Novel True Random Number Generator (TRNG) Modules on Different FPGA Platforms

Dr. Hossam O. Ahmed

American University of the Middle East (AUM), Kuwait.

I – Introduction:

• In today's digital world, security is crucial to our daily lives.

• The increasing amount of sensitive information stored and transmitted online requires strong security measures.

• Cryptographic algorithms are vital for safeguarding user data privacy.

• These algorithms depend on cryptographic keys to maintain data security.

• True Random Number Generators (TRNGs) are crucial for many important security applications.

II – Propose TRNG entropy sources

• All the proposed novel TRNG architectures in this project depend on race hazard and time jitter as the source entropy.

• Race Hazard:
- Utilizes the unpredictable timing differences in electronic circuits.
- Exploits the race condition where two or more signals compete to affect the outcome.
- Generates random numbers based on which signal wins the race.

• Jitter:
- Relies on the natural variations in signal timing (jitter).
- Measures the small, random deviations in signal edges.
- Uses the jitter-induced timing noise to produce random numbers.

III – FPGA boards used:

• Intel® Stratix® 10 DX FPGA Development Kit
• Starter Platform for OpenVINO™ Toolkit
• Altera DE2-115 Development and Education Board

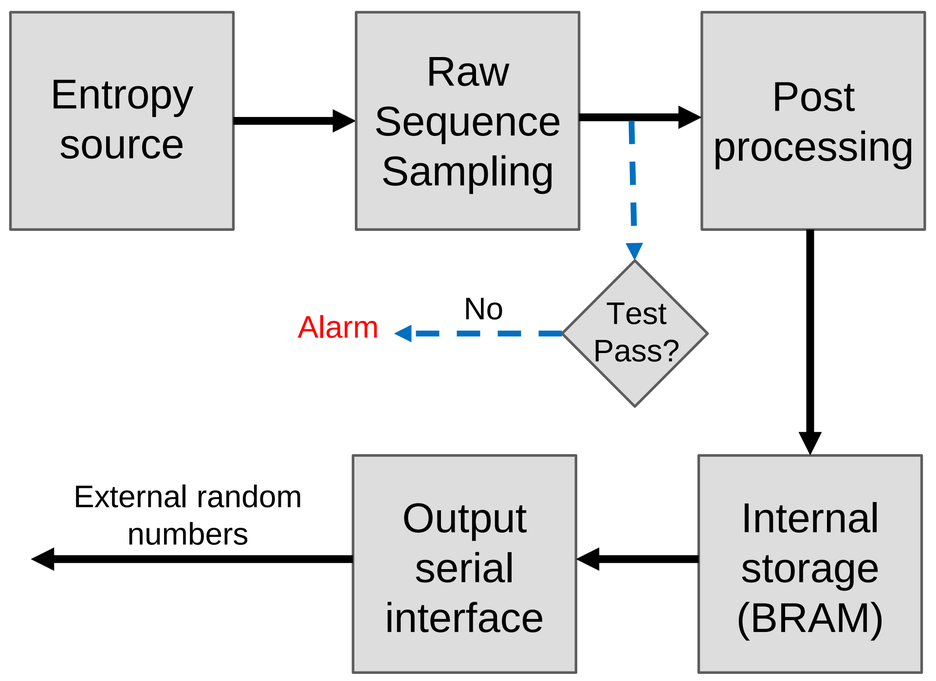

Fig. 1 A generic architecture of a True Random Number Generator (TRNG) circuit

IV – Archived performance

• Max. throughput: 300 Mbps to 2.4 Gbps
• Min entropy per bit > 0.99
• Compliant with NIST 800-90B standard.
• Compliant with AIS-31 PTG.2 standard.

V – Main project objective

• To be integrated with other modules to leverage security measures for processor communication links used in the Autonomous Landing Guidance Assistance System (ALGAS) using FPGA as in Ref [1-2].

References:

1) H. O. Ahmed and D. Wyatt, "Adaptive Prognostic Malfunction Based Processor for Autonomous Landing Guidance Assistance System Using FPGA," in *IEEE Access*, vol. 12, pp. 2113-2122, 2024
2) H. O. Ahmed, "Coarse Grained FLS-based Processor with Prognostic Malfunction Feature for UAM Drones using FPGA," 2023 Integrated Communication, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 2023