Technische Universität Braunschweig

UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR TECHNISCHE INFORMATIK

INSTITUTE OF COMPUTER AND NETWORK ENGINEERING

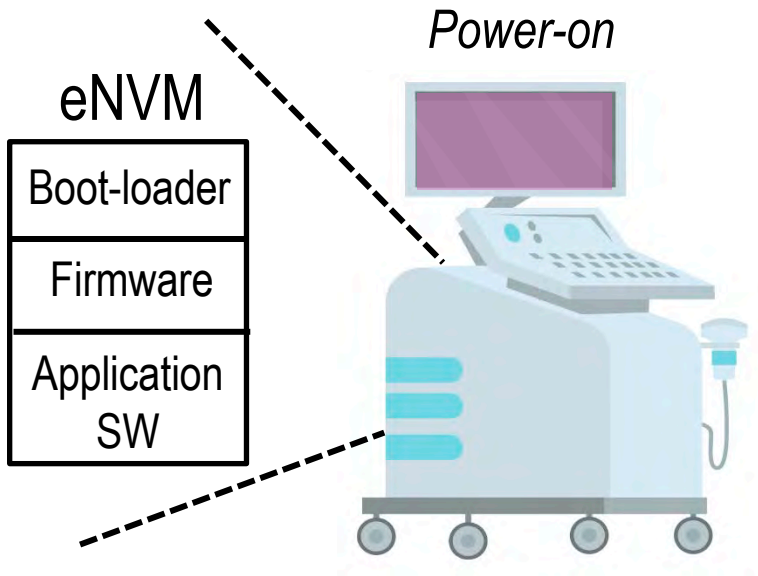
Clone-Resistant Secured Booting Based on Unknown Hashing Created in Self-Reconfigurable Platform

Randa Zarrouk, Saleh Mulhem, Wael Adi, and Mladen Berekovic

International Symposium on Applied Reconfigurable Computing ARC 2021

29.06.2021

Introduction



Medical device

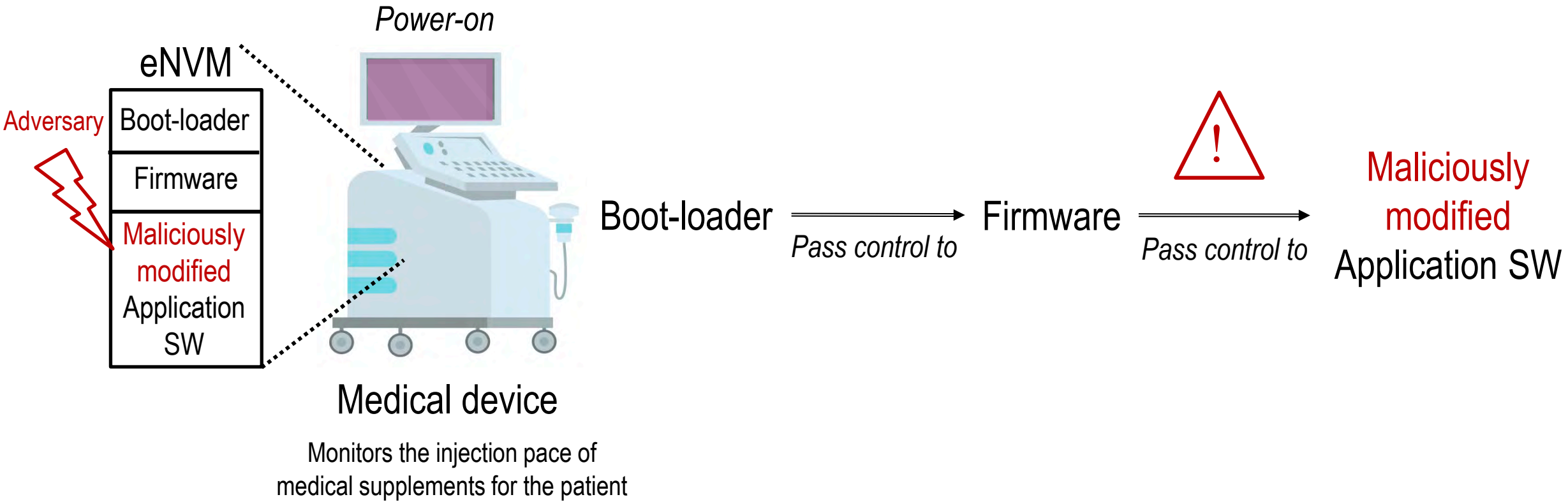
Monitors the injection frequency of medical supplements for the patient

Boot-loader → Firmware → Application SW

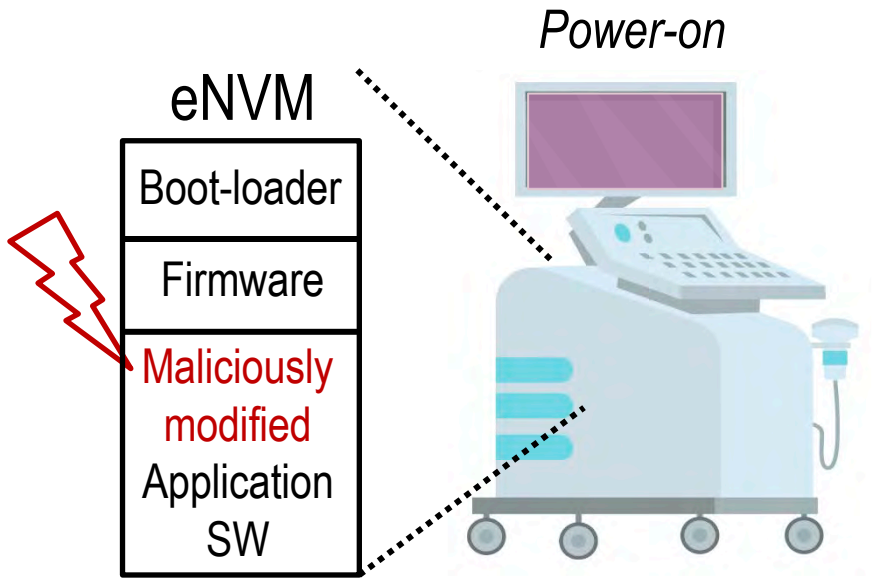
Passes control to *Passes control to*

Boot sequence

Introduction

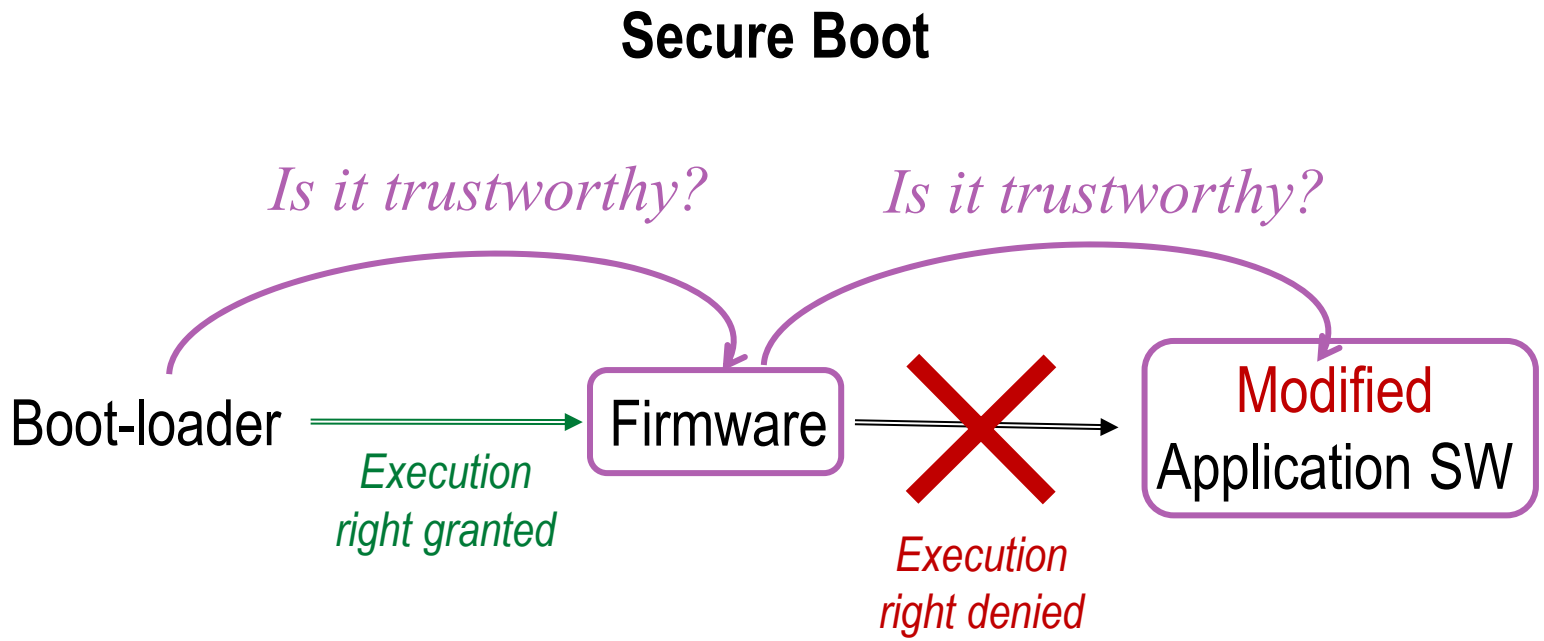


Introduction



Medical device

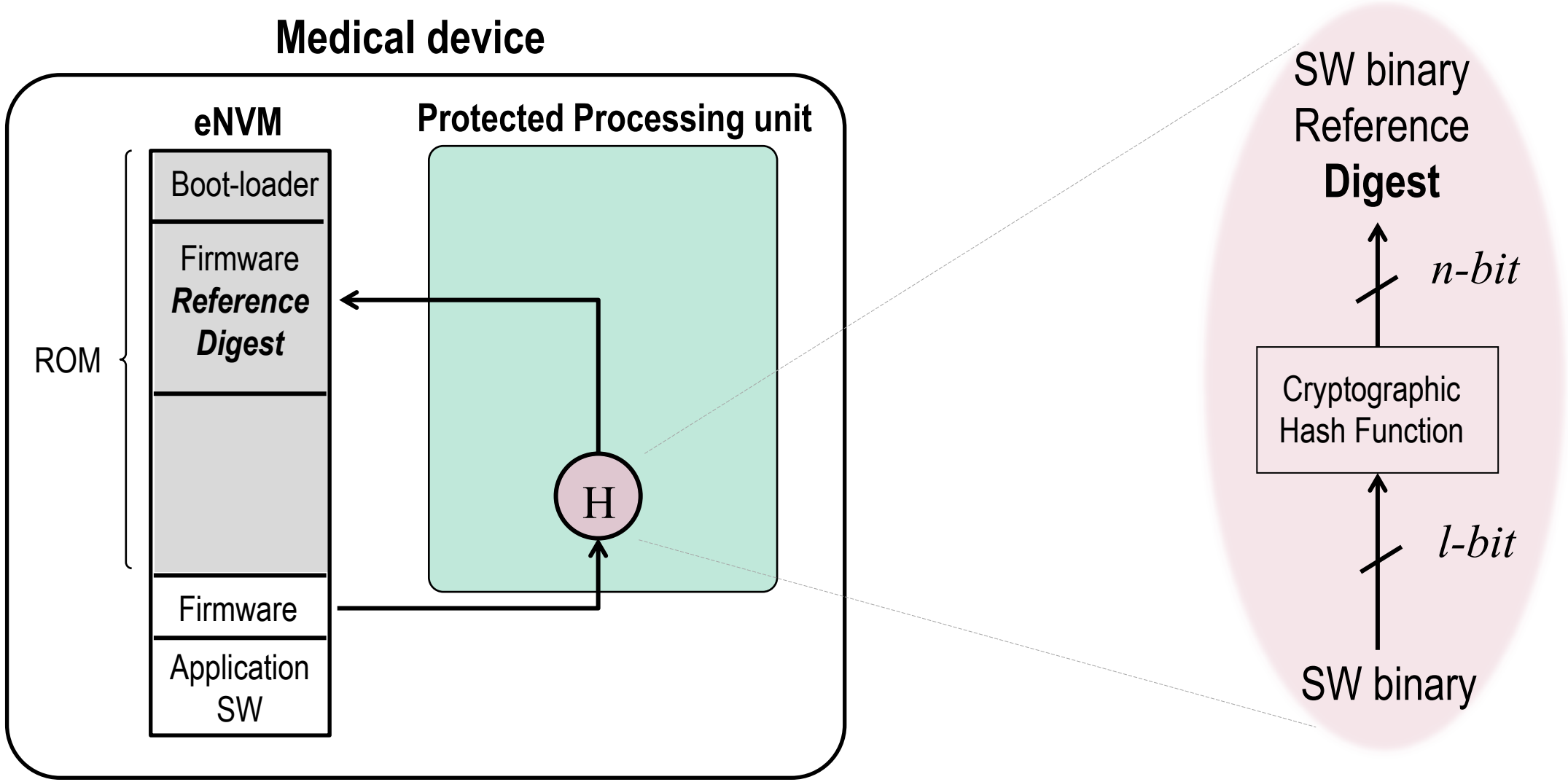
Monitors the injection pace of medical supplements for the patient



Outline

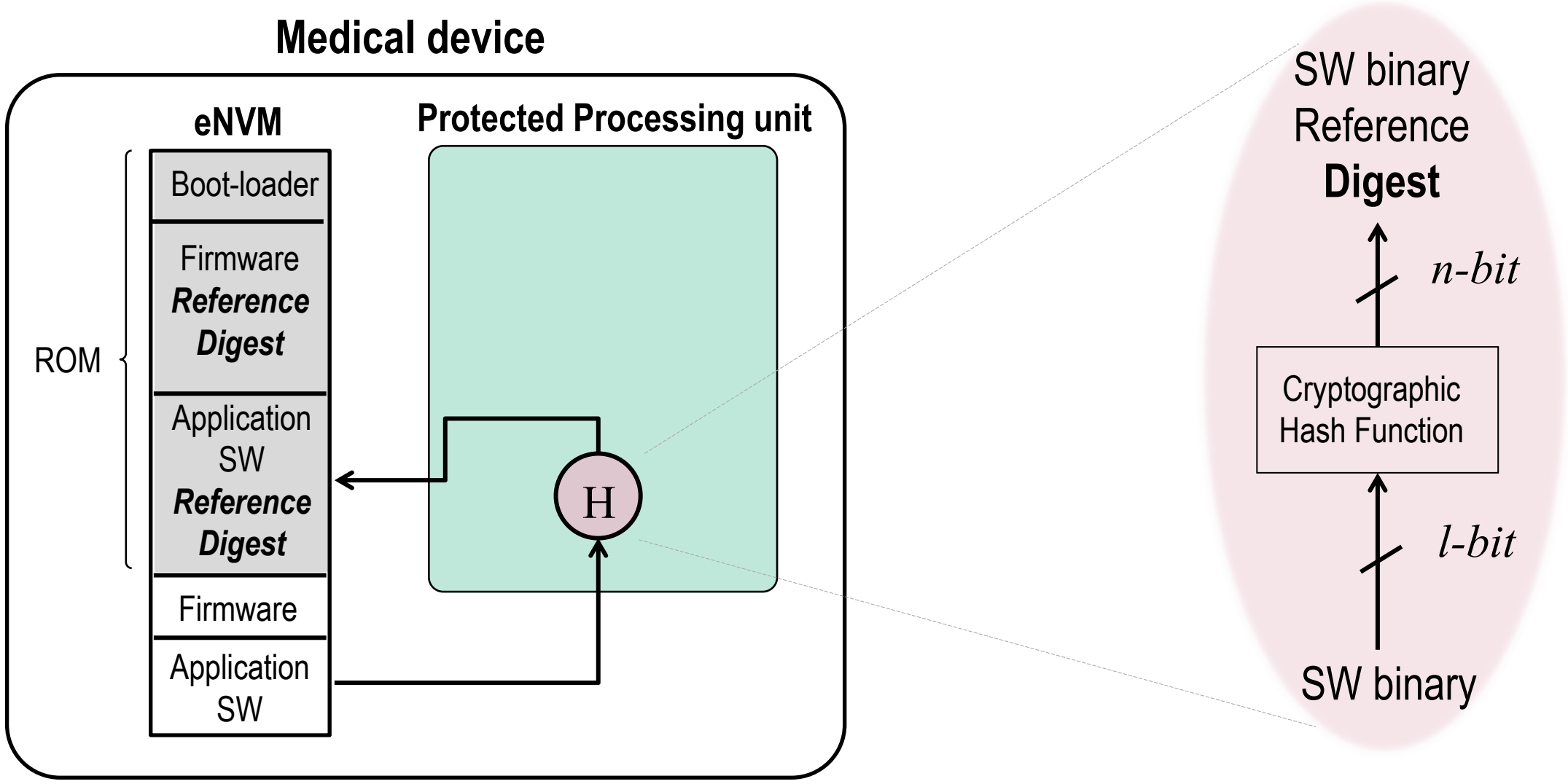
- Software Turstwothiness via cryptographic premitives
- Device-Specific Secure Boot
- Secret Unknown Hash (SUH) Concept
- SUH Sample Variant
- Conclusion

Integrity Verification



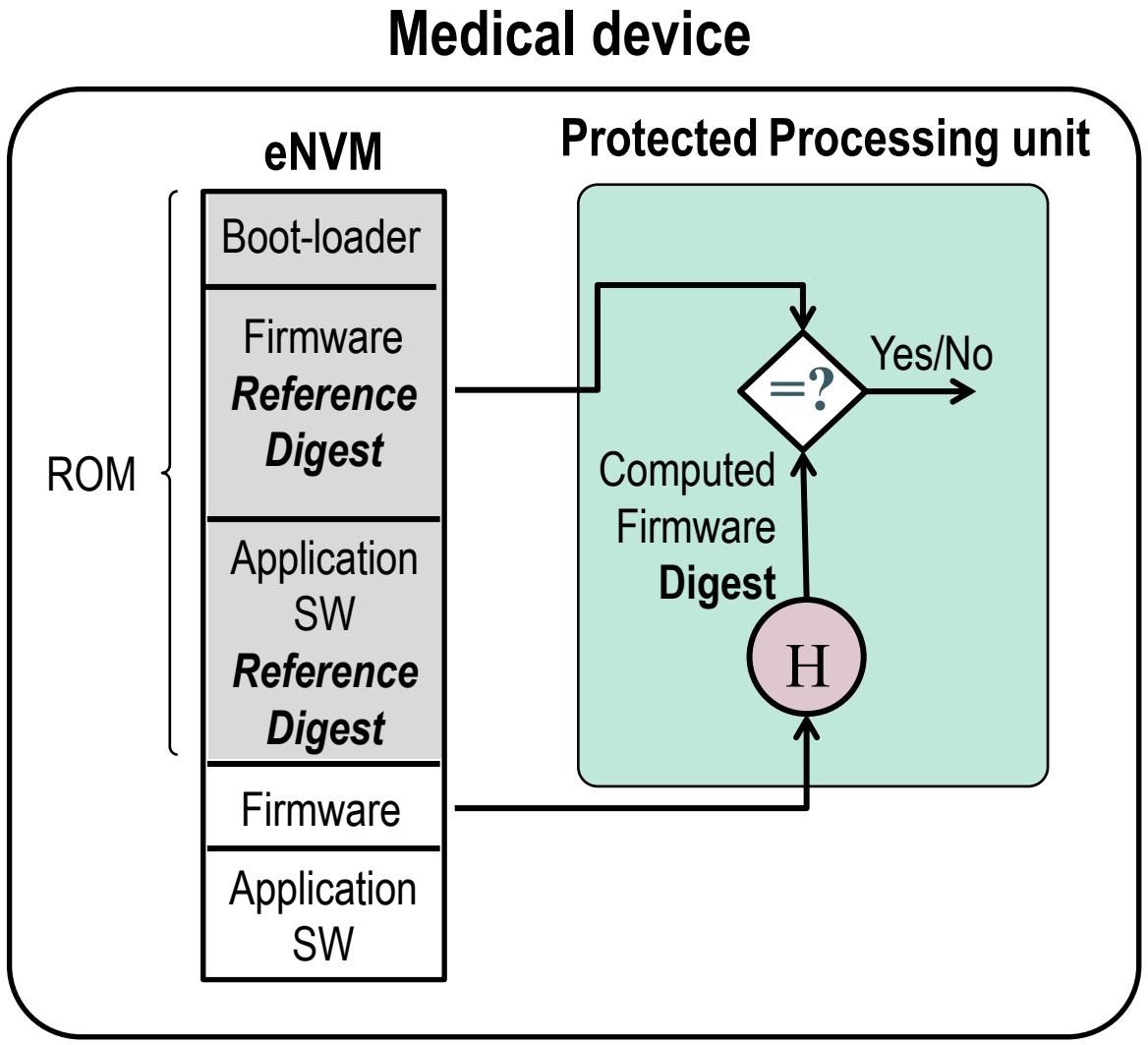
H: Cryptographic Hash Function **ROM:** Read Only Memory

Integrity Verification



H: Cryptographic Hash Function **ROM:** Read Only Memory

Integrity Verification

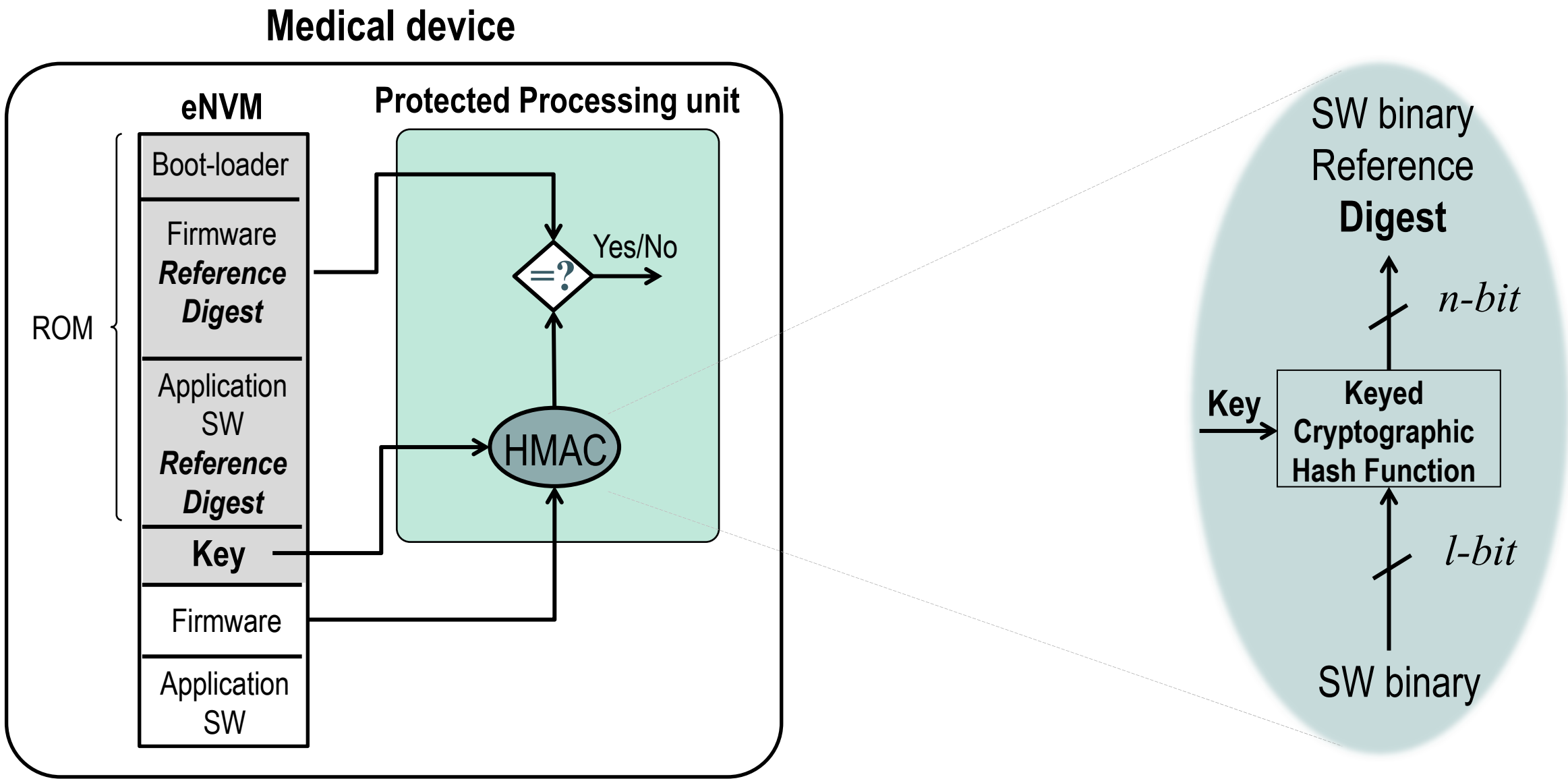


H: Cryptographic Hash Function

ROM: Read Only Memory

Integrity + Authenticity Verification

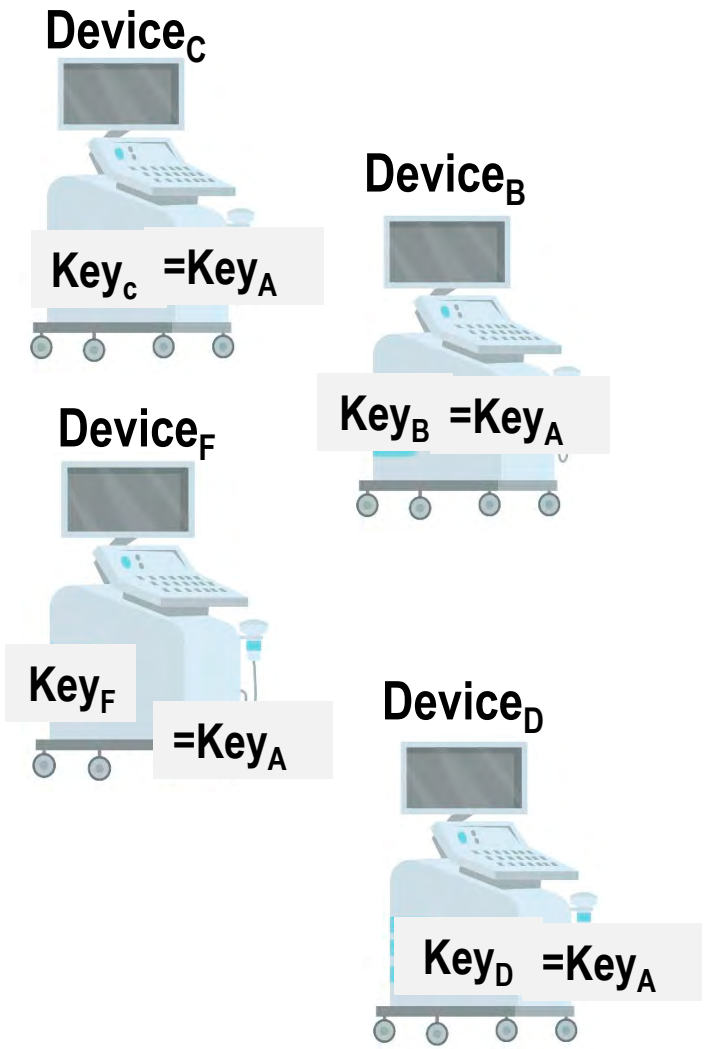
System in use



* Keyed Cryptographic Hash Function or so-called HMAC

Authentication Key

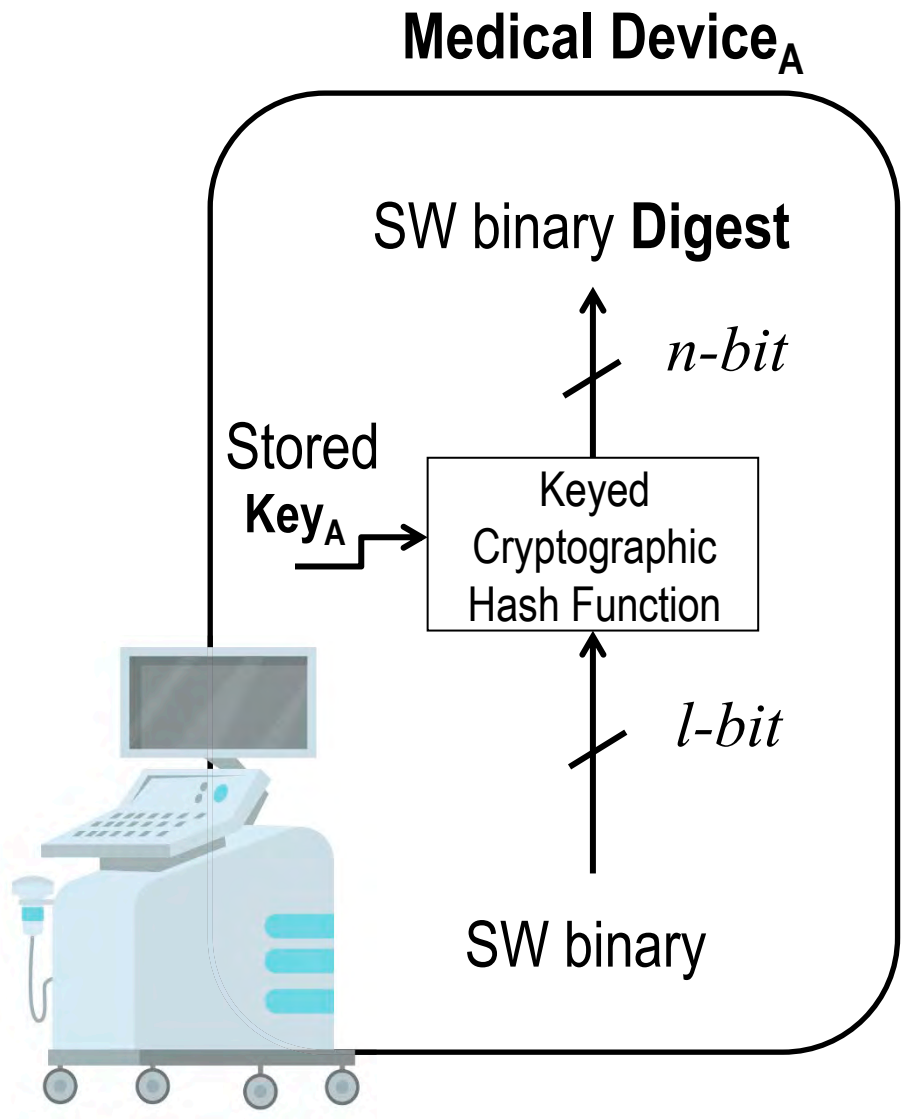
Provisioned by the Manufacturer



- Prone to readback attacks
- Manufacturer knows the **keys**

  $\Rightarrow$ Can trick the end-user and provision the same key for different devices.

Known key, cloneable key!



Physical Unclonable Function (PUF)

Created from the unique properties and physical characteristics of an electronic device.

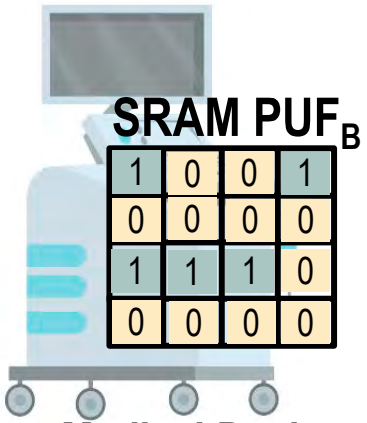
Some PUF types

- Coating PUF
- Arbiter PUF
- Controlled PUF
- RO PUF
- **SRAM PUF [1]**

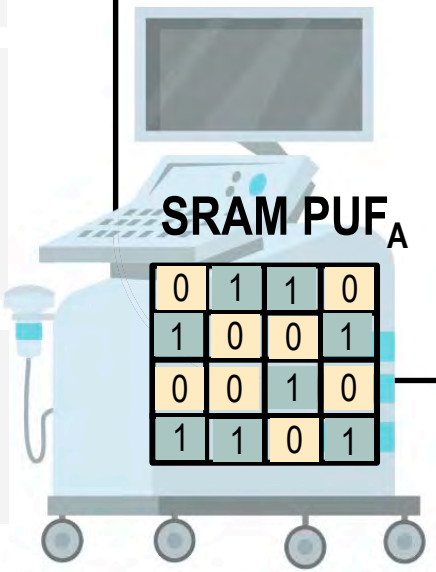
Variations in the production process give every transistor slightly random electric properties

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

The start-up values are unique to each device can be turned into a finger print for the device



Medical Device$_B$



Medical Device$_A$

SW binary **Digest**

n-bit

Physical Unclonable Function

Unknown Key

Keyed Cryptographic Hash Function

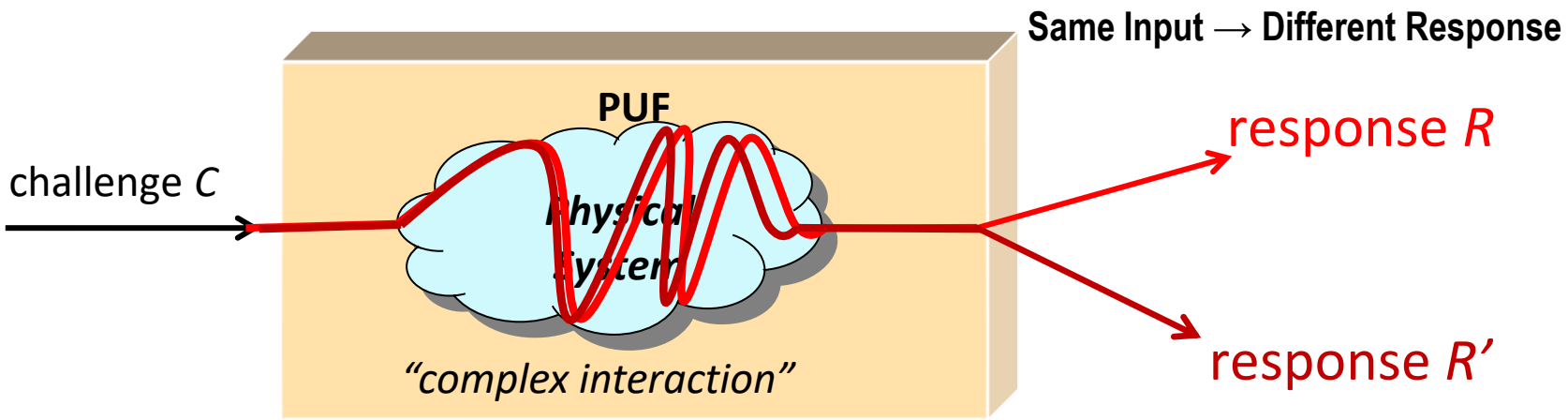
l-bit

SW binary

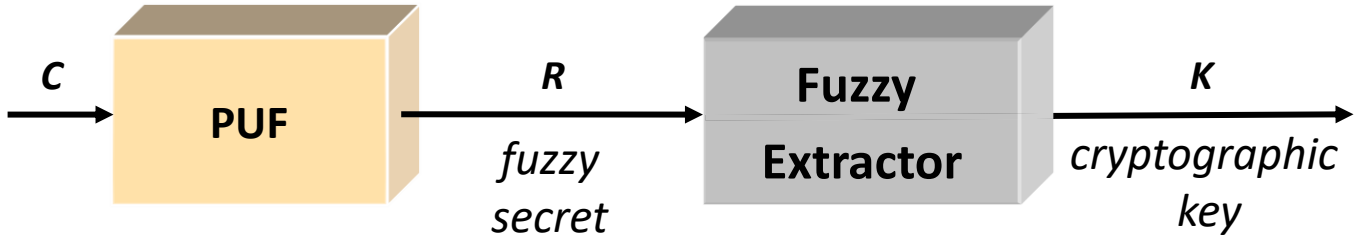
***H:** Cryptographic Hash Function* ***ROM:** Read Only Memory*

Vulnerabilities

❑ Inconsistency in ***Response reproducibility*** due to noise, aging, and other factors



- Fuzzy Extractor was proposed as a remedy.



❑ Predictability (for unprotected Strong PUF)

❑ Response length expansion

Why not to create **an in-device hardwired cryptographic function** that serves as **device secret** that:

no body knows,

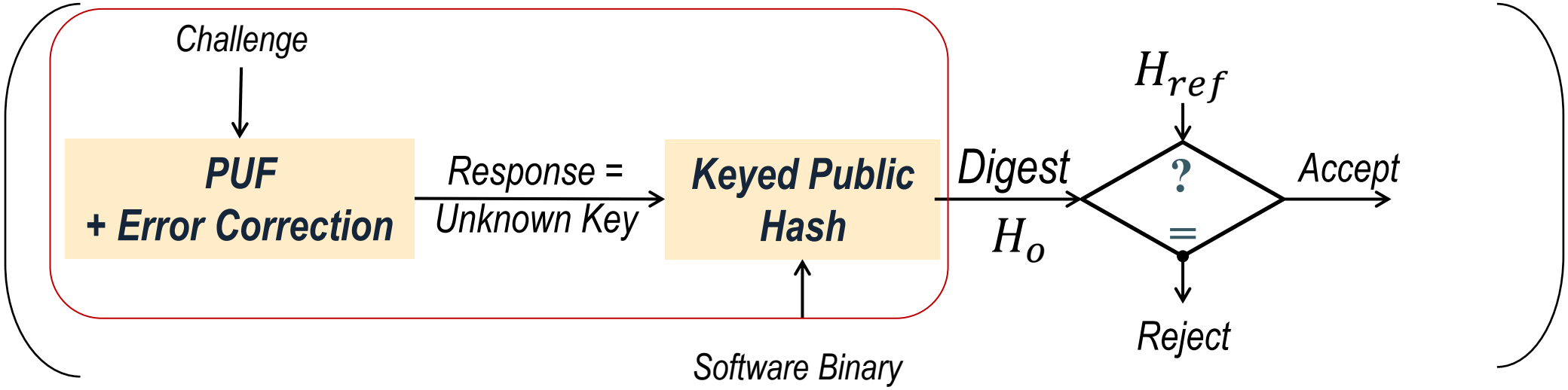
specific to each device,

with consistent response reproducibility,

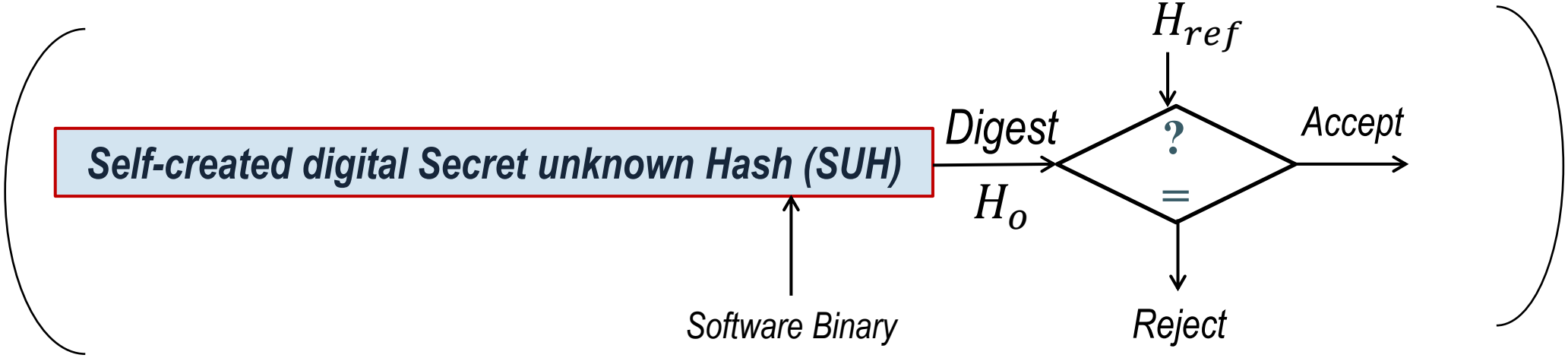
?

PUF-based Vs. SUH-based

System in use



PUF-based Secure Boot

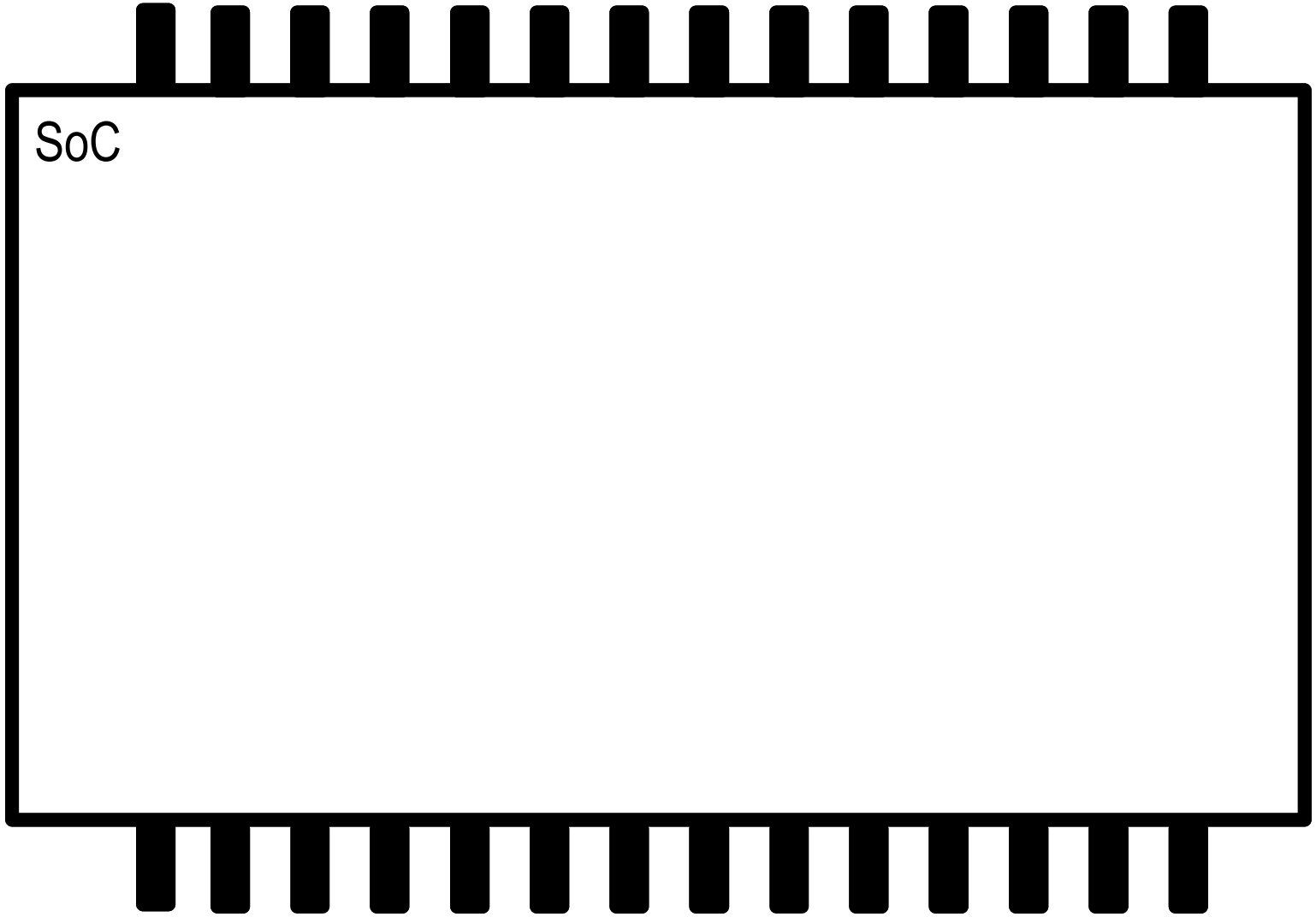


New concept:
SUH-based Secure Boot

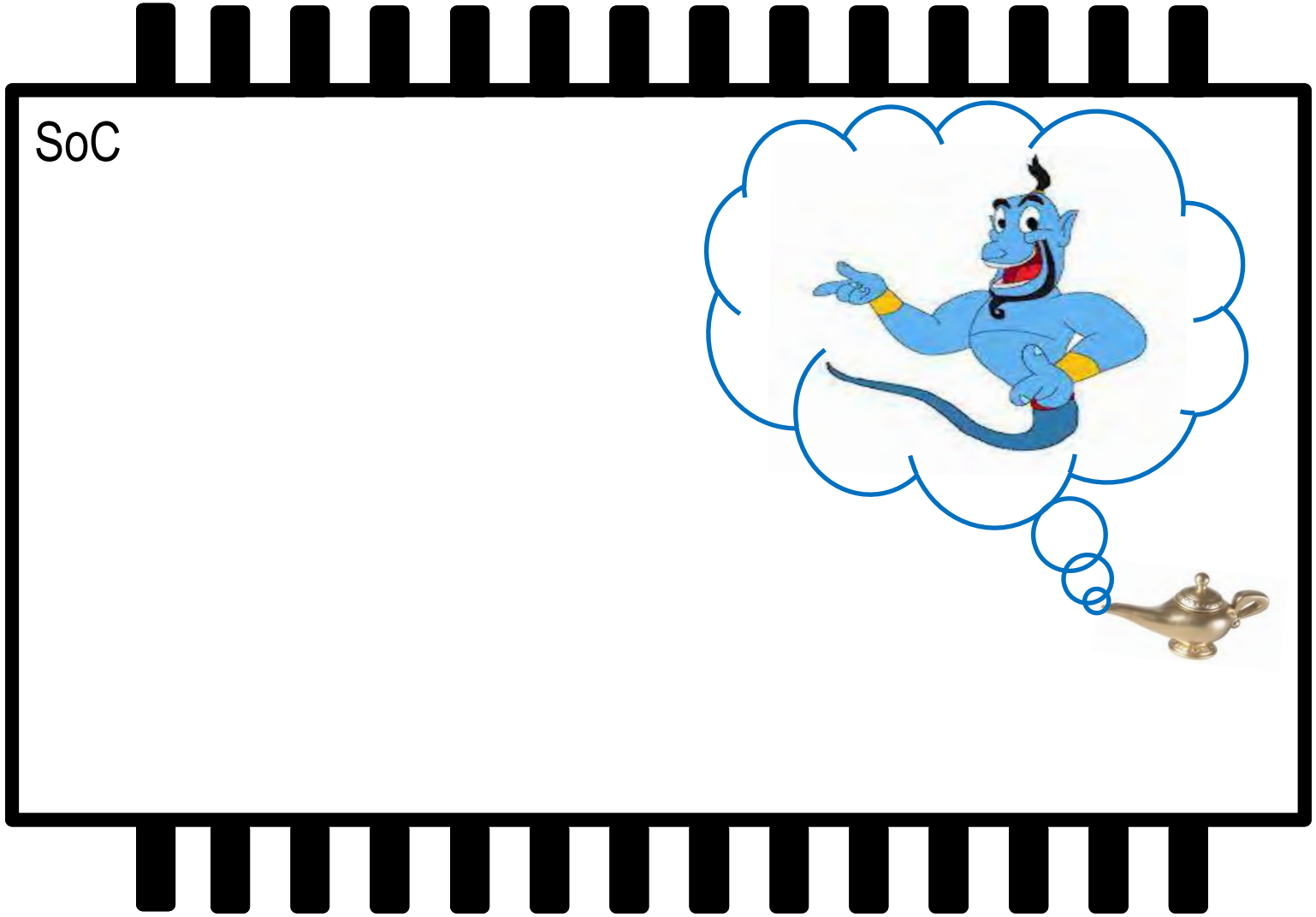
PUF-based Vs. SUH-based

Characteristics	Secure boot- based on	
	PUF + A hardwired traditional hash function	SUH
Offers data integrity	yes	yes
Offers data authentication	yes	yes
Offers device authentication	yes	yes
Requires additional measurements for a consistent response reproducibility	yes	no
Uses a key	yes	no
Created in Post-manufacturing setting	no	yes

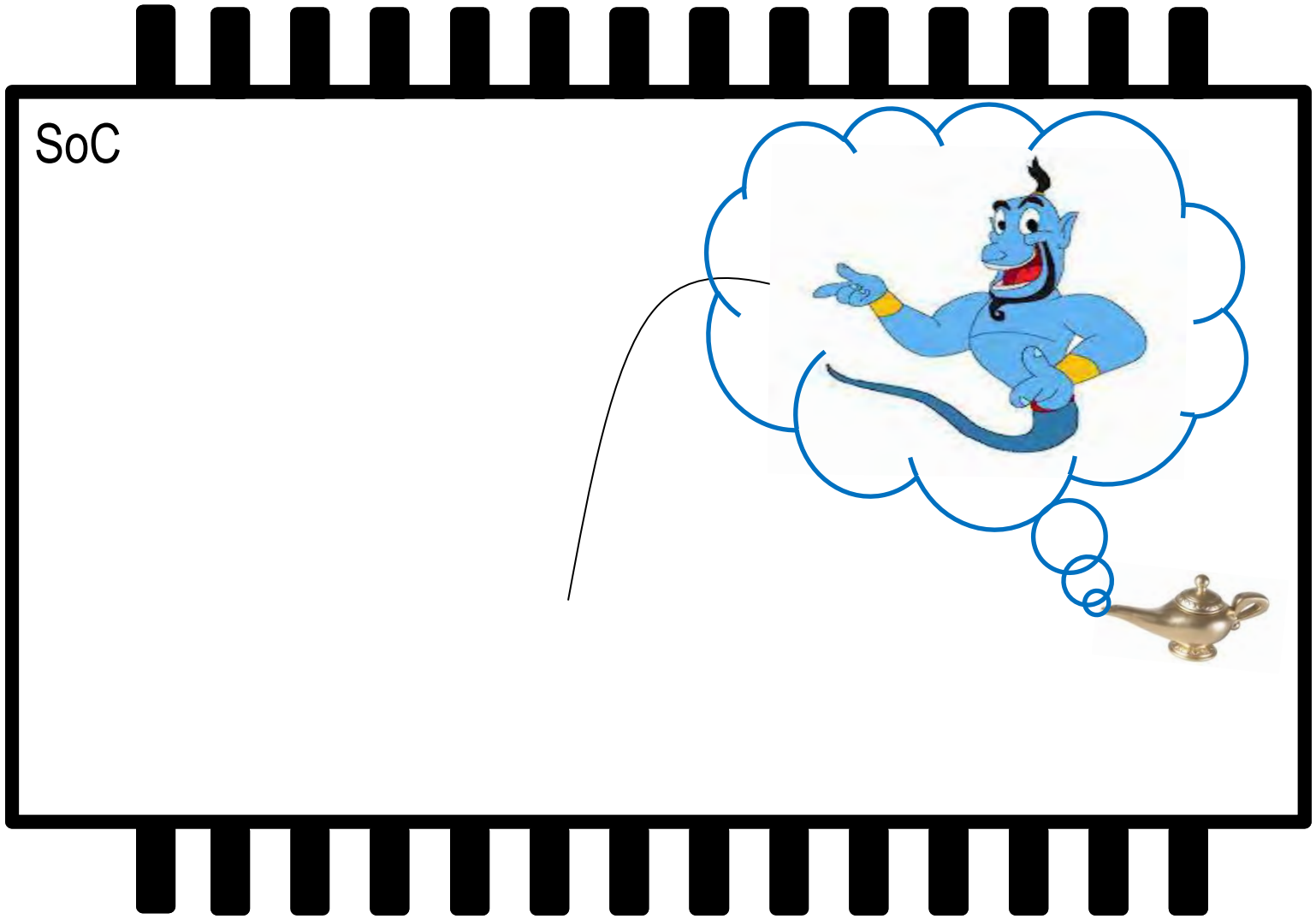
Concept



Concept

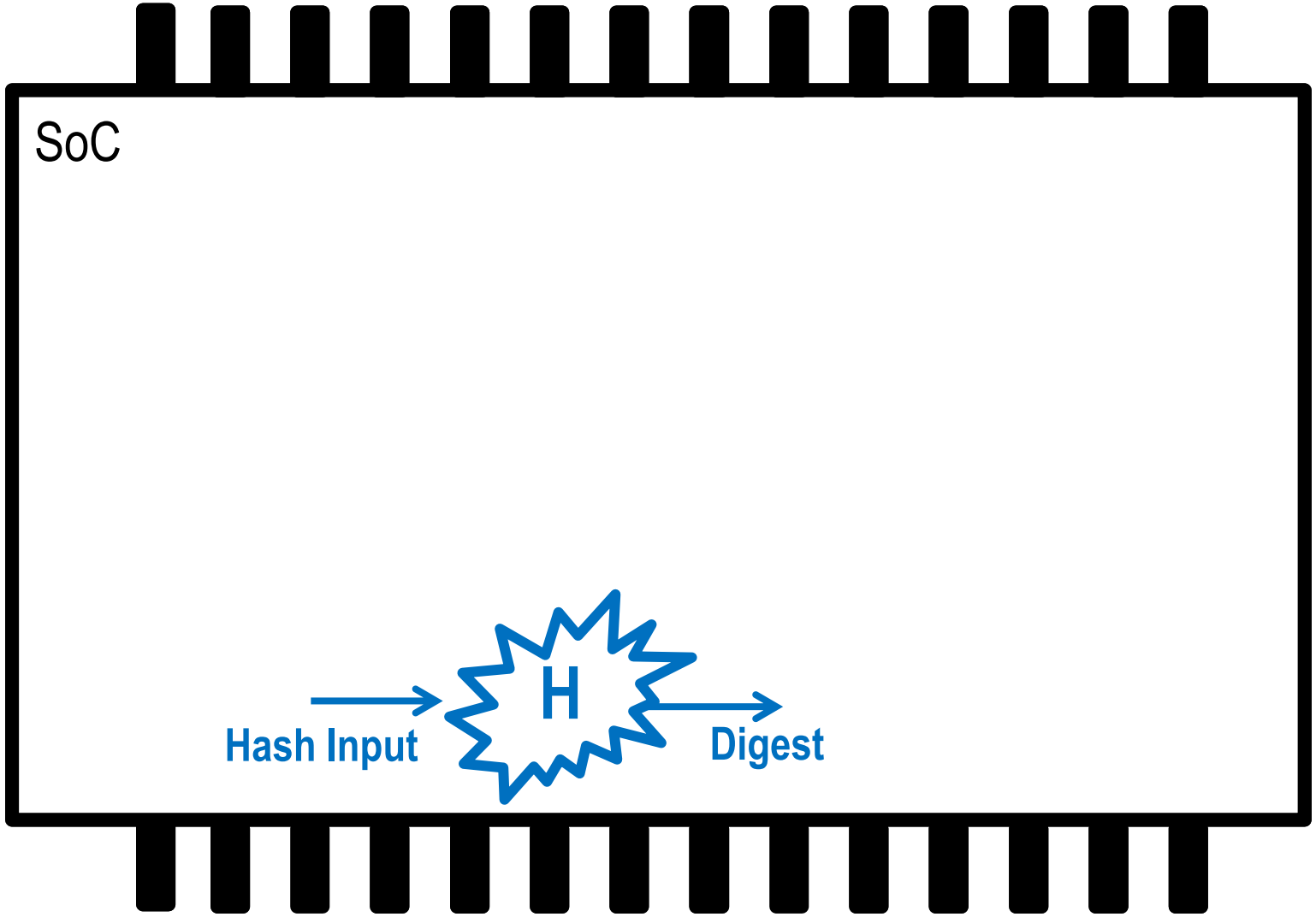


Concept

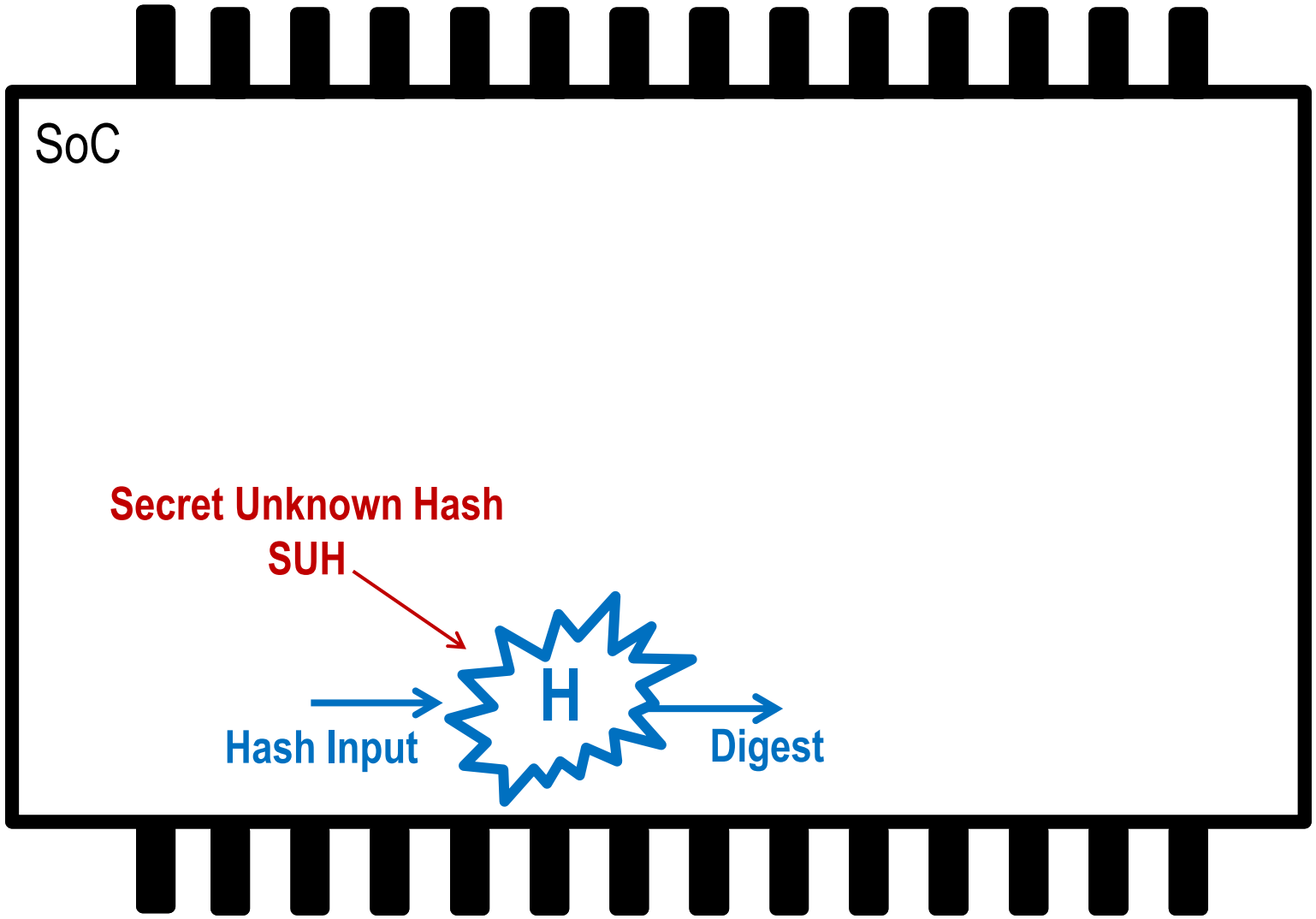


Secret Unknown Hash

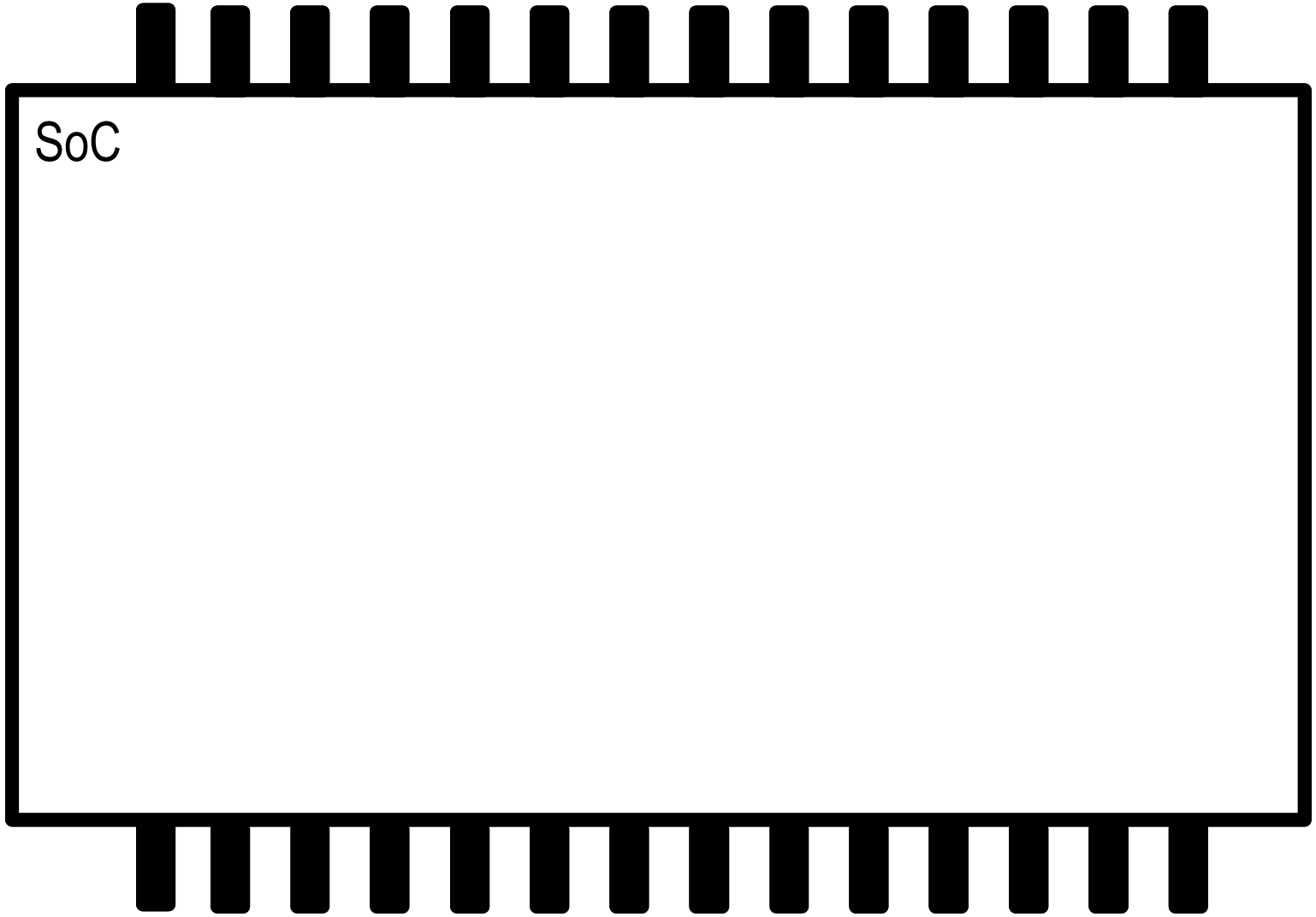
Concept



Concept



Secret Unknown Hash Creation

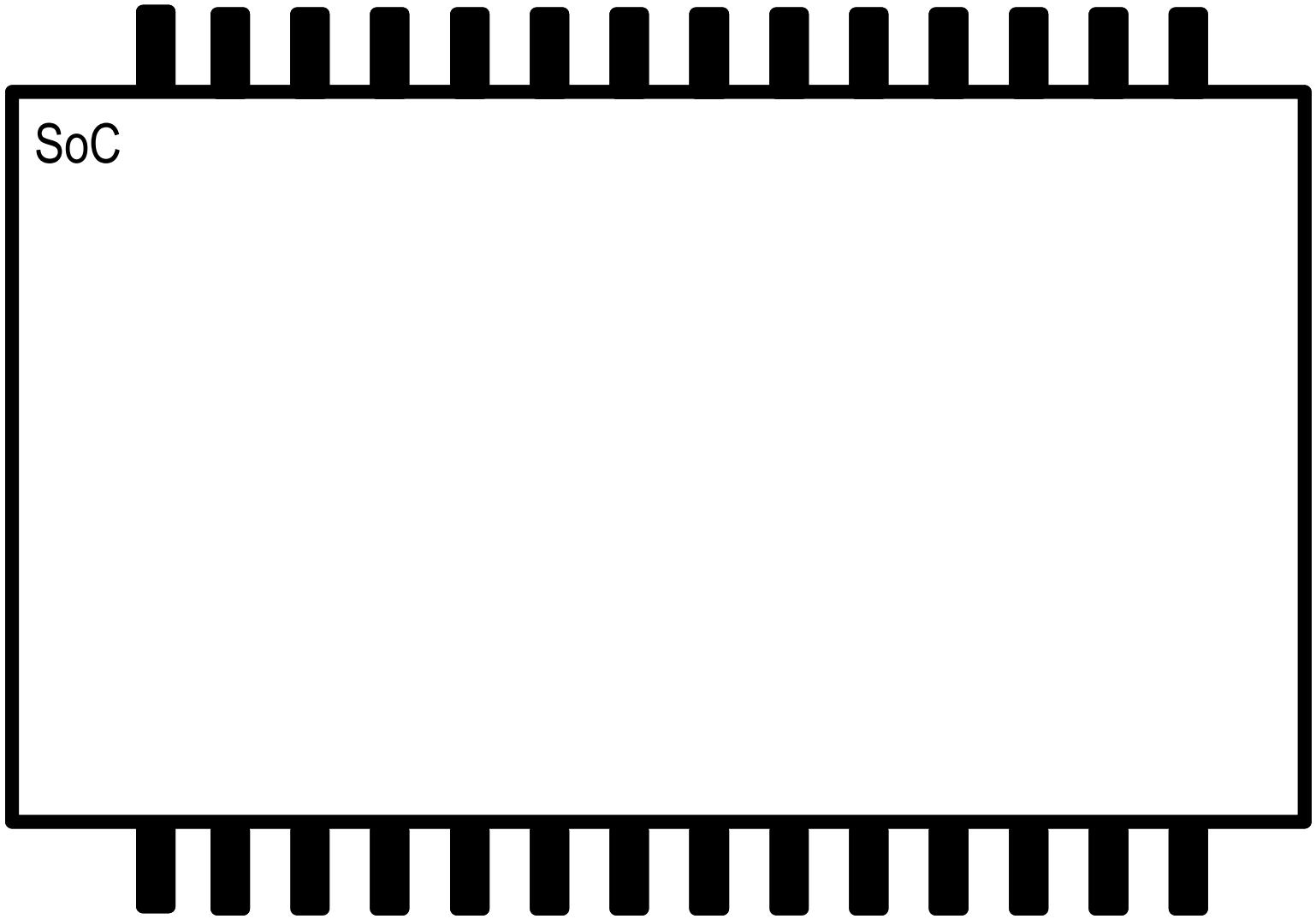


System on Chip with:

Self-
Reconfigurable
Non-Volatile
HW Fabric

Microsemi
a Microchip company

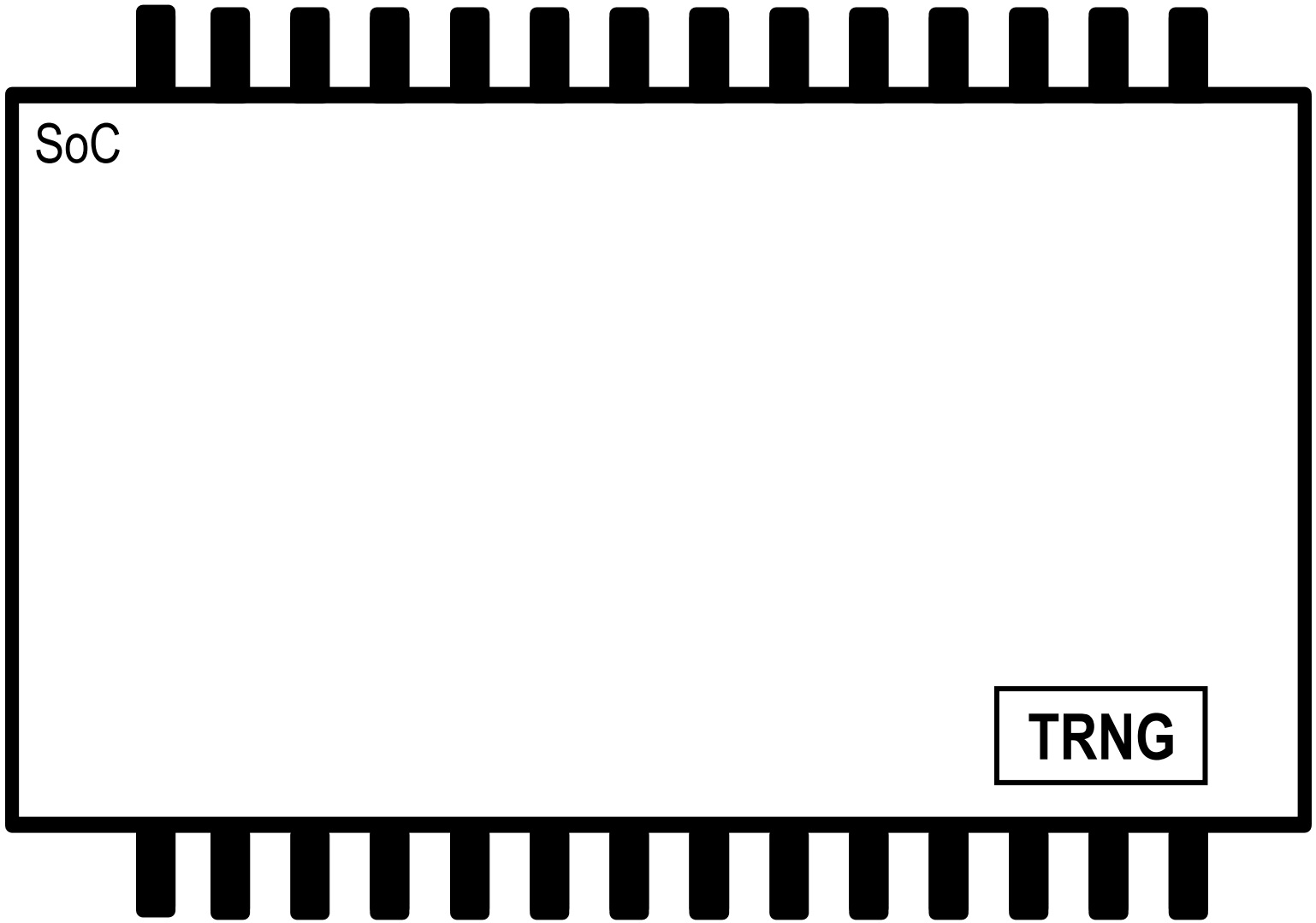
Secret Unknown Hash Creation



System on Chip with: Self-Reconfigurable Non-Volatile HW Fabric

Secret Unknown Hash Creation

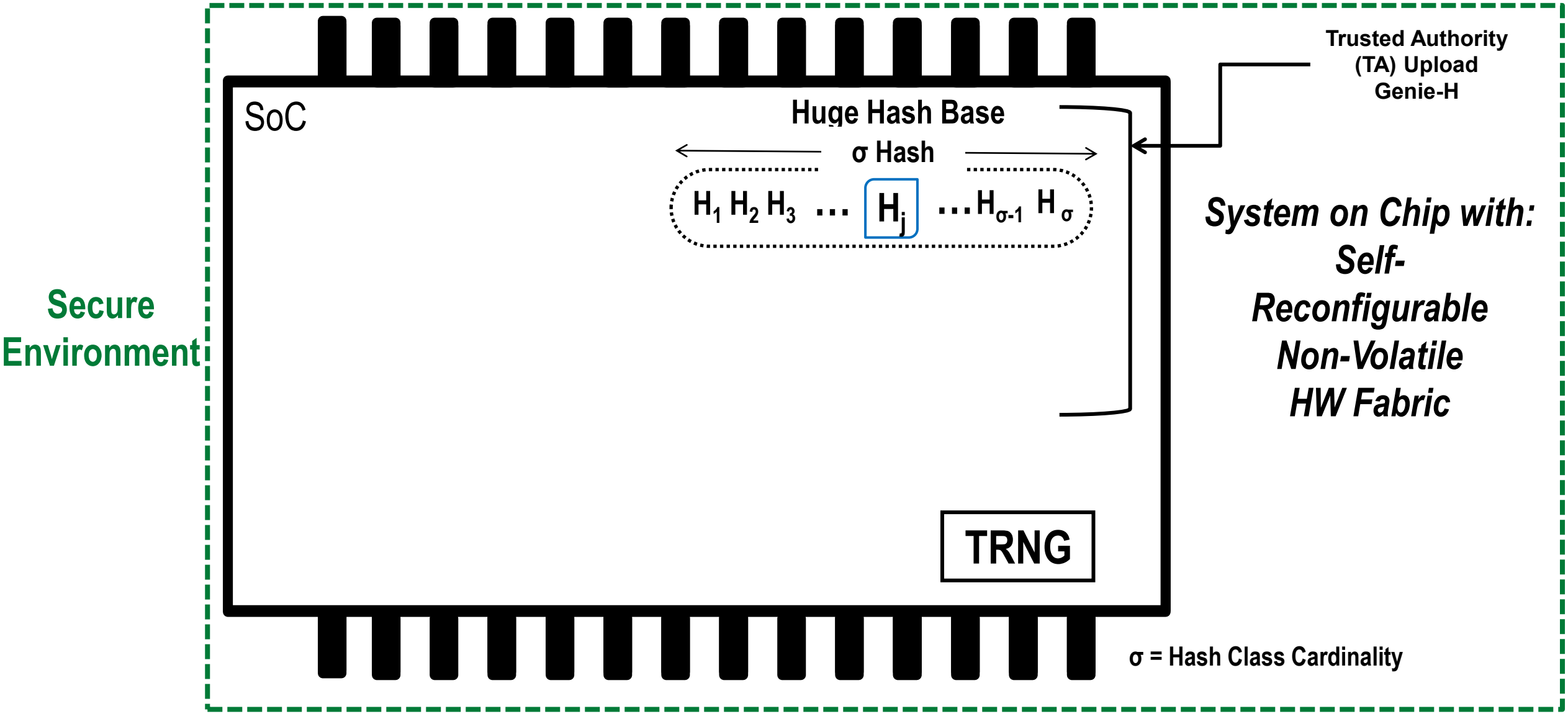
Secure Environment



System on Chip with: Self-Reconfigurable Non-Volatile HW Fabric

TRNG: True Random Number Generator

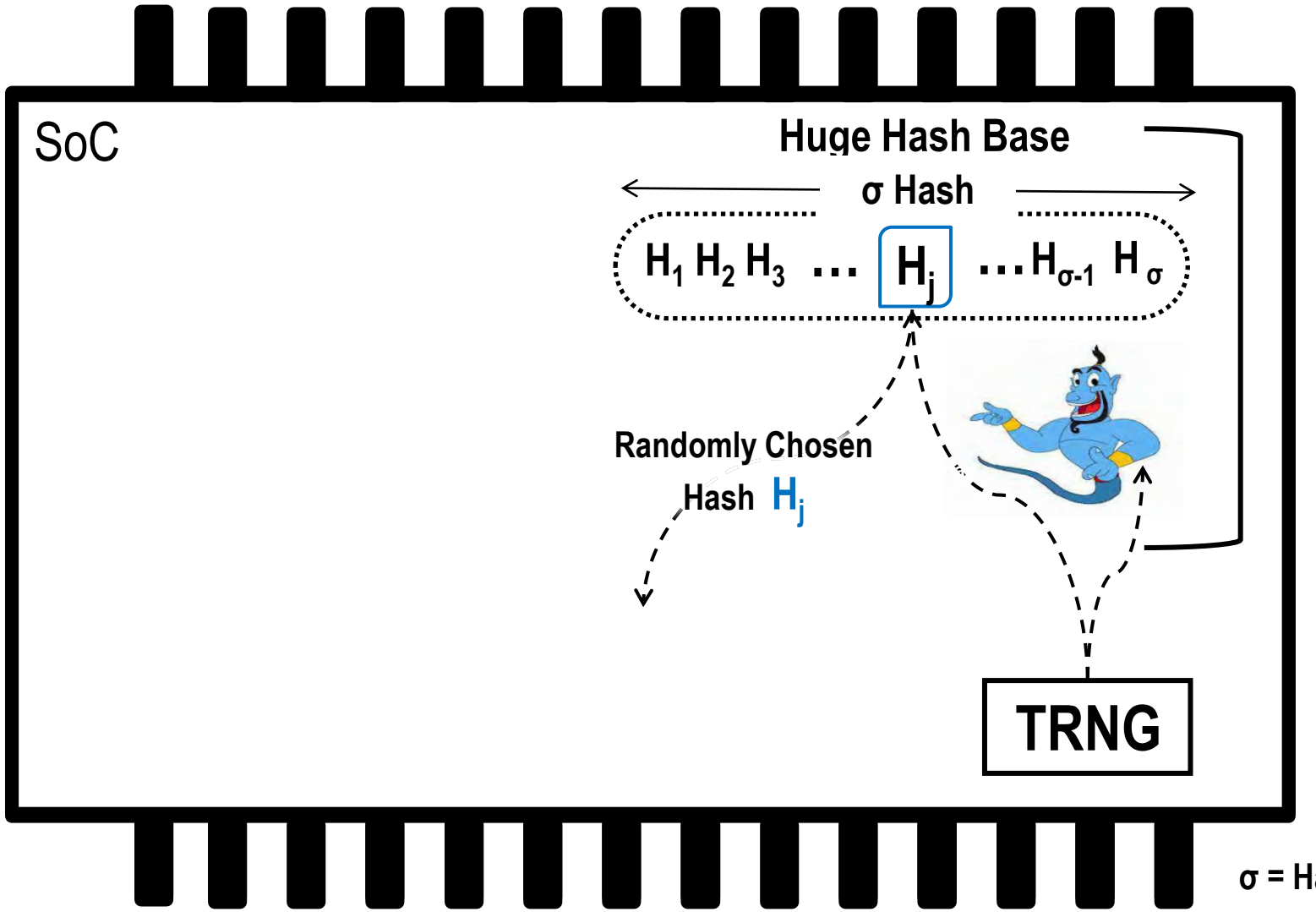
Secret Unknown Hash Creation



TRNG: True Random Number Generator

Secret Unknown Hash Creation

Secure Environment



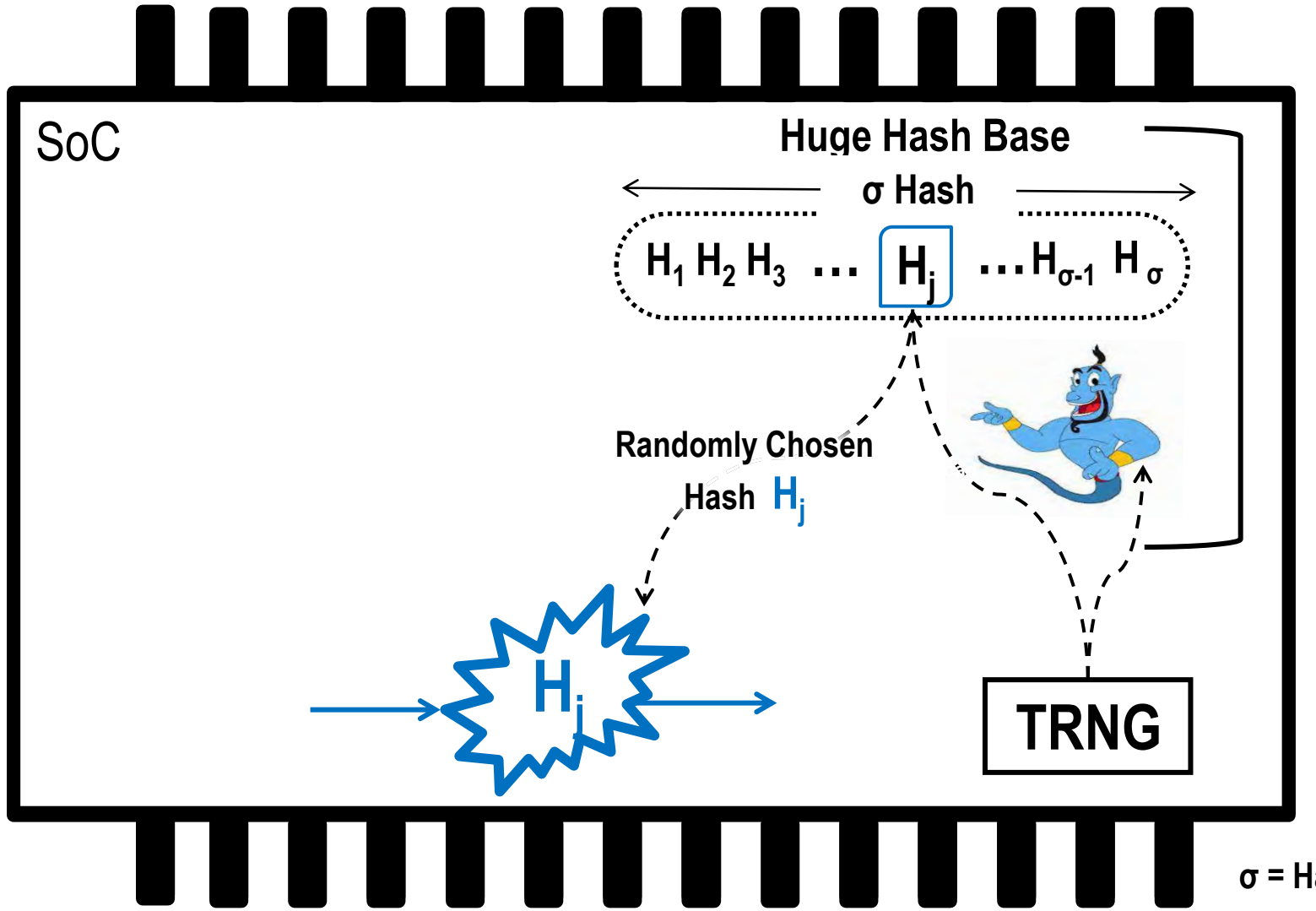
System on Chip with: Self-Reconfigurable Non-Volatile HW Fabric

σ = Hash Class Cardinality

TRNG: True Random Number Generator

Secret Unknown Hash Creation

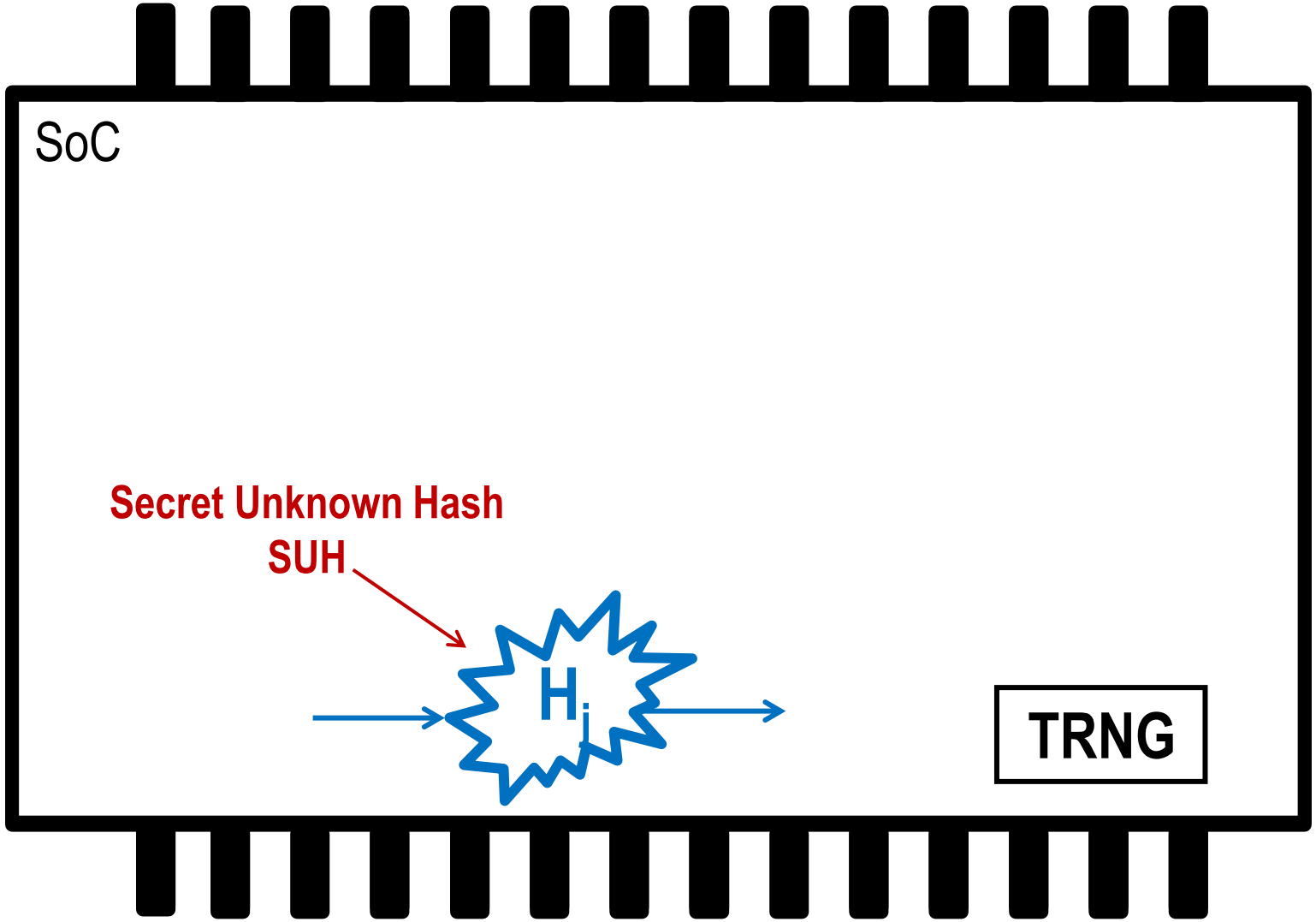
Secure Environment



System on Chip with: Self-Reconfigurable Non-Volatile HW Fabric

σ = Hash Class Cardinality

TRNG: True Random Number Generator

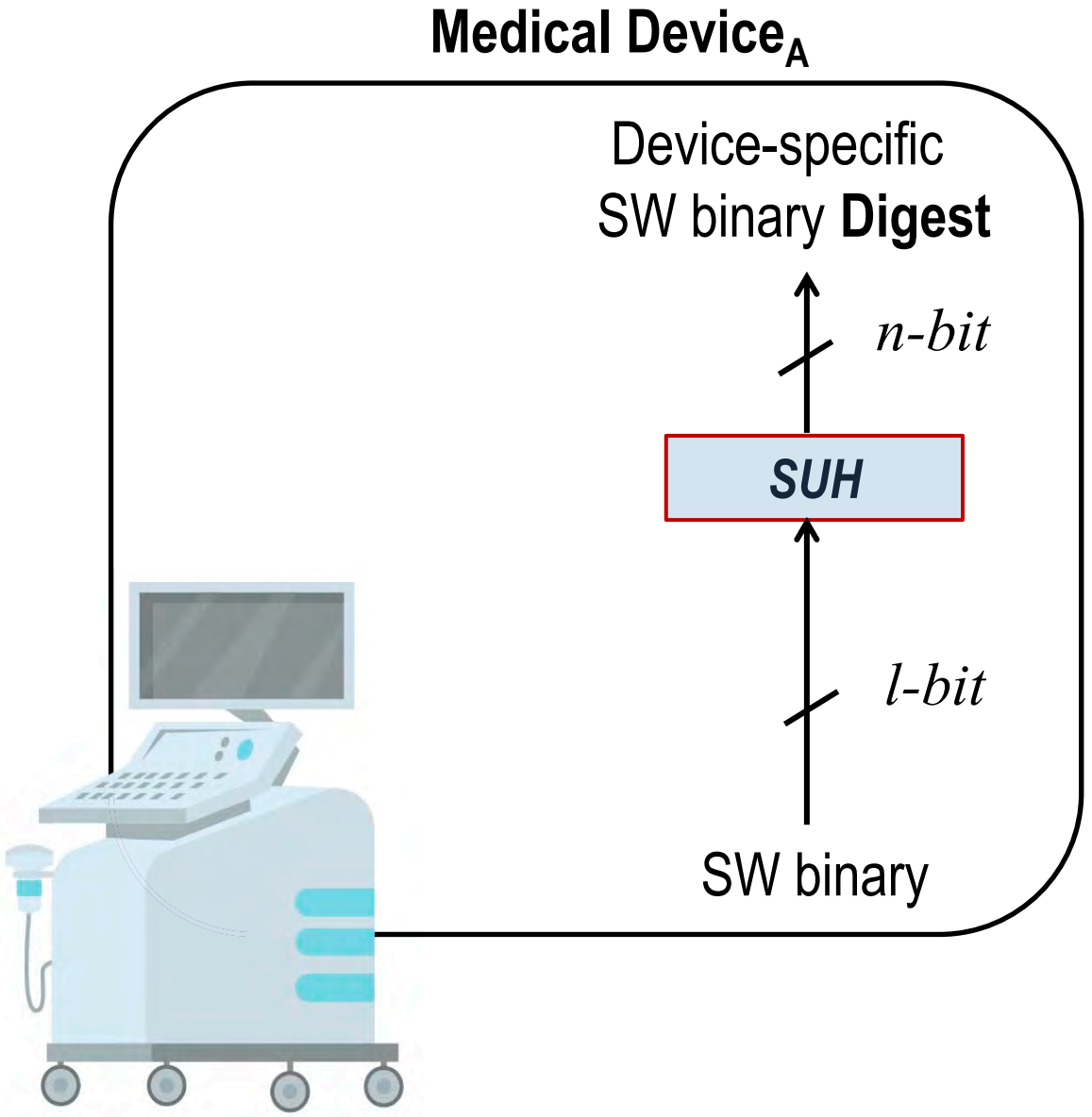


System on Chip with: Self-Reconfigurable Non-Volatile HW Fabric

TRNG: True Random Number Generator

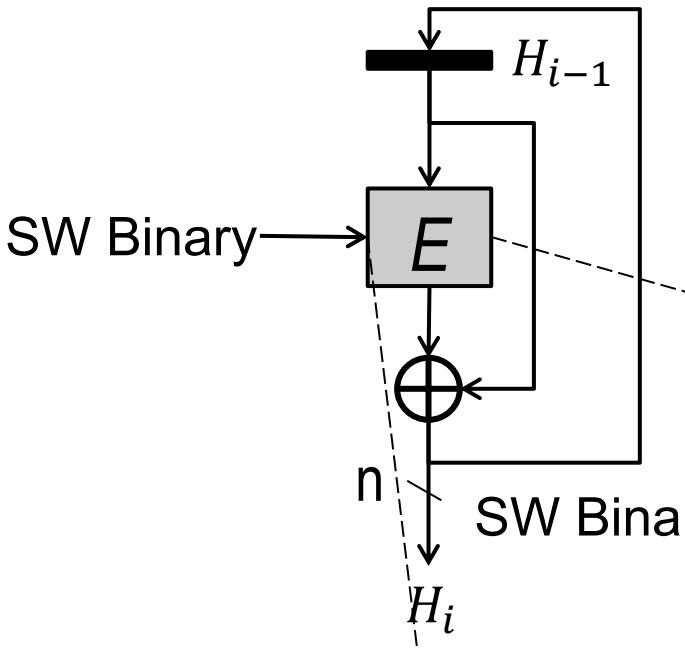
Secret Unknown Hash

- No body knows it
- Manufacturer independent
- Specific to each device
- Offers a consistent response reproducibility (Pure digital structure)



Sample Variant

Davis-Meyer scheme



Security Bound

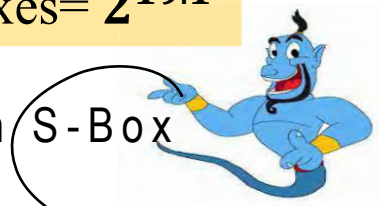
of all Possible SUH as **E= PRESENT-like**:

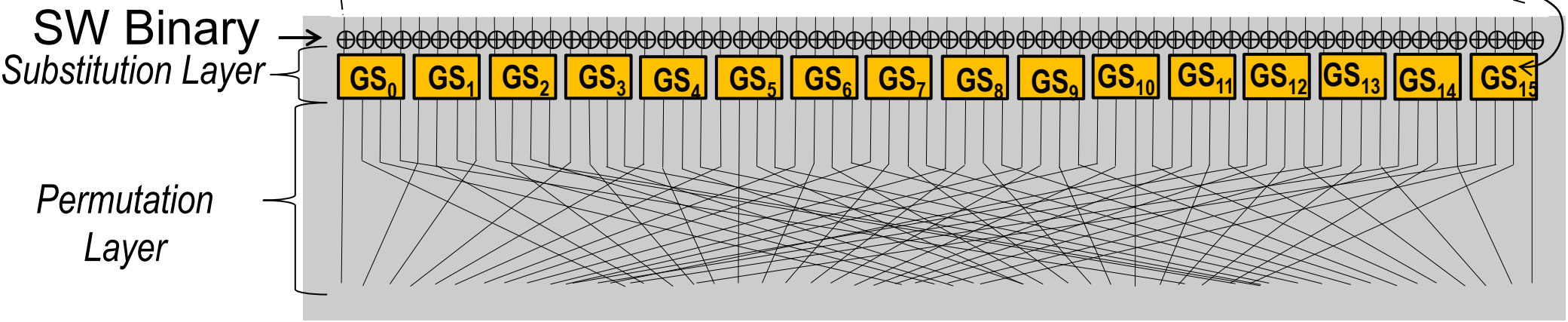
$$\left(2^{19.1}\right)^{16} = 2^{305.6}$$

Consumed resources

SmartFusion®2 SoC FPGA family	4-input LUTs	Flip-Flops
M2S005	8.67%	5.46%
M2S010	4.35%	2.73%
M2S025	1.89%	1.19%
M2S050/M2S060	0.93%	0.58%
M2S090	0.61%	0.38%
M2S150	0.35%	0.22%

# of golden Sboxes= $2^{19.1}$

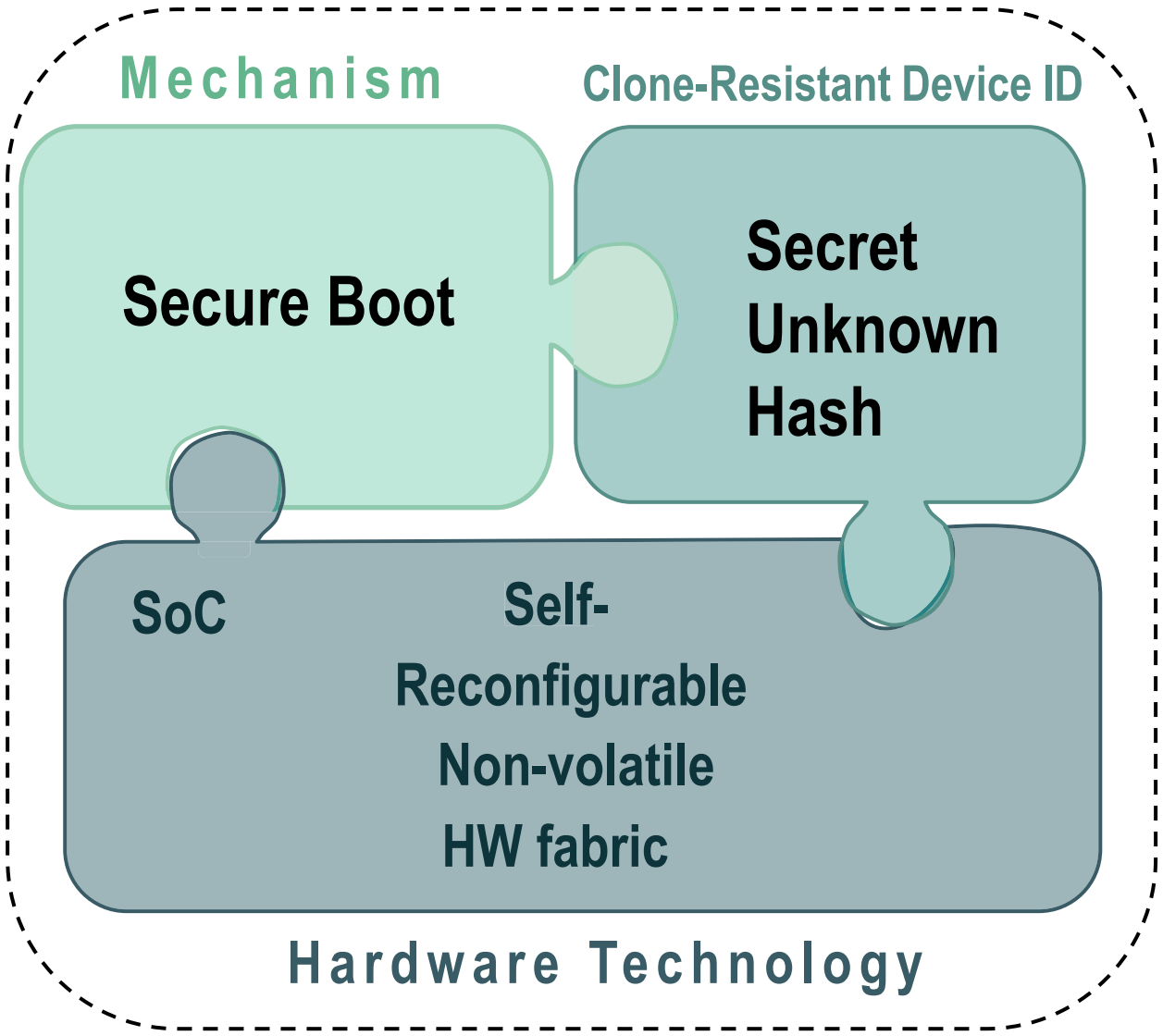




H is an n-bit length final digest. E as PRESENT-like Block Cipher

Conclusion

- Device-specific secure boot
- Highly resilient digital structures
- The clone-resistant device ID is manufacturer independent
- Scalable security level.
- SUH as low-cost Identity is practical for real field applications such as IoT applications
- SUH as a new security paradigm for reconfigurable environment



Technische Universität Braunschweig

UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR TECHNISCHE INFORMATIK

INSTITUTE OF COMPUTER AND NETWORK ENGINEERING

Clone-Resistant Secured Booting Based on Unknown Hashing Created in Self-Reconfigurable Platform

Randa Zarrouk, Saleh Mulhem, Wael Adi, and Mladen Berekovic

randa.zarrouk@tu-bs.de

International Symposium on Applied Reconfigurable Computing ARC 2021

29.06.2021

References

[1] **SRAM PUF Technology** https://www.intrinsic-id.com/sram-puf/

Freepick: https://de.freepik.com/vektoren-kostenlos/flache-artikel-set-fuer-medizinische-geraete-in-kliniken-und krankenhaeusern_11235272.htm#page=1&query=medical%20device&position=12