PUFsecurity

AN eMemory COMPANY

Solving **Chip Security's** Weakest Link

Complete Secure Boundary
with PUF-based Hardware Root of Trust

2021 December

PUFsecurity
AN eMemory COMPANY

PUFsecurity

Integrated PUF-based Hardware Security IPs

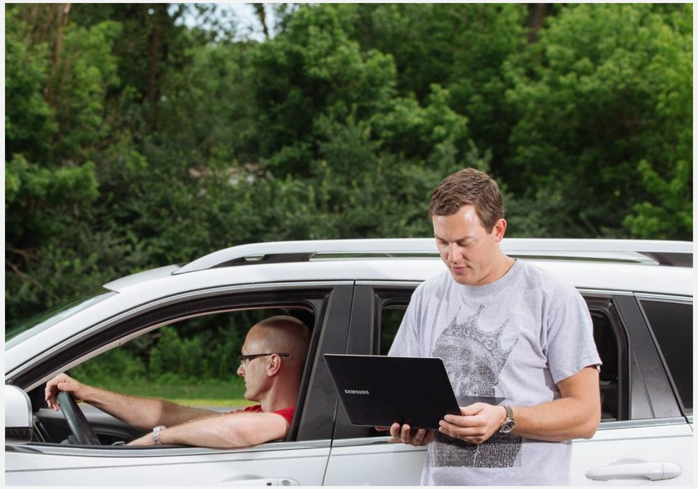
John Chou

Business Development and Technical Marketing Manager

For over 12 years, Mr. Chou has worked with talented teams at start-ups or high-growth Semiconductor IP companies building and promoting cutting-edge technology. He is currently responsible for market development across North America and Europe at PUFsecurity.

Hacking is Everywhere

Threat to **Life**



Hackers Remotely Kill a Jeep on the Highway

1.4 million vehicle recall by Chrysler, the age of hackable vehicles begins.

Link

Threat to **Privacy**

IoT Security Camera hacking demonstration on YouTube

Step by step guides for hacking IoT devices are widely available online.

Link

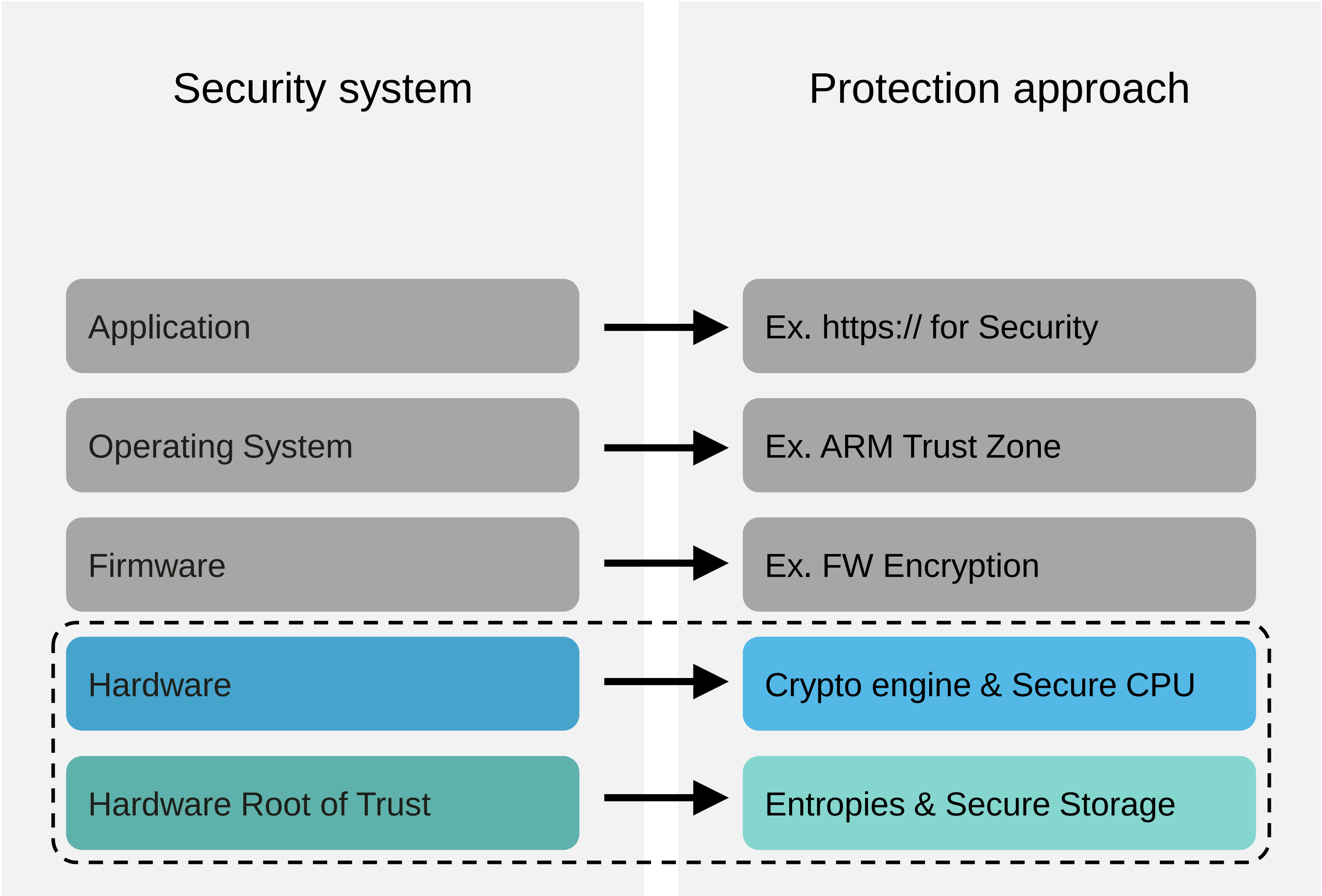
Threat to **Finances**

Colonial Pipeline pay $4.4m to end ransomware attack

massive shutdown of approximately half of the USA's East Coast fuel supply

Link

Only secure as the **weakest link**



- Insecure eFuse key storage can compromise a whole system
- Hackers always finds the weakest link to the system

Combining Hard and Soft IPs

Security Subsystem

Hard Macro
(process dep.)

- Anti-Tamper Design
- **TRNG** (entropy)
- **OTP** (Secure Storage)
- **PUF** (Chip Fingerprint)

Soft IP
(process indep.)

- Secure CPU
- HASH Crypto
- Sym. Crypto
- Asym Crypto

Security systems rely on OTP Memory

Secure OTP is replacing eFuse

Crypto engines require TRNG

TRNG is digital + analog

External Key injection is expensive

PUF has zero-touch provisioning

PUF / OTP / TRNG / Anti-tampering
Combined into one single
Hardware Root of Trust is Ideal

The **Three Fundamentals** of Hardware Root of Trust.

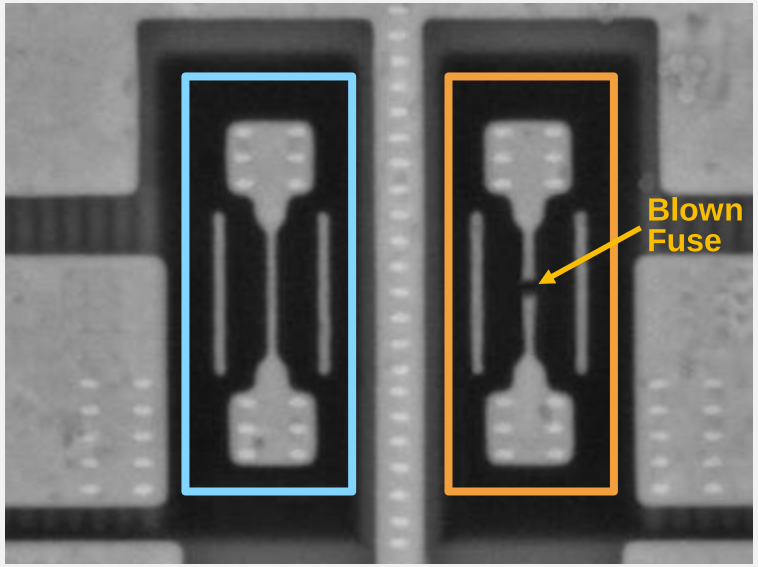
1. Secure Key Storage
2. Root Key Generation
3. High-Quality Entropy

Key Storage: Insecure eFuse

- **Invisibility** means an inherent resistance to Invasive Attacks
- Low programming current ➔ Suitable for **In-field programming**
- **High Reliability** even in advanced nodes

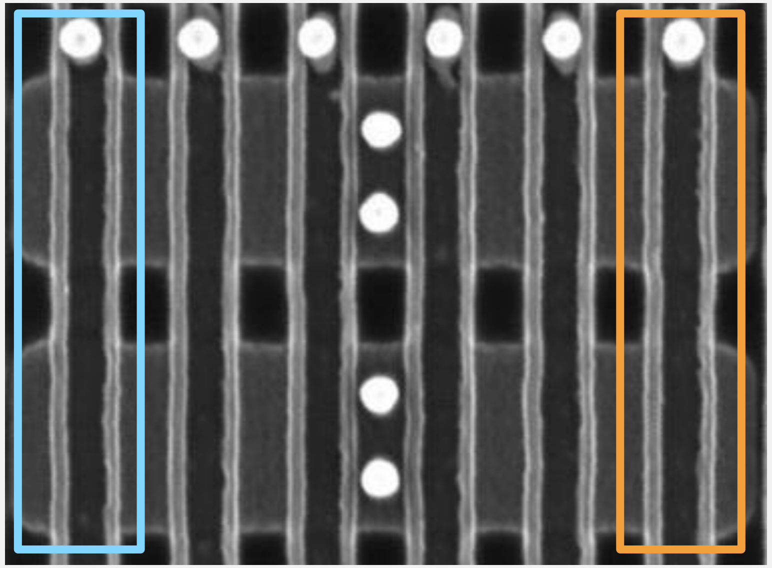
e-Fuse

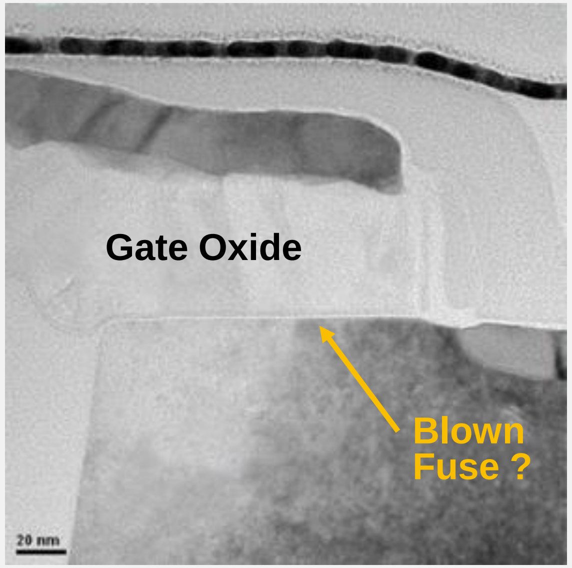
UN-PROGRAMMED PROGRAMMED



anti-Fuse OTP

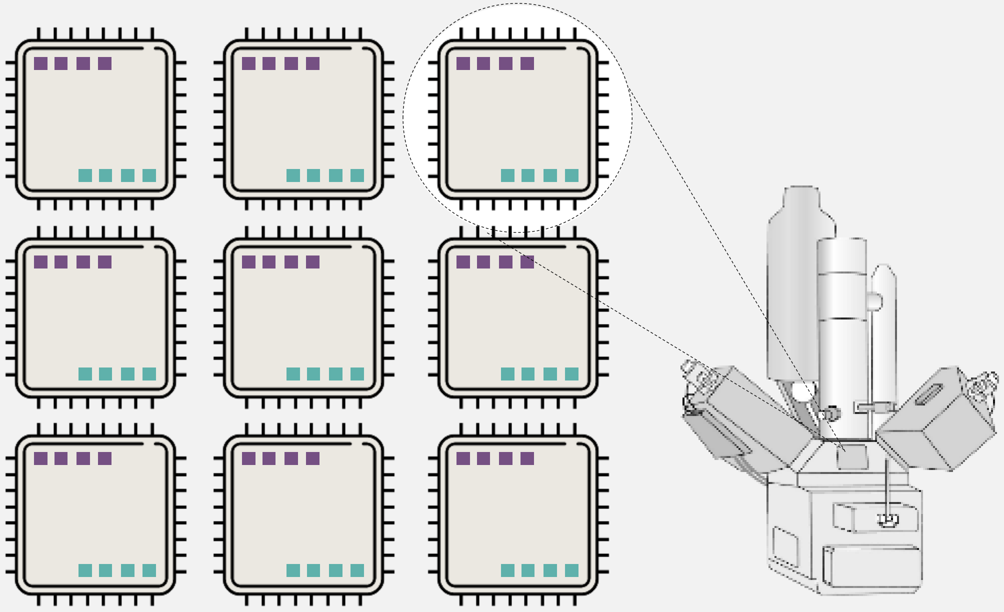
UN-PROGRAMMED PROGRAMMED (Cross-section)





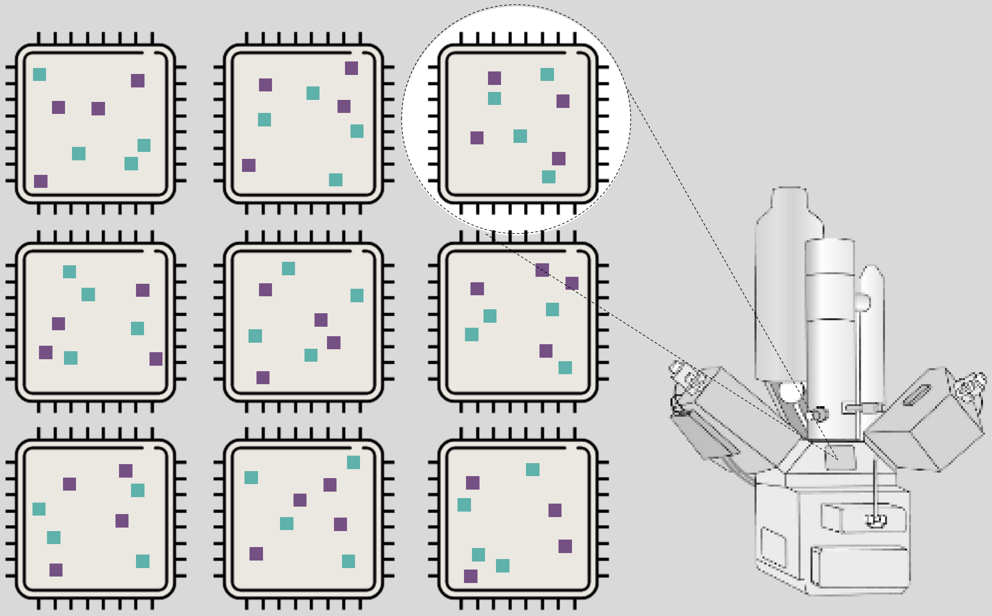
Key Storage: with Secure OTP

Anti-Fuse OTP
No PUF-based Storage



- OTP address can be easily located

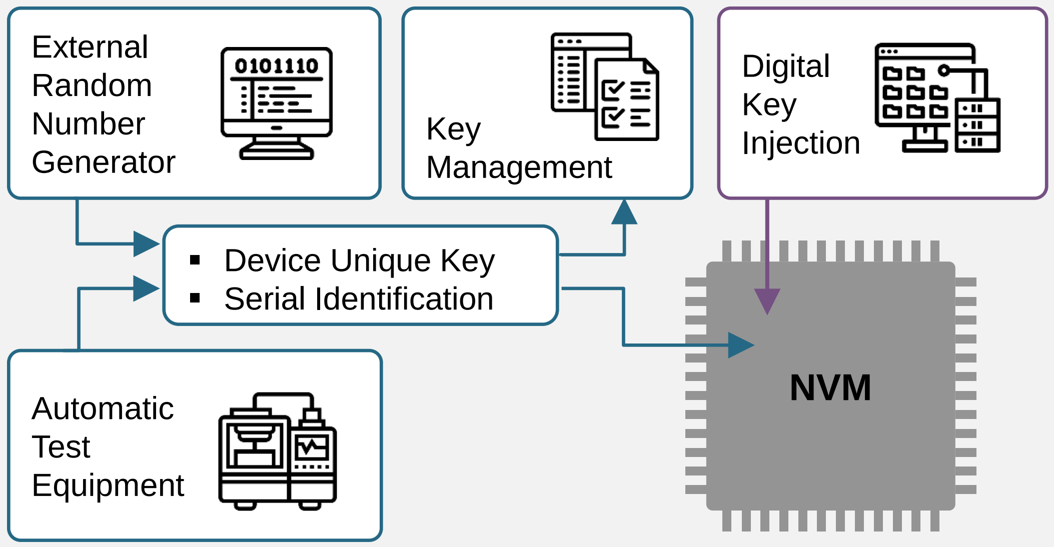
Secure OTP
With PUF Protection



- Different Physical location for each chip

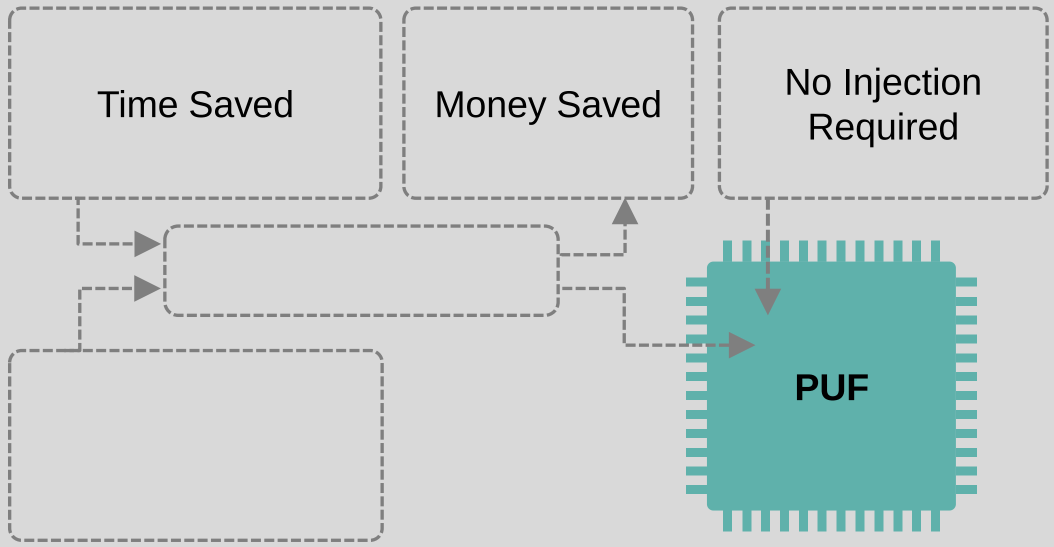
Root Key: Generated by Inborn PUF

Without PUF
Centralized Identification



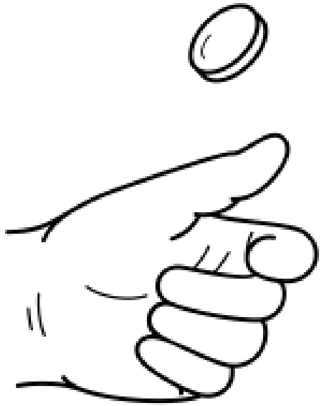
- **Initial injection required** for Key Management Server
- Key Injection must be done during CP or FT
- **Extra $0.5~$2/eu cost** and secure room (audit) needed

With PUF
De-Centralized Identification



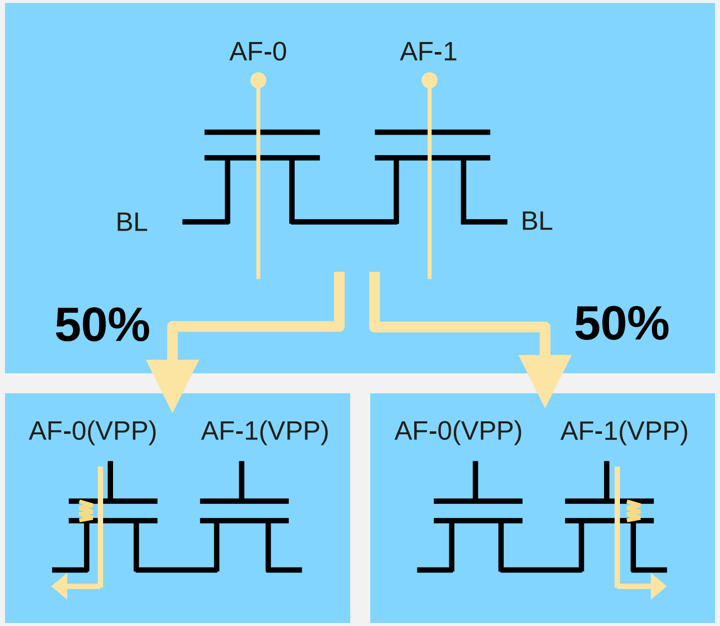
- Inborn Unique **PUF used directly as UID / HUK**
- Key Injection during CP or FT can be relieved until in-field product to **comply with Zero-Touch IoT**

Root Key: from an Ideal PUF



- Process variation always exists in semiconductor devices, however, adjacent devices are nearly identical
- **NeoPUF** leverages this microscopical minute variations to achieve ideal PUF (ISSCC2019 Outstanding Paper)
- **Ideal for Inborn-Key / UID ➔** No need for key provisioning

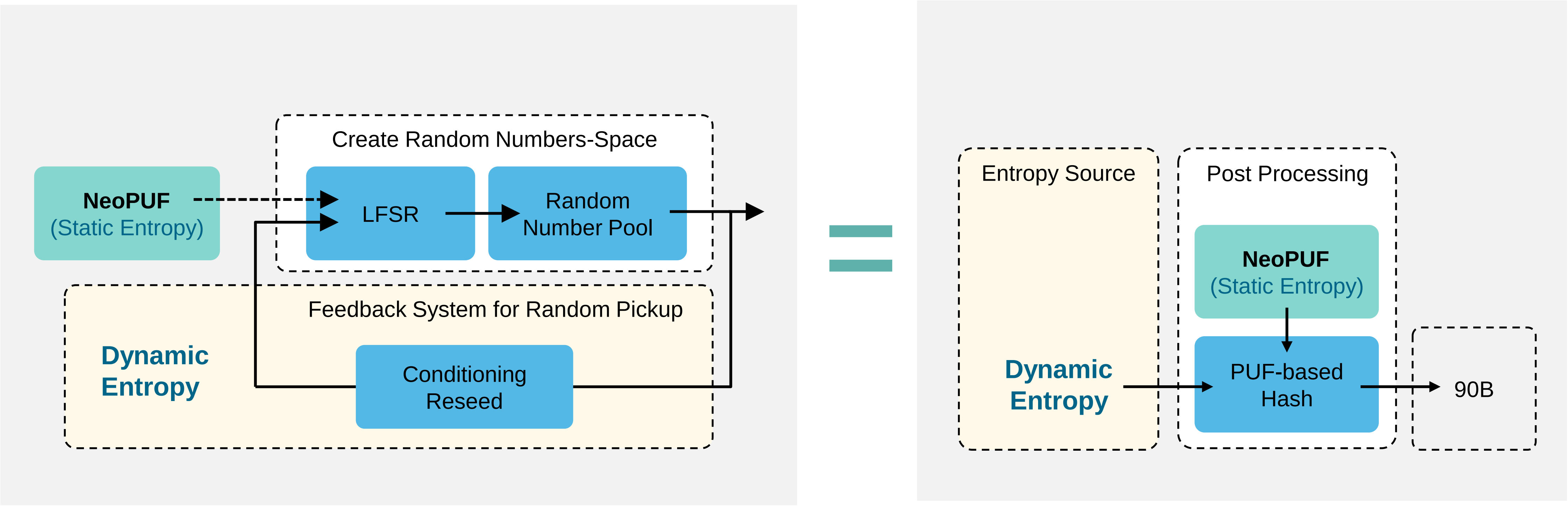
Quantum Tunneling PUF



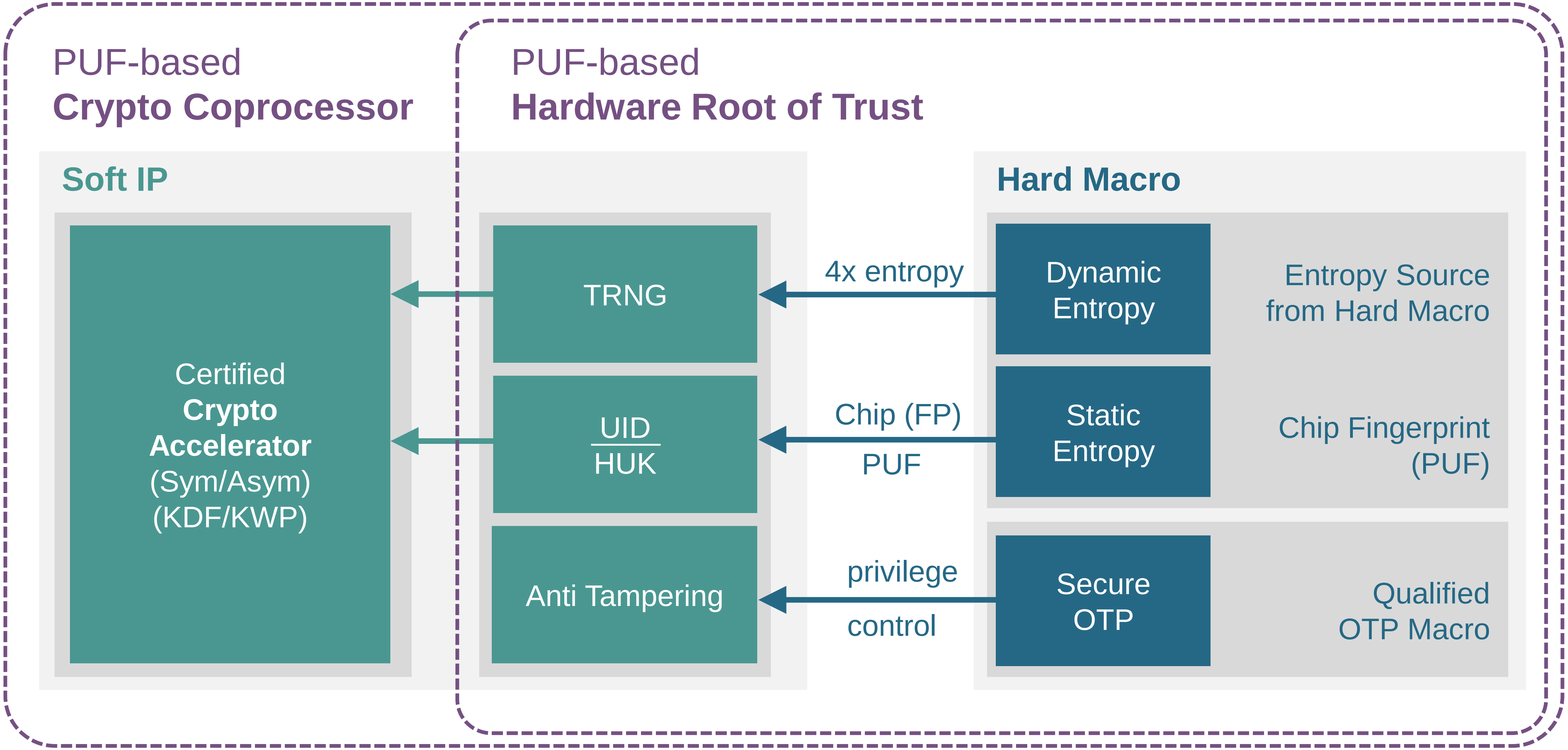
Metric	**Checked by**	**Ideal PUF**	**NeoPUF**
Randomness	Hamming Weight (HW)	50%	50%
Uniqueness	Hamming Distance (HD)	50%	50%
Robustness	Bit Error Rate (BER)	0%	0% for all PVT
Helper Data	Error Correction Code	No Need	No Need
Entropy Quality	Min. entropy of bits	1	~1
Invisibility	Reversed Engineering	Untraceable	Untraceable
Manufacturability	Yield and Reliability	100%	100%, all Tech.
Radiation Hardening	Gamma Ray Radiation	Radhard	Radhard

High-Quality Entropy: PUF-based TRNG

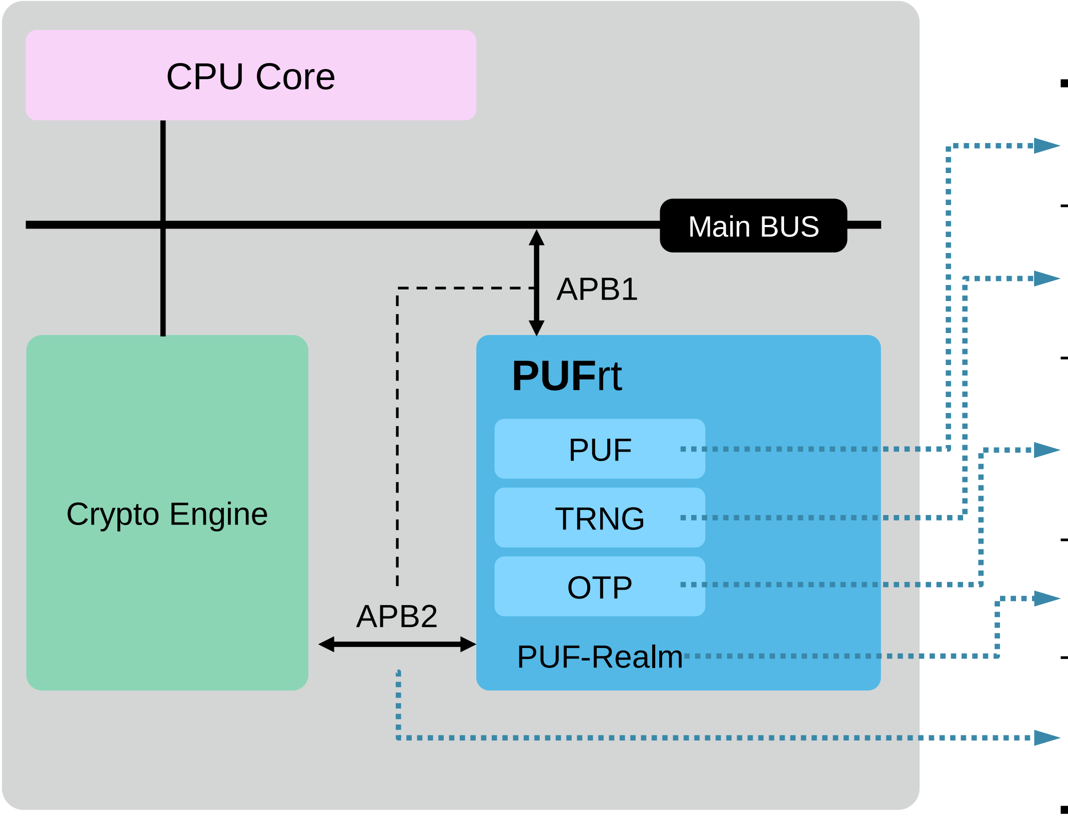
- **NeoPUF:** 1Kbits, pre-load into the 1K registers
- **Random Number Sets:** 32-bit LFSR combined a PUF with three ways expansion
- **Feedback System:** Output reseeds LFSR using two dynamic entropies and conditioning



Concept of **PUF-based** Hardware Root of Trust

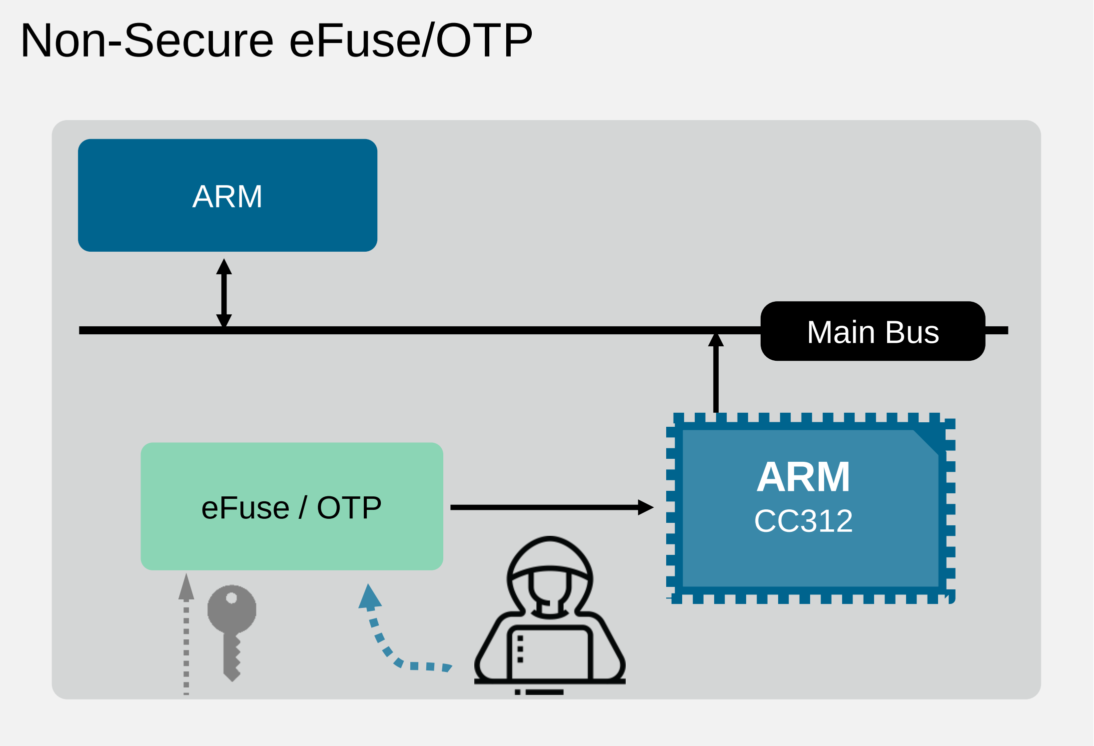


PUFrt: PUF-based Hardware Root of Trust

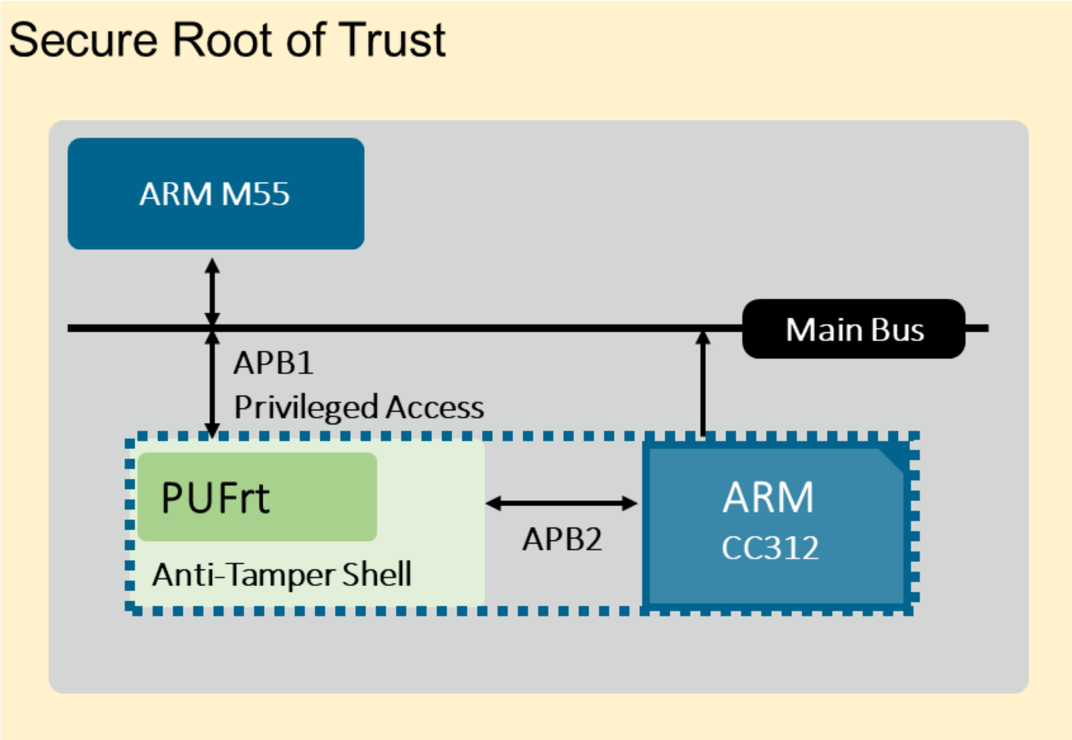


PUFrt	Features / Benefits
Secure Storage (8Kb)	▪ **Secure OTP** ▪ Anti-physical/electrical attack
Integrated TRNG	▪ Instant ready 90b in 100us ▪ **Plug & Play dynamic entropy source** ▪ NIST SP800-90B / 800-22 compliant
Inborn PUF (1Kb)	▪ **Alternative to key injection process (~$0.5-2 per device)** ▪ Instant ready without helper
Anti-Tamper	▪ The design and entropy will protect macro, operation and interface
Dual Interface	▪ Standard APB-s Controller ▪ **Privileges to Secure/Non-secure** ▪ Customizable to TCM and TileLink

PUFrt: The missing piece of the puzzle



- Visible eFuse
- No security policy
- Insecure channel possible fault injection, etc.



- Inborn chip fingerprint by PUF
- Complete anti-tampering shell
- Comprehensive secure boundary

Thank You

PUFsecurity

AN eMemory COMPANY