Attack ID No	Sequence	Description of Attack
2	1	Attack ID2: Cyberattacks on IP companies (IP Piracy Attack), the attacker is tring to collect information

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	**Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2**	**Class 2 - Adversary An academic research group Attack Level can wage 1-3**	**Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3**	**Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4**
Highest Level	**2**	**3**	**3**	**4**
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?	Yes	Yes	Yes	Yes		

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Weak security defences in IT infrastructures • This type of attack aims to steal design secrets and intellectual properties (IP)

Defence ID (Card)	Defence
10 (5)	IP Piracy: Prevention Method: Split Manufacturing
11 (6)	IP Piracy: Prevention Method: Hardware Obfuscation - IC Camouflaging
12 (7)	IP Piracy: Prevention Method: Hardware Obfuscation - Combinational Logic Locking
13 (8)	IP Piracy: Prevention Method: Hardware Obfuscation - Sequential Logic Locking
14 (9)	IP Piracy: Detection Method: Watermarking - Digital Watermarking to hide information in the signal

Attack ID No	Sequence	Description of Attack
1	2	IC Overproduction – the adversary is able produce more copies by fraudulently imitating an original IC

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?			Yes			

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Outsourcing the IC fabrication • Ease of access to IC black markets • Ineffective regulations or law enforcement measures to protect IPs • Technical difficulty associated with detection of overproduced chips

Defence ID (Card)	Defence
3 (7)	Detection Method: Fingerprinting Conventional serial numbers
4 (8)	Detection Method: Fingerprinting DNA Marking
5 (9)	Detection Method: Fingerprinting: Physical Unclonable Functions
6 (10)	Detection Method: Fingerprinting: Digital Fingerprinting

Attack ID No	Sequence	Description of Attack
4	3	Fault Injection Attack - In this case, an adversary can induce errors during the computation of a cryptographic algorithm to generate faulty results

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	False	True
Attacker	**Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2**	**Class 2 - Adversary An academic research group Attack Level can wage 1-3**	**Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3**	**Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4**
Highest Level	**2**	**3**	**3**	**4**
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Susceptibility of electronics circuit to temperature variations, supply voltage fluctuations and electromagnetic interference
Defence ID (Card)	Defence
27 (K)	Prevention Method: Fault Injections Attacks Tamper Resistant Techniques

Attack ID No	Sequence	Description of Attack
5	4	Chip reverse engineering attack – the attacker has access to a working chip files and able to extract the IP gate-level netlist using a range of tools and reverse engineering technologies

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	**Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2**	**Class 2 - Adversary An academic research group Attack Level can wage 1-3**	**Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3**	**Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4**
Highest Level	**2**	**3**	**3**	**4**
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?				Yes		

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Correlation between circuit layout and the gate-level netlist and ultimately the design functionality
Defence ID (Card)	Defence
10 (5)	IP Piracy: Prevention Method: Split Manufacturing
11 (6)	IP Piracy: Prevention Method: Hardware Obfuscation - IC Camouflaging
12 (7)	IP Piracy: Prevention Method: Hardware Obfuscation - Combinational Logic Locking
13 (8)	IP Piracy: Prevention Method: Hardware Obfuscation - Sequential Logic Locking
14 (9)	IP Piracy: Detection Method: Watermarking - Digital Watermarking to hide information in the signal

Attack ID No	Sequence	Description of Attack
3	5	Rowhammer attack used as a mechanism by waging a persistent attack to cause large number of errors

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	True	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • This is a form of fault attack which exploits the fact that repeated accesses to DRAM can cause bits to flip in adjacent DRAM rows

Defence ID (Card)	Defence
19 (10)	Detection Method: Monitoring the rate of cache misses for unusual peaks using
21 (Q)	Prevention Method: Increase memory refresh frequency, use less leaky memory technology

Attack ID No	Sequence	Description of Attack
19	6	An attacker installs a Trojan in attempt to perform malicious operations (Side-channel analysis)

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Correlation between side-channel information and secret data being computed

Defence ID (Card)	Defence
15 (10)	SCA Detection Method: Side Channel Analysis - Leakage reduction approaches; Noise injection methods
16 (J)	SCA Detection Method: Side Channel Analysis - Architecture Optimisation
17 (Q)	SCA Prevention Method: Speculative Execution Attacks - Bounds check bypass; Branch target injection; Rogue data cache load

Attack ID No	Sequence	Description of Attack
12	7	An attacker can compromise the software updates or patch to add own functionality to gain control of a system

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	True	False
Attacker	**Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2**	**Class 2 - Adversary An academic research group Attack Level can wage 1-3**	**Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3**	**Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4**
Highest Level	**2**	**3**	**3**	**4**
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Software updates/patches (SolarWinds/Stuxnet)
Defence ID (Card)	Defence
20 (J)	Prevention or Detection Methods: Cyber Physical Attacks Monitor predefined constraints; Strict one-way communication from IC to cyber physical system command centre

Attack ID No	Sequence	Description of Attack
14	8	An attacker has access to a fabrication facility and ability to obtain a gate-level netlist of the chip through reverse engineering or other IP piracy methods to clone the ICs

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?						

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Ease of access to IC black markets • Lack of regulations or law enforcement measures to protect IPs • Technical difficulty associated with detection of cloned chips
Defence ID (Card)	Defence
5 (9)	Detection Method: Fingerprinting: Physical Unclonable Functions

Attack ID No	Sequence	Description of Attack
7	9	Recover discarded chips then repackaged and sold in the market as new

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?						Yes

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Availability of remarking technologies • Unmatched demands for certain types of ICs (e.g. military grade, discontinued chips)
Defence ID (Card)	Defence
3 (7)	Detection Method: Fingerprinting Conventional serial numbers
4 (8)	Detection Method: Fingerprinting DNA Marking
5 (9)	Detection Method: Fingerprinting: Physical Unclonable Functions
6 10)	Detection Method: Fingerprinting: Digital Fingerprinting

Attack ID No	Sequence	Description of Attack
22	10	An attacker can compromise a cryptosystem by analysing the time taken to execute cryptographic algorithms (Cache timing attack)

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • The dependency of the memory access time on the location of data item being fetched (e.g. whether or not it is present in the cache or the main memory)
Defence ID (Card)	Defence
15 (10)	SCA Detection Method: Side Channel Analysis - Leakage reduction approaches; Noise injection methods

Attack ID No	Sequence	Description of Attack
28	11	An attacker has, collected a subset of all challenge–response pair (CRPs) of the IC PUF and uses Machine Learning to derive a numerical model from this CRP data, which correctly predicts the PUF's responses to arbitrary challenges with high probability

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • PUF design is simple hence can be modelled using machine learning algorithms
Defence ID (Card)	Defence
18 (K)	Prevention Method: PUF Modelling Attacks - Response Obfuscation, Multi-PUF Design

Attack ID No	Sequence	Description of Attack
11	12	Hardware Trojan inserted by attacker into the design file

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	False	True
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?	Yes					

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Outsourcing of IP development and IC fabrication • High complexity of integrated circuits that makes it harder to detect Trojan

Defence ID (Card)	Defence
23 (9)	Prevention Method: Hardware Trojan Insert Replace functional cells to implement an LFSR/MISR-like circuit that generates a digital signature
24 (10)	Prevention Method: Hardware Trojan Insert Pre-silicon detection
25 (J)	Prevention Method: Hardware Trojan Insert Post-silicon detection
26 (Q)	Detection Method: Hardware Trojan Insert Runtime detection

Attack ID No	Sequence	Description of Attack
17	13	An attacker uses a Rowhammer techniques to undermine the integrity of electronics systems by facilitating an elevation of privilege attack

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	True	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?						

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • DRAM physical structure and fabrication technology
Defence ID (Card)	Defence
21 (Q)	Prevention Method: Increase memory refresh frequency, use less leaky memory technology

Attack ID No	Sequence	Description of Attack
20	14	An attacker can break the isolation between different applications running on the same machine, which they can then steal/copy sensitive data from a victim process (Speculative execution attack)

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Speculative operations can affect the micro-architectural state, such as information stored in Translation Lookaside Buffers (TLBs) and caches, which may lead to leakage of sensitive data when combined with Cache side-channel attacks
Defence ID (Card)	Defence
15 (10)	SCA Detection Method: Side Channel Analysis - Leakage reduction approaches; Noise injection methods
16 (J)	SCA Detection Method: Side Channel Analysis - Architecture Optimisation
17 (Q)	SCA Prevention Method: Speculative Execution Attacks - Bounds check bypass; Branch target injection; Rogue data cache load

Attack ID No	Sequence	Description of Attack
25	15	An attacker is able to recycle ICs and repackage them as new IC and able to pass physical inspection

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?						Yes

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Availability of remarking technologies • Unmatched demands for certain types of ICs (e.g. military grade, discontinued chips)
Defence ID (Card)	Defence
2 (6)	Detection Method: Physical Inspection: X-Ray Inspection; Visual Inspection

Attack ID No	Sequence	Description of Attack
16	16	An attacker has Access to PUF response/challenge pairs and can complete a PUF modelling attack (PUF modelling attack)

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • PUF design is simple hence can be modelled using machine learning algorithms
Defence ID (Card)	Defence
18 (K)	Prevention Method: PUF Modelling Attacks - Response Obfuscation, Multi-PUF Design

Attack ID No	Sequence	Description of Attack
24	17	An attacker can create copies of smartcard by monitoring the power consumption is able break the cryptographic functions create unauthorized signatures and clone the device

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Correlation between side-channel information and secret data being computed
Defence ID (Card)	Defence
1 (5)	Detection Method: Side Channel Analysis Differential Power Analysis (DPA)

Attack ID No	Sequence	Description of Attack
27	18	A malicious recycling centres can recycle ICs as if they were new and can be used as ICs are not chip locked

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?						Yes

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • The standard chip/package/system level tests are often inadequate in detecting various forms of counterfeit ICs • IC authentication are often not attractive due to significant design effort
Defence ID (Card)	Defence
8 (Q)	Prevention Method: Anti-fuse-Based Package-Level Defence

Attack ID No	Sequence	Description of Attack
23	19	An attacker can monitor the external outputs of the hardware while cryptographic operations are running with the goal of attempting to gain information which would result in the security of the device being compromised

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Correlation between side-channel information and secret data being computed
Defence ID (Card)	Defence
15 (10)	SCA Detection Method: Side Channel Analysis - Leakage reduction approaches; Noise injection methods

Attack ID No	Sequence	Description of Attack
9	20	Remote CLKSCREW (read as "clock screw") attack that exploits the security of energy management systems in ICs to compromise the system's availability

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	True	False
Attacker	**Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2**	**Class 2 - Adversary An academic research group Attack Level can wage 1-3**	**Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3**	**Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4**
Highest Level	**2**	**3**	**3**	**4**
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Unfettered software access to energy management hardware • Ability of the hardware regulators to be able to push voltage/frequency past the operating limits • Using the same power domain across security boundaries

Defence ID (Card)	Defence
22 (K)	Prevention or Detection Methods: Tamper-Proof Design

Attack ID No	Sequence	Description of Attack
13	21	Attack is able to insert Trojan in the RTL code, during the system integration or during the manufacturing of the Integrated Circuit (IC)

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	False	True
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?			True			

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Outsourcing of IP development and IC fabrication • High complexity of integrated circuits that makes it harder to detect Trojan

Defence ID	Defence
23 (9)	Prevention Method: Hardware Trojan Insert Replace functional cells to implement an LFSR/MISR-like circuit that generates a digital signature
24 (10)	Prevention Method: Hardware Trojan Insert Pre-silicon detection
25 (J)	Prevention Method: Hardware Trojan Insert Post-silicon detection
26 (Q)	Detection Method: Hardware Trojan Insert Runtime detection

Attack ID No	Sequence	Description of Attack
30	22	An attacker can replace valid firmware images with malicious images or make alterations to existing firmware

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	True	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?			Yes	Yes	Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • The firmware is not signed, or integrity checked by trusted element on the component

Defence ID (Card)	Defence
22 (K)	Prevention or Detection Methods: Tamper-Proof Design

Attack ID No	Sequence	Description of Attack
29	23	An attacker in the untrusted foundry has access only to the complete IC design as by manufacturing the front-end-of-line (FEOL) layers and back-end-of-line (BEOL) in same foundry

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?			Yes			

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Many design companies cannot afford owning and acquiring expensive foundries; hence, outsourcing their fabrication process

Defence ID (Card)	Defence
10 (5)	IP Piracy: Prevention Method: Split Manufacturing

Attack ID No	Sequence	Description of Attack
26	24	A malicious foundry can replicate programable data and overbuild the ICs because of transparency of their designed IP to the foundry that requires a complete description of the design components and layout to fabricate the ICs

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	**Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2**	**Class 2 - Adversary An academic research group Attack Level can wage 1-3**	**Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3**	**Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4**
Highest Level	**2**	**3**	**3**	**4**
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?			Yes			

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Vulnerability of the serial numbers and digital identification numbers to cloning
Defence ID (Card)	Defence
7 (J)	Prevention Method: Active IC Metering: Active metering, force new IC process to be activated

Attack ID No	Sequence	Description of Attack
21	25	An attacker uses microprobing by attaching a microscopic needle onto the internal wiring of a chip, which allows reading out internal signals and revealing sensitive data that are not meant to leave the chip

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					True	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • The transmission of sensitive information on the internal wires without sufficient protection
Defence ID (Card)	Defence
14 (9)	IP Piracy: Detection Method: Watermarking - Digital Watermarking to hide information in the signal

Attack ID No	Sequence	Description of Attack
18	26	The attacker is to be able to inject an intentional fault, using a series of techniques to manipulate the environmental conditions of a circuit, that results in the desired fault effect

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	False	False	True
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?					Yes	

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	28
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Inject a fault in the computation against almost all known ciphers
Defence ID (Card)	Defence
28 (8)	IP encrypted so that even if the IC is physically attacked, its IP cannot be deciphered

Attack ID No	Sequence	Description of Attack
10	27	Reverse engineering attack – by using De-capsulation that is the removal of the chip's packaging and De-processing which consists of removing the chip layers one by one in reverse order and photographing each layer, this information will be used to re-construct the netlist and ultimately expose design secrets

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	3			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?			Yes			

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Correlation between circuit layout and the gate-level netlist and ultimately the design functionality

Defence ID (Card)	Defence
11 (6)	IP Piracy: Prevention Method: Hardware Obfuscation - IC Camouflaging
12 (7)	IP Piracy: Prevention Method: Hardware Obfuscation - Combinational Logic Locking
13 (8)	IP Piracy: Prevention Method: Hardware Obfuscation - Sequential Logic Locking

Attack ID No	Sequence	Description of Attack
15	28	An attacker has access to a fabricated chips and IC remarking tool to remark ICs

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?			Yes	Yes	Yes	Yes

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Ease of access to fabricated ICs • Availability of remarking technologies • Unmatched demands for certain types of ICs • Lack of regulations or law enforcement measures to protect IPs • Technical difficulty associated with detection of cloned chips

Defence ID (Card)	Defence
3 (7)	Detection Method: Fingerprinting Conventional serial numbers
4 (8)	Detection Method: Fingerprinting DNA Marking
6 (10)	Detection Method: Fingerprinting: Digital Fingerprinting

Attack ID No	Sequence	Description of Attack
8	29	IP theft attack by a malicious engineer in the SoC design house, who has access to third party IPs, can steal design secrets

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	False	True	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?	Yes	Yes				

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Single company having access to the layout files of the design, making it easy to recover the IP by rogue employees
Defence ID (Card)	Defence
10 (5)	IP Piracy: Prevention Method: Split Manufacturing

Attack ID No	Sequence	Description of Attack
6	30	Selling defective chips Defective ICs are chips that have failed the functional or parametric tests or found to be out of spec, and subsequently placed in the market as authentic products

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	1			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?				Yes		

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Ease of access to IC black markets
Defence ID (Card)	Defence
9 (K)	Prevention Method: Supply Chain Compromise IC Supply Chain Assurance