Research Migration Project

https://esim.fossee.in/research-migration-project

The Research Migration Project is an initiative of FOSSEE, IIT Bombay that promotes the use of eSim for reproducing published research circuits originally implemented using proprietary simulation tools. The objective is to migrate these validated designs to eSim to build an open source resource database.

Name of the participant : Harshitha Kota

Affiliation / Institution : Department of Electronics and Communication Engineering, Rajiv Gandhi University of Knowledge and Technologies (RGUKT), Nuzvid, Andhra Pradesh, India.

Title of the circuit : FIGARO TRNG: Fibonacci-Galois Ring Oscillator Based True Random Number Generator

Theory/Description :

True Random Number Generators (TRNGs) play a vital role in cryptographic key generation, hardware security anchors, nonces, authentication protocols, and Monte Carlo simulations. Unlike Pseudo-Random Number Generators (PRNGs) which rely on deterministic mathematical algorithms, TRNGs extract true physical non-determinism from microscopic physical noise phenomena such as thermal noise, breakdown noise, and phase jitter present in semiconductor devices.

The FIGARO (FIbonacci and GAlois Ring Oscillator) TRNG topology proposed in this work combines two distinct structural classes of multi-feedback Ring Oscillators (ROs) to achieve exceptionally high entropy rates and robust immunity against external injection locking:

- Fibonacci Ring Oscillator (FIRO): Consists of an odd number of inverting/non-inverting delay stages connected in a closed ring loop, supplemented by multiple feedback lines connected to an XOR gate tree fed back into the primary input stage. The complex multi-loop feedback induces multi-frequency collapse and rich phase jitter accumulation.
- Galois Ring Oscillator (GARO): Features XOR feedback gates placed directly between adjacent delay stages along the ring path. The decentralized Galois feedback configuration spreads thermal jitter and phase noise evenly across all intermediate node transitions, preventing frequency synchronization.
- Combination & Entropy Extraction: High-frequency jittery clock streams generated independently by u_firo and u_garo modules are combined using a top-level two-input XOR gate. This XOR combination effectively multiplies phase jitter variations and eliminates deterministic harmonics.
- Sampling & Output Registering: The raw combined clock (raw_figaro_clk / sw_figaro_clk) is sampled by a reference system clock (clk_sample) using D-type flip-flops (random_bit_reg). A single random bit output (random_bit) is captured on every rising clock edge, while an 8-bit shift register (random_byte_reg[7:0]) aggregates sequential random bits into full random byte outputs (random_byte[7:0]) suitable for hardware security applications.

Reason to reproduce with eSim :

1. Open-Source Hardware Cryptography Resource: Migrating physical security primitives such as True Random Number Generators (TRNGs) into eSim (open-source EDA tool by FOSSEE, IIT Bombay) enriches the open-source hardware security repository for researchers and students globally.

2. Democratization of VLSI Security Research: Validating that complex mixed-signal phase-jitter entropy sources can be accurately modeled and simulated in open-source EDA tools (eSim / Ngspice / Verilog / GTKWave) without relying on expensive proprietary software suites.

3. Educational Impact: Serves as an exemplary reference project for students at RGUKT Nuzvid and other institutions studying Advanced Digital System Design, VLSI Cryptography, and FPGA/ASIC Hardware Security.

4. Verification of Jitter Accumulation & Randomness: Demonstrates eSim's capability to simulate mixed ring oscillator topologies and analyze non-linear logic behavior under digital timing testbenches.

Expected Outcome/outputs :

1. Ring Oscillator Startup & Oscillation: Self-sustained high-frequency oscillations from both FIRO (u_firo) and GARO (u_garo) modules upon releasing active-low reset (rst_n = 1) and enabling the module (enable = 1).

2. Raw Combined Clock: Top-level XOR gate output (raw_figaro_clk) generating a rapid jittery clock waveform produced by combining FIRO and GARO phase variations.

3. Single Bit Random Output: A continuous stream of un-seeded, non-deterministic random binary bits (random_bit) sampled at reference clock edges (clk_sample).

4. 8-Bit Byte Registration: Sequential byte formation (random_byte[7:0]) updating every clock cycle, transitioning through varied hex values (e.g. 0x00, 0x01, 0x03, 0x07, 0x0F, 0x1F, 0x3F, 0x7F, 0xFE, 0xFC, 0xF8, 0xF0, 0xE0, 0xC1, 0x83...), demonstrating uniform bit shifting and byte accumulation.

Block Diagram (s) :

The high-level architecture diagram illustrating functional blocks, control inputs (rst_n, enable, clk_sample), FIRO & GARO ring oscillators, top-level XOR combination, and output registers (random_bit_reg, random_byte_reg) is shown below:

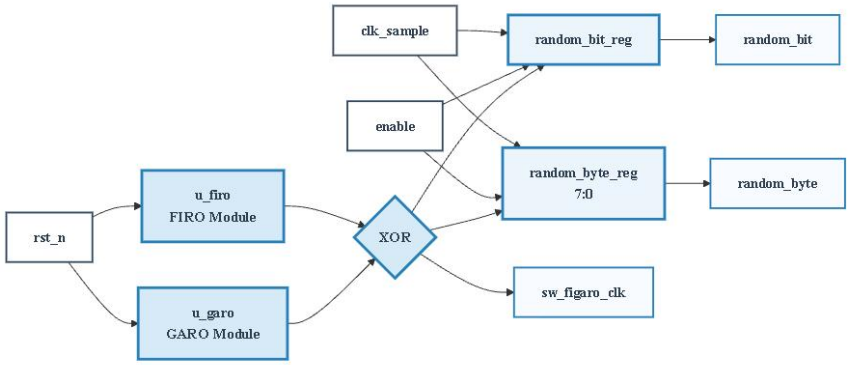

Figure 1: High-Level Architectural Block Diagram of FIGARO TRNG System

Circuit Diagram(s)

The detailed RTL elaborated schematic diagram showing internal logic gates, feedback paths, multiplexers, XOR trees, and register connections for u_firo and u_garo modules is shown below:

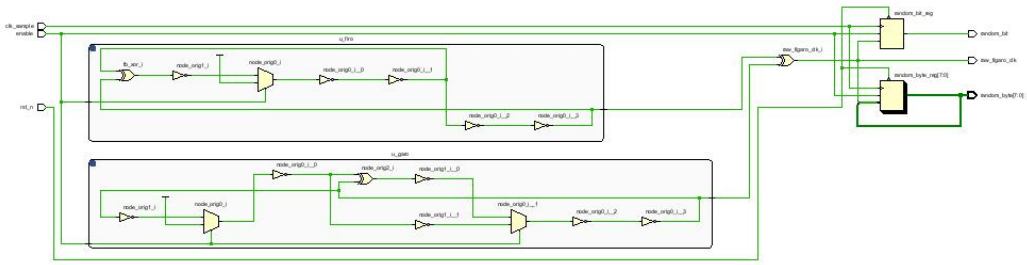

Figure 2: Elaborated RTL Schematic Diagram of FIGARO TRNG showing FIRO & GARO Gate Topologies

Expected Results (Input, Output waveforms and/or Multimeter readings) :

The simulation results obtained from the Verilog testbench (tb_figaro_trng.v) demonstrate correct functional timing and randomness generation across all control signals:

Figure 3: Waveform Simulation Result showing Reset Activation (rst_n), Oscillator Enable (enable), raw_figaro_clk Generation, and 8-bit Random Byte Shifting

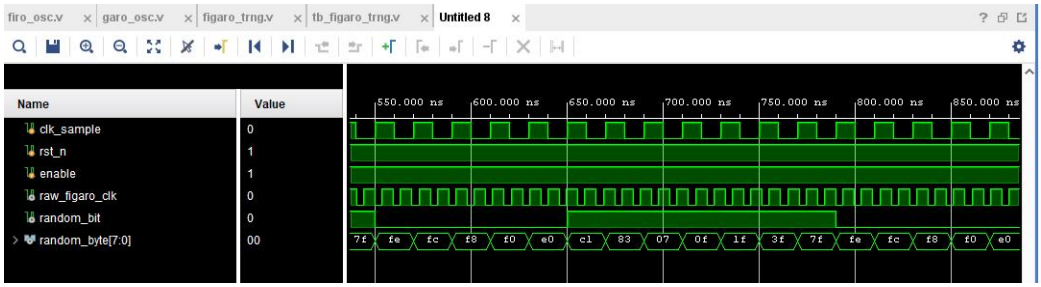

Figure 4: Detailed Waveform View showing Sampling Clock (clk_sample), Random Bit Generation (random_bit), and Hexadecimal Byte Values

- **Waveform Signal Analysis —** clk_sample: System reference sampling clock operating at ~40 MHz (25 ns clock period).
- rst_n: Active-low reset signal. At t = 0 to 50 ns, rst_n is held LOW (0), keeping output registers in reset state (0x00). At t = 50 ns, rst_n goes HIGH (1) to release reset.
- enable: Control enable signal. Asserted HIGH (1) at t = 70 ns, initiating ring oscillator oscillations.
- raw_figaro_clk: XOR-combined output clock from FIRO and GARO rings, toggling rapidly to supply phase-jittered clock edges.
- random_bit & random_byte[7:0]: Random bit stream sampled on clk_sample rising edges, shifting into random_byte[7:0] register and producing dynamic hexadecimal sequences (0x00 -> 0x01 -> 0x03 -> 0x07 -> 0x0F -> 0x1F -> 0x3F -> 0x7F -> 0xFE -> 0xFC -> 0xF8 ...).

Research Paper/Journal/etc. :

Title : Design and Implementation of Multiple Ring Oscillator-Based TRNG Achitecture by Using ADPLL

Author : HUIREM BHARAT MEITEI , MANOJ KUMAR

Link : https://ieeexplore.ieee.org/document/10835068/