QUAC-TRNG

High-Throughput True Random Number Generation Using Quadruple Row Activation in Real DRAM Chips

Ataberk Olgun

Minesh Patel A. Giray Yağlıkçı Haocong Luo

Jeremie S. Kim F. Nisa Bostancı Nandita Vijaykumar

Oğuz Ergin Onur Mutlu

SAFARI kasırga

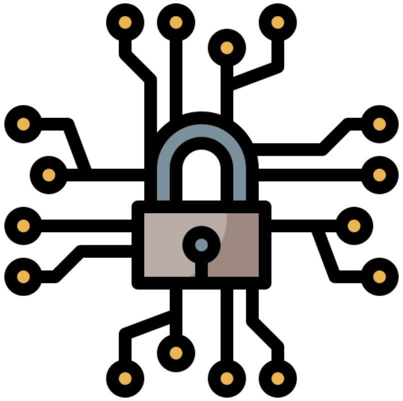
ETH zürich TOBB ETÜ University of Economics & Technology UNIVERSITY OF TORONTO

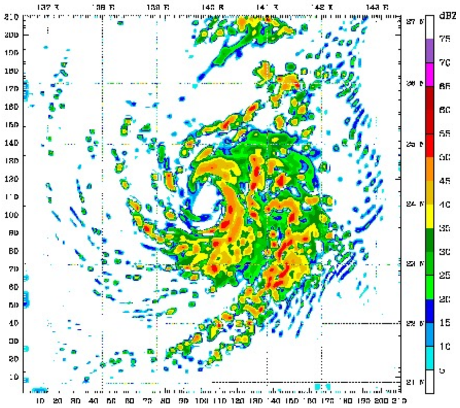
Executive Summary

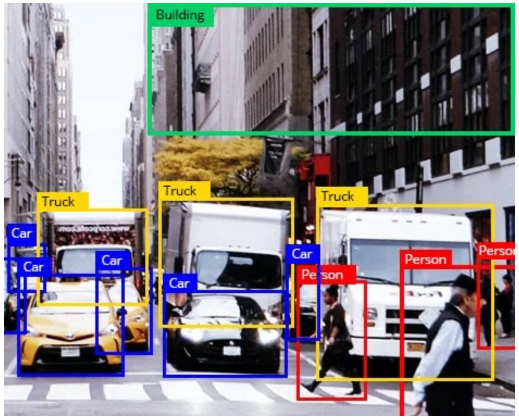
- **Motivation**: DRAM-based true random number generators (TRNGs) provide **true random numbers at low cost** on **a wide range** of computing systems
- **Problem**: Prior DRAM-based TRNGs are slow:
  1. Based on fundamentally slow processes → **high latency**
  2. Cannot effectively harness entropy from DRAM rows → **low throughput**
- **Goal**: **Develop** a **high-throughput** and **low-latency** TRNG that uses **commodity DRAM** devices
- **Key Observation:** Carefully engineered sequence of DRAM commands can activate **four DRAM rows** → **QU**adruple **AC**tivation **(QUAC)**
- **Key Idea**: **Use QUAC** to activate DRAM rows that are initialized with **conflicting data** (e.g., two ‘1’s and two ‘0’s) to generate random values
- **QUAC-TRNG:** DRAM-based TRNG that generates true random numbers at **high-throughput** and **low-latency** by **repeatedly performing QUAC operations**
- **Results:** We evaluate QUAC-TRNG using **136** real DDR4 chips
  1. **5.4 Gb/s** maximum (**3.4 Gb/s** average) TRNG throughput per DRAM channel
  2. Outperforms existing DRAM-based TRNGs by **15.08x** (base), and **1.41x** (enhanced)
  3. QUAC-TRNG has low TRNG latency: **256-bit RN** in **274 ns**
  4. QUAC-TRNG passes **all 15** NIST randomness tests

Use Cases of True Random Numbers

High-quality true random numbers are critical to many applications







True random numbers can only be obtained by sampling random physical processes

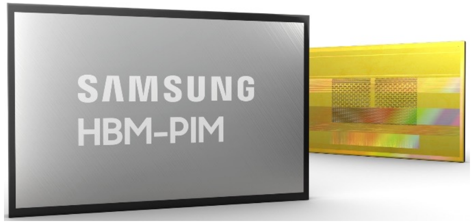
Not all computing systems are equipped with TRNG hardware (e.g., dedicated circuitry)

DRAM-Based TRNGs

DRAM is ubiquitous in modern computing platforms

DRAM-based TRNGs enable low-cost and high-throughput true random number generation within DRAM

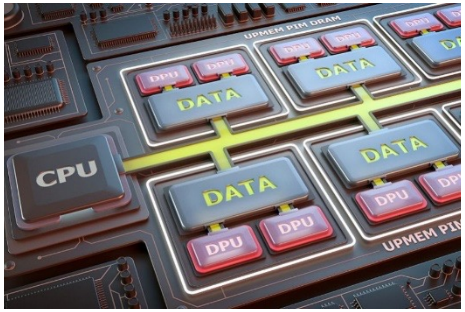
- Requires no specialized hardware: Benefits constrained systems
- Open application space: Provides high-throughput TRNG



[Samsung]

Processing-in-Memory (PIM) systems perform computation directly within memory

- Avoid inefficient off-chip data movement



[UPMEM]

DRAM-based TRNGs

- Enable PIM workloads to sample true random numbers directly within the memory chip
- **Avoid communication to possible off-chip TRNG sources**

Motivation and Goal

Prior DRAM-based TRNGs are slow, these TRNGs:

1. Are based on fundamentally slow physical processes
    - DRAM retention-based TRNGs
    - DRAM startup value-based TRNGs
2. Cannot effectively harness entropy from DRAM rows
    - DRAM timing failure-based TRNGs

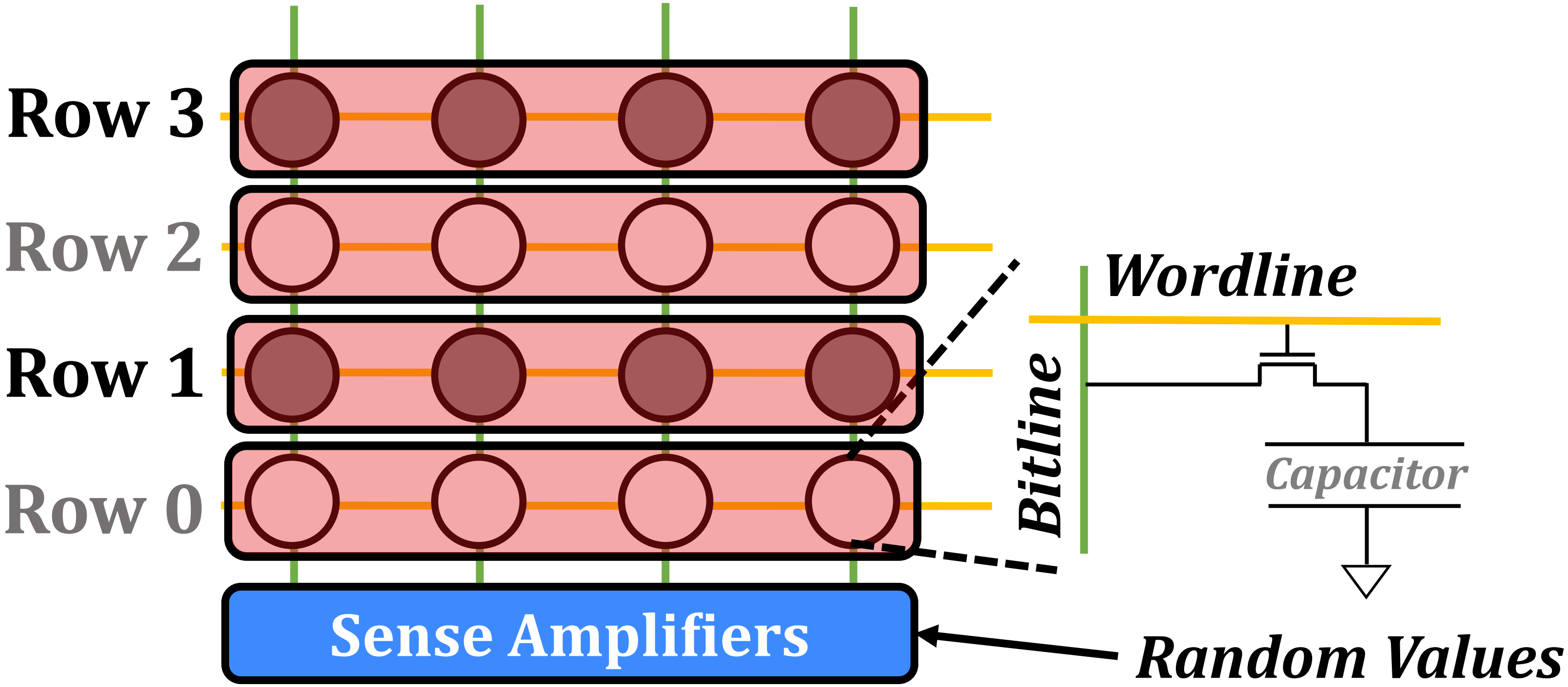
Goal: Develop a high-throughput and low-latency TRNG that can be implemented using commodity DRAM devices

Key Observation

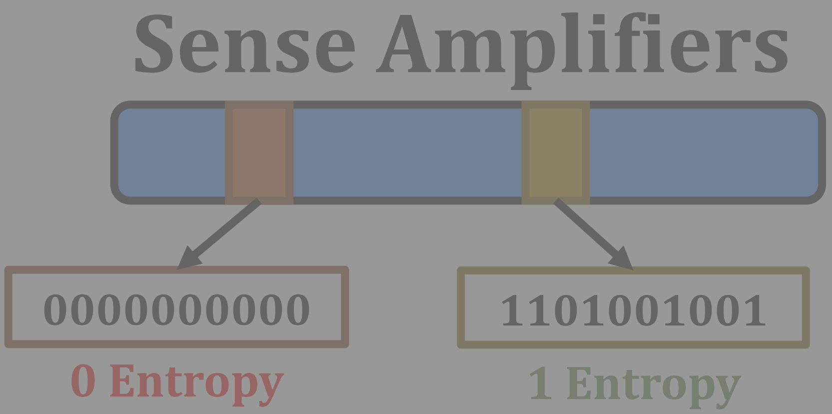
QUadruple **AC**tivation (**QUAC**): Carefully-engineered DRAM commands can activate four DRAM rows in real chips

Using QUAC to Generate Random Values

Use QUAC to activate DRAM rows that are initialized with conflicting data (e.g., two ‘1’s and two ‘0’s) to generate random values

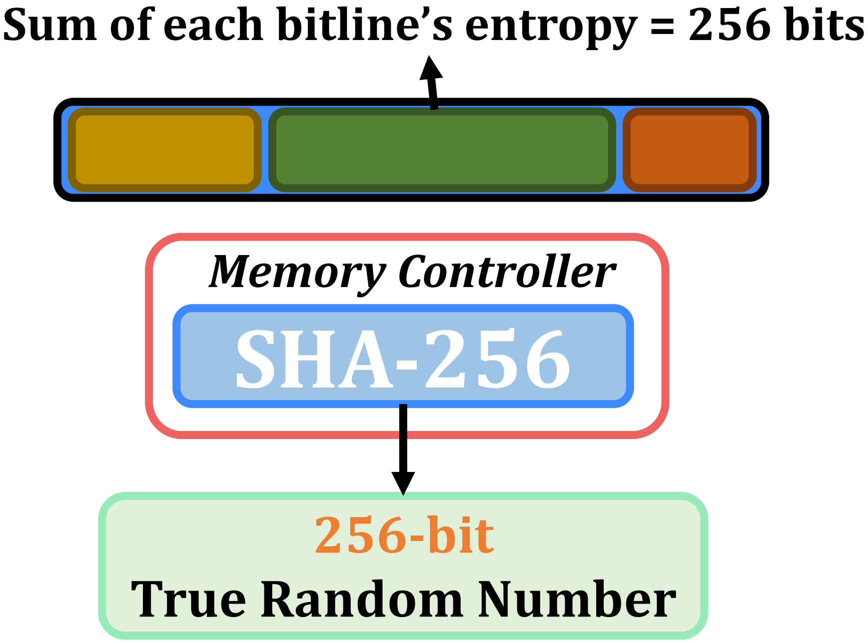


QUAC-TRNG



One-time Characterization

Find Shannon Entropy of Each Sense Amplifier



① Initialize Rows

② Perform QUAC

③ Read Block

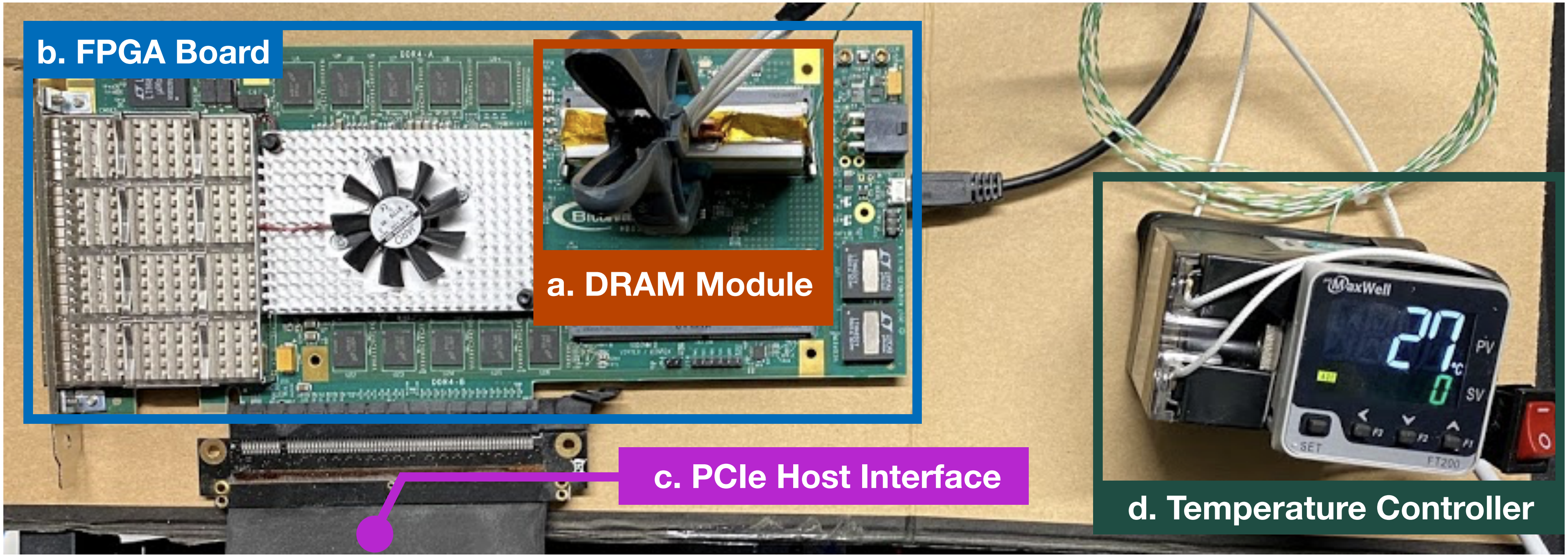
④ Post-process

Experimental Methodology

Experimentally study QUAC and QUAC-TRNG using 136 real DDR4 chips

- Spatial distribution of entropy
- Data pattern dependency of entropy

DDR4 SoftMC → DRAM Testing Infrastructure



[Hassan+ HPCA'17] *https://github.com/CMU-SAFARI/SoftMC*

Key Results

- 5.4 Gb/s TRNG throughput (3.44 Gb/s on average) per channel
- Outperform state-of-the-art base by 15.08x and enhanced by 1.41x
- Low latency: Generates a 256-bit random number in 274 ns

- Passes all 15 standard NIST randomness tests

- Negligible area cost: 0.04% of a contemporary CPU
- Negligible memory overhead: 0.002% of an 8 GiB DRAM module

- Entropy changes with temperature
- Entropy remains stable for at least up to a month

QUAC-TRNG

High-Throughput True Random Number Generation Using Quadruple Row Activation in Real DRAM Chips

Ataberk Olgun

Minesh Patel A. Giray Yağlıkçı Haocong Luo

Jeremie S. Kim F. Nisa Bostancı Nandita Vijaykumar

Oğuz Ergin Onur Mutlu

SAFARI kasırga

ETH zürich TOBB ETÜ University of Economics & Technology UNIVERSITY OF TORONTO