Unpredictable by Design: Race Hazard & Jitter-Enhanced TRNG with Braided Logic Gates on FPGA

Hossam O. Ahmed, College of Engineering and Technology, American University of the Middle East, Kuwait - Orcid: 0000-0002-6825-9786

Co-authors:

- Donghoon Kim, Department of Aerospace Engineering and Engineering Mechanics, University of Cincinnati, USA

- William J. Buchanan, School of Computing, Engineering and the Built Environment, Edinburgh Napier University, U.K.

Why TRNG is Important?

- **Cryptographic Security:** TRNGs provide unpredictable keys, making it extremely difficult for attackers to guess or reproduce encryption keys used in secure communications.
- **Authentication & Digital Signatures:** Strong randomness is required for secure authentication protocols and digital signatures to prevent impersonation and replay attacks.
- **Protection Against Side-Channel Attacks:** High-quality random numbers prevent attackers from exploiting predictable patterns in hardware or software implementations.
- **Quantum-Resilient Security:** TRNGs enable quantum-resistant cryptographic algorithms, ensuring robust security in the face of future quantum computing threats.
- **AI Model Integrity:** In artificial intelligence, random initialization and data shuffling enabled by TRNGs are essential for robust model training and preventing bias or overfitting.
- **Secure Data Generation for AI:** TRNGs are fundamental to synthetic data generation, privacy-preserving algorithms, and federated learning, where trustworthiness and unpredictability are crucial.

The Proposed B+HCCES TRNG Module

- In this work, we propose a True Random Number Generator (TRNG) architecture named **Braided and Hybrid Cross-Coupled Entropy Source (B+HCCES) TRNG** module.
- The proposed B+HCCES TRNG module generates random numbers based on the race hazard and jitter of braided and cross-coupled combinational logic gates.
- The B+HCCES architecture depends on: 1) Proposed HCCLG module. 2) Proposed B-XOR-LG module.

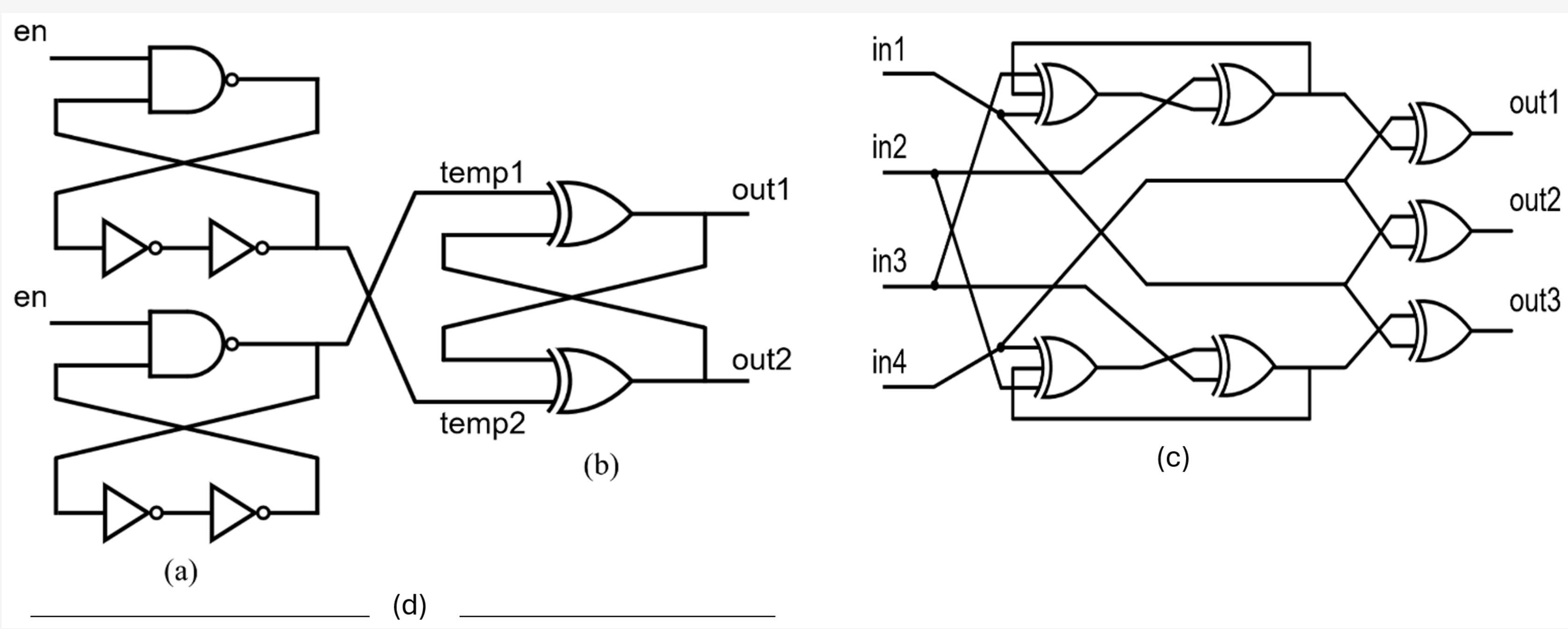

Figure 1: (a) ring Oscillator. (b) CCX module. (c) Proposed B-XOR-LG module. (d) the proposed HCCLG module.

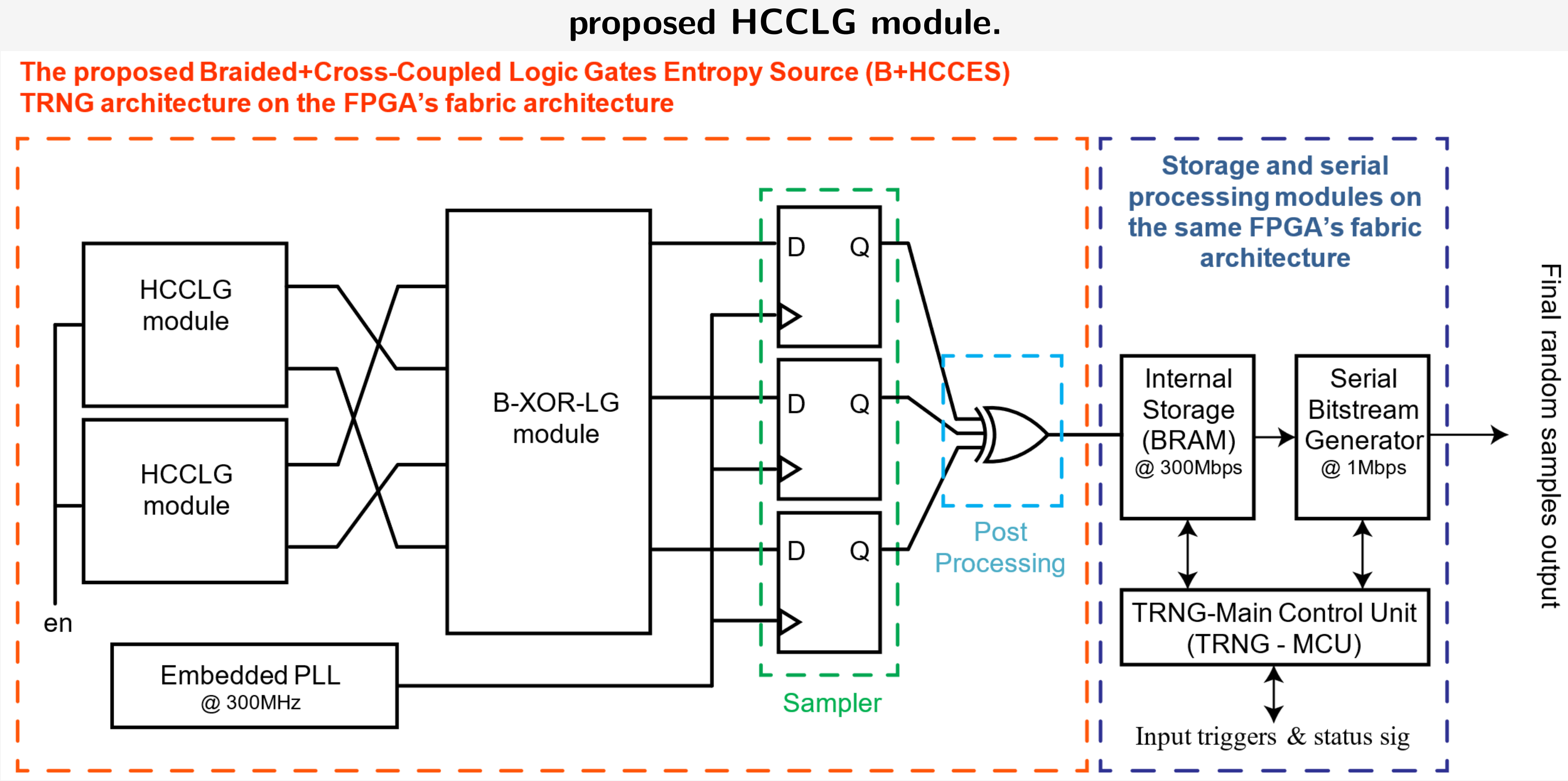

Figure 2: The detailed structure of the B+HCCES TRNG architecture with the storage control module, and the serial module.

The Summary of Computational Performance and Power Consumption for the Proposed B+HCCES Unit Across the FPGA Chip

Combinational ALUT	23
Dedicated Flip-flops	3
ALMs needed [A-B+C] *	11.5
Combinational cell thermal power dissipation	0.02 mW
Clock enable block thermal power dissipation	1.79 mW
Register cell thermal power dissipation	0.04 mW
I/O thermal power dissipation	2.46 mW
Total thermal power dissipation	4.31 mW
Energy efficiency (pJ/bit)	0.01436

** A: ALMs used in final placement. B: Estimate of ALMs recoverable by dense packing. C: Estimate of ALMs unavailable.*

Entropy Test Results

RESULTS OF AIS-31 TEST

	TEST	Pass Rate
P1/T0	Disjointness	Passed
P1/T1	Monobit	257/257
P1/T2	Poker	257/257
P1/T3	Run	257/257
P1/T4	Long run	257/257
P1/T5	Auto-correlation	257/257
T6-a	Uniform dist. (S<0.025)	|P(1) - 0.5| = 0.001730
T6-b	Uniform dist. (S<0.020)	p(01) = 0.50044 p(11) = 0.49811 |p_(01) - p_(11)| = 0.002329
T7-a	Comparative multinomial, width=3 (S<15.13)	test size [0] = 0.269121 test size [1] = 0.006480
T7-b	Comparative multinomial, width=4 (S<15.13)	test size [0] = 0.095220 test size [1] = 3.836958 test size [2] = 0.144500 test size [3] = 0.856983
T8	Entropy (S>7.976)	7.996781

RESULTS OF NIST SP90-B TEST

Test	C[0]	C[1]	C[2]
Excursion	18	0	6
NumDirectionalRuns	6	0	9
LenDirectionalRuns	17	6	0
NumIncreasesDecreases	66	0	6
NumRunsMedian	53	1	5
LenRunsMedian	420	6	0
AvgCollision	6	0	9
MaxCollision	4	2	28
periodicity (1)	70	0	6
Periodicity (2)	21	0	6
Periodicity (8)	6	0	37
Periodicity (16)	64	0	6
Periodicity (32)	56	1	5
Covariance (1)	7	0	6
Covariance (2)	15	0	6
Covariance (8)	12	0	6
Covariance (16)	6	0	28
Covariance (32)	136	0	6
Compression	6	0	9
Chi-square independence	p-value = 0.594202		
Chi-square goodness of fit	p-value = 0.517031		
length of longest repeated substring test	Passed		
Restart test	Passed		
Min entropy per bit	0.992343		
Min entropy per Byte	7.938744		

Restart Test Results

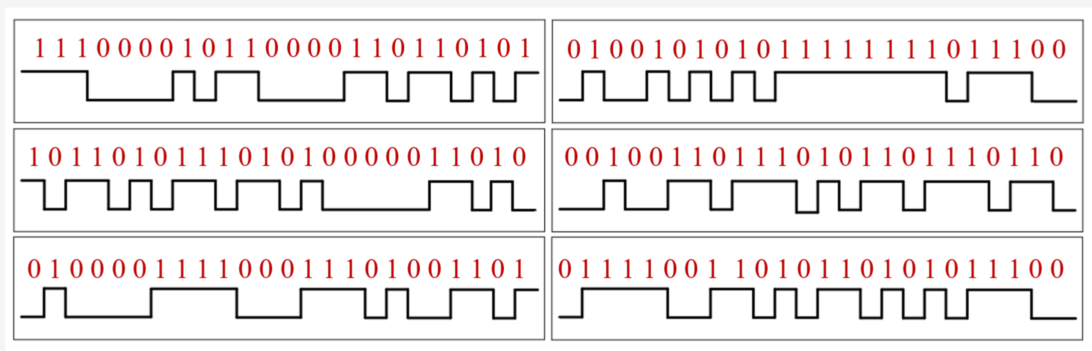

Figure 3: Test results of six restart cycles.

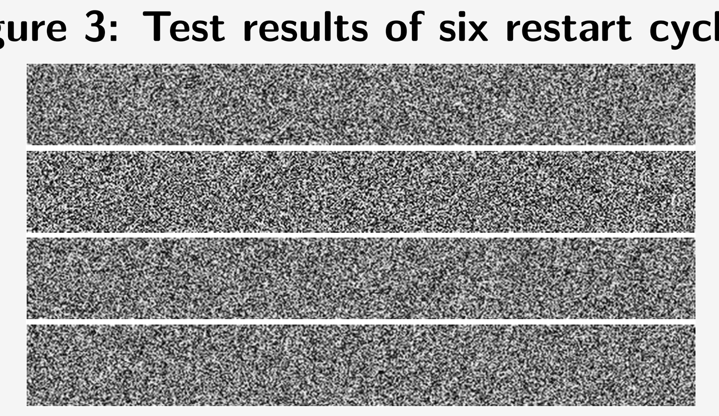

Figure 4: Distributions of four power-up batches: Each batch consists of 250 samples, each with a 1000-bit length.

Conclusion and Future Work

- **High Throughput:** The B+HCCES TRNG, implemented on a Cyclone-V GT FPGA, achieves a data rate of 300 Mbps.
- **Resource Efficiency:** Utilizes a minimal number of 23 LUTs and just 3 DFFs, ensuring efficient use of FPGA resources.
- **Standards Compliance:** Successfully passes stringent evaluations, including the NIST SP800-90B and BSI AIS-31 test suites for randomness and entropy quality.
- **Scalability and Adaptability:** The architecture is highly scalable, making it suitable for a wide range of applications without sacrificing performance.
- **Security and Reliability:** Sets a new benchmark in random number generation for FPGA-based systems, enhancing the security and reliability of cryptographic and AI applications.
- **Future-Proof Design:** The efficient architecture paves the way for further innovation and adoption of high-quality TRNGs in advanced digital systems.

References

[1] H. O. Ahmed, D. Kim and W. J. Buchanan, "A True Random Number Generator Based on Race Hazard and Jitter of Braided and Cross-Coupled Logic Gates Using FPGA," in IEEE Access, vol. 12, pp. 182943-182955, 2024.