

# OTP-less HW Root of Trust with Invisible Keys

Intrinsic ID, Worldwide Leader in PUF Technology

Pim Tuyls

CEO & Founder



**INTRINSIC ID**™

Authenticate Everything

# Intrinsic ID Profile



## Global Presence

Silicon Valley, Austin, Phoenix, Eindhoven, China  
Israel, Japan and Korea representation

## Core Technology

Solid patent portfolio in PUF technology

## Investors

Prime Ventures  
Robert Bosch Venture Capital



## Markets Served



Datacenters/HPC



Internet of Things



Secure Transactions

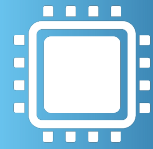


Aerospace & Defense

# Industry Leaders Rely on Intrinsic ID



Defense  
Contractors



**400M+**

Deployments in the Field



**4 of Top 5**

MCU Vendors as a Customer



**100+**

Design Wins



**Top 4**

FPGA Platforms



**10+**

Global certifications and  
Government programs



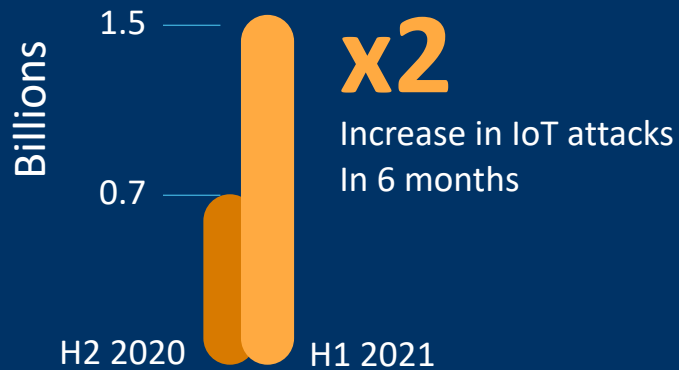
# IoT Attacks Are on the Rise

**"98% of all IoT device traffic is unencrypted"**

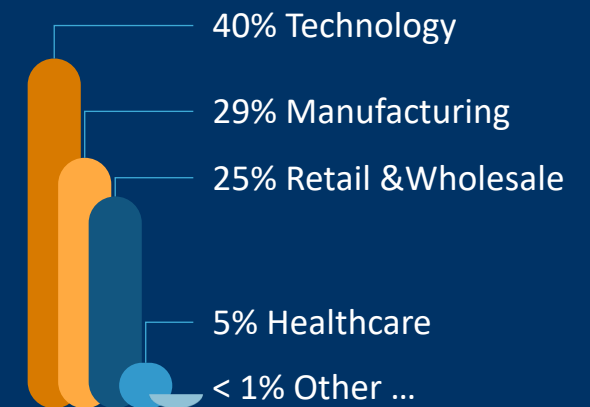
Palo Alto Networks

**"Only 4% of deployed IoT products have security"**

GlobalPlatform



## IoT Attacks by Industry





# Cryptography Needed to Prevent Attacks



## Authentication



Provides  
Trusted Source

## Signing



Provides Data  
Integrity

## Encryption



Provides Data  
Confidentiality

# What is Required: Root of Trust



- Root of Trust for **Secrecy**

- Secret that no other entity can get information about
- Guarantees that the device can not be impersonated and that it can keep confidentiality



**Confidentiality**  
**Device Authentication**

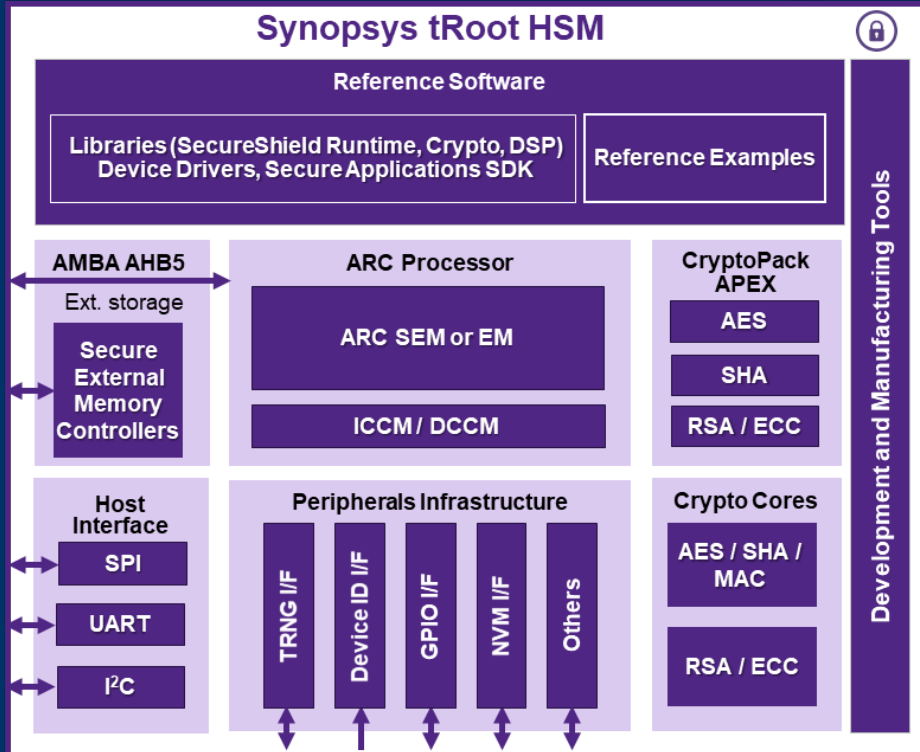
- Root of Trust for **Integrity**

- Circuit and data that can not be changed
- Guarantees that no un-authorized data and SW can be run on the device



**SW Integrity**

# A Prime Example: Synopsys tRoot Family



- Hardware secure modules
- TEE
- Secure services
- Secure boot
- Integrity protection
- Anti-tampering
- Memory access protection
- Scalable cryptography

**What about secure key storage?**



# Kerckhoffs's Principle



“A Cryptosystem should be secure even if everything about the system, except the secret key, is public knowledge”

*Auguste Kerckhoffs*



Security depends on the  
**secrecy** of the **key**

# Requirements for Secret Keys in Silicon

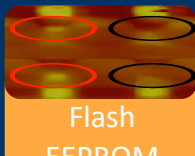


```
100101110101000111
011011001000101011
111010010101000100
  011110101
```

## Physical Element



Anti-fuse



Flash  
EEPROM



ROM



Fuses

## Mathematical Requirements

- ✓ Unpredictable
- ✓ Unique - preferably unique per device

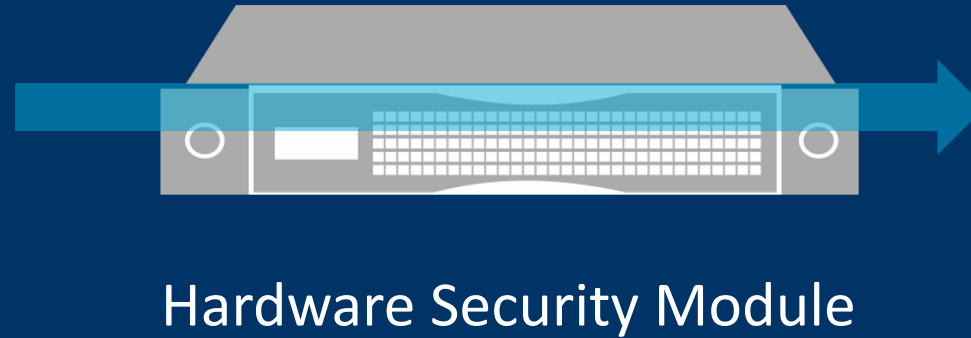
## Physical Requirements

- ✓ Invisible to Attackers
- ✓ Unclonable
  - ✓ Cannot be copied from one device to another
- ✓ Immutable
  - ✓ Not changeable by attackers
  - ✓ No change over time e.g. no silicon degradation
- ✓ Easily Accessible

# Traditional Method: Key Injection

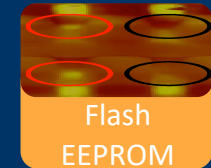


```
100101110101000111
011011001000101011
111010010101000100
  011110101
```



Hardware Security Module

## Physical Element



**High Cost**

**Low Flexibility**

**Low Security**



# Challenges Towards Advanced Technology Nodes



## NVM

Fuse, anti-fuse, flash

- Scaling is challenging
- Less reliable key storage

Where to securely and reliably store keys?

## Basic Components

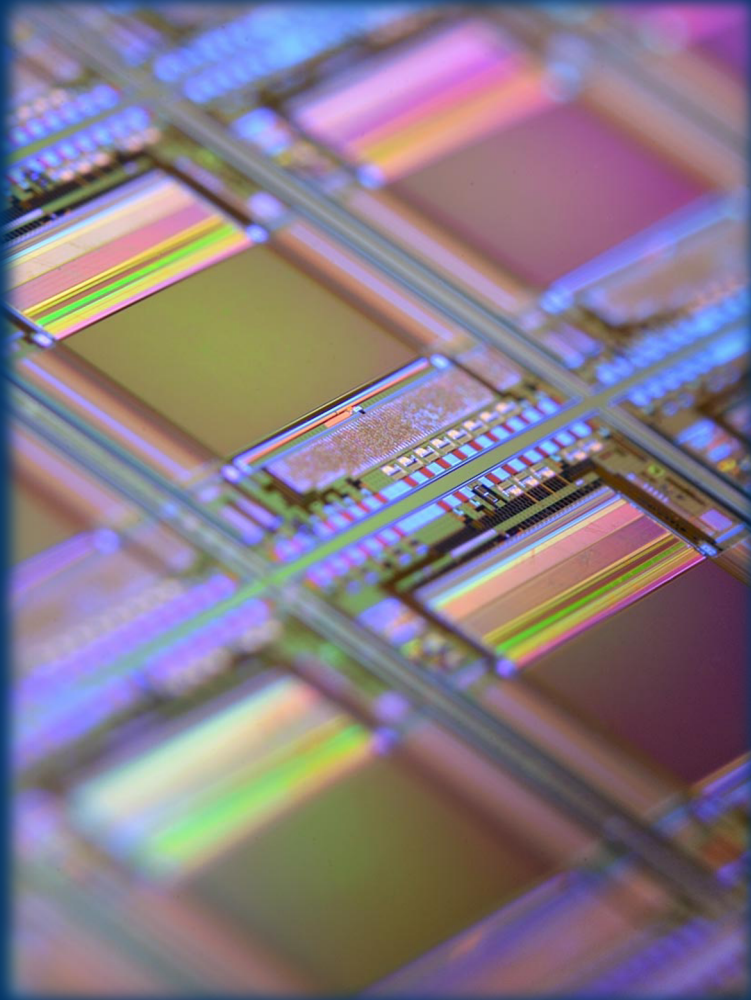
gates, flip-flops, SRAM



NVM in larger node

No NVM available on chip

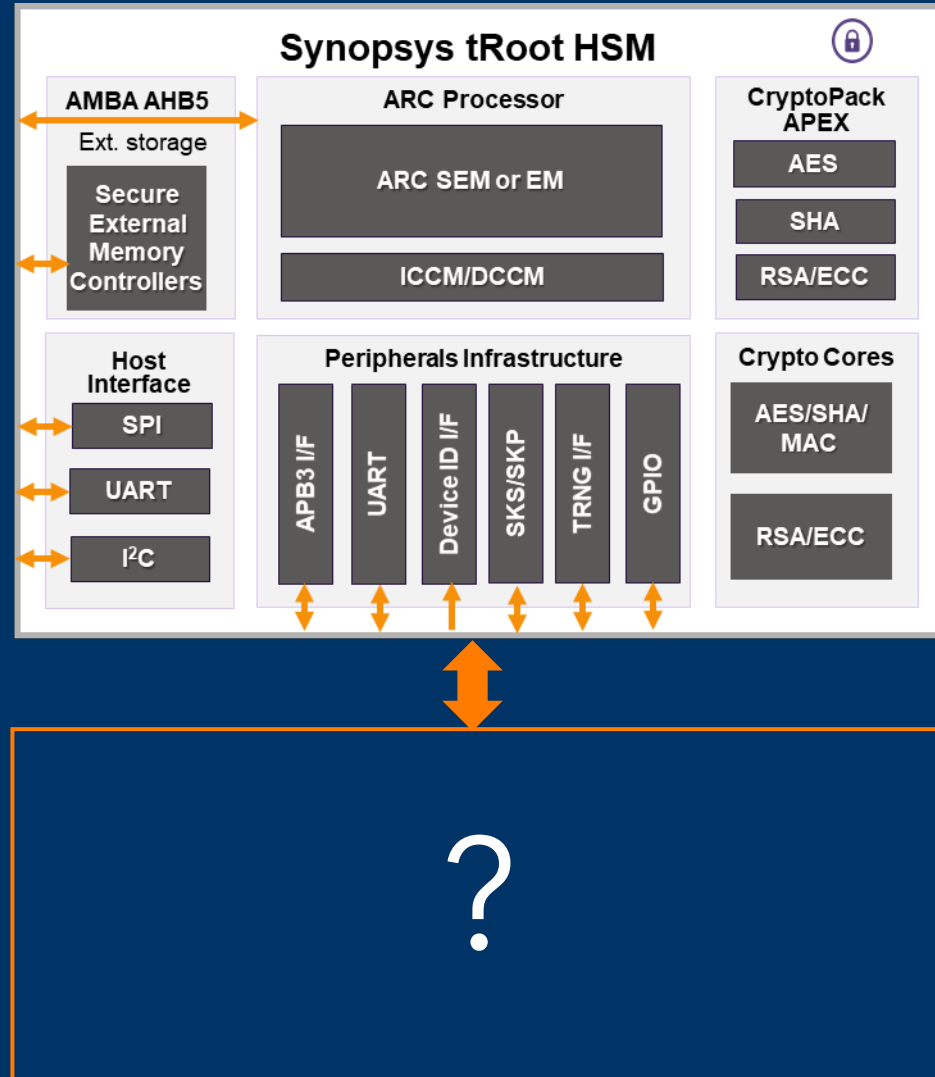
# The Need for New Key-Storage Solutions



In advanced nodes **OTP solutions** are costly and less reliable

**Technology Scaling** and **Increased Attack Surface** require new solutions

# Secure Key Storage for tRoot Without OTP?





# SRAM PUF Keys from Silicon



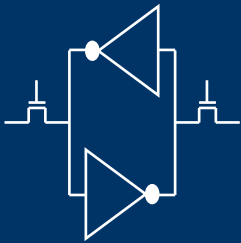
1



## Process Variation

Deep sub-micron variations in the production process give every transistor slightly random electric properties

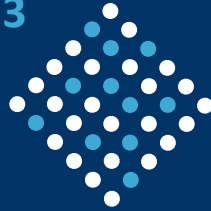
2



## SRAM Start-up Values

When the SRAM is powered on this randomness is expressed in the start-up values (0 or 1) of SRAM cells

3



## Silicon Fingerprint

The start-up values create a highly random and repeatable pattern that is unique to each chip

4



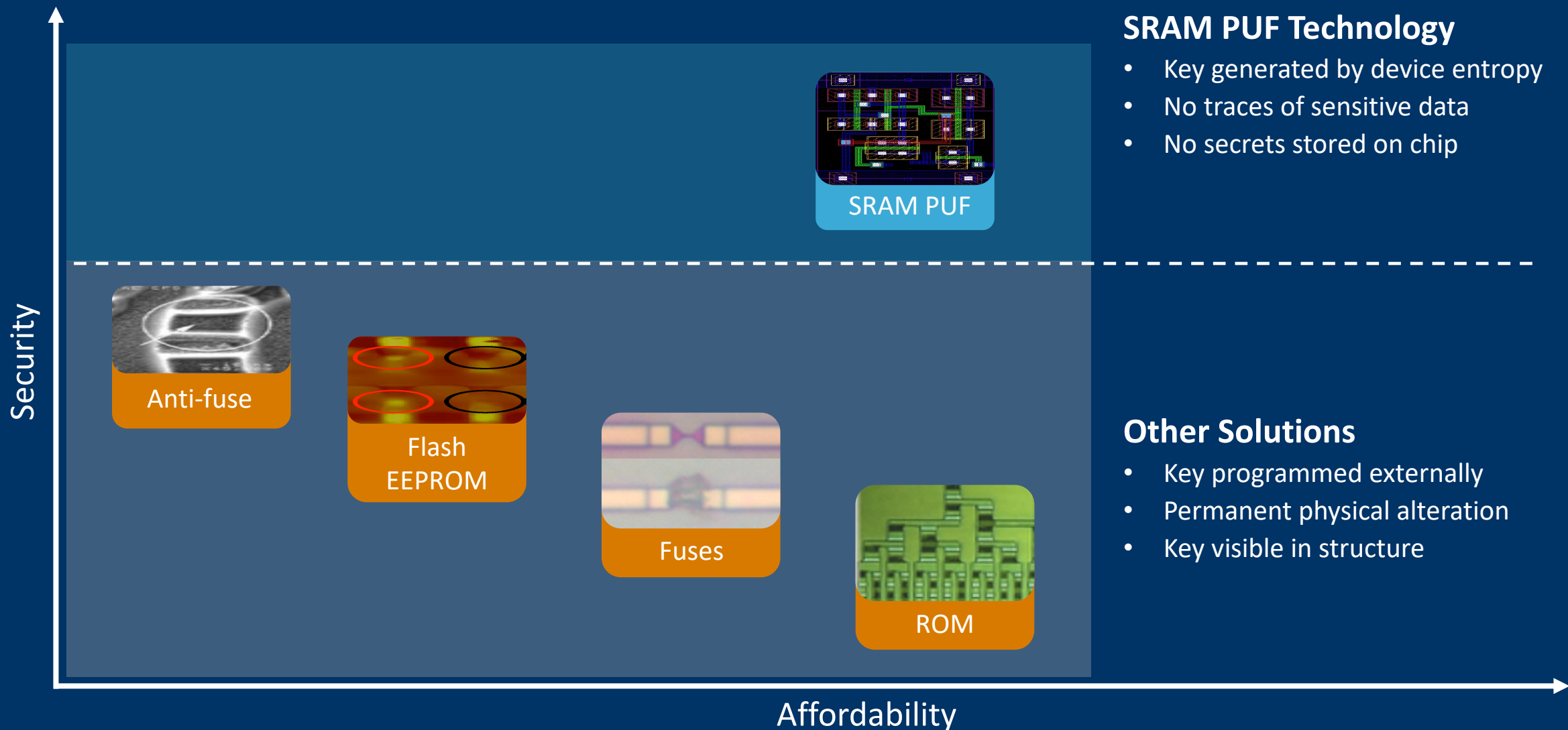
## SRAM PUF Key

The silicon fingerprint is turned into a secret key that builds the foundation of a security subsystem

## SRAM PUF Benefits

- Device-unique, unclonable fingerprint
- Leverages entropy of mfg. process
- No key material programmed

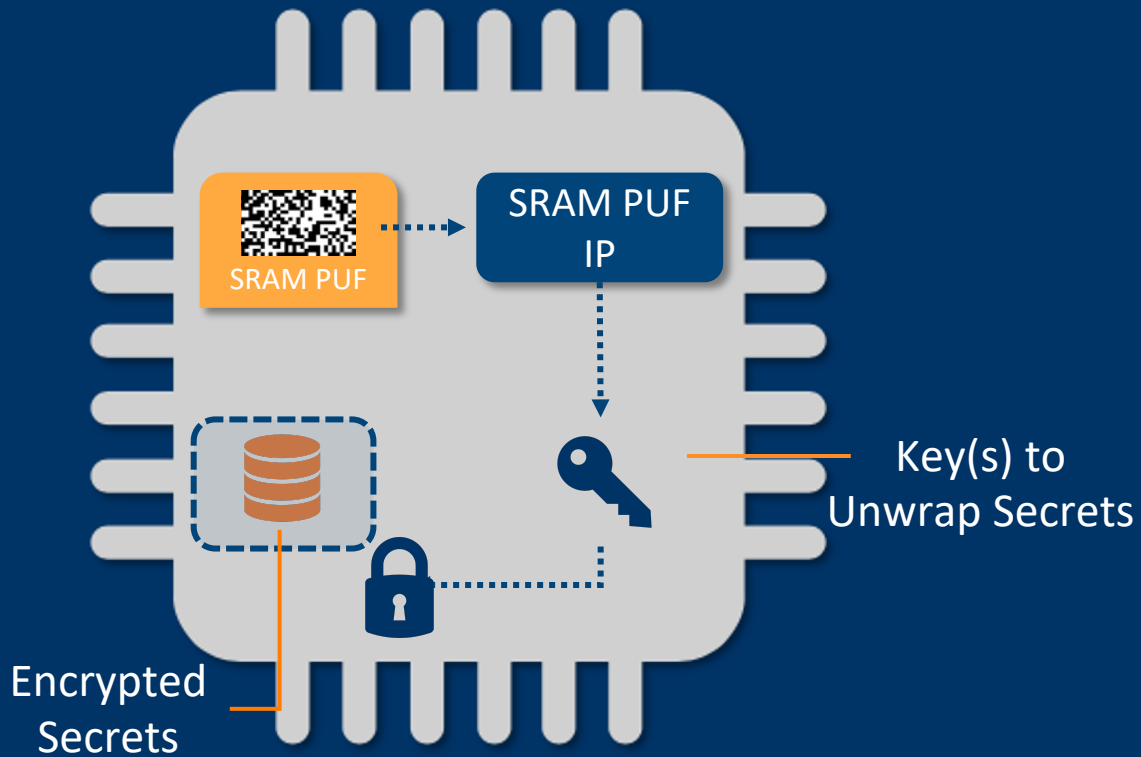
# SRAM PUF Advantages in Secure Key Storage



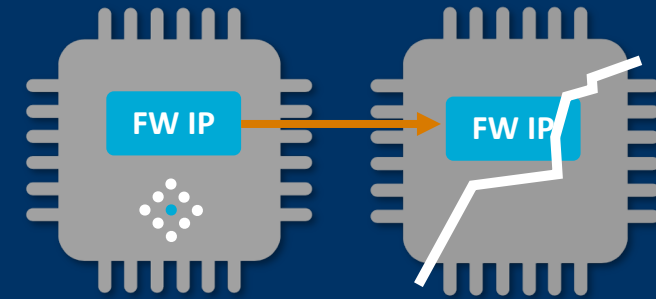
# Typical SRAM PUF Use Cases



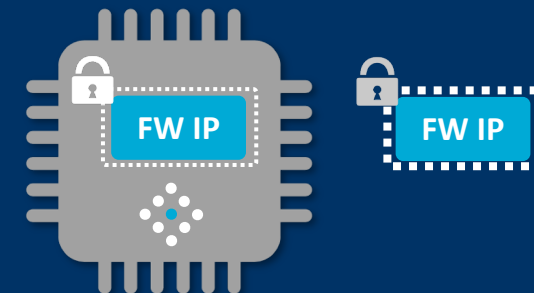
## Secure Vault



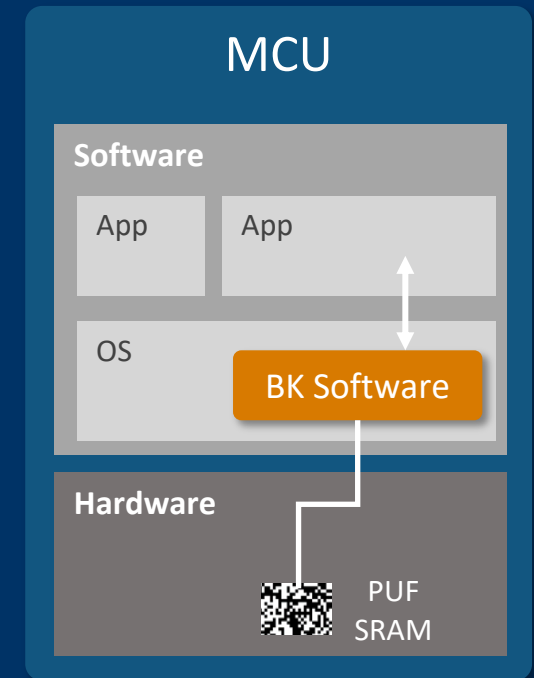
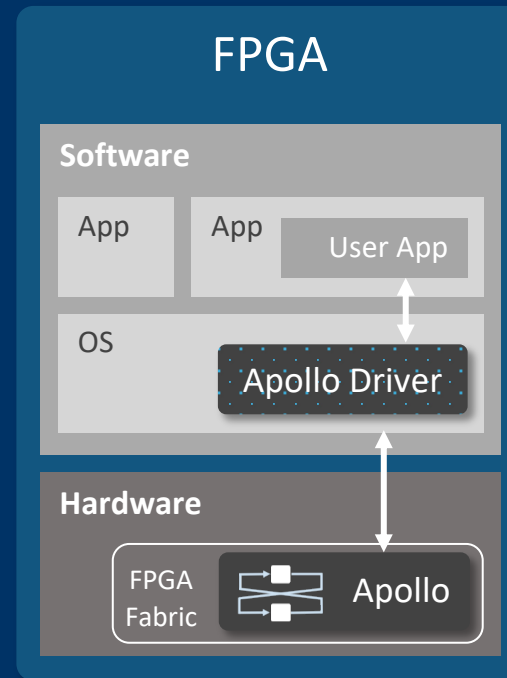
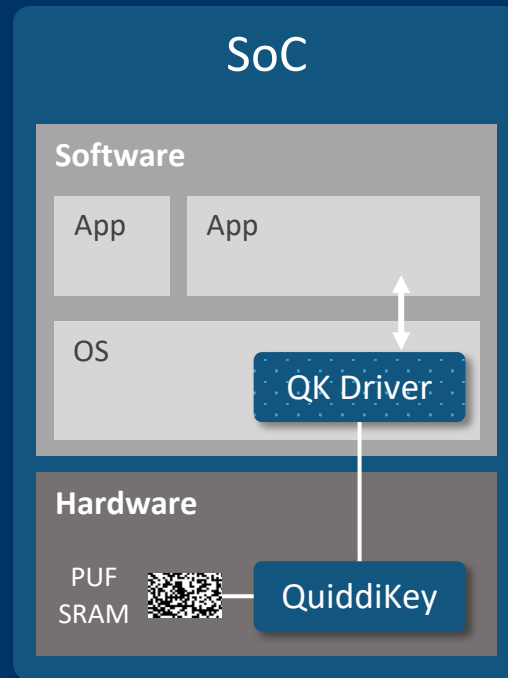
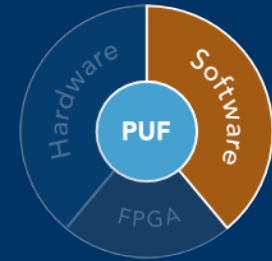
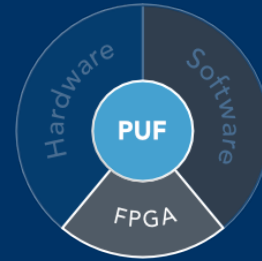
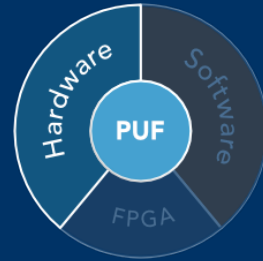
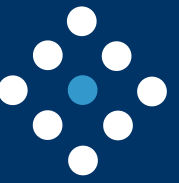
## Anti-Cloning



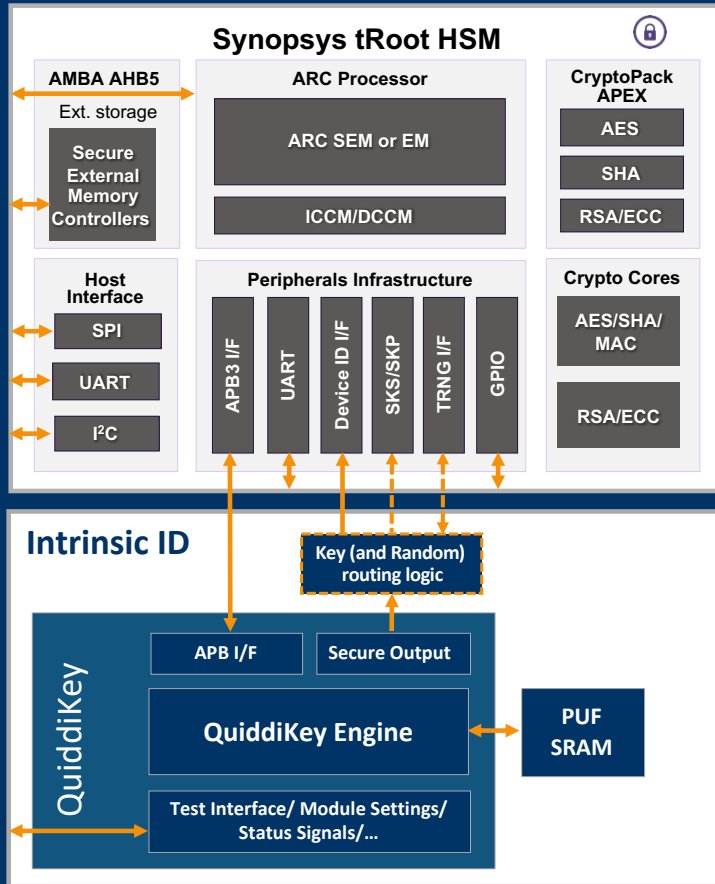
## Preventing Reverse-Engineering



# PUF Solutions in Hardware, Software, and on FPGA

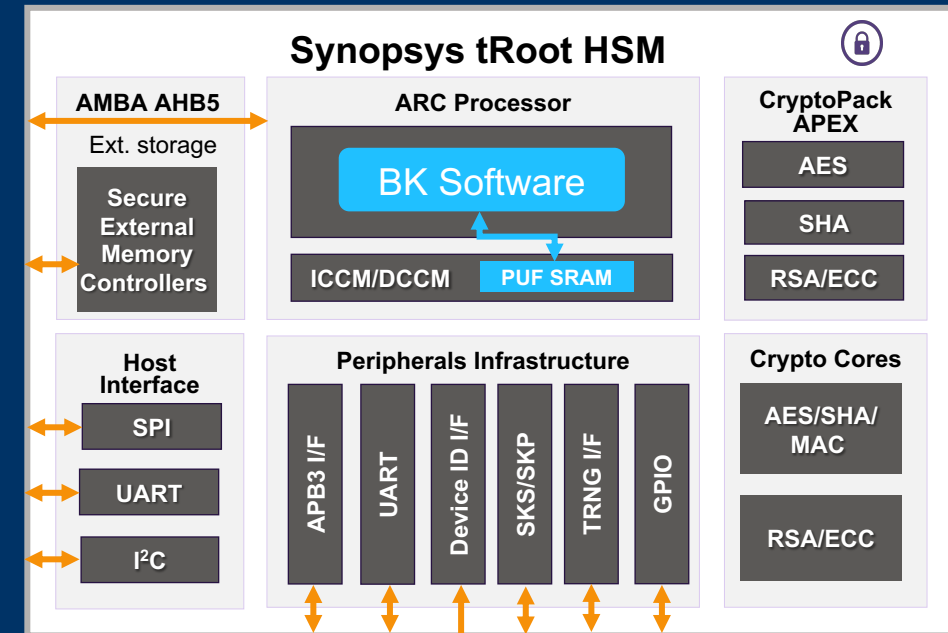


# tRoot Integration – Hardware/Software



## QuiddiKey Integration

Full black-box hardware solution



## BK Software Integration

Retrofitting PUF technology on existing devices

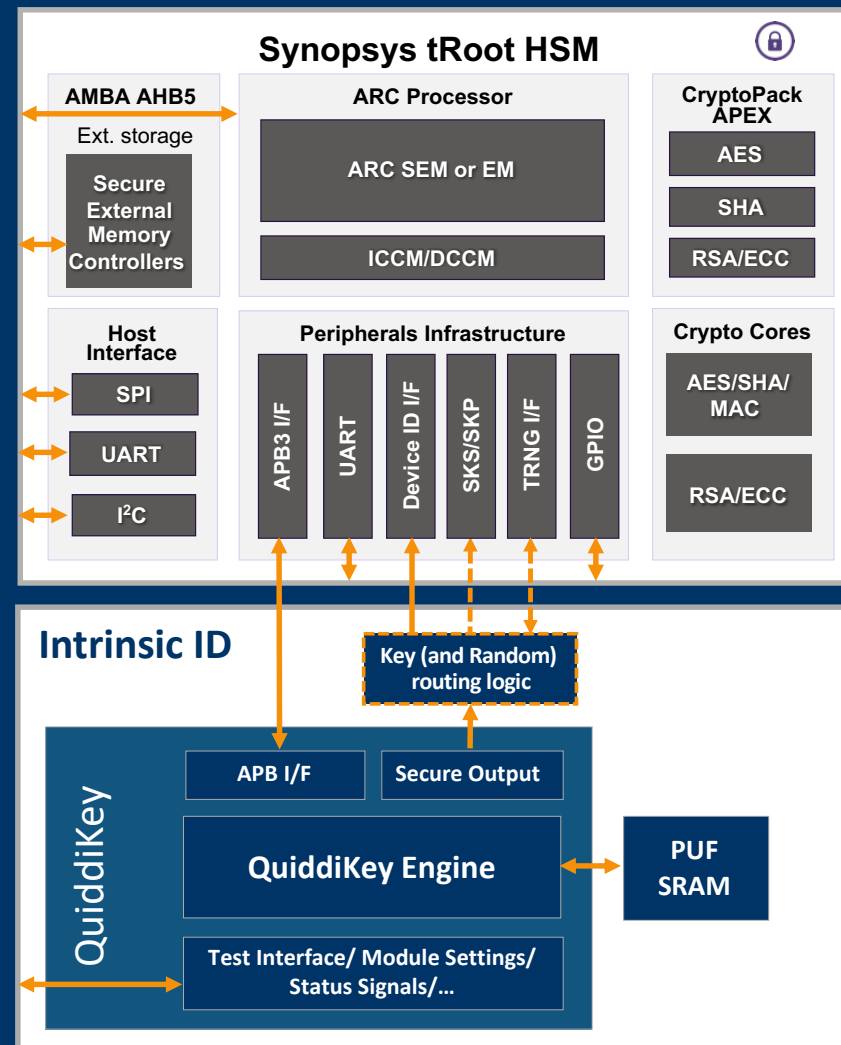
# SRAM PUF – tRoot Integration Benefits



- ✓ Off-the-shelf integration
- ✓ Technology scaling independent
- ✓ Does not require any OTP
- ✓ Reliable and secure key storage mechanism
  - ✓ Temperature range from -55°C up to 150°C
  - ✓ >25 years lifetime
- ✓ QuiddiKey/BK controlled by tRoot
  - No interface change for tRoot users





**OTP-less Root-of-Trust Solution**





# How is the Solution Delivered?



	<b>QuiddiKey</b> Hardware solution	<b>BK Software</b> Retrofitting PUF technology on existing devices
	<ul style="list-style-type: none"><li>• Standard QuiddiKey delivery (RTL, C code, documentation, ...)</li></ul>	<ul style="list-style-type: none"><li>• Standard BK Software delivery (Compiled library, documentation, ...)</li></ul>
<b>Together</b>	<ul style="list-style-type: none"><li>• Glue logic (RTL)</li><li>• Software package with QuiddiKey driver pre-integration (C code, documentation)</li><li>• Example code for QuiddiKey usage</li></ul>	<ul style="list-style-type: none"><li>• Reference design using BK (C code and documentation)</li><li>• Integration documentation</li><li>• Example code for BK usage</li></ul>
	<ul style="list-style-type: none"><li>• Standard tRoot delivery (RTL, C code, documentation, tools,...)</li></ul>	<ul style="list-style-type: none"><li>• Standard tRoot delivery (RTL, C code, documentation, tools, ...)</li></ul>

Fully digital IP delivery packages, no technology dependency

# Stop By and See the Demo!



ARC IoT Development Kit

Authentication based  
on BK Software



# Summary



- Technology scaling and increased security needs require secure key storage **solutions without OTP**
- The Intrinsic ID PUF scales well with all technology nodes and offers the **highest security** for key storage
- The integration of Intrinsic ID PUF solutions in Synopsys tRoot offer an **OTP-less RoT solution**



## **Intrinsic ID Collaborates with Synopsys to Boost SoC Security and Accelerate Time to Market**

*Seamless Integration between Intrinsic ID PUF and Synopsys tRoot HSM Security IP Solutions Provide Strong Device-Level Protection*

SUNNYVALE, Calif., Sept 6, 2022 – **Intrinsic ID**, the world's leading provider of Physical Unclonable Function (PUF) security IP today announced a renewed collaboration with **Synopsys, Inc.** to provide pre-verified PUF and hardware secure module (HSM) security solutions that protect connected devices against advanced security threats. The **Synopsys tRoot™ HSM IP** now offers easy integration with Intrinsic ID **QuiddiKey®** hardware IP implementing SRAM PUF, enabling designers with little security experience to quickly add system and data protection features to their SoC designs. Additionally, Intrinsic ID CEO Pim Tuyls will be speaking about the collaboration at the **Synopsys ARC**



INTRINSIC ID™

Thank You!

Pim Tuyls

Pim.Tuyls@Intrinsic-ID.com

[www.Intrinsic-ID.com](http://www.Intrinsic-ID.com)