晶片安全.

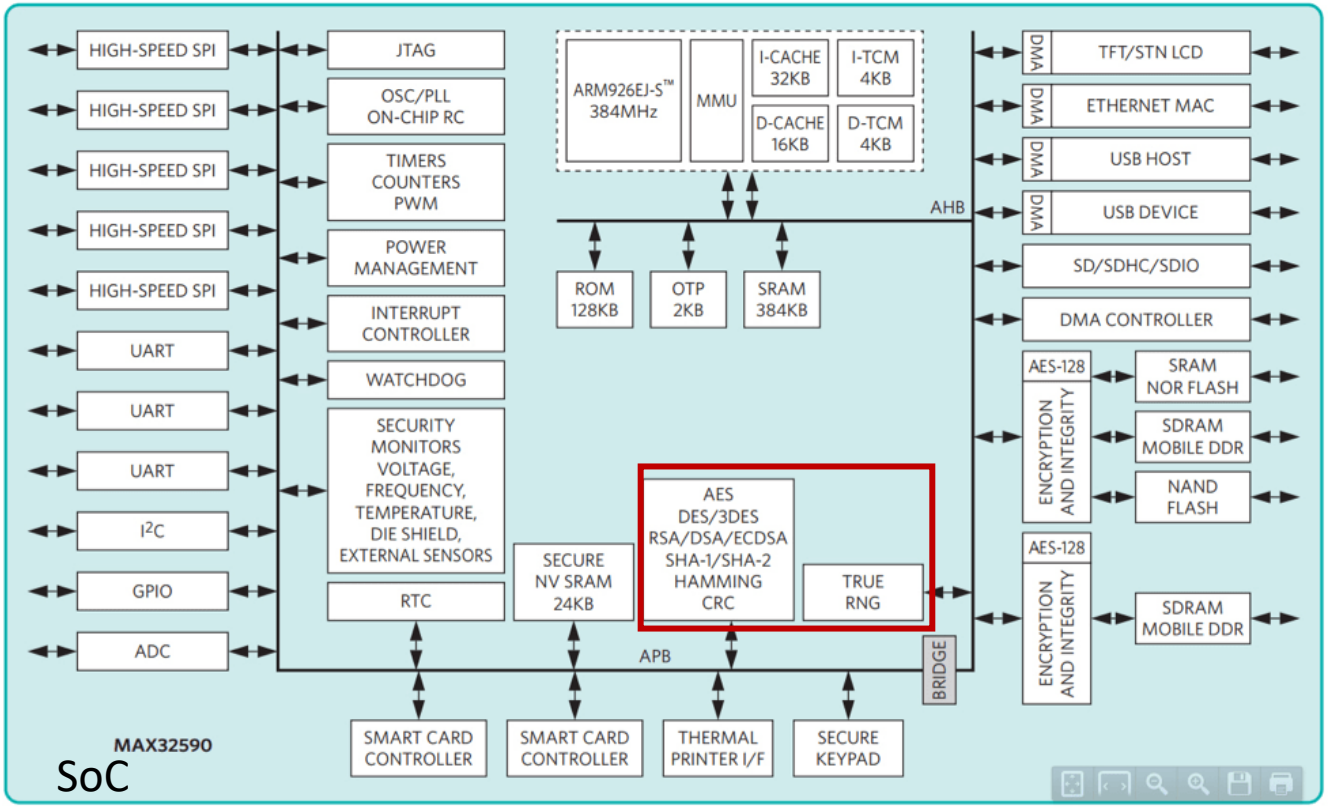
2025 Feb/21

PUF security
AN ememory COMPANY

Agenda

1. From IP to SoC
2. Importance of Security
3. Threats and Root-of-Trust
4. Functionality of the Hardware Root of Trust

All IP in an SoC .



https://semiengineering.com/its-all-ip-in-an-soc/

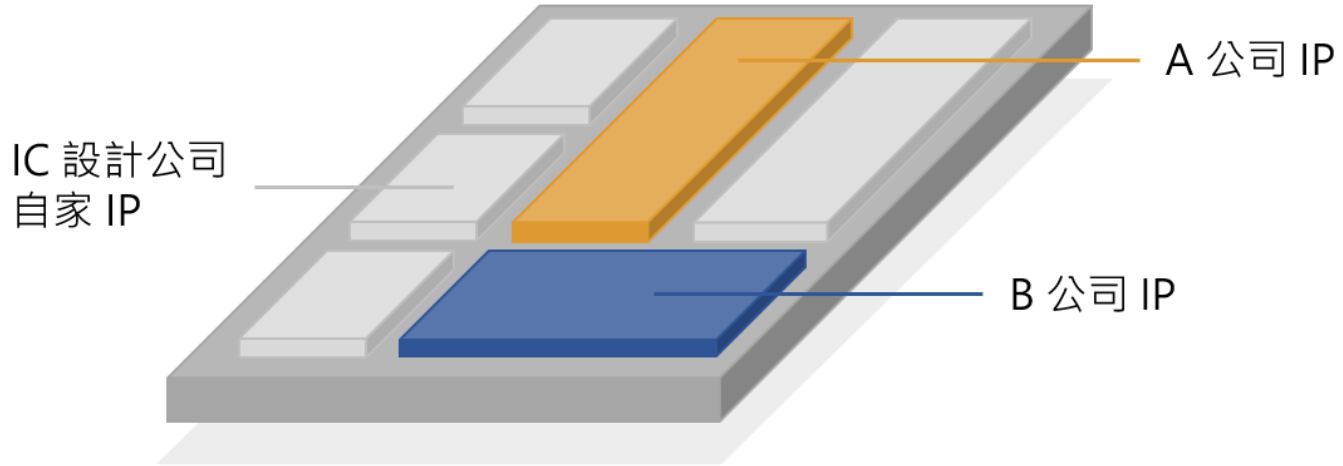
IP Business .

超愛喝牛奶,

自己養牛會不會更划算？

All IP in an SoC .

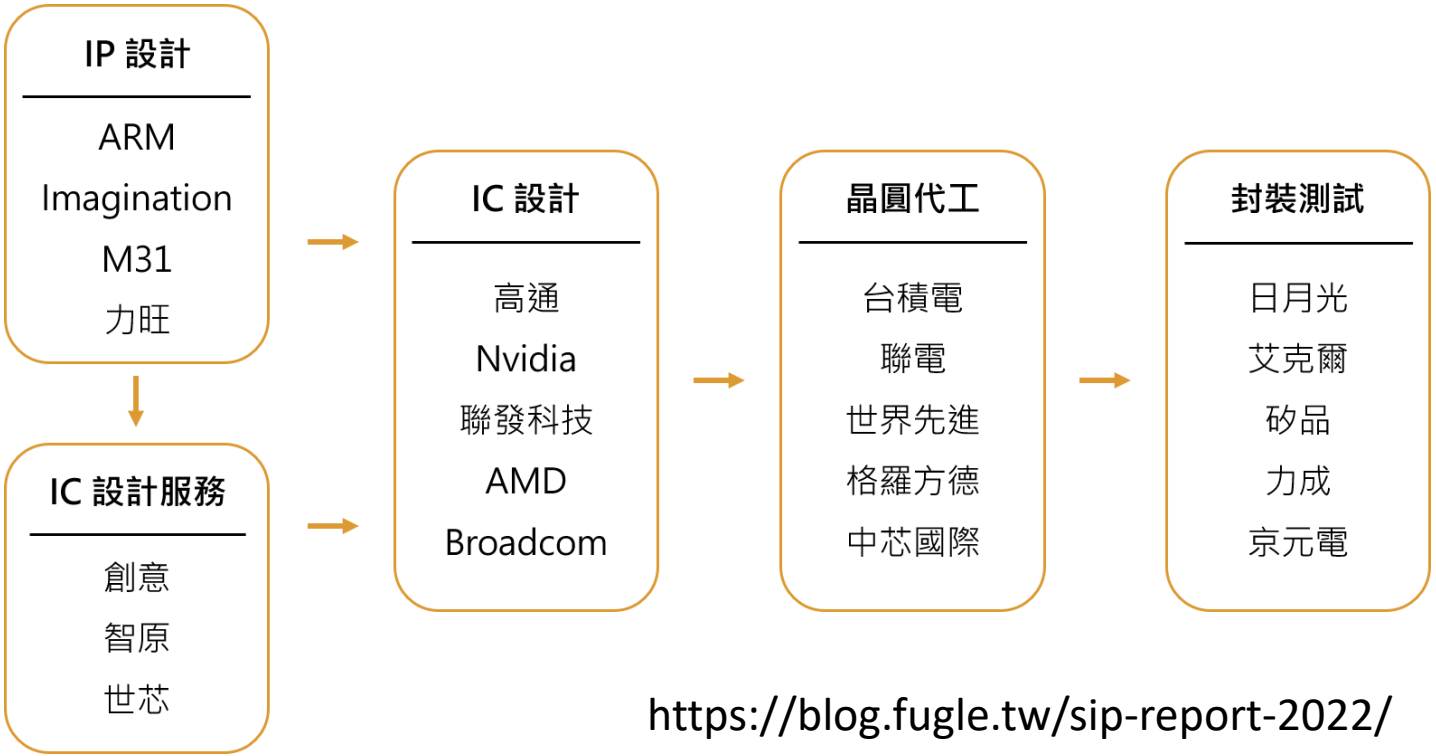
IC 設計公司可透過使用不同公司 IP 簡化晶片開發流程



IC 內部電路設計

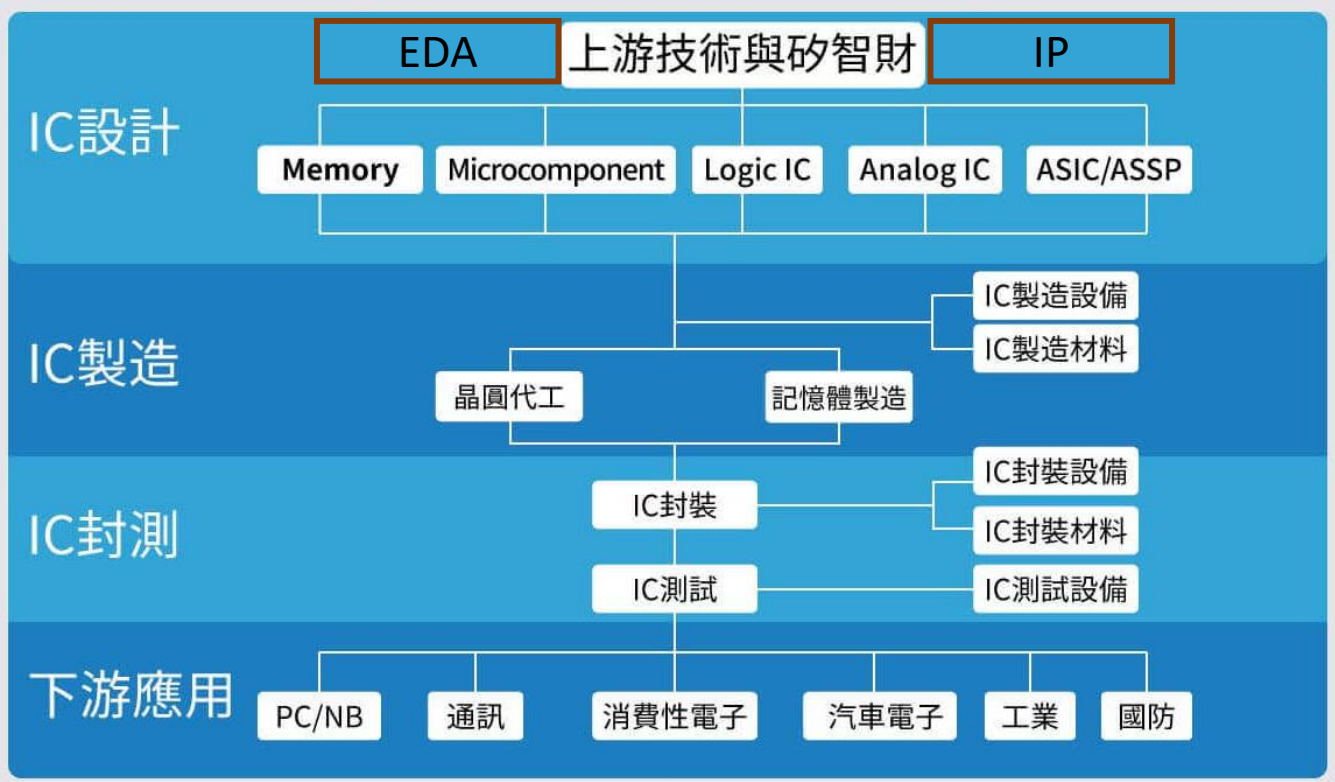
https://semiengineering.com/its-all-ip-in-an-soc/

Supply Chain of IC industry .



https://blog.fugle.tw/sip-report-2022/

Semiconductor Industry Overview .



https://semi.com.tw/semiconductor/半導體供應鏈/

2021/2022 World Top10 IP Vendors .

Semiconductor Design IP Revenue by Company, Worldwide, 2021 and 2022 (Millions of Dollars)

Rank	Company	2021	2022	Growth	2022	Cum. Share
1	ARM (Softbank)	2 202,1	2 741,9	24,5%	41,1%	41,1%
2	Synopsys	1 076,6	1 314,8	22,1%	19,7%	60,8%
3	Cadence	315,3	357,8	13,5%	5,4%	66,1%
4	Imagination Technologies	153,0	188,4	23,1%	2,8%	68,9%
5	Alphawave	89,9	175,0	94,7%	2,6%	77,4%
6	Ceva	122,7	134,7	9,8%	2,0%	72,8%
7	Verisilicon	109,4	133,6	22,1%	2,0%	74,8%
8	SST	102,9	122,0	18,6%	1,8%	70,8%
9	eMemory Technology	84,8	105,1	23,9%	1,6%	79,0%
10	Rambus	47,7	87,9	84,3%	1,3%	80,3%
	Top 10 Vendors	**4 304,4**	**5 361,2**	**24,6%**	**80,3%**	**80,3%**
	Others	1 217,7	1 316,0	8,1%	19,7%	100,0%
	Total	**5 522,1**	**6 677,2**	**20,9%**	**100,0%**	**100,0%**

Source: IPnest (Avr 2023)

https://semiwiki.com/semiconductor-services/327734-design-ip-sales-grew-20-2-in-2022-after-19-4-in-2021-and-16-7-in-2020/

Agenda

1. From IP to SoC
2. Importance of Security
3. Threats and Root-of-Trust
4. Functionality of the Hardware Root of Trust

Every Application Needs Security .

IoT

Low-power, low-cost hardware security is needed to protect customer privacy

AI

How to protect AI training models and parameters raises concerns today.

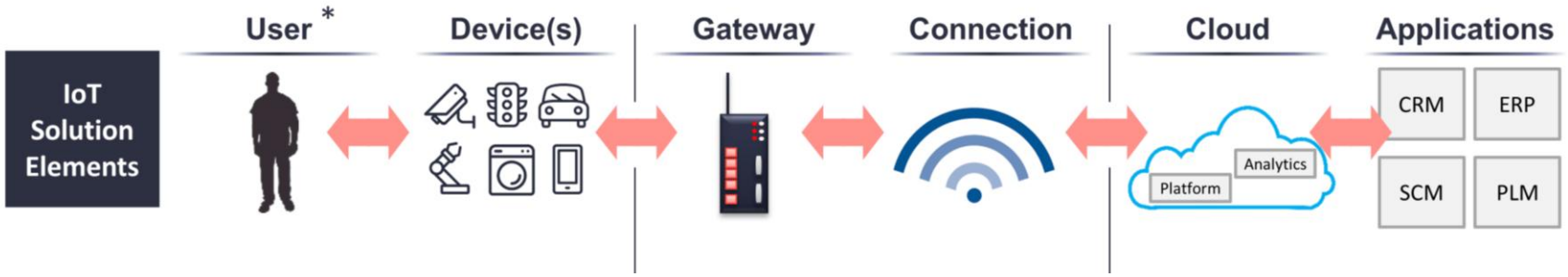
Automotive

In IoV, (Internet of Vehicles) applications, illegal devices increase the potential for malicious attacks on cars

Fintech

PUF-based inborn ID provide the trustworthy devices for fintech services, can help provide the solutions across virtual and physical for these applications.

Security Threat (IOT) is Everywhere .



End Device Security

- Malicious counterfeit devices
- Key / data stored in devices stole
- Secure Boot failed (root access)

Connectivity / Communication

- Malicious file injected during OTA update
- Data-in-transit intercepted

Cloud Applications

- Services accessed by malicious device
- Data-in-transit intercepted

Product lifecycle Management

- Hacked during remote control or update

(Source: IoT Analytics, PUFsecurity)

Real Threats for a SoC: SW to HW Security .

HW Layers

- SoC
- Analog Design
- Digital Design

Threats

- Clone/Counterfeit
- Side Channel Attack
- Reverse Engineering

Firmware

- API
- Driver
- Embedded System

Threats

- Clone/Pirate
- Jailbreak

SW Layers

- Applications
- OS
- Cloud

Threats

- Clone/Pirate
- Privacy/Assets
- Virus

Example: Game Console .

強悍的世嘉五代MD遊戲機專用燒錄卡ME...

PWD	SW (Clone)	SW/FW (FP overflow)	HW (Glitch FI/Debug)
→ 直接拷貝 **+ ROM/DVD**	→ 買台片、燒錄卡。 **+ 增加光碟片認證檢查**	→ 軟破 for Homebrew **+ 虛擬機、Runtime 檢查**	→ 硬破 to skip secure boot **+ 記憶體保護、硬體抗攻擊。**

Agenda

1. IP to SoC
2. Importance of Security
3. Threats and Root-of-Trust
4. Functionality of the Hardware Root of Trust

Hacking is Everywhere Today .

Threat to
Life

Hackers Remotely Kill a Jeep on the Highway

Sparking a 1.4 million vehicle recall by Chrysler, marking the start of the age of hackable vehicles.

Link

Threat to
Privacy

IoT Security Camera hacking demonstration on YouTube

Step by step guides for hacking IoT devices are widely available online.

Link

Threat to
Assets

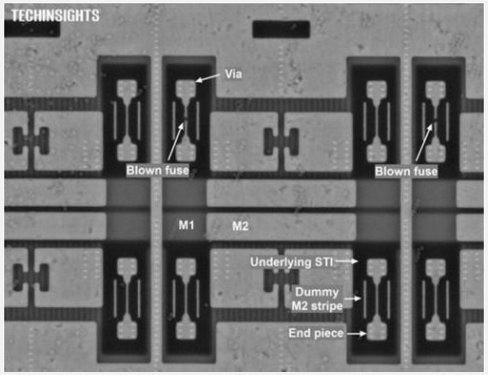
Colonial Pipeline pay $4.4m to end ransomware attack

ending the massive shutdown of approximately half of the USA's East Coast fuel supply

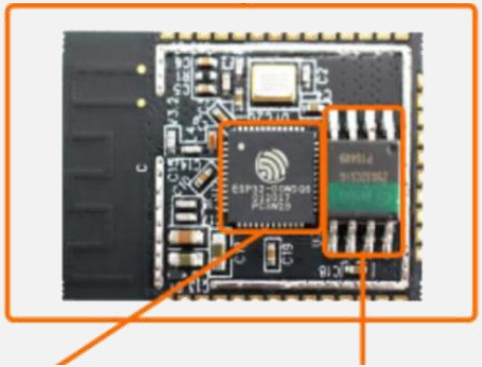
Link

Hardware Attacks are Reality Today .

De-cap
E-fuse keys stolen

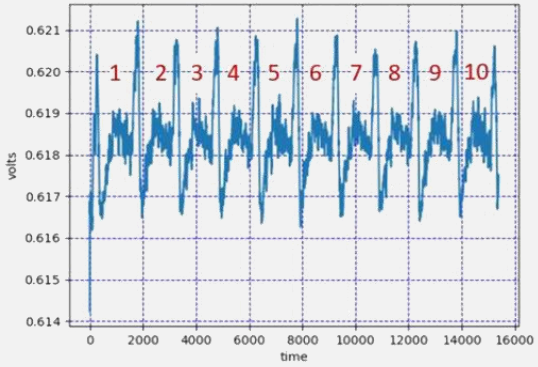


Fault Injection
IoT WiFi Chip Hacked



ESP32 Flash Memory (SPI)

DPA
MCU AES key found



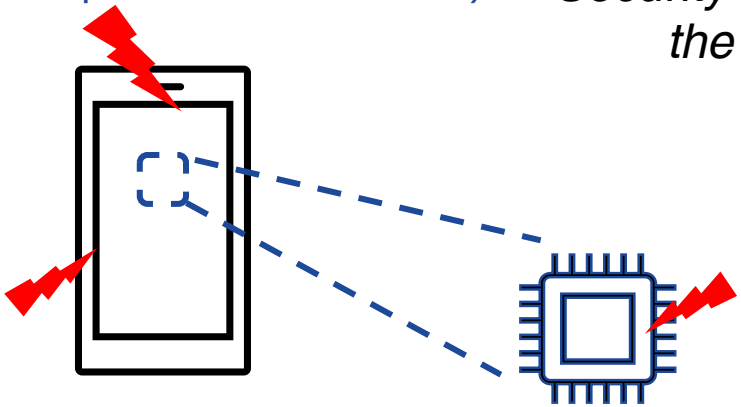
Need Invisible OTP

Need Anti-SCA / Anti-Tampering Design

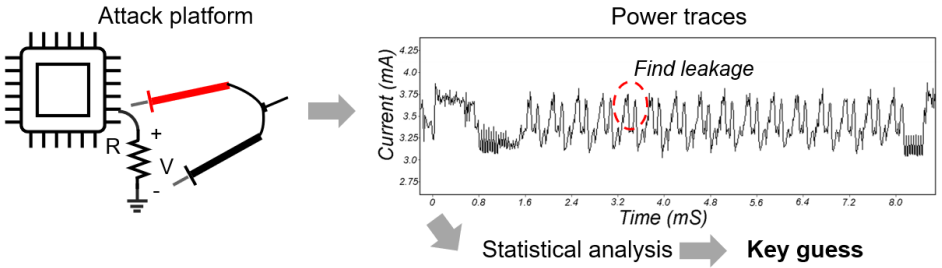
Attacks (Key Leakages) can happen Anywhere .

Software attacks
(e.g. buffer overflow, interrupts, malware software)

"Security is only as strong as the weakest link"



Side-channel attacks
(e.g. power analysis)



Hardware attacks

- Invasive attacks (ex. SEM/TEM)
- Semi-Invasive Attack (ex. Probe/Laser FI)
- Non-Invasive Attack (ex. Laser FI/Power)

Advantage of HW Security .

Hardware Root of Trust

Use of a standalone security element or embedded with hardware security function.
➔Isolated Sensitive Data
➔Less Vulnerability

Accelerated Crypto Engine

Hardware crypto engine provide high efficient, real-time cryptographic functions.
➔Less Power/CPU Loading
➔Less Vulnerability

Binding Software & Hardware

Software binding with hardware provides a robust and anti-tampering security function.
➔ Less Vulnerability

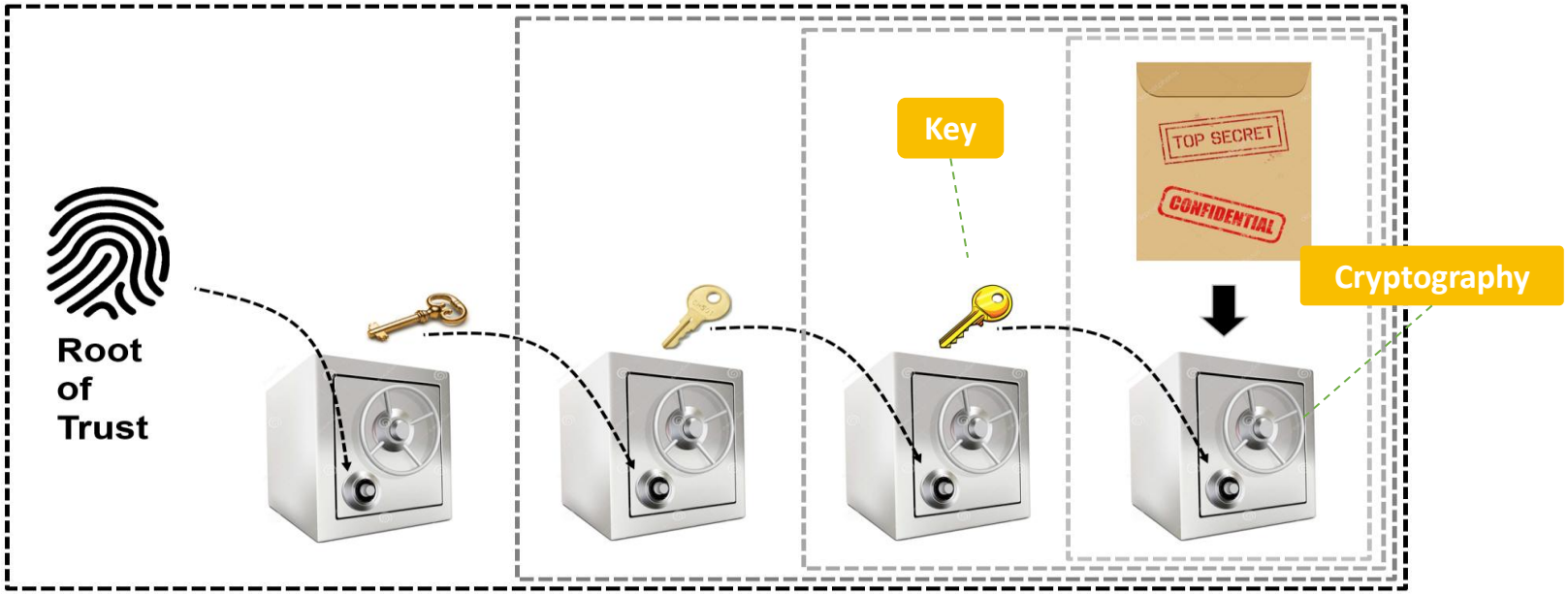
How to protect the important data? It uses the only "Root-of-Trust" as the starting point to protect all data based on it.

Is it Safe? .

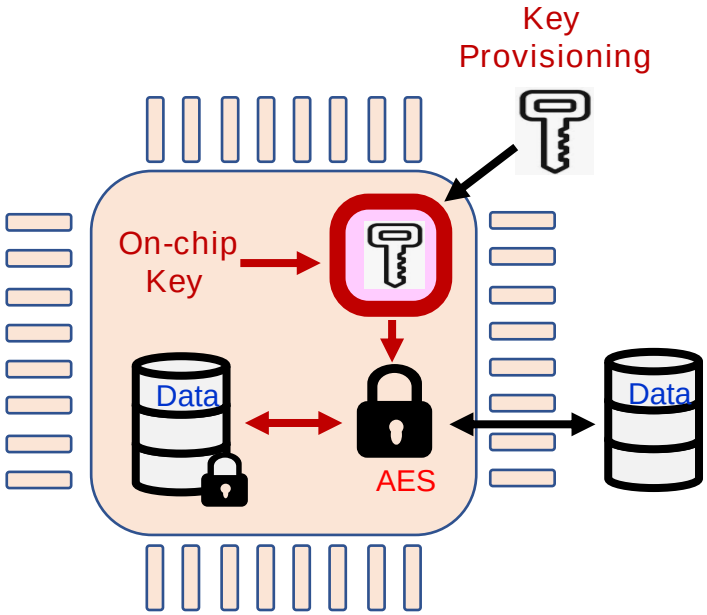
Security is Only as Strong as the Weakest Link .

Kerckhoffs's principle: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

→ The root key has highest level security authority.



How to Build and Protect a RoT .



How to protect the data?
→ Crypto Operation (block-cipher)

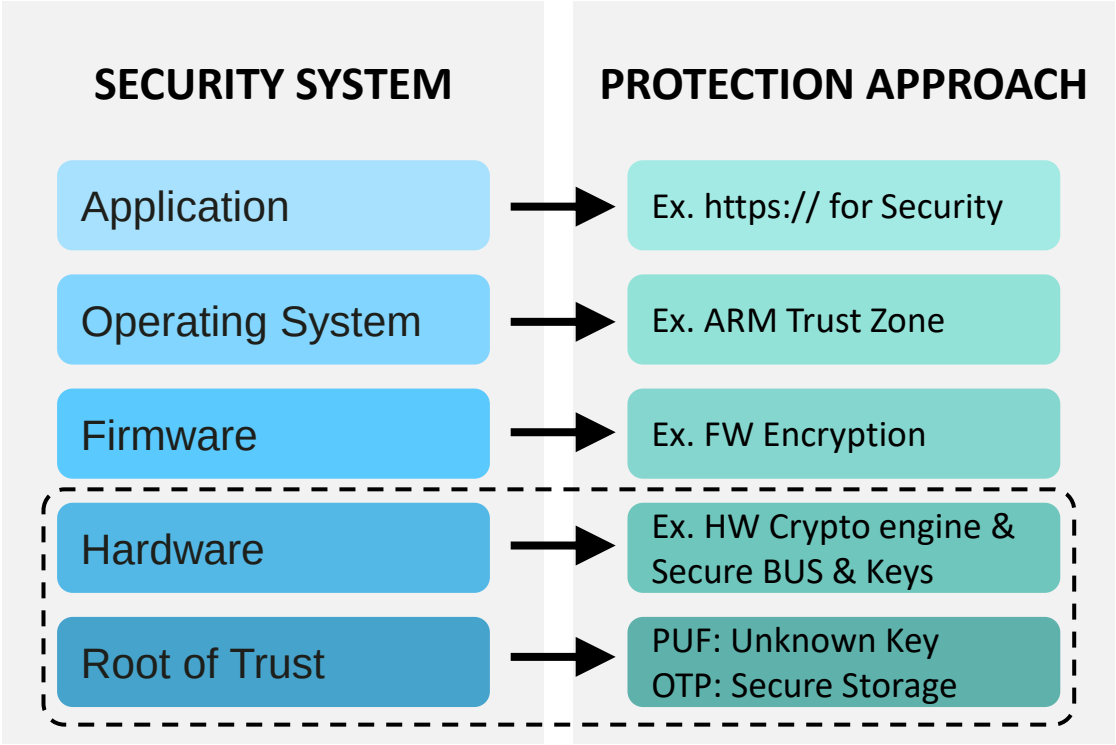
How to protect the key injection?
→ Secure Storage
→ Anti-Tampering Design

How to protect the OTP?
→ UID/HUK (Static Entropy PUF)

How to protect operation
→ TRNG (Dynamic Entropy)

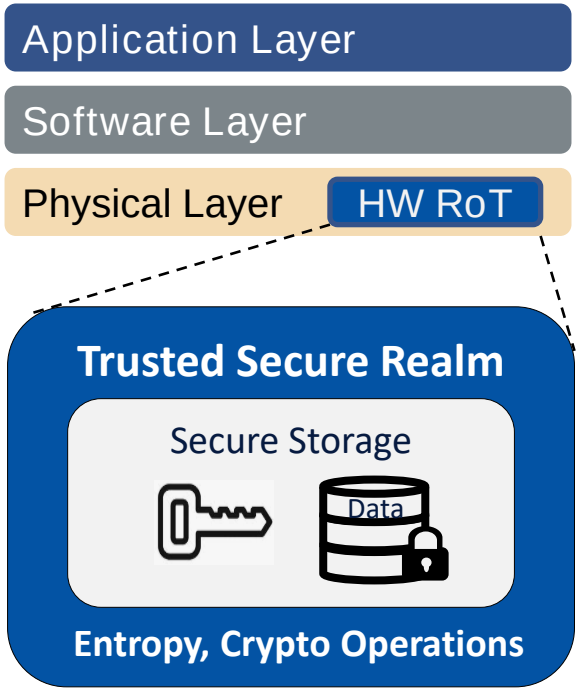
Obviously, UID, secure storage, entropy and tamper-proof can make a HRoT

Layered Security from HRoT to SW/Application .



- HW and SW security are equally important
- SW can be updated at the field, but HW cannot
- Insecure key storage (e.g., eFuse) can be compromised the whole system
- Hacker always can find the weakest link to the system

Composition of HW Root-of-Trust (HRoT) .



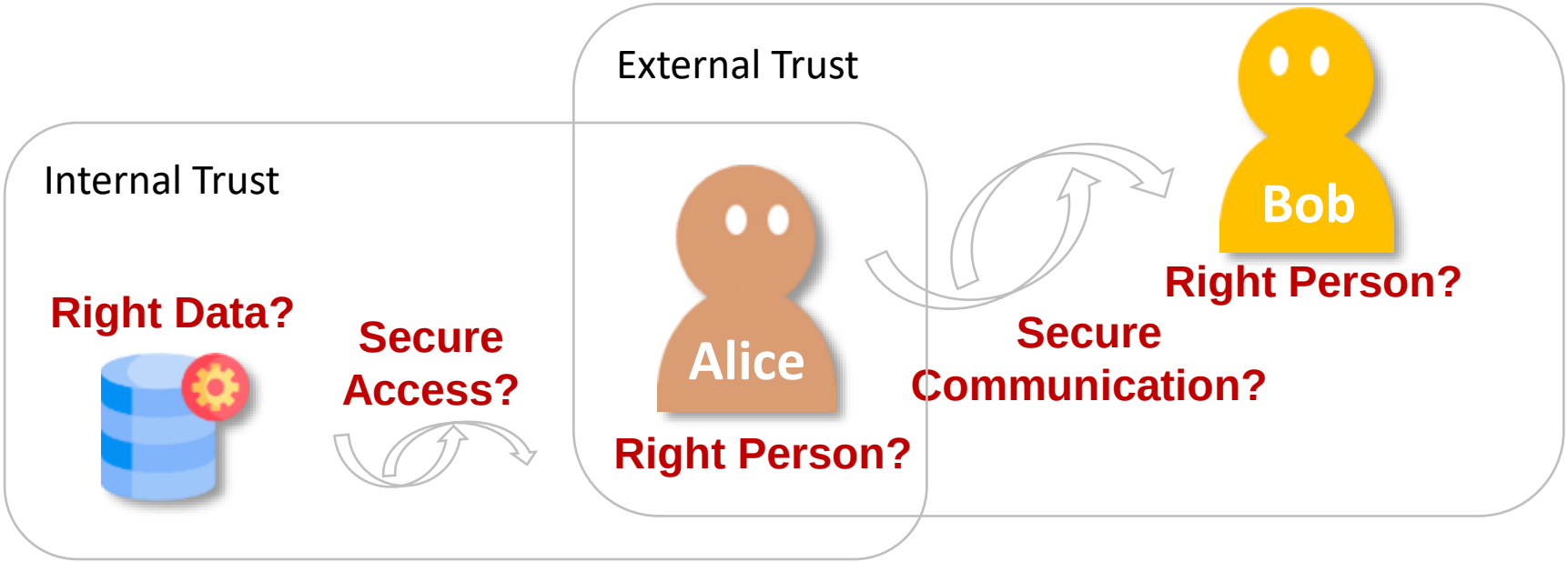
HRoT is the security anchor with

1. Anti-Tampers
2. Secure Storage
3. Entropy (TRNG/PUF)
4. Crypto-Engines: Secure operations
5. Secure Enclave: Trusted boundary

Agenda

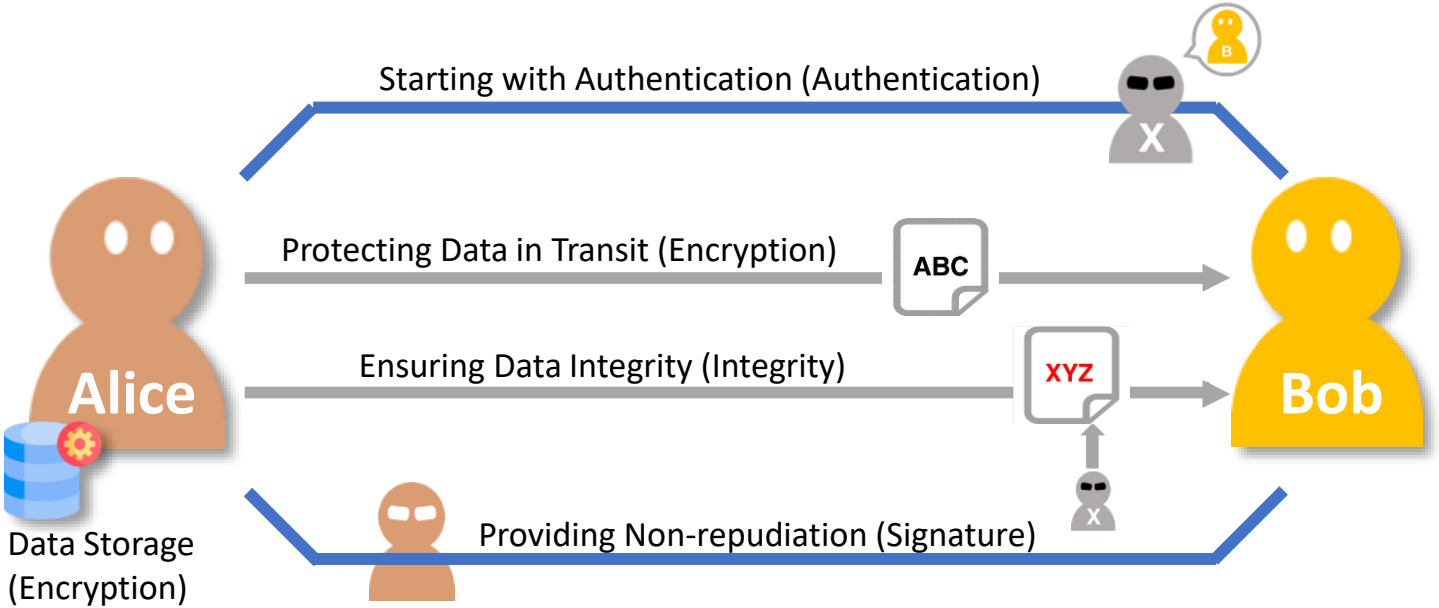
1. IP to SoC
2. Importance of Security
3. Threats and Root-of-Trust
4. Functionality of the Hardware Root of Trust

RoT for Internal and External Trusted Basis .



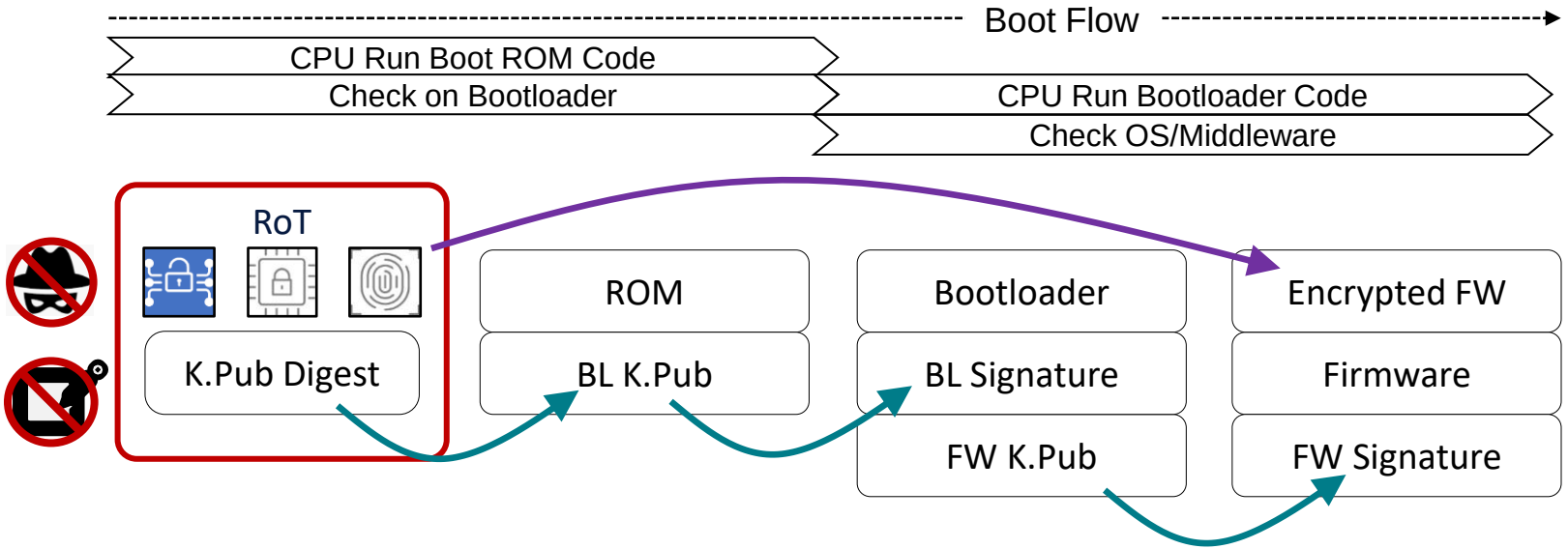
Root-of-Trust is the root of information. It should be trusted and free from doubt.

External Security: Secure Communication .



Security fundamentals: 1. trusted keys 2. certificate for authentication
3. digest for integrity check 4. cryptography for protecting the transmission

Internal Security: Secure Boot .



HRoT provides **Secure Storage**, **HUK** and **Cryptos** for: 1. As anchor of chain of trust, 2. RSA/ECC and SHA for digest and verification 3. FW protection using AES with local PUF key

Information that A RoT Should Protect .

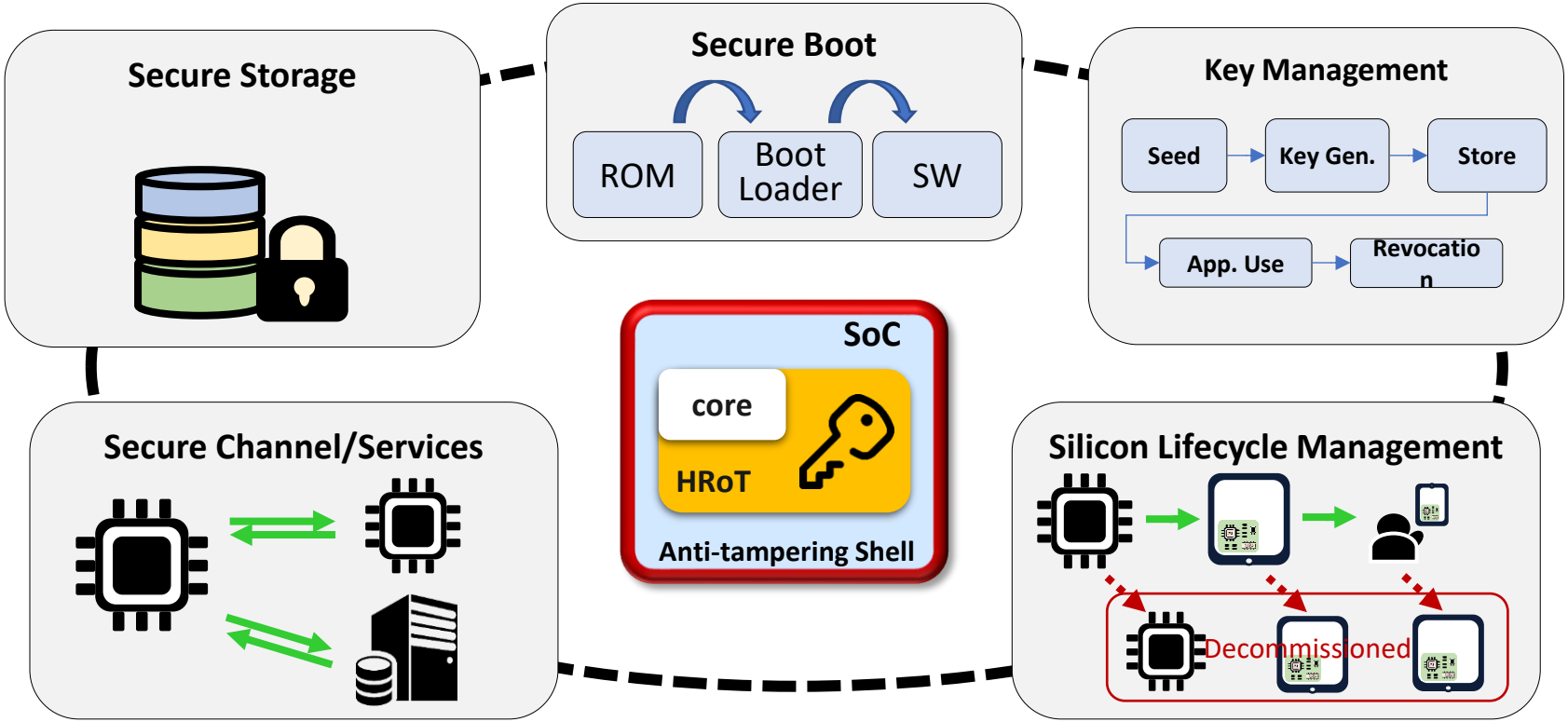
	For External Security	For Internal Security
Keys	• UID • Root Key (HUK) • Private/Public Key • Shared Key • CA Public key (Digest) • Global FW Key	• Root Key (HUK) • Private/Public Key • FW Public Key • Local KEK/Local FW Key
Certificate	Service Certificate (X.509)	FW Signature (Secure Boot) Key Certificate (X.509)
Secure Info.	Chip Lock/Unlock PWD	Versioning/Debugging

Can't be stolen (Must Important): HUK(Private Key), KEK (Local Key) and FW Key

Can’t be revised (For Secure Boot, Authentication): CA Public key and Certificate.

→ HRoT is needed to robustly protect these secret keys and information than RoT

HRoT: Supporting Secure Applications .



Fundamentals of HRoT .

Primitives	Design by	Reference
Anti-tampers	Analog + digital design	線上課程
Entropy: PUF	Analog + digital design	
Entropy: TRNG	Analog + digital design	
Secure Storage	NVM device + Anti-tampers	可選修類比電路 與記憶體設計相關課程
Cryptos-Engines	Digital design for AES, SHA, PKC	線上課程
Secure Enclave	SoC Architecture: Isolated boundary	W11 硬體安全設計及操作