Clone-Resistant Structures in Microsemi SoC Units

Cryptarchi 2017

18-21 June 2017
Smolenice Castle, Slovakia

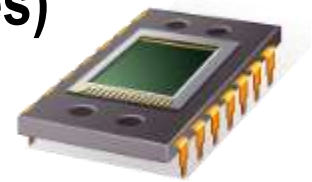
W. Adi, A. Mars

IDA, Institute of Computer and Network Engineering
Technical University of Braunschweig
Germany

Contents

Why clone-resistant physical units?

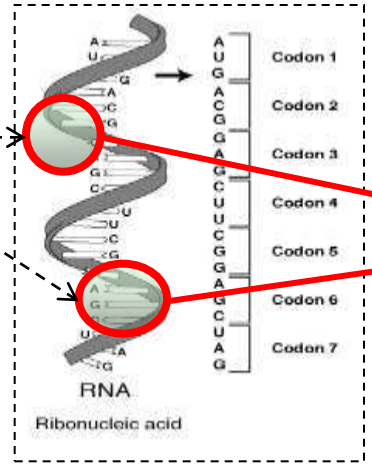
- Commercial-economic reasons (Cloning)
- Identity (Privacy)
- Know-How protection (IP-Cores)
- Medical
- Automotive units
- E-Money ….
- Smart-Home, -City, -Gouvernement, Consumer, IoT ..



Best physical Identity: As the born DNA-like provable identification

Biological DNA

Select Markers



Chemical Extractor → Chemical Markers

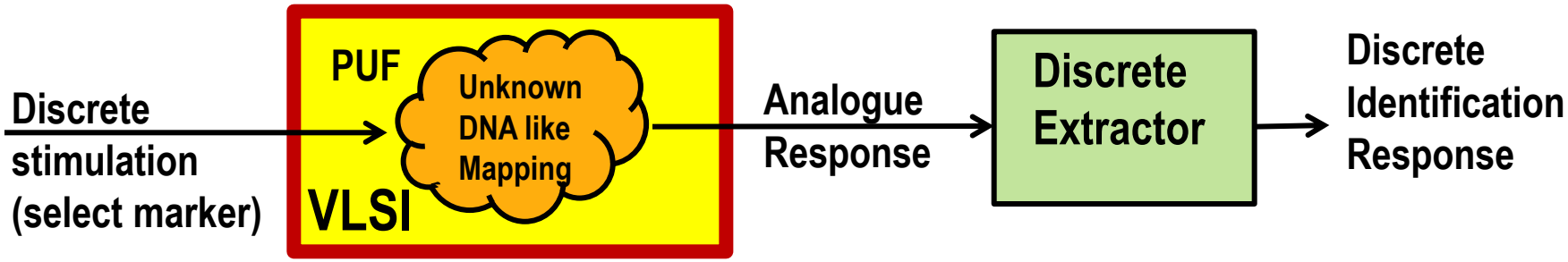
Bio DNA: 2^{48} combinations $\approx 3 \cdot 10^{12}$

Identification by matching markers

Physical Unclonable Functions PUFs offer DNA like Identification Techniques

Ideal PUFs are: Born unpredictable and unclonable physical VLSI properties.

In other words: PUFs are analogue non-linear, hard to model or to copy, unpredictable huge mapping in a semiconductor VLSI device

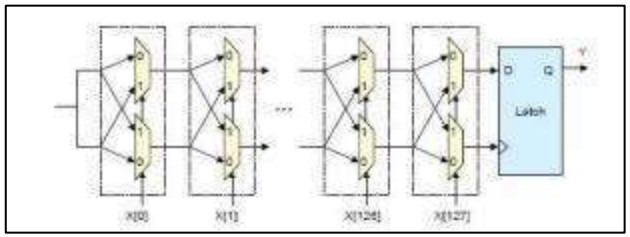


State of the Art: Unclonable Devices by:
Analog Physical Unclonable Functions (PUFs)

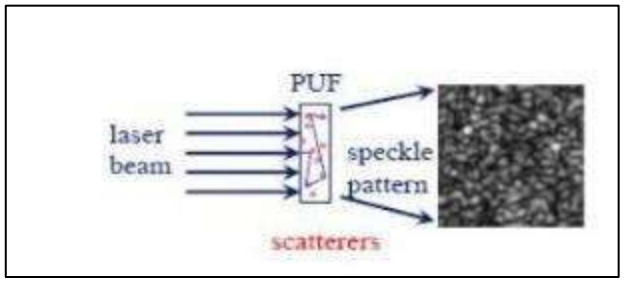
Since 2000 many proposals

optical PUF
coating PUF
Silicon PUF
optical fiber PUF
RF COA
LC-PUF
S-RAM PUF
Arbiter PUF
fluorescent PUF

Unclonable
DNA-Chain



Delay based



Optical

Delay PUF
Butterfly PUF
diode breakdown PUF
reconfigurable PUF
acoustic PUF
controlled PUF
phosphor PUF
...

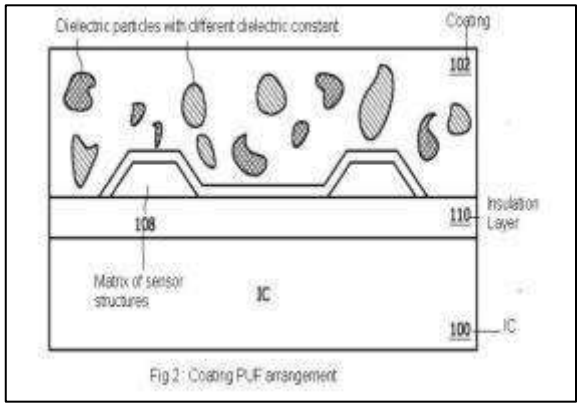


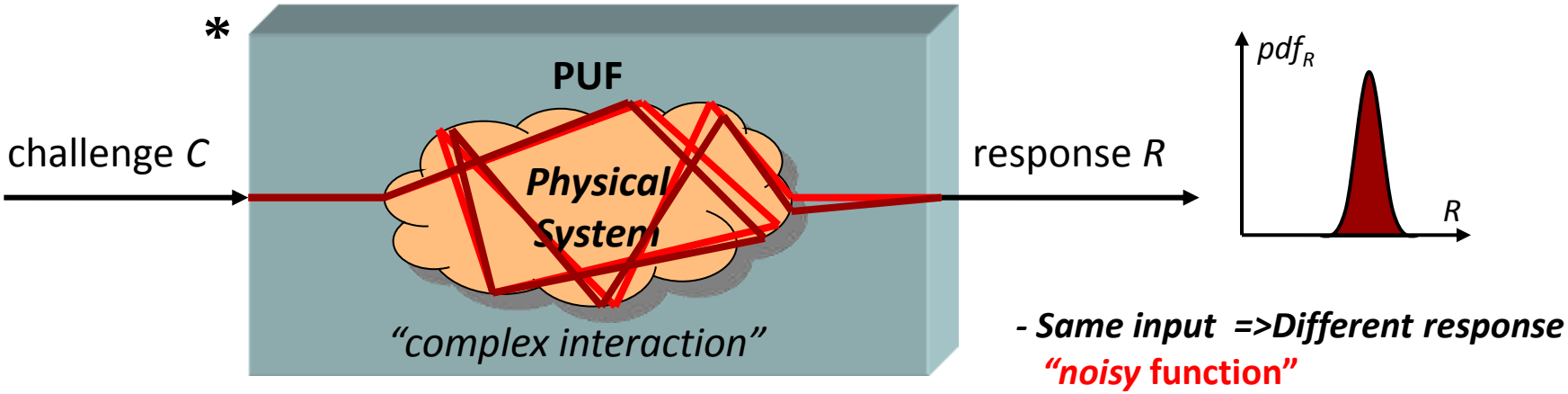
Fig 2: Coating PUF arrangement

Coating PUF (Capacity)

So far all have "Reproducibility" problems!
Analog functions!!!

Born properties: Similar to the biological DNA

PUFs inconsistency and aging difficulties



- ***Same input =>Different response***
  "noisy function"

Bad reproducibility due to : Operating conditions, quantization (Metastability) , Aging, …

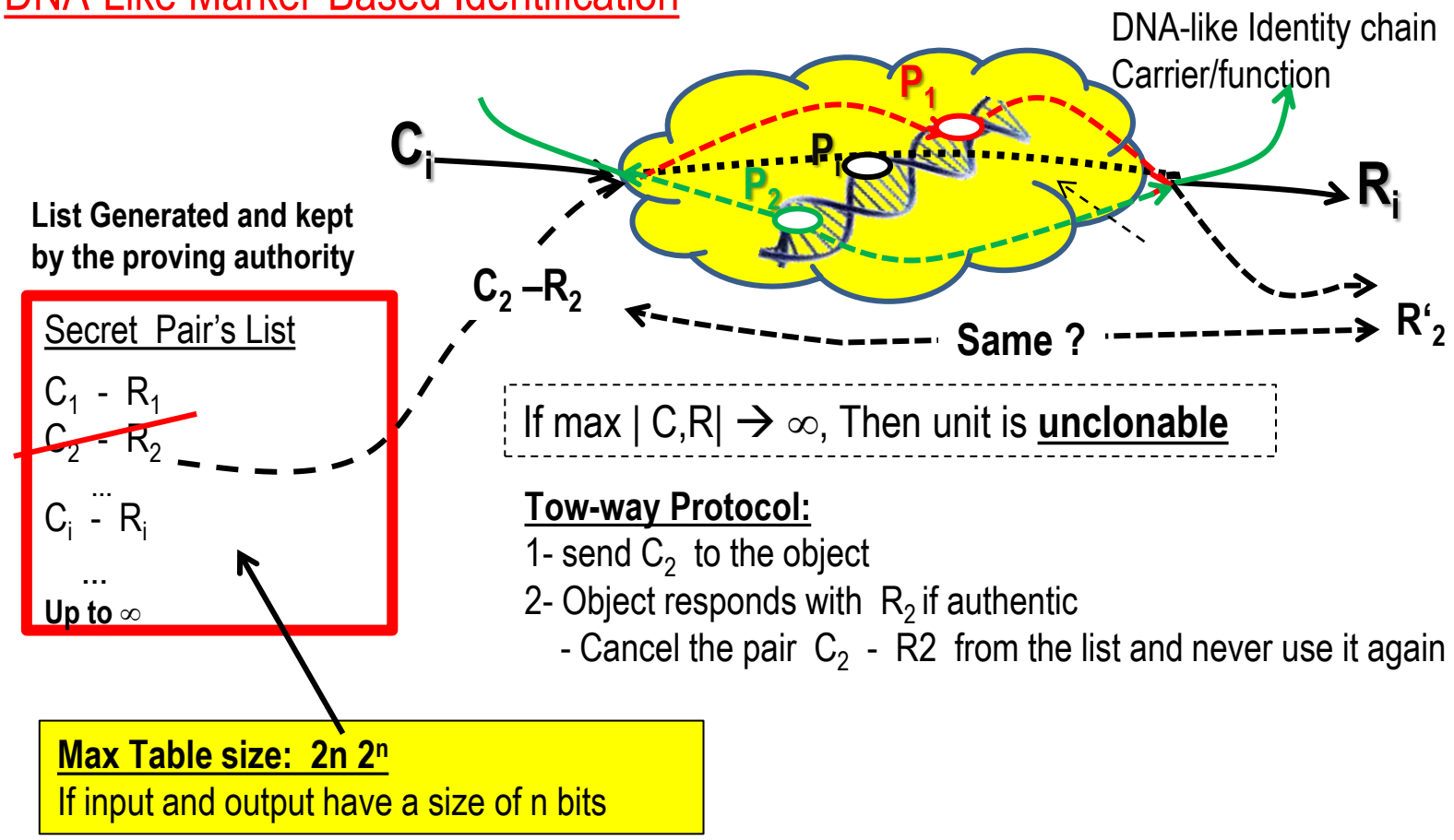
Fuzzy Extractors: Complex, Costly (Sign. Proc + ECC)

*** Source: Roel Maes, ESAT/COSIC, K.U.Leuven, BCRYPT Workshop:**

Bio-Inspired Identification Protocol

DNA-Like Marker-Based Identification

DNA-Like Marker-Based Identification



Our Proposal:

1. Avoid analog-world
   and use pure digital structures
   => 100% reproducibility, no aging!
   => Resilient/robust Identification Technology
   => Target cost → 0

2. Accept less strict security requirements
   for mass consumer products.

Less-strict security requirements

Pragmatic Security for mass products:

- System is considered as clone-resistant if:
  - Cloning do not economically pay off
  - Cloning is useless after some time

Security Requirements

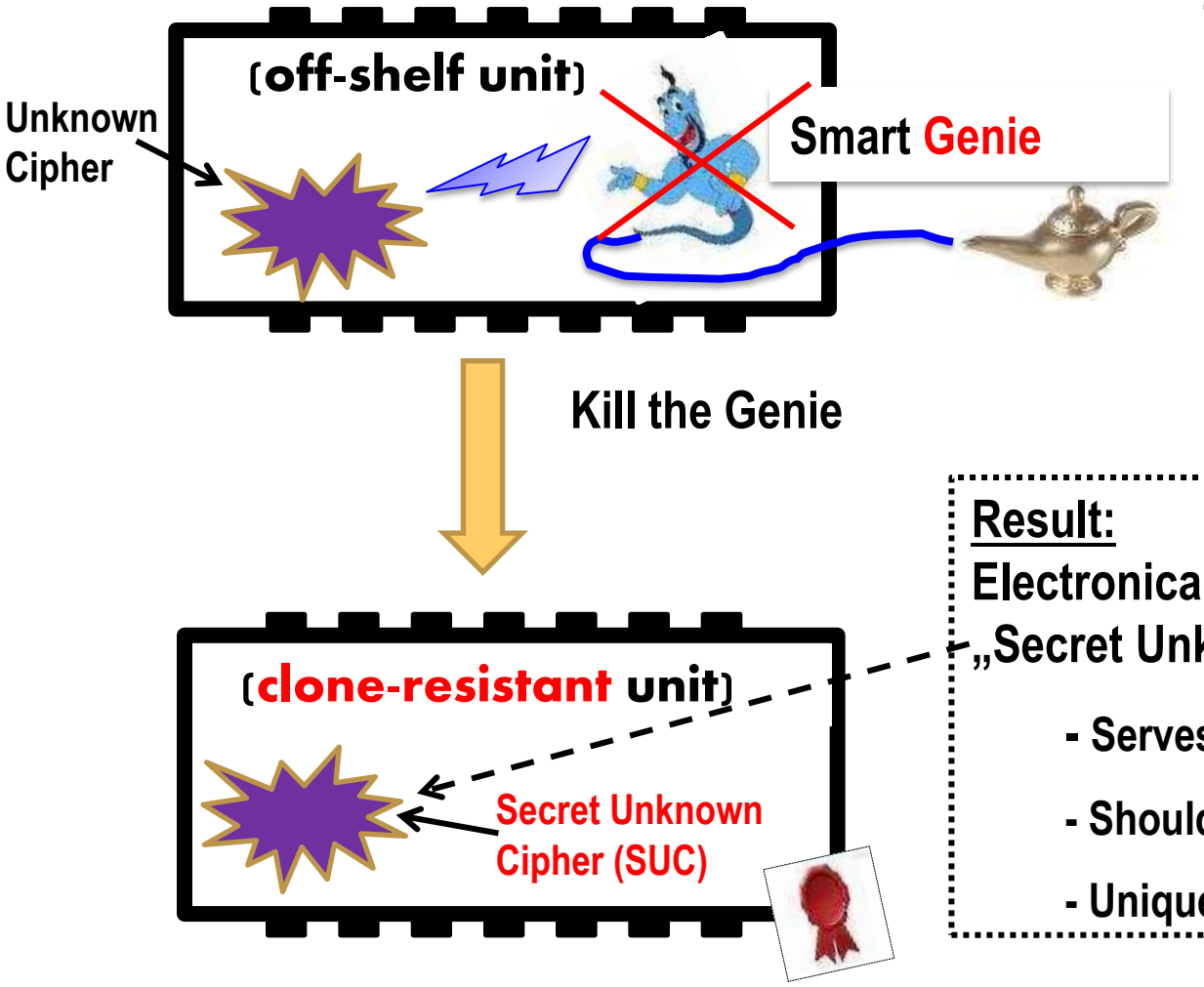
- Enforce attacker to do expensive physical invasive attacks
  ⇒ System should be side channel attack resistant

- "Break-one break-all" should be hard or impossible
  ⇒ Each unit is individually unique

Target applications: Mass-products, Automotive .. Consumer, Smart phones

Key Idea: Electronic DNA-Mutation!

In Post Fabrication: "Mutating a digital "Secret Unknown Cipher" (SUC)



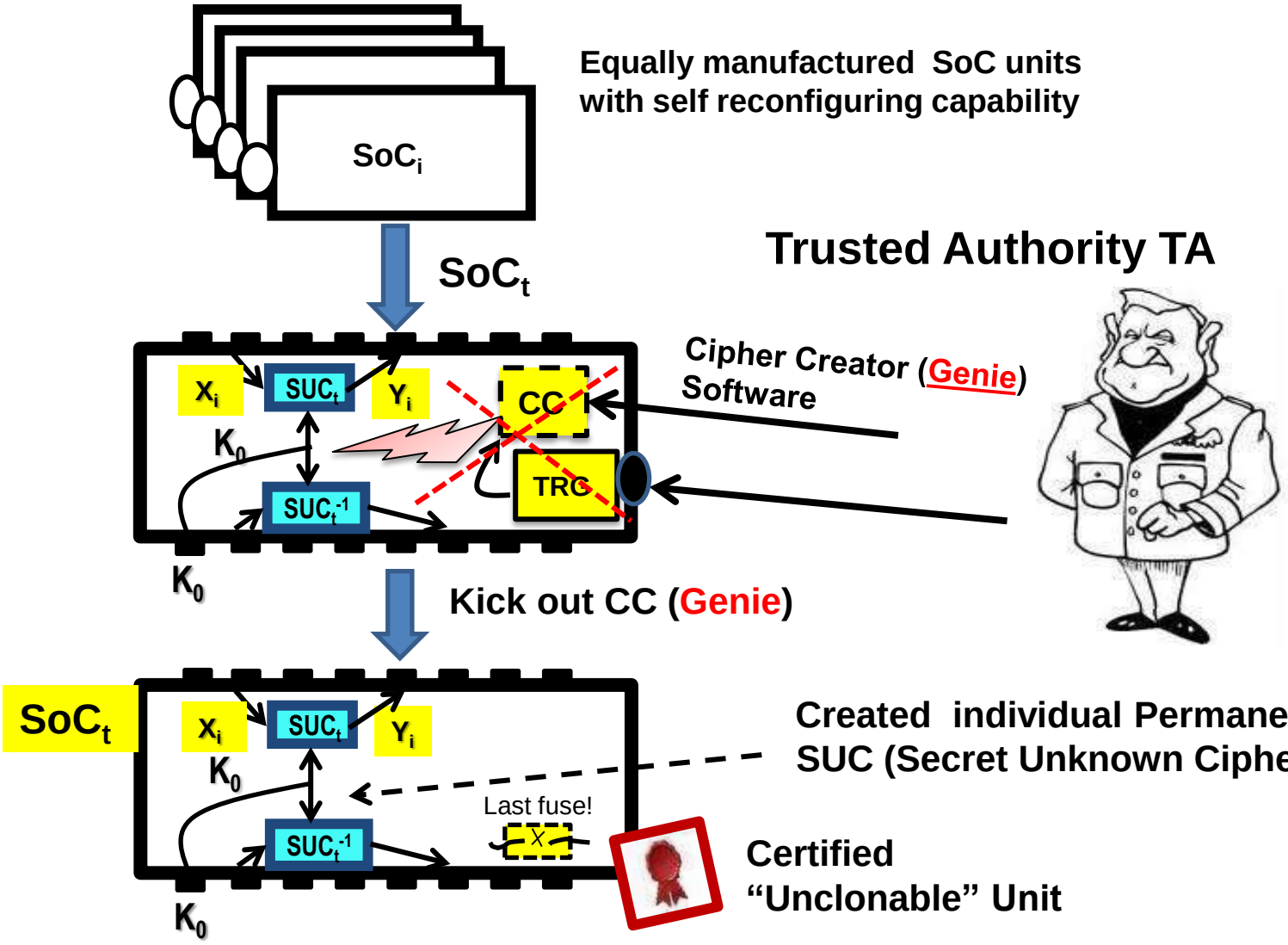
Result:

Electronically mutated (e-Mutation) „Secret Unknown Cipher" (SUC)

- Serves as electronic DNA (e-DNA)
- Should be permanent! (MICROSEMI)
- Unique for each unit!

Production Procedure: in post fabrication

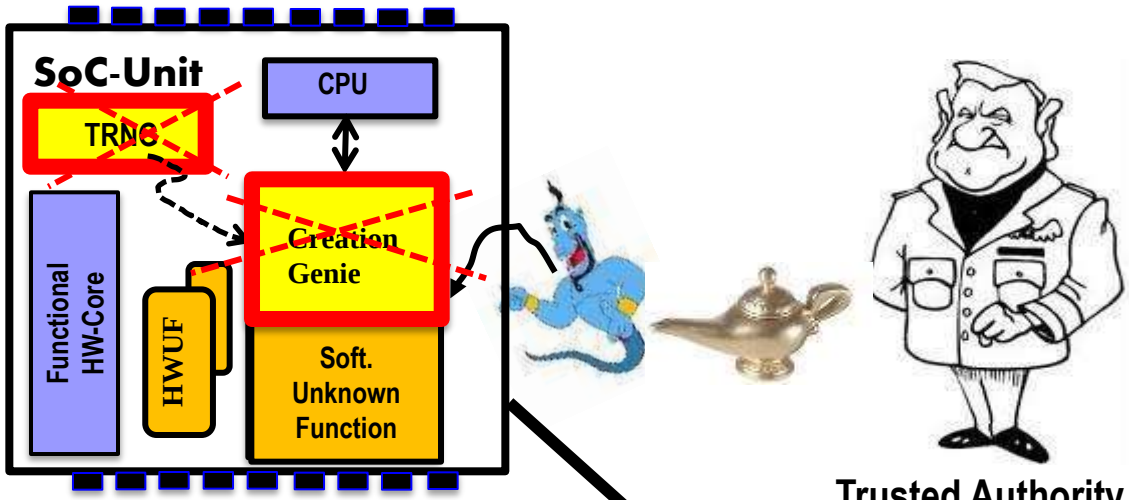
"Mutate SUC"



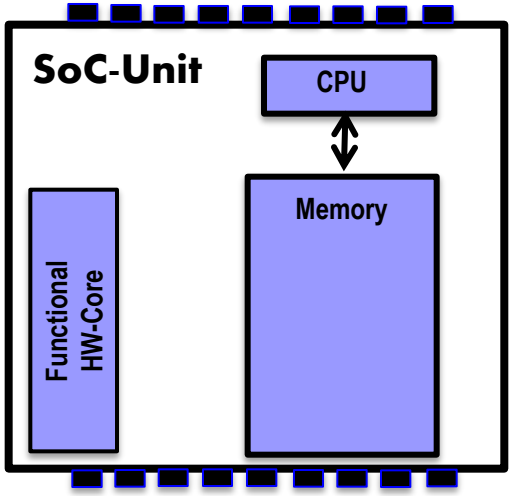
Possible SoC Scenario

Possible system concept
to mutate operational unknown
functions in a SoC unit

Smart Genie requires Powerful computational infrastructure!

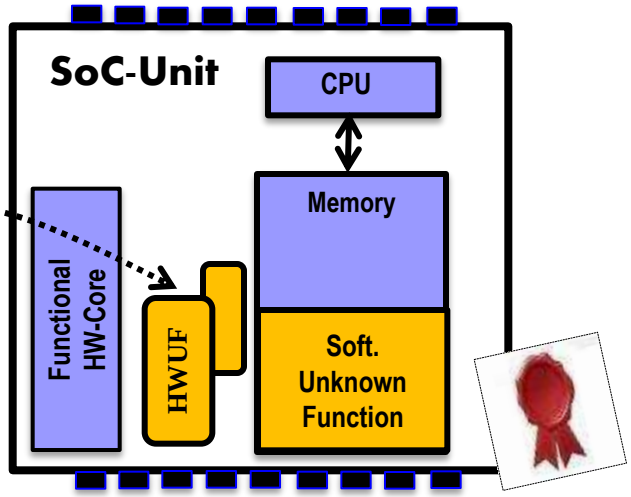


(Single-event Enrollment Process)



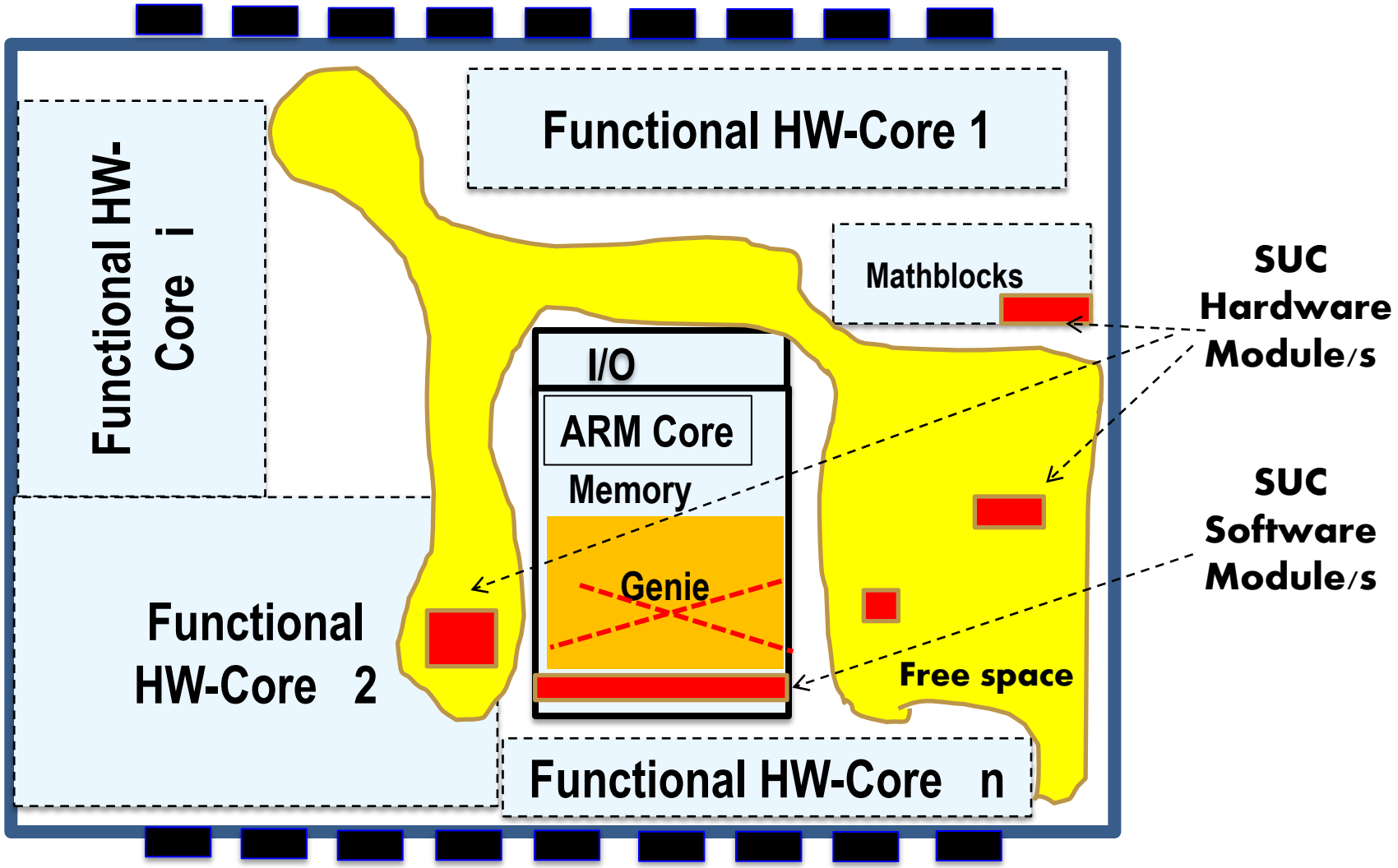
Off-Shelf SoC Before (SMART MOBILE)

Created Unknown Soft and Hardware Functions

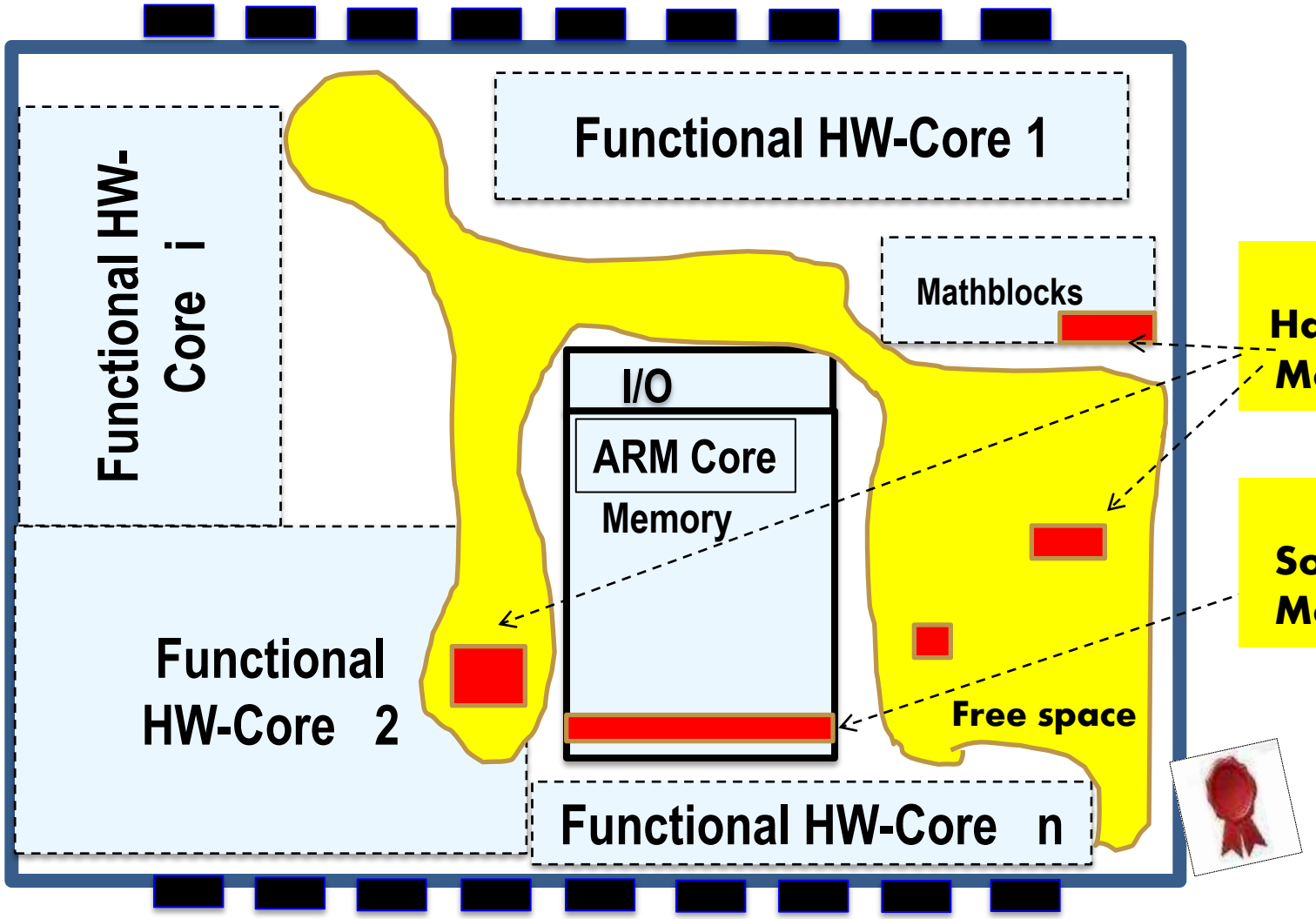


SoC (SMART MOBILE) After

SUC Prototype in SmartFusion2 SoC FPGA

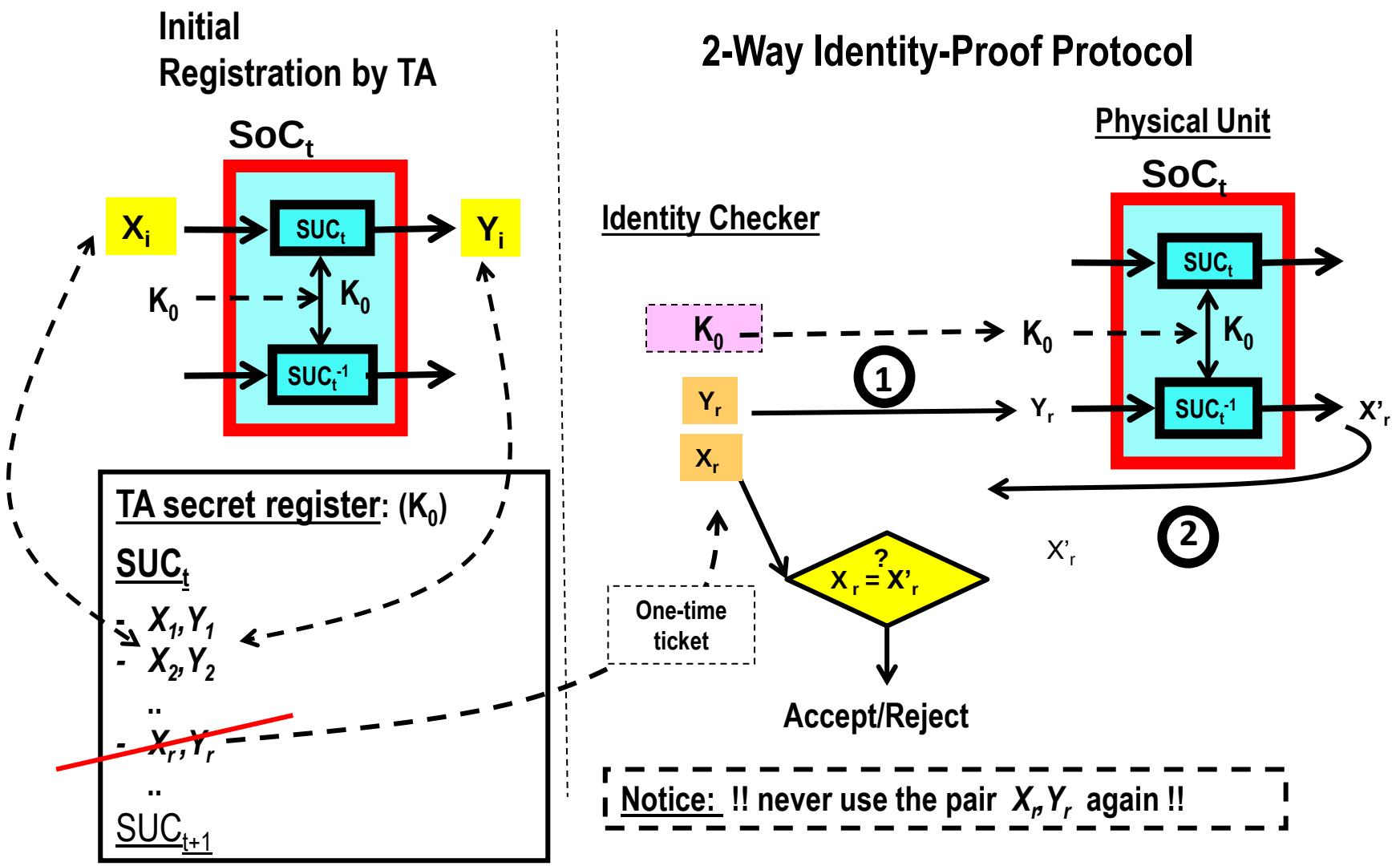


Clone-Resistant SoC FPGA Unit



Identification Protocol with a SUC

What can you do with a cipher which nobody knows?



Q: Is the system realizable today?

- **In ultimate form , No!** (Emerging .. Technology)

  Reason: non-volatile self reconfiguring hardware in SoC architecture is not yet available

  However: ***"Microsemi non-Volatile technology"*** **(Actel) is a possible future emerging technology therefore**

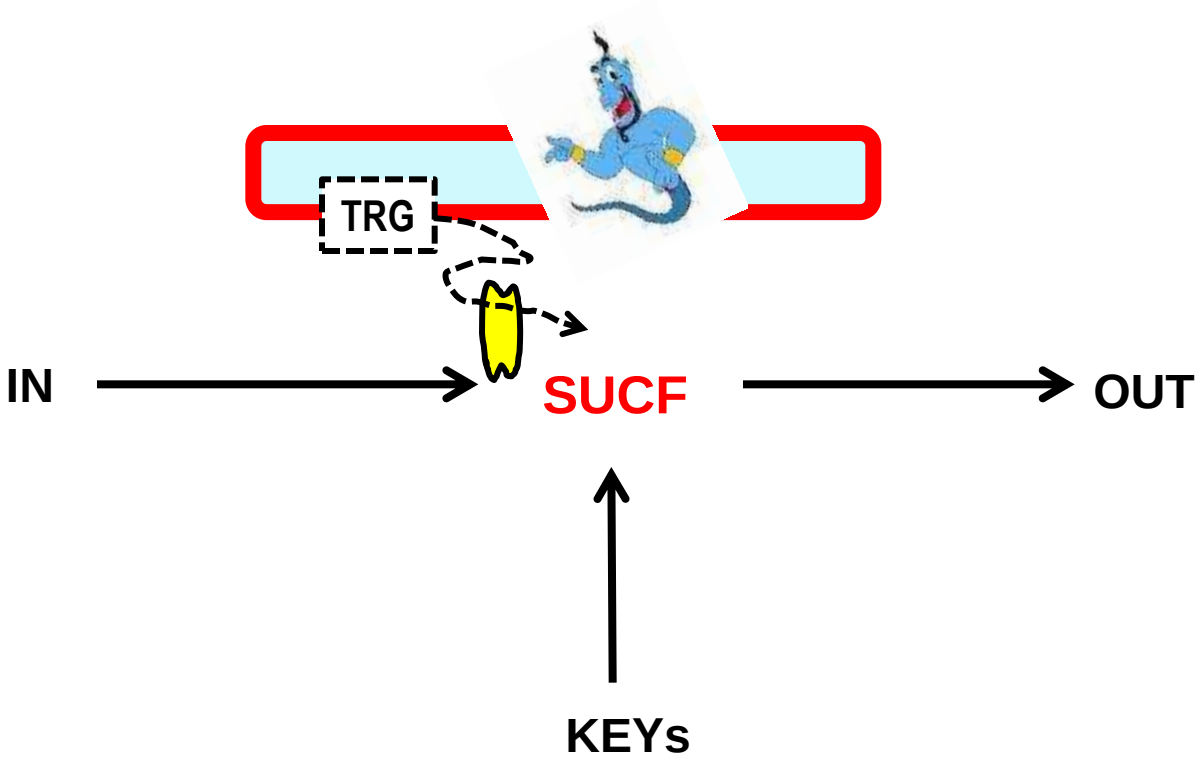
Alternative "Pure Software" solution?:

"ARM SoC" architecture is a possible infrastructure
However less secure, low-cost soft version (in Smart phones)

Generalized Concept of Unknown Secret-key Crypto as Clone-Resistant Mutated Digital E-DNA Functions

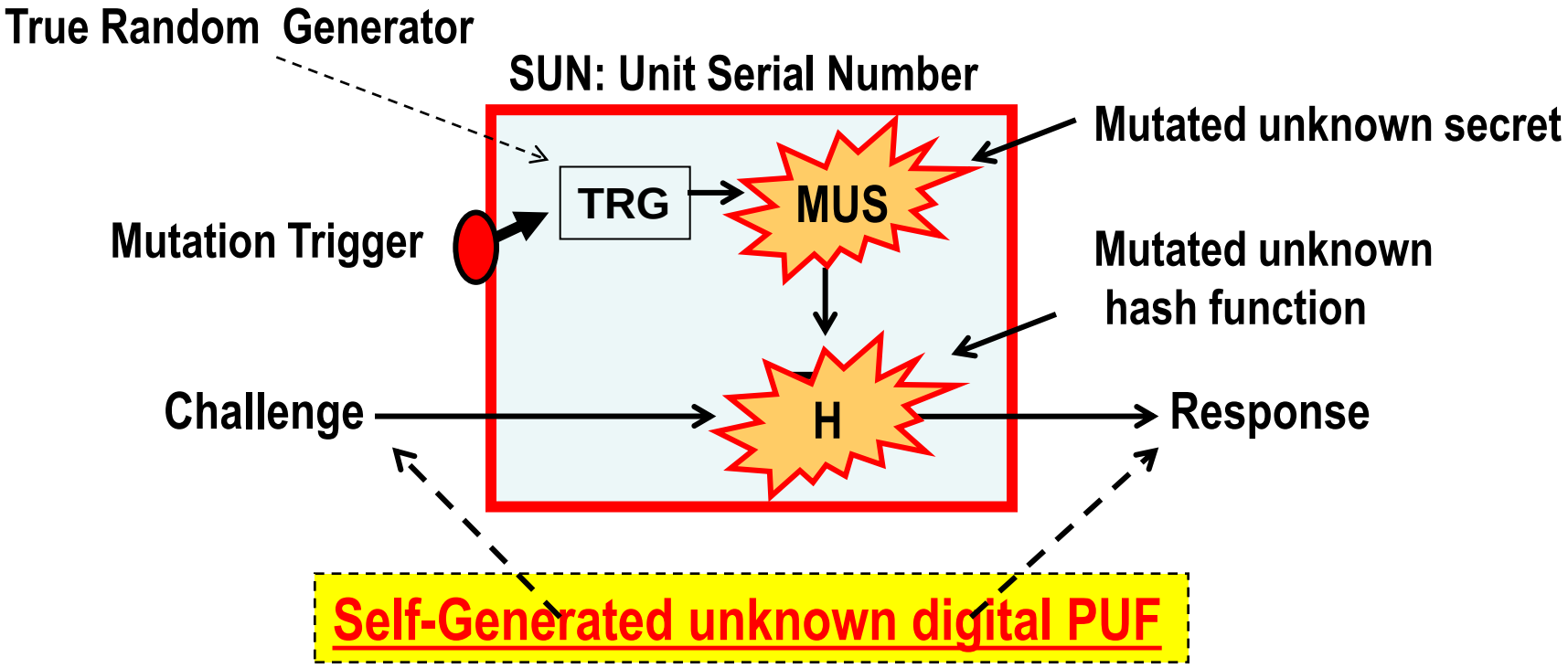
Created Functions

Secret Unknown Crypto-Functions" SUCF



Use Case 1: Mutating Unknown Hash & key

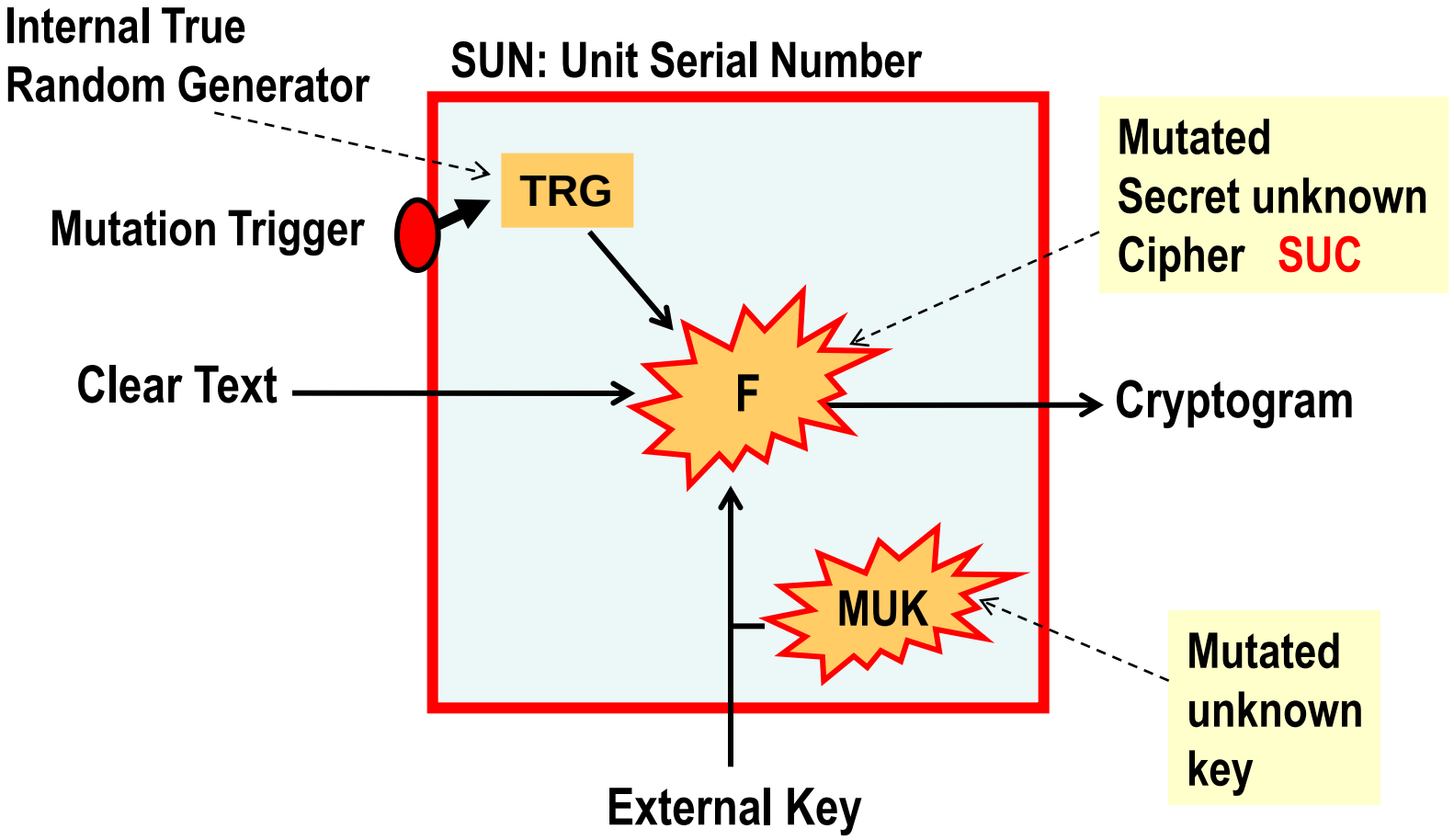
Mutated secret identity



In comparison: Analog PUF: Space size → ∞ (theoretically perfect)

Digital PUF : Space size → finite (theoretically not perfect)

Use Case 2: Mutating Unknown Secret Physical Cipher



The only perfect secret is the one which nobody knows!

Sample Implementation Case

SUC in Microsemi SmartFusion®2 SoC FPGAs

Ultimate SUC

"is not Realizable"

in Contemporary Technologies!

Why?:

1. No self-reconfiguring non-Volatile Technologies
2. Bitstream Format is not disclosed
3. Bitstream is encrypted

First Pragmatic Implementation Scenario:

Concept:

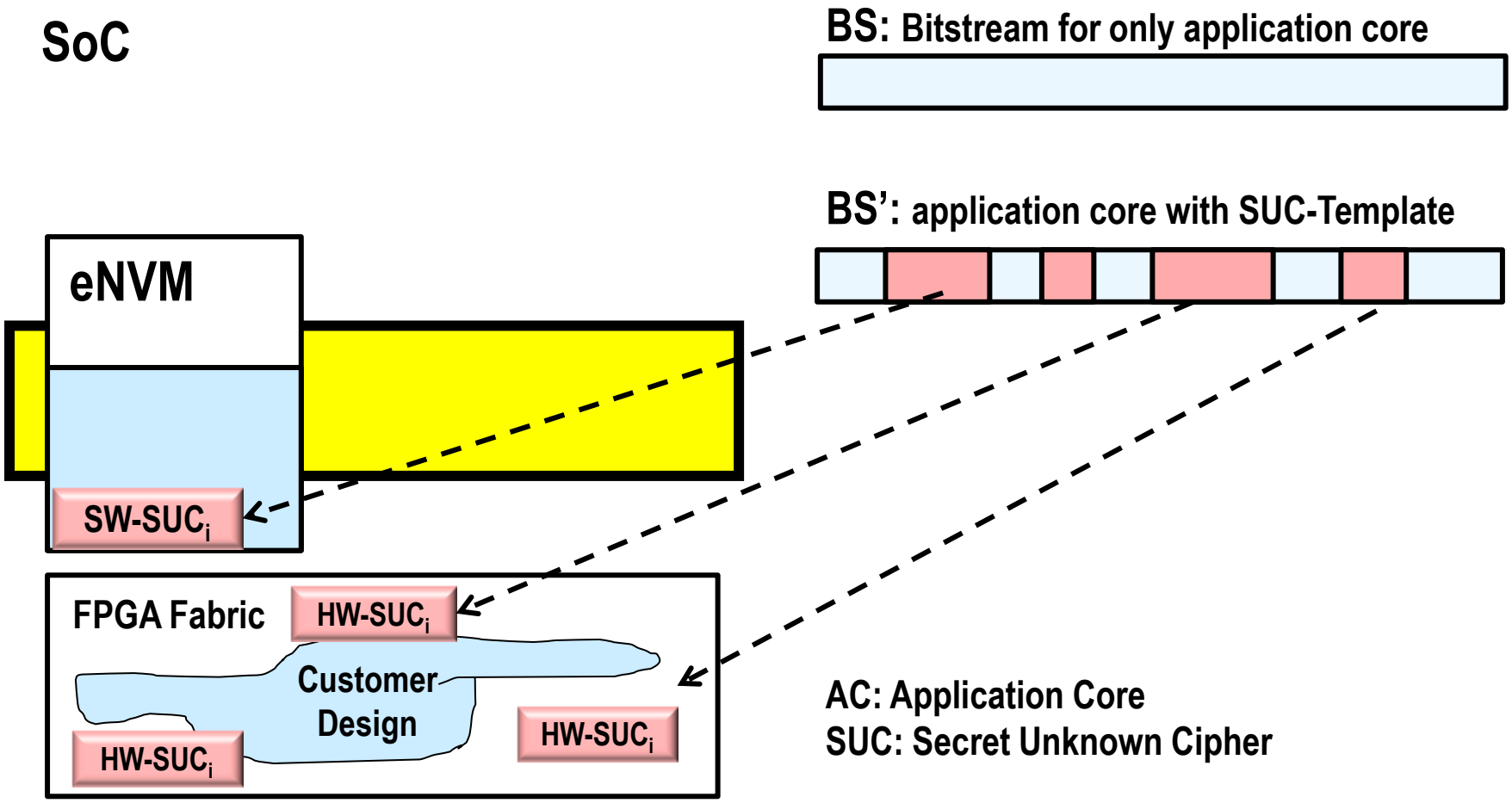
1. Use existing technologies
2. Accept lower security

Note:

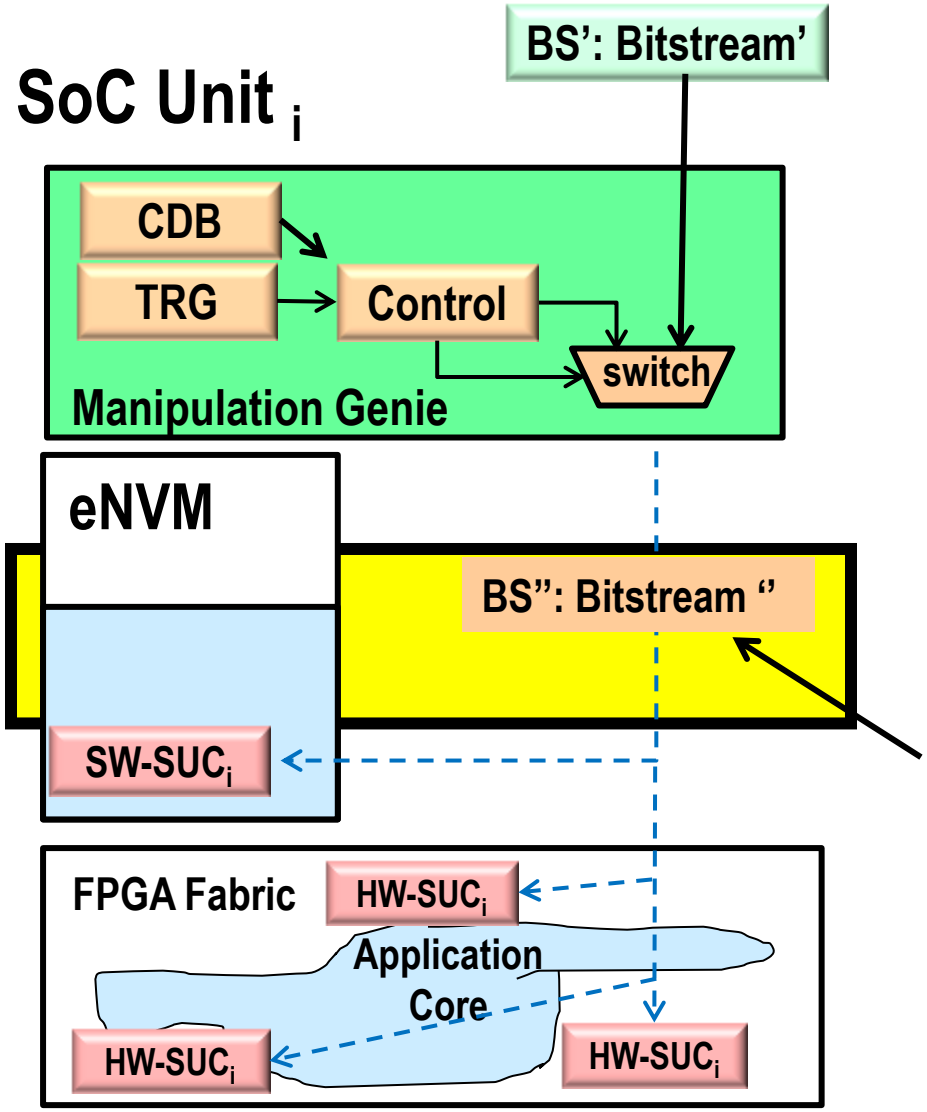
Self-Reconfiguring "Volatile Technologies" do exist, however result with quite weak security for unclonability

Prototyping Key Idea: (realizable if Bitstream encryption is switched off)

Step-1: Creating SUC as a "Hardware Layout Template"



Prototyping Key Idea: Step-2: Template personalization



Initial setup:

- Create a SUC template in SoC,

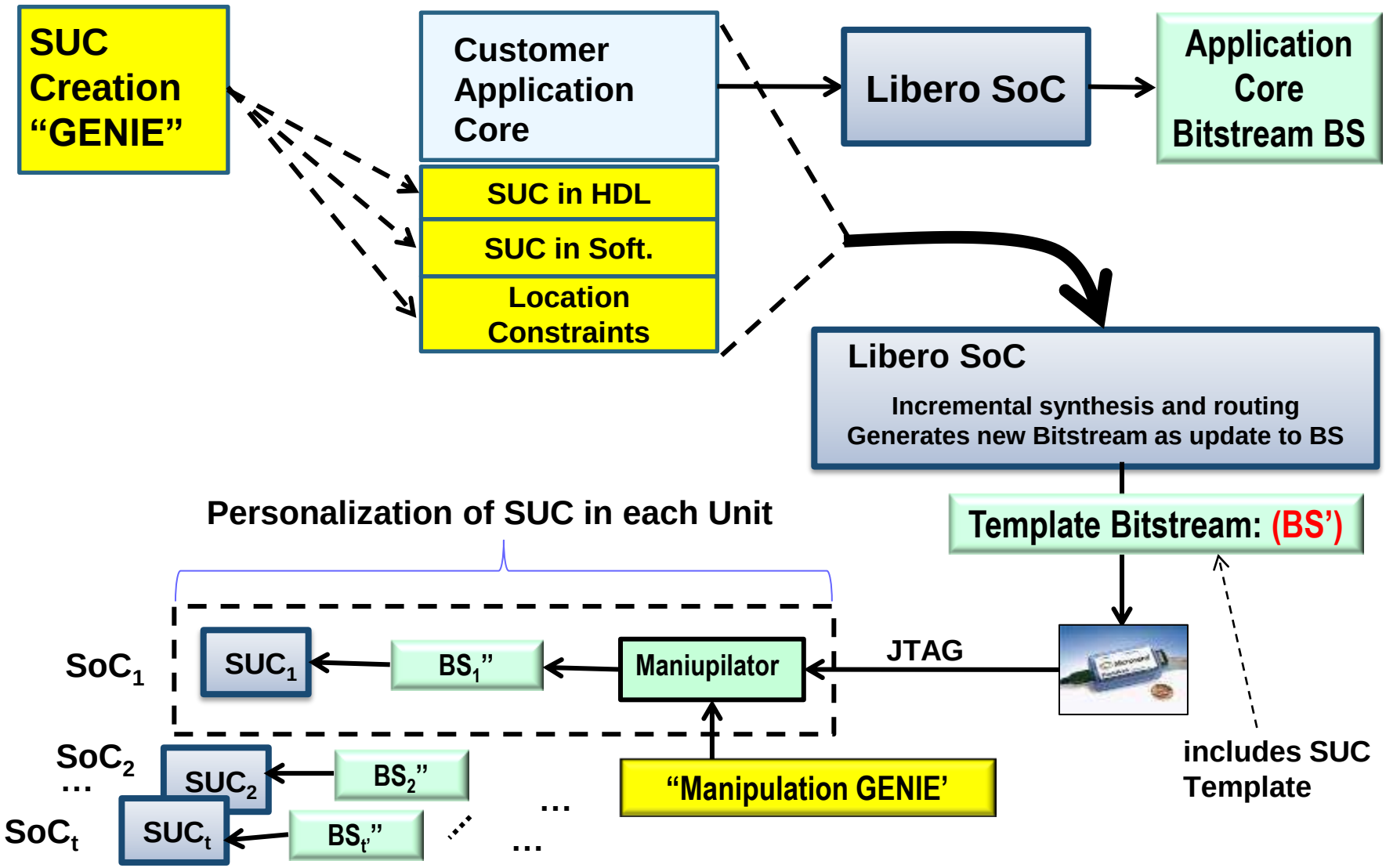
Personalize Units by a Manipulation GENIE!:

1. Trigger GENIE' by a random stream of bits from the TRG
2. Chose randomly some mappings from the cipher data base (CDB)
3. Manipulate the configuration bitstream BS' accordingly
4. After completing the SUC personalization, the GENIE' is deleted (killed)

BS": Bitstream after personalization

AC: Application Core
CDB: Cipher Data Base
TRG: True Random Generator
SUC: Secret Unknown Cipher

Design Flow for Creating SUC in Microsemi SoC FPGAs:



Actual SUC Implementation in non-volatile SoC FPGAs:

GENIE

Smart program

PRNG

SUC Creator

Design Constraints

SW Design "SW_UF"

HW Design "HW_UF"

Generate Configuration Bitstream for "…/SUC"

Libero SoC Generate bitstream

SofConsole Folder

Constraint Folder

HDL folder

Constraint Folder

Configuration Bitstream

Libero SoC Project: …/SUC

MSS

SW_UF

FPGA Fabric

HW_UF

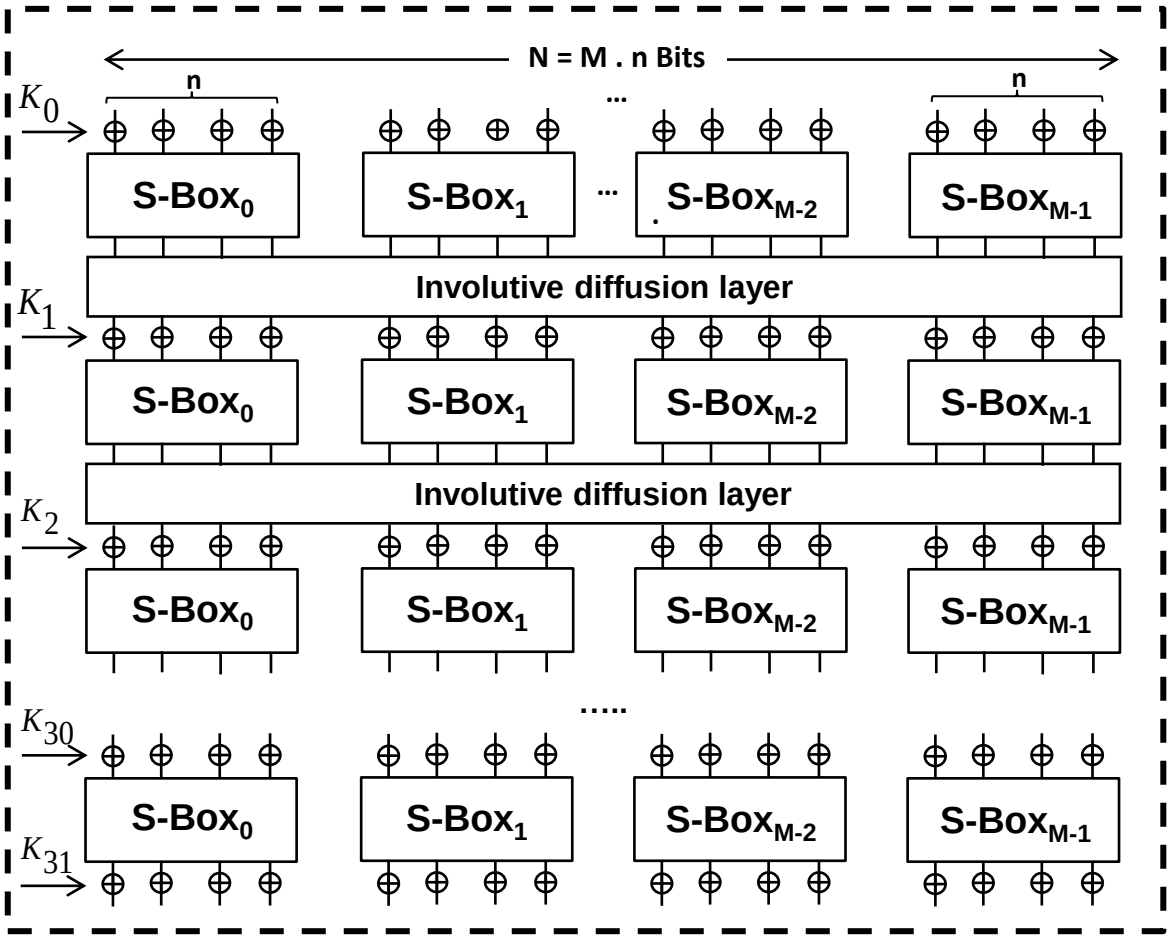
SoC FPGA

Trusted environment

Proposed Randomized Involution Block Cipher as SUC:

Requirements: Secure design, lightweight, involutive, and random cipher

proposed SUC : has a block size N=64 bits and 32 rounds



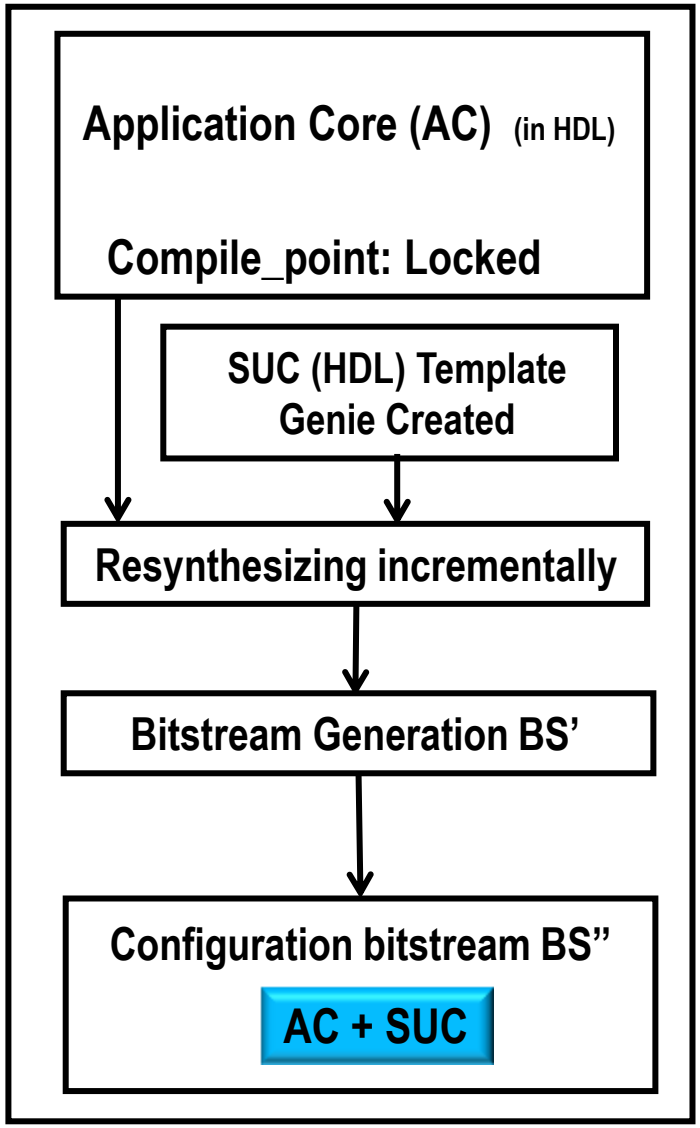
Cipher Cardinality:

- The cardinality of this class of random cipher is 2^{274}

Attack complexity:

- Linear cryptanalysis: $\geq 2^{80}$
- Differential cryptanalysis: $\geq 2^{80}$

Soft-Design flow: Incremental SUC Synthesis and Routing



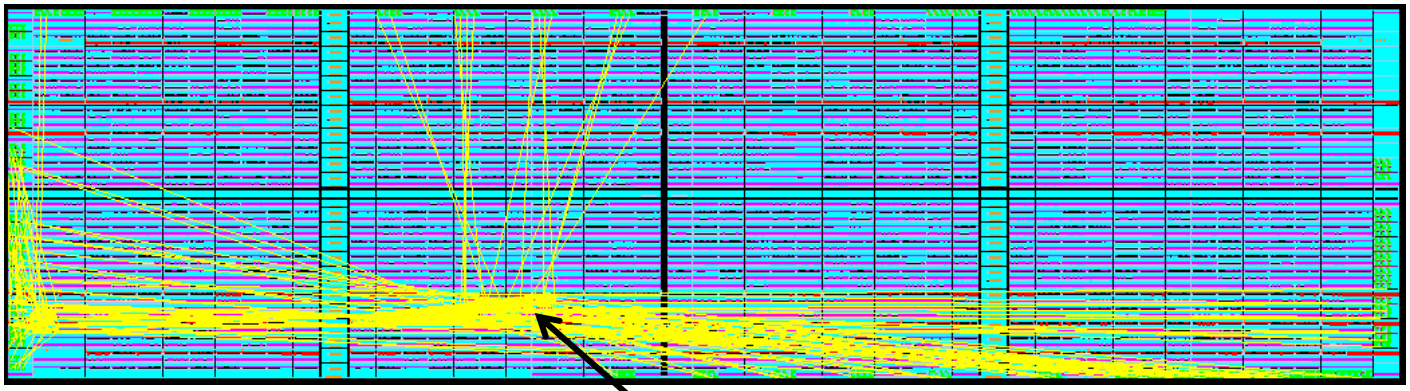
- Compile points are RTL partitions of the design that you define before synthesizing the design
- Each compile point is treated as a block

  → Independent synthesis, optimization and place and route

- The SUC design template can be added to locked Application Core,
- The software will treats separately the SUC design which will reduce the time required for personalization

Sample Layout: By incremental synthesis and routing

Complete layout



Pure SUC portions and their locations

Hardware complexity:

The following table presents the hardware complexity of SUC (in percent) for different SmartFusion®2 SoC FPGAs Families

Gate Complexity: 213 LUTs + 72 DFFs

SmartFusion2 SoC FPGA Families	*Resources usage*	
	LUTs % of usage	*DFFs % of usage*
M2S005	3,51	1,19
M2S010	1,76	0,6
M2S025	0,77	0,26
M2S050	0,37	0,12
M2S060	0,37	0,12
M2S090	0,24	0,08
M2S150	0,14	0,04

Summary of the First SUC Prototyping

Concept:

1. Template based
2. Fixed cipher architecture
3. Only mapping-contents are variable
4. Low Complexity. Very high personalization speed

Disadvantages:

1. Attacker knows the structure
2. Attacker knows the physical locations
3. No crypto-mappings diversity (fixed template!)

However,
overall security level is still relatively: "Very good"

CONCLUSIONS

- Relatively low-cost pure Digital PUFs (in best case "zero-cost")
- "Highly robust digital physical identity"
  (compared to analog PUFs !)
- Negligible aging!
- Scalable security level!.
- System inherently more resistant to „Side Channel Attacks"
- Security is, manufacturer and trusted authority independent

Work in Progress:

- Investigating new "GENIEs", operation scenarios and use protocols
- Practical real field applications,
- Task is multidisciplinary and challenging!

Thanks