architecture. The system can be controlled by users through a web browser served by the ThingSpeak cloud. The Artix-7 FPGA device is used to implement the proposed wireless communication system, for which design and synthesis were done using the Xilinx Vivado 2015.2 tool. The proposed system uses a low amount of power and is suitable for a standalone, highly secure TRNG-based IoT application. The National Institute of Standard and Testing (NIST SP 800-22) test showed that ADPLL with finite impulse response (FIR) filter-based TRNGs are better for encrypting IoT devices for secure wireless communication.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Huirem Bharat Meitei

Department of Electronics and Communication Engineering, National Institute of Technology Manipur

Imphal, India

Email: thinktank453@gmail.com

1. INTRODUCTION

The internet of things (IoT) is a paradigm of revolutionary innovation in which devices like sensors and actuators are linked, so they can talk to each other and analyze data with the least amount of assistance from people. The produced information will be analyzed to offer consumers useful functions. Thingspeak is a cloud-based IoT analytics platform that collects, visualizes, and assesses real-time data. Moreover, there are presently few IoT frameworks enabling home automation, and field-programmable gate array (FPGA) is rarely used in most of this ecosystem. Considering the significance of IoT network, it is imperative to maintain information accuracy as well as confidentiality [1]. FPGAs already can outperform Raspberry Pi-like embedded systems in a variety of areas [2]. FPGA chips with IoT applications are great for smart homes because of their longer lifespan as well as over 100 GPIO (general input/output) ports (e.g. 150 GPIO for cyclone IV device). This study, RIAT-WCS (real-time IoT application based on true random number generator (TRNG) wireless communication systems), uses the VHDL programming language to design and build architecture that takes advantage of the device parallel processing in FPGAs to serve as a localized data analysis unit for Internet of Things. It also shows the potential of FPGA with TRNG with all digital phase lock loop (ADPLL) as cryptographic system for secure IoT applications. Increased demand for internet-based services in the present day needs efficient information gathering and transmission. In this perspective, the IoT

promises to connect hardware objects and automobiles through sensing devices and the internet to facilitate effective information retention and exchange. To achieve optimal IoT performance for an operation, efficient sensing and monitoring solutions are necessary. The internet of things has triggered a transformation around the globe and has become a fascinating aspect of our lives [3]. Because of the IoT's enormous importance in every field, the day has come for every sector to embrace it as well [4]. As the IoT becomes more common, it is used for remote access to nearby specifications and other objects through the use of sensors that allow online detection of real-time information. As wearable and implantable solutions for different IoT applications become more popular, people are starting to worry about the security of the transmission infrastructure for these IoT devices.

This work describes the design, implementation, and characterization of a TRNG that uses jitter and metastability generated by ADPLL, Ring Oscillators, FF, and other primitives as sources of entropy. All secure communication devices must have a random number generator (RNG) because random numbers are necessary to produce encryption keys. Since the beginning of time, data protection has been difficult for mankind. With the introduction of integrated circuits, numerous ways of protecting them have been devised. As a result of the Internet's rapid expansion, the demand for data protection in a variety of companies is growing, and information security is attracting more attention globally [5], [6]. This criterion may typically be met by combining several software or hardware setups that can create random sequence configurations and offer the necessary public and private credentials for effective information encryption [7]. TRNGs built on FPGAs enable the use of several configurable logic blocks (CLBs) linked via programmable interconnects, making it easier to build a robust architecture that is especially useful for digital VLSI systems. Additionally, because the noise source offers an unfiltered data block, periodic post-processing is required to increase the unpredictability of the resulting random patterns. Compared to analog circuit-based TRNGs, TRNGs based on FPGA technology offer more adaptability, superior performance, and decreased complication [8]. Thus, an ADPLL-based method for producing random sequences that are sufficiently secure is proposed for our proposed secure wireless system. ADPLL-based TRNGs provide several advantages over PLL-based TRNGs, particularly easy synthesis and rapid customization [9].

This article describes the layout, development, and interpretation of a design for true random number generators that employed the jitters created by an ADPLL centered on an finite impulse response (FIR) filter [10] as a digital low pass filter and the jitters obtained from the suggested ring oscillators as randomness sources. Ansari *et al.* [11] TRNG-generated random numbers can be used to create highly secure cryptographic keys for the transmission and receipt of data in IoT devices. In comparison, FPGAs provide a resource-constrained ecosystem (fixed logic blocks) devoid of analog blocks that are generally employed to create high entropic outputs. Contrary to existing techniques, we describe ways to create a reliable TRNG design utilizing only the built-in features of the FPGA XC7A35T-CPG236-1 hardware. Also, we compare the proposed TRNG's efficiency to that of other TRNGs that have been shown to work well in the field. The proposed architecture uses a lot less resources but still has a very high throughput percentage at low power can be used for TRNG base secure standalone IoT application. TRNG architectures generate random number patterns with an output data sequence that passes the National Institute of Standard and Testing (NIST) test, indicating their appropriateness for usage in smart cards, IoT devices, and cyber security communications networks. The paper consists of the following sections: Section 1. Introduction; Section 2. The proposed wireless communication system in the IoT platform and section 3. FPGA realization of the proposed wireless communication network used for secured IoT application section 4. Experiment results for secure wireless communication in IoT platform section 5. Conclusion.

2. THE PROPOSED WIRELESS COMMUNICATION SYSTEM IN THE IOT PLATFORM

Figure 1 depicts the proposed model for the real-time TRNG-based secure wireless communication system for IoT application. Here the MQ-2 gas sensor and tracking sensor value are XORed [12] with the used TRNG to produce encrypted data which is transferred to receiver architecture by using the Esp8266 Wi-Fi module. The securely encrypted information is transferred in the Thingspeak cloud using Esp8266 Wi-Fi module on the Tx side. After receiving the encrypted data from the Tx side decryption is done at the Rx side for generating the original message.

2.1. Sensing and monitoring operation flow chart

Figure 2 explained about the IoT operation flowchart for the thing speak-based sensing network outlines. This process provides a simple and effective solution for data collection, analysis, and monitoring of various parameters. The steps and processes involved in the operation of the TRNG architecture that utilizes the ThingSpeak platform for data collection and analysis is typically given in the below flowcharts.

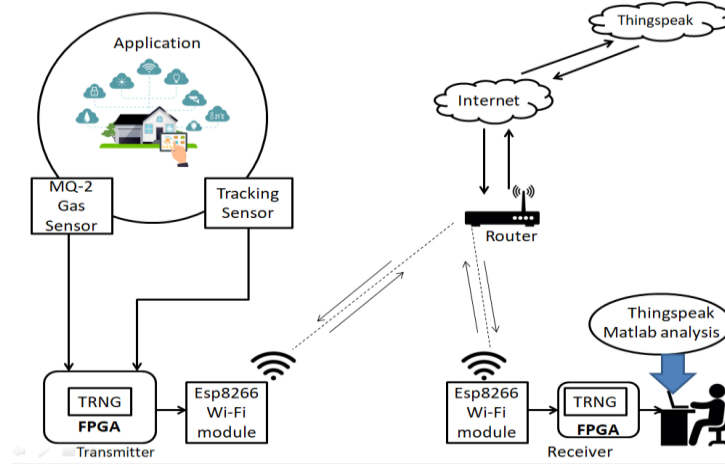


Figure 1. Proposed model for the real-time TRNG-based secure wireless communication system

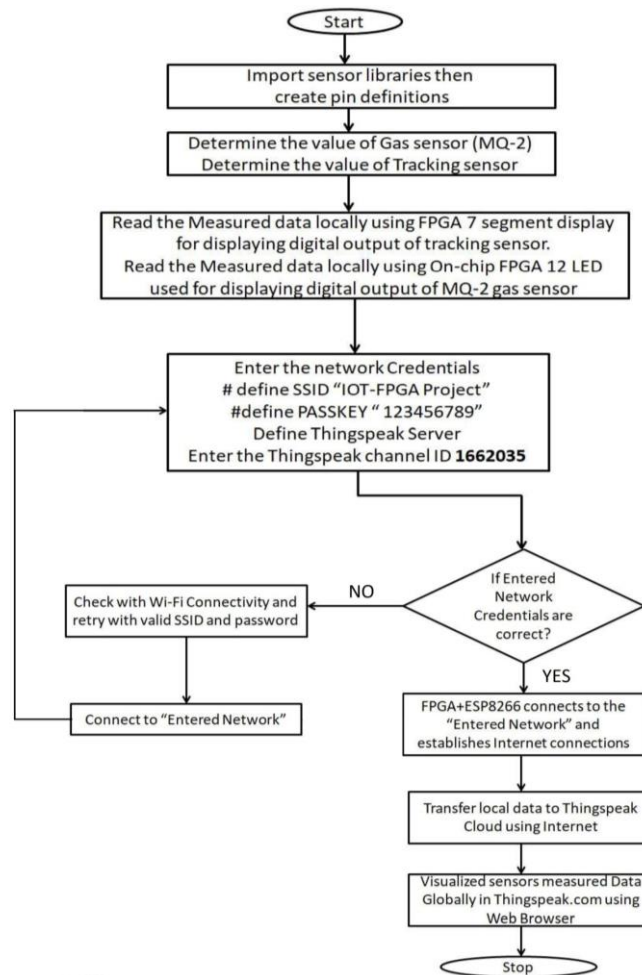


Figure 2. Flowchart: The IoT operation flowchart for the thing speak-based sensing network

3. FPGA REALIZATION OF THE PROPOSED WIRELESS COMMUNICATION NETWORK FOR SECURED IOT APPLICATION

FIR based ADPLL is one of the important elements which is used in our TRNG as an important source of entropy other than flip flop and ring oscillators. ADPLLs are digital systems at the circuit level, the majority of the functional blocks may be reproduced using FPGA. In simple terms, ADPLL is a completely digital

phase-locked loop (PLL) [13]. It comprises 3 components: phase detectors (PD), loop filters (LF), along with digital control oscillators. The three devices are linked in a closed-loop feedback control system. The 3rd order broadcast low passes FIR filter is used as a loop filter to reduce unwanted frequency content or noise. ID counters operate analogously to DCOs such as they modify the frequencies following the LF signal output. Figure 3 depicts the first-order circuit diagram of an ADPLL with FIR filter based on Keiser window. Mf_0 , that is the clock for the FIR filter clock pulse, is equivalent to the FIR filter clock. ID Clock, equivalent to $2Nf_0$, is the DCO clock signal, while M and N are the FIR filter and DCO modulus controls, respectively. The output of the XOR gate, XOR-out, and the clock are fed to the FIR filter's source, which produces a carry signal (ca) [13]. The XOR-gate serves as a phase detector [14].

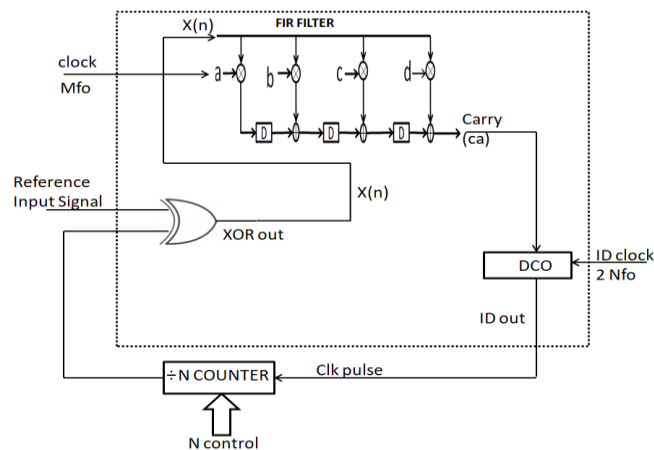


Figure 3. First-order ADPLL circuit diagram [10]

The basic architecture of the ADPLL-based TRNG used in our proposed design is depicted in Figure 4. The existing TRNG using two identically design RO is very challenging to match the period while implementing in FPGA. Furthermore, TRNG should not be technology-dependent. As [14], analogue PLL was utilised to perform in many technique like coherent sampling (CS) phenomenon. But due to the non-availability of the PLL in all the FPGA family makes difficult for designers. Moreover, PLL-based TRNG requires more energy and takes up more space than ADPLL-based TRNG [15]. So our noval real-time IoT application based on TRNG wireless communication systems (RIAT-WCS) could get completely manufactured and enhanced in a brief period because of their ADPLL with FIR-based digital construction. And the difficulties in matching the period are also avoided due to the use of single free-running ROs. To create a pulse signal which is used as the clock of the used TRNG architecture we employed a pulse generator system which is made up of a string of 51 inverters in our RO architecture. TRNG designs based on an FIR-based ADPLL are created using VHDL. Considering all significant sources of entropy, including jitter form ADPLLs [16] and with ring oscillators, in addition to the flip-flop metastability state. The ring oscillator's jitter is in phase with the jitter created by the ADPLL used as an entropy source.

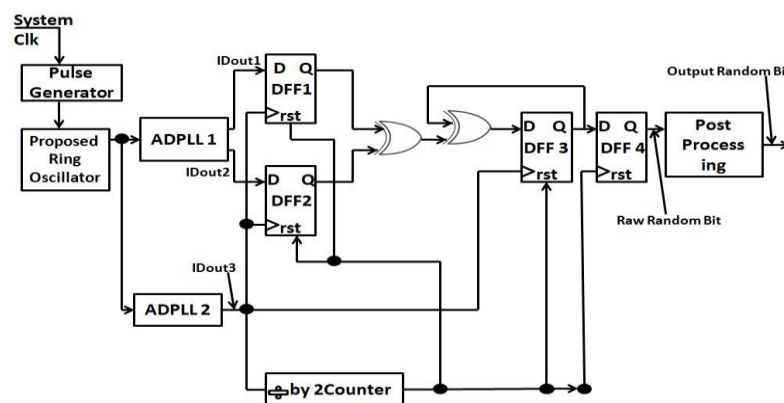


Figure 4. Proposed TRNG with ADPLL based on FIR filter used in RIAT-WCS architecture [10]

As seen in Figure 4, our proposed design consists of two ADPLLs set up independently of one another, a sampled network, as well as a controller. An all-digital phase locked loop is used to link the frequency, inputting phase, and outputting phase. As a result, phase difference is utilized in ADPLL to diminish the disparity among the 2 impulses. The design of this investigation was influenced by Kohlbrenner and Gaj's TRNG proposal in [17]. Retaining the existing design but replacing the ROs with two ADPLLs, a single free-running RO, and pulse generators. The architectural design of the ADPLL with FIR-based TRNG was realized with two ADPLLs. Because both ADPLL 1 and ADPLL 2 use a single free-running ring oscillator as their input signal, the outputs of both ADPLLs are mutually connected. Figure 5 depicts the DSO output waveform of the TRNG architecture used in RIAT-WCS.

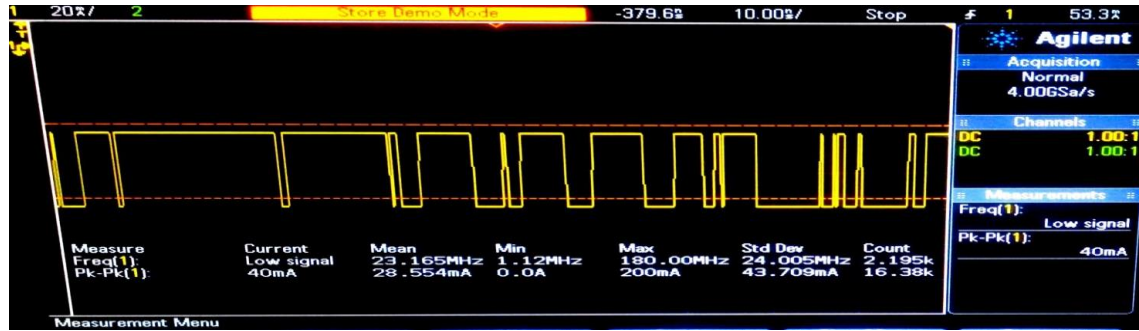


Figure 5. DSO waveform of TRNG used in RIAT-WCS architecture [10]

The test was carried out using an Artrix-7 FPGA system and the resulting pattern is captured using a digital storage oscilloscope. The FPGA pinouts for the TRNG implementation centered on ADPLL with Esp8266 for IoT application are listed in Tables 1 and 2. The overall system clock is provided by using the W5 input mode and the V17 T-FF input. The result is linked to JB1:A14, the live probe of the DSO, and JB5:GND, the ground probe.

Table 1. Pin details for implemented transmitter architecture

Symbol	Details	Mode:-In=Input Out=Output	FPGA Pin	Esp8266	Test-1 (MQ-2 gas sensor)	Test-2 (Tracking sensor)
CLK	System clock	In	W-5			
t	T-FF	In	V-17			
rst	Reset	In	V-16			
q1	Output random bit	Out	A-14			
sensors	Sensor information	In	K-17		Data	Data
xorout	Encrypted data	Out	M-18			
Tx	UART TX output	Out		Txd		
Rx	UART RX input	In		Rxd		
Vcc	Power supply	n/a	USB port	Vcc	Vcc	Vcc

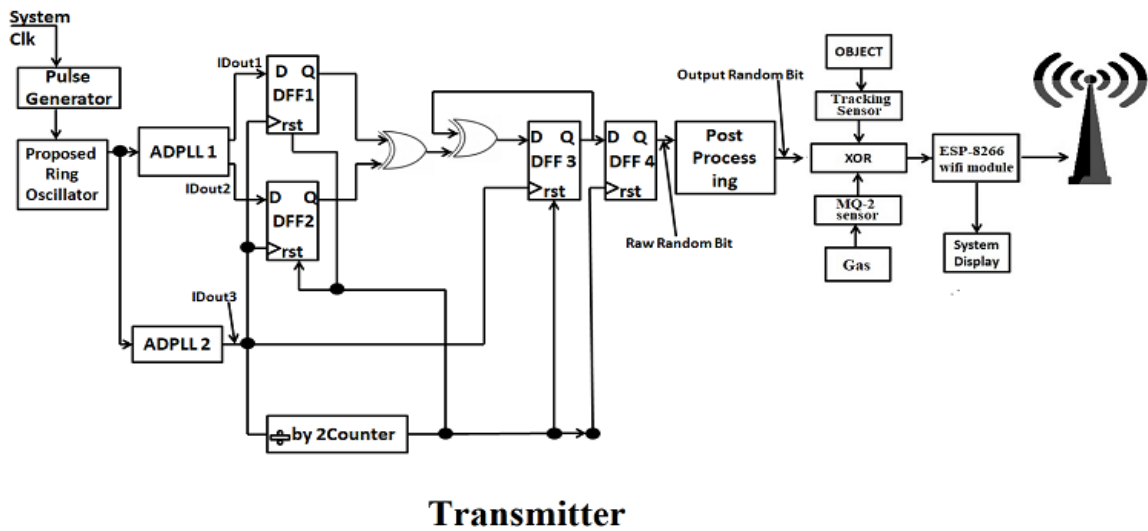
Table 2. Pin details for implemented receiver architecture

Symbol	Details	Mode:-In=Input, Out=Output	FPGA Pin	Esp8266 Wi-Fi module
CLK	System Clock	In	W-5	
t	TFF	In	V-17	
rst	Reset	In	V-16	
q3	Output random bit	Out	A-14	
Tx	UART Tx output	Out		TXD
Rx	UART Rx input	In		RXD
Vcc	Power Supply	n/a	USB-port	Vcc

3.1. Details of transmitter architecture

Figure 6 depicts the proposed transmitter block diagram used in our proposed wireless system and Figure 7 represents the Tx setup with MQ-2 sensor showing the detection of gas. XORing the jitter noise generated by dual ROs with the 400 MHz ID output stream (DCO out) between the ADPLL with Q1 of DFF1-derived feedback loops. The outcome of DFF1's Q1 is subsequently transferred to DFF2's d2, alongside the counter's CLK signals. Q2 of DFF2 subsequently transmits the generated random stream of bits. The ADPLL

circuitry was developed with a frequency range (f_0) of 50 MHz and a modulus factor (k) of 4. f_0 represents the centre frequency, N equals 8, and M equals 16. In this case, M is a factor with usual values of 8, 16, and 32. The ID clock pulse has a value of $2Nf_0$, which corresponds to the DCO clock signal. After XORing the unpredictable data generated from the TRNG using the entropy of the sensor information, a stream of encrypted messages is formed and subsequently interfaced using the Esp8266 for wireless communication. In addition, a serial monitor exhibited relayed sensor data. Information or data exchanged securely utilizing a TRNG-encrypted framework for IoT applications, therefore, becomes extremely safe when employing this cryptographic algorithm.



Transmitter

Figure 6. Block diagram of the transmitter architecture used in IoT based wireless communication system



Figure 7. Tx setup with gas detection using MQ-2 sensor

3.2. Specifications of receiver architecture

The receiver is intended to efficiently retrieve information transferred through the transmitting end. The information is decrypted by the receiver (Rx) that used a decryption technique. This part explains the device configuration needed for the proposed operation, in addition to the specifics of each hardware module needed to initially create the overall unit. To extract the original data after wirelessly retrieving encrypted messages through the Wi-Fi module, decryption is conducted utilizing an XOR operation in connection using an ADPLL-based TRNG design. The block diagram of the receiver, as depicted in Figure 8, is comprised of two key elements: a Wi-Fi module Esp8266 and TRNG architecture centered on ADPLL with an FIR filter for decryption. The information transferred by the transmitter is intercepted securely by the receiver, which then XORs the received data with TRNG to uncover the actual information. Figure 9, illustrate the receiver (Rx) hardware setup for RIAT-WCS architecture used in our projects.

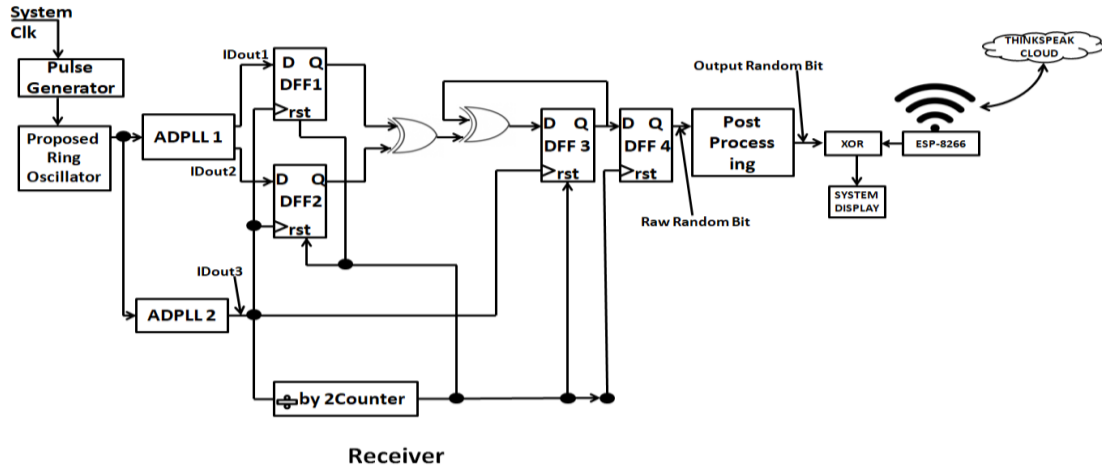


Figure 8. Block diagram of the receiver architecture used in IoT-based wireless communication system

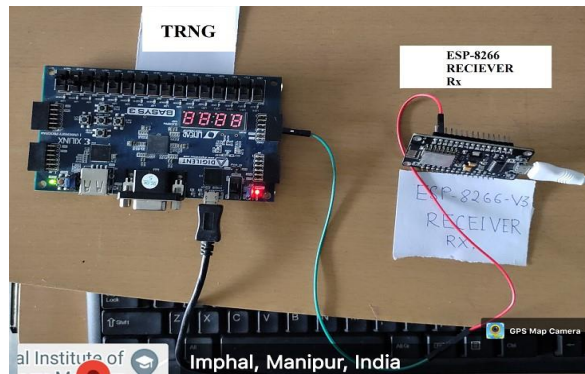


Figure 9. Receiver Rx setup for RIAT-WCS architecture

3.3. XADC wizard detail implementation

The XADC wizard is effectively integrated into the vivado development package. Channel sequencer which is present in XADC wizard (3.1) in vivado v2015.2 is used for generating more than one analog channel in the FPGA board [18]. So that we can connect numerous analog input sensors to the FPGA board. PMOD JXADC is used for on-chip ADC conversion. 7 segment displays is used for displaying the digital output of the tracking sensor connected with PMOD JXADC of Channel 1 (CH 1), whereas on-chip FPGA 12-LED is used to display the digital output of the MQ-2 gas sensor connected with PMOD JXADC of Channel 3 (CH 3).

4. EXPERIMENT RESULTS FOR SECURE WIRELESS COMMUNICATION IN THE IOT PLATFORM

Vivado 2015.2 the Xilinx ISE tool is used to encrypt sensor data and to design the TRNG architecture for IoT applications. The XC7A35TCPG236-1 device (Artrix-7 FPGA board) is used to design a proposed wireless communication system. Table 3 discusses the FPGA pinouts for the ADPLL-based TRNG implementation of transmitter used in wireless communication technology. Analog input of the MQ-2 gas sensor is interfaced with the FPGA board by using XADC. Analog output of the tracking sensor is interfaced with FPGA by using channel 1(CH 1) PMOD JXADC whereas the analog output of the MQ-2 gas sensor is interfaced with FPGA channel 3 (CH 3) PMOD JXADC. If the MQ-2 gas sensor value crossed a fixed threshold value then gas is detected and the MQ-2 gas sensor value is logic high. If the MQ-2 value doesn't cross a fixed threshold value then gas is not detected and the MQ-2 gas sensor value is logic low. This logic high and logic low value of the MQ-2 gas sensor is XORed using TRNG architecture to produce encrypted data. Similarly for tracking sensor value logic high is shown according to the fixed threshold value which is then XOR with TRNG random bit too produced encrypted data which is transferred wirelessly using ESP 8266 wifi module. After transferring from the transmitter side through the cloud the receiver then decrypted the data to produce the original sensor value which is then analyzed using MATLAB think speak IoT cloud. The transmitter (Tx) side

consumed an area of 1 LUTs along with a power of 74 mW whereas the receivers (Rx) side utilized 2 LUTs and a power of 76 mW. According to the device utilization data presented in table, the suggested RIAT-WCS utilizes a total of three LUTs implying that the overall resource consumption is low in comparison to previous architectures in these sectors.

Table 3. IP catalog for On-chip ADC conversion

Channel		Negative	Positive	Address	Sensor interface with XADC
CH 1	vauxp4 vauxn4	JXAC10:N1	JXAC10:N2	0010100	Tracking Sensor
CH 3	vauxp14 vauxn14	JXAC8:M3	JXAC8:L3	0001110	MQ-2 Gas Sensor

4.1. Testing

The US-NIST publishes the probabilistic test package for random and pseudo-random number generators [19] for encryption algorithms. The suggested design uses VHDL to create random bits that are stored in a text file. To ensure the uniqueness and stochastic nature of the produced random sequence, NIST tests are performed on 150 numbers of random bits from the TRNG architecture using MATLAB version R2015a. With a confidence level of 99.9%, a configuration having a P-value greater than or equal to 0.001 is regarded to fulfill the NIST test for randomness [20]. Table 4 shows the NIST analysis findings of the proposed TRNG used in our RIAT-WCS architecture, which show that the resulting pattern is indeed stochastic. Figures 10 and 11 illustrate the MATLAB Thinkspak IoT application output waveforms collected and analyzed by the Thinkspaeak analyzer. After displaying the data in Thingspeak, the next stage is to assess the detected data in MATLAB analyzers toolkits.

Table 4. NIST (SP 800-22) test result [10]

NIST Test	P-value
Frequency	0.722
Block frequency	0.994
Run	0.041
Rank	0.000*
DFT	0.022
Serial test	0.994
Linear complexity Test	0.599
Longest run Test	0.000*
Approximate entropy Test	0.030
Cumulative sum Test	0.999
Random excursions Test	0.050

* When the p factor is 0.000, NIST fails

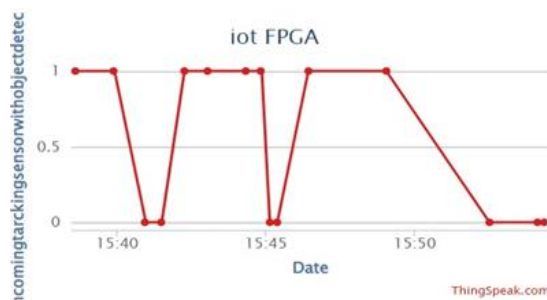


Figure 10. Tracking sensor with object detection

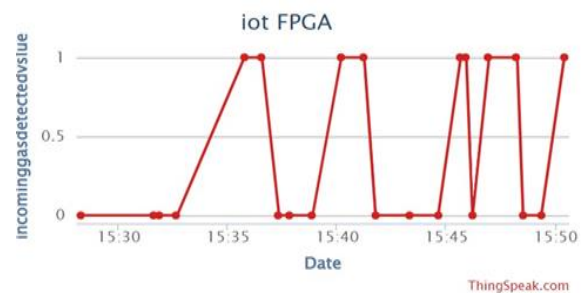


Figure 11. MQ-2 gas sensor detection analysis

4.2. Comparison with the existing design

Table 5 evaluates the performance of different TRNGs, while Table 6 analyzes the architectures of several TRNGs using the synthesis review. The method we suggested maximizes the usage of existing hardware components. In addition, the Tx design uses 7.4 mW and the Rx design uses 7.6 mW, which is significantly lower than prior research. With a maximum bit rate of 202.47 Mbps for the Transmission system and 680.73 Mbps for the receivers, tables demonstrates that the design's entire output throughput is unchanged despite using fewer hardware components and spending minimum power.

Table 5. Performance comparison among various architectures

Paper	Entropy source	Device	Hardware resource	Post-processing
Transmitter for RIAT-WCS	Jitter or Metastability	Xilinx Artrix-7 FPGA	1 LUT	yes
Receiver for RIAT-WCS	Jitter or Metastability	Xilinx Artrix-7 FPGA	2 LUTs	yes
Nannipieri <i>et al.</i> [21]	Jitter and Metastability	Intel Stratix IV	288 LUTs	N/a
Fujieda [22]	Latches oscillatory Metastability	Xilinx Artrix-7 FPGA	40 LUTs	N/a
Wang <i>et al.</i> [23]	Self-time Ring oscillator	Xilinx Artrix-6 FPGA	56 LUTs	N/a
Lin <i>et al.</i> [24]	Jitter and Metastability	Xilinx Artrix-7 FPGA	50 LUTs	N/a
Jun and Kocher [25]	Chaotic ring oscillator	Xilinx XC6SLX16	44 LUTs	yes
Jessa and Matuszewski [26]	Ring oscillator	Xilinx XC5VLX50T	147 LUTs	yes
Hata and Ichikawa [27]	RS-Latch	Xilinx XC4VFX20	580 Slices	No
Yang <i>et al.</i> [28]	Metastability	Altera Cyclone III	511 LUTs	yes
Fischer <i>et al.</i> [29]	PLL jitter	Altera Stratix	120 LE	yes
Ben-Romdhane <i>et al.</i> [30]	Metastability	Virtex-5	n/a LUT 64 Latches	No
Yang <i>et al.</i> [31]	Free running ring oscillator	Xilinx Spartan-6 FPGA	10 LUTs and 5 FFs	No

Table 6. Synthesis results in comparison among different TRNG architectures

Paper	Area	Power	Out bit rate	Post processing	Testing	Platform
Transmitter for RIAT-WCS	N/A	74mW	202.47 Mbit/s	Yes	NIST SP800-22	FPGA
Receiver for RIAT-WCS	N/A	76mW	680.73 Mbit/s	Yes	NIST SP800-22	FPGA
Zhang and Wang [32]	0.02mm ²	0.8mW	25 Mbit/s	No	FIPS 140-2	0.09 μ m CMOS
Akgul <i>et al.</i> [33]	N/A	N/A	4.59Mbit/s	XOR	FIPS 140-1 and NIST SP800-22	FPGA
Wannaboon <i>et al.</i> [34]	0.038mm ²	1.32mW	50Mbit/s	Von Neumann	NIST SP800-22 and TestU01	0.18 μ m CMOS
Moqadasi and Ghouschi [35]	N/A	N/A	447.83 Mbit/s	XOR and 32-bit edition	NIST SP 800-22	CPU
Cicek <i>et al.</i> [36]	N/A	125 mW	1.5Mbit/s	N/A	NIST SP800-22	FPGA
Teh <i>et al.</i> [37]	N/A	N/A	2.02Mbit/s	6 bit LFSR	FIPS 140-1	0.18 μ m CMOS
Park <i>et al.</i> [38]	93.1mm ²	1.097mW	127Mbit/s	XOR	NIST	0.45 μ m CMOS
Ergün and Özoğuz [39]	0.057mm ²	26.1mW	300Mbit/s	XOR	NIST	0.35 μ m CMOS

4.3. Discussion

Fujieda [22], the researchers prove that the TERO significantly relies on the source of placement; thus, they present a specific TERO (TC-TERO) that prevents this difficulty at the expense of implementing FPGA-dependent primitives, thereby losing hardware flexibility. Wang *et al.* [23], researchers describe a second implementation based on STRs. Lin *et al.* [24], the paper presented a highly competitive option in areas of entropy, complexity, as well as resource consumption. Jun and Kocher [25], it is possible to design a chaotic Ring Oscillators based TRNG having a throughput of 125 Mbps that is both simple and resilient. According to the proposed TRNG systems [31], requires a larger number of LUTs and generates the lowest throughput. According to recent studies, TRNG can also use a digitised version of ADPLL with finite-difference time ROs for secure wireless data transmission via Bluetooth connections over short distances. Keeping into account chaos' lower frequency and narrowband, TRNG is built on a conventional chaotic oscillator as the source of randomness, comparable to no-equilibrium chaotic systems [33], Jerk circuitry [34], and Chua's circuits [35]. The entire output pattern of various TRNGs based on discrete-time chaos demonstrates that [37] is substantially faster than other chaotic outcome values due to its processing. The area of [39] is bigger than the TRNG space of the equivalent CMOS technology in [38]. This is due to the fact that the researchers constructed systems with a 2-stage pipelines ADC and a 8-stage pipelines ADC. ADC is frequently used to generate chaotic patterns having random variables; it is quicker but necessitates a significant amount of storage.

5. CONCLUSION

This study explores the design and implementation of an intelligent and highly secure IoT-based network that operates in real-time. Encryption and decryption are performed using a TRNG architecture built on ADPLL using an FIR loop filter. An IoT-based smart and highly secure system could be developed effectively with the TRNG encryption technique built on FPGA devices. The peripheral sensory interface designed with FPGA architecture is configurable, consumes less power, and is highly accurate. This property

makes the TRNG an ideal option for incorporation into larger crypto algorithms and the best choice for a secure IoT data transmission system. By utilizing the entire source of entropy generated by the ADPLL, flip-flop, and other device components, a secure and efficient TRNG is formed. By incorporating FIR-based ADPLL within the TRNG architectures, we were capable of minimizing power demand and employing fewer system resources (1LUT for Transmitter design and 2 LUT for Receiver) while optimizing the capability of the FPGA device. Using Vivado v.2015.2, the developments, as well as simulation, are performed using a Xilinx artix-7 FPGA. Power consumption is reduced to 74 mW for TRNG used in Tx architecture and 76mW for TRNG used in Rx architecture after post-processing. Using this approach, the possibility of safeguarding security through the employment of TRNG's methodologies for IoT appears promising, making it a more reliable and robust alternative for a wide range of industries like information security, financial safety, Smart home, and Internet of Everything and so on.

ACKNOWLEDGEMENTS

Throughout the process of writing up this research work, the author would like to express his appreciation to Dr. Manoj Kumar for all of the assistance and support he provided.




REFERENCES

- [1] I. Andrea, C. Chrysostomou, and G. Hadjichristofi "Internet of things: security vulnerabilities and challenges," In: 2015 IEEE *symposium on computers and communication (ISCC)*, pp. 180-187, 2015, doi: 10.1109/ISCC.2015.7405513.
- [2] S. Narayan and C. Lakshminarayana, "Performance enhancement in active power filter (APF) by FPGA implementation," *International Journal of Electrical and Computer Engineering*, vol. 81, pp. 689-698, 2018, doi: 10.11591/ijece.v8i2.pp689-698.
- [3] D. Meisner, C. M. Sadler, L. A. Barroso, W.-D. Weber, and T. F. Wenisch, "Power management of online data-intensive services," *SIGARCH Comput. Archit. News*, vol. 39, no. 3, pp. 319-330, 2011, doi: 10.1145/2024723.2000103.
- [4] R. K. Pradhan and M. A. Gregory, "Access network energy efficient dynamic power scaling," *Australasian Telecommunication Networks and Applications Conference (ATNAC) 2012*, Brisbane, QLD, Australia, 2012, pp. 1-5, doi: 10.1109/ATNAC.2012.6398068.
- [5] L. Zhou, F. Tan, and F. Yu, "A robust synchronization-based chaotic secure communication scheme with double-layered and multiple hybrid networks," in *IEEE Systems Journal*, vol. 14, no. 2, pp. 2508-2519, June 2020, doi: 10.1109/JSYST.2019.2927495.
- [6] Z. Xia, Z. Fang, F. Zou, J. Wang, and A. K. Sangaiah, "Research on defensive strategy of real-time price attack based on multiperson zero-determinant," *Security and Communication Networks*, 2019, doi: 10.1155/2019/6956072.
- [7] G. D. P. Stanchieri, A. D. Marcellis, E. Palange, and M. Faccio, "A true random number generator architecture based on a reduced number of FPGA primitives," *AEU - International Journal of Electronics and Communications*, vol. 105, pp. 15-23, Jun. 2019, doi: 10.1016/j.aeue.2019.03.006.
- [8] R. Gupta, A. Pandey, and R. K. Baghel, "Efficient design of chaos based 4 bit true random number generator on FPGA," *International Journal of Engineering & Technology*, vol. 7, no. 3, p. 1783, Aug. 2018, doi: 10.14419/ijet.v7i3.16586.
- [9] H. B. Meitei, and M. Kumar "FPGA implementation of true random number generator architecture using all digital phase-locked loop," *IETE Journal of Research*, vol. 68 no. 3, 2021, doi: 10.1080/03772063.2021.1963333.
- [10] H. B. Meitei and M. Kumar, "FPGA implementations of TRNG architecture using ADPLL based on FIR filter as a loop filter," *SN Applied Sciences*, vol. 4, no. 4, Mar. 2022, doi: 10.1007/s42452-022-04981-6.
- [11] U. Ansari, A. K. Chaudhary, and S. Verma, "Enhanced true random number generator (TRNG) using sensors for IoT security applications," *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*, Kannur, India, 2022, pp. 1593-1597, doi: 10.1109/ICICICT54557.2022.9917919.
- [12] H. B. Meitei and M. Kumar, "FPGA implementation of a wireless communication system for secure IR sensor data transmission using TRNG," *International Journal of Engineering Trends and Technology*, vol. 70, no. 7, pp. 220-237, Jul. 2022, doi: 10.14445/22315381/ijett-v70i7p223.
- [13] A. K. Chaudhary and M. Kumar, "Design and implementation of ADPLL for digital communication applications," *2017 2nd International Conference for Convergence in Technology (I2CT)*, Mumbai, India, 2017, pp. 397-401, doi: 10.1109/I2CT.2017.8226159.
- [14] M. Fischer, and V. Drutarovsky, "True random number generator embedded in reconfigurable hardware," in *Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems (CHES'02)*, ser. *Lecture Notes in Computer Science*, vol. 2523. Springer-Verlag, 2002, pp. 415-430.
- [15] K. S. Moon and M. S. Kim, "0.18 μ m CMOS low power ADPLL with a novel local passive interpolation time-to-digital converter based on tri-state inverter," - DRS. <https://repository.library.northeastern.edu/files/neu:1338> (accessed Jan. 17, 2023).
- [16] S. Radhapuram, T. Yoshihara, and T. Matsuoka, "Design and emulation of all-digital phase-locked loop on FPGA," *Electronics*, vol. 8, no. 11, p. 1307, Nov. 2019, doi: 10.3390/electronics8111307.
- [17] P. Kohlbrenner, and K. Gaj, "An embedded true random number generator for FPGAs," *ACM/SIGDA International Symposium on Field Programmable Gate Arrays - FPGA*, vol. 12, pp. 71-78, 2004, doi: 10.1145/968280.968292.
- [18] Documentation Portal. Docs.xilinx.com, Series-FPGAs-and-Zynq-7000-SoC-XADC-Dual-12-Bit-1-MSPS-Analog-to-Digital-Converter-User-Guide-UG480, 2015.
- [19] Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *NIST Special Publication*, 800-22 (revised May 15 2002).
- [20] L. Bassham *et al.*, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Csrc.nist.gov. <https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final>, 2010.
- [21] P. Nannipieri *et al.*, "True random number generator based on fibonacci-galois ring oscillators for FPGA," *Appl. Sci.*, vol. 2021, vol. 11, p. 3330, doi: 10.3390/app11083330.
- [22] N. Fujieda, "On the feasibility of TERO-based true random number generator on xilinx FPGAs," *2020 30th International Conference on Field-Programmable Logic and Applications (FPL)*, Gothenburg, Sweden, 2020, pp. 103-108, doi: 10.1109/FPL50879.2020.00027.




- [23] X. Wang *et al.*, "High-throughput portable true random number generator based on jitter-latch structure," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 2, pp. 741-750, Feb. 2021, doi: 10.1109/TCSI.2020.3037173.
- [24] J. Lin, Y. Wang, Z. Zhao, C. Hui, and Z. Song, "A new method of true random number generation based on galois ring oscillator with event sampling architecture in FPGA," *2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, Dubrovnik, Croatia, 2020, pp. 1-6, doi: 10.1109/I2MTC43012.2020.9129357.
- [25] B. Jun and P. Kocher "Intel Random Number Generator," Rambus, Apr. 22, 1999. <https://www.rambus.com/intel-random-number-generator/> (accessed Jan. 17, 2023).
- [26] M. Jessa and L. Matuszewski, "Enhancing the randomness of a combined true random number generator based on the ring oscillator sampling method," *2011 International Conference on Reconfigurable Computing and FPGAs*, Cancun, Mexico, 2011, pp. 274-279, doi: 10.1109/ReConFig.2011.35.
- [27] H. Hata and S. Ichikawa "FPGA implementation of metastability-based true random number generator," *IEICE Trans Inf Syst*, vol. 95, no. 2, pp. 426-436, 2012, doi: 10.1587/trans inf. e95.d. 426.
- [28] Y. Yang *et al.*, "A reliable true random number generator based on novel chaotic ring oscillator," In: *2017 IEEE international symposium on circuits and systems (ISCAS)*, 2017.
- [29] V. Fischer, M. Drutarovsky, M. Šimka, and N. Bochar, "High performance true random number generator in altera stratix FPLDs," *Field Progr Log Appl.*, 2004, doi: 10.1007/978-3-540-30117-2_57.
- [30] M. Ben-Romdhane, T. Graba, and J.-L. Danger "Stochastic model of a metastability-based true random number generator," *Trust Trust Comput.*, 2013, doi: 10.1007/978-3-642-38908-5_7.
- [31] B. Yang, V. Rožic, M. Grujic, N. Mentens, and I. Verbauwhede, "ESTRNG: a high-throughput, low-area true random number generator based on edge sampling," *IACR Trans Cryptogr Hardw Embed Syst*. 2018, doi: 10.13154/tches.v2018.i3.267-292.
- [32] X. Zhang and C. Wang, "A novel multi-attractor period multi-scroll chaotic integrated circuit based on CMOS wide adjustable CCCII," in *IEEE Access*, vol. 7, pp. 16336-16350, 2019, doi: 10.1109/ACCESS.2019.2894853.
- [33] A. Akgul, H. Calgan, I. Koyuncu, I. Pehlivan, and A. Istanbulu, "Chaos-based engineering applications with a 3D chaotic system without equilibrium points," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 481-495, Nov. 2015, doi: 10.1007/s11071-015-2501-7.
- [34] B. Wannaboon, M. Tachibana, and W. San-Um, "A 0.18- μm CMOS high-data-rate true random bit generator through $\Delta\Sigma$ modulation of chaotic jerk circuit signals," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 28, no. 6, p. 063126, Jun. 2018, doi: 10.1063/1.5022838.
- [35] H. Moqadasi and M. B. Ghaznavi-Ghouschi, "A new Chua's circuit with monolithic Chua's diode and its use for efficient true random number generation in CMOS 180 nm," *Analog Integrated Circuits and Signal Processing*, vol. 82, no. 3, pp. 719-731, Feb. 2015, doi: 10.1007/s10470-015-0498-y.
- [36] Cicek, A. E. Pusane, and G. Dundar, "A new dual entropy core true random number generator," *Analog Integrated Circuits and Signal Processing*, vol. 81, no. 1, pp. 61-70, May 2014, doi: 10.1007/s10470-014-0324-y.
- [37] J. S. Teh, A. Samsudin, M. Al-Mazrooie, and A. Akhavan, "GPUs and chaos: a new true random number generator," *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1913-1922, Jul. 2015, doi: 10.1007/s11071-015-2287-7.
- [38] M. Park, J. C. Rodgers, and D. P. Lathrop, "True random number generation using CMOS Boolean chaotic oscillator," *Microelectronics Journal*, vol. 46, no. 12, pp. 1364-1370, Dec. 2015, doi: 10.1016/j.mejo.2015.09.015.
- [39] S. Ergün and S. Özoğuz, "Truly random number generators based on non-autonomous continuous-time chaos," *International Journal of Circuit Theory and Applications*, vol. 38, no. 1, pp. 1-24, Feb. 2010, doi: 10.1002/cta.520.

BIOGRAPHIE OF AUTHORS



Er. Huirem Bharat Meitei    is presently a Chartered Engineer (CEIEI). He is also a Ph.D scholar at the National Institute of Technology, Manipur (India) and earned M.Tech degree in Electronic and Communication Engineering specialized in embedded system from JNTU Kakinada, Andhra Pradesh. Embedded design, TRNG, IoT, FPGA design, and network security are among his research interests. With technical expertise in FTTH, fiber network design he work in different project like Google fiber, verizon and also work on different renewable energy project. He can be contacted at email: thinktank453@gmail.com.



Dr. Manoj Kumar    is currently working as an Assistant Professor in Department of Electronics and Communication Engineering, National Institute of Technology, Manipur. Having completed his B.Tech Degree from NIT Calicut, and MTECH degree from Indian Institute of Information Technology (IIIT), Allahabad, he started working as an Assitant Professor in NIT Manipur and received his PhD degree from National Institute of Technology Manipur. He has published several research articles in national and international reputed journals and attended various conferences across India. His research area includes VLSI design, VLSI-DSP, digital electronics, and communications. He has published over 35 scientific articles in International, National Journals of repute and in several conferences. He can be contacted at email: manoj@nitmanipur.ac.in.