

# Poster: Hardware Root of Trust Reconsidered — Reconfigurable DRAM-PUFs via Timing Violations and Spatial Correlation

Owen Millwood<sup>\*†</sup>, Prosanta Gope<sup>†</sup>, Mannpreeth M K<sup>†</sup>, Lucas Norpchen<sup>†</sup>, Witali Bartsch<sup>\*</sup>

<sup>\*</sup>WIZnet Germany GmbH, Kleinniedesheim, Germany

Email: {owen.millwood, witali.bartsch}@wiznet.de

<sup>†</sup>Department of Computer Science, University of Sheffield, United Kingdom

Email: {p.gope, mmohankumarkrishnachari1, lnorpchen1}@sheffield.ac.uk

**Abstract**—Physical Unclonable Functions (PUFs) are widely adopted as hardware roots of trust for IoT device identity, deriving unique cryptographic keys from intrinsic variations in silicon manufacturing. However, conventional PUF architectures produce a fixed, immutable Hardware Unique Key (HUK): once compromised, the device is permanently vulnerable with no recovery path short of physical replacement. We present ongoing work investigating *intrinsically reconfigurable* PUFs based on DRAM timing violations and spatial correlation effects. By varying the timing parameters under which DRAM cells are read and by controlling neighbour-cell data patterns prior to readout, we hypothesise that cryptographically independent responses can be derived from the same physical hardware. If validated, this enables server-initiated re-keying in which a fresh HUK is generated on demand, operational keys are re-wrapped, and the previous identity is cryptographically revoked — without modifying the underlying silicon. This poster describes the problem motivation, our dual-parameter characterisation methodology, and integration with a zero-knowledge device enrolment protocol.

**Index Terms**—Physical Unclonable Functions, DRAM security, hardware root of trust, reconfigurable PUF, IoT device identity

## 1. Introduction

The proliferation of IoT devices has created an unprecedented device identity problem. Each device requires a unique private key, a certificate, and a hardware root of trust. In current provisioning models, credentials are generated in vendor facilities under vendor-controlled PKI, and customers inherit whatever trust the manufacturer established.

PUFs address part of this problem by deriving device-unique keys from intrinsic manufacturing variations, thereby eliminating the need to store secrets. Unlike OTP or flash-based key storage — where the key exists at rest — a PUF generates keys ephemerally from the physics of the device itself. DRAM is a particularly promising substrate, already present in most systems, capable of yielding large numbers of identifiers [1], and supporting noise-resilient authentication [2].

However, conventional PUFs produce a *static* HUK. The same challenge always yields the same response. If an attacker extracts the PUF response through repeated physical access, fault injection, or ML modelling, the HUK cannot be rotated, and physical replacement is the only remediation.

## 2. Approach: Intrinsically Reconfigurable PUFs

We investigate whether DRAM timing violations can serve as an *intrinsically reconfigurable* PUF primitive, in which the challenge is a physical operating parameter that produces genuinely independent entropy from the same silicon.

### 2.1. Parameter A: Timing Violations

DRAM cells require minimum timing intervals (e.g. Row to Column Delay -  $t_{RCD}$ ) to reliably transfer charge to sense amplifiers in order to read/write a logical bit [1]. When deliberately violated, a subset of cells fails to produce correct values. Which cells fail depends on (i) intrinsic charge retention characteristics from manufacturing variation and (ii) the specific timing parameters applied.

We hypothesise that distinct timing regimes produce failure maps that are both *stable* (reproducible under the same regime) and *independent* (low cross-correlation between regimes), as illustrated in Fig. 1. Each timing configuration, location and location can constitute an independent ‘soft challenge’, yielding a cryptographically distinct key.

### 2.2. Parameter B: Spatial Correlation

We additionally investigate whether neighbouring cell data content influences flip behaviour during a timing violation. Due to electrical coupling, the charge state of surrounding cells may alter the threshold at which a target cell fails. By controlling the data pattern written to neighbours before a timing-violated read — uniform patterns (all 0s, all 1s) versus mixed patterns (checkerboard) — we hypothesise that the failure outcome can be reliably modulated (Fig. 2). If certain bit-cell couplings produce distinct, repeatable flip

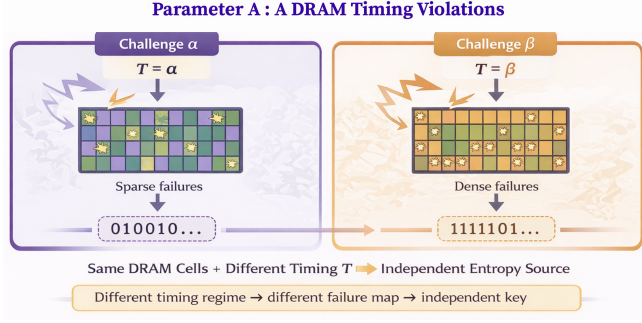


Figure 1. Timing violations applied to the same DRAM cells: relaxed timing ( $T=\alpha$ ) yields sparse failures; aggressive timing ( $T=\beta$ ) produces a denser, independent failure pattern.

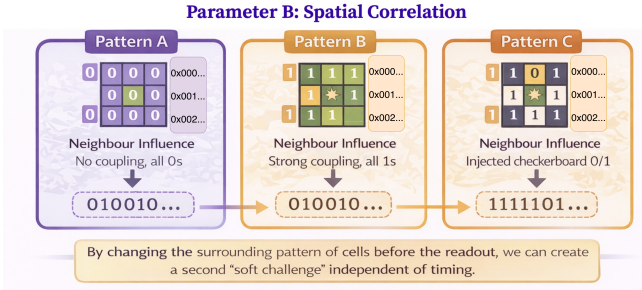


Figure 2. Spatial correlation: varying neighbour cell content before readout produces different failure outcomes from the same target cell, creating a second independent challenge axis.

behaviour across finer surrounding patterns, the challenge-response space expands to include the number of unique patterns that yield cryptographically desirable results. If stable, this provides a second dimension of challenge orthogonal to timing.

### 2.3. Reconfigurable HUK Architecture

These parameters integrate into a re-keying architecture (Fig. 3). A reconfigurable PUF derives an HUK from fixed hardware entropy combined with a controllable soft challenge. When re-keying is required, a trusted server issues a new authenticated challenge; the PUF generates a fresh HUK' to re-wrap operational keys via AES Key Wrap, and the previous HUK becomes cryptographically useless. This integrates with WIZnet's zero-knowledge device enrolment protocol [3], with privacy-preserving re-authentication [4] supporting repeated re-keying. As in the traditional Root of Trust assumption, no knowledge of the HUK is needed by any party. Therefore preventing un-authenticated HUK re-keying forms an essential topic for investigation.

## 3. Methodology

Experiments are conducted on a Xilinx Zynq-7000 (Zed-Board) with direct access to DRAM timing parameters via its memory controller. We systematically violate  $t_{RCD}$

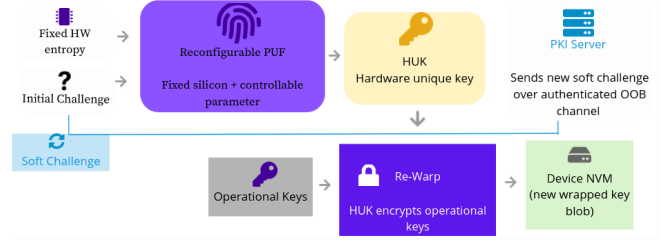


Figure 3. Reconfigurable HUK re-keying: a PKI server issues a new soft challenge, the PUF derives a fresh independent HUK, and operational keys are re-wrapped.

across a range of values, recording per-cell failure maps over repeated trials. For spatial correlation, controlled patterns are written to regions surrounding target cells and the resulting change in failure probability is measured.

Key metrics include: *intra-regime stability* (Hamming distance between same-challenge repetitions); *inter-regime independence* (Hamming distance and mutual information across challenges); *spatial entropy* (information-theoretic neighbour-dependency assessment); and *uniqueness* (inter-device variation). High stability, near-ideal independence ( $\approx 50\%$  fractional Hamming distance), and reliable spatial modulation would validate intrinsically reconfigurable DRAM-PUFs.

## 4. Discussion and Outlook

This work-in-progress investigates whether DRAM timing violations and spatial correlation can provide *intrinsic* reconfigurability at the silicon level — fundamentally different from circuit/logically reconfigurable PUFs [5]. If confirmed, the combination with zero-knowledge enrolment [3] and lightweight reconfigurable authentication [4] would yield an architecture where the user controls device identity from enrolment through post-compromise recovery. We are currently completing the experimental validation and plan to publish full results in a subsequent paper.

## References

- [1] J. S. Kim, M. Patel, H. Hassan, and O. Mutlu, “The DRAM Latency PUF: Quickly Evaluating Physical Unclonable Functions by Exploiting the Latency-Reliability Tradeoff in Modern Commodity DRAM Devices,” in *Proc. IEEE Int. Symp. High Performance Computer Architecture (HPCA)*, Feb. 2018, pp. 194–207.
- [2] O. Millwood, J. Miskelly, P. Gope *et al.*, “PUF-Phenotype: A Robust and Noise-Resilient Approach to Aid Group-based Authentication with DRAM-PUFs Using Machine Learning,” *IEEE Trans. Inf. Forensics Security*, 2023.
- [3] W. Bartsch, O. Millwood, and E. B. Kavun, “Zero Knowledge Registration of PKI Authentication for Symbiotic Security in FIDO IoT,” *J. Surveill. Secur. Saf.*, vol. 4, pp. 155–179, 2023.
- [4] P. Gope, F. Hongming, and B. Sikdar, “Lightweight and Privacy-Preserving Reconfigurable Authentication Scheme for IoT Devices,” *IEEE Trans. Services Computing*, 2025.
- [5] S. Baek *et al.*, “A Reconfigurable SRAM-Based CMOS PUF with Challenge to Response Pairs,” *IEEE Access*, vol. 9, pp. 90127–90137, 2021.



### The Device Identity Problem

### Methodology

### Reconfigurable PUF: HUK Re-Keying

#### Every device requires:

- A **unique** private key
- A certificate proving **identity**
- A hardware **root of trust**



#### The Supply Chain Question

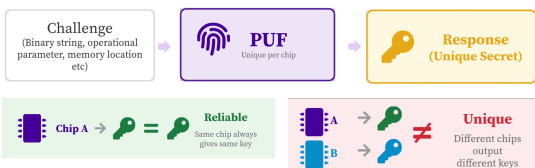
##### Who:

- **Generates** the key?
- **Injects** them?
- Controls the **PKI** (Public Key Infrastructure)?
- Can be trusted?

Device identity is determined long before customer deployment. Customers inherit **vendor-generated keys** and **vendor controlled trust hierarchies**

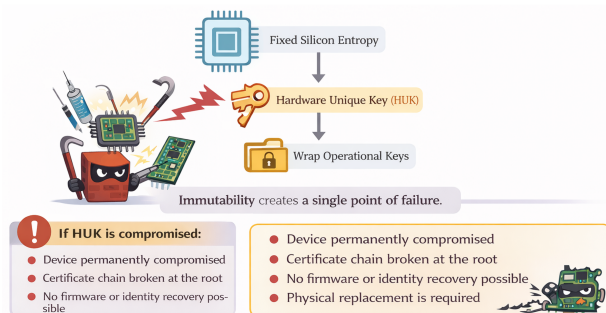
#### What is a PUF?

A hardware security primitive that generates a unique and unpredictable digital fingerprint from tiny manufacturing variations in a chip, allowing it to produce device-specific cryptographic keys.

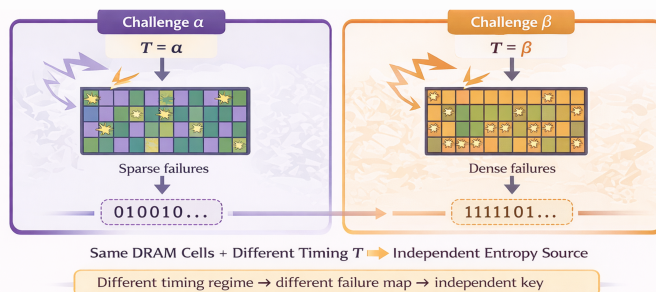


#### The Static Root Problem

Traditional PUFs derive a fixed, **immutable** hardware unique key (HUK) tied to intrinsic silicon properties. Once compromised, immutability leads to **permanent vulnerability**



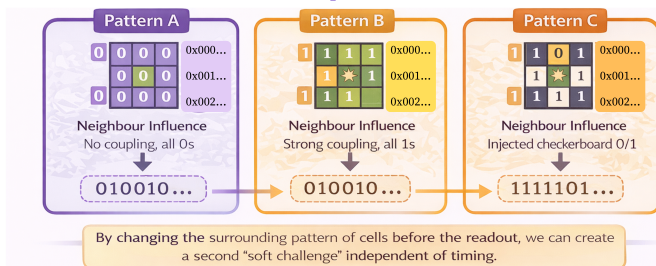
#### Parameter A : A DRAM Timing Violations



Different DRAM timing parameters applied to the same physical cells produce distinct failure patterns due to natural manufacturing variations in charge retention:

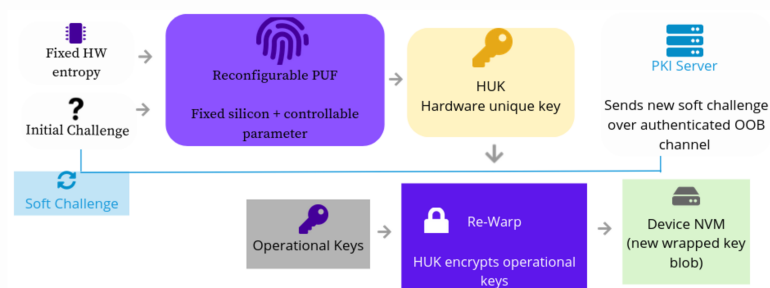
- **Mild timing violation ( $T = \alpha$ )**: only sparse bit failures occur, generating one response pattern, **Aggressive timing ( $T = \beta$ )**: failures become denser, potentially producing significantly different response
- Each regime results in a unique failure map, enabling the generation of independent cryptographic keys from the same DRAM hardware

#### Parameter B: Spatial Correlation



- Under a timing violation, a DRAM cell's flip behaviour is influenced not only by its own charge but also by electrical coupling from neighbouring cells
- By deliberately **controlling the data pattern written to adjacent cells before a read**, the flip outcome of a **target cell can be altered** — creating a second '**soft challenge**' dimension independent of timing
- Uniform neighbour patterns (all 0s or all 1s) and mixed patterns can lead to different hold or flip behaviours
- If reliable, spatial data patterns expand the PUF challenge space and enable additional independent key generation from the same hardware

Providing observations are cryptographically significant (**high uniqueness and reliability**), this phenomena would contribute to a PUF which exhibits intrinsic reconfigurability, not logical reconfigurability — containing the **benefits of hardware-derived entropy** without the limitation of it remaining static.



- A reconfigurable PUF derives a Hardware Unique Key (HUK) from **fixed hardware entropy** combined with a **controllable challenge parameter**
- A trusted server can issue a new **authenticated soft challenge**, prompting the PUF to generate a fresh and independent HUK without modifying the underlying silicon
- This HUK is used to encrypt (re-wrap) the device's operational keys, which are securely stored in non-volatile memory for later use in application-layer authentication (HUK remains unknown to all parties, never leaves the hard PUF engine)



#### Protocol Layer

*WIZnet patented architecture*

Blank devices → customer-controlled enrollment → zero-knowledge authentication → on-device key generation → customer PKI. Solves supply chain trust and enables operational re-provisioning.



#### Hardware Layer — IEEE S&P

*Sheffield-WIZnet collaboration*

Reconfigurable DRAM PUF → fresh hardware identity on demand → compromise triggers re-keying, not replacement.  
Eliminates the irrecoverable failure mode at the silicon level.

#### Related Work:

O. Millwood, P Gope et al. "A Generic Obfuscation Framework for Preventing ML-Attacks on Strong-PUFs through Exploitation of DRAM-PUFs," IEEE European Symposium on Security and Privacy (Euro S&P 2023), 3-7 July, Delft, Netherlands, 2023.

O. Millwood, J. Miskelly, P Gope et al. "PUF-Phenotype: A Robust and Noise-Resilient Approach to Aid Group-based Authentication with DRAM-PUFs Using Machine Learning," IEEE Transactions on Information Forensics & Security, 2023

P. Gope, F. Hongming and B. Sikdar, "Lightweight and Privacy-Preserving Reconfigurable Authentication Scheme for IoT Devices," IEEE Transactions on Services Computing, 2025 (SCI, EI)

J. S. Kim, M. Patel, H. Hassan, and O. Mutlu, "The DRAM Latency PUF: Quickly Evaluating Physical Unclonable Functions by Exploiting the Latency-Reliability Tradeoff in Modern Commodity DRAM Devices," in Proc. IEEE Int. Symp. High Performance Computer Architecture (HPCA), Feb. 2018