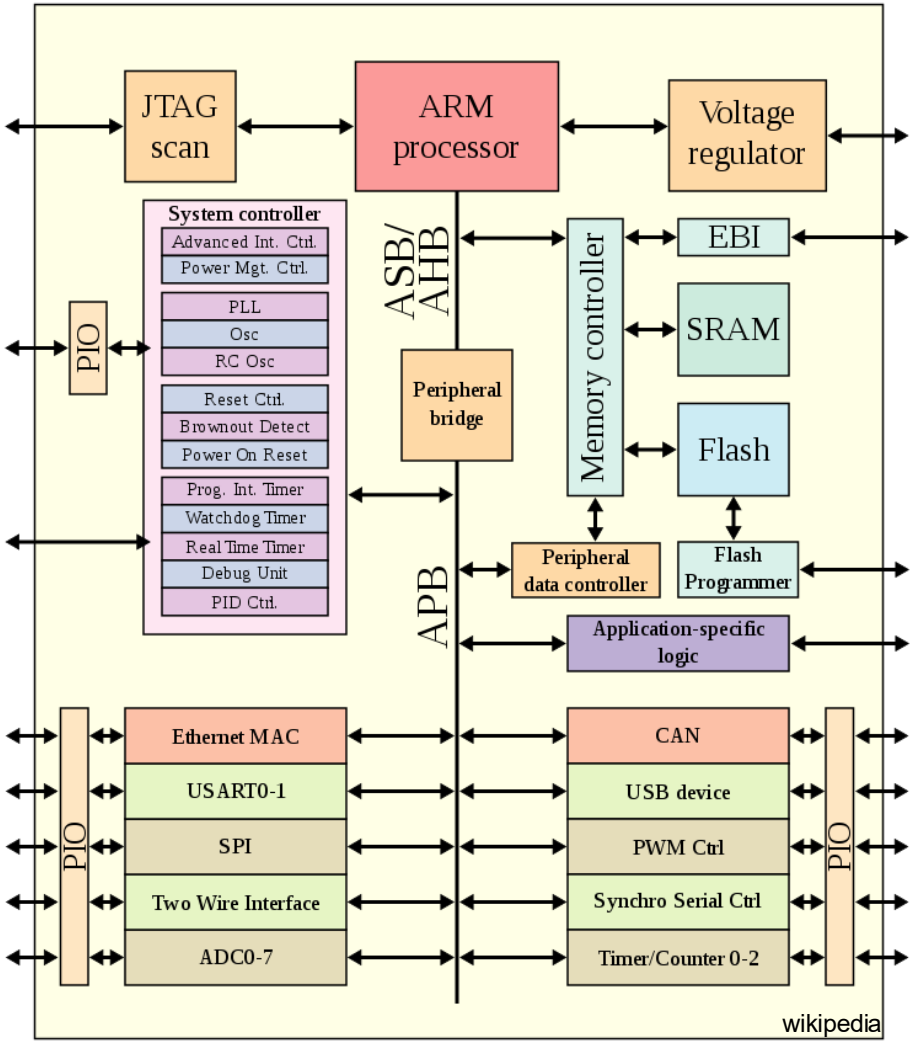
SAP: Silicon Authentication Platform for System-on-Chip Supply Chain Vulnerabilities

Authors: Md Sami Ul Islam Sami, Jingbo Zhou, Sujan Kumar Saha, Fahim Rahman,
Farimah Farahmandi, Mark Tehranipoor

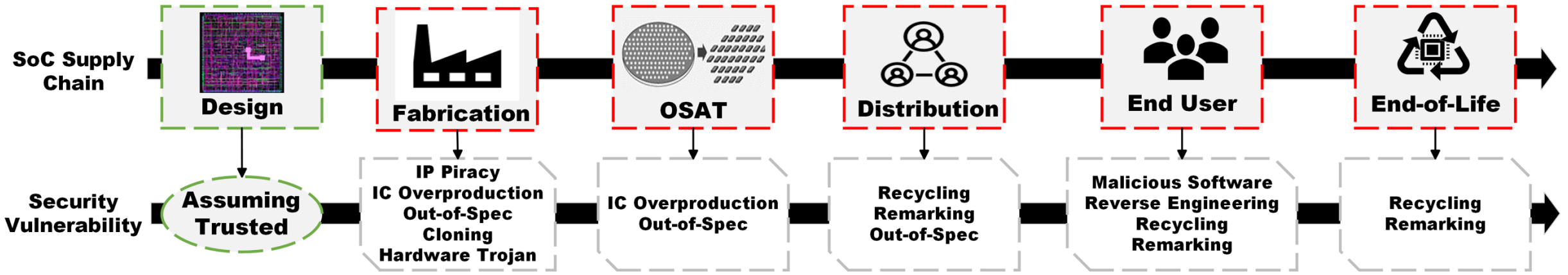
Presented by: Md Sami Ul Islam Sami

Motivation

- **Relentless drive towards accommodating more functionalities in SoC designs.**
- **Increased reliance on external sources worldwide.**
  - Third-party IP vendors,
  - Offshore fabrication, and
  - Outsourced semiconductor assembly and testing (OSAT) entities
- **SoCs contain diverse security assets to perform cryptographic operations.**



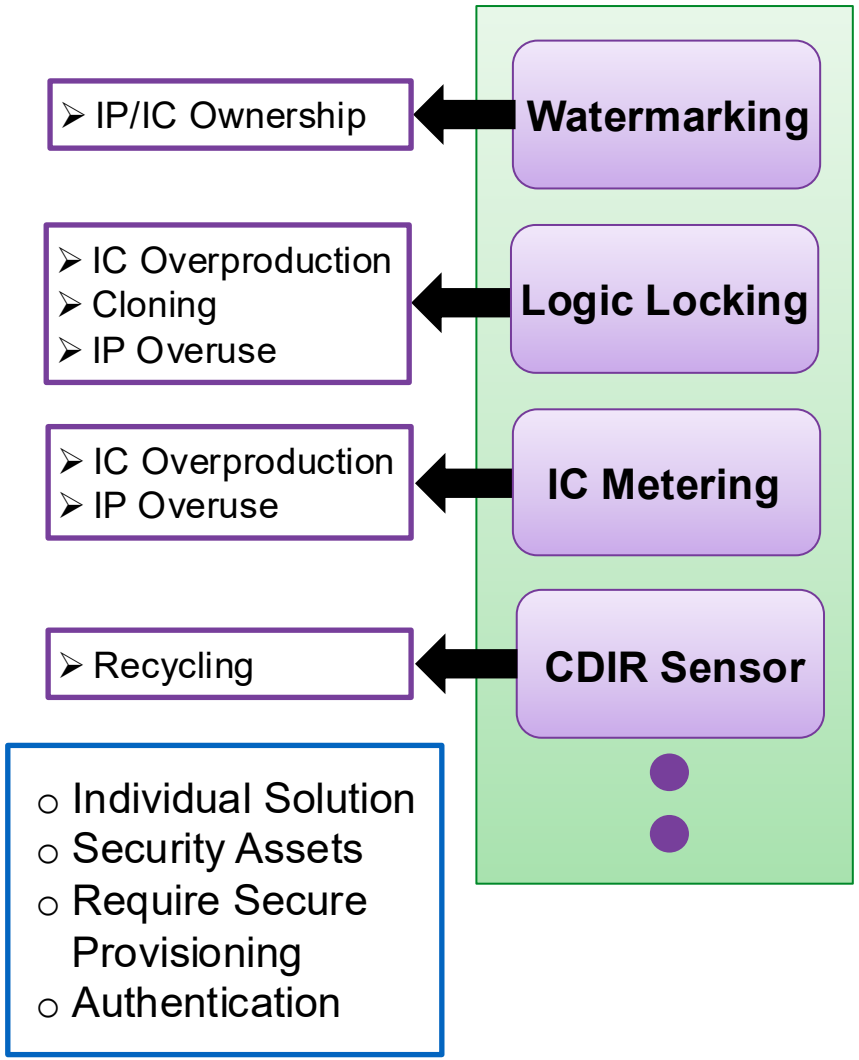
Motivation



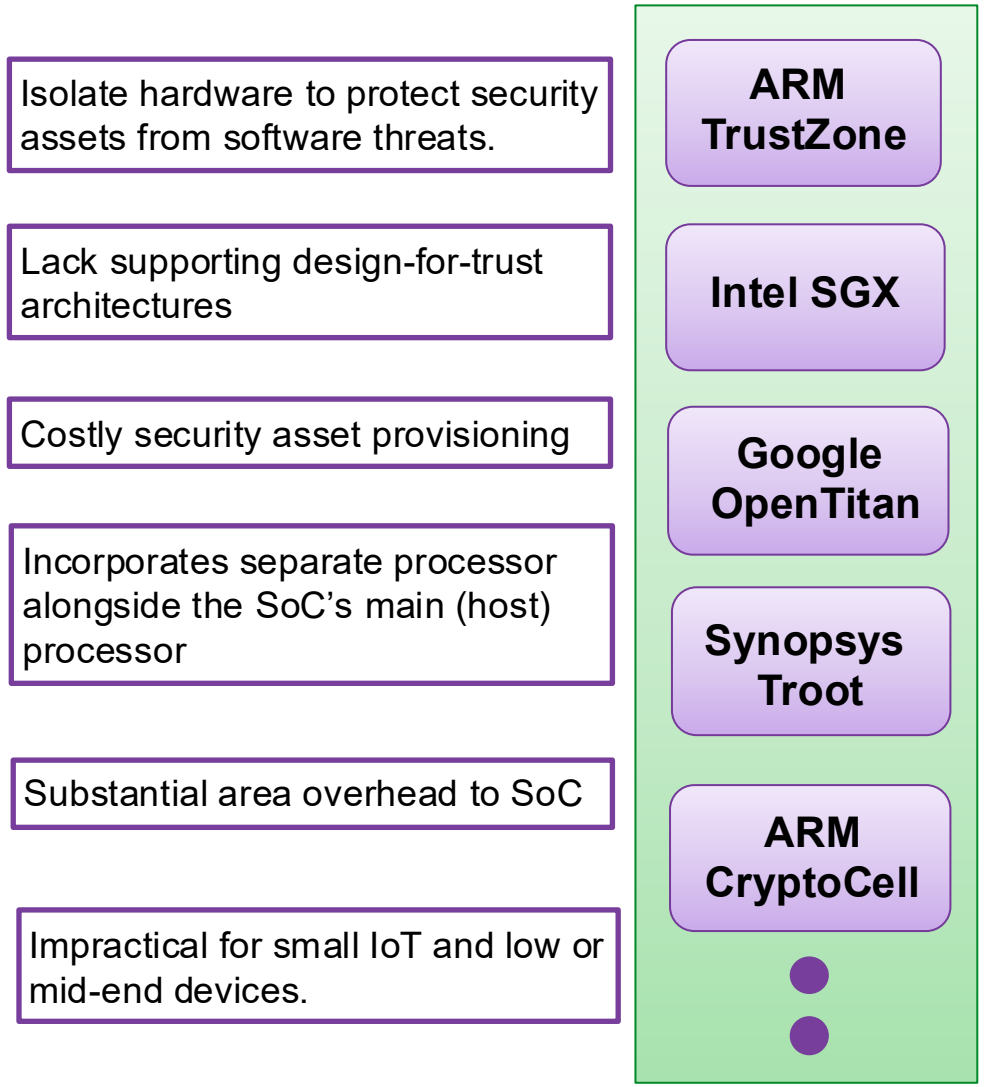
- **Global integration has expedited chip manufacturing.**
- **Relinquishing complete control of the fabless design houses over the manufacturing process.**
- **Instigating trust concerns within the SoC supply chain.**
- **Exposing chips to various security vulnerabilities, including**
  - IP theft, counterfeiting, integrated circuit (IC) overproduction, recycling, etc.

Motivation

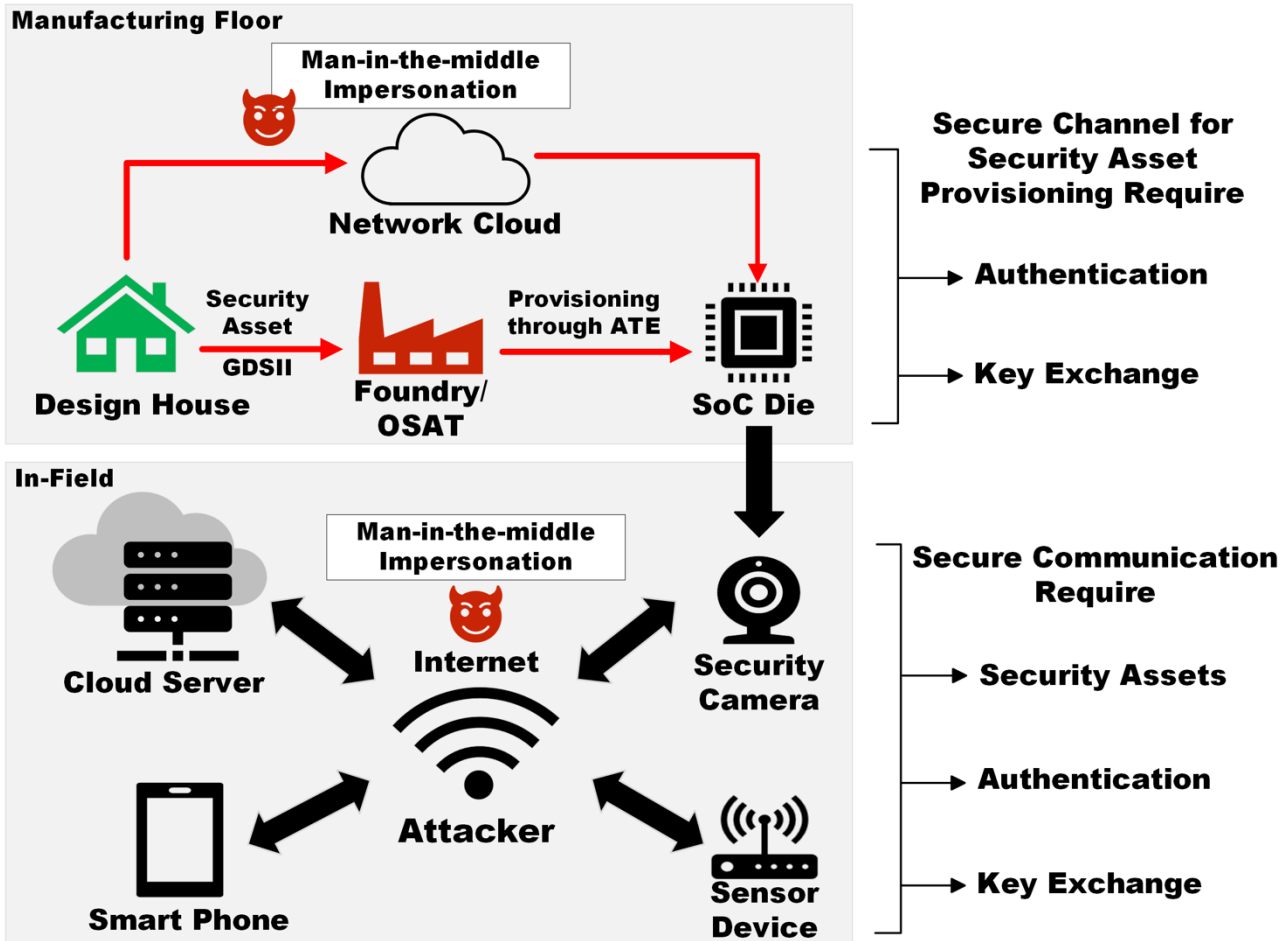
Various Design-for-Trust Measures



Existing Root-of-Trusts



Motivation



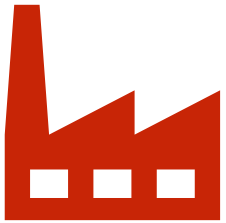
Secure SoC requires holistic security measure

- Authentication of the SoC at the manufacturing facility.
- Establishment of secure communications for security asset provisioning.
- Secure enrollment of device identity or fingerprint (e.g., PUF).
- Integration of design-for- trust architectures
  - Device lifecycle management,
  - Support for logic locking key provisioning, and more.
- Authentication of the chip to support security protocols designed for in-field operations.
- Enabling cryptographic support for various security protocols.

SAP - Silicon Authentication Platform for Supply Chain Security

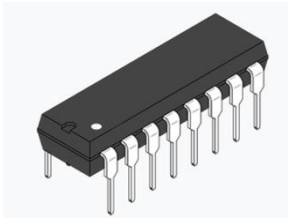
Threat Model

Foundry



- Offshore foundry is untrusted.
  - Access to GDSII fie.
- Designer has no control on the fabrication process.
- No secrets can be concealed in side the netlist.
- Cannot be trusted with security assets.
- Design-for-Trust techniques, become vulnerable to attacks.

OSAT and Test Equipment



- Offshore OSAT is untrusted.
- Has access to the design.
- Cannot be trusted with security asset.
- Malicious software of ATE can read or store transferred data.

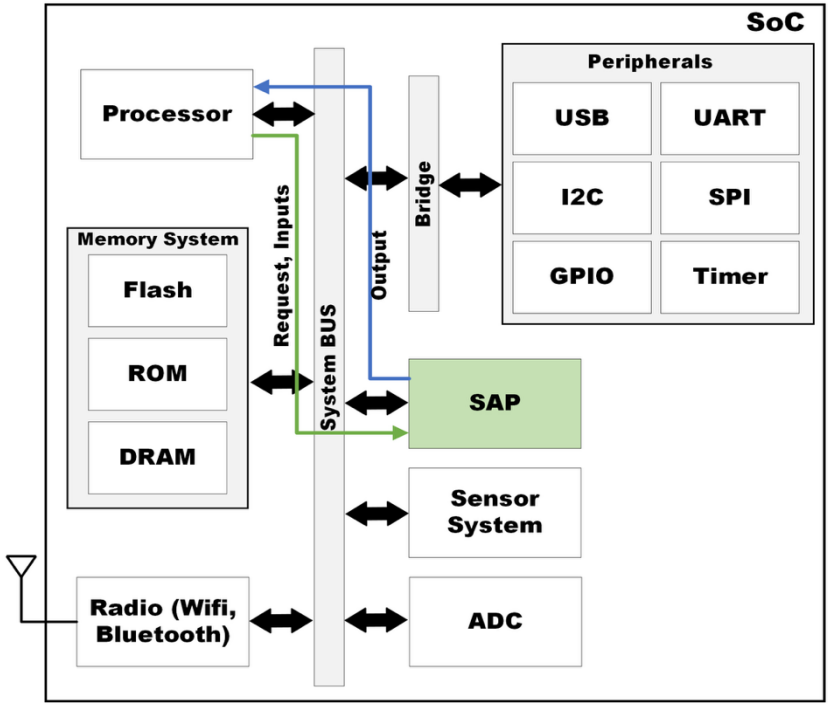
Malicious End User

- Execute malicious software on the host processor.
- Gain unauthorized access to the functional chip (debug port).
- Results in compromising the security protocols.
- May recycle or remark ICs, raising reliability concerns.

Proposed Architecture - SAP

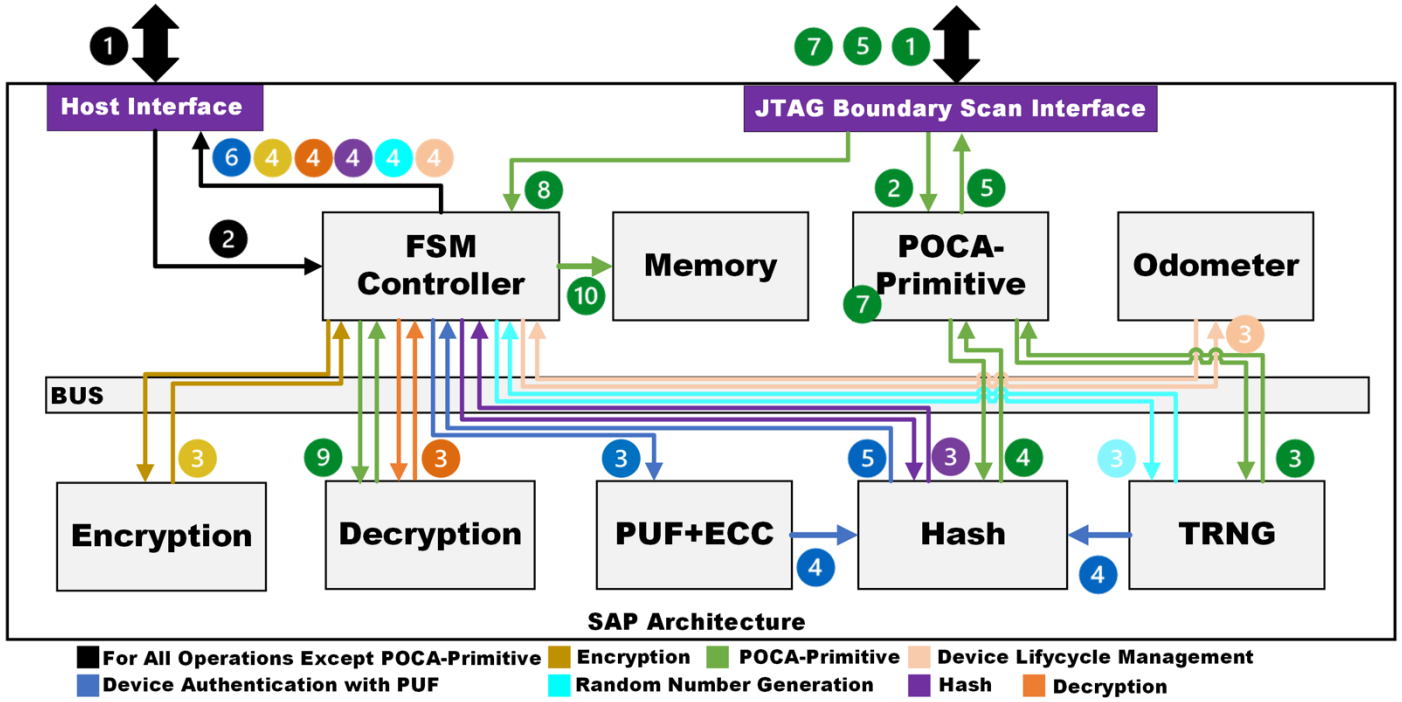
SAP – Lightweight Security IP

- SAP uses a finite state machine (FSM).
- Design house specifies the security requirement during design phase.
- Seamless integration into the SoC's system bus as a plug-and-play IP.
- No need for a separate intricate subsystem dedicated solely to security operation.
- Security operations within SAP are classified into two types: **External** and **Internal**.
- SAP extends cryptographic support to the host processor through its external operations.
- SAP ensures confidentiality of the security assets for internal operations, keeping them hidden from the host processor.



Request Type	Request Code	SAP Operation
01 (External)	0001	Encryption
	0010	Decryption
	0011	Hash
	0100	Random Number Generation
	0111	Device Lifecycle Management
10 (Internal)	1011	PUF Response Generation
	1100	Authentication, Key Exchange and Secure Provisioning of Assets at Manufacturing Facility

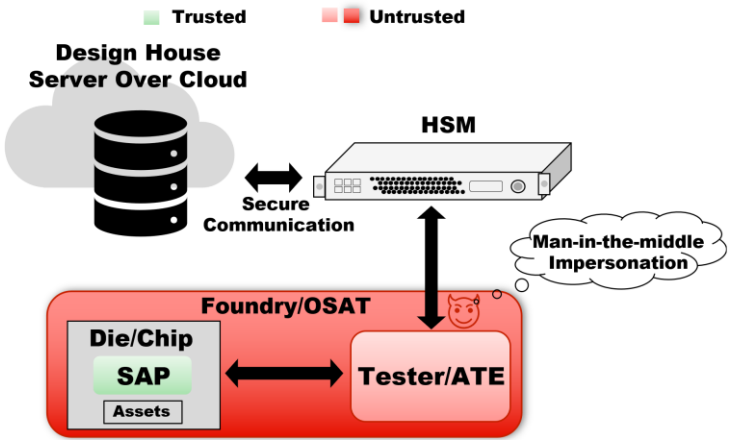
High-level Overview of SAP Architecture



- **SAP Supply Chain Security Features**
  - Authentication and Key Exchange using POCA-Primitive
  - Security Asset Provisioning
  - Secure Enrollment of PUF
  - Device Lifecycle Management

- **SAP Features at the In-Field Operation**
  - Device Authentication with PUF
  - Support for Cryptographic Operation

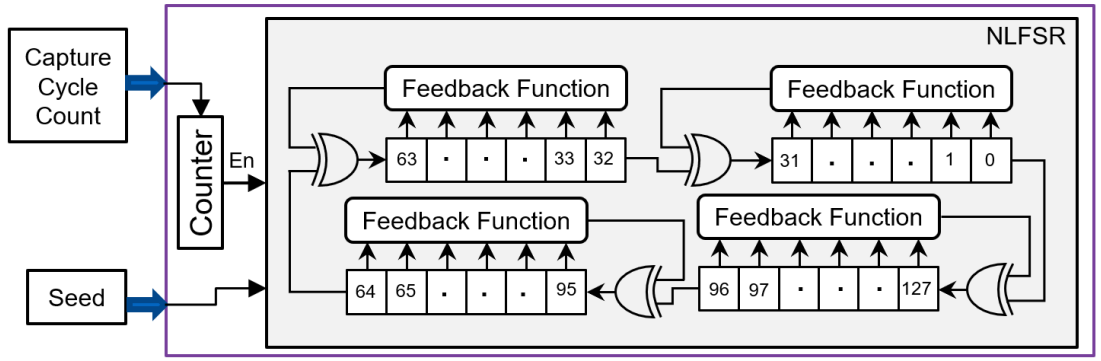
Authentication and Key Exchange using POCA-Primitive



Untrusted Manufacturing Environment

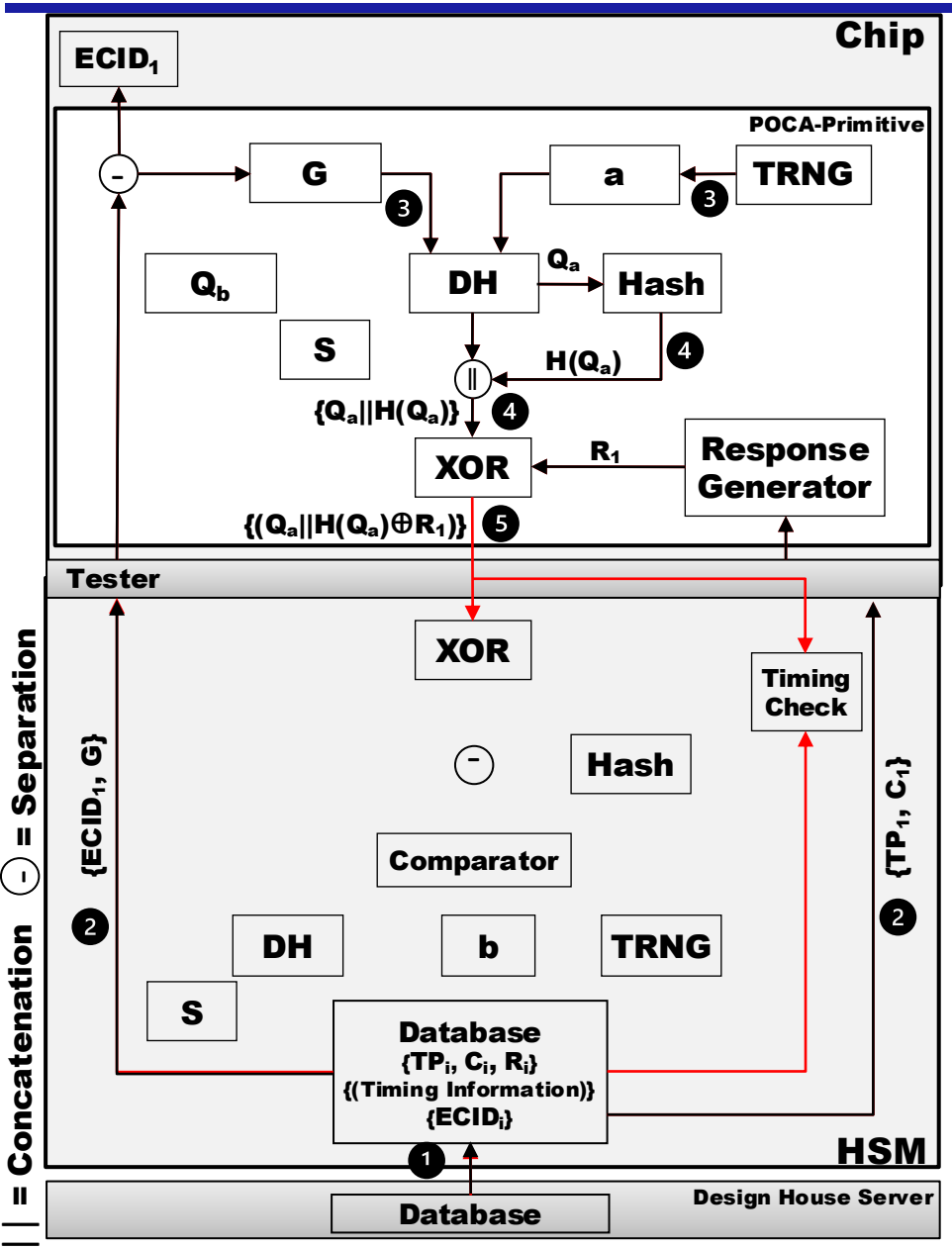
- The design house server authenticates the chip before sending any security assets.
- The chip contains no assets to be authenticated and PUF enrollment is not possible.
- POCA-Primitive is designed to authenticate the chip in the untrusted manufacturing floor.
- HSM is used as a physical intermediate trusted media for the POCA-Primitive protocol.

- Non-linear feedback shift register (NLFSR) is utilized to design the response generator.
- It takes two challenges.
  - **Capture cycle count**: It is a randomly generated number of cycles the NLFSR runs.
  - **Seed**: Randomly generated seed for each session.
- At every session, response generator generates a unique response of the chip.
- During the design phase, the challenges and responses are stored in the server.



Response Generator Architecture

Authentication and Key Exchange using POCA-Primitive



1. The design house server sends the database to HSM through the secure communication channel.

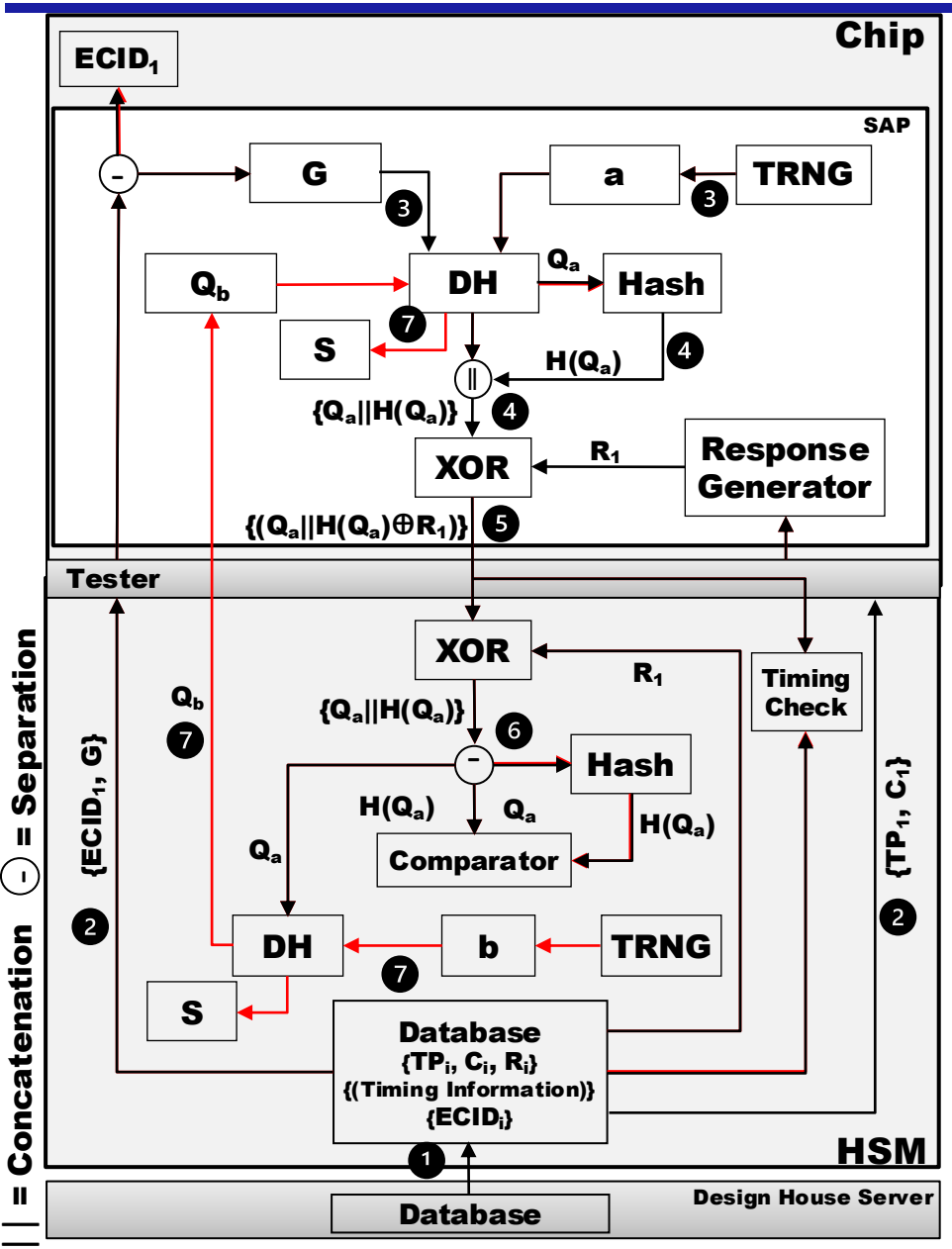
2. The HSM randomly picks two challenges $\mathbf{TP_1}$ and $\mathbf{C_1}$ from the database, transmits them to the chip with SAP request code (101100), and activates the timer. Also, HSM randomly picks an ***ECID*** and sends with the base point (***G***) of the elliptic curve to the chip. Inside the chip $\boldsymbol{ECID_1}$ and ***G*** are separated and stored.

3. The TRNG produces a chip's private key (**a**). The private key (**a**) and the base point (**G**) are utilized by the **DH** module to derive the chip's public key ($\mathbf{Q_a}$).

4. The response generator creates the response ($\mathbf{R_1}$). The public key ($\mathbf{Q_a}$) is hashed ($\mathbf{H(Q_a)}$) and both $\mathbf{Q_a}$ and $\mathbf{H(Q_a)}$ are combined and XORed with $\mathbf{R_1}$.

5. The tester relays $\{\mathbf{(Q_a||H(Q_a) \oplus R_1}\}$ to the HSM for verification. The HSM halts the timer and assesses whether the response was received within the prescribed Ti threshold. If the response is within Ti, the HSM proceeds with response verification. However, if the response surpasses Ti, the chip is classified as non-authentic, and the HSM advances to step 2 to authenticate the next chip.

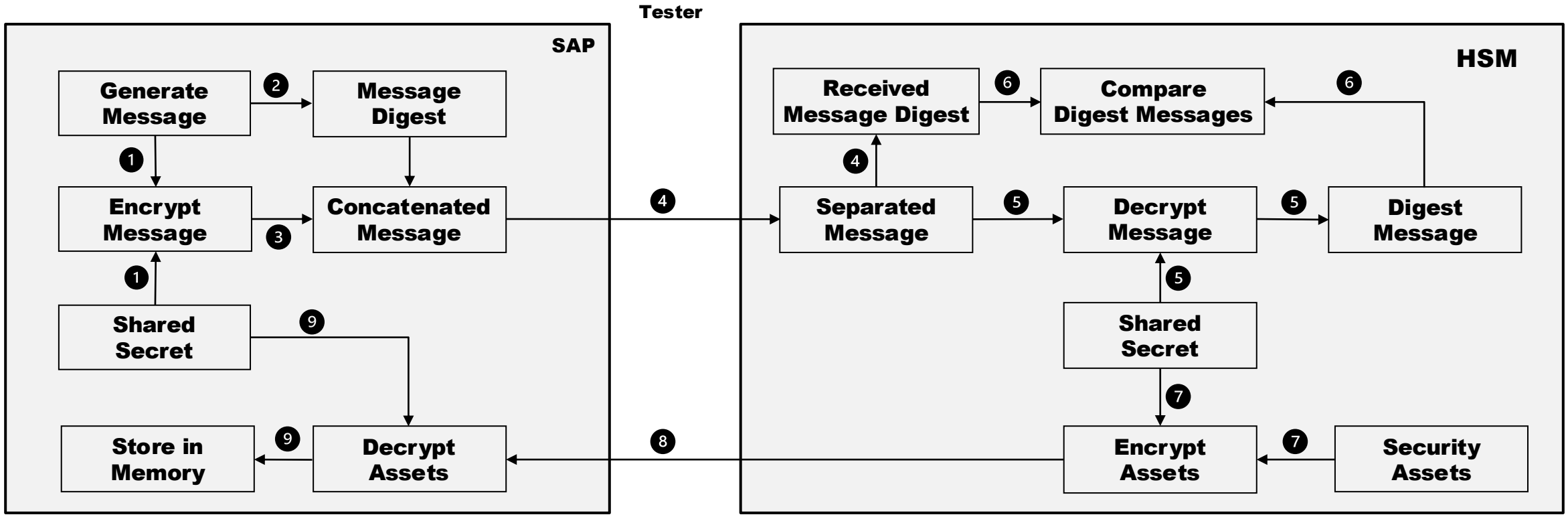
Authentication and Key Exchange using POCA-Primitive



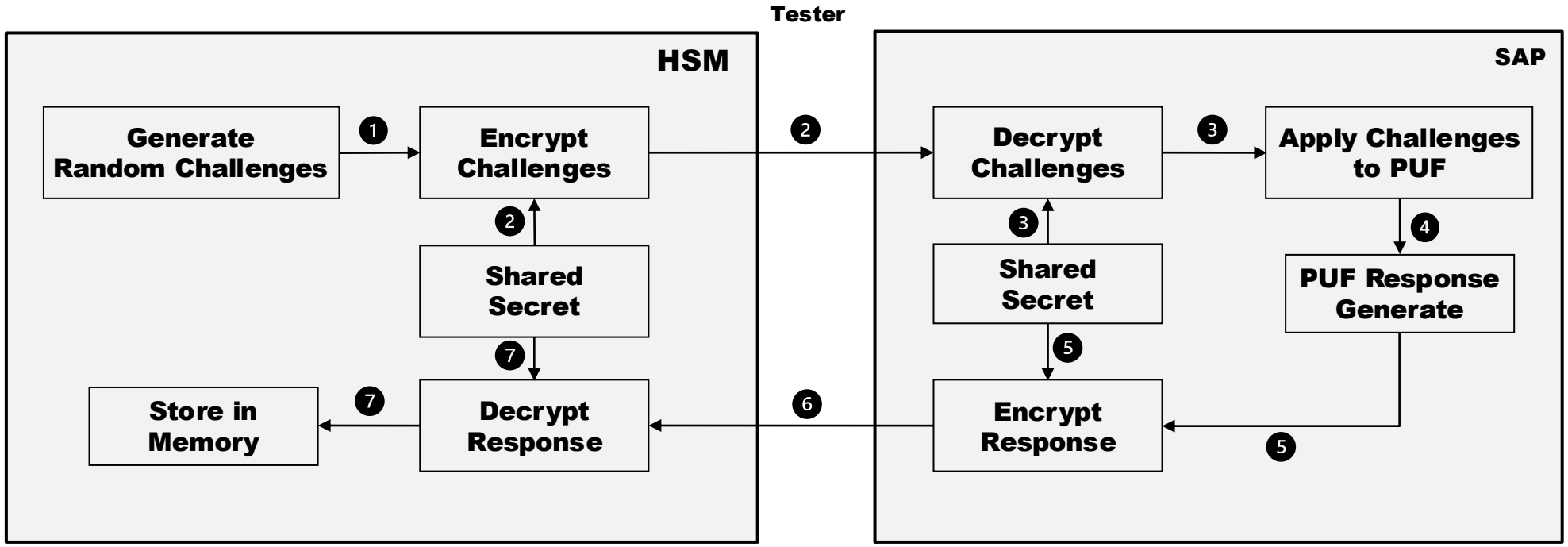
6. The HSM performs XOR operation on $\{(Q_a||H(Q_a)\oplus R_1\}$ using the corresponding R_1 derived from the database. The HSM segregates $\{Q_a||H(Q_a)\}$ and generates $H(Q'_a)$ with the Q_a provided by the chip. If $H(Q'_a)$ matches $H(Q_a)$, the HSM confirms the response and designates the chip as authentic. Conversely, if the values do not align, the HSM labels the chip as non-authentic.

7. The HSM generates its private key (**b**) and public key (Q_b). It transmits Q_b to the chip and calculates the shared secret key ($S = aQ_b$). Likewise, the chip computes its shared secret key ($S = bQ_a$). The secret key can be hashed at both ends, and the resulting hashed key is employed for securing the provisioning of security assets. The HSM then discards the utilized challenges, reverts to step 2, and initiates the authentication procedure for the next chip.

Security Asset Provisioning

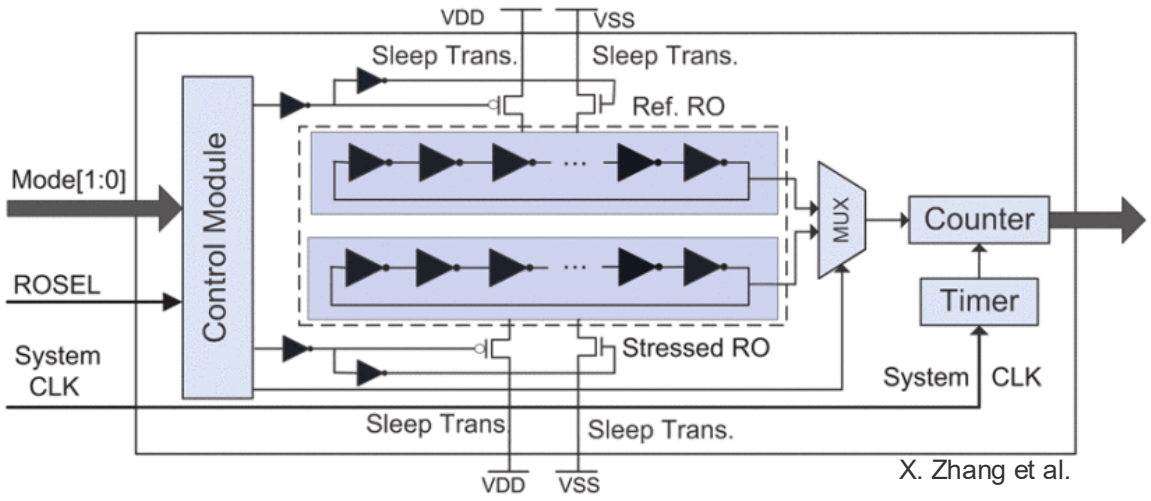


Secure Enrollment of PUF



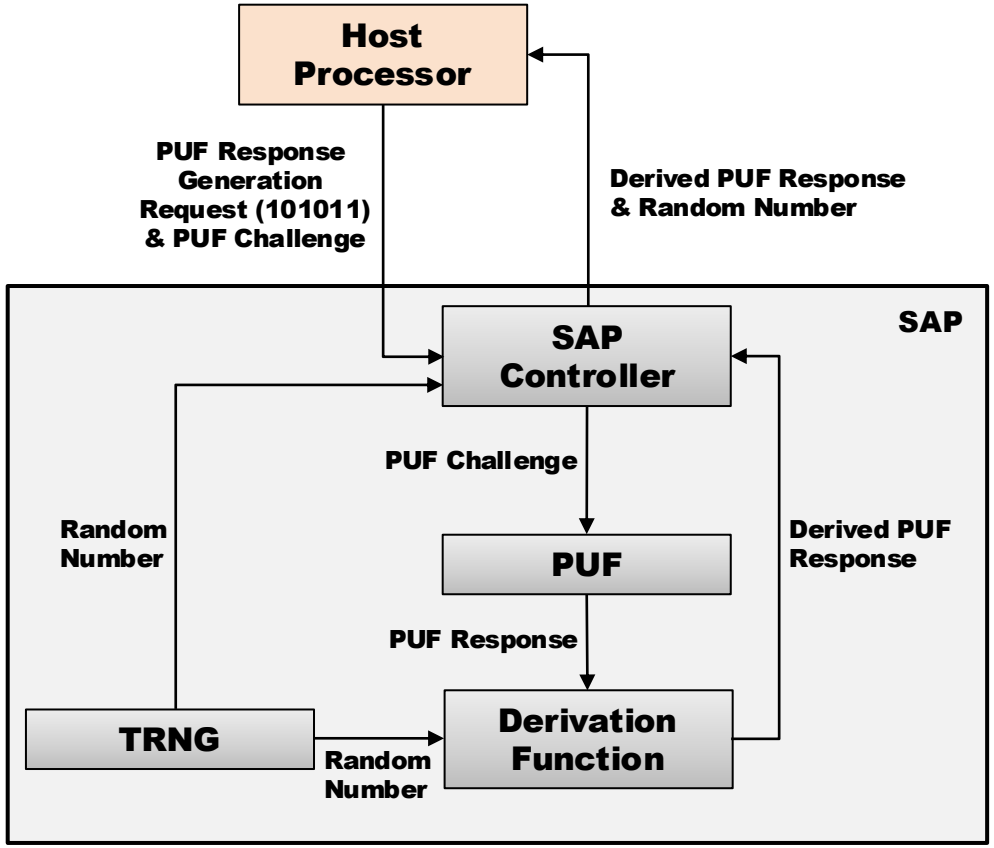
Device Lifecycle Management

- SAP includes Combating die and IC recycling (CDIR) sensor, safeguarding against recycled ICs.
- Contains to Ring Oscillator.
  - The first RO, known as the reference RO, is designed to age slowly.
  - The second RO, the stressed RO, age significantly faster. The stressed ROs decrease their frequency due to rapid aging.
- The difference in the RO frequencies indicates prior chip usage.
- The design house registers the frequencies of the two ROs in the design house server.
- The HSM sends a request code (010111) to SAP requesting the reading of the device's lifecycle information.
- SAP provides the frequencies of the two ROs.



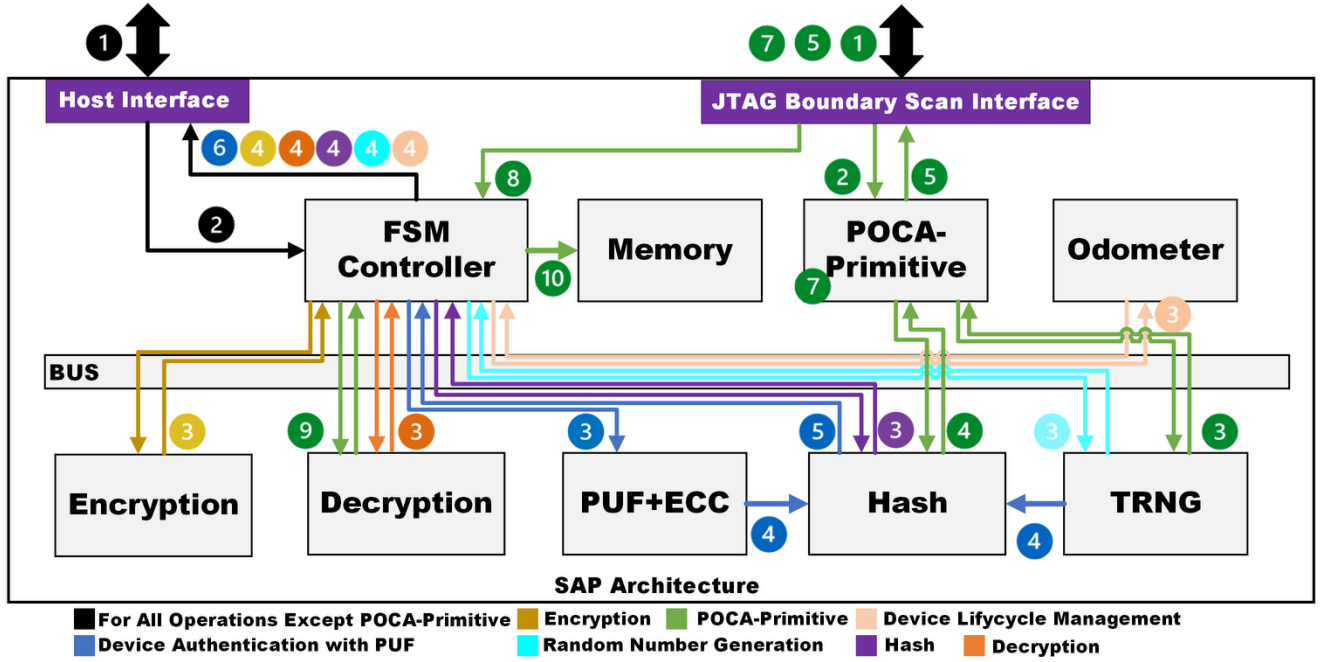
RO-CDIR Sensor for Lifecycle Management

Device Authentication with PUF



- SAP refrains from transmitting the PUF response directly to the host processor in plaintext.
- Instead, SAP shares a derived PUF response with the host processor.
- It safeguard PUF response from potential threats posed by malicious software running on the host processor.
- Utilizing the PUF response enables the design house to integrate various PUF-based authentication protocols.

Support for Cryptographic Operation



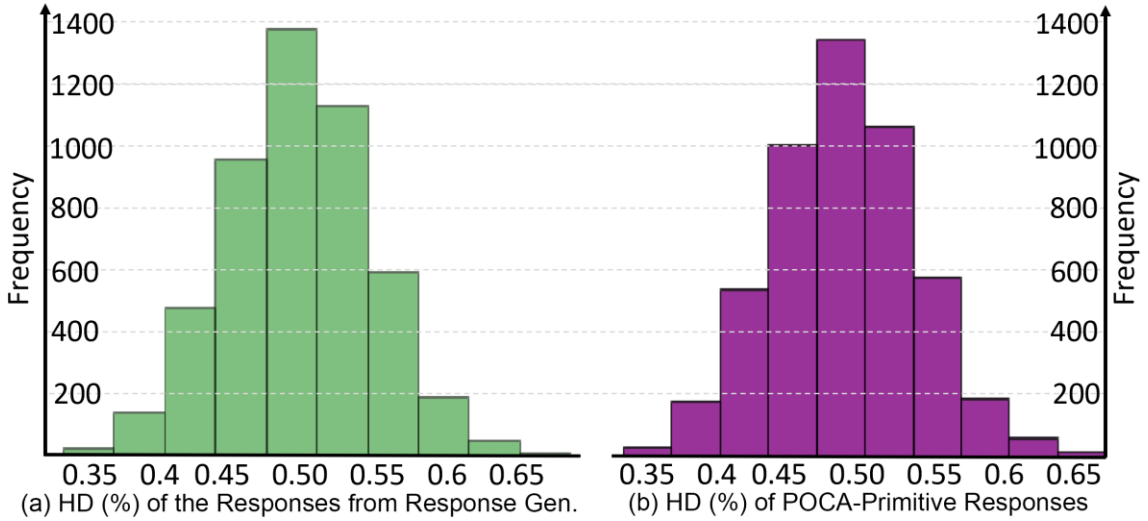
- SAP provides essential cryptographic support to the host processor for applications.
  - Encryption,
  - Decryption,
  - Random number generation, and
  - Hash operations.
- The host processor transmits a request code with input data.
- SAP decodes the request code, execute the operation and provide the output.

Security Analysis

- **Resilient against Man-in-the-Middle Attack**
  - Do not reveal any information related to the secret key through mere observation.
  - The challenges and responses are distinct per session.
  - Any manipulations on the challenges and Diffie-Hellman parameters can be detected during verification.
- **Resilient against Impersonation Attack**
  - Simulation and Emulation using software program are not possible as it is slower than hardware.
  - Impersonating using overproduced chip does not benefit the attacker as only one chip will generate the shared secret key with the HSM.
  - HSM only authorized a certain number of genuine chips.
- **Resilient against Precomputed Database by the Foundry**
  - Size of challenge (160bit) is large for modern SoCs.
  - Recreating the database nearly impossible, and the likelihood of finding a match within the threshold time is minimal.

Security Analysis

- **Resilient against Replay Attack**
  - The same test pattern will never be used for authenticating other chips.
  - Each chip will produce a different response for different capture cycles.
- **Secrecy of Responses**
  - Hamming distance (HD) between the responses of POCA-Primitive and the response generator is approximate 50% .



  - Both responses display unique and random attributes.
  - Consequently, the response does not reveal any information about the chip's response or secret key.
- **Unique PUF-Response**
  - Hash function is utilized as derivation function.
  - The attacker is unable to deduce the original PUF response from the derived response due to one way function.

Results

# of Cycle*	20	40	60	80	100	120	140	160	180	200	500
Sim Time+	1.36	2.38	3.26	4.21	5.24	5.90	6.96	7.94	8.91	9.71	24.17

*: $(C_i \times 10^3)$ Simulation Runtime in $(second)$

Simulation Runtime for Different Capture Cycle Count

Components	Resources	
	# of LUT	# of FF
SAP Controller, Decoder and Memory*	3662	6891
POCA-Primitive*	2702	2478
Odometer*	43	20
Hash*	1803	1883
PUF*	1043	603
TRNG*	152	140
Total SAP (This Work)	9405	12015
ROCKET CORE [45], [46]	55156	46657
SHAKTI [46], [47]	74840	55174
CVA6 [46], [48]	95895	77463
BROOM CORE [46], [49]	261294	123685

*: SAP Components

Area Overhead Comparison between SAP Components and Different Processing Units

Area Overhead		Estimated Power	
Components	Gate Count	Leakage Power (mW)	Dynamic Power (mW)
Combinational Cells	36924	4.004	41.274
Sequential Cells	9926		
BUF/INV	5772		

Area Overhead and Estimated Power in ASIC

	Execution Time (Cycles)	
SAP Operations	FSM Controller	Component
Encryption	42	13
Decryption	57	13
Lifecycle Management	24	17
Hash	67	144
Secure PUF	404	126
TRNG	34	202
POCA-Primitive	87	907

Performance of Each Operation in SAP