PET ENGINEERING COLLEGE

An ISO 9001:2015 Certified Institution

Accredited by NAAC, Approved by AICTE, Recognized by Government of Tamil Nadu and Affiliated to Anna University

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – IV

HARDWARE SECURITY

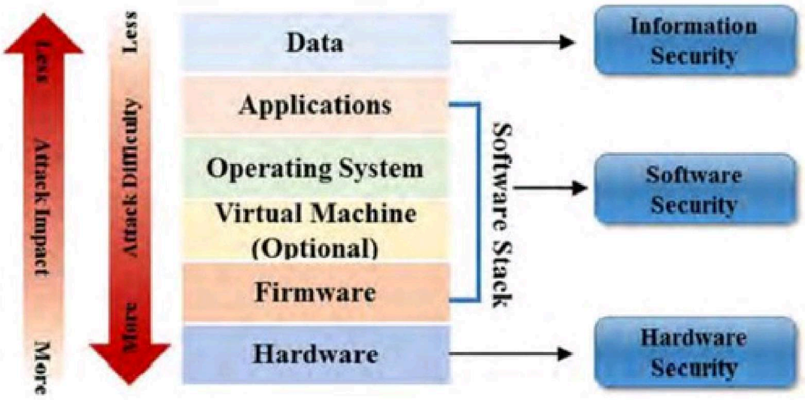
CLASS	**: S4 ECE**
SUBJECT CODE	**: EC3401**
SUBJECT NAME	**: NETWORKS AND SECURITY**
REGULATION	**: 2021**

UNIT V HARDWARE SECURITY 9

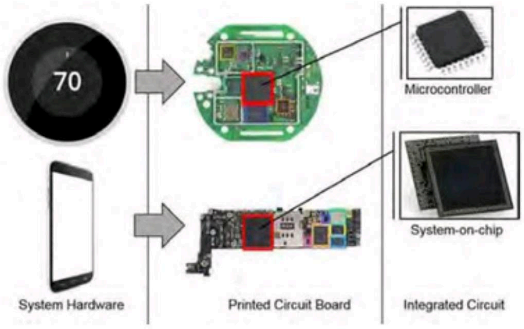
Introduction to hardware security, Hardware Trojans, Side – Channel Attacks – Physical Attacks and Countermeasures – Design for Security. Introduction to Block chain Technology.

LAYERS OF A COMPUTING SYSTEM:

- Modern computing systems can be viewed as an organization consisting of multiple layers of abstraction.
- The hardware layer lies at the bottom of it, followed by the firmware that interfaces with the physical hardware layer.
- The firmware layer is followed by the software stack, comprising of an optonal virtualization layer, the operating system (OS), and then the application layer.
- The data being processed by a computing system is stored in the hardware layer in volatile (for example, static or dynamic random access memory) or non-volatil (such as NAND or NOR flash) memory and accessed by the software layers.
- A system is connected to another system or to the Internet using networking mechanisms that are realized by a combination of hardware and software components.
- Computer security issues span all these layers



ELECTRONIC HARDWARE The hardware in a computing system can, itself, be viewed as consisting of three layers **System-level hardware**, that is, the integration of all physical components (such as PCBs, peripheral devices, and enclosures) At the next level, one or more PCBs used which provide mechanical support and electrical connection to the electronic components that are required to meet the functional and performance requirements of a system. At the bottom-most layer, we have active components (such as ICs, transistors, and relays), and passive electronic components.

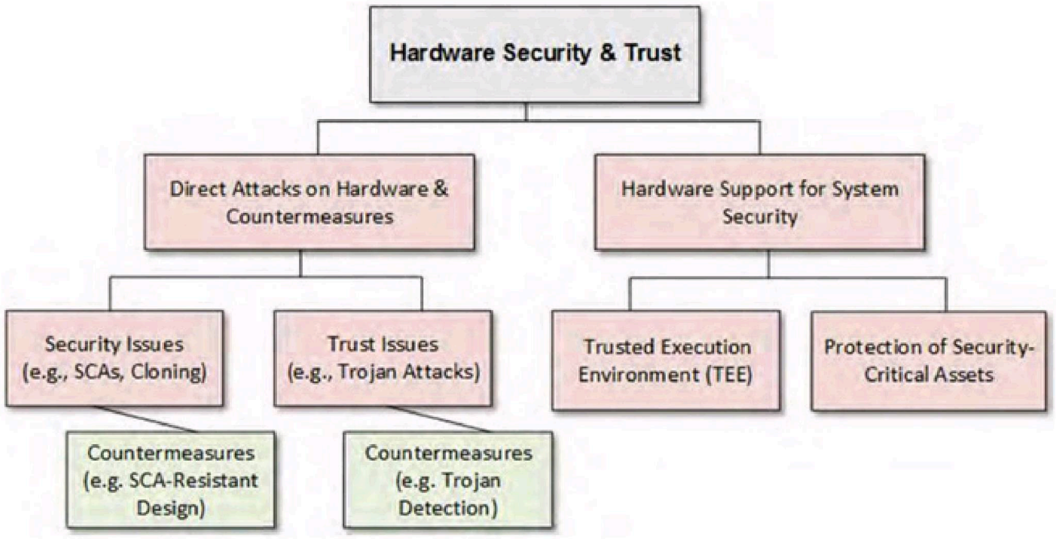


□ **HARDWARE SECURITY:** Emerging trends in electronic hardware production, such as intellectual-property-based (IP- based) system on chip (SoC) design, and a long and distributed supply chain for manufacturing and distribution of electronic components—leading to reduced control of a chip manufacturer on the design and fabrication steps—have given rise to many growing security concerns

□ Malicious modifications of ICs, also referred to as Hardware Trojan attacks , in an untrusted design house or foundry

□ Another important aspect of hardware security relates to th hardware design, implementation, and validation to enable secure and reliable operation of the software stack.

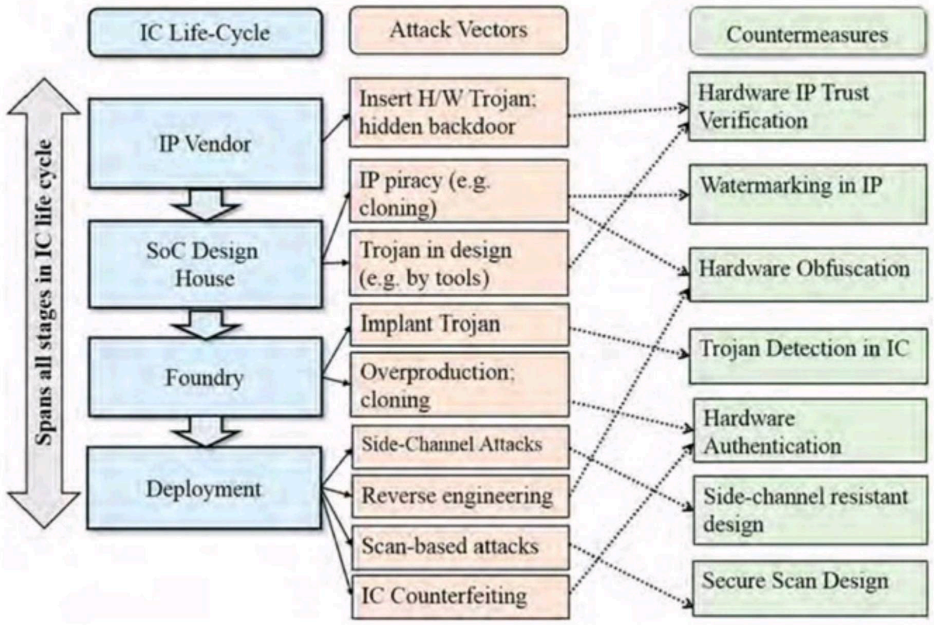
□ It deals with protecting sensitive assets stored in hadware from malicious software and network, and providing an appropriate level of isolation between secure and insecure data and code, in addition to providing separation between multiple user applications.


Hardware Security & Trust
Direct Attacks on Hardware & Countermeasures
Hardware Support for System Security
Security Issues (e.g., SCAs, Cloning)
Trust Issues (e.g., Trojan Attacks)
Trusted Execution Environment (TEE)
Protection of Security-Critical Assets
Countermeasures (e.g. SCA-Resistant Design)
Countermeasures (e.g. Trojan Detection)

□ **Hardware Trust:** Hardare trust issues arise from involvement of untrusted entities in the life cycle of hardware, including untrusted IP or computer-aided design (CAD) tool vendors, and untrusted design,
fabrication, test, or distribution facilities. These parties are capable of violating the trustworthiness of a hardware component or system.

□ They can potentially cause deviations from intended functional behavior, performance, or reliability.

□ Trust issues often lead to security concerns; for example, untrusted IP vendor can include malicious implant in a design, which can lead to denial of service (DoS), or information leakage attacks during field operation.



Hardware Trojans:

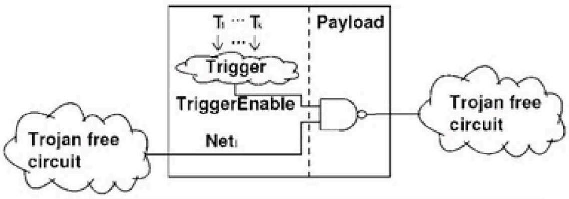
Hardware Trojans are malicious modifications to original circuitry inserted by adversaries to exploit hardware or to use hardware mechanisms to create backdoors in the design Hardware Trojans have reportedly been usd as ‘kill switches’ and backdoors in foreign military weapon system **Detection of hardware Trojans is extremely difficult, for several reasons:** Given the large number of soft, firm, and hard IP cores used in SoCs, and the high complexity of today’s IP
□ blocks, detecting a small malicious alteration is extremely difficult.
Nanometer SoC feature sizes make detection by physical inspection and destructive reverse
□ engineering very difficult, time consuming, and costly.
Trojan circuits, by design, are typically activated under very specific conditions which makes
□ them unlikely to be activated and detected using random or functional stimuli.
Tests used to detect manufacturing faults, such as stuck-at and delay faults cannot guarantee
□ detection of Trojans. Even when 100% fault coverage for all types of manufacturing faults is possible, there are no guarantees as far as Trojans are concerned.
As physical feature sizes decrease because of improvements in lithography, process and
□ environmental variations have an increasingly greater impact on the integrity of the circuit parametric behavior.

HARDWARE TROJAN STRUCTURE

The basic structure of a Trojan in a 3PIP (Party Intellectual Property) can include two main parts,
□ ~~**trigger and payload**~~
A Trojan trigger is an optional part that monitors various signals and/or a series of events in the
□ cir~~cuit. The paylo~~ad usually taps signals from the original circuit and the output of the trigger.

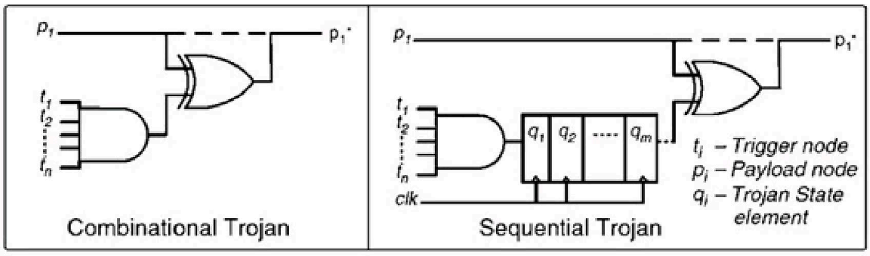
□

- Once the trigger detects an expected event or condition, the payload is activated to perform malicious behavior. Typically, the trigger is expected to be activated under extremely rare conditions, so the payload remains inactive most of the time. When the payload is inactive,
- the IC acts like a Trojan-free circuit, making it difficult to detect the Trojan.
- Figure shows the basic structure of the Trojan at gate level. The trigger inputs (T1,T2,...,Tk) come from various nets in the circuit. The payload taps the original signal Neti from the original (Trojan-free) circuit and the output of the Trigger.
- Since the trigger is expected to be activated under rare condition, the payload output stays at the same value most of the time, Neti. However, when the trigger is active, that is, Trigger Enable
- is “0”, the payload output will be different from Neti; this could result in injecting an erroneous value into the circuit and causing error at the output.



TROJAN MODELING

- In this model, it is assumed that a Trojan will be activated by rare circuit node conditions and will have its payload as a critical node in term of functionality, but low observable node in terms of testing, to evade detection during normal functional testing. If the Trojan includes
- sequential elements, such as rare-event triggered counters, then the Trojan may be even harder to detect. Figure shows generic models for combinational and sequential Trojans. The trigger condition is an n-bit value at internal nodes, which is assumed to be rare enough
- to evade normal functional testing. The payload is defined as a node that is inverted when the Trojan is activated.



- To make it more difficult to detect, one might consider a sequential Trojan, which requires the
- rare event to repeat 2m times before the Trojan gets activated and inverts the payload node.
- The sequential state machine is considered in its simplest form to be a counter, and the effect of the output on the payload is considered to be an XOR function to have maximal impact.

In more generic models, the counter can be replaced by any Finite State Machine (FSM) and the circuit can be modified as a function of Trojan output and the payload node.

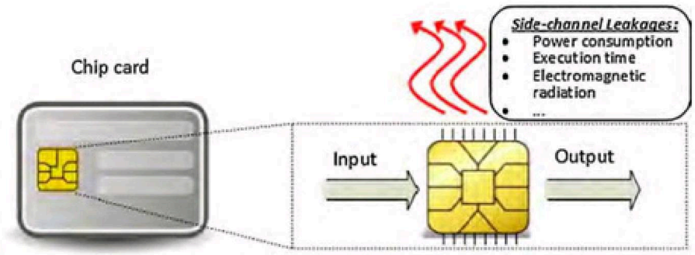
Side-channel attacks (SCA):

- It is a noninvasive attack that is based on targeting the implementation of a cryptographic algorithm rather than analyzing its statistical or mathematical weakness.

□ These attacks exploit physical information leaking from various indirect sources or channels, such as, the target device’s power consumption, electromagnetic (EM) radiation, or the time taken for a computation. These channels are referred to as “side channels”. The information

□ embedded in side-channel parameters depend on the intermediate values computed during the execution of a crypto-algorithm, and are correlated with the inputs and the secret key of the cipher An adversary can effectively extract the secret key by observing and

□ analyzing side-channel parameters with relatively cheap equipment, and within a very short time span, ranging from a few minutes to a few hours.

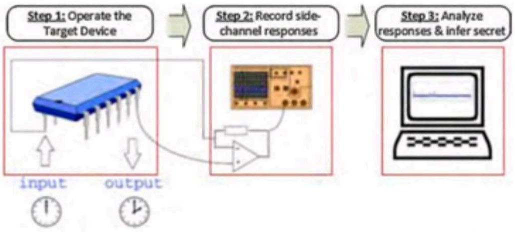


□ Figure illustrates how a device leaks side-channel information while operating. Common sidechannel attacks, such as power attacks, monitor the device’s power consumption. Typically, this is done by incorporating a current path at Vdd or GND pin of a chip, which is performing the cryptographic operation, to record power dissipation or such an operation.

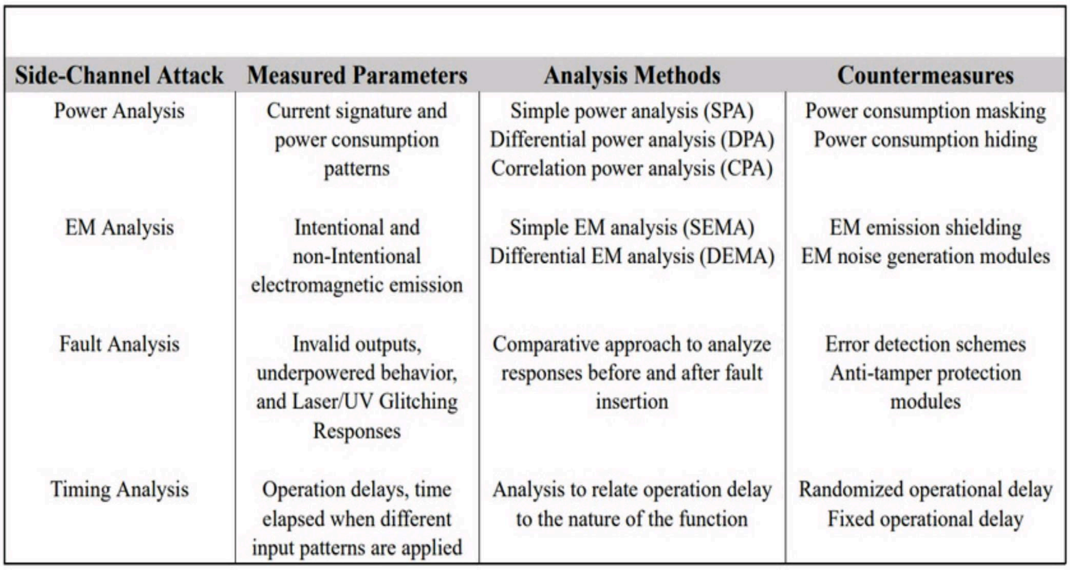
□ The device’s power consumption captures switching activity of the relevant transistors, which depends on inputs to a cryptographic function, uch as the plaintext and the key.

□ Simple power analysis (SPA) is a technique to directly interpret the collected traces of power consumption for a set of inputs.

□ It requires relatively detailed knowledge about the implementation of a cryptographic algorithm and a skilled adversary to interpret secret key information by visually examining the power consumption.


Step 1: Operate the Target Device
Step 2: Record side-channel responses
Step 3: Analyze responses & infer secret
input
output

Analysis of side channel effects



Side-Channel Attack	Measured Parameters	Analysis Methods	Countermeasures
Power Analysis	Current signature and power consumption patterns	Simple power analysis (SPA) Differential power analysis (DPA) Correlation power analysis (CPA)	Power consumption masking Power consumption hiding
EM Analysis	Intentional and non-Intentional electromagnetic emission	Simple EM analysis (SEMA) Differential EM analysis (DEMA)	EM emission shielding EM noise generation modules
Fault Analysis	Invalid outputs, underpowered behavior, and Laser/UV Glitching Responses	Comparative approach to analyze responses before and after fault insertion	Error detection schemes Anti-tamper protection modules
Timing Analysis	Operation delays, time elapsed when different input patterns are applied	Analysis to relate operation delay to the nature of the function	Randomized operational delay Fixed operational delay

Physical attacks and countermeasures:

Physical attacks are divided into three categories: noninvasive, semi-invasive, and invasive attacks.

Noninvasive attack:

□ It does not require any initial preparations of the device under test, and will not physically harm the device during the attack.

□ The attacker can either tap the wires to the device, or plug it into a test circuit for the analysis.

□ **Invasive attack:**

□ It requires direct access to the internal components of the device, which normally requires a well-equipped and knowledgeable attacker to succeed.

These attacks are more demanding and expensive, as feature sizes shrink, and device complexity increases.

Semi Invasive attack:

□ There is a large gap between noninvasive and invasive attacks. Many attacks fall into this gap, called semi-invasive attacks.

□ They are not very expensive as classical penetrative invasive attacks, but are as easily repeatable as noninvasive attacks.

Reverse Engineering:

□ Reverse engineering (RE) is the process involving the thorough examination of an object to achieve a full understanding of its construction and/or functionality.

□ RE is now widely used to clone, duplicate, or reproduce systems and devices in various security-critical applications, such as smartcards, smartphone, military, financial, and medical systems

Chip Level RE:

□ A chip is an IC comprised of electronic devices that are fabricated using semiconductor material.

□ A chip has package material, bond wires, a lead frame, and die. Each die has several metal layers, vias, interconnections, passivation, and active layers

□ RE of chips can be nondestructive or destructive. X-ray tomography is a nondestructive method of RE that can provide layer-by-layer images of chips, and is often used for the analysis of internal vias, traces, wire bonding, capacitors, contacts, or resistors.

PCB-level RE:

□ Electronic chips and components are mounted on a laminated nonconductive PCB and

□ electrically interconnected using conductive copper traces and vias.

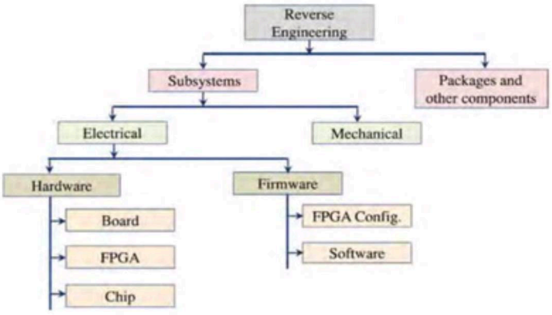
□ The board might be single or multilayered, depending on the complexity of the electronic system.

Delayering or x-ray imaging could be used to identify the connections, traces, and vias of the internal PCB layers.

System-level RE:

□ Electronic systems are comprised of chips, PCBs, and firmware.

□ A system's firmware includes the information about the system's operation and timing, and is typically embedded within nonvolatile memories (NVMs), such as ROM, EEPROM, and Flash



Equipments used for the analysis:

□ Optical high/super-resolution microscopy (digital).

□ Scanning electron microscopes.

□ Transmission electron microscopes.

□ Focused ion beam

□ Scanning capacitance microscopy.

□ High-resolution x-ray microscopy.

Board level PCB:

□ The goal of board-level RE is to identify all components on the board and the connections

□ between them.

□ All of the components used in a design are called the bill of materials (BOM)

□ Some electronic components mounted on the PCB can be identified easily through the use of IC markings, but fully custom and semicustom ICs are difficult to identify.

Using standard off-the-shelf parts with silkscreen annotations will assist the RE process.

The IC Markings normally divided into four parts

• The first is the prefix, which is the code that is used to identify the manufacturer. It could be a one to a three-letter code, although a manufacturer might have several prefixes. • The second part is the device code, which is used to identify a specific IC type. • The next part is the suffix, which is used to identify the package type and temperature range. Manufacturers modify their suffixes frequently. • A four-digit code is used for the date, where the first two digits identify the year and the last two identify the number of the week.

□ If the IC marking is not readable, because it has faded away due to prior usage in the field or the manufacturer did not place a marking for security purposes, the reverse engineer could strip off the package, and read the die markings to identify the manufacturer and the chip's functionality

Probing Attack Targets

□ It is essential for both attackers and countermeasure designers to determine which signals are more likely to be targeted in a probing attack. Such signals are termed as assets. **Keys:** Keys of an encryption module are archetypal assets. They are usually stored in nonvolatile memory on the chip. If the key is leaked, the root of trust it provides will become compromised, and could serve as a gateway to more serious attacks. **Firmware and configuration bit stream:** Electronic intellectual properties (IPs), such as low-level program instruction sets, manufacturer firmware, and FPGA configuration bit streams are often sensitive, mission critical, and/or contain trade secrets of the IP owner **On-device protected data:** Sensitive data, such as health and personal identifiable information, should be kept private **Device configuration:** Device configuration data control the access permissions to the device. They specify which services or resources can be accessed by each individual user

Essential Steps of a Probing Attack:

□ Decapsulation

□ Reverse Engineering

□ Locating target wires

□ Reaching target wire and extracting information

Existing countermeasures and Limitations:

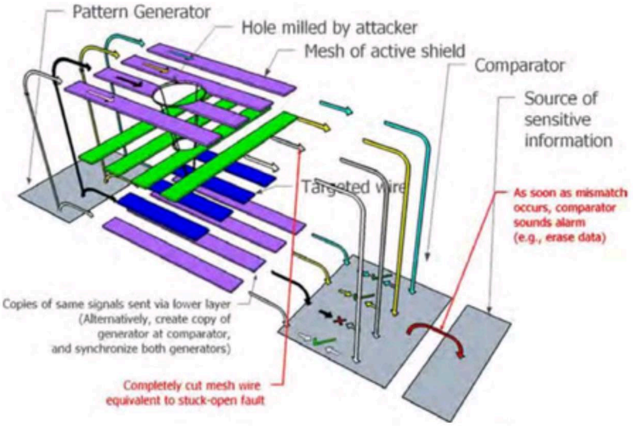
Active Shields

□ In this approach, a shield which carries signals is placed on the top-most metal layer to detect holes milled by FIB.

□ The shield is referred to as "active" because signals on these top layer wires are constantly monitored to detect if milling has cut them

□ A digital pattern is generated from a pattern generator, transmitted through the shield wires on top-most metal layer, and then compared with a copy of itself transmitted from lower layer.

□ If an attacker mills through the shield wires on top layer to reach target wire, the hole is expected to cut open one or more shield wires, thereby leading to a mismatch at the comparator and triggering an alarm signal to erase or stop generating sensitive information.


Pattern Generator
Hole milled by attacker
Mesh of active shield
Comparator
Source of sensitive information
Targeted wire
As soon as mismatch occurs, comparator sounds alarm (e.g., erase data)
Copies of same signals sent via lower layer (Alternatively, create copy of generator at comparator, and synchronize both generators)
Completely cut mesh wire equivalent to stuck-open fault

Analog Shields and Sensors

□ Instead of generating, transmitting, and comparing digital patterns, analog shields monitor parametric disturbances with its mesh wires.

□ In addition to shield designs, the probe attempt detector (PAD) also uses capacitance measurement on selected security critical wires to detect additional capacitance introduced by a metal probe.

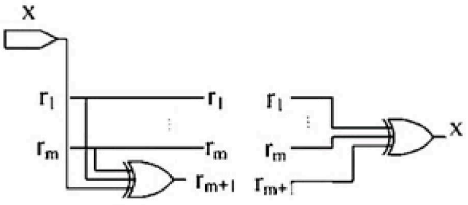
- Compared to active shields, analog shields detect probing without test patterns and require less area overhead.
- The PAD technique is also unique in remaining effective against electrical probing from the back-side.

The problem with analog sensors or shields is that analog measurements are less reliable due to process variations, a problem further exacerbated by feature scaling

t-Private Circuits

- The t-private circuit technique is proposed based on the assumption that the number of concurrent probe channels that an attacker could use is limited, and exhausting this resource deters an attack.
- In this technique, the circuit of a security-critical block is transformed so that at least t + 1 probes are required within one clock cycle to extract one bit of information.
- First, masking is applied to split computation into multiple separate variables, where an important binary signal x is encoded into t + 1 binary signals by XOR ing it with t independently generated random signals (rt+1 = x⊕r1⊕···⊕rt)
- The computations on x are performed in its encoded form in th transformed circuit. x can be recovered (decoded) by computing rt+1 = x⊕r1⊕···⊕rt.

The major issue with t-private circuit is that the area overhead involved for the transformation is prohibitively expensive.



Input and Output decoder for masking in t-private circuits

Other Countermeasure Designs

- One known countermeasure that deters decapsulation stage of probing attacks is a light sensor that is sometimes included in a tamper-resistant design.

Some other techniques include scrambling wires and avoiding repetitive patterns in shield mesh to impede the locating-targetwire stage of probing attacks.

Design for Security:

- The baseline architecture is typically derived from legacy architectures for previous products, adapted to account for the policies defined for the system under exploration. A SoC design may have a significant number of assets, often in the order of thousands, if not more. Not all assets are statically defined; many assets are created at different IPs during the system execution.

During system execution, these modes are passed to the cryptographic engine, which generates the cryptographic keys for different IPs, and transmits them through the system network-onchip (NoC) to the respective IPs. Each participant in this process has sensitive assets during different phases of the system execution. The security architecture must account for any potential access to these assets at any point of

- execution, possibly under the relevant adversary model.
- There are different Trusted Execution Environment(TEE) frameworks specifically developed for SoC designs .Some are,

Samsung KNOX: This architecture is specifically targeted toward smartphones, and provides secure separation features to enable information partition between business and personal content to coexist on the same system. It permits hot swap between these two content worlds, for example without requiring system restart. This architecture permits several system-level services, including the following:

- **Trusted boot** that is, preventing unauthorized OS and software from being loaded onto the device at startup.
- **Trust-zone-based integrity measurement architecture (TIMA)**, which continually monitors kernel integrity.
- **Security enhancement (SE)** for Android, an enforcement mechanism providing protection of system/user data based on confidentiality and integrity requirements through separation.
- **KNOX container**, which offers a secure environment in which protected business applications can run with guaranteed information separation from the rest of the device.

ARM Trust Zone

□ Trust Zone technology is a system-wide approach to provide security on high-performance
□ computing platforms.

□ The Trust Zone implementation relies on partitioning the SoC's hardware and software resources, so that they exist in two worlds: secure and nonsecure.

□ The hardware supports access control and permissions for the handling of secure/non secure applications, and the interaction and communication among them.

The software supports secure system calls and interrupts for secure runtime execution in a multitasking environment.

□ This protection extends to input/output (I/O), connected to the system bus via the Trust Zone enabled AMBA3 AXI bus fabric, which also manages memory compartmentalization.

Intel SGX

□ SGX is an architecture for providing a trusted execution environment provided by the underlying hardware to protect sensitive application and user programs or data against potentially malicious or tampered operating systems.

□ SGX permits applications to initiate secure enclaves or containers, which serve as so-called "islands of trust".

□ It is implemented as a set of new CPU instructions that can be used by applications to set aside such secure enclaves of code and data.

This enables

1) Applications to preserve the confidentiality and integrity of sensitive data without disrupting the ability of legitimate system software to manage the platform resources;

2) End users to retain control of their platforms, applications, and services even in the presence of malicious system software.

Introduction to Block chain technology:

□ Block chain is the backbone Technology of Digital CryptoCurrency BitCoin.

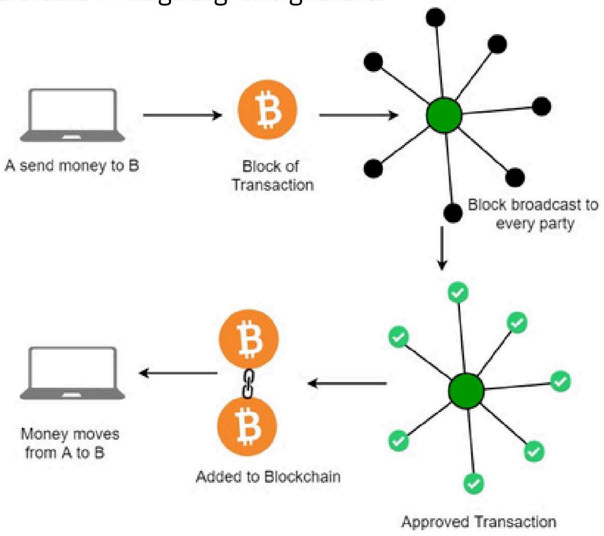
□ The block chain is a distributed database of records of all transactions or digital event that have
□ been executed and shared among participating parties.

□ Each transaction verified by the majority of participants of the system. It contains every single record of each transaction.

Bit Coin is the most popular crypto currency an example of the block chain.

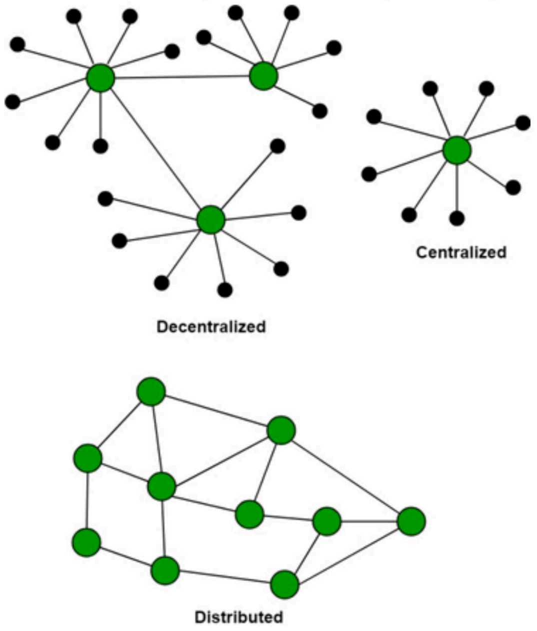
Bitcoin is a crypto currency and is used to exchange digital assets online.

- Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the internet.
- Each transaction protects through digital signature.



Distributed Database:

There is no Central Server or System which keeps the data of the Block chain.
The data is distributed over Millions of Computers around the world which are connected to the Block chain.
This system allows Notarization of Data as it is present on every node is publicly verifiable.



A network of nodes:

- A node is a computer connected to the Block chain Network.
- Node gets connected with Block chain using the client.
- Client helps in validating and propagating transaction on to the Block chain.
- When a computer connects to the Blockchain, a copy of the Block chain data gets downloaded into the system and the node comes in sync with the latest block of data on Block chain.

- The Node connected to the Block chain which helps in the execution of a Transaction in return for an incentive is called Miners.

Benefits of Block chain Technology:

- **Time-saving:** No central Authority verification needed for settlements making the process faster and cheaper.
- **Cost-saving:** A Block chain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of shared ledger.
- **Tighter security:** No one can temper with Block chain Data as it shared among millions of Participant. The system is safe against cybercrimes and Fraud.
- **Collaboration:** It permits every party to interact directly with one another while ot requiring third party negotiate.
- **Reliability:** Block chain certifies and verifies identities of every interested party. This removes double record, reducing rates and accelerates transactions.

Applications of Block chain:

- Leading Investment Banking Companies like Credit Suisse, JP Morgan Chase, Goldman Sachs and Citigroup have invested in Block chain and are experimenting to improve the banking experience and secure it. Following the Banking Sector, the Accountants are following the same
- path. Accountancy involves extensive data, including financial statements spreadsheets containing lots of personal and institutional data. Booking a Flight requires sensitive data ranging from the passenger’s name, credit card numbers, immigration details, identification,
- destinations, and sometimes even accommodation and travel

information. So the sensitive data can be secured uing block chain technology. Russian Airlines are working towards the same.

- Barclaysuses Block chain to streamline the Know Your Customer (KYC) and Fund Transfer processes while filling patents against these features.
- Visauses Blockchain to deal with business to business payment services.
- Unileveruses Block chain to track all their transactions in the supply chain and maintain the product’s quality at every stage of the process.
- Walmart has been using Block chain Technology for quite some time to keep track of their food items coming right from farmers to the customer.