Multi-ring: A Fast True Random Number Generator

Motivation

- **RANDOM DATA:** used in
  - Cryptographic Key Generation
  - Scientific Simulations, Games
  - Statistical Sampling, etc.
- **TRNG:** generates random data i.e. non-repeating sequences of bits
- **EXISTING TRNG'S:** Have different area and performance characteristics
- **OUR GOAL:** Design a new high-speed and area ptimized TRNG

Project Description

TRNG: Overview

Randomness Source
- *RO Clock Jitter*
- *Thermal Noise*

Extraction
- *Rings + STR*
- *XOR Network*

Post Processing (optional)
- *Von Neumann*
- *SHA-2*

Our Design

- Randomness Source: Clock Jitter in Oscillating Rings
- High-speed rings (up-to 420 MHz)
- AXI peripheral for easy integration with ARM or Microblaze embedded processors

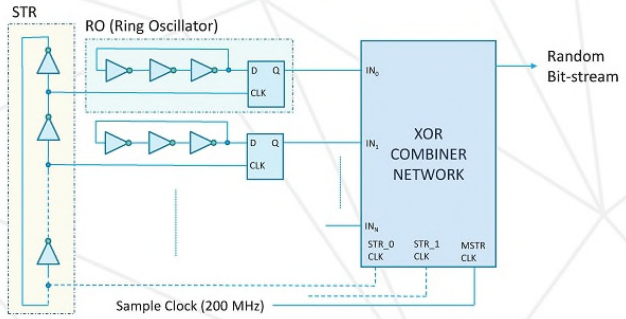
Resource Utilization (ARTIX-7)

Resource	LUT1	LUT2	FDCE	FDRE	OBUFT	SLICES
Count	58	9	16	10	32	31

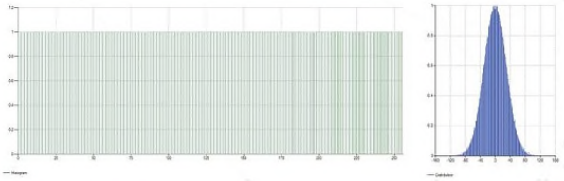
Performance & Area

- High throughput: 200 Mb/s
- Significantly smaller: (3x to 4x) than similar Ring Oscillator (RO) based designs.

Resource Utilization (ARTIX-7)



Design Characteristics



Min-Entropy (estimates) compared to AES-CTR

NIST TEST	AES-CTR	THIS WORK
Most Common Value (MCV)	7.89262	7.89295
Collision	6.61547	7.16014
Markov	5.78534	5.76644
Compression	7.26080	7.16958
t-Tuple	7.94845	7.94879
LRS	8.00235	8.00368

Future Work

- Implementations on latest Generation FPGA's.
- Possible ASIC implementation and testing.
- Streaming AXI modes for even faster transfer rates.

Arpan Jati[1], Naina Gupta[1] & Anupam Chattopadhyay[2]
[1]IIIT DELHI, INDIA [2]NTU, SINGAPORE
{arpanj, nainag}@iiitd.ac.in, anupam@ntu.edu.sg