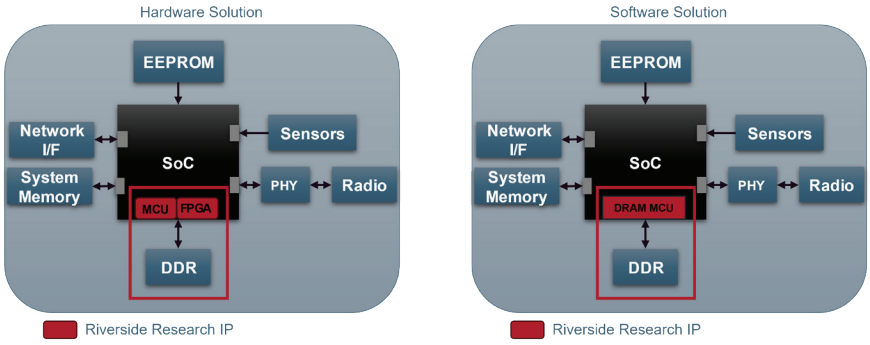
Physically Unclonable Functions (PUFs)

Providing usable hardware security to existing microelectronic devices without requiring physical modifications

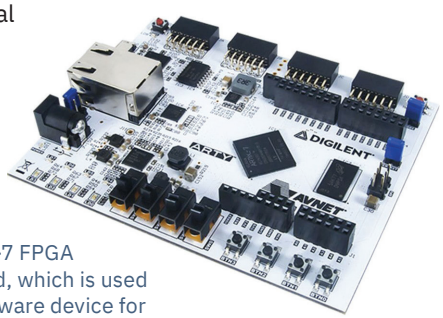
PUFs are used across various areas to address microelectronic and embedded Internet of Things (IoT) security. While other memory based PUFs (SRAM, Flash, etc.) can implement delay-based PUFs (arbiters, ring oscillators, etc.), they often require extra circuitry for run-time usage, which can then fall victim to common modeling attacks. DRAM PUFs can instead be implemented without needing these dedicated circuities—at run-time.

We presented six different applications addressed by Dynamic Random Access Memory (DRAM) PUF technology: extended trust, secure boot, memory protection, key encryption key (KEK), anonymous authentication, and random number generation as an entropy source.



Procedure

- Select development boards using widely available DRAM chips
- Modified device memory controller and build software tools to configure the hardware
- Showcase DRAM decay and collect preliminary data across various inputs
- Model probability that each bit decays in the DRAM cell and identify which decay time offers the highest overall entropy
- Measure Hamming Distance (HD) between 10 different boards and all memory locations
- Select which bits will be used, construct PUF, and verify overall PUF output
- Replication of open-source alternative software-only DRAM PUF, still utilizing decay
- Build infrastructure to test environmental characteristics of the PUF and other embedded systems



Arty A7-100T Artix-7 FPGA Development Board, which is used as the current hardware device for the PUF IRAD.

RIVERSIDE RESEARCH

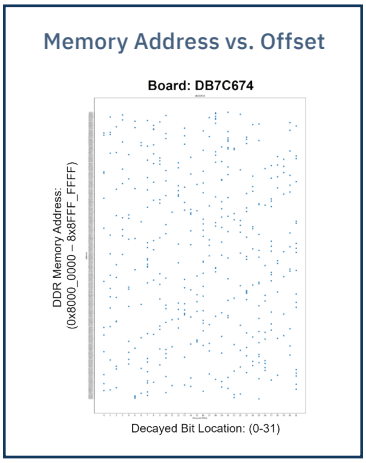
Key Features

- Advance current Riverside IP to higher TRL, to match identified customer needs
- Software utilizes DDR chips, which are found within many Embedded IoT and Microelectronic systems, and doesn't require any additional hardware to be added to the system
- Creates environmental testing environment and Riverside IP for Microelectronic and Embedded System Devices

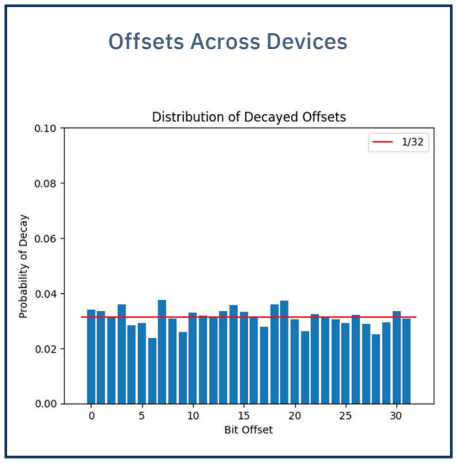
Physically Unclonable Functions (PUFs)

Observations

DDR chips found within many embedded IoT and microelectronics systems can be used seamlessly with our innovation. PUFs creates testing environment without requiring additional hardware.

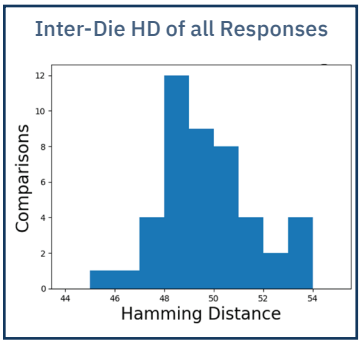


No matter what portion of the DRAM memory is used, there is no bias—removing an attack point for Reverse Engineering (RE).



Chip aging, temperature, and voltage fluctuations often affects the overall decay speed. We are testing other ways to speed up this decay and see if software-only solutions offer any improvement for decay speed.

Our IRAD project has constructed a DRAM PUF, at TRL 3, which can generate bits of entropy uniquely per a unique device. We confirmed this by testing our IP on 10 different devices, and measuring their results. We now look to advance our IP to TRL 4, and verify the stability of our PUF across various environmental conditions, as well as variations in the initialization and usage of DRAM PUFs.



This shows that there is no clear bias in the output, as a skewed response would create an attack point for RE.

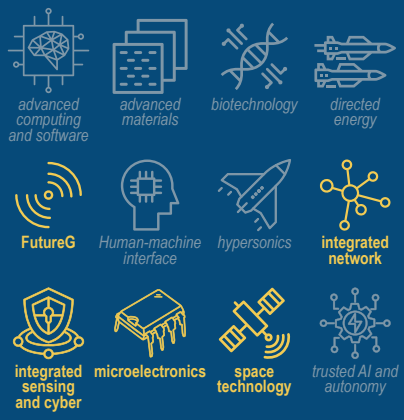
Next Steps

All work performed at Riverside Research for environmental testing and aging will be applicable to any software or hardware PUF, not just DRAM. Our next steps include:

- Building software to test environmental effects and aging on hardware and software controlled PUFs, as well as other embedded devices
- Continuing development of DRAM PUF technologies, focusing on software-only solutions that don't assume hardware reconfiguration access

RIVERSIDE RESEARCH

Critical Tech Areas



DoD Priorities

1 2 3 4 5 6
7 8 9 10 11 12
13 14 15 16 17

1. Southwest Border Activities
2. Combating Transnational Criminal Organizations in the Western Hemisphere
3. Audit
4. Nuclear Modernization (including NC3)
5. Collaborative Combat Aircraft (CCAs)
6. Virginia-class Submarines
7. Executable Surface Ships
8. Homeland Missile Defense
9. One-Way Attack/Autonomous Systems
10. Counter-small UAS Initiatives
11. Priority Critical Cybersecurity
12. Munitions
13. Core Readiness, including full DRT funding
14. Munitions and Energetics Organic Industrial Bases
15. Executable INDOPACOM MILCON
16. Combatant Command support agency funding for INDOPACOM, NORTHCOM, SPACECOM, STRATCOM, CYBERCOM, and TRANSCOM
17. Medical Private-Sector Care