Cybersecurity Solution in Hardware

Ujjwal Guin

Department of Electrical and Computer Engineering
Auburn University, AL, USA

Cybersecurity Solution in Hardware

Outline

- Motivation
  - Counterfeiting and piracy
- Detection and avoidance of counterfeit ICs
  - Design-for-Anti-Counterfeit (DfAC) measures
  - Proposed on-chip aging structure
  - End-to-end protection
- Detection of counterfeit/cloned electronics
  - Use of Blockchain to enable device traceability
  - Firmware Obfuscation

Counterfeiting and Piracy

Counterfeiting & Piracy

Amount of total counterfeiting globally has reached to 1.2 Trillion USD in 2017 and is bound to reach 1.82 Trillion USD by the year 2020.

Counterfeit Electronics

Electronics companies suffer a loss of around $100 billion every year because of counterfeiting [AGMA].

Counterfeit ICs

Counterfeit components pose a risk of $169B per year for global electronic supply chain [IHS].

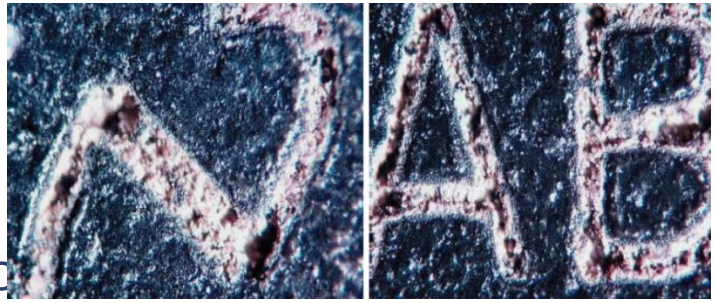
Images: Google

AUBURN UNIVERSITY

Counterfeit Electronic Parts

A counterfeit component [US Dept. Of Commerce, 2010]

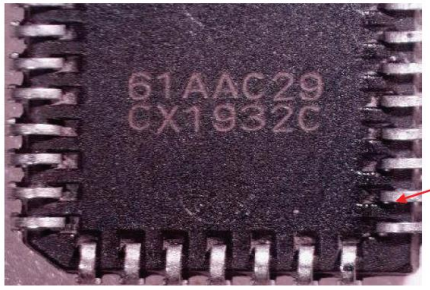
- is an unauthorized copy;
- does not conform to original OCM design, model, and/or performance standards;
- is not produced by the OCM or is produced by unauthorized contractors;
- is an off-specification, defective, or used OCM product sold as "new" or working; c
- has incorrect or false markings and/or documentation.



Looks simple enough Intel device, marking not too bad, OH OH!!

The ink dot that identifies a reject from wafer sort.

Here is the chip ID found after decap, looks good and matches the package marking



Backside, look at the black shiny paint like substance in the lower right side, the mold pin cavity is almost gone, look at the bent leads, looks like it may have been painted over to hide sanding marks and then fraudulently remarked

AUBURN UNIVERSITY

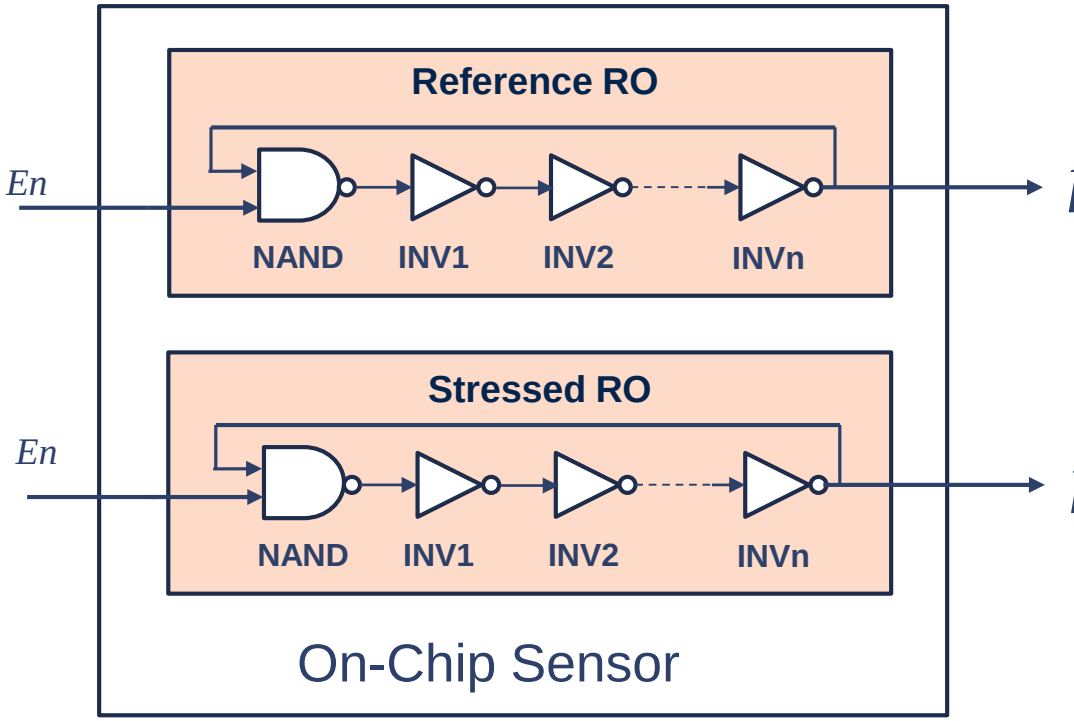
Outline

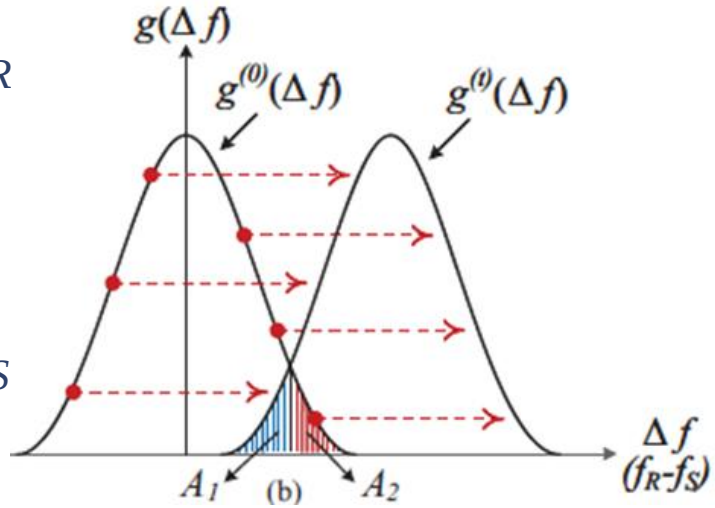
- Motivation
  - Counterfeiting and piracy
- Detection and avoidance of counterfeit ICs
  - Design-for-Anti-Counterfeit (DfAC) measures
  - Proposed on-chip aging structure
  - End-to-end protection
- Detection of counterfeit/cloned electronics
  - Use of Blockchain to enable device traceability
  - Firmware Obfuscation

AUBURN UNIVERSITY

Design-for-Anti-Counterfeit (DfAC)

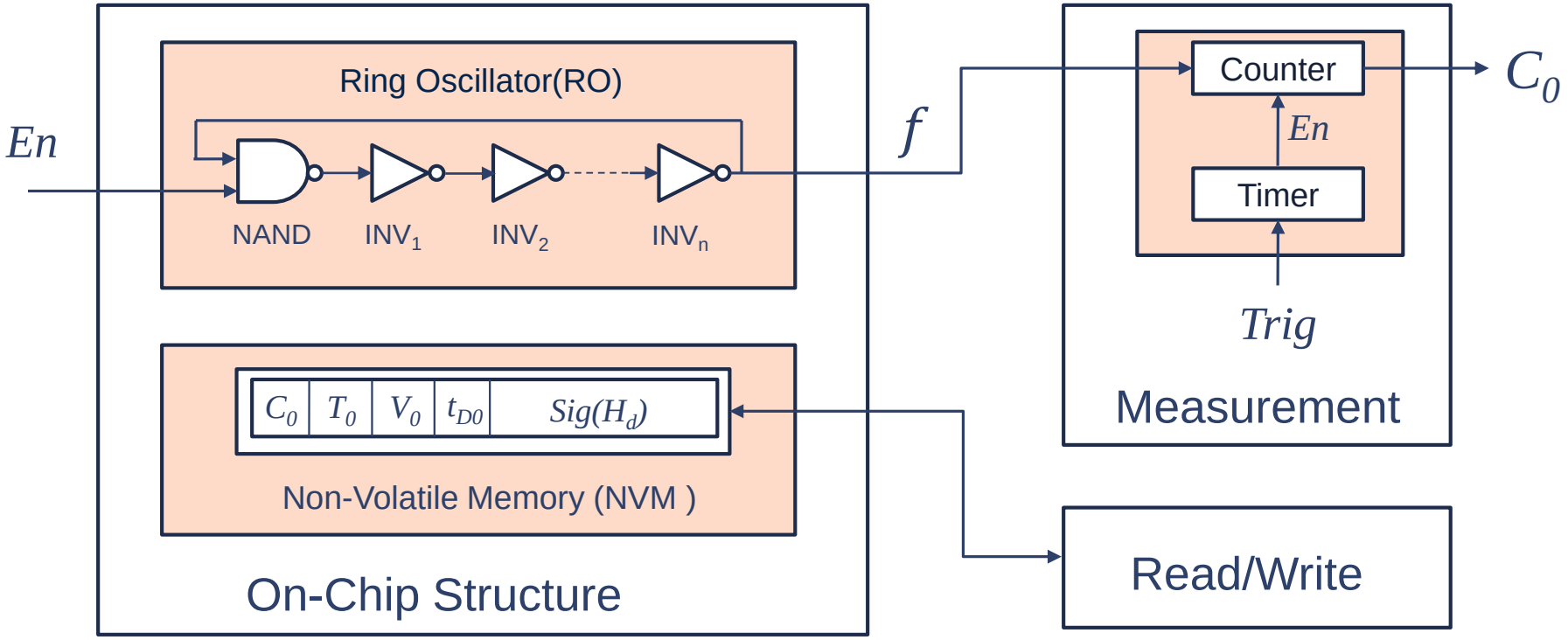
- Challenges
  - Process variation impacts detection accuracy.
- Design goal
  - Low implementation cost
  - Low cost measurement unit
  - Automated detection process





Loss of detection accuracy

Proposed On-Chip Aging Structure

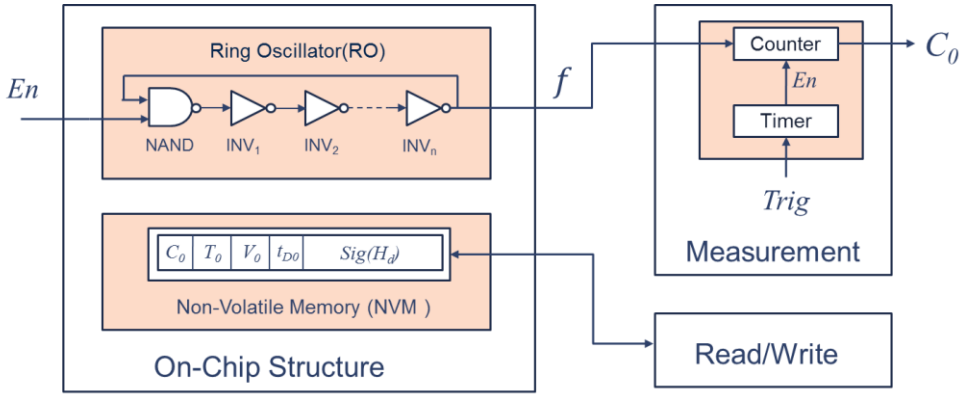


- Utilize a ring oscillator (RO) and a non-volatile memory (NVM).
- Eliminate the process variation completely.
- NVM Content
  - Frequency (C_0), Supply voltage(V_0), Temperature (T_0), Time duration (t_{D0}), Digital signature (Sig(H_d)) on the data *d.*

AUBURN UNIVERSITY

Registration Process

Measure RO Frequency (C_0), and Read $ECID$



Construct Data (D)

$RD=\{C_0||T_0||V_0||t_{D0}\}$

$D=\{ECID||RD\}$

Compute Hash (H_D)

$H_D=Hash_{SHA\text{-}2/SHA\text{-}3}(D)$

Compute Signature ($Sig(H_D)$)

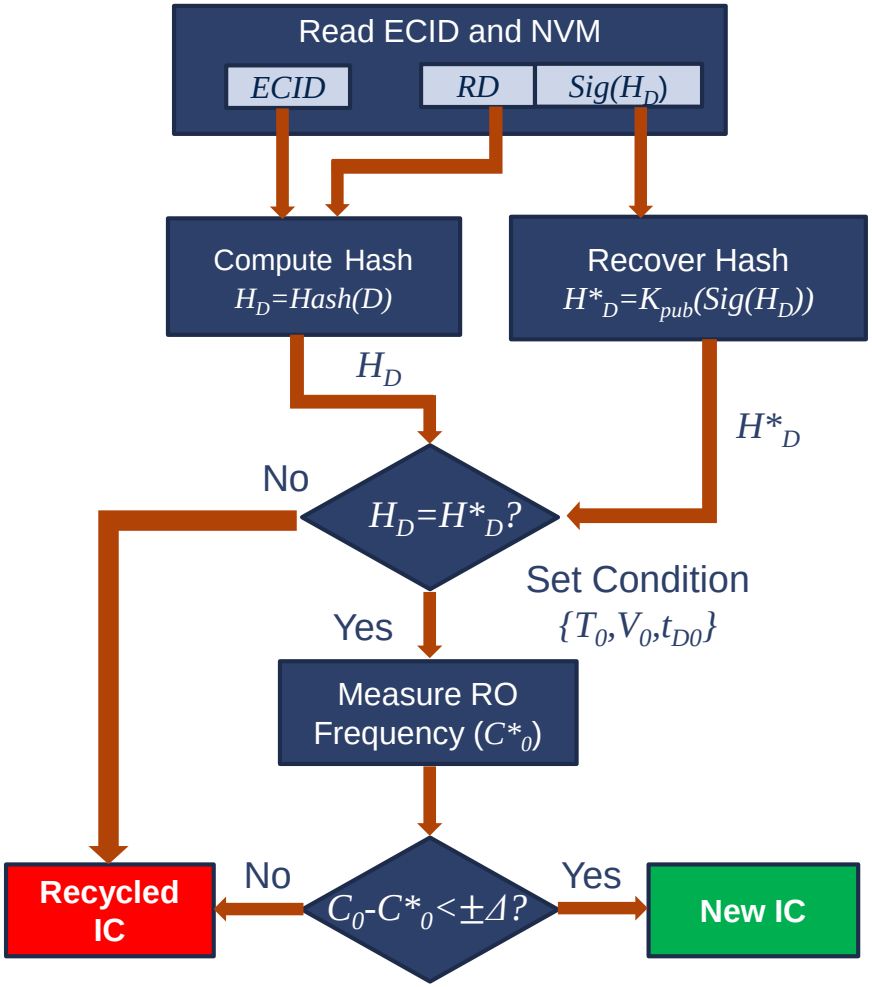
$Sig(H_D)=E_{Kpri}(H_D)$

Program NVM

$\{RD,Sig(H_D)\}$

AUBURN UNIVERSITY

Authentication Process



- Two-Level Authentication Process
  - Level-1: Hash comparison
    - Applicable for detecting Recycling, Remarking, and cloning.
  - Level-2: Frequency comparison
    - Applicable for detecting recycling.

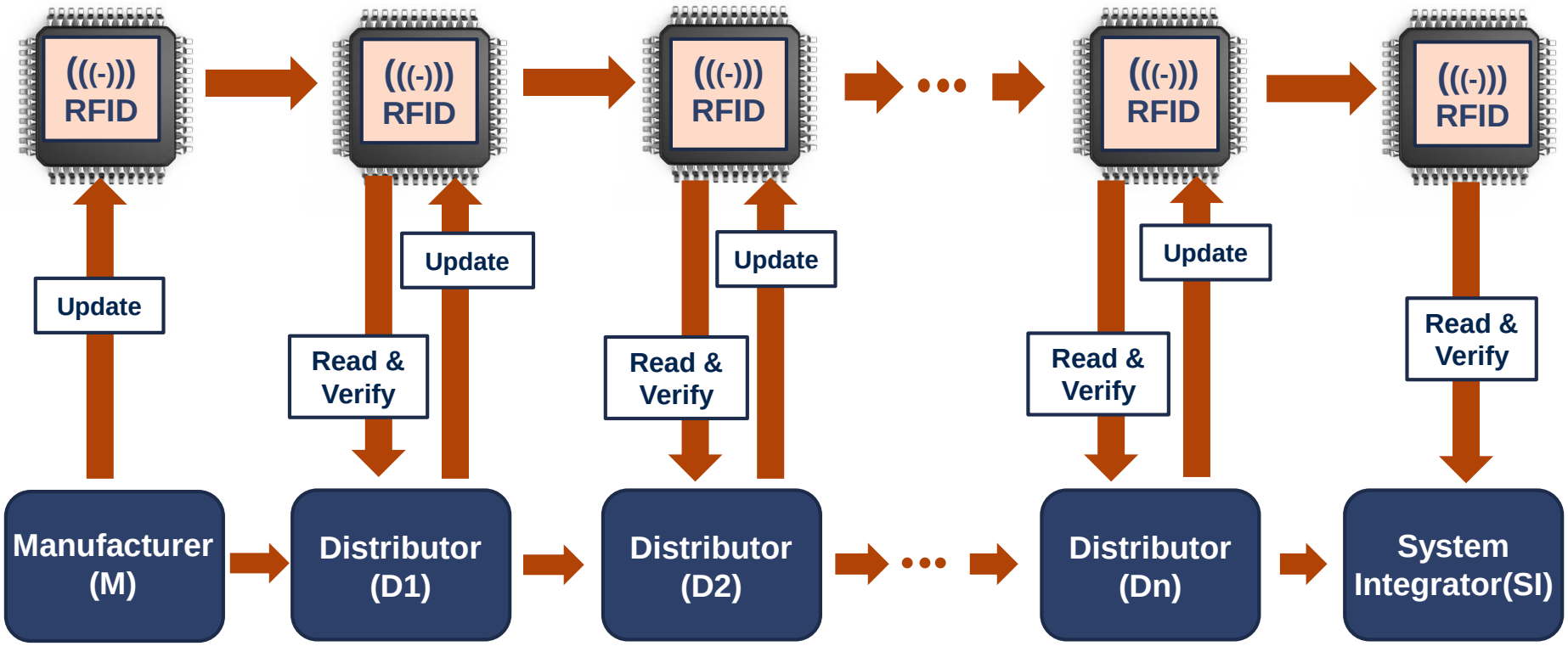
AUBURN UNIVERSITY

Semiconductor Supply Chain

- Authenticating a chip at a distributor's site is extremely challenging
  - Distributor may not have the necessary equipment to power up the chip.
  - Without powering up a chip prior authentication process is inapplicable.
- Potential solution
  - Integrate RFID in the chip package.
  - Provide authentication using RFID

AUBURN UNIVERSITY

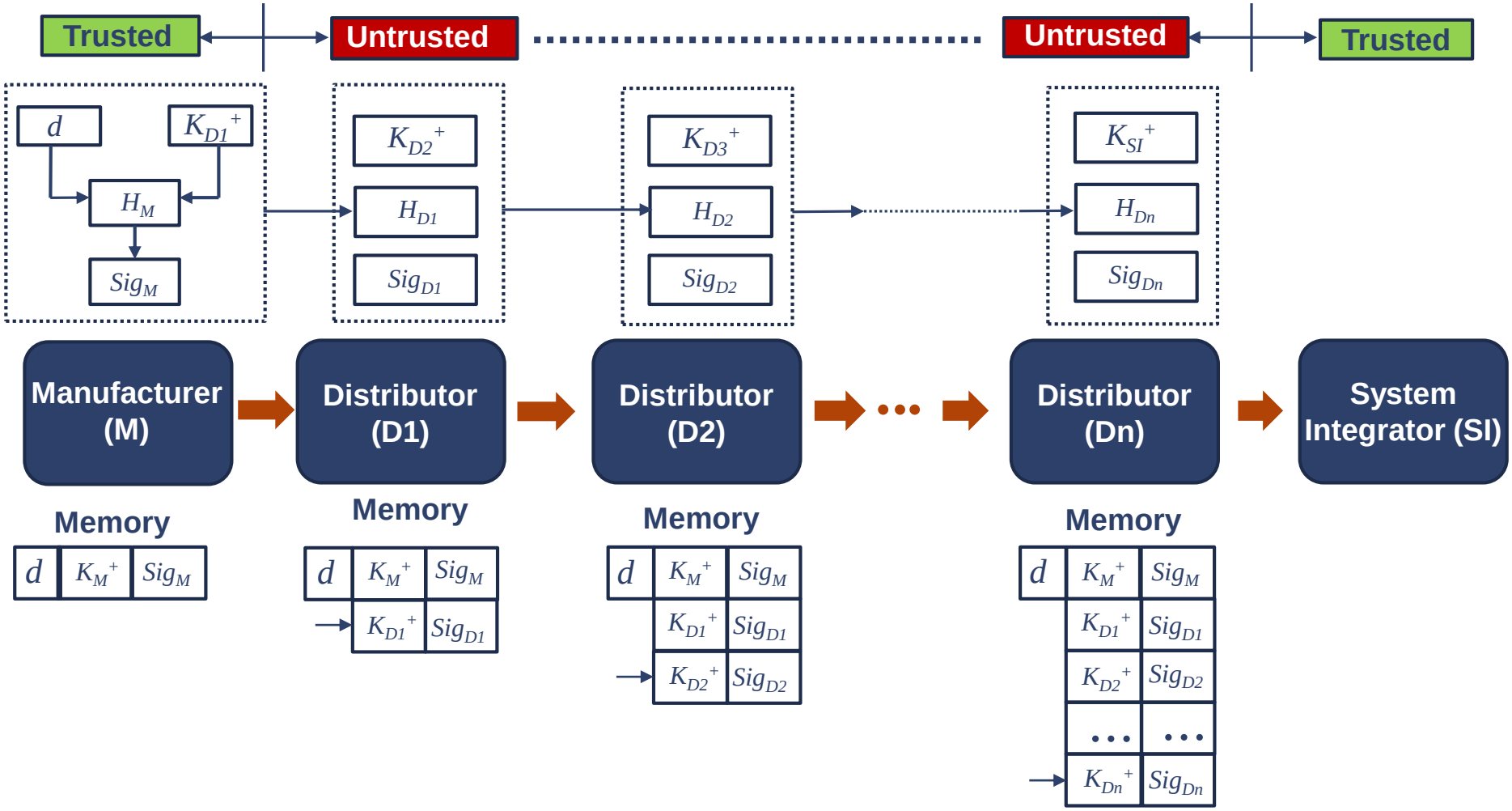
Proposed End-to-End Protection



- Read RFID Content
  - Extract the information in the tag with a reader.
- Verify RFID Content
  - Perform signature verification.
- Update RFID Content
  - Update its own signature.

AUBURN UNIVERSITY

Proposed End-to-End Protection- Cont.



AUBURN UNIVERSITY

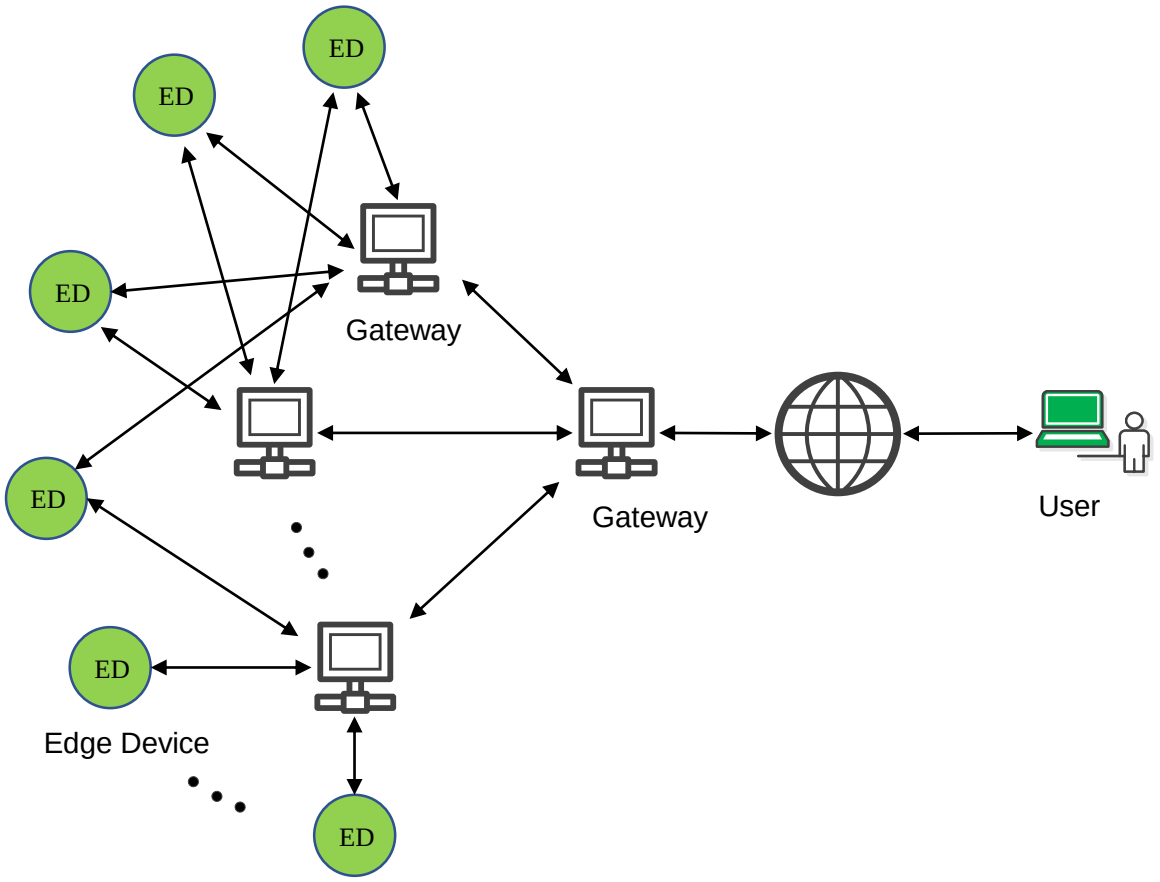
Outline

- Motivation
  - Counterfeiting and piracy
- Detection and avoidance of counterfeit ICs
  - Design-for-Anti-Counterfeit (DfAC) measures
  - Proposed on-chip aging structure
  - End-to-end protection
- Detection of counterfeit/cloned electronics
  - Use of Blockchain to enable device traceability
  - Firmware Obfuscation

AUBURN UNIVERSITY

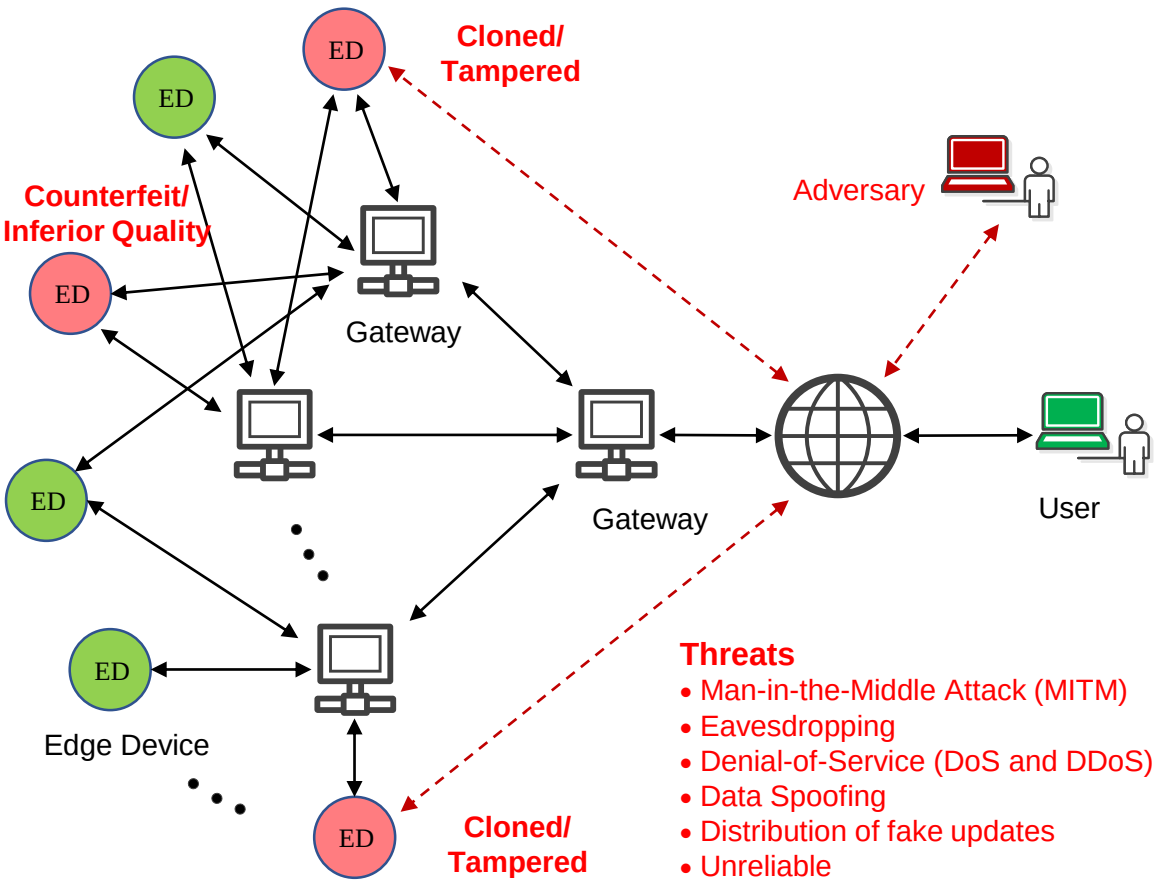
Motivation

- Rapid growth of IoT devices (20-50 billion by 2020)
- Ensuring security and authenticity is a challenge due to severe resource constraints
  - Low power requirements, low area budget, limited memory, and/or extremely low-cost.
  - Traditional cryptographic solutions become infeasible.
- Unsecure supply chain
  - Counterfeit, cloned and tampered devices.



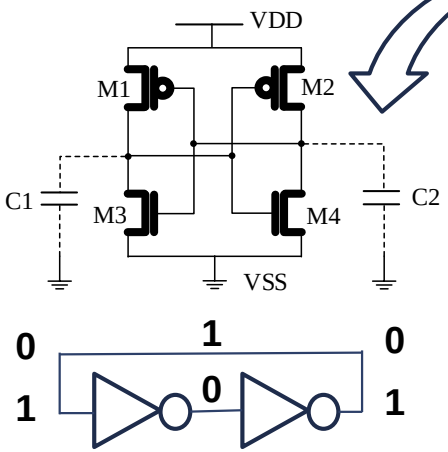
Motivation-Cont.

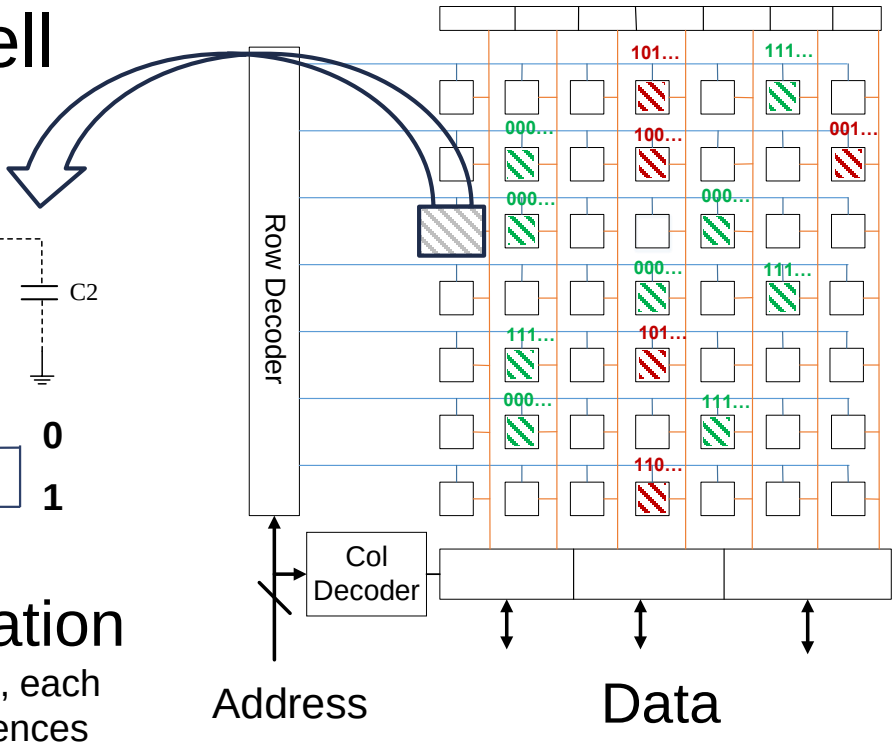
- Rapid growth of IoT devices (20-50 billion by 2020)
- Ensuring security and authenticity is a challenge due to severe resource constraints
  - Low power requirements, low area budget, limited memory, and/or extremely low-cost.
  - Traditional cryptographic solutions become infeasible.
- Unsecure supply chain
  - Counterfeit, cloned and tampered devices.



Physically Unclonable Functions (PUF)

SRAM Cell



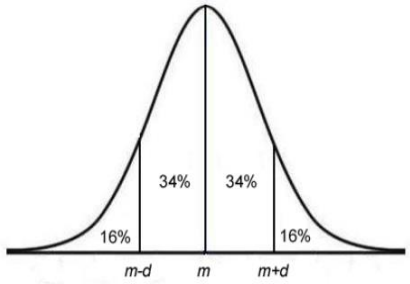


SRAM Array

When the SRAM is powered on, each SRAM cell will come up with 1 or 0 randomly across whole array. Some cells will consistently generate 1 or 0 during successive power-ons.

Process Variation

During chip fabrication, each MOS transistor experiences process variation and possesses unique electrical properties.



SRAM Power-up State

When the SRAM cell is powered up, the SRAM state will be 1 or 0 due to the process variation

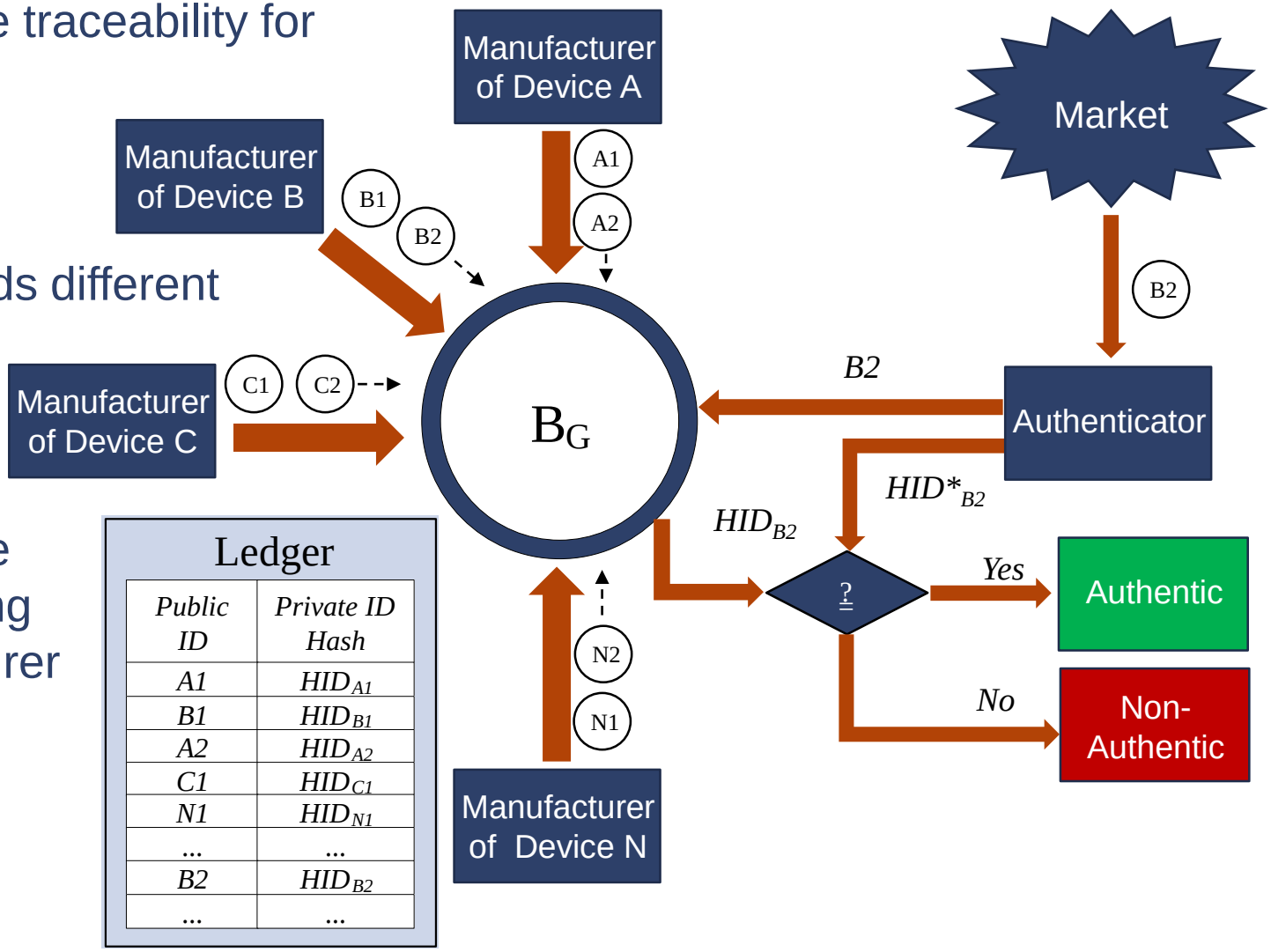
SRAM PUF ID

These stable will be the fingerprint (ID) of the device.

AUBURN UNIVERSITY

Global Identity Blockchain (B_G)

- Aims to provide traceability for edge device
- Across hundreds different manufacturers
- Verify a device without tracking the manufacturer

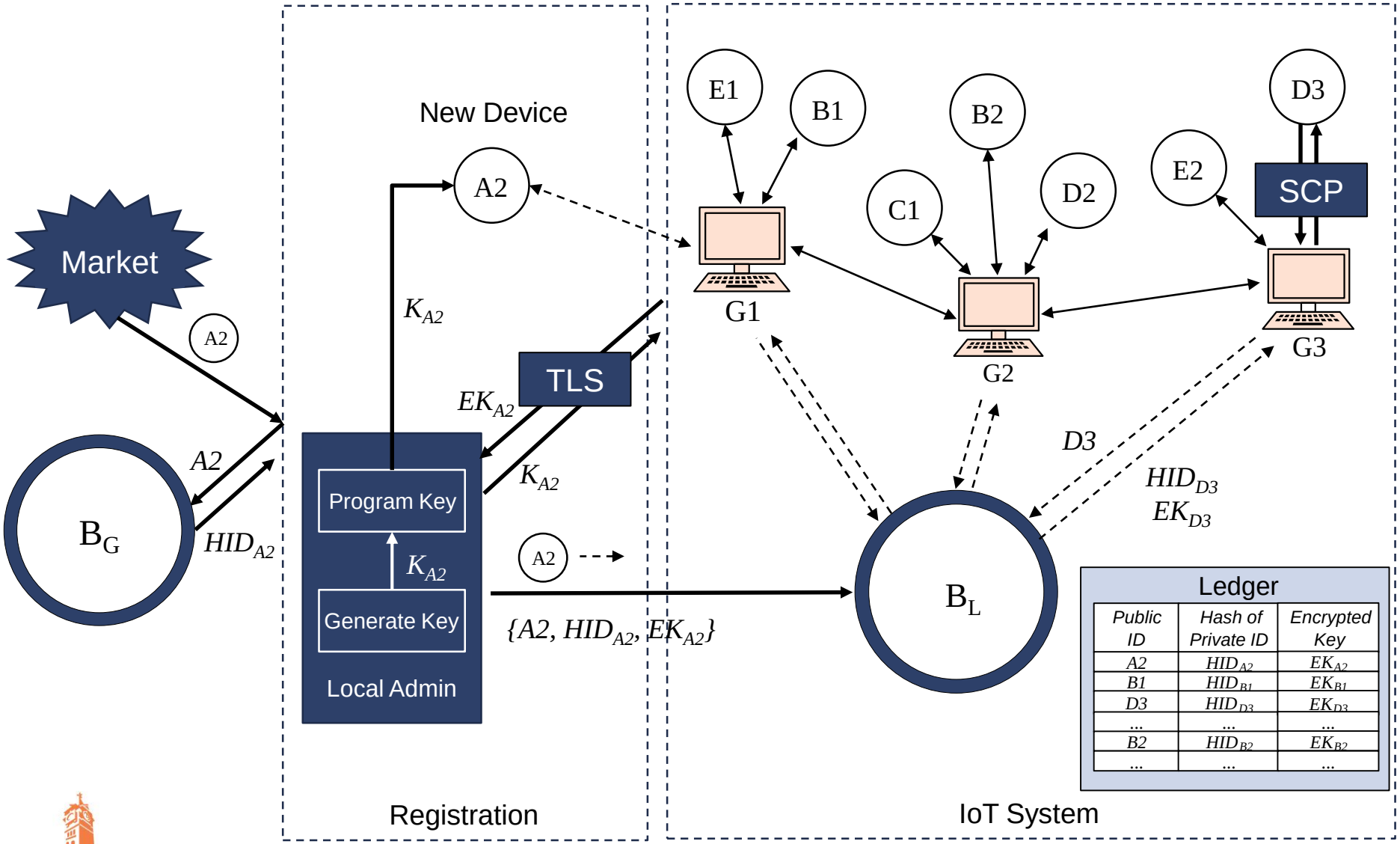


Local Identity Blockchain (B_L)

- Locally *permissioned* blockchain infrastructure
  - A local administrator can register an authentic edge device.
- IoT Devices can be authenticated periodically to prevent device cloning
  - A device could be compromised during lifespan
- A secret key is generated and burned into the on-chip, one-time programmable memory.
  - Once the key is programmed, direct access of device ID is prohibited to protect it from being copied.

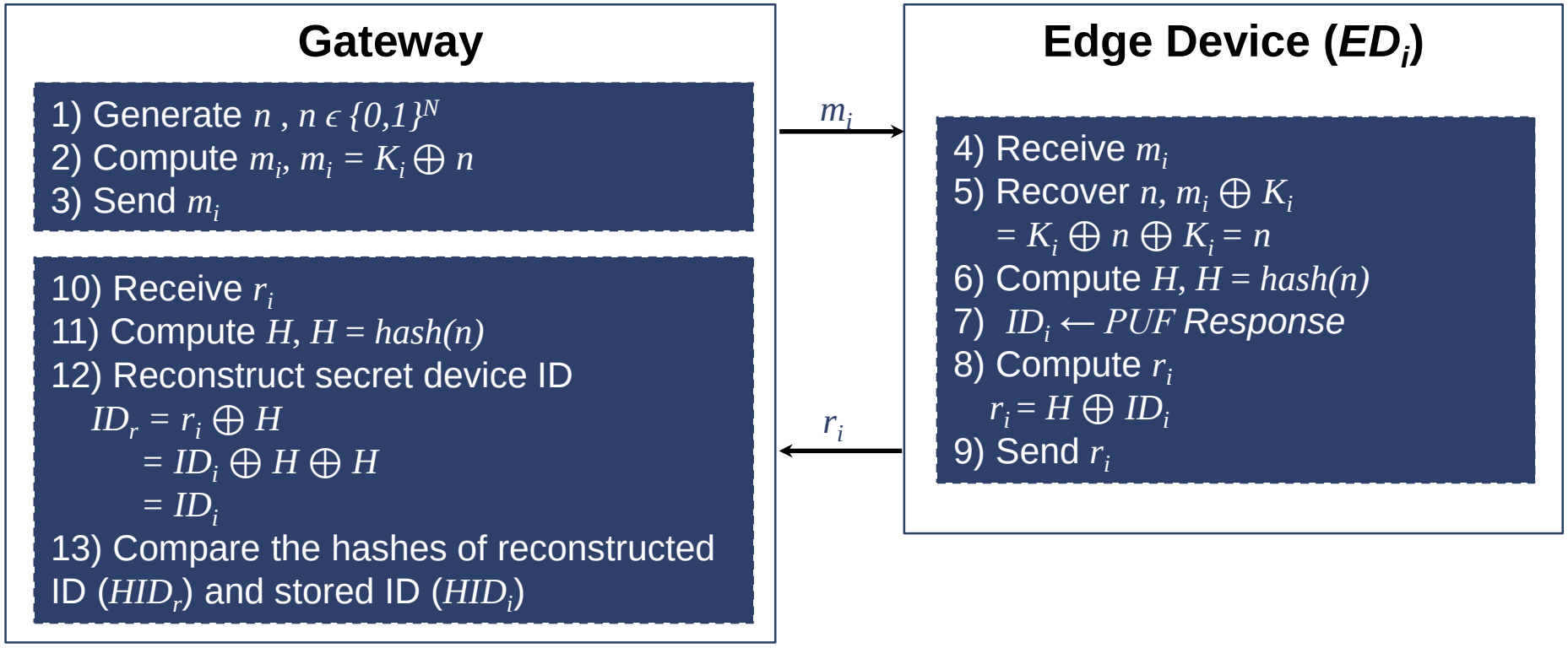
AUBURN UNIVERSITY

Local Identity Blockchain



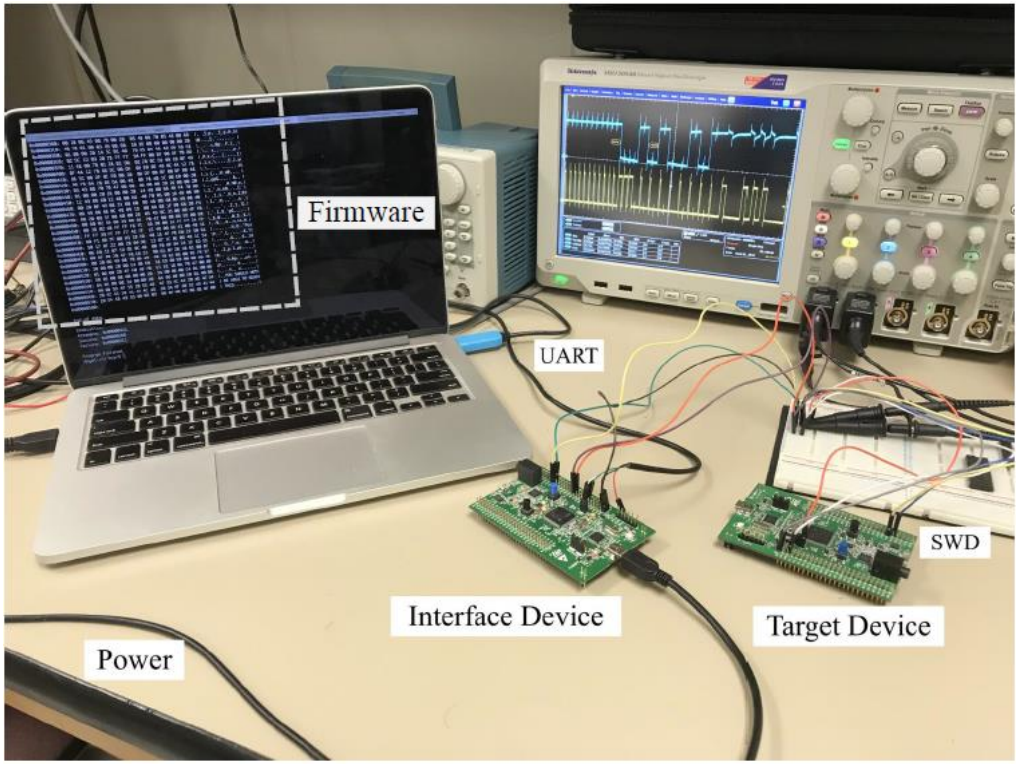
SCP: Secure Communication Protocol

- Securely transfer PUF ID to the gateway.
- Lightweight and can be implemented in the edge devices.



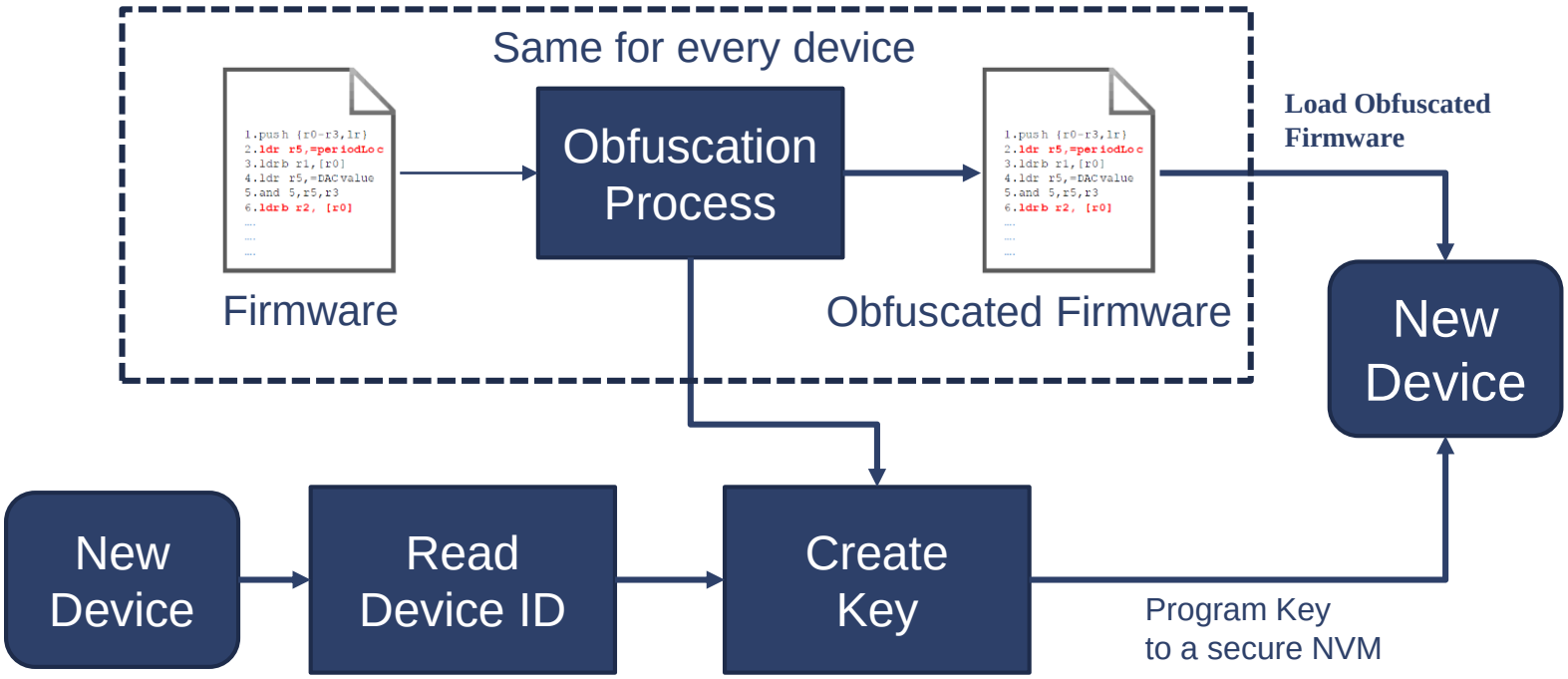
Firmware Obfuscation

- Microcontroller STM32F4 has two levels of memory protection to defend against firmware extraction
- Firmware integrity checking (e.g. CRC) during start-up can be used to bypass the level-I security.
- Even level-II security can be bypassed using UVC.
- Firmware can be copied, which makes cloning easy.

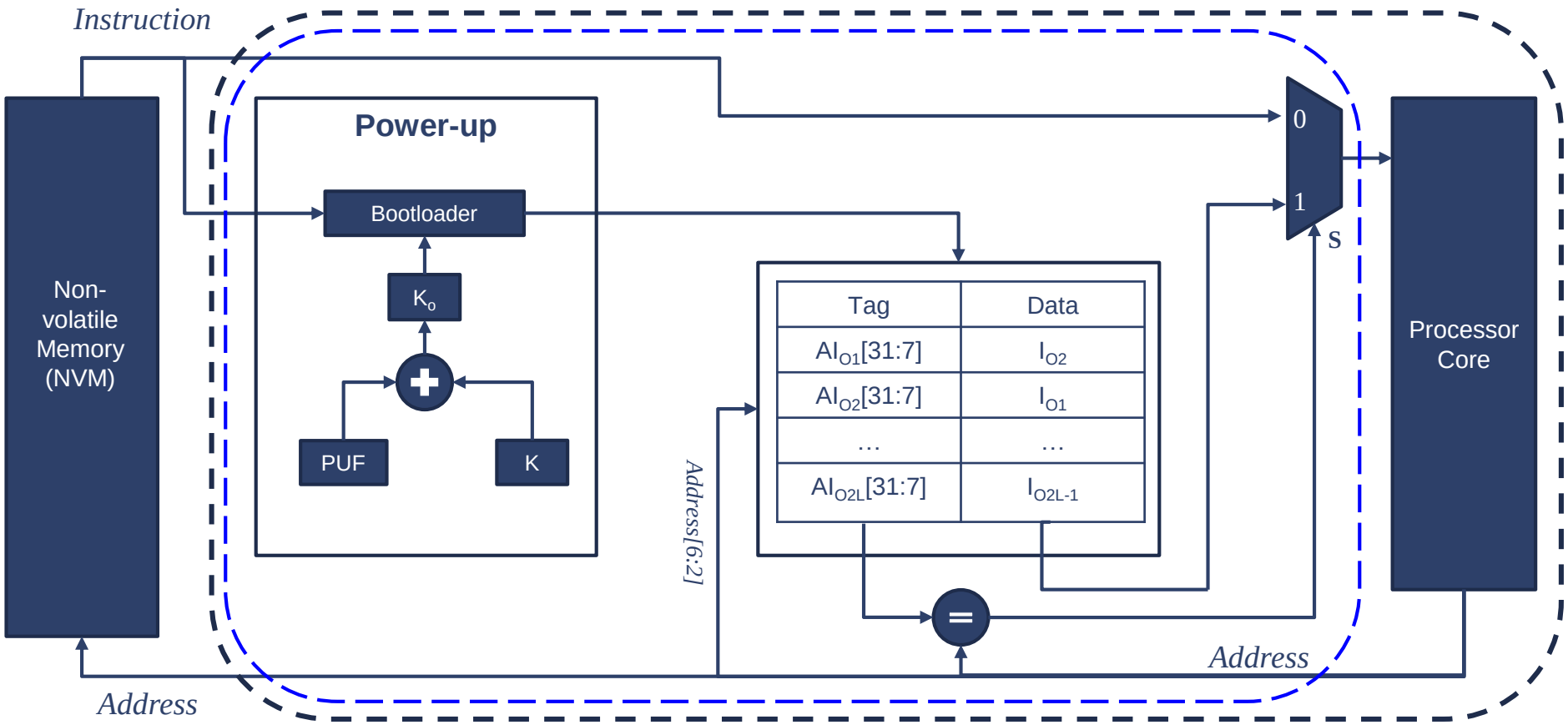


Experimental Setup to extract the firmware from STM32F4

Firmware obfuscation process



Firmware Reconstruction Process



Conclusion

- Counterfeiting and piracy
- Design-for-Anti-Counterfeit (DfAC) measures for detecting counterfeit ICs
  - On-chip aging structure
  - End-to-end protection for component supply chain
- Device authentication scheme using Blockchain technology to detect clones
  - Global Blockchain Infrastructure (B_G) for implementing Traceabilty of IoT edge devices
  - Local Blockchain (B_L) for edge device registration and authentication
  - SCP: Secure Communication Protocol for edge device authentication
- Firmware obfuscation to prevent cloning

AUBURN UNIVERSITY

Thank you!

Any Questions?

AUBURN UNIVERSITY