Permission to Use Conditions

1. Permission is granted to copy and distribute this slide set for educational purposes only, provided that the complete bibliographic citation and following credit line is included: “Hardware Security Slides by F. Gebali. ©2024. Gebali”.
2. Permission is granted to alter and distribute this material provided that the following credit line is included: “Adapted from Hardware Security Slides by F. Gebali. ©2024. Gebali"
3. This material may not be copied or distributed for commercial purposes without express written permission of the copyright holder.

ECE 448/548 Cyber-System Security

Introduction

F. Gebali

EOW 433

Office Phone: 250-721-6509

https://ece.engr.uvic.ca/~fayez/

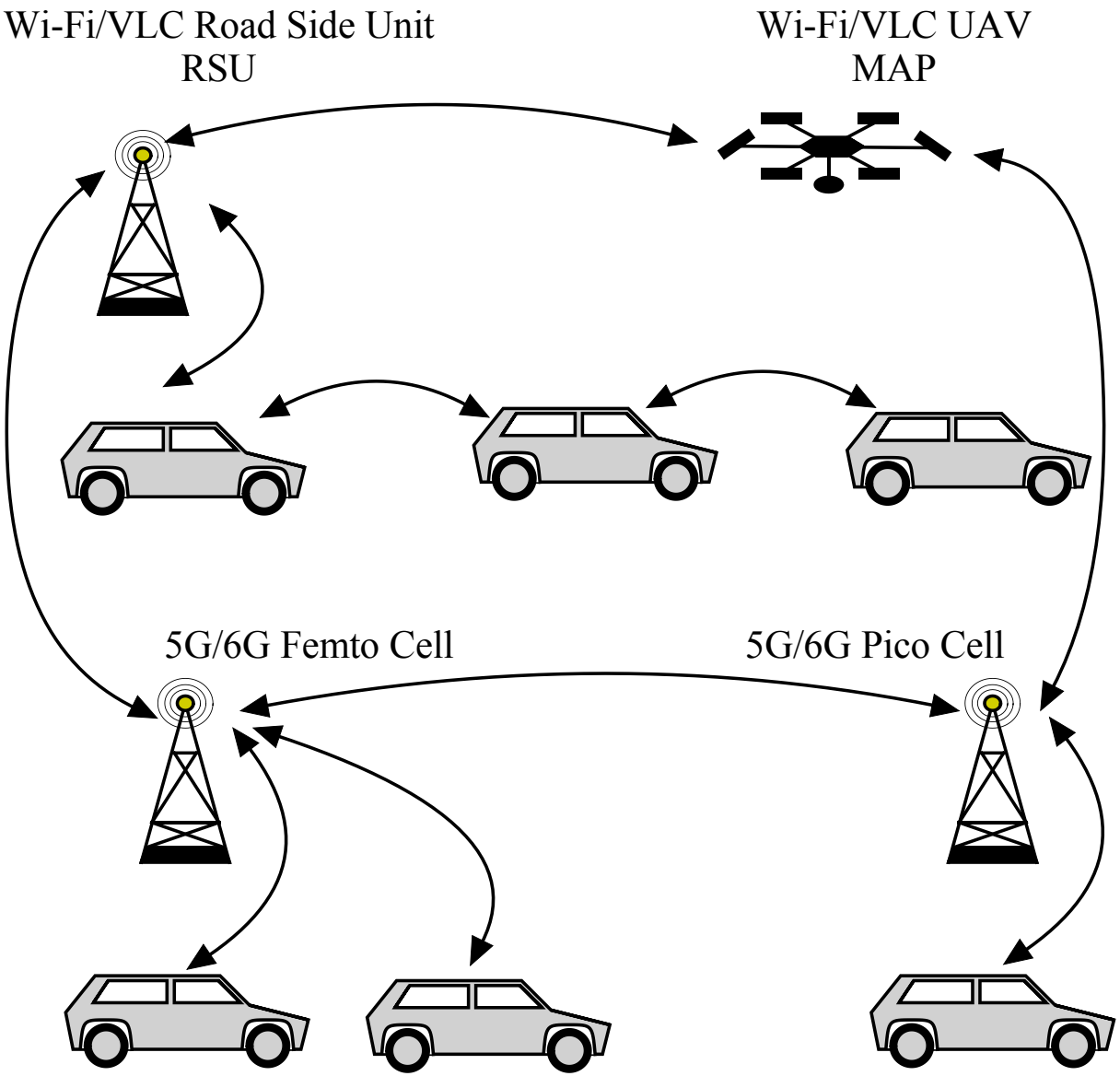
Outline

Introduction

Examples of Cybersystems

- Utilities
- Building Automation
- Manufacturing
- Government
- Agriculture
- Healthcare
- Retail & Wholesale
- Entertainment
- Education
- Transportation
- Finance

Case of 5G/6G & Wi-Fi: IoV, V2V, V2I, V2X, etc.

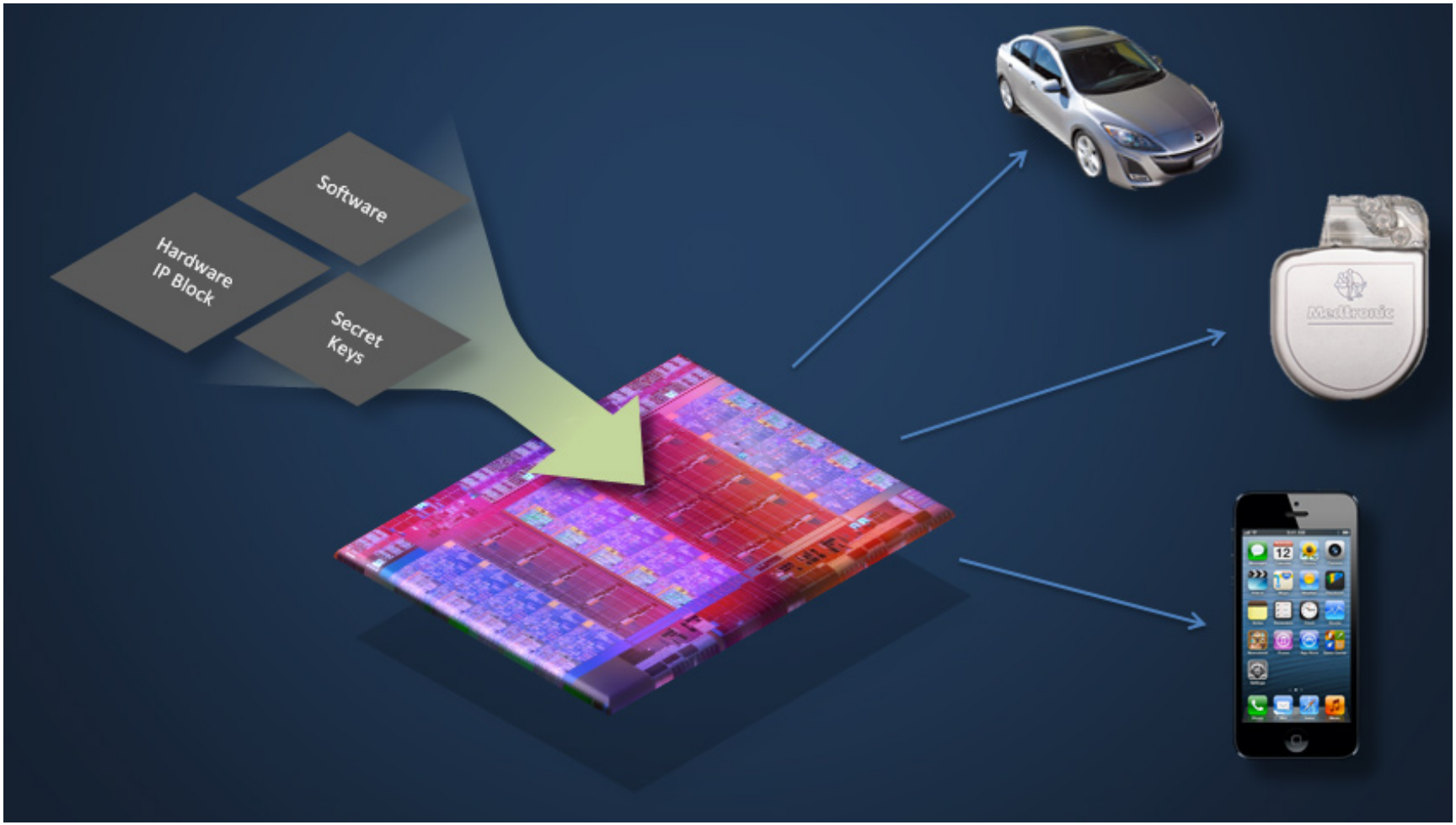


The Different Facets of Hardware Security

Elements of Security in General

1. Privacy (Data Hiding): Encryption & Decryption
2. Digital signature (non repudiation)
3. Authentication: Data, Humans, Hardware
4. Key management: generation, exchange, storage
5. Random number generation: PRNG, TRNG

Hardware Security: Embedded Systems



Motivation to Study Hardware Security

1. Embedded systems are in virtually all products.
2. Hardware was/is assumed a root of trust in a system.
3. Entropy source in random number generators
4. ICs are found in cybersystems:
    1. health care
    2. transportation
    3. industrial control (water treatment plants)
    4. power management
    5. military
    6. financial institutions
    7. Communications

Different Meanings of Hardware Security

1. Dedicated system that monitors network traffic (e.g. firewall)
2. Hardware security module (cryptoprocessor) in charge of doing: encryption; decryption; hashing; key managment
3. Critical infrastructure security (military, health, commerce, power)
4. IoT devices that must be protected

Prevalence of IoT Infrastructure: Biden-Harris Announcement

Traditional/Legacy Industrial Security Measures

1. Providing physical security such as access cards
2. Access control password protection for secured device
3. Install firewalls around secured device
4. Equipment security

IoT Attack Surface

1. Devices
2. Communication channels
3. Applications and software

Computer Security

- Network security: Attacks, availability, reliability
- Software security: Attacks, reliability
- Data security: authentication, availability, confidentiality, integrity, non-repudiation, utility
- Hardware security: Attacks, protection, trust

Why Encrypt Data?

1. Cryptography is essential for security
2. Protection against hacking
3. Regulations demand it for government, health care, commerce

Challenges of IoT Key Management

1. Generating many strong secret keys
2. Keeping those secret keys secret!
3. Sharing those keys with communicating entities

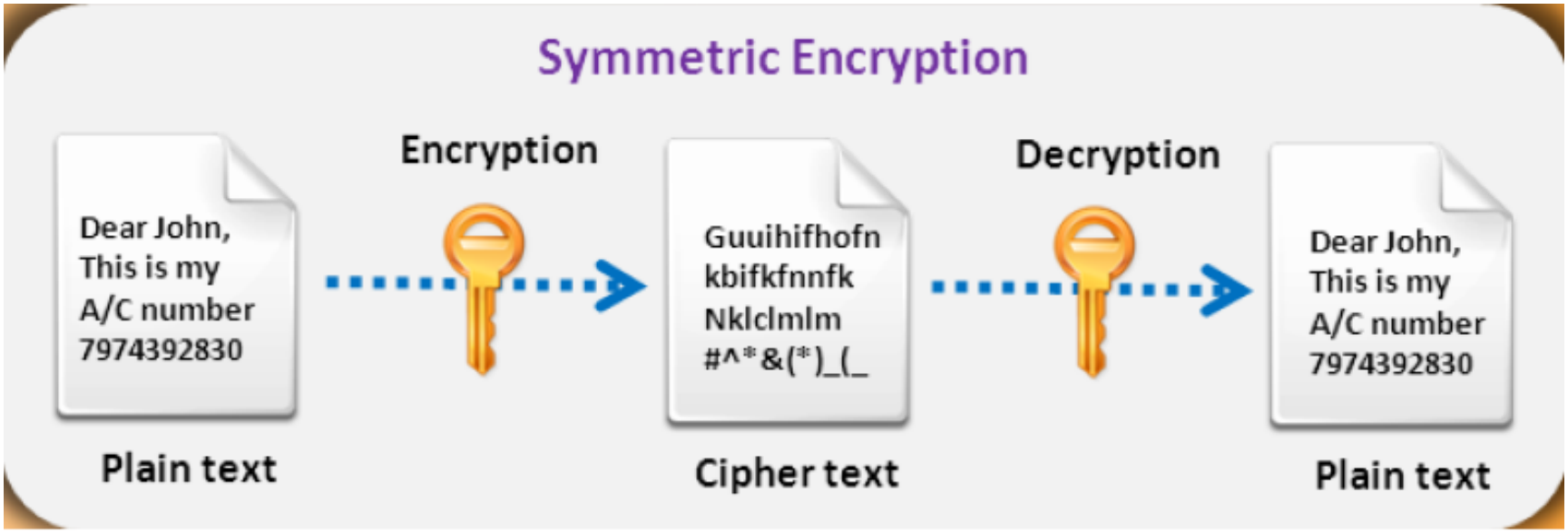
Ideal Solution to Key Management

1. Device has a set of strong root keys that are protected within the security boundary and not permanently stored
2. Device can generate many derived secret keys with different contexts (length, user, etc.)
3. Protect all keys
4. All of the above point to using PUFs

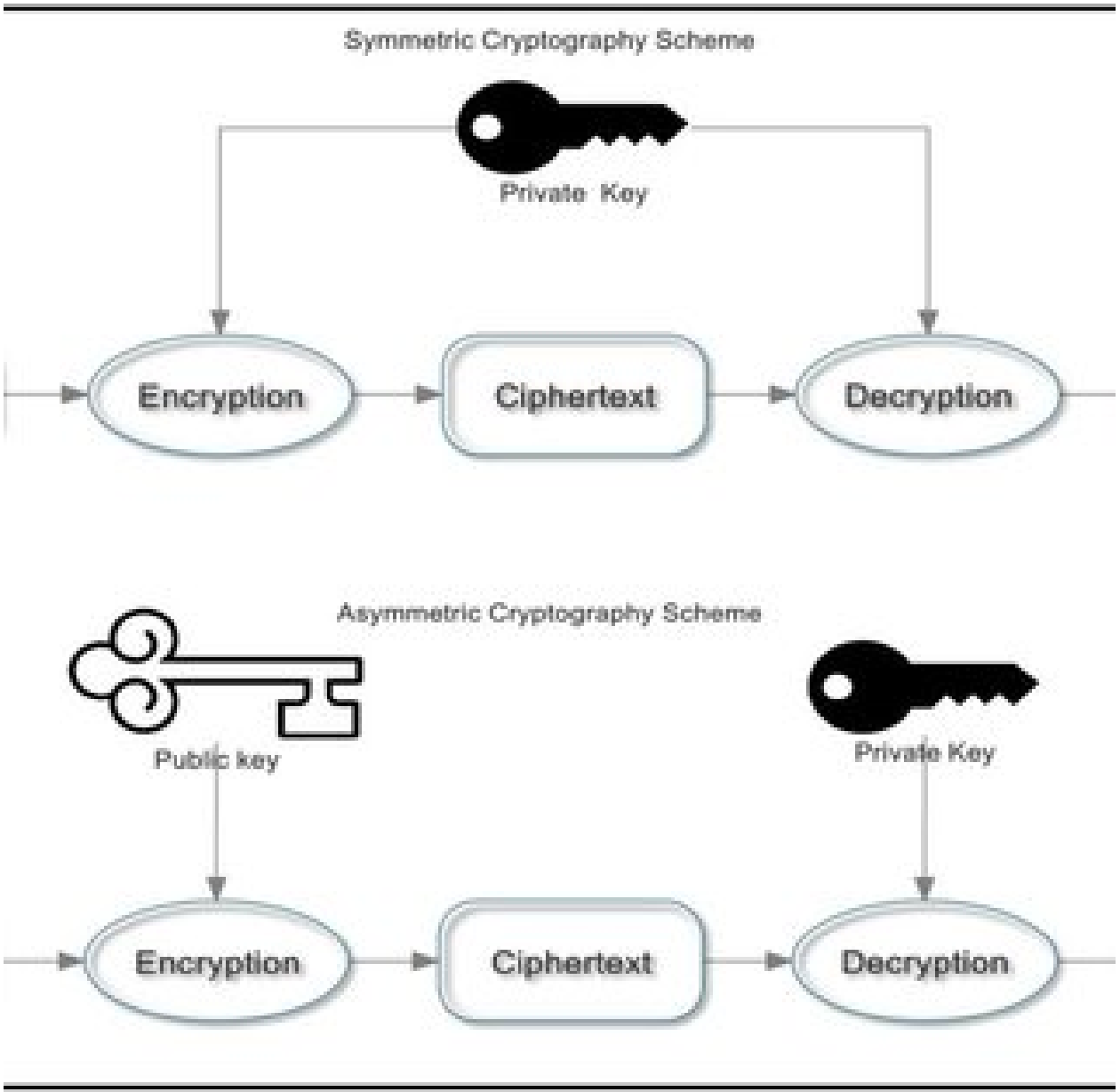
Three Types of Security Algorithms

1. Symmetric (secret key cryptography): AES, DES
   1. Encrypt and decrypt using same key
   2. Used in privacy and confidentiality
2. Asymmetric (public key cryptography): RSA, ECC
   1. Two related keys: one public, other secret
   2. Used for signatures, authentication, non-repudiation & key exchange
3. Hashing: SHA-1, SHA-3
   1. Compute a “cryptographic checksum” or “message digest” of messages or files
   2. Used for integrity & authentication

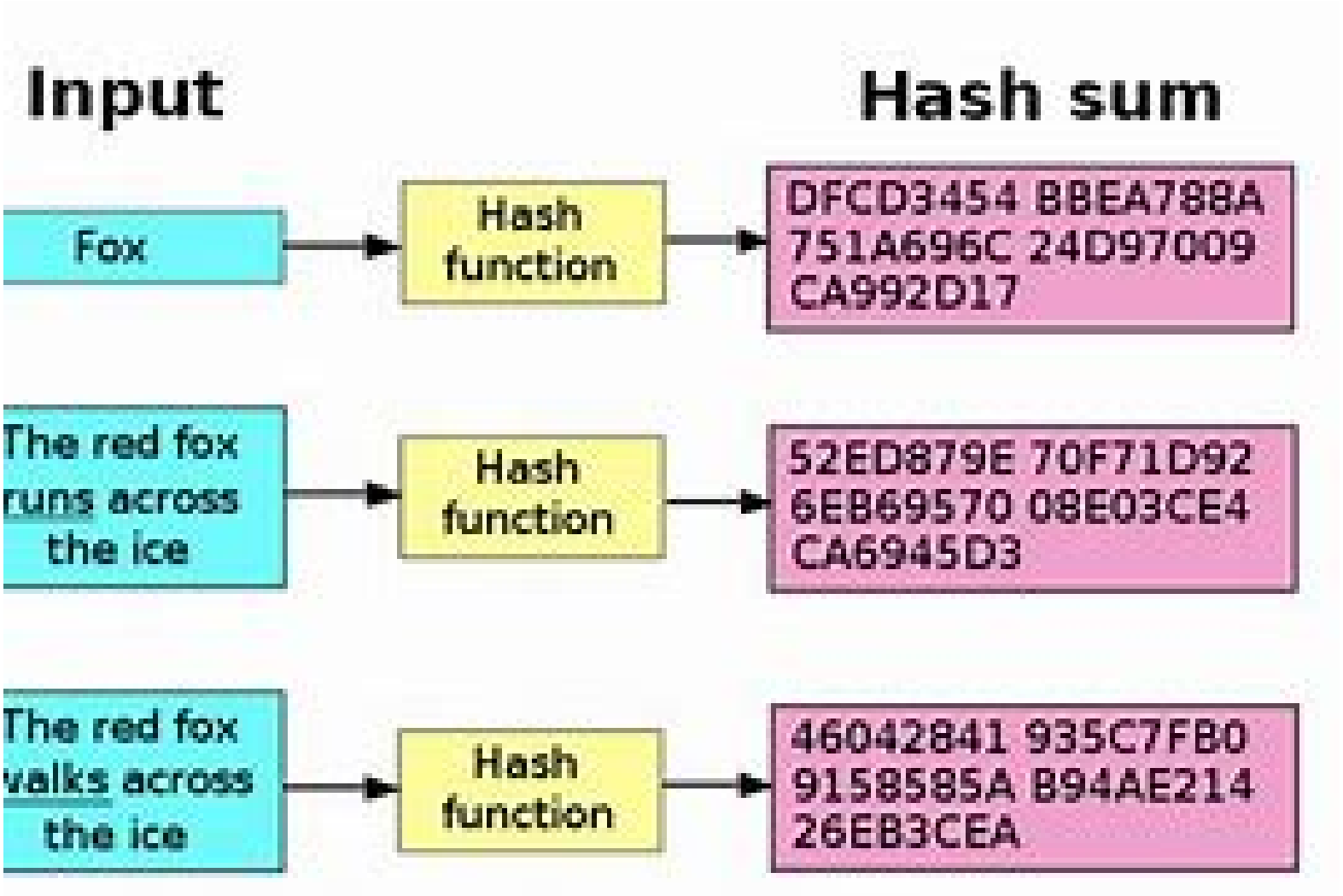
Symmetric Encryption: Same key for Encoding and Decoding



Asymmetric Encryption: K_s & K_p



Hashing: Different message length, same hash length



Security Threats

1. Storage and communication of confidential information
2. Management and control of important equipment
3. Critical security applications and systems

CIA Triad [1]

1. Confidentiality (privacy)
2. Integrity
3. Availability

Security Elements (mostly data and actors)

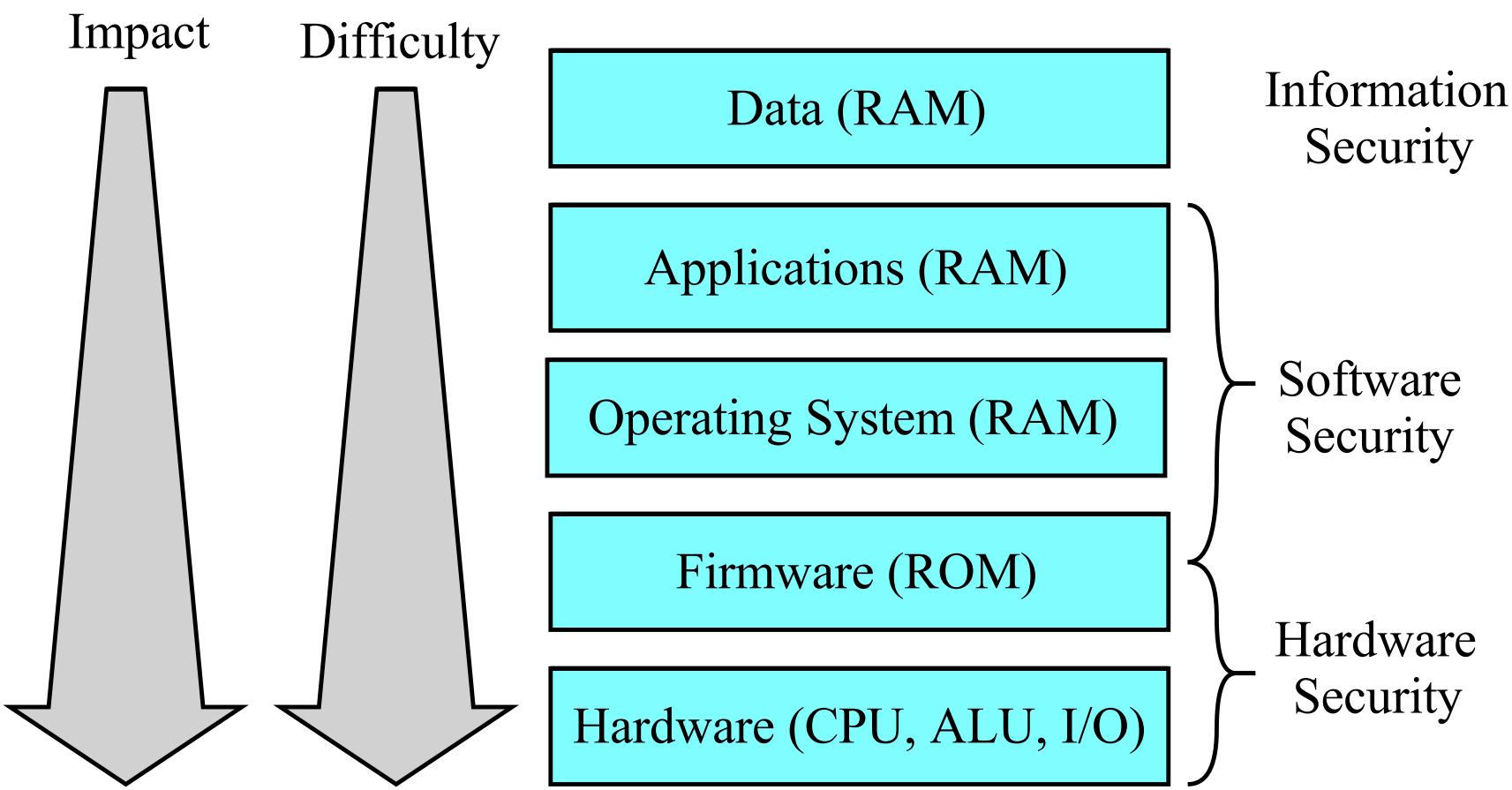
1. Authentication: Ensure entity is the one that it claims to be
2. Availability: Data can be accessed by authorized users
3. Confidentiality/Access control: allow only authorized users
4. Integrity: received data is exactly sent data
5. Non-repudiation: prevent denial by a user
6. Utility: Data is protected and can be recovered when needed

Hardware Role in Securing Software Stack

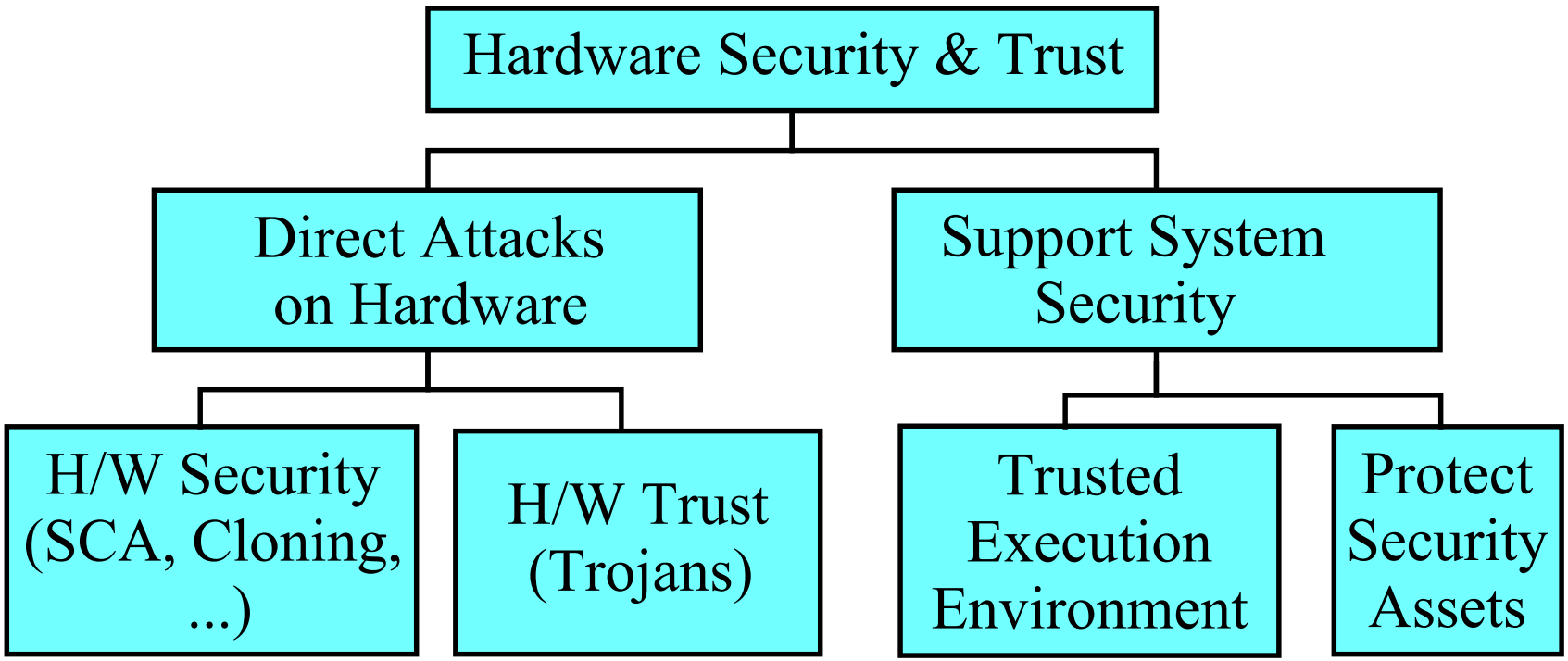
1. Hardware design, validation & implementation must ensure secure operation of S/W stack
2. Protect sensitive assets stored in hardware from malicious S/W & network activities
3. Separation between multiple user applications
4. Isolate secure and insecure data & code with respect to:
   1. Confidentiality: ability to observe data
   2. Integrity: ability to change it
   3. Availability: ability to access data/code by rightful owner

Hardware Attacks

Hardware Attacks Impact and Difficulty



Scope of Hardware Security & Trust



Scope of Hardware Security & Trust

1. Hardware security removes H/W vulnerability to attacks
2. Hardware security also supports S/W & system security
3. Hardware trust is about removing untrusted entities during H/W lifecycle

Scope of Hardware Attacks

1. Hardware attack types
2. Hardware attack avoidance
3. Hardware attack detection
4. Hardware attack countermeasures

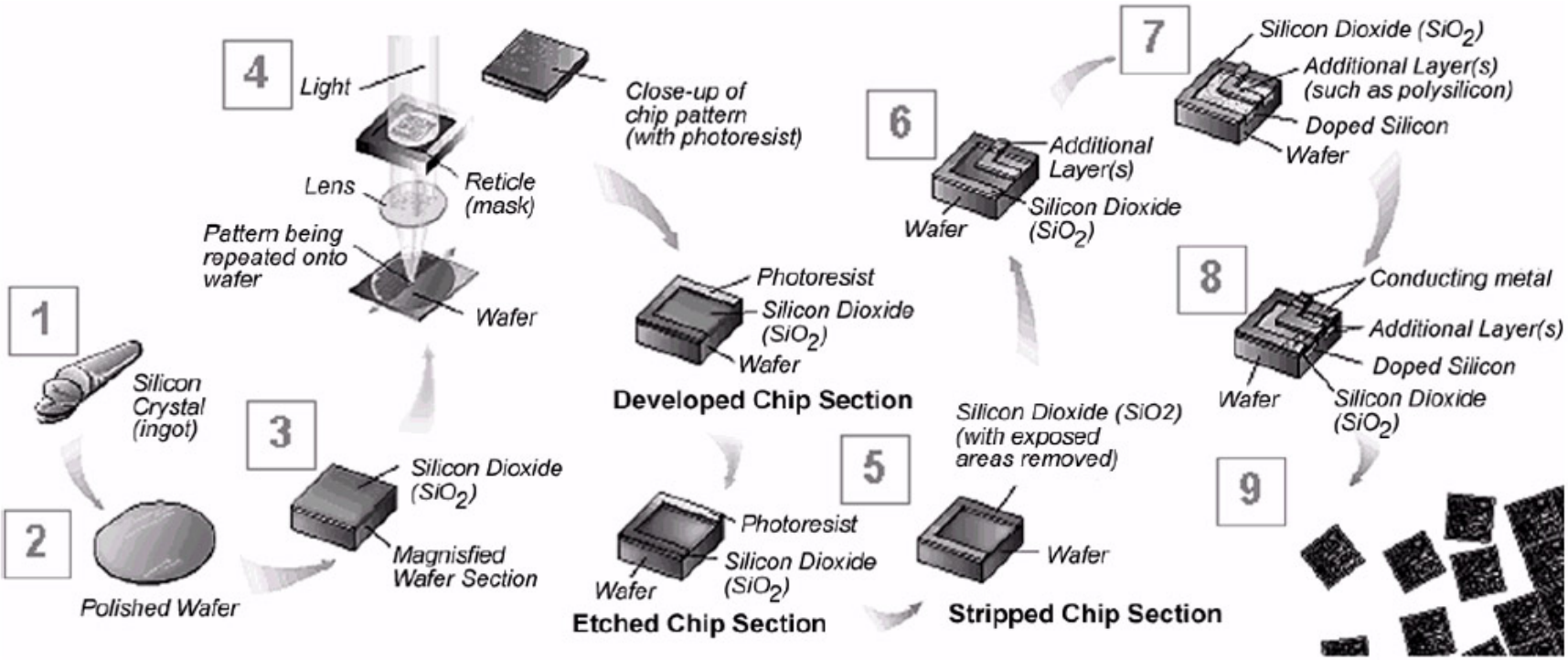
Hardware Attack Types

Hardware Attack Types

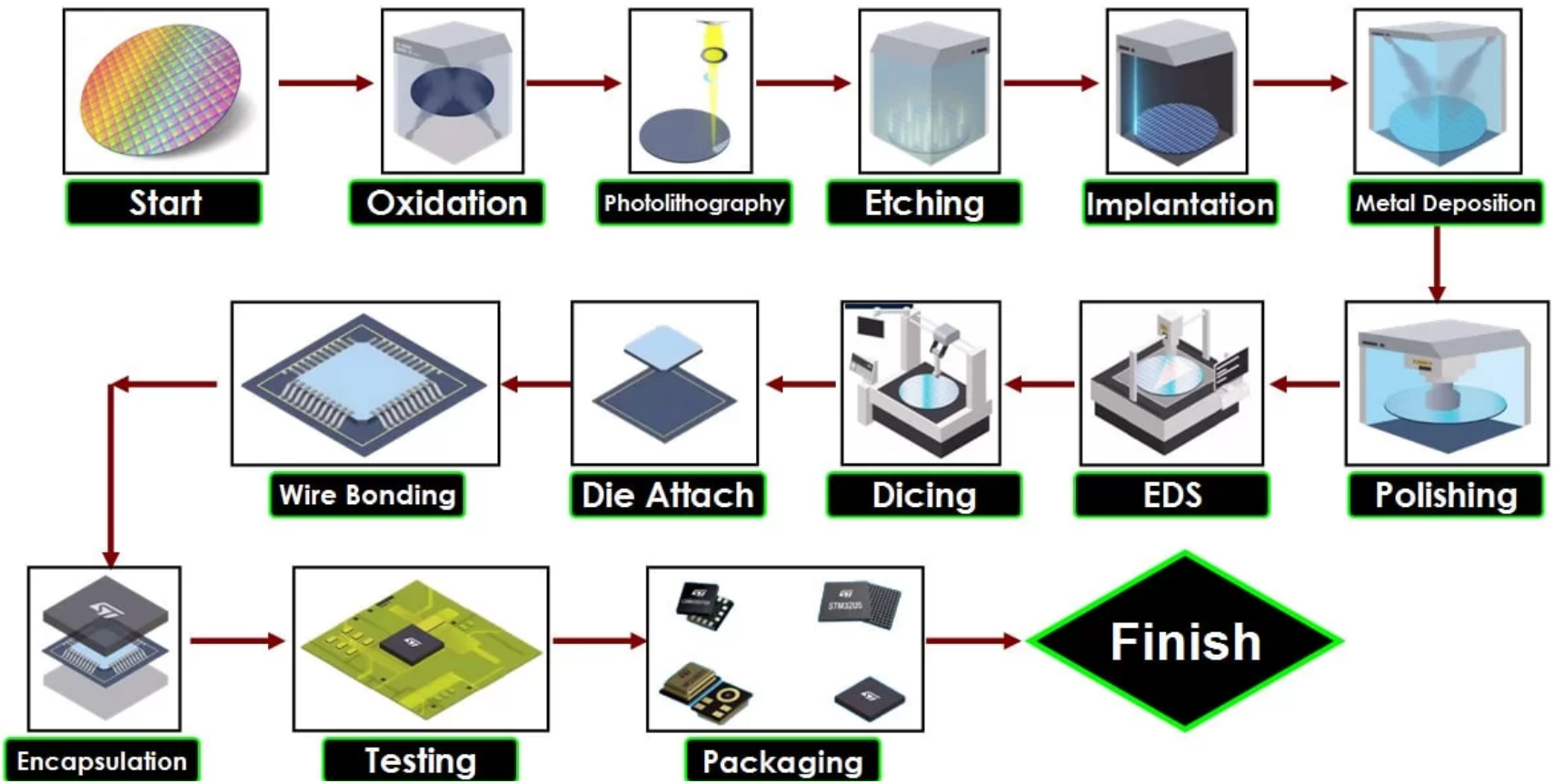
1. Piracy: cloning, counterfeiting, overproduction & recycling
2. Fault injection (FIA) [2] (e.g. Fuzzing or zero-day attacks)
3. Hardware Trojans (HW)
4. Reverse engineering (IP theft)
5. Attacks utilizing design for test (DFT) features
6. Side-channel attack (power, timing, radiation, etc.)
7. Tampering

Hardware IC Lifecycle/Supply Chain

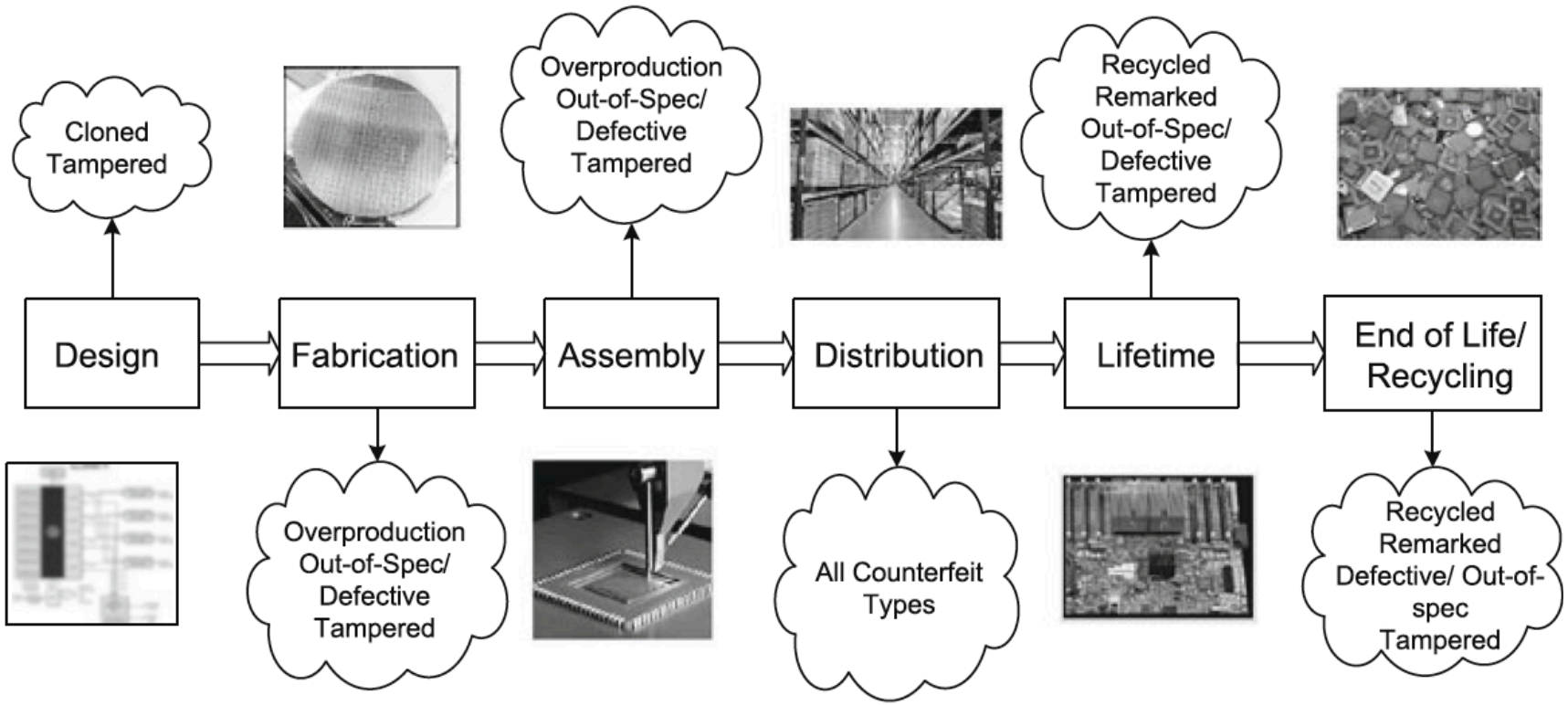
IC Fabrication Steps



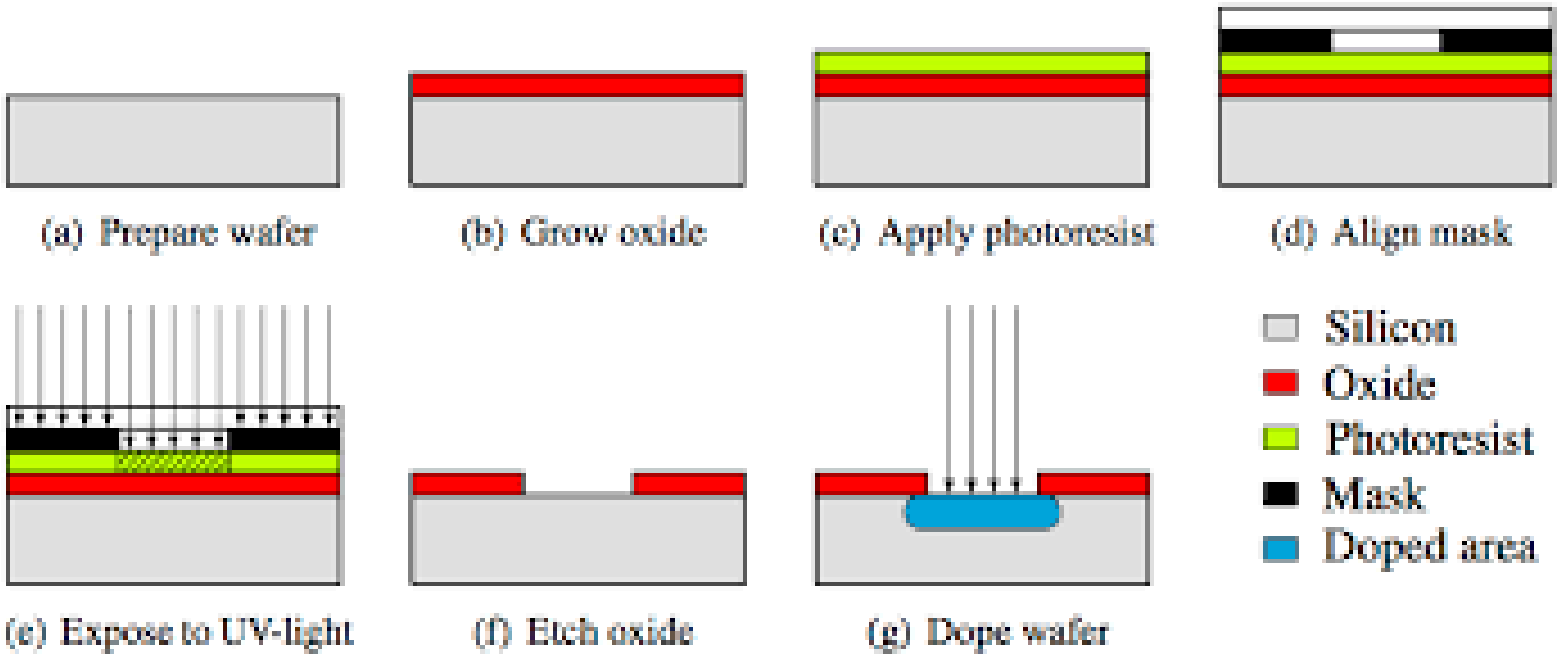
Another View of IC Fabrication Steps



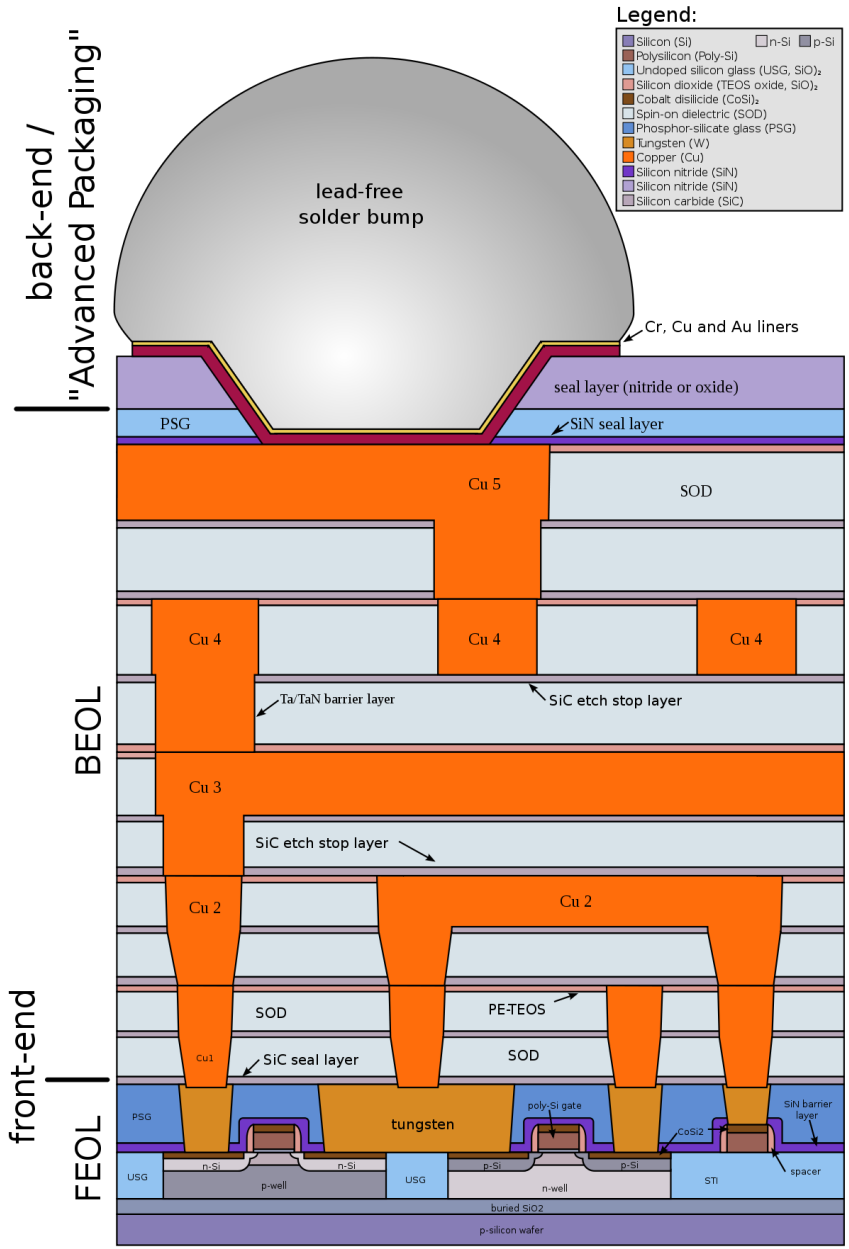
ICs Supply Chain & Potential Attacks [3]



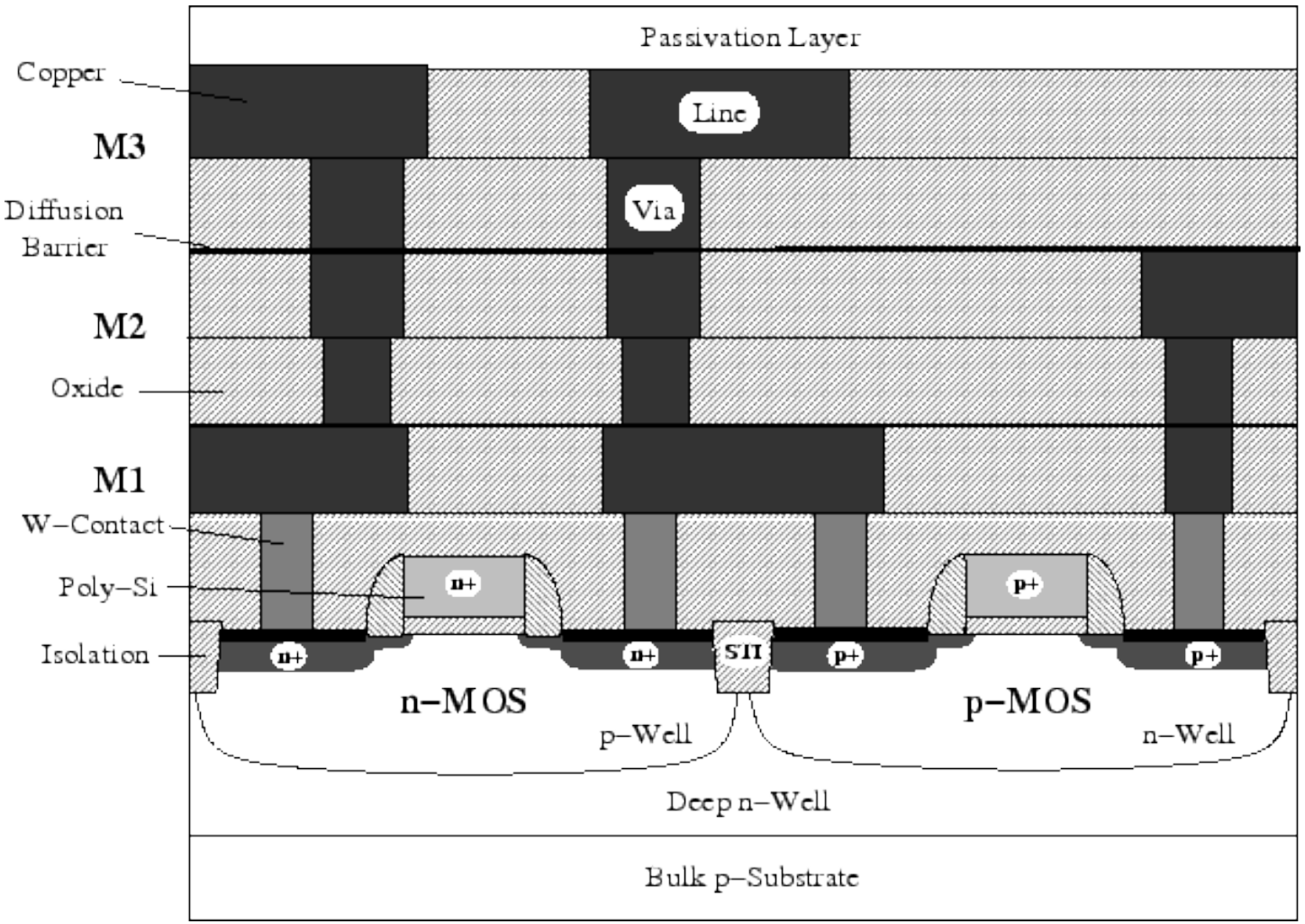
IC Masking Step: Nanometer resolution



Advanced CMOS IC Layers



Advanced CMOS IC Layers: Dual Well Technology



Hardware Lifecycle: Hardware Attack Opportunities

1. Hardware design specification & 3^{rd} party IP (3PIP)
2. Validation
3. Physical layout & mask fabrication
4. IC fabrication at silicon foundry (fab house)
5. IC test
6. IC packaging
7. System assembly
8. Operation in field
9. Firmware updates

Hardware Attack Enablers

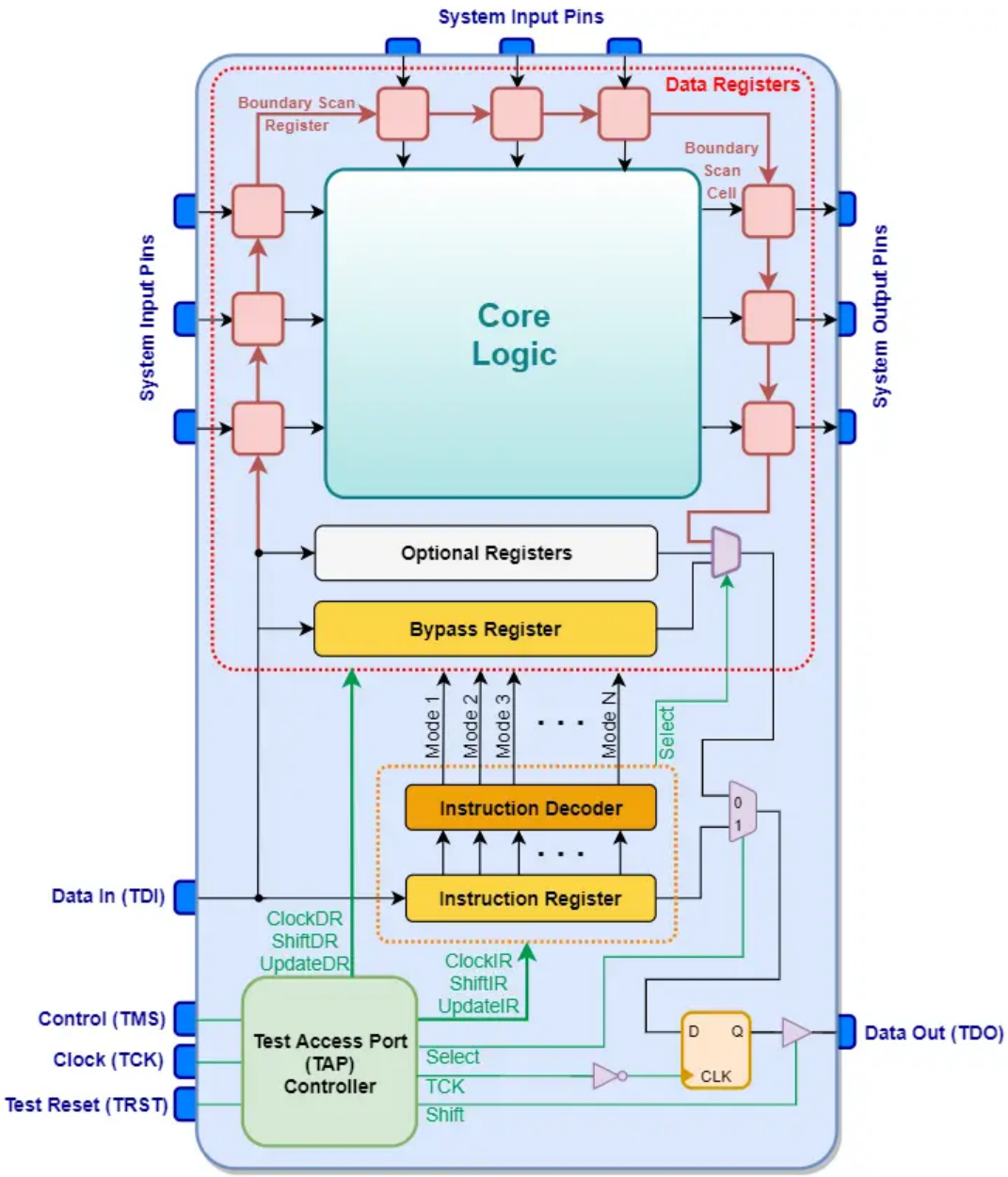
1. PCB outsourcing & contain ICs from many suppliers
2. IC fabrication outsourcing (overproduction)
3. IC designed using 3-rd party IPs (3PIP)
4. IC packaged by another company
5. IC distribution (recycle)

Conflict of Hardware Testing and Hardware Attacks

Conflict of Hardware Testing and Hardware Attacks

1. Design for test (DFT) is based on controllability and observability
2. Scan chain
3. Boundary scan (JTAG)
4. Built-in self test (BIST)

Joint Test Action Group (JTAG) Details



Hardware & Trust

1. Many occasions for attack during lifecycle (design, fabrication, test, etc.)
2. Hardware is vulnerable to side-channel, Trojan, tampering & piracy
3. Firmware updates

Security Attacks

1. Passive attacks: traffic analysis, side-channel attack
2. Active attacks: tampering, counterfeit, reverse engineering, Trojans

Motivation for Studying Hardware Attacks

1. Hardware Trojans are malicious alterations to the circuit during design or fabrication.
2. Trojan can destroy system or leak information.
3. Globalization of semiconductor design and fabrication introduces vulnerabilities.
4. Threats to military, transportation, financial, and civilian systems.

Past Incidents

1. European μp is being used in military systems and maker built backdoor to disable the system.
2. Processor test usually confined to test its functionality only. Extra non-interfering circuitry won't show up.
3. Attacks originate from countries that supplied the chip.
4. JTAG port contains undocumented commands
5. How can you test for "unspecified functions"?

What Can a Trojan Do?

1. Kill switch
2. Backdoor
3. The action could be triggered by:
    1. Issuing a command
    2. Rare combination of signals
    3. After a time period
    4. At random

Characteristics of a Kill Switch

1. Extra area or logic is added to the design.
2. Extra chip delay
3. Extra power consumption
4. The VHDL source code is modified.
5. Modify IC layout, doping, or gate oxide thickness

Hardware Attack Vectors: Attack Approaches

1. Side-channel
2. Trojans
3. IP piracy
4. Processor tampering

Hardware Attack Surface: Attack Types

1. Chip-level attacks: reverse engineering, cloning, Trojans, side-channel attacks, counterfeit
2. PCB-level attacks: tampering, piracy, JTAG ports, Trojans

[1] W. Chai, “What is the CIA triad (confidentiality, integrity and availability)?” https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA, 2023.

[2] B. Stevens, “Fault injection attacks: A growing plague,” https://www.eeweb.com/profile/bstevens/articles/fault-injection-attacks-a-growing-plague, Mar. 2019.

[3] M. Tehranipoor, H. Salmani, and X. Zhang, *Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection*. Springer, 2014.