Hardware Security Conference Keynote Content

Prepared For: hardwear.io
Hardware Security Conference and Training

Cryptography Research at Rambus

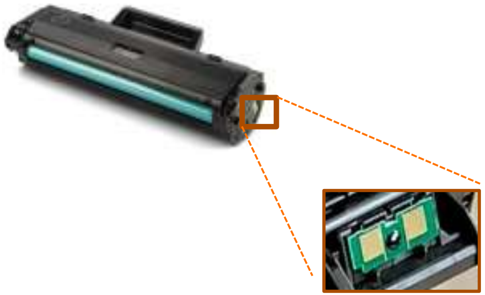
Presenter: Scott Best
31 May 2024

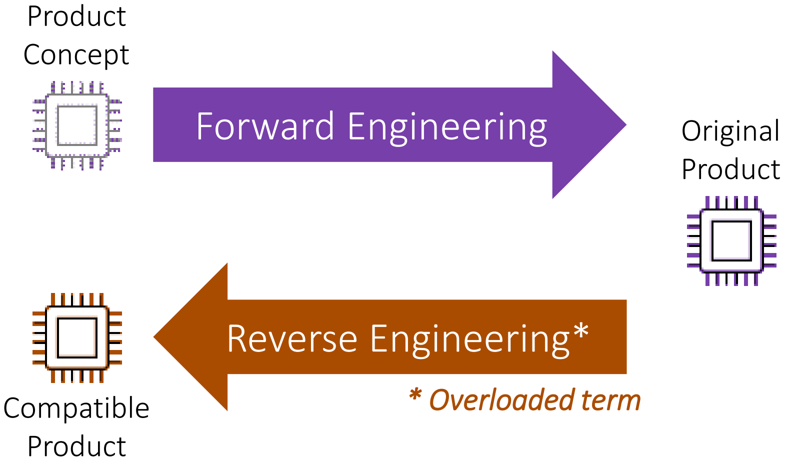
Introduction to Me

- Mixed-Signal Circuit Engineer
  - Most interesting thing I ever built: chaotic TRNG
  - sbest@cryptography.com
- Arrived in Silicon Vally in 1989
- Joined Rambus in 1998
  - PlayStation 3
  - Rambus Labs
  - Cryptography Research subsidiary
- Engineering -> Product Management
  - Anti-Counterfeiting
  - U.S. Defense

https://www.linkedin.com/in/scottcbest/

Today’s Talk: reverse-engineering vs. “forward-engineering”





Product Concept

Forward Engineering

Original Product

Reverse Engineering*

Compatible Product

** Overloaded term*

Motivations to prevent R.E.:

- Revenue
- Brand Protection
- Product Safety
- National Defense

~$30B market

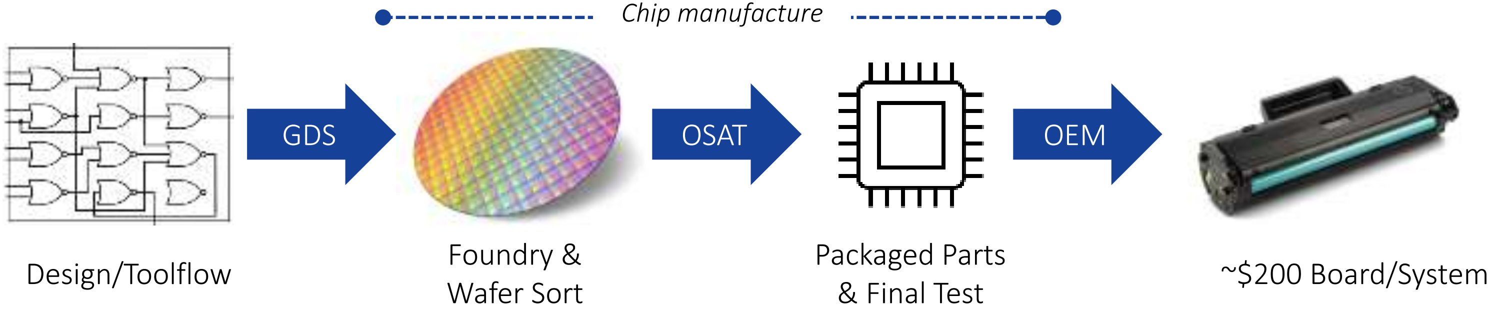
~$10B market

~$20B market

Motivations to succeed at R.E.:

- *LOTS* of Revenue
- ~~Brand Protection~~
- ~~Product Safety~~
- National Defense
- Design Recovery

Forward Talk: How Security Chips Are Built



Chip manufacture

GDS

OSAT

OEM

Design/Toolflow

Foundry &
Wafer Sort

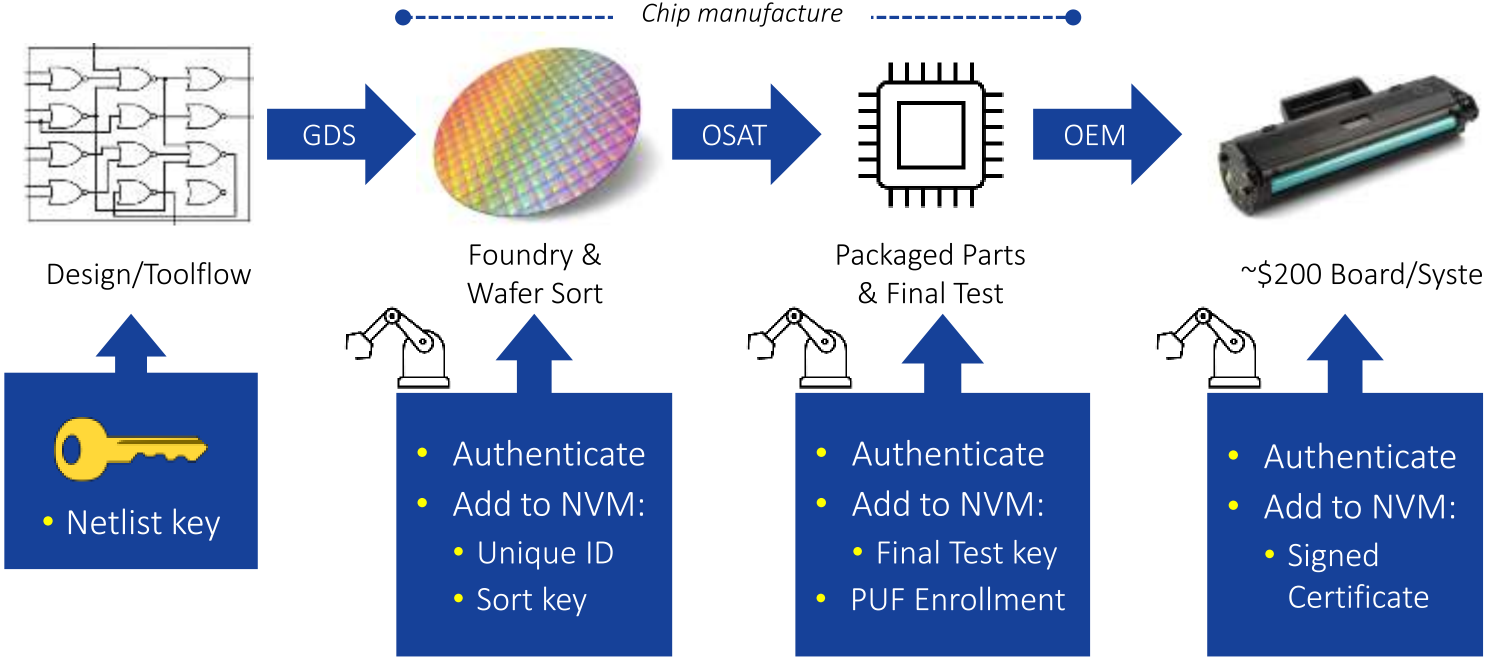
Packaged Parts
& Final Test

~$200 Board/System

- A 300mm wafer has about 70k mm2 of useable area
- A state-of-the-art authentication chip is about 2.5 mm2
- Each wafer: 28,000 die; each wafer lot: 25 wafers
- SAM value of one wafer lot: $140M

Reverse Talk: Don’t Overthink It … Start with “Basic Theft”

Forward Talk: Supply Chain Security is Essential



- Netlist key

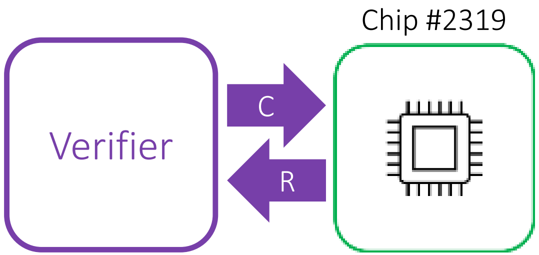
- Authenticate
- Add to NVM:
  - Unique ID
  - Sort key

- Authenticate
- Add to NVM:
  - Final Test key
- PUF Enrollment

- Authenticate
- Add to NVM:
  - Signed Certificate

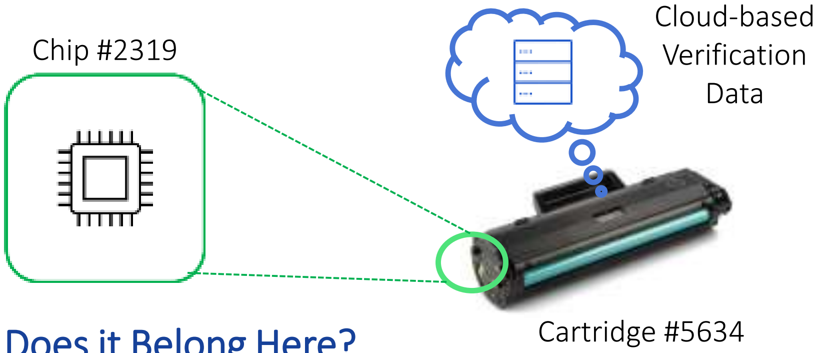
Reverse Talk: Next easiest: Recover Discards, Re-Manufacture Them

Forward Talk: Secure Provenance Defeats Remanufacture



1. Is this Chip Authentic?

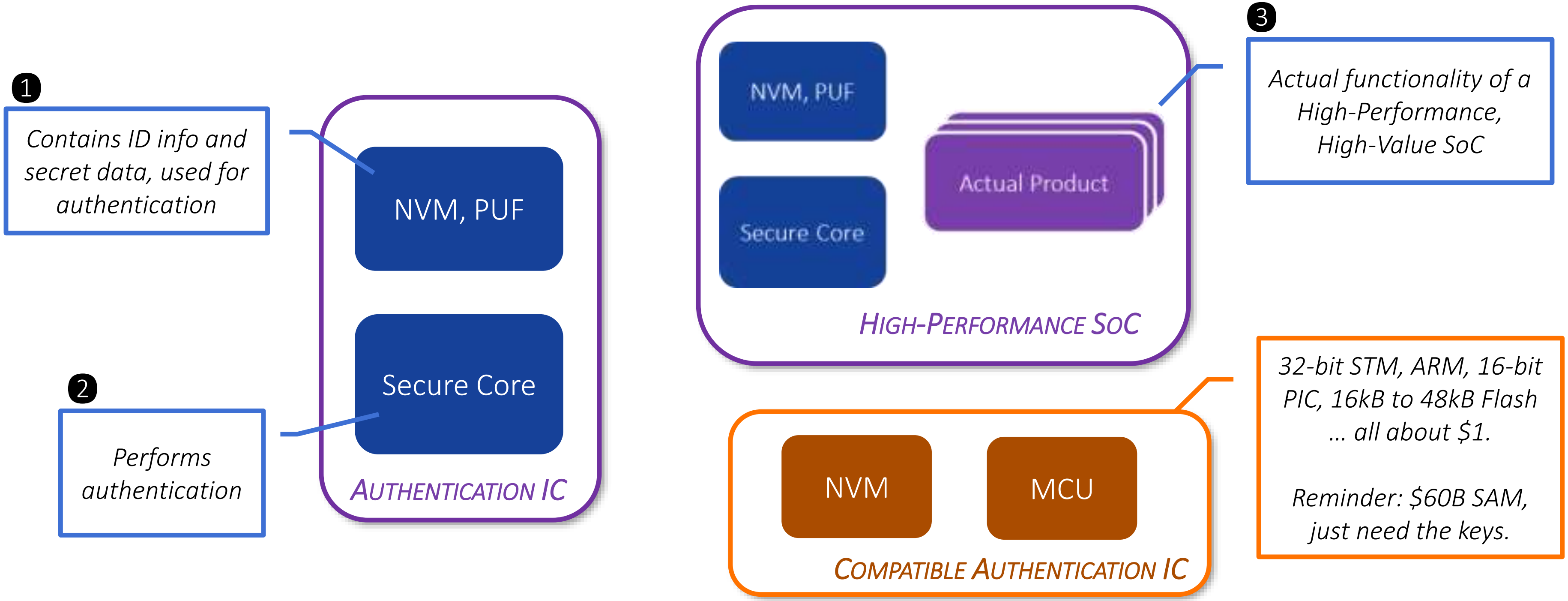
- Authenticity questions can be answered with a Verifier., e.g., an SoC on the same board, a chiplet in the same MCM, an HSM attached during manufacture, etc.
- A chip alone can't tell you if it's been stolen or remanufactured (potentially after malicious modification)



2. Does it Belong Here?

- The "Provenance" of a chip can be tracked by the same secure manufacturing system that provisioned the key material
- If that provenance info is available to the verifier (e.g., secure cloud), stolen or remanufactured chips can be detected
- *Difficult at large commercial scale*

Forward Talk: Backing up … How to Secure Authentic Chips?



1 *Contains ID info and secret data, used for authentication*

2 *Performs authentication*

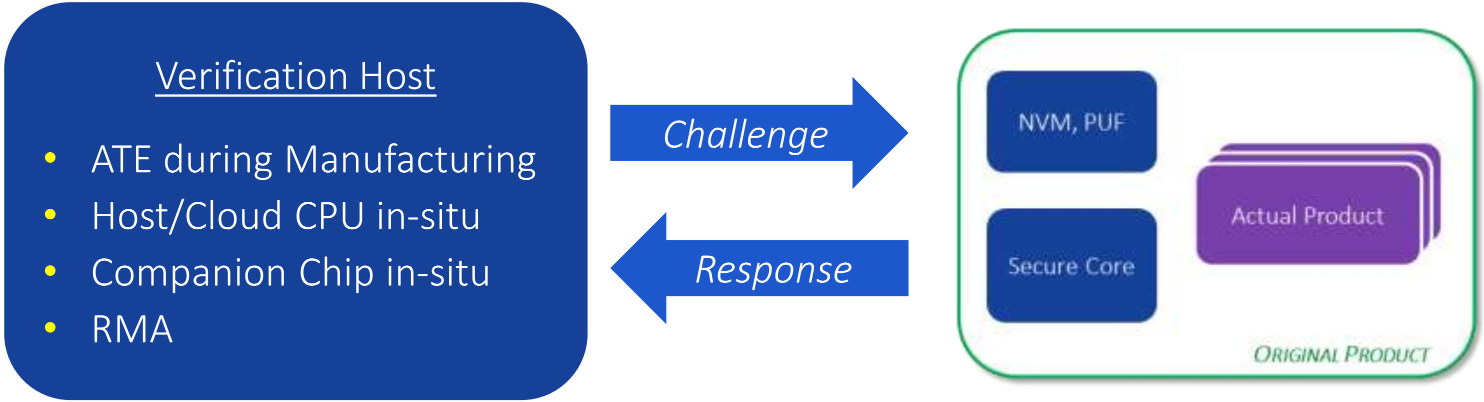
3 *Actual functionality of a High-Performance, High-Value SoC*

32-bit STM, ARM, 16-bit PIC, 16kB to 48kB Flash … all about $1.

Reminder: $60B SAM, just need the keys.

Reverse Talk: How to Obtain Key Material for a Clone or Compatible?

Forward Talk: Practical Magic to Protect Authentication

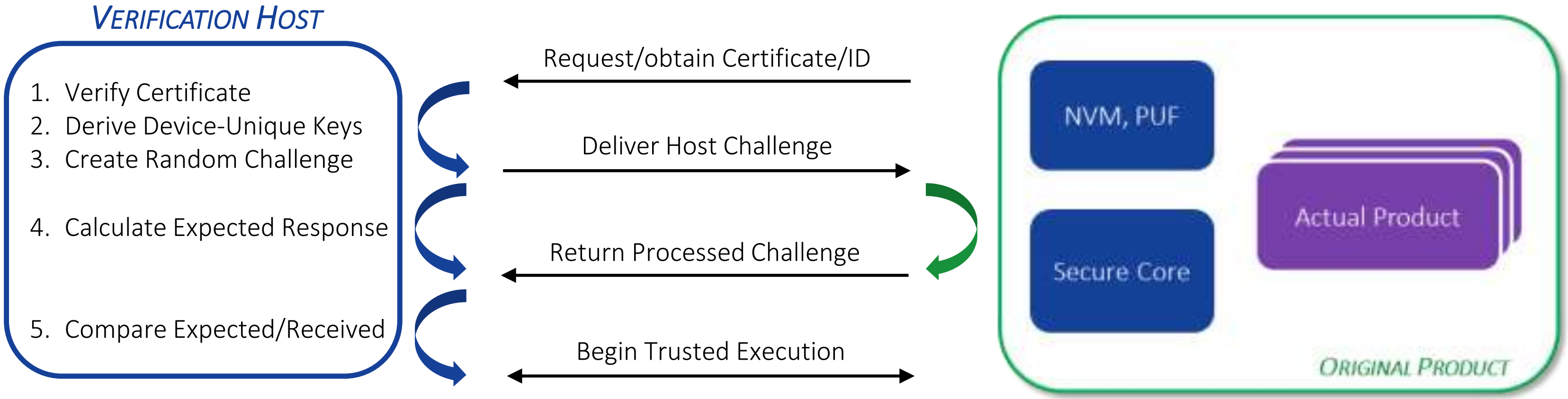


Verification Host

- ATE during Manufacturing
- Host/Cloud CPU in-situ
- Companion Chip in-situ
- RMA

Reverse Talk: Authentication has Many Attack Surfaces

Forward Talk: Authentication Basics



Verification Host

1. Verify Certificate
2. Derive Device-Unique Keys
3. Create Random Challenge
4. Calculate Expected Response
5. Compare Expected/Received

Request/obtain Certificate/ID

Deliver Host Challenge

Return Processed Challenge

Begin Trusted Execution

NVM, PUF

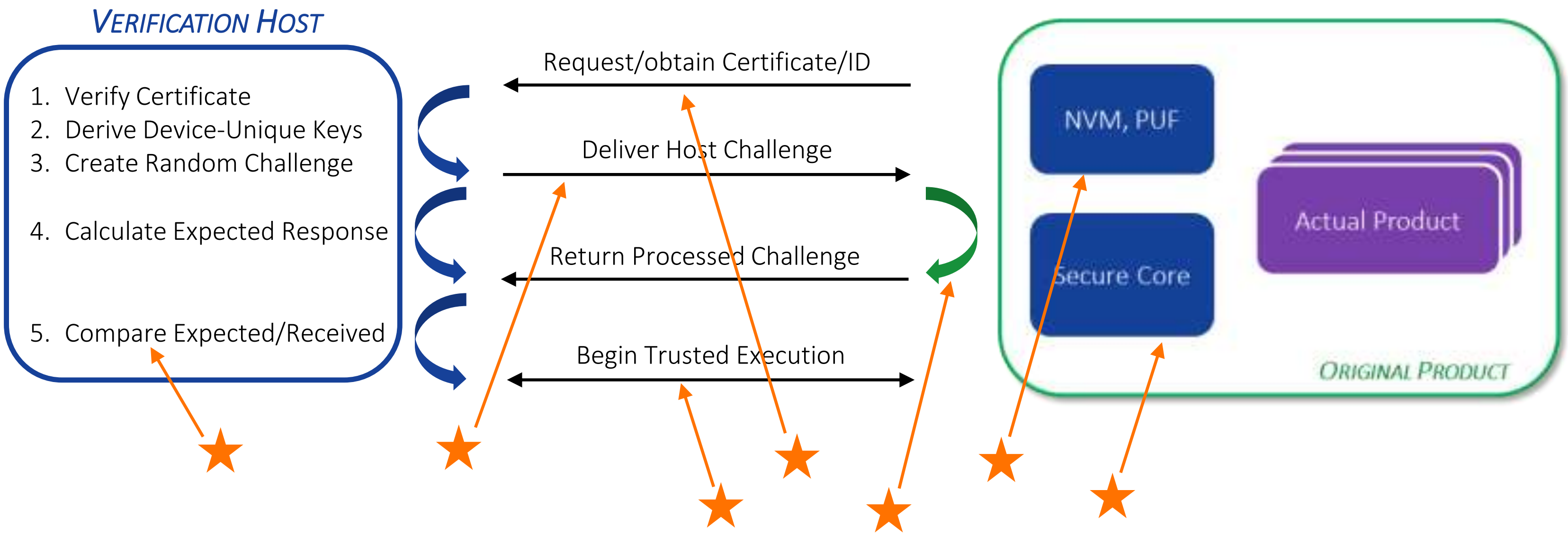
Secure Core

Actual Product

Original Product

Reverse Talk: Choose Attack Surface optimized for Time/Money

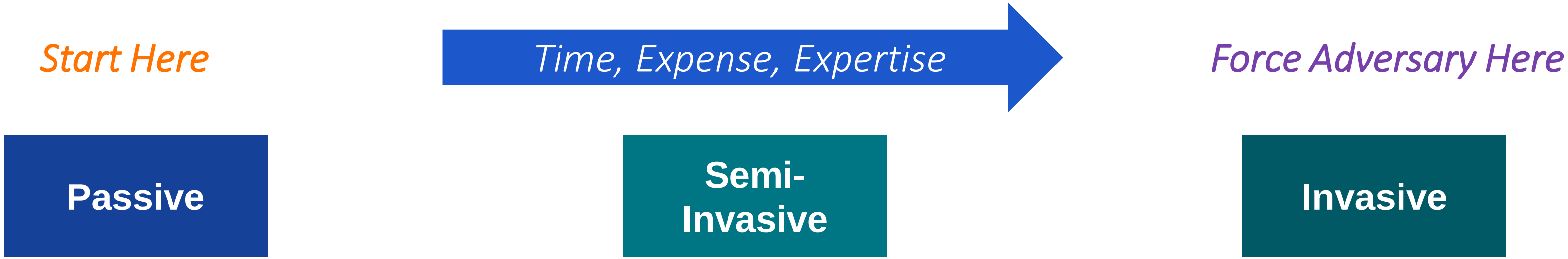
Forward Talk: Authentication Basics



VERIFICATION HOST
1. Verify Certificate
2. Derive Device-Unique Keys
3. Create Random Challenge
4. Calculate Expected Response
5. Compare Expected/Received
Request/obtain Certificate/ID
Deliver Host Challenge
Return Processed Challenge
Begin Trusted Execution
NVM, PUF
Secure Core
Actual Product
ORIGINAL PRODUCT

Reverse Talk: Choose Attack Surface optimized for Time/Money

Forward Talk: Attack Surfaces to Worry About



Start Here

Time, Expense, Expertise

Force Adversary Here

Passive

- Insider attack (e.g. buy the keys)
- De-compiling firmware
- C/R Protocol fuzzing
- Replay, MitM attacks
- Cryptanalysis, key search
- Power-analysis side channel

Semi-Invasive

- Environmental/Timing attacks
- Fault injection via glitching
- Fault injection via laser probing
- Key/code injection
- Scan interface attacks

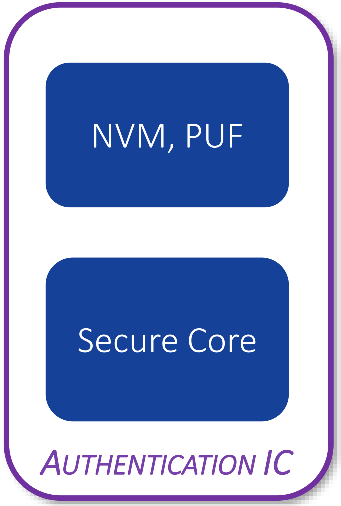
Invasive

- Optical side-channel
- Electrical probing
- Non-volatile memory ("NVM") key extraction
- Reverse-engineering (delayering and die imaging)
- Die-modification via focused ion-beam ("FIB")

Reverse Talk: Attack Surfaces to Embrace and Deploy

Forward Talk: Technologies I choose to Not Talk About Today…

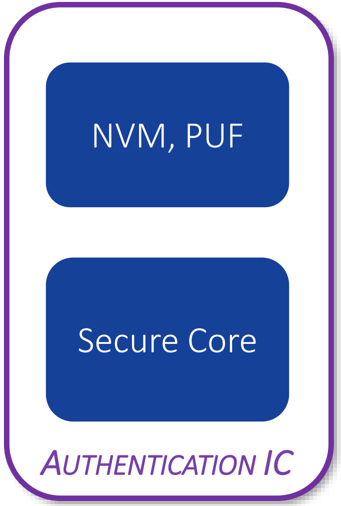
1. DRAM (e.g., RowHammer)
2. Hardware Trojans
3. Laser-Voltage Probing (LVP)
4. Anti-tamper Sensors
5. Camouflage Logic
6. Logic Locking



Reverse Talk: Many "Countermeasures" Assume Unmotivated Attackers

Forward Talk: Technologies To Talk About

1. Verifiable Provenance ✓
2. Power-Analysis Side-Channel
3. Mutual Authentication
4. Proof-of-Work 2FA
5. Protected NVM
6. Weak PUFs
   - When used correctly
7. Strong PUFs
   - Tamper-evidence



NVM, PUF

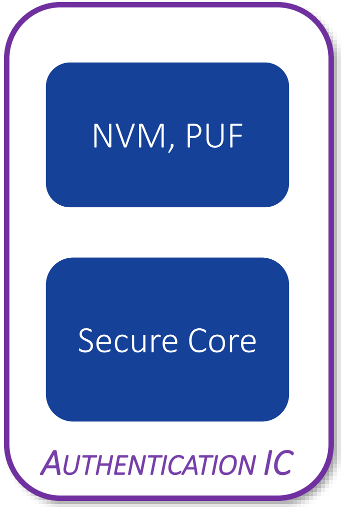
Secure Core

AUTHENTICATION IC

Reverse Talk: Attack Surfaces Exist in the Gaps

Forward Talk: State-of-the-Art Practical Magic

1. Verifiable Provenance ✓
2. Power-Analysis Side-Channel
3. Mutual Authentication
4. Proof-of-Work 2FA
5. Protected NVM
6. Weak PUFs
   - When used correctly
7. Strong PUFs
   - Tamper-evidence

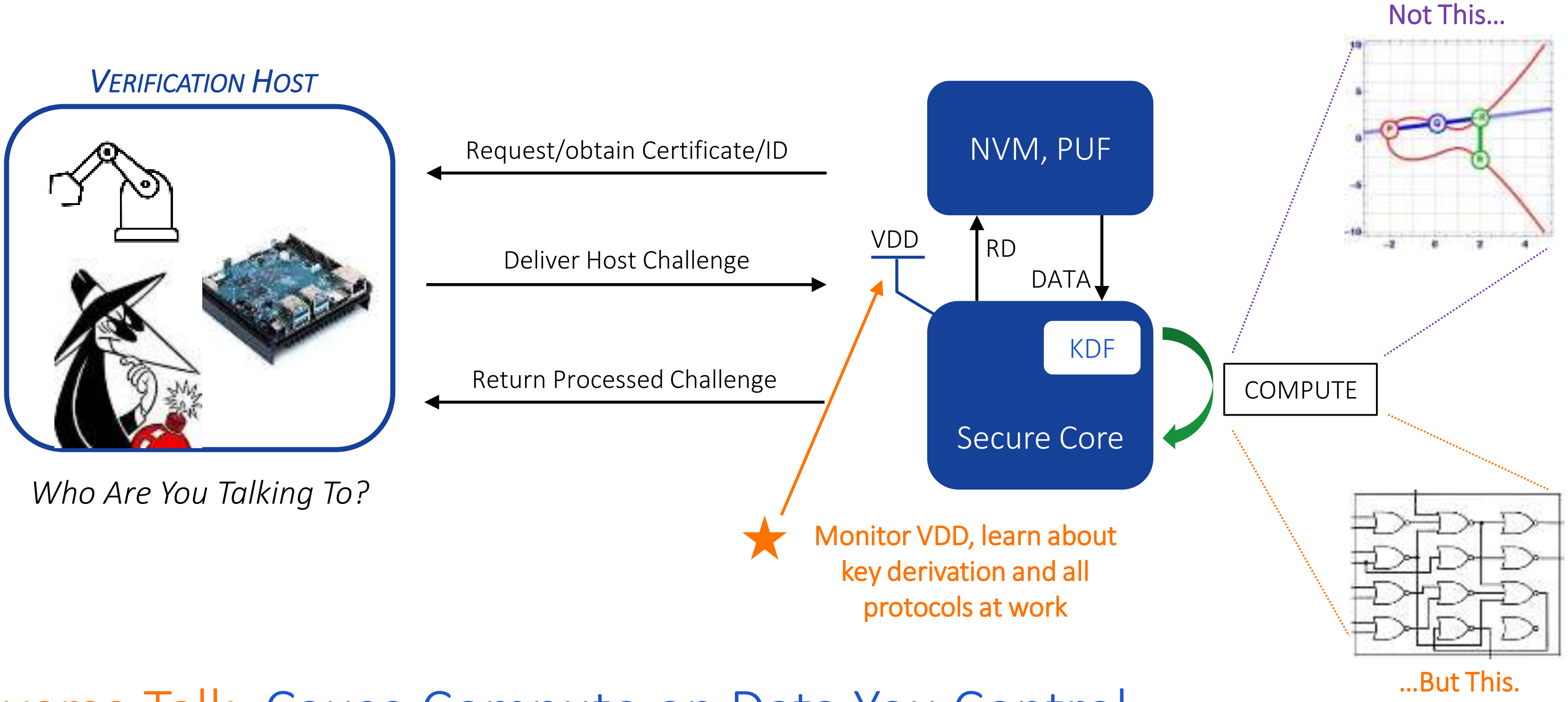


Keep in Mind the Goals:

- Cannot prevent R.E. in general, can only prevent rapid, easily affordable R.E.
- Force your opponent to a **full netlist recovery** with lots of FIBs and **manual electrical measurements**
- Force your opponent to **produce custom silicon**, more than an easily programmed MCU

Reverse Talk: Attack Surfaces Exist in the Gaps

Forward Talk: Power-Analysis Side Channel

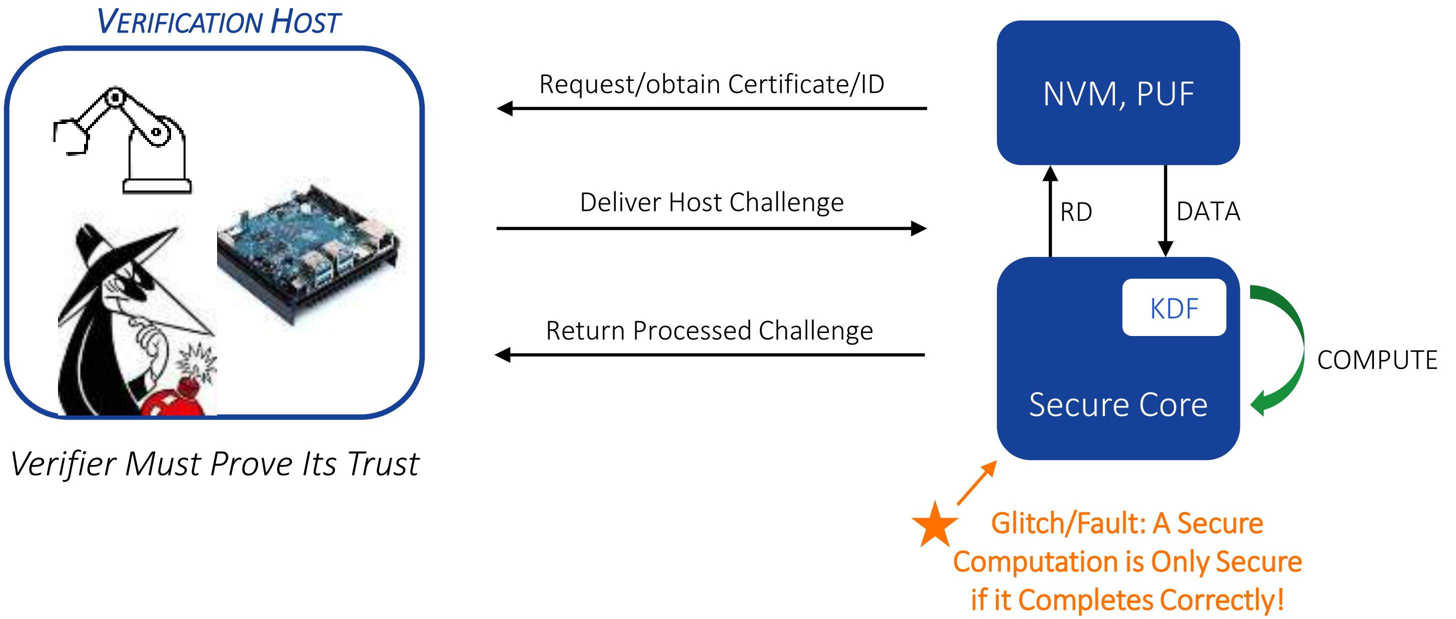


Who Are You Talking To?

Monitor VDD, learn about key derivation and all protocols at work

Reverse Talk: Cause Compute on Data You Control

Forward Talk: Mutual Authentication



VERIFICATION HOST

Request/obtain Certificate/ID

Deliver Host Challenge

Return Processed Challenge

NVM, PUF

RD

DATA

KDF

Secure Core

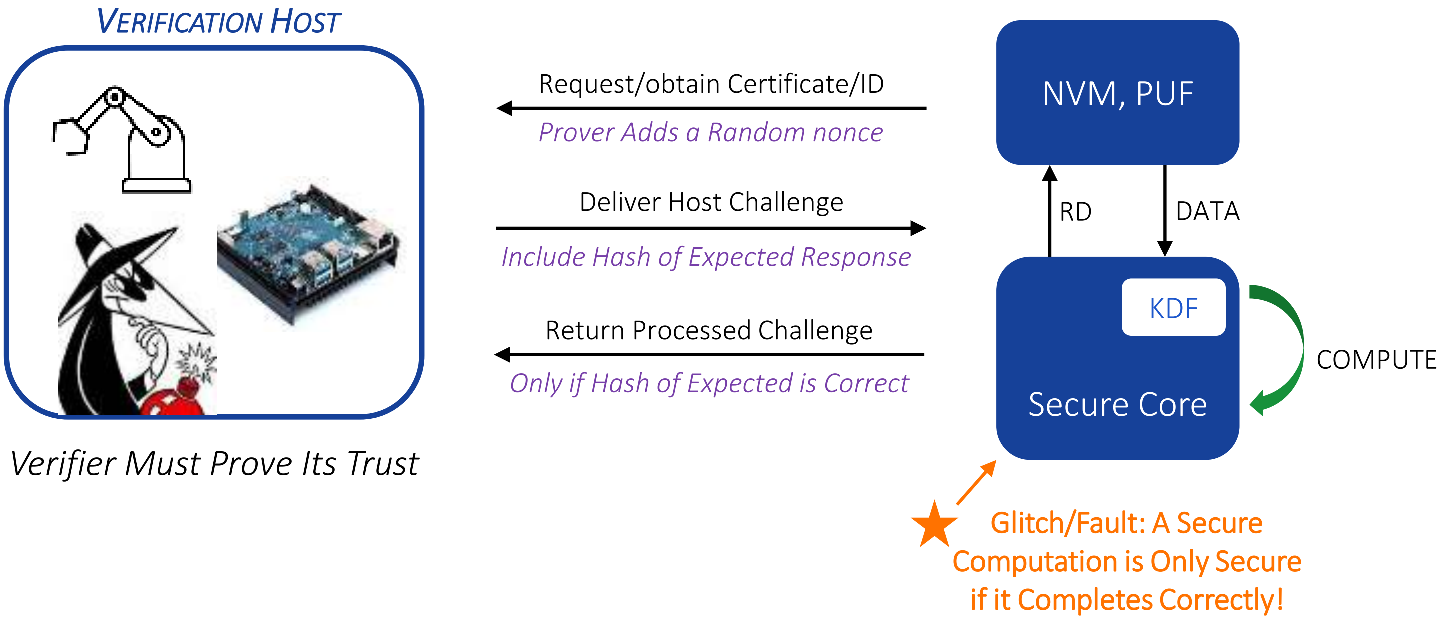
COMPUTE

Verifier Must Prove Its Trust

Glitch/Fault: A Secure Computation is Only Secure if it Completes Correctly!

Reverse Talk: Cause compute / Harvest Responses to Your Data

Forward Talk: Mutual Authentication



VERIFICATION HOST

Verifier Must Prove Its Trust

Request/obtain Certificate/ID

Prover Adds a Random nonce

Deliver Host Challenge

Include Hash of Expected Response

Return Processed Challenge

Only if Hash of Expected is Correct

NVM, PUF

RD

DATA

KDF

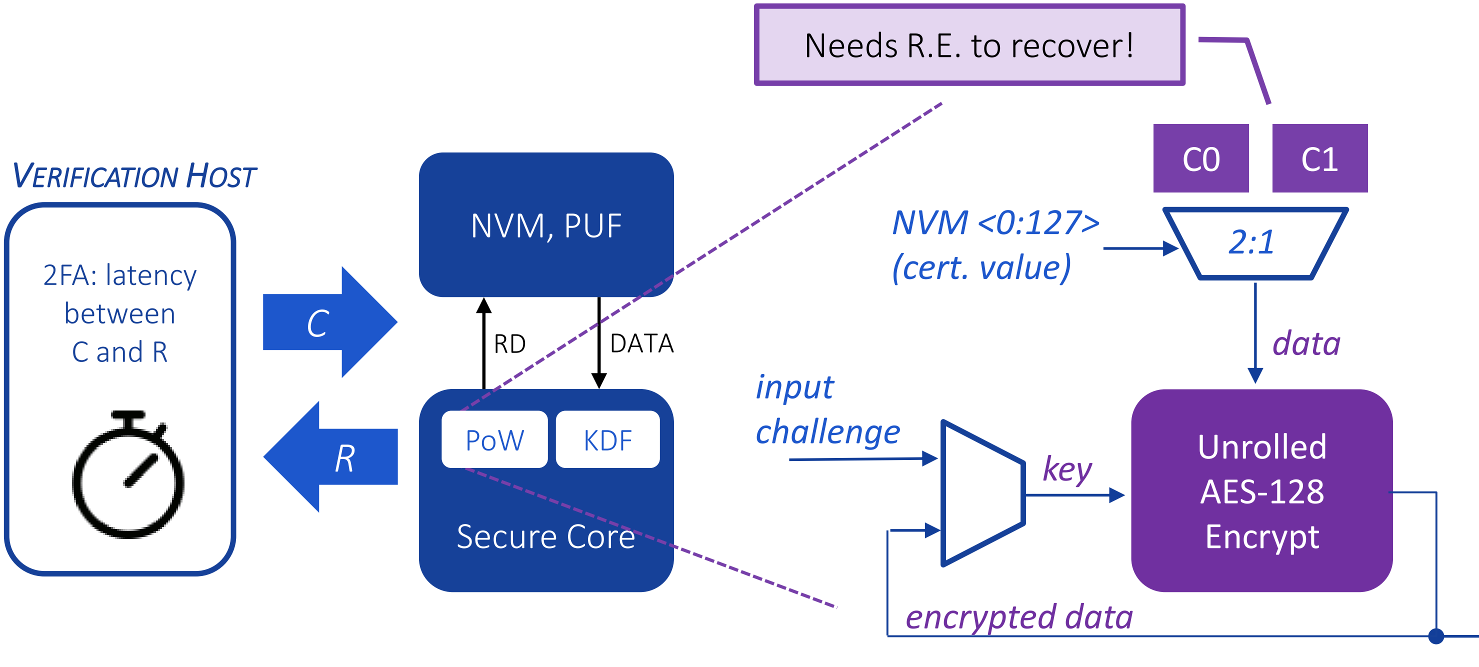
Secure Core

COMPUTE

Glitch/Fault: A Secure Computation is Only Secure if it Completes Correctly!

Reverse Talk: Cause compute / Harvest Responses to Your Data

Forward Talk: Proof of Work Can Force Custom Silicon

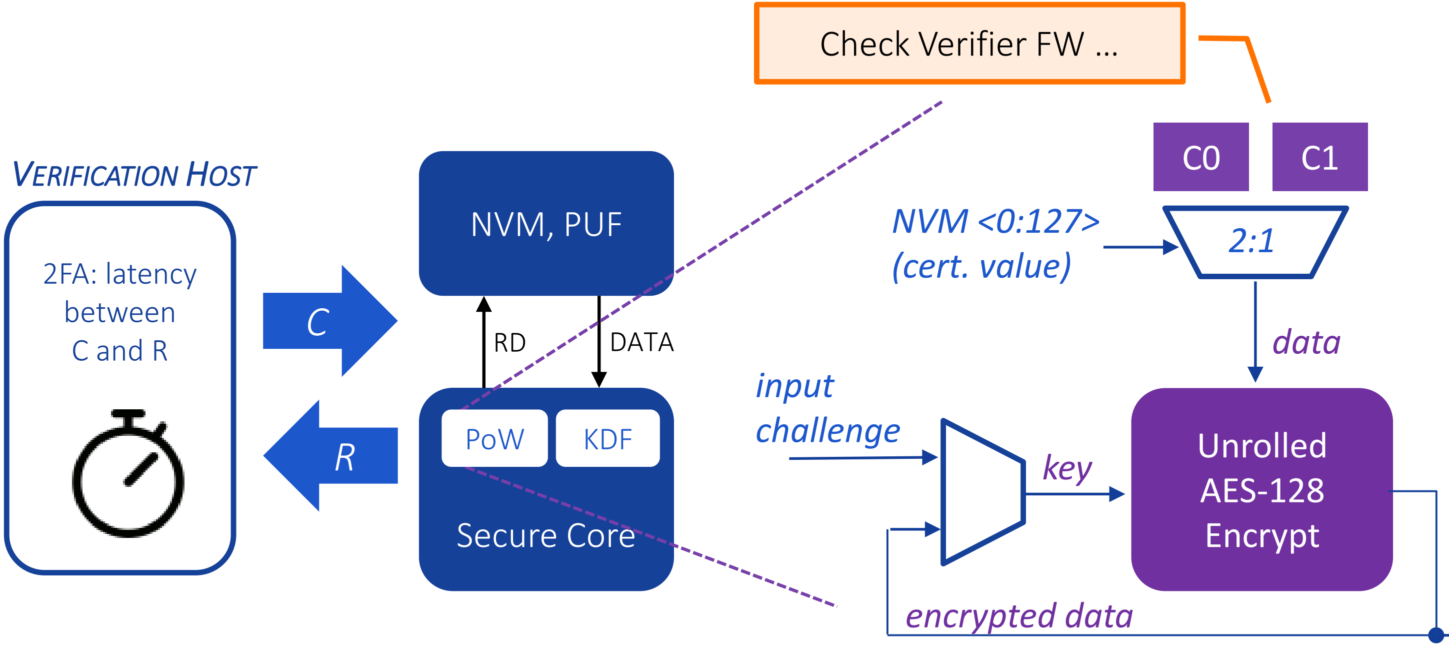


Work Effort:

- 128 AES encryptions
- 10 rounds per encrypt
- 32 SBOXs per round
- 32-SBOX core: 41k cycles
- 320-SBOX core: 1.28k cycles

Reverse Talk: Adjust Clocking if Measured-Timing Matters

Forward Talk: Proof of Work Can Force Custom Silicon

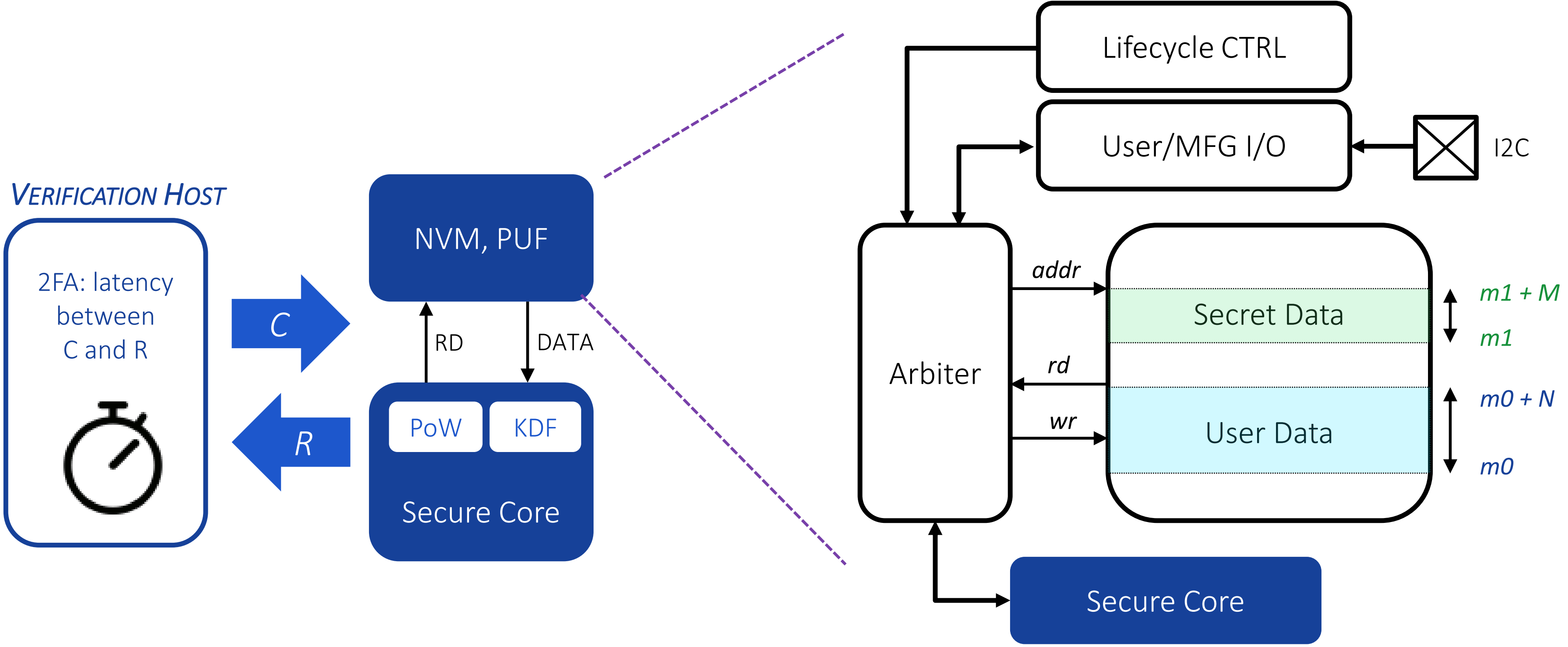


Work Effort:

- 128 AES encryptions
- 10 rounds per encrypt
- 32 SBOXs per round
- 32-SBOX core: 41k cycles
- 320-SBOX core: 1.28k cycles

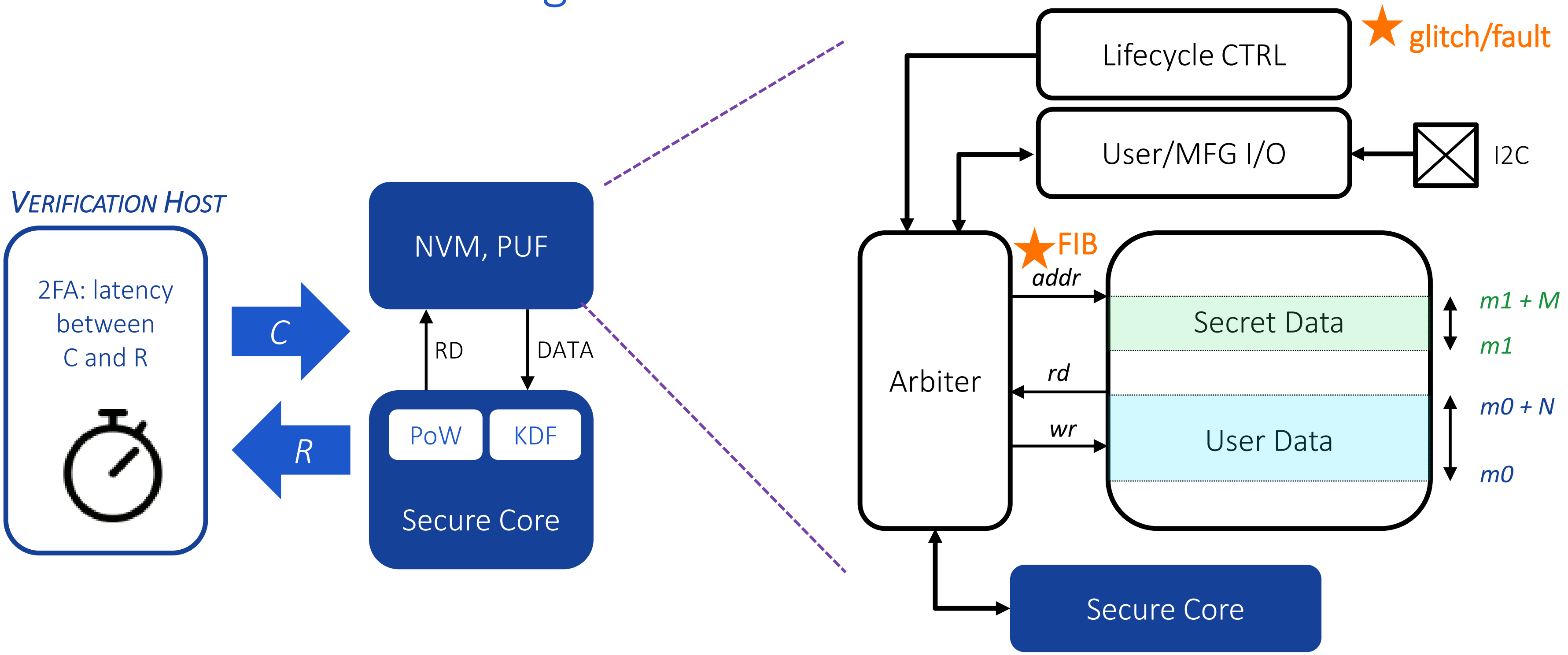
Reverse Talk: Adjust Clocking if Measured-Timing Matters

Forward Talk: Protecting NVM



Reverse Talk: NVM has Numerous Attack Surfaces

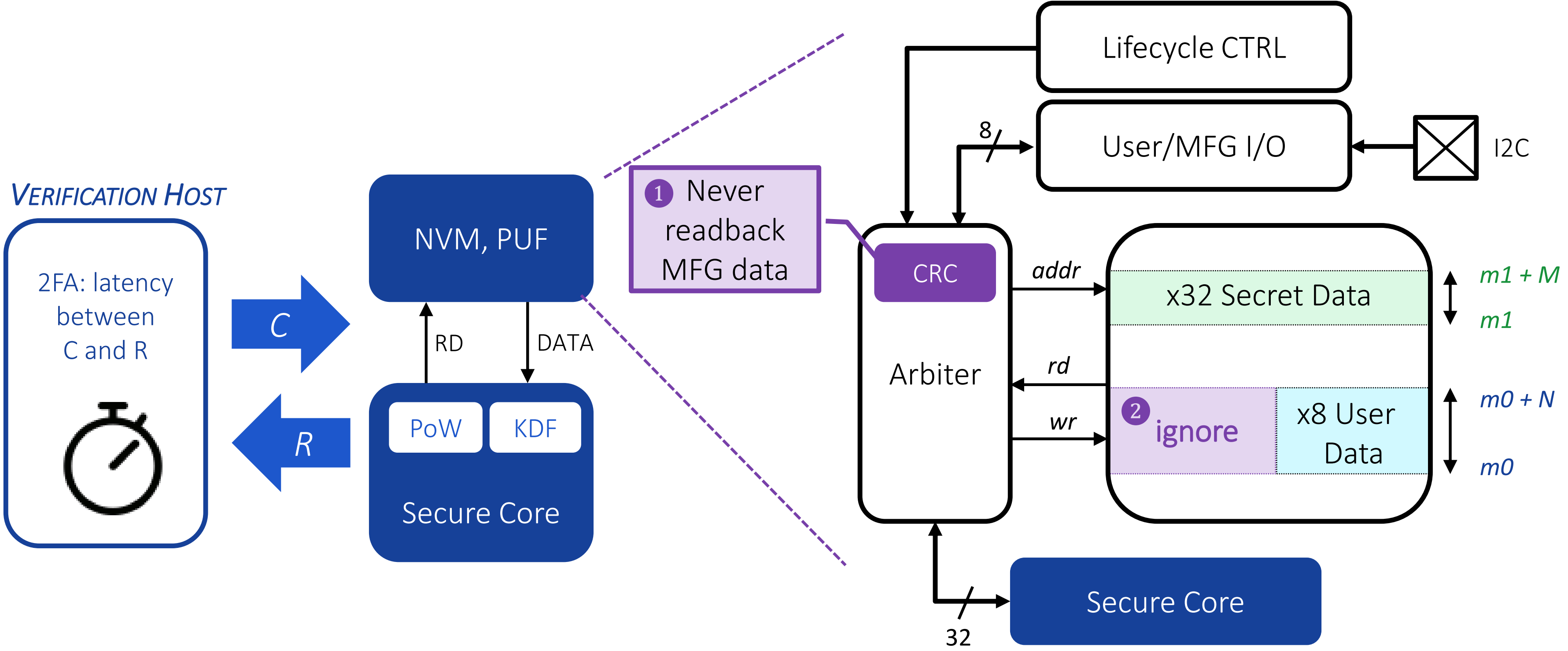
Forward Talk: Protecting NVM



Reverse Talk: NVM has Numerous Attack Surfaces

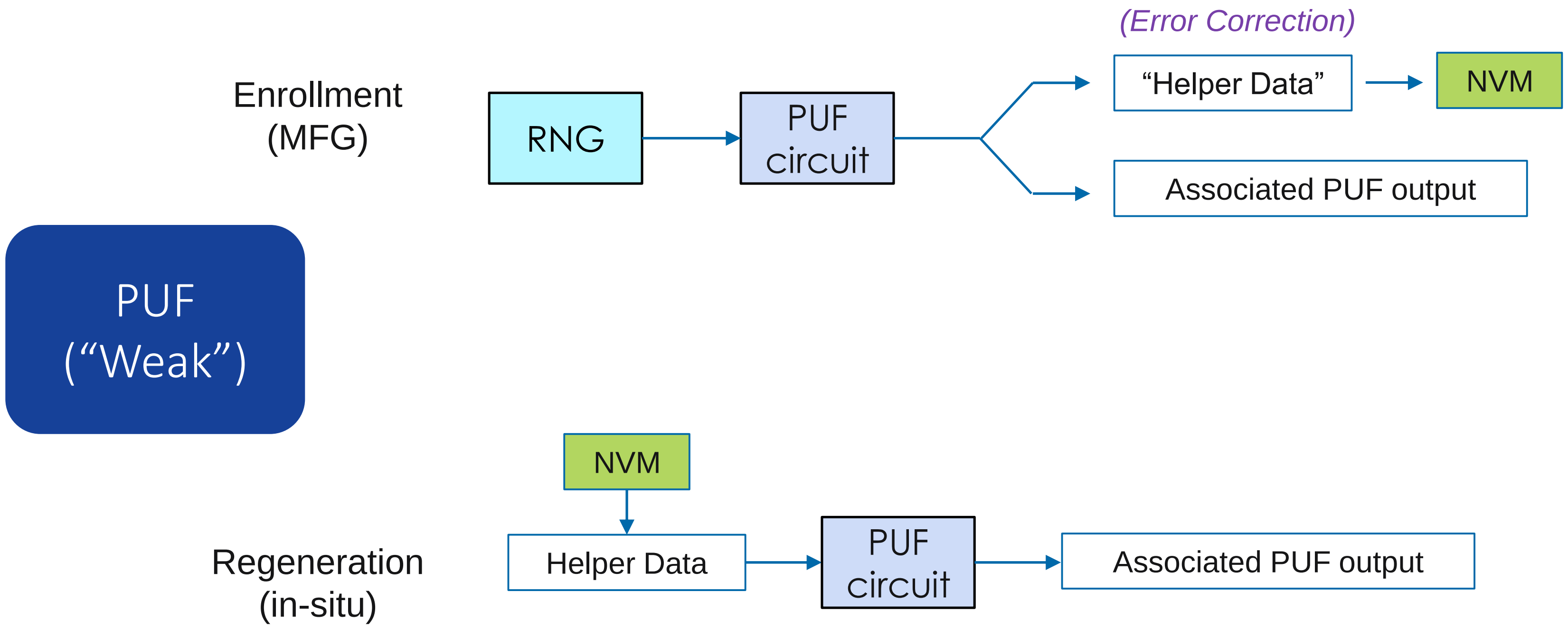
Proprietary and Unclassified

Forward Talk: Protecting NVM



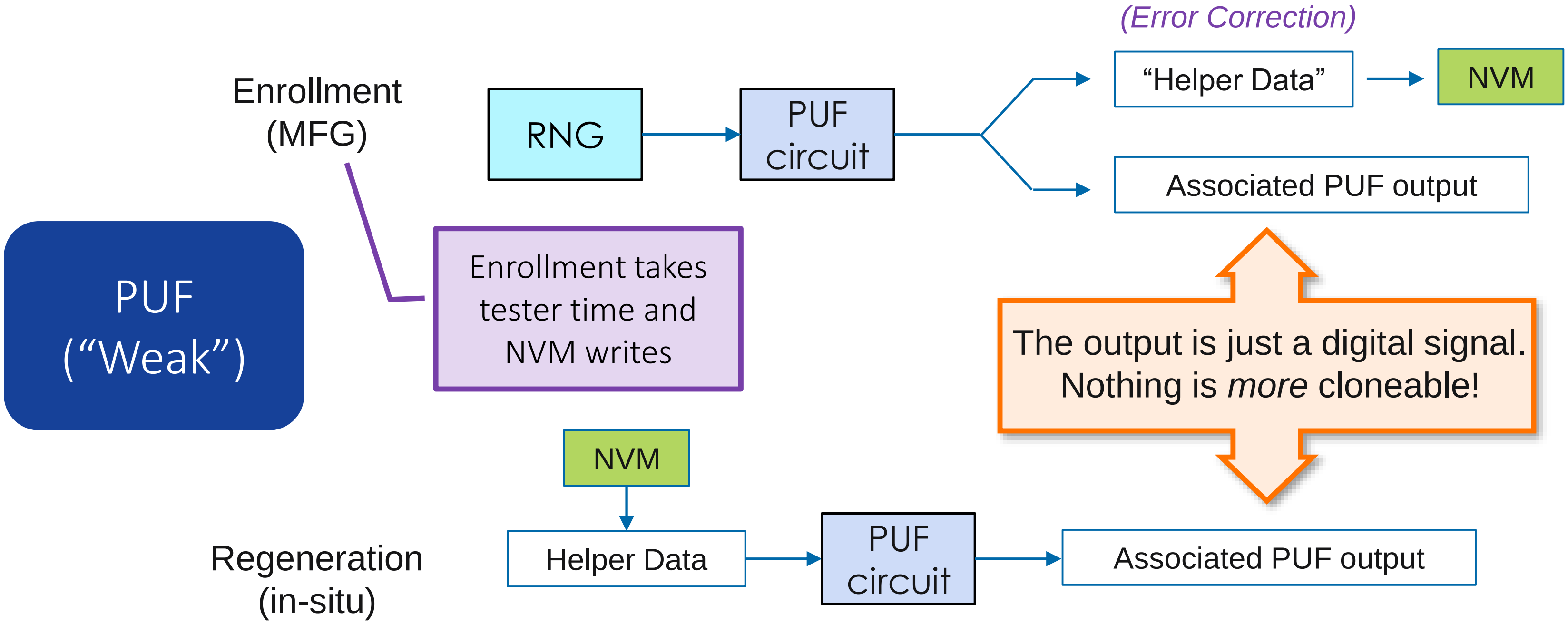
Reverse Talk: NVM has Numerous Attack Surfaces

Forward Talk: PUFs – Physically Unclonable Functions



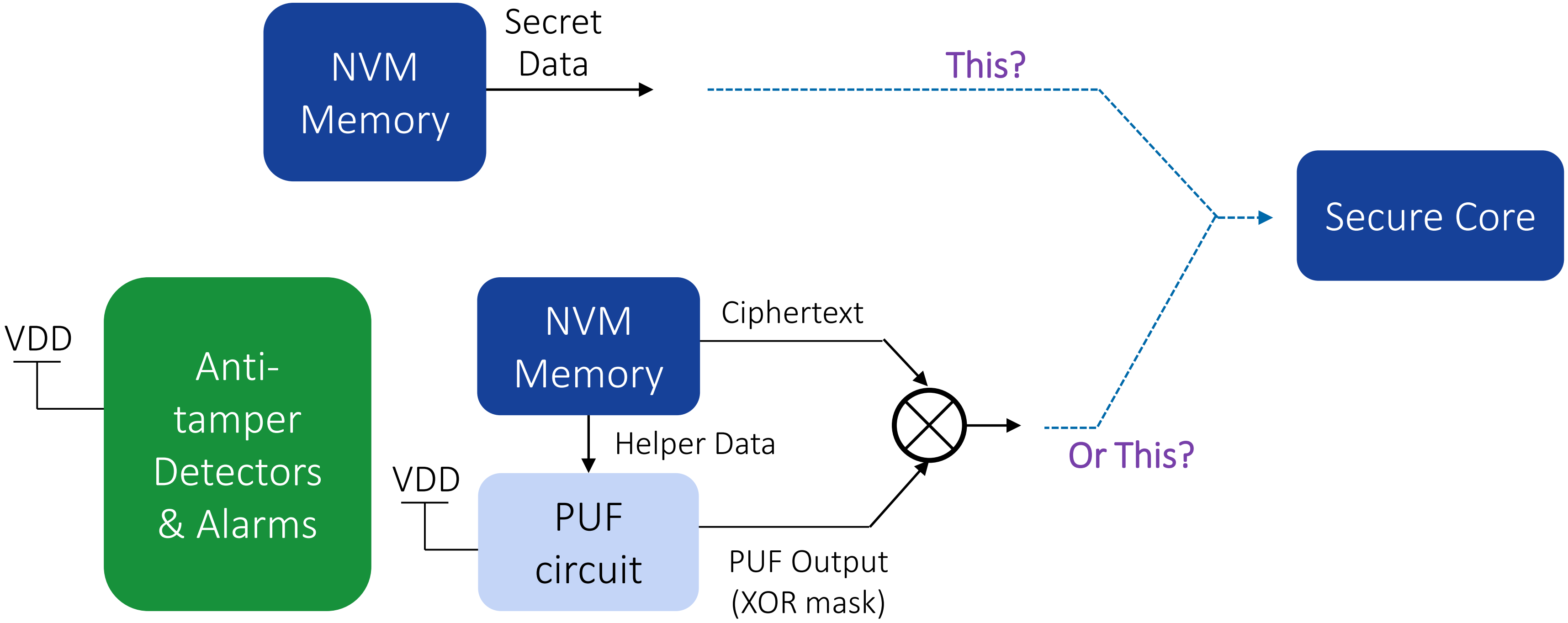
Reverse Talk: Most PUFs are Incorrectly Used

Forward Talk: PUFs – Physically Unclonable Functions



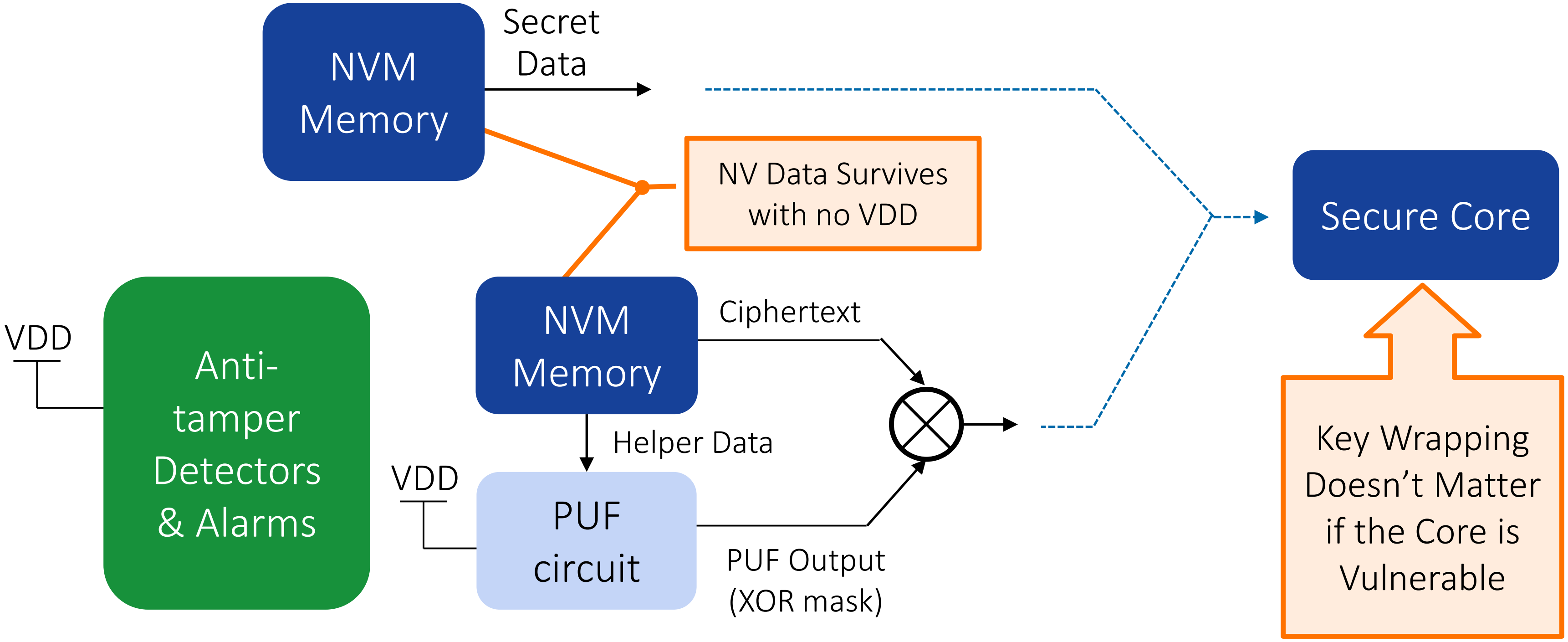
Reverse Talk: Most PUFs are Incorrectly Used

Forward Talk: PUFs – One Way to Use them Well: “Key Wrapping”



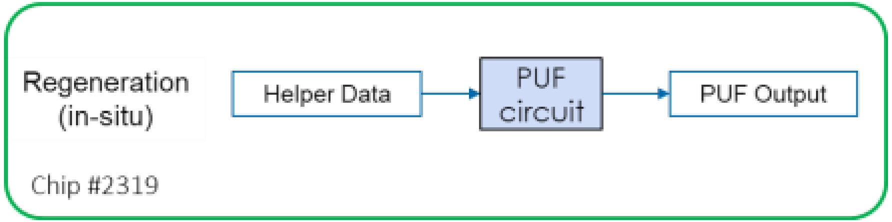
Reverse Talk: Key Wrapping Might Not Matter

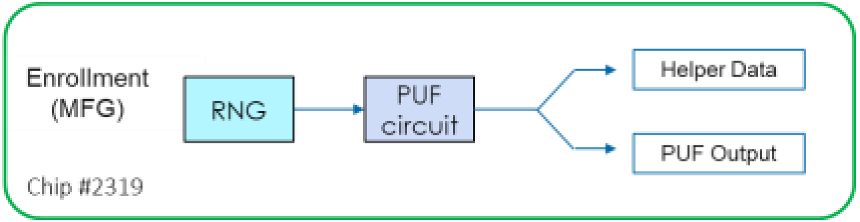
Forward Talk: PUFs – One Way to Use them Well: "Key Wrapping"


NVM Memory
Secret Data
NV Data Survives with no VDD
Secure Core
VDD
Anti-tamper Detectors & Alarms
NVM Memory
Ciphertext
Helper Data
VDD
PUF circuit
PUF Output (XOR mask)
Key Wrapping Doesn't Matter if the Core is Vulnerable

Reverse Talk: Key Wrapping Might Not Matter

Forward Talk: Backing Up … What about a PUF is *Actually* Unclonable?



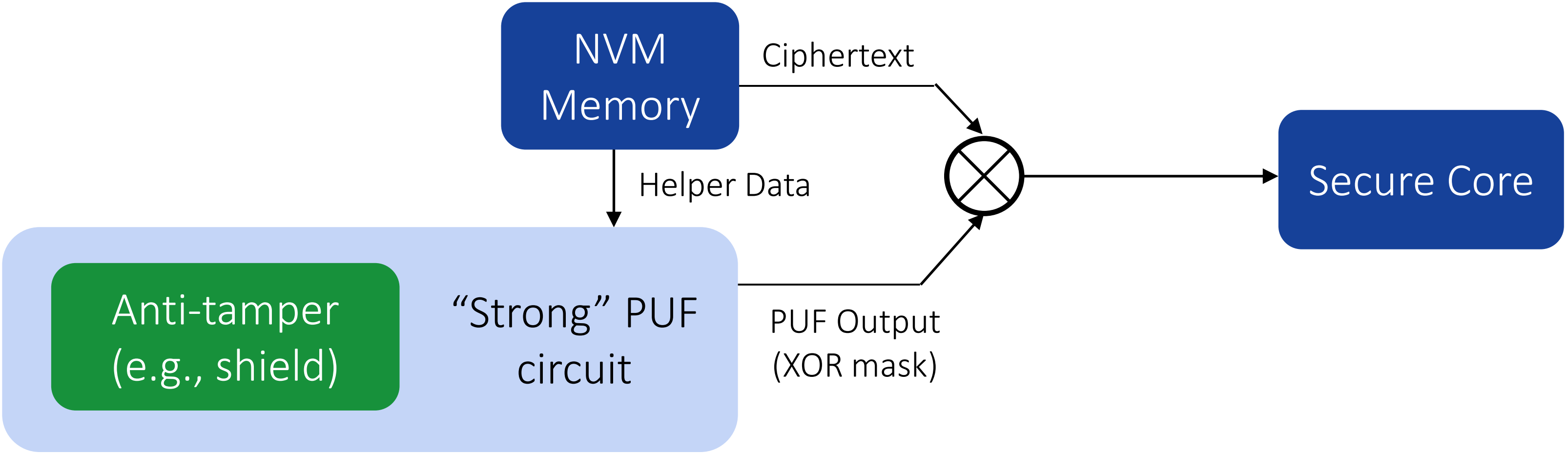


- The PUF Circuit on Chip #2319 is performing a Unique, Unclonable Transformation!
- $\mathrm{PUF\_Output}_{\#2319} = \mathrm{f}_{\#2319}\{\,\mathrm{Helper\_Data}_{\#2319}\,\}$

- Enrollment is a RNG process and can be performed more than once!
- Imagine ten Helper Data images were generated during MFG of Chip #2319…

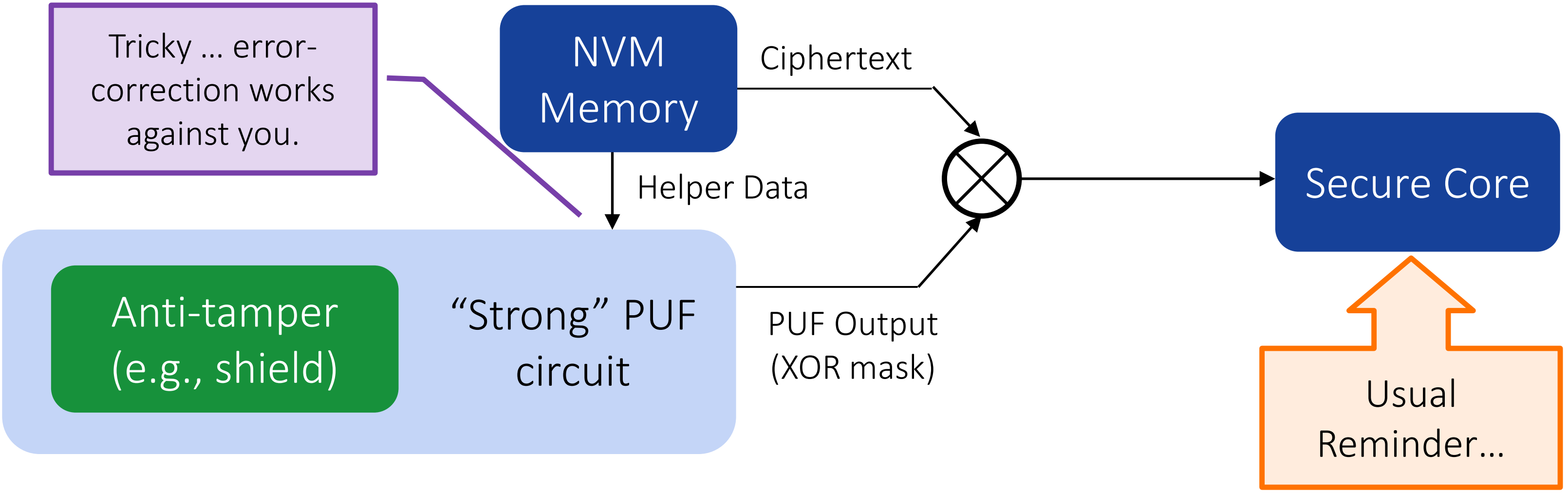
Reverse Talk: Correlation between Helper Data and PUF Output?

Forward Talk: PUFs – Another Use: "Tamper-Evidence"



Reverse Talk: Very Difficult to Detect Very Small Changes Everywhere

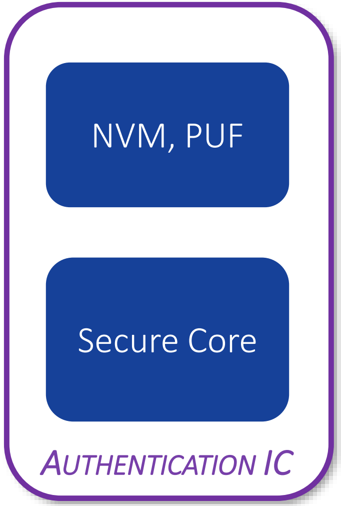
Forward Talk: PUFs – Another Use: "Tamper-Evidence"



Reverse Talk: Very Difficult to Detect Very Small Changes Everywhere

Forward Talk: In Conclusion…

1. Verify Provenance ✓
2. Power-Analysis Side-Channel ✓
3. Mutual Authentication ✓
4. Proof-of-Work 2FA ✓
5. Protected NVM ✓
6. Weak PUFs ✓
   - When used correctly
7. Strong PUFs ✓
   - Tamper-evidence



Keep in Mind the Goals:

- Force your opponent to a **full netlist recovery** with lots of FIBs and **manual electrical measurements**
- Force your opponent to **produce custom silicon**, more than an easily programmed MCU

Keep in Mind the Goals:

- Expertise in Firmware, Side-Channel, and Fault: access to at least 25% of $60B/yr

Attendees, Organizers, Antriksh S.

…Thank you

Questions?

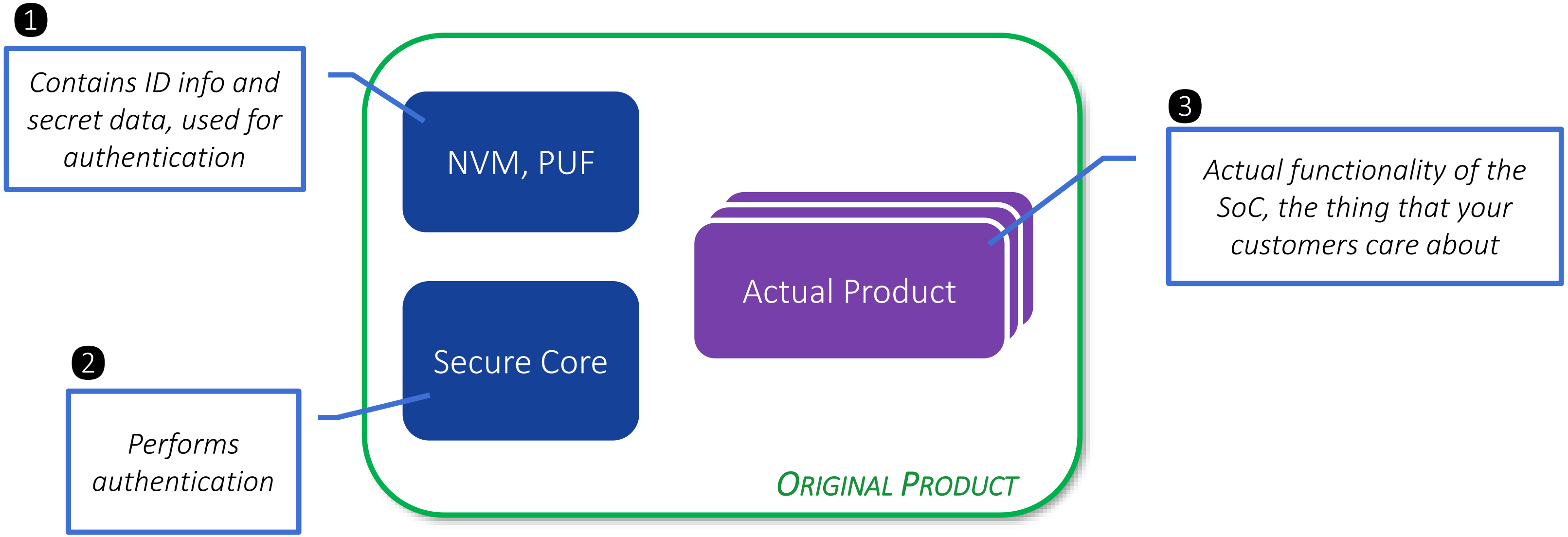
Backup

Just In Case

Agenda

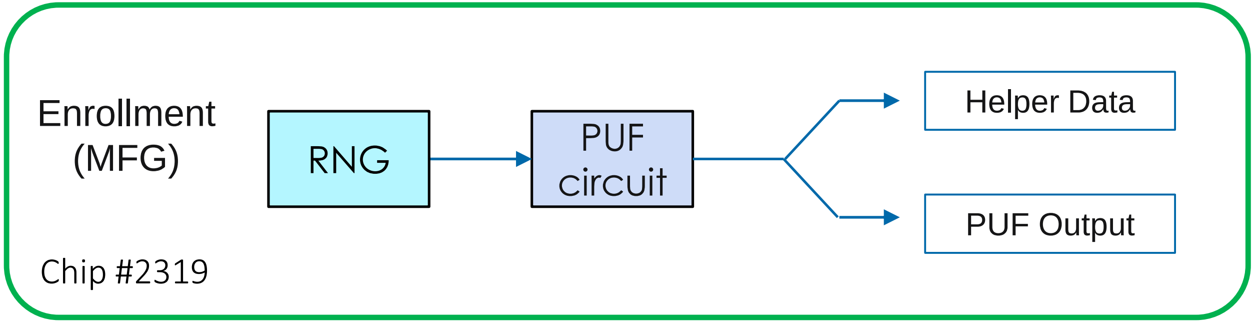
- Introduction to me
- Approach: F.E. Team vs. R.E. Team
  - Motivations (Saturn-V urban legend)
- Adversarial Concept
  - Forward/Reverse
- Manufacturing theft, Provenance Verification
- Product concepts
  - Low-cost MCU
  - Basic challenge-response; provenance verification
- Where are secrets kept?
  - Combo of Netlist, NVM (provisioned), PUF (self-generated)
- How to attack all of those?

Forward Talk: How to prevent Reverse-Engineering


1
Contains ID info and secret data, used for authentication
NVM, PUF
2
Performs authentication
Secure Core
Actual Product
3
Actual functionality of the SoC, the thing that your customers care about
ORIGINAL PRODUCT

Reverse Talk: How to defeat anti-R.E. countermeasures

Forward Talk: Backing Up … What in a PUF is *Actually* Unclonable?

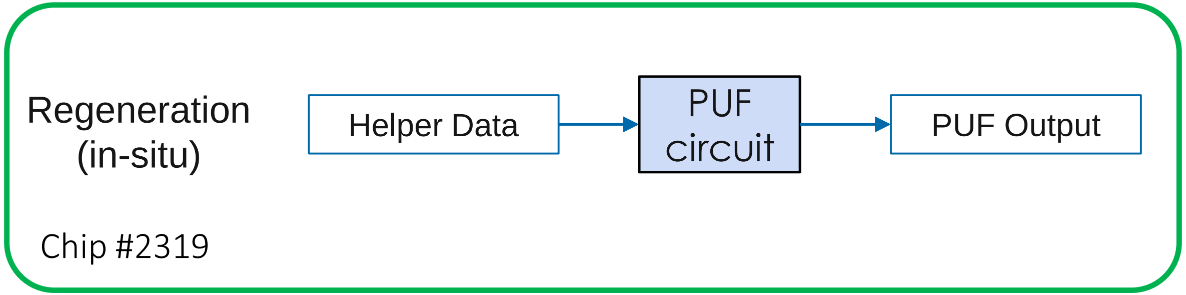


- The PUF Circuit on Chip #2319 is performing a Unique, Unclonable Transformation!
- $\text{PUF\_Output}_{\#2319} = f_{\#2319}(\text{ Helper\_Data}_{\#2319})$

- Enrollment is a random process and can be performed more than once!
- Imagine ten Helper Data images were generated during MFG of Chip #2319…

Reverse Talk: Correlation between Helper Data and PUF Output?

Forward Talk: Backing Up … What in a PUF is *Actually* Unclonable?



- The PUF Circuit on Chip #2319 is performing a Unique, Unclonable Transformation!
- $\text{PUF\_Output}_{\#2319} = f_{\#2319}(\text{Helper\_Data}_{\#2319})$

- Enrollment is a random process and can be performed more than once!
- Imagine ten Helper Data images were generated during MFG of Chip #2319…

Reverse Talk: Correlation between Helper Data and PUF Output?