Design and Implementation of a Fast, Platform-Adaptive, AIS-20/31 Compliant PLL-Based True Random Number Generator on a Zynq 7020 SoC FPGA

Oğuz Yayla[1] and Yunus Emre Yılmaz[1,2]

[1] Institute of Applied Mathematics, Middle East Technical University, 06800 Ankara, Turkey
[2] Aselsan Inc., Ankara, Turkey
oguz@metu.edu.tr, yeylmz@gmail.com

Abstract. Phase-locked loops (PLLs) integrated within field-programmable gate arrays (FPGAs) or System-on-Chip FPGAs (SoCs) represent a promising approach for generating random numbers. Their widespread deployment, isolated functionality within these devices, and robust entropy, as demonstrated in prior studies, position PLL-based true random number generators (PLL-TRNGs) as highly viable solutions for this purpose. This study explicitly examines PLL-TRNG implementations using the ZC702 Rev1.1 Evaluation Board featuring the Zynq 7020 SoC from Xilinx, utilizing a configuration involving three such boards for experimental validation. Parameters governing the PLL-TRNG are optimized using a backtracking algorithm. Additionally, a novel methodology is proposed to enhance the rate of random data bit generation while preserving entropy characteristics. Performance metrics are rigorously evaluated against the criteria set by the German Federal Office for Information Security (BSI) AIS-20/31 Tests, accompanied by detailed descriptions of the implementation process. Furthermore, the suitability of our PLL-TRNG designs, attributed to their low resource utilization, is demonstrated.

Keywords: random number generation, PLL-TRNG, AIS-20/31

1 Introduction

Random numbers are essential for cryptographic systems, requiring high statistical quality, which is provided by True Random Number Generators (TRNGs) based on physical phenomena to ensure unpredictability. In this study, jitter, defined as the fluctuation of clock periods in the time domain, is used as the entropy source. Phase-Locked Loops (PLLs), commonly found in field-programmable gate arrays (FPGAs) and System-on-Chip (SoC) platforms, are selected for entropy harvesting due to their inherent noise and jitter. The simplicity of PLL-based TRNGs (PLL-TRNGs) and their effective cryptographic properties have been demonstrated in previous works, with designs utilizing one or two PLLs, as explained in [1], [2], [3], and [4], along with a stochastic model introduced in [5].

Additionally, the implementation details of PLL-TRNGs are analyzed in [6] and [7], highlighting their straightforward design, coherent sampling, and isolated locations in FPGAs and SoCs, making them highly suitable for secure random number generation.

The primary challenge in PLL-TRNG design is the selection of optimal PLL settings from a vast configuration space. The chosen parameters must yield both a sufficient entropy rate and an adequate output bit rate. This study adopts the parameter determination process outlined in [10]. Notably, the backtracking algorithm employed in [10] offers significant advantages over previous search algorithms for PLL-TRNG design, as presented in [1], [8], and [9].

While it is advantageous to implement PLL-TRNG considering its high entropy and isolated locations of PLL, one of the main drawbacks of the PLL-TRNG is its relatively low random data output speed. A new PLL-TRNG method using four PLLs is proposed to overcome this disadvantage. For this purpose, we chose Xilinx Zynq 7020 SoC instead of an FPGA. Since they offer higher integration, lower power, smaller board sizes, and higher bandwidth communication between the processor and FPGA.

Once random numbers are generated, their quality must be assessed. For this evaluation, the AIS-20/31 standard [11], a methodology proposed by the German Federal Office for Information Security (BSI), is chosen.

This research culminates in the implementation of a four-PLL TRNG (4-PLL-TRNG) on the Xilinx Zynq 7020 SoC. To elucidate the design progression, a referenced configuration utilizing two PLLs and two intermediate configurations utilizing three PLLs are developed. PLL parameter optimization is achieved through a backtracking algorithm as outlined in [10]. Subsequently, four distinct PLL-TRNG configurations are implemented on the Xilinx (AMD) ZC702 Evaluation Kit Rev1.1, incorporating the Zynq 7020 SoC. To ensure design independence from the specific board, three evaluation kits are employed. Rigorous testing against AIS-20/31 standards is conducted on the generated random data. Hence, a comparative analysis with existing PLL-TRNG implementations is performed. Also, the utilization rates of 4-PLL-TRNG for three different configurations are calculated.

Our work presents three primary contributions:

1. We design a new structure of PLL-TRNG that is adaptive to new FPGAs or SoCs, which can be used to increase the bit rate without worsening cryptographic properties.
2. We conduct our new, fast, and adaptive design implemented on Xilinx Zynq 7020 SoC with respect to AIS-20/31 Tests and compare our results with previous works.
3. We demonstrate the low resource utilization of our proposed 4-PLL-TRNG and highlight its suitability for integration into IoT systems.

The paper is organized as follows. Section 2 provides the basic background information to explain how PLL-TRNG works. In Section 3, the implementation details of our proposed PLL-TRNG are explained. In Section 4, the test results

of one referenced and three proposed PLL-TRNGs are presented and compared with previous works. In the end, Section 5 concludes the paper.

2 Background Information About PLL-TRNG Implementation

2.1 Basics of Phase-Locked Loops (PLLs)

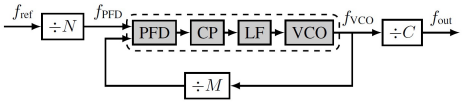

Fig. 1. Block diagram of a PLL (PFD: phase frequency detector, CP: charge pump, LF: loop filter, VCO: voltage-controlled oscillator) [10]

Table 1. Table of ranges of possible values for the PLL parameters and frequencies for Zynq-7000 SoC [14], [15]

Parameters	Xilinx Zynq-7000	
	Min	Max
f_{ref} (MHz)	19	800
P_{VCOd}	1	1
M	2	64
N	1	56
C	1	128
$f_{PFD}(MHz)$	19	450
$f_{VCO}(MHz)$	800	1600
f_{out} (MHz)	6.25	464

A PLL is a circuit (as depicted in Fig. 1) that uses an input signal to synchronize a signal from an embedded oscillator on it. The grey blocks represent the analog components, which cannot be parameterized, whereas the M, N, and C integer division coefficients, depicted in white blocks, need to be configured. These coefficients are essential for calculating the output frequency of the PLL (f_{out}) from the reference frequency (f_{ref}), as described in Equation (1).

$$f_{out} = f_{ref} \times \frac{M}{N \times C} \tag{1}$$

2.2 Random Bit Generation Principle of the PLL-TRNG

The working principle of the PLL-TRNG with one PLL, and also two PLL versions of PLL-TRNG, is presented in Fig. 2. The jittered clock signal clk_1 from the PLL is sampled by a D flip-flop (D-FF) using the reference clock signal clk_0. The 1-bit counter records the number of samples that equal one. Due to the frequency relationship established by the PLL, a pattern with a period $T_Q = K_D \times T_0 = K_M \times T_1$ emerges at the flip-flop output. As a result, certain samples consistently yield a value of one (indicated in blue in Fig. 2, specifically the 4th and 7th dots), while others consistently yield zero (shown in green for the 2nd and 5th dots). Additionally, some samples display random values (marked in red for the 1st, 3rd, 6th, and 8th dots). By applying the coherent sampling

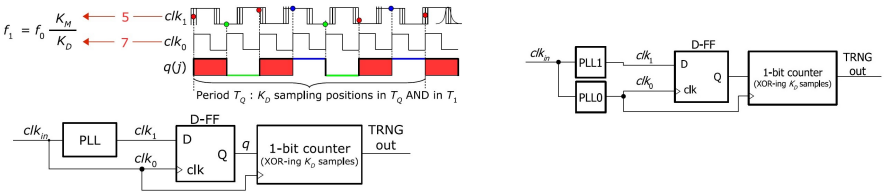

Fig. 2. [Left Figure]: Principle of the PLL-TRNG with one PLL [16]
[Right Figure]: PLL-TRNG with two PLLs configuration [16]

principle and rearranging the samples based on their positions, the waveform of one period of clk_1 can be reconstructed as explained in [1], [16].

This work adopts a two PLL-TRNG architecture as a reference model due to its better performance characteristics. The incorporation of two PLLs significantly enhances design flexibility by expanding the practical operating ranges for critical parameters, K_M and K_D, consequently increasing attainable bit and entropy rates. Moreover, this configuration substantially reduces autocorrelation between output bits. While incurring increased implementation costs, these can often be mitigated through resource sharing with other system components, as proposed in [8].

In this two PLLs case, firstly, as it is stated in Fig. 2:

$$\frac{f_1}{f_0} = \frac{K_M}{K_D} \tag{2}$$

where K_M and K_D are integer values representing frequency multiplication and division factors, depending on the configuration of PLLs. Each PLL has its multiplication and division factors. Moreover, they are related to K_M and K_D as:

$$K_M = K_{M_1} \cdot K_{D_0} \tag{3}$$

$$K_D = K_{M_0} \cdot K_{D_1} \tag{4}$$

The output (Q) of DFF in the left part of Fig. 2 has a pseudo-random pattern with a certain period. After XORing that pattern in the decimator or 1-bit counter, the bit rate of the PLL-TRNG is defined as follows:

$$R = \frac{f_0}{K_D} = \frac{f_1}{K_M} \tag{5}$$

The entropy rate per bit at generator output depends on the parameters of the jitter and on the parameters of the generator, which are characterized by its sensitivity to the jitter:

$$S = \Delta^{-1} = f_0 \cdot K_M = f_1 \cdot K_D \tag{6}$$

The design of PLL-TRNG relies on choosing appropriate PLL multiplication and division factors. However, selecting these factors can be challenging due to

the physical constraints of the PLL, such as the maximum and minimum values of N, M, C, and the input, output, PFD, and VCO frequency range. Consequently, determining these values is an optimization problem, and our solution to this problem is explained in Section 3.2 for Zynq 7020 SoC values listed in Table 1.

3 PLL-TRNG Implementation Details

3.1 Implemented PLL-TRNG Configurations

A primary limitation of PLL-TRNGs is their comparatively low output data rate. To address this constraint, this work proposes a methodology to enhance output capacity by leveraging additional PLLs available within the SoC. The Zynq 7020 SoC, featuring four PLLs, represents the upper bound for this implementation. However, prior to full-scale implementation, intermediate configurations employing three PLLs are investigated to facilitate a systematic design process. This study elucidates the design rationale for the four-PLL system by providing detailed explanations of these intermediate steps. Consequently, four distinct PLL-TRNG configurations are presented in Table 2 and visually depicted in Fig. 3:

Table 2. Configurations of PLL-TRNG Implementations

Codes of PLL-TRNG Designs Depicted in Fig. 3	Number of PLLs	Purpose of Use of PLL		PLL-TRNG Design Type
		As Reference Clock	As Jittered Clock	
(a)	2	1	1	Referenced Design
(b)	3	1	2	Intermediate Step for Proposed Approach
(c)	3	2	1	Intermediate Step for Proposed Approach
(d)	4	2	2	Proposed Design

3.2 Determining PLL-TRNG Parameters

In this work, as the parameter search algorithm, the backtracking algorithm in [10] is selected. Given a set of variables explained in Section 2.1 and Section 2.2 and constraints listed in Table 1, this backtracking method iteratively investigates potential solutions. Unlike a brute-force approach, it promptly eliminates any variable values that fail to meet a constraint, then backtracks to explore other possible values until all valid solutions are identified. The algorithm detailed in [10] involves determining the PLL-TRNG parameters that comply with both physical constraints and application requirements.

The code in the backtracking is open-source shared in [19]. Hence, we can modify it for Zynq 7020 SoC parameters provided in Fig. 1. Table 1 presenting the range of PLL values of Zynq 7020 SoC is prepared using [15]. However, the maximum value of f_{out} is not determined by PLL parameters, it is determined by BUFG properties. BUFG must be used in the SoC design, and hence, it restricts f_{out} value for the search algorithm. That maximum value can also be found in [15].

After generating results for our case, the results of the algorithm are ordered with respect to three different configurations. Those are the maximum bit rate

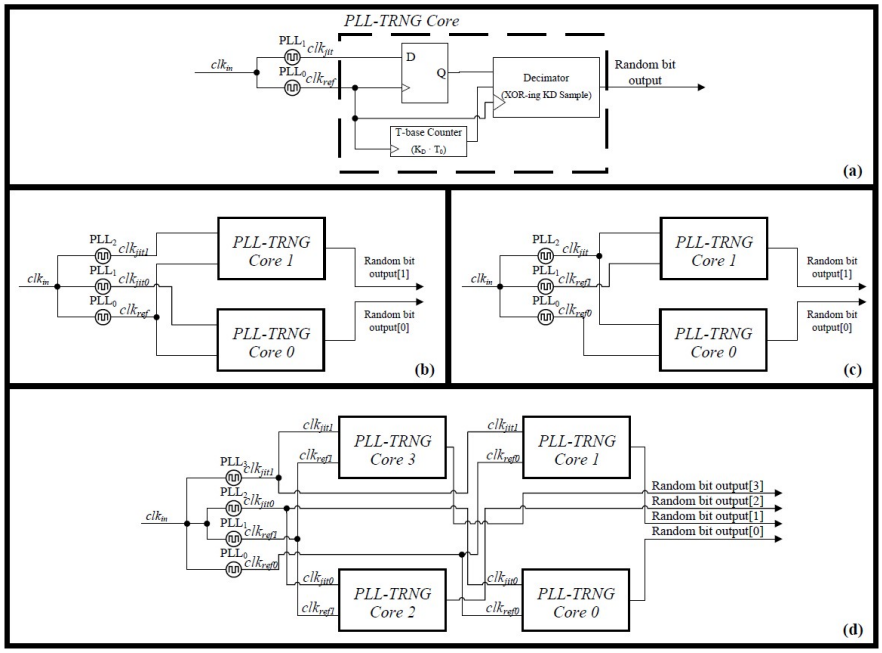

Fig. 3. Implemented PLL-TRNG Configurations: (a), (b), (c), and (d)

(max. R), the maximum sensitivity to jitter (max. S), and the maximum $R \cdot S$ value as the optimization between max. S and max. R.

After obtaining the candidate results for three different configurations, those results must be tested with one more criterion. The sampling process of the jittered clock with the reference clock is illustrated in Fig. 2. In order to obtain random numbers at the output of this PLL-TRNG, at least one sample is required to be affected by the jitter. This necessitates that the distance between any edge of clk_0 and its corresponding edge on clk_1 must be less than Δ. This condition is met if the following condition holds [4], [7]:

$$\sigma_{jit} > max(\Delta T_{min}) \tag{7}$$

where σ_{jit} is the standard deviation of the jitter at the output of the PLL, and $max(\Delta T_{min})$ is the largest distance between the two closest edges of clk_0 and clk_1. This can be computed as [4], [7]:

$$max(\Delta T_{min}) = \frac{T_{clk_0}}{4K_M} gcd(2K_M, K_D) = \frac{T_{clk_1}}{4K_D} gcd(2K_M, K_D) \tag{8}$$

where gcd is the greatest common divisor of two integers.

Upon executing the backtracking algorithm and obtaining results for the selected SoC, the maximum value of $max(\Delta T_{min})$ can be determined. However, accurately measuring or estimating σ_{jit} presents significant challenges. At this juncture, the estimation tool named *Clocking Wizard* in Vivado 2019.1 can be utilized. This tool provides an estimation of the jitter at the PLL's output clock, given the PLL parameters. Consequently, the results from the backtracking algorithm are first examined, and max. R, max. S and the max. $R \cdot S$ are identified.

These three candidates are then evaluated against Equation (7). Candidates failing to satisfy the equation are discarded, and alternative candidates from the backtracking results are considered. The results of the search algorithms are listed in Table 3. As it can be seen, all the selected configurations satisfy Equation (7).

Table 3. Determined Parameters for the PLL-TRNG Implementations

Config.	f_{ref} (MHz)	(M_0, N_0, C_0) (M_1, N_1, C_1)	f_0 (MHz) f_1 (MHz)	K_M	K_D	R (Mbit/s)	S (ps^{-1})	$R \cdot S$	σ_{jit}	$max(\Delta T_{min})$
Max. R	125	(51,4,4) (11,1,3)	398.438 458.333	176	153	2.60417	0.07013	0.18263	76.706	3.56506
Max. S	125	(51,4,4) (32,3,3)	398.438 444.444	512	459	0.86806	0.204	0.177084	100.882	1.22549
Max. $R \cdot S$	125	(37,5,2) (32,3,3)	462.5 444.444	320	333	1.38889	0.148	0.20556	100.882	1.68919

3.3 Implementation Setup

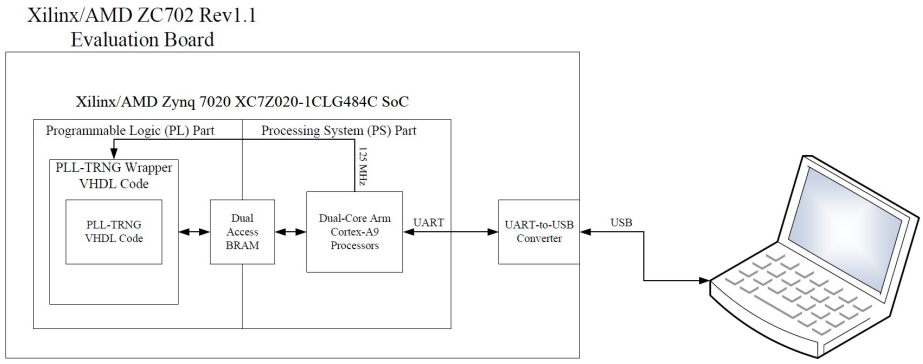

Fig. 4. Block Diagram of Implementation Setup

The implementation setup employed in this study is illustrated in Fig. 4. It utilizes the ZC702 Rev1.1 Evaluation Board [12], which incorporates the Zynq 7020 XC7Z020-1CLG484C SoC to facilitate the implementation of four distinct PLL-TRNG configurations as detailed in Section 3.1. In the Programmable Logic (PL) section, four distinct designs, specified in Table 2, are developed using Vivado 2019.1 [13] in VHDL. To enable real-time transmission of generated random numbers to a personal computer (PC), a dual-access Block RAM (BRAM) is employed. One port of this BRAM is connected to the PL, while the other is connected to the processing system (PS) section. The requisite code for the PS section is written in the C programming language. The PL section generates random numbers and writes a predefined value to a specific BRAM address to indicate that the random bits are ready. Once this indication is given, the software in the PS section outputs the random bits to the UART serial port, which are then converted to USB and transmitted to the PC. The received bits on the PC are saved in their ASCII-coded hexadecimal form and later converted to binary form offline to serve as input for AIS-20/31 Tests [17]. Both Procedure A and Procedure B Tests of AIS-20/31 are conducted for each result. Given that these tests require ∼7Mb of random bits, each output file is generated to have

a size of ∼7.2Mb. Additionally, a 125 MHz clock frequency is selected for the system's main clock (clk_{in}) due to timing constraints inherent in the SoC.

In conclusion, three ZC702 Rev1.1 Evaluation Boards are employed to demonstrate that the implemented PLL-TRNG configurations are not specific to a particular device. The backtracking algorithm and the elimination criteria outlined in Equation (7) are used to determine the PLL-TRNG configuration parameters for maximizing S, R, and the product $R \cdot S$. Subsequently, five random output bit files are generated for each of the four configurations described in Section 3.1 and tested on the three evaluation boards. The results are stored on a PC, and AIS-20/31 Tests are conducted. The outcomes of these tests are detailed in Section 4.

4 Results and Comparisons

The implementation results are presented in Table 4. In this table, each row corresponds to a unique configuration defined by the number of PLLs in the PLL-TRNG and the parameter configuration. By considering our four different PLL-TRNG configurations and three different PLL parameter selections, we have twelve distinct rows, in other words, twelve different results. For each row, five different ∼7.2Mb random number files are generated for each of the ZC702 Boards. Hence, the arithmetic mean of these fifteen values is used for the Shannon Entropy calculation in the table. In addition to these, it is important to highlight that all four PLL-TRNG designs successfully passed both Procedure A and Procedure B Tests of AIS-20/31 tests across three different configurations on three distinct boards for all generated files.

Table 4. PLL-TRNG Implementation Results

PLL Configuration	Parameter Configuration	R (Mbit/s)	Output Bit Rate (Mbit/s)	S (ps^{-1})	$R \cdot S$	Entropy (Shannon)
2-PLL with one reference clock and one jittered clock	Max. R	2.6042	2.60417	0.0701	0.18263	**0.999999986833568**
	Max. S	0.8681	0.86806	0.204	0.17708	0.999999986516413
	Max. $R \cdot S$	1.3889	1.38889	0.148	0.20556	0.999999981069240
3-PLL with one reference clock and two jittered clocks	Max. R	2.6042	5.20834	0.0701	0.18263	0.999999976364641
	Max. S	0.8681	1.73612	0.204	0.17708	0.999999977771549
	Max. $R \cdot S$	1.3889	2.77778	0.148	0.20556	0.999999980834110
3-PLL with two reference clocks and one jittered clock	Max. R	2.6042	5.20834	0.0701	0.18263	0.999999985962200
	Max. S	0.8681	1.73612	0.204	0.17708	0.999999961780714
	Max. $R \cdot S$	1.3889	2.77778	0.148	0.20556	0.999999966076834
4-PLL with two reference clocks and two jittered clocks	Max. R	2.6042	**10.41668**	0.0701	0.18263	0.999999972332402
	Max. S	0.8681	3.47224	0.204	0.17708	0.999999971434251
	Max. $R \cdot S$	1.3889	5.55556	0.148	0.20556	0.999999956486246

Table 5 provides a comparative analysis of our work with previously implemented PLL-TRNGs. The results of our 4-PLL-TRNG implementation significantly enhance the output bit rate of the PLL-TRNG design while maintaining robust cryptographic properties. Specifically, the table shows that a speed of approximately 10.4 Mb/s can be achieved, notably higher than any other reported PLL-TRNG implementation. Additionally, our results exhibit superior Shannon Entropy compared to earlier PLL-TRNG designs.

In Table 6, the utilization rates of different resource types for 4-PLL-TRNG are shown. Despite the inclusion of both the 4-PLL-TRNG and the necessary

Table 5. PLL-TRNG Implementation Results Comparison with [10], [7], and [18]

	Results of 4-PLL-TRNG			Results in [10] for Xilinx Spartan-6		
Parameter Configs	**Output Bit Rate (Mbit/s)**	**S (ps^-1)**	**Entropy (Shannon)**	**Output Bit Rate (Mbit/s)**	**S (ps^-1)**	**Entropy (Shannon)**
Max. R	10.41668	0.07013	0.999999972332402	1.042	0.094	1
Max. S	3.47224	0.204	0.999999971434251	0.521	0.167	0.99999
Max. R*S	5.55556	0.148	0.999999956486246	N/A	N/A	N/A
	Results in [7] for Xilinx Spartan-6			**Results in [18] for Xilinx Spartan-6**		
Parameter Configs	**Output Bit Rate (Mbit/s)**	**S (ps^-1)**	**Entropy (Shannon)**	**Output Bit Rate (Mbit/s)**	**S (ps^-1)**	**Entropy (Shannon)**
Max. R	0.555	0.0913	0.997	0.44	N/A	0.999931407560694
Max. S	0.555	0.0913	0.997	0.44	N/A	0.999931407560694
Max. R*S	0.555	0.0913	0.997	0.44	N/A	0.999931407560694

state machines in the PL section, the overall resource utilization remains relatively low, with the exception of the PLLs. These low utilization rates underscore the 4-PLL-TRNG's potential for TRNG applications in IoT systems.

Table 6. Utilization Table Generated Using Vivado 2019.1 [13] for 4-PLL-TRNG Implementation

Resource Type	**Avaliable Resource Quantity**	**Utilization Quantity (Utilization Rate as %) of Max. R Configuration**	**Utilization Quantity (Utilization Rate as %) of Max. S Configuration**	**Utilization Quantity (Utilization Rate as %) of Max. $R \cdot S$ Configuration**
LUT	53200	1539 (2.89%)	1542 (2.90%)	1536 (2.89%)
LUTRAM	17400	72 (0.41%)	72 (0.41%)	72 (0.41%)
FF	106400	1884 (1.77%)	1884 (1.77%)	1884 (1.77%)
BRAM	140	2 (1.43%)	2 (1.43%)	2 (1.43%)
IO	200	8 (4.00%)	8 (4.00%)	8 (4.00%)
PLL	4	4 (100.00%)	4 (100.00%)	4 (100.00%)

5 Conclusion

This paper presents the design and implementation of an innovative, high-speed PLL-TRNG that employs the coherent sampling method of jittered PLL clocks. By utilizing a backtracking algorithm for parameter selection and incorporating four PLLs, as constrained by the Xilinx Zynq 7020 SoC, the design enhances the output bit rate compared to conventional two-PLL designs. The method is adaptable to any FPGA or SoC platform with at least three PLLs, ensuring broad applicability. The proposed PLL-TRNG demonstrates AIS-20/31 compliance, producing high-quality random numbers with excellent performance relative to previous approaches. Its scalability and adaptability make it a promising candidate for future FPGA, SoC, and ASIC implementations, particularly for IoT applications where low resource utilization, high output rates, and high entropy are critical.

Acknowledgements. The authors express their gratitude to the anonymous reviewers for their valuable comments and suggestions, which contributed to the improvement and clarity of this paper. Additionally, the authors acknowledge the support of Aselsan Inc. in the preparation of this work, as well as their provision of three Xilinx ZC702 Evaluation Boards used for the implementation of the PLL-TRNG algorithms presented in the paper.

References

1. Fischer V., Drutarovský M.: True Random Number Generator Embedded in Reconfigurable Hardware. CHES 2002, (2002)
2. Drutarovský M., Simka M., Fischer V., Celle F.: A Simple PLL-based True Random Number Generator for Embedded Digital Systems. (2004)
3. Liu C., McNeill J.: A Digital-PLL-based True Random Number Generator. PhD Research in Microelectronics and Electronics, vol. 1, 2005, pp. 113–116, (2005)
4. Fischer V., Drutarovský M., Simka M., Bochard N.: High Performance True Random Number Generator in Altera Stratix FPLDs, (2004)
5. Bernard F., Fischer V., and Valtchanov B.: Mathematical Model of Physical RNGs Based on Coherent Sampling, (2010)
6. Petura O., True Random Number Generators for Cryptography: Design, Securing and Evaluation. Micro and Nanotechnologies/Microelectronics. Université de Lyon. English. NNT: 2019LYSES053. tel-02895861, (2019)
7. Allini E. N., Characterization, Evaluation and Utilization of Clock Jitter as Source of Randomness in Data Security. Cryptography and Security [cs.CR]. Université de Lyon. English. NNT : 2020LYSES019. tel-03207261, (2020)
8. Petura O., Mureddu U., Bochard N., Fischer V.: Optimization of the PLL-based TRNG Design Using the Genetic Algorithm, (2017)
9. Allini E. N., Petura O., Fischer V., Bernard F.: Optimization of the PLL Configuration in a PLL-based TRNG Design, (2018)
10. Colombier B., Bochard N., Bernard F., Bossuet L.: Backtracking Search for Optimal Parameters of a PLL-based True Random Number Generator, (2020)
11. B. für Sicherheit in der Informationstechnik (BSI), AIS 20/31 - Functionality Classes for Random Number Generators (2011) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.html Accessed: 2023-11-01
12. AMD, Xilinx Zynq-7000 SoC ZC702 Evaluation Kit. https://www.xilinx.com/products/boards-and-kits/ek-z7-zc702-g.html Accessed: 2023-09-01
13. AMD, Xilinx Vivado 2019.1 Design Software for Xilinx (AMD) Adaptive SoCs and FPGAs. https://www.xilinx.com/support/download/index.html/content/xilinx/en/downloadNav/vivado-design-tools/archive.html Accessed: 2023-09-01
14. AMD, 7 Series FPGAs Clocking Resources User Guide (UG472) (v1.14) https://docs.amd.com/v/u/en-US/ug472_7Series_Clocking Accessed: 2023-10-01
15. AMD, Zynq-7000 SoC: DC and AC Switching Characteristics (DS187) (v1.21) https://docs.amd.com/v/u/en-US/ds187-XC7Z010-XC7Z020-Data-Sheet Accessed: 2023-10-01
16. Fischer, V., Bernard, F., Bochard, N.: Modern random number generator design – Case study on a secured PLL-based TRNG, (2019)
17. BSI. Implementation of Test Procedure A and Test Procedure B for Application Notes and Interpretation of the Scheme (AIS) 20/31 Standard. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_testsuit_zip.zip Accessed: 2023-12-01
18. Petura O., Mureddu U., Bochard N., Fischer V. and Bossuet L.: A survey of AIS-20/31 compliant TRNG cores suitable for FPGA devices, (2016)
19. The source code of the backtracking algorithm in [10] https://gitlab.univ-st-etienne.fr/sesam/pll-trng-constraint-programming/tree/master Accessed: 2023-11-01