iems
intelligente eingebettete
mikrosysteme

HW Security in the Industrial Internet/IoT Domain

Dr. Tobias Schubert

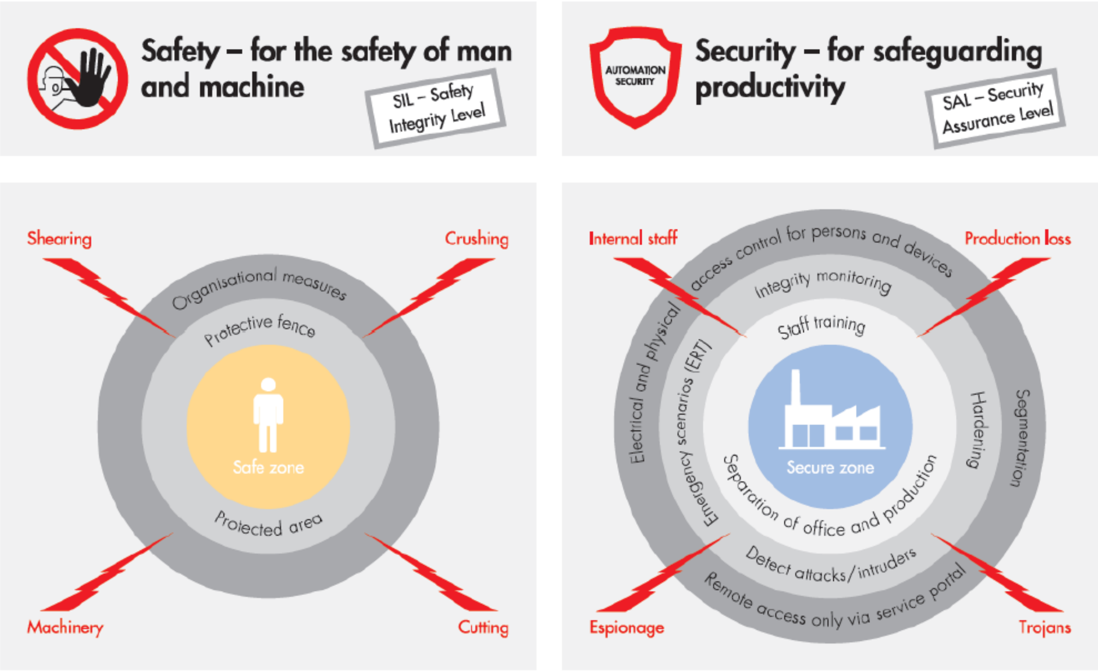
Professur für Rechnerarchitektur

Institut für Informatik, Technische Fakultät

UNI FREIBURG

DHBW
Duale Hochschule
Baden-Württemberg
Lörrach

Safety vs. Security



Prozess	**Safety**	**Security**
Systemgrenzen	Anlage, Maschine, …	Zone, Netz, …
Bedrohungen	Materialzuführung, Wartungstüre, …	ERP-Datenaustausch, Wartungszugang, IPC, …
Ergebnis Risikoanalyse	Quetschen, Scheren, Schneiden, …	Unberechtigter Zugriff, Auslesen von Daten, …
Maßnahmen	Not-Halt, Lichtgitter, Drehzahlüberwachung,…	Firewall, virtuelle Netze, VPN, Autentifikation, Verschlüsselung, SNMP, …
Kontrolle	Abnahmen, Audits, Tests, …	Verifikation, Monitoring, Logging, …

Quelle: Armin Glaser, Pilz GmbH & Co KG

Bekannte Sicherheitsvorfälle

Hacker steuern Jeep Cherokee fern

22.07.2015 06:20 Uhr – Ronald Eikenberg

heise Security

Durch eine Schwachstelle im Infotainmentsystem konnten Sicherheitsforscher die Kontrolle über einen Jeep übernehmen – über das Internet. Anfällig sind möglicherweise weitere Modelle des Fiat-Chrysler-Konzerns. Ein erstes Update schafft Abhilfe.

Quellen: http://www.heise.de/security/meldung/Hacker-steuern-Jeep-Cherokee-fern-2756331.html, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

- Uconnect-System in PKW in den USA per Mobilfunkbetreiber Sprint mit dem Internet verbunden
- Zwei Sicherheitsforschern gelang darüber der Zugriff auf die Diagnose-Schnittstelle (CAN-Bus)
- In einem Versuch (mit eingeweihtem Fahrer) wurde schrittweise die Kontrolle über das Fahrzeug übernommen und dieses in den Straßengraben gesteuert

Bekannte Vorfälle Maschinen betreffend

BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk

17.12.2014 15:58 Uhr – Fabian A. Scherschel

heise Security

- **Angreifer infiltrieren** durch Spear-Phishing **gezielt** das **Büronetz** des Werks
- Von dort erlangten sie **Zugriff zum Produktionsnetz** und konnten **Steuerungskomponenten manipulieren**
- Ein **Hochofen** konnte **nicht geregelt heruntergefahren** werden
- ➢ Massive **Beschädigungen der Anlage**

Bei einem bislang unbekannten Angriff beschädigten die Angreifer einen Hochofen schwer. Doch neben den gezielten Angriffen auf Industrieanlagen bilanziert das BSI auch eine steigende Gefahr für Endanwender.

Quelle: http://www.heise.de/security/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html

- Spear-Phishing: In der Regel per E-Mail initiierte Betrugsversuche
- Beispiel
  - Angreifer gibt sich als System-Administrator aus und fordert mit einer authentisch aussehenden Mail vertrauliche Informationen von Mitarbeitern an
  - Bspw. soll sich der Mitarbeiter auf einer präparierten Webseite mit Benutzernamen und Passwort anmelden oder auf einen Link klicken, über den dann Spyware heruntergeladen wird

Bekannte Vorfälle Maschinen betreffend

Schwachstellen in Fernsteuerungs-App für Industrieanlagen von Siemens geschlossen

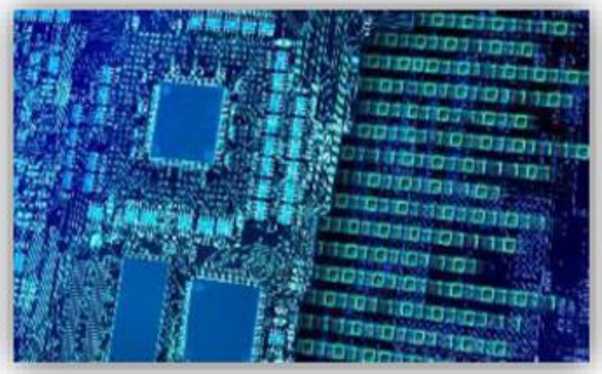
15.01.2015 06:30 Uhr – Ronald Eikenberg

Kraftwerke und Co. kann man inzwischen bequem per App fernsteuern. Ganz ungefährlich ist das offenbar jedoch nicht: Forscher fanden in den WinCC-Apps von Siemens haarsträubende Sicherheitslücken.

Quelle: http://www.heise.de/security/meldung/Schwachstellen-in-Fernsteuerungs-App-fuer-Industrieanlagen-von-Siemens-geschlossen-2517783.html

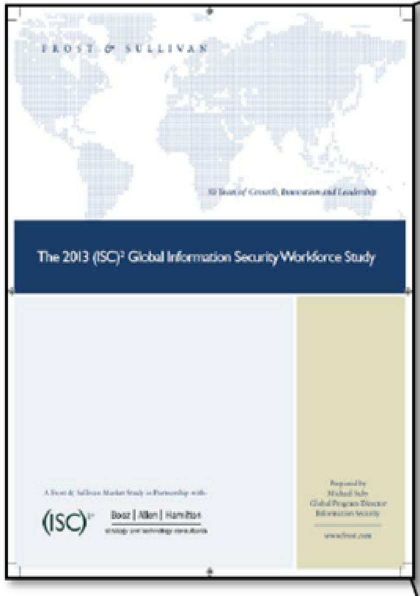
- SCADA = Supervisory Control and Data Acquisition → Überwachen und Steuern technischer Prozesse mittels eines „Rechners“
- Allein der Zugriff auf das Gerät genügt, um APP-Passwort & Zugangsdaten zum Sm@rtServer zu extrahieren
- Zudem wird das Passwort nicht erneut abgefragt, wenn die App bereits im Hintergrund war und wieder aktiviert wird
- WinCC kommt u.a. in deutschen Atomkraftwerken zum Einsatz

IT-Sicherheit: Potentielle Gefahrenherde

Unsicheres Design	Unsichere Netze	Unsichere Daten
		
Entwurfs- und Implementierungsfehler bei Geräten und Software, unzureichende Sicherheitsmechanismen	Internetkommunikation ist offen; jeder hat Zugang - Authentifizierungsmechanismen	Verschlüsselung zur Sicherung der Vertraulichkeit Absicherung

Quelle: Christoph Meinel, HPI Potsdam

Global Inform. Security Workforce Study 2013



- Web-basierte Umfrage unter 12.000 Information Security Professionals
  - davon 5% aus Maschinenbau
  - 13% aus IT
  - 21% aus Professional Services
- TOP 5 Sicherheitsbedenken
  1) Schwachstellen in Softwareanwendungen
  2) Malware
  3) Mobile Endgeräte
  4) Eigene Mitarbeiter
  5) Cloud-basierte Services
- Secure Software Development essentiell wichtig

VDMA-Studie zu Produktpiraterie

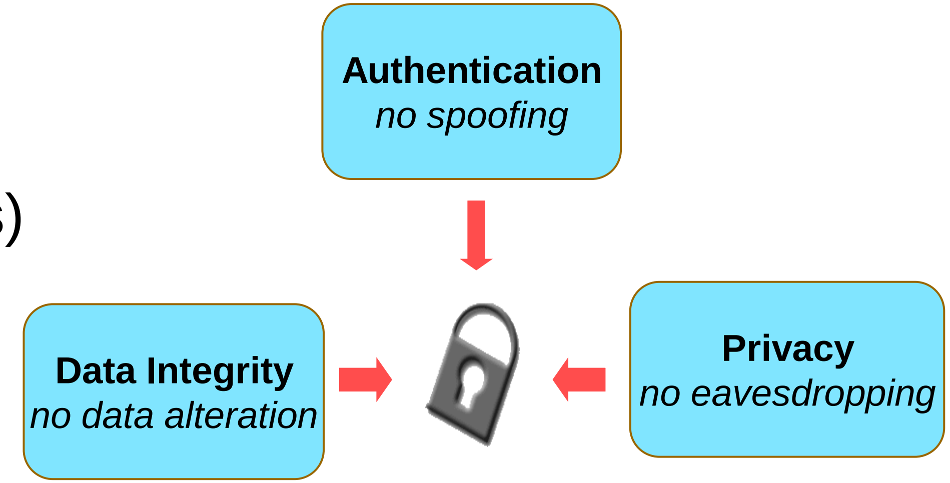
- **Produktpiraterie:** unzulässiger Nachbau (Plagiat) unter Verletzung von Sonderschutzrechten oder in wettbewerbswidriger Weise (i.d.R. Täuschung über den Hersteller der Originalware)

- 337 Mitgliedsunternehmen des VDMA befragt
  - **71%** sind von Produktpiraterie **betroffen**
  - Maschinen- und Anlagenbauer berichten vor allem von **Plagiaten ganzer Maschinen, Komponenten und Ersatzteilen**
  - **Geschätzter Schaden** für deutsche Maschinen- und Anlagenbauer: **7,9 Mrd. €** in **2013**
  - **19%** sind von **Industriespionage** betroffen
  - **38% nutzen technische Schutzmaßnahmen** (z. B. Produktkennzeichnung, konstruktive Maßnahmen, Know-How-Schutz, Embedded Security, Track & Tract)

Security (nicht nur bei Industrie 4.0)

…ist ein sehr breitgefächertes Gebiet mit vielfältigen Aspekten wie u.a.

- Cryptography
- Crypto processor design
- Physical unclonable functions
- Security for “simple” devices (e.g. RFID, smartcards)
- Counterfeit avoidance



Hier mit speziellem Fokus auf “HW-Security & Trust”!

die nachfolgenden Folien gehen z.T. zurück auf Mohammad Tehranipoor, University of Florida

Cryptography (in a Nutshell)

Definition

- The art of secret message writing
- Creating texts that can only be read by authorized individuals only
- “Adds an envelope (encoding) to an open postcard (plaintext)”

Principle

plaintext P → **ENCRYPTION / ENCODING / ENCIPHERING / E** → ciphertext C → **DECRYPTION / DECODING / DECIPHERING / D** → original plaintext P

Cryptography (in a Nutshell)

Cryptography is used since many, many years: Caesar‘s cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

↓ *rotate 13 positions*

NOPQRSTUVWXYZABCDEFGHIJKLM

HELLO WORLD		*Plaintext*
↓	*13*	*Key*
URYYB JBEYQ		*Ciphertext*

Cryptography (in a Nutshell)

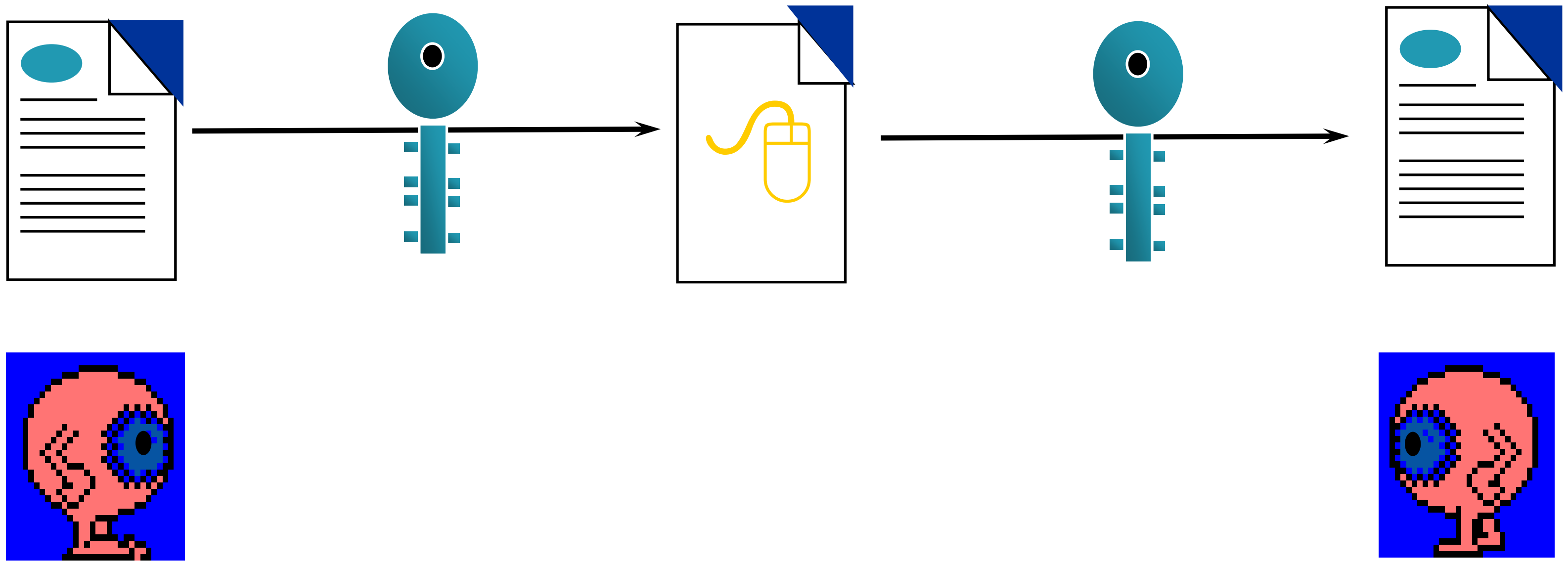
General Principles

- Longer keys make better ciphers
- Random keys make better ciphers
- Good ciphers produce “random” ciphertext
- Best keys are used once and thrown away

Cryptography (in a Nutshell)

Symmetric cryptography (private key)

- Examples: DES, AES, RC5, IDEA, Skipjack
- Advantages: fast
- Disadvantages: Must distribute key in advance, key must not be disclosed



Cryptography (in a Nutshell)

DES: Data Encryption Standard

- Widely published & used – US federal standard for many years (1977 – 2002)
- Complex series of bit substitutions, permutations and recombinations (“rounds”)
- Basic DES: 56-bit keys
  - Crackable in about a day using specialized hardware by a brute-force attack
- Triple DES: effective 112-bit key
  - Perform three stages of DES with different keys
  - Stronger, but heavily depends on the choice of the keys

Cryptography (in a Nutshell)

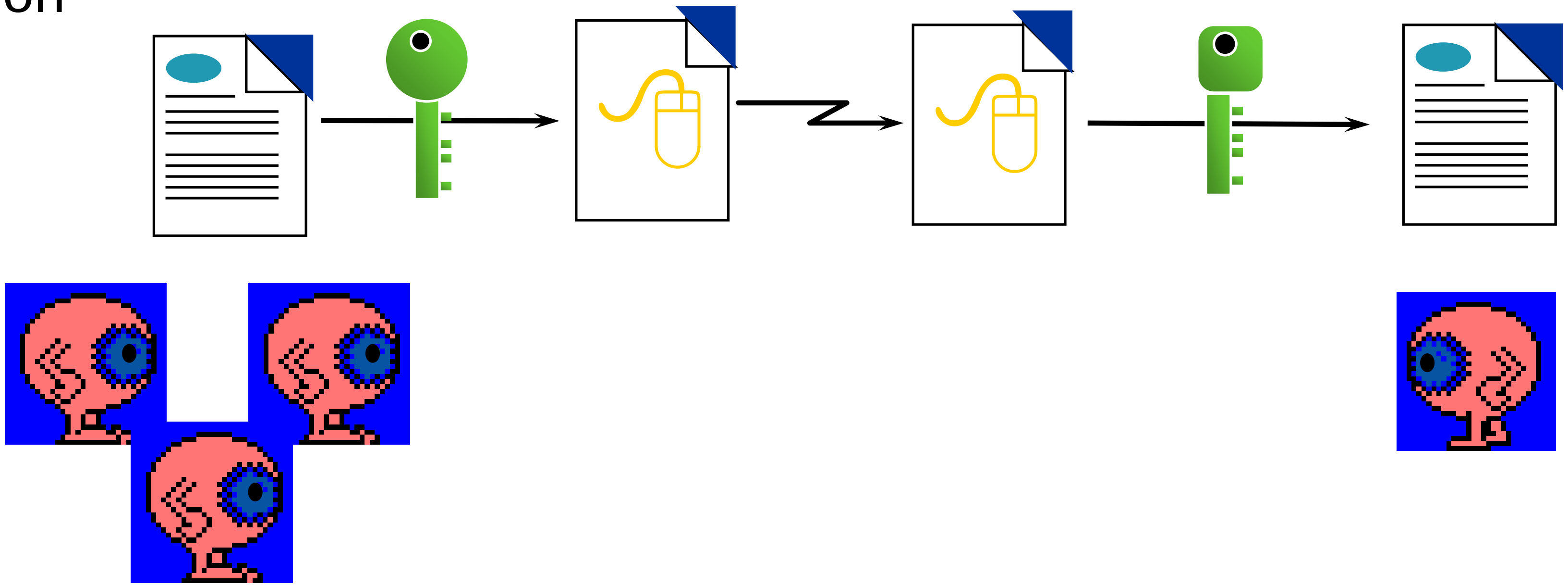
AES: Advanced Encryption Standard

- Standard replacement for DES for US government since 2002
- Winner of the AES (Advanced Encryption Standard) competition run by NIST (National Institute of Standards and Technology in US) in 1997 – 2000
- Comes from Europe (Belgium) by Vincent Rijmen and Joan Daemen → Unlike DES "X-files" stories less likely!
- Symmetric block-cipher (128, 192 or 256 bits) with variable keys (128, 192 or 256 bits, too)
- Fast and a lot of good properties, such as good immunity from timing and power (electric) analysis
- Construction deceptively similar to DES (XORs etc.) but really different

Cryptography (in a Nutshell)

Asymmetric cryptography (public key)

- Examples: RSA (by Rivest, Shamir, Adleman), Diffie-Hellman, ElGamal
- Advantages: public key widely distributable, does digital signatures
- Disadvantages: orders of magnitude slower than (3)DES & AES → hybrid approaches, combining AES for data encryption and RSA for symmetric key encryption



Cryptography (in a Nutshell)

RSA

- Algorithm patented by RSA Data Security
- Uses special properties of modular arithmetic
  - $C = P^e \pmod{n}$ → cipher text
  - $P = C^d \pmod{n}$ → plain text
  - e, d, and n all hundreds of digits long and derived from a pair of large prime numbers
    - (e, n) → public key
    - (d, n) → private key
- Keys lengths from 512 to 4096 bits

Crypto Processor Design

What is a crypto processor?

- A specialized processor that executes cryptographic algorithms within hardware
- Definition varies, but the standard definition includes
  - Acceleration of encryption
  - Protection against tampering
  - Intrusion detection
  - Protection of data
  - Secure I/O

Crypto Processor Design

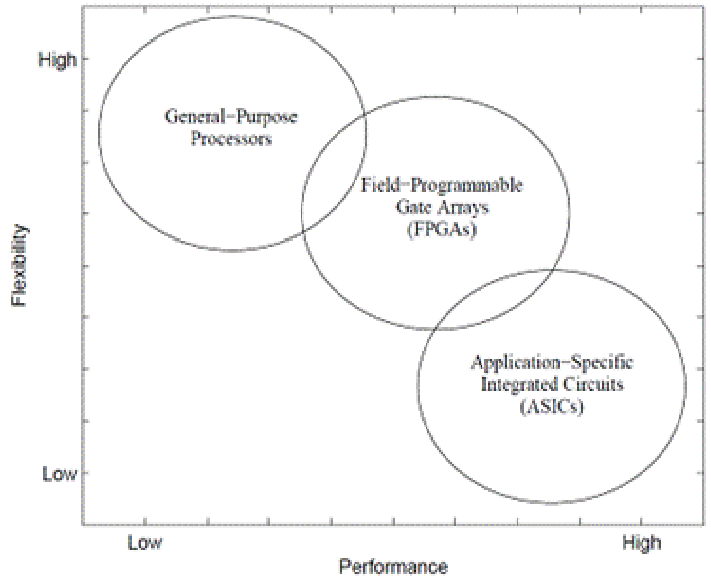
Why crypto processors?

- Most modern security work is based on either protecting or cracking vulnerabilities in target‘s operating system
  - Majority of systems use conventional processors, standard operating systems, and standard communication channels
  - A lot of good work has been done here but may be seen as a dead-end for high security
  - Software isn’t enough to protect system, need physical protection
- Protection of intellectual property (algorithms, FPGA bitstreams, …)
- Offer advantages in speed and power consumption (crypto algorithms implemented in hardware)

Crypto Processor Design

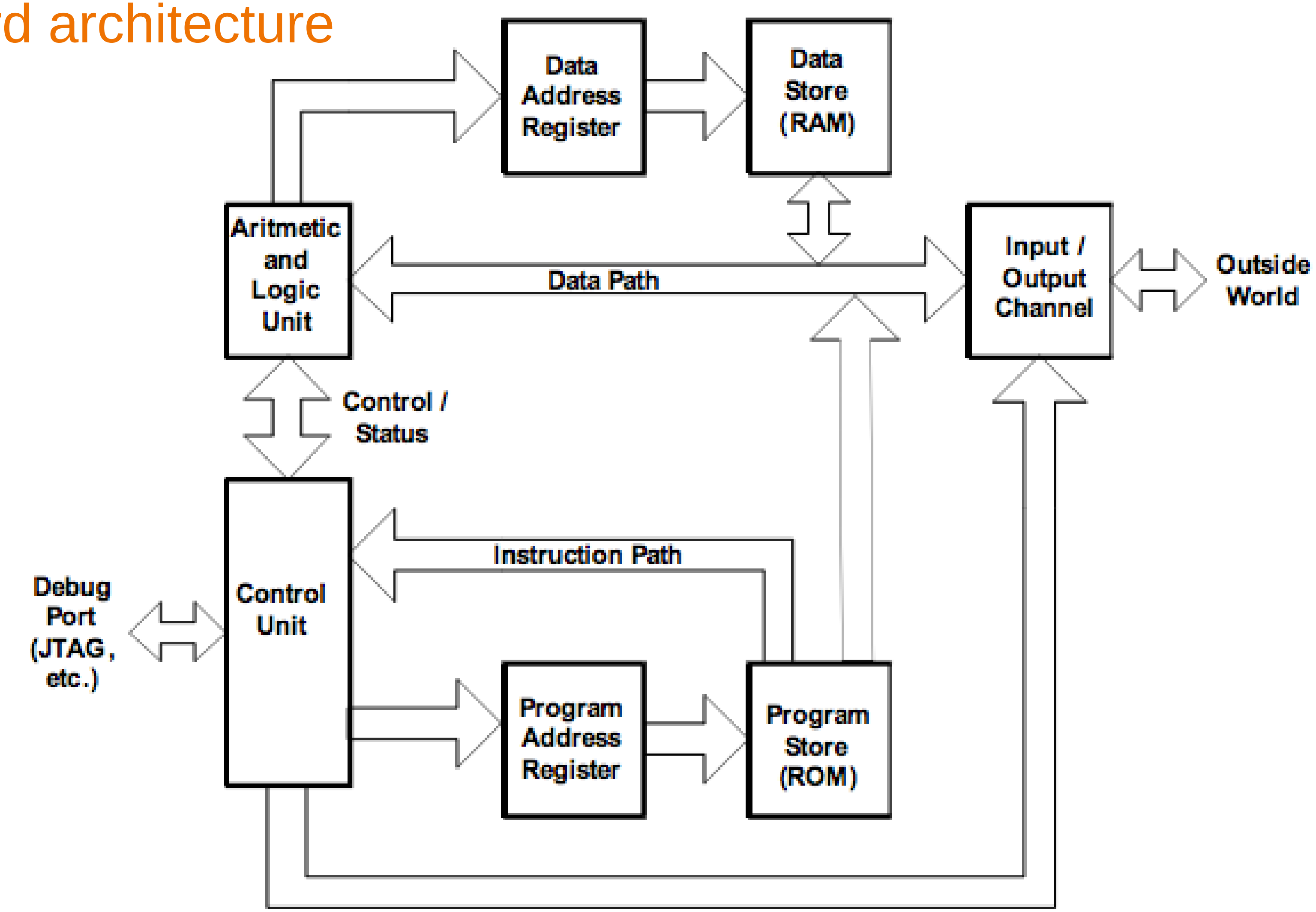
Families of crypto processors

- Double encryption
  - Protects programs and data
- Standard processor architecture + dedicated crypto blocks
  - Increased throughput
- Implementations
  - General-purpose processors
    - Crypto algorithms implemented in software
    - High flexibility but slow
  - FPGA implementation
    - Flexible and allow efficient complex arithmetic operations
  - ASIC implementation
    - Fast and low power consumption



Crypto Processor Design

Conventional Harvard architecture



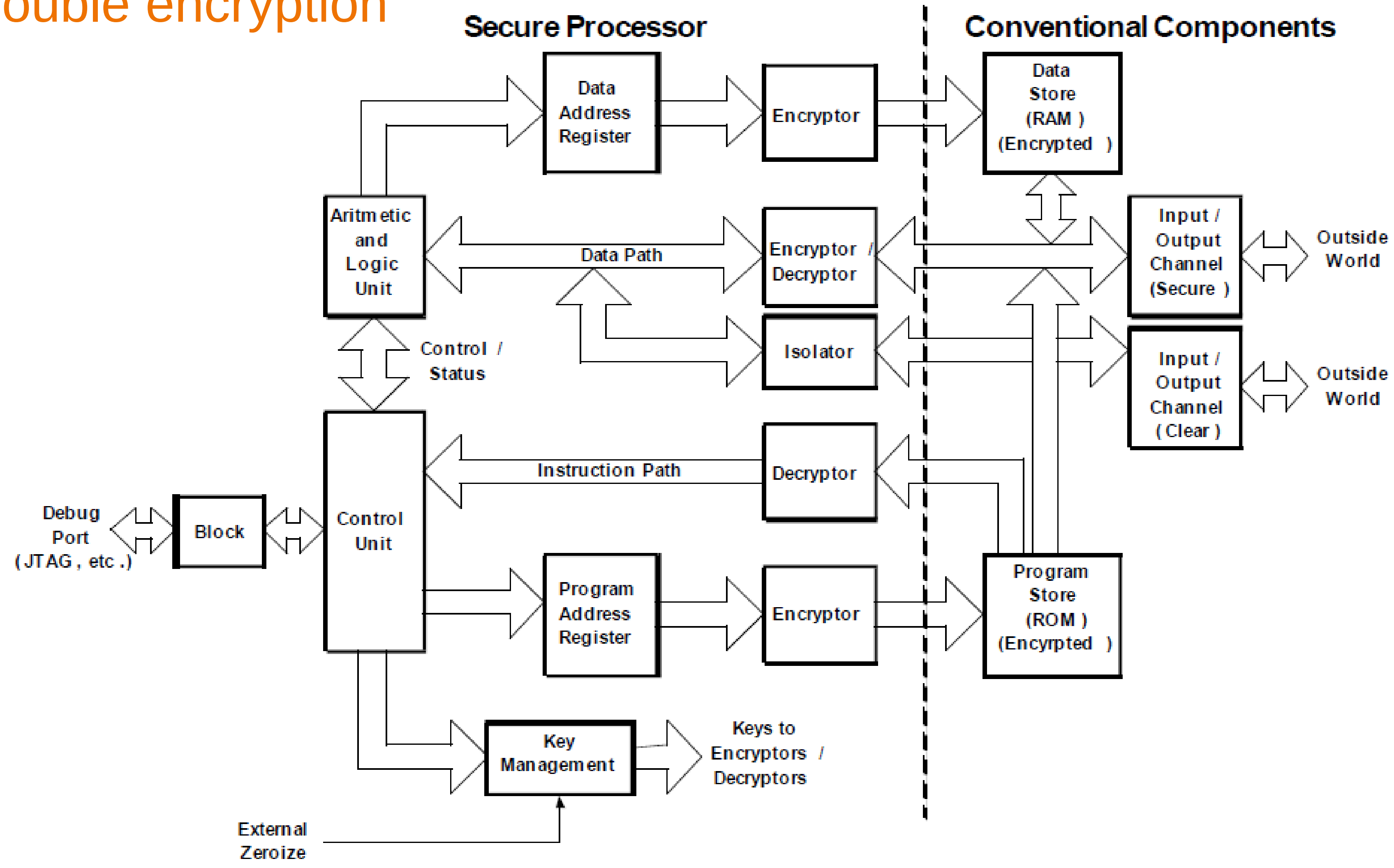
Crypto Processor Design

Double encryption

- This type of crypto processor protects the programs running and the data
  - Data and addresses are encrypted
- All info is decrypted within the security of the processor and then encrypted again before memory storage or I/O transmission
  - A barrier of encryptors and decryptors stands between the processing elements, data storage, and I/O elements

Crypto Processor Design

Processor with double encryption



Crypto Processor Design

Double encryption

- New section for key management
  - Keys are “hardwired” in the sense that are not generated internally but just stored (externally loadable)
  - Hardwiring in the keys generally allows them to be zeroized
  - Hardwired keys are generally not visible to the outside world under any (reasonable) conditions
- There is both a secure and a non-secure I/O channel
  - The strength of the security in the processor is directly dependent on how well these two channels are isolated
  - The easiest place to attack would be at this point of isolation
    - Results in data transactions being monitored “in the clear”

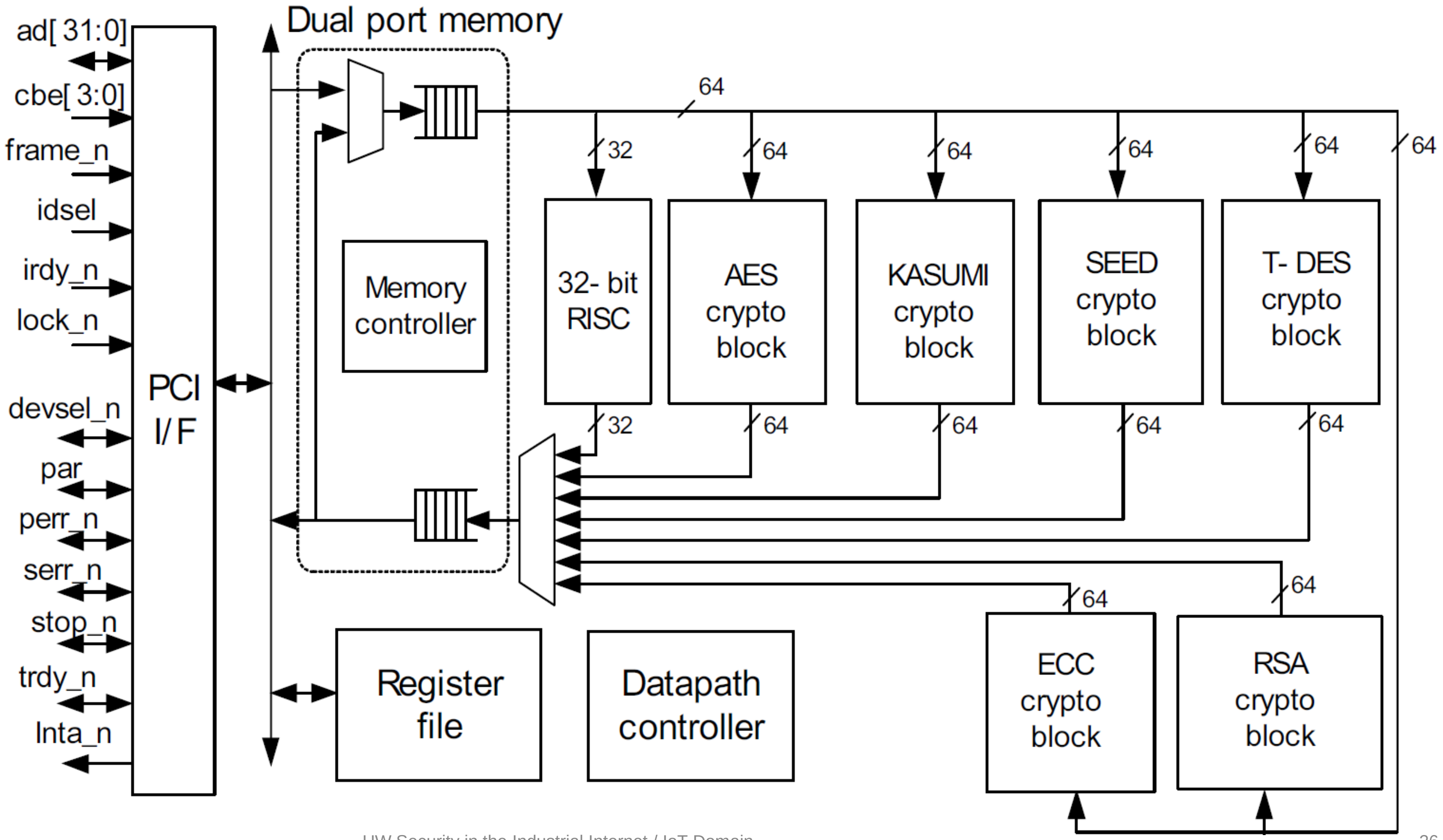
Crypto Processor Design

Processor with dedicated crypto blocks

- Build upon standard processor architectures with the addition of multiple dedicated crypto algorithm blocks
  - Parallel connections to data bus
- Processor instructions are not secure
  - Handle large quantities of encrypted data, but do not need the instructions to be secure
- Ideal for network routers
  - Greatly increase throughput in network applications
  - Multiple cryptographic algorithms

Crypto Processor Design

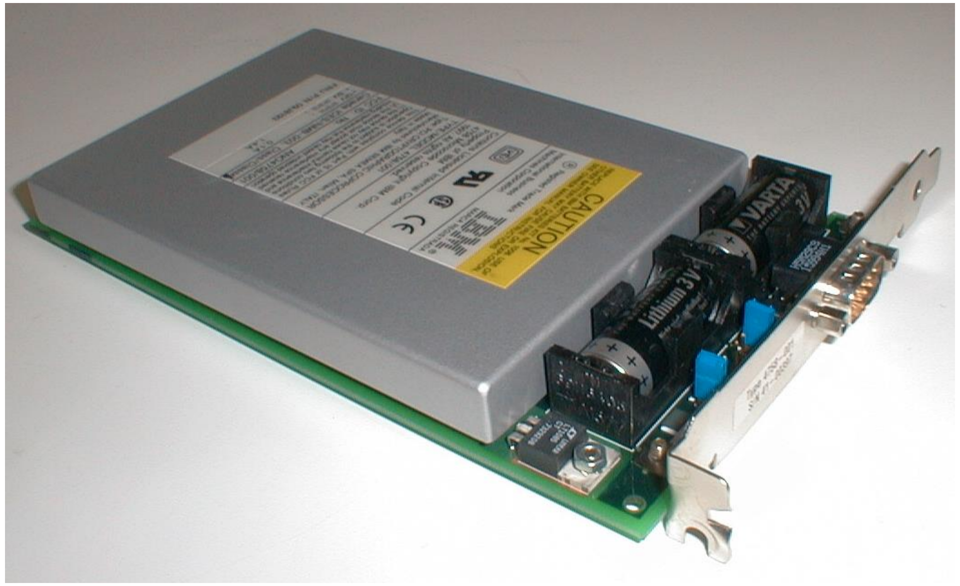
Processor with dedicated crypto blocks



Crypto Processor Design

Example: IBM PCIeCC Cryptographic Coprocessor

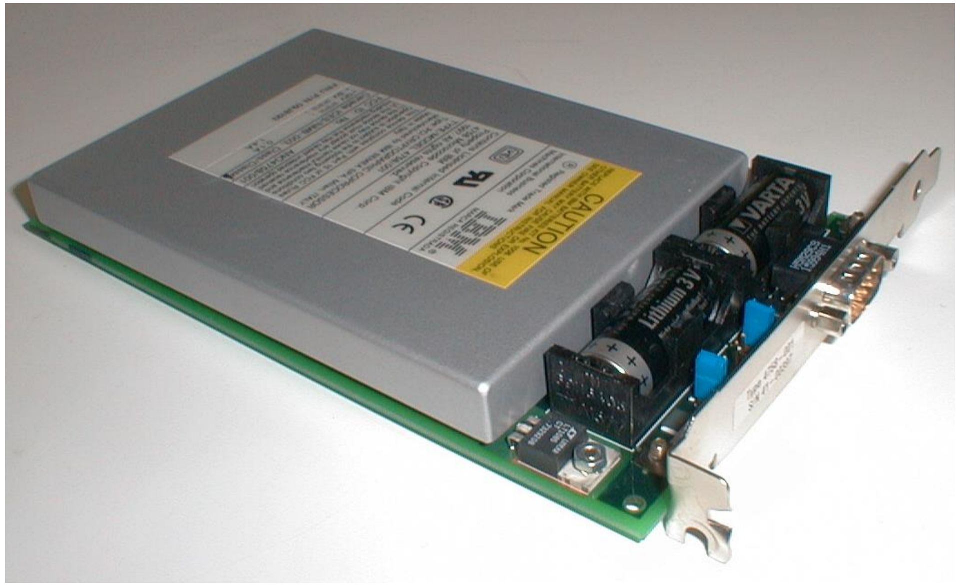
- Rated at highest level of tamper-resistance
- FIPS level 4 (“Federal Information Processing Standard”, highest available level)
- Specialized hardware for various crypto algorithms (AES, DES, RSA, …)
- True random number generator
- Internal batteries for backup power
- Applications
  - Financial transactions
  - Public key infrastructures, …



Crypto Processor Design

Example: IBM PCIeCC Cryptographic Coprocessor

- Rated at highest level of tamper-resistance
- FIPS level 4 (“Federal Information Processing Standard”, highest available level)
- Specialized hardware for various crypto algorithms (AES, DES, RSA, …)
- True random number generator
- Internal batteries for backup power
- Applications
  - Financial transactions
  - Public key infrastructures, …



But: The predecessor – IBM 4758 – was hacked by simply dropping a logic analyzer onto the microprocessor bus and using the recorded information to break all keys within one day of „cracking time“.

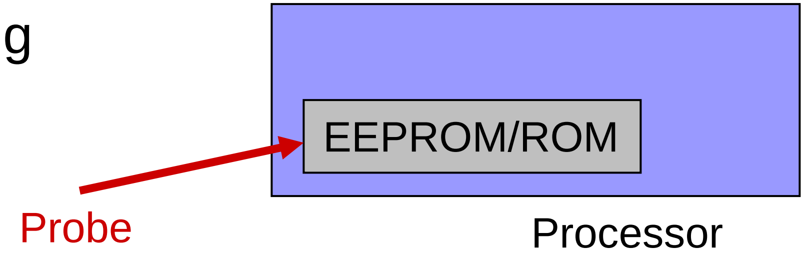
Physical Unclonable Functions

Attacker goals

- To get the crypto keys stored in RAM or ROM
- To learn the secret crypto algorithm used
- To obtain other information stored in the chip (e.g. PINs)
- To modify information on the card (e.g. calling card balance)

Problem

- Storing digital information in a device in a way that is resistant to physical attacks is difficult an expensive
- E.g. attackers can physically extract secret keys from EEPROM while processor is off
- Trusted party must embed and test secret keys in a secure location
- EEPROMs add additional complexity to manufactoring



Physical Unclonable Functions

Potential alternative

- Usage of one-way hash functions
- Maps a variable length input to a fixed length output (challenge/response pair)
- Easy to evaluate in one direction but hard to reverse in the other
- Changing one bit in the input alters nearly half of the output bits (Avalanche Property, „Lawineneffekt“)
- Use chaotic physical structures of the device that are hard to model instead of mathematical one-way functions!

→ Physical one-way hash functions

  - Inexpensive to fabricate
  - Prohibitively difficult to duplicate
  - No compact mathematical representation
  - Intrinsically tamper-resistant (e.g. if dependent on overlaid metal layers and package)

UNI FREIBURG

Physical Unclonable Functions

In IC manufacturing process variation (length, widths, oxid thickness) is an issue

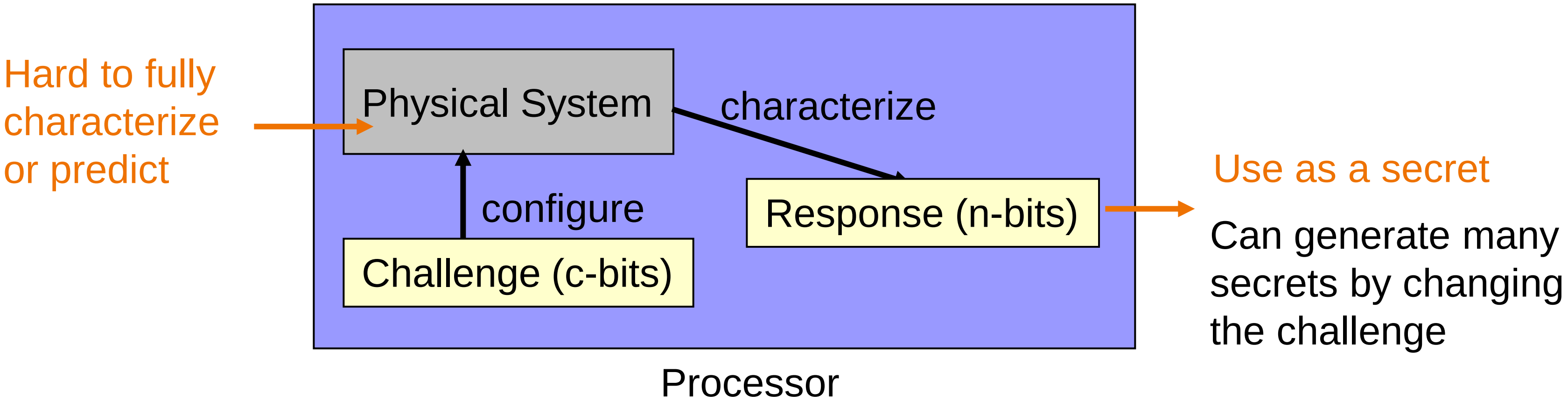
- Impact circuit performance
- Functional failure (e.g. timing delay faults)
- Nowadays, a major obstacle to the continued downscaling of IC technology!

But what about turning the „bug“ of process variation into a „feature“?

- Each IC has unique properties!
- Use these unique properties of a particular IC to realize an individual one-way hash function!

Physical Unclonable Functions

Idea: Generate keys from a complex physical system



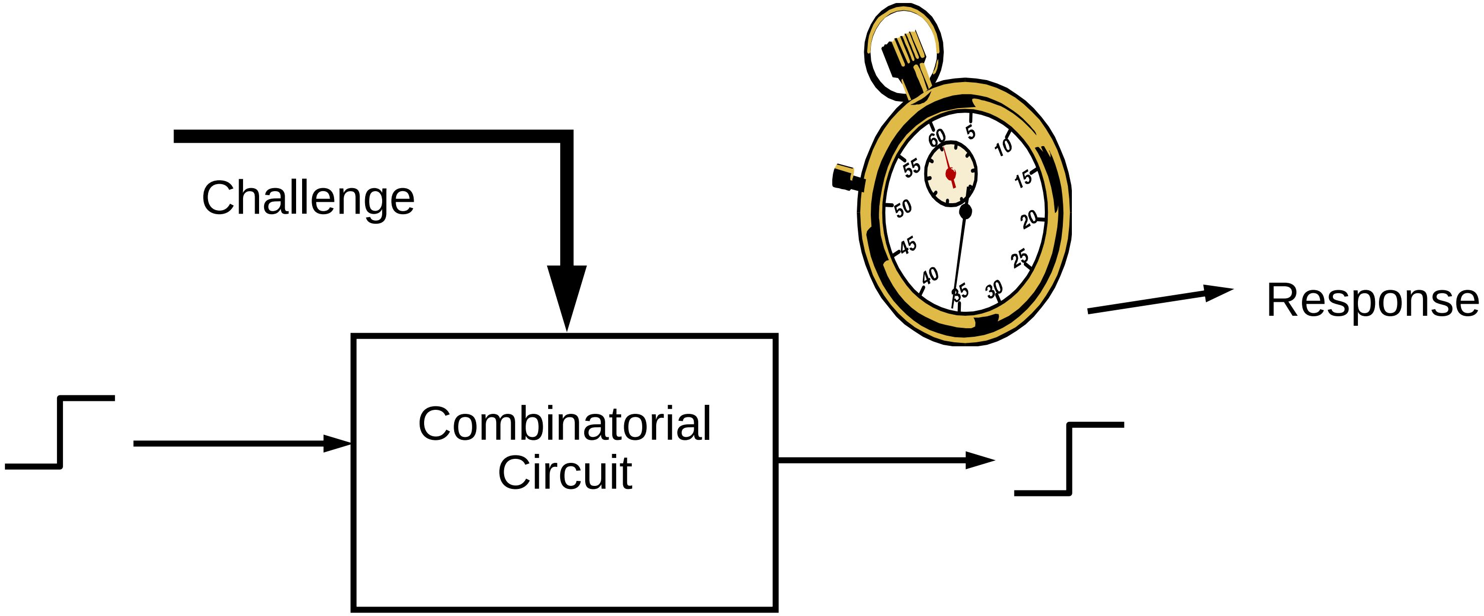
Security advantage

- Keys are generated on demand → no non-volatile secrets
- No need to program the secret
- Can generate multiple (master) keys

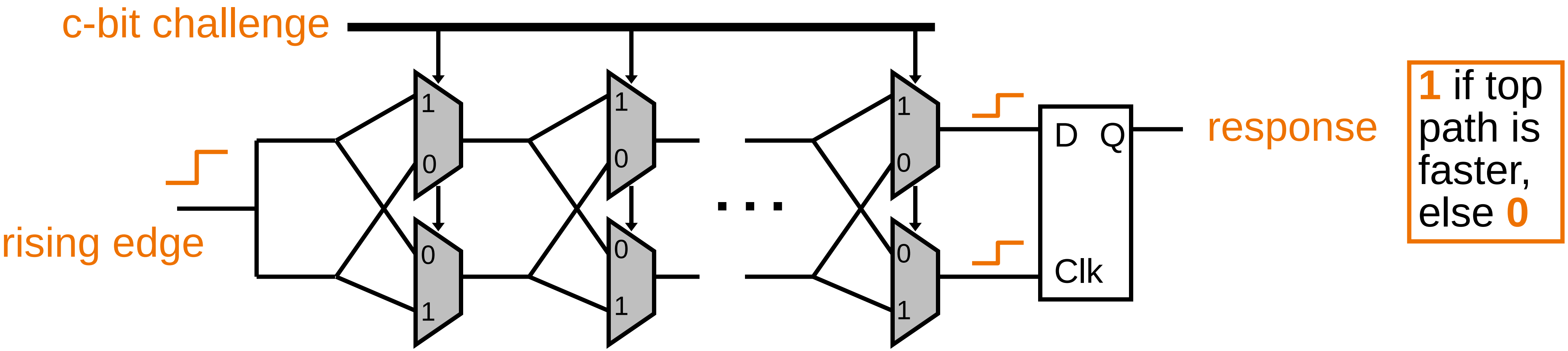
Physical Unclonable Functions

Proof of concept

- Experiments in which identical circuits with identical layouts were placed on different FPGAs show that path delays vary across ICs → no two integrated circuits are identical, use path delays for identification!

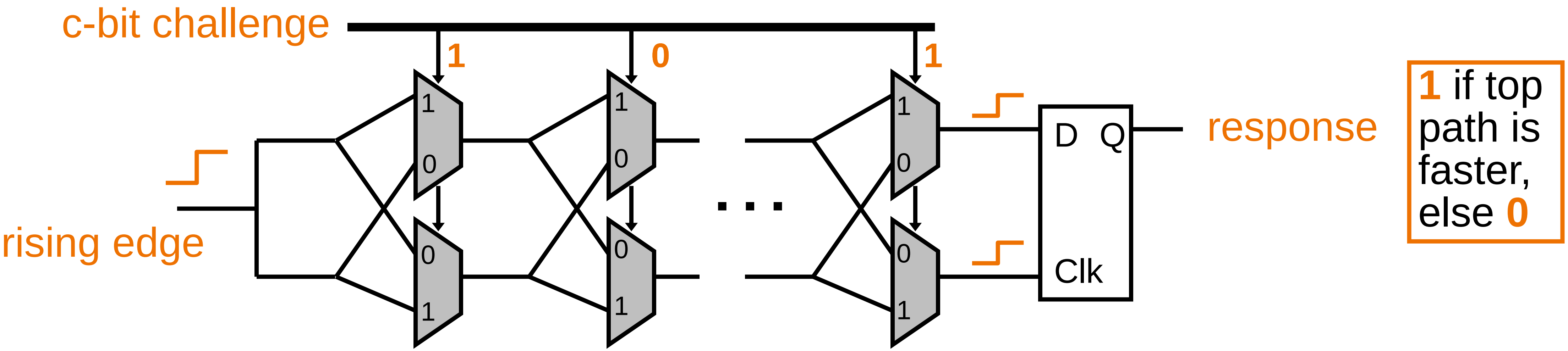


Physical Unclonable Functions: Arbiter PUF



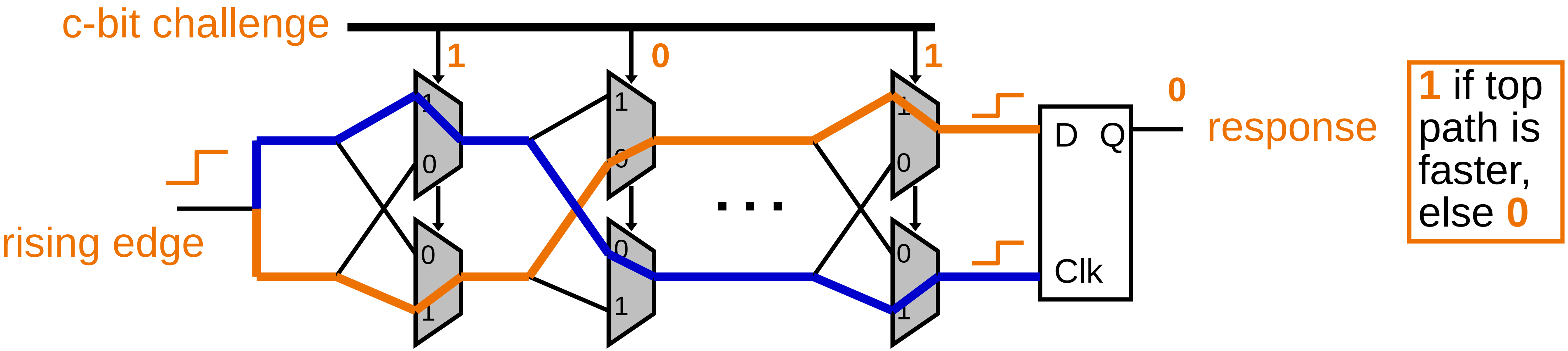
- Compare two paths with an identical delay in design
  - Random process variation determines which path is faster
  - An arbiter outputs 1-bit digital response
- Path delays in an IC are statistically distributed due to random manufacturing variations

Physical Unclonable Functions: Arbiter PUF



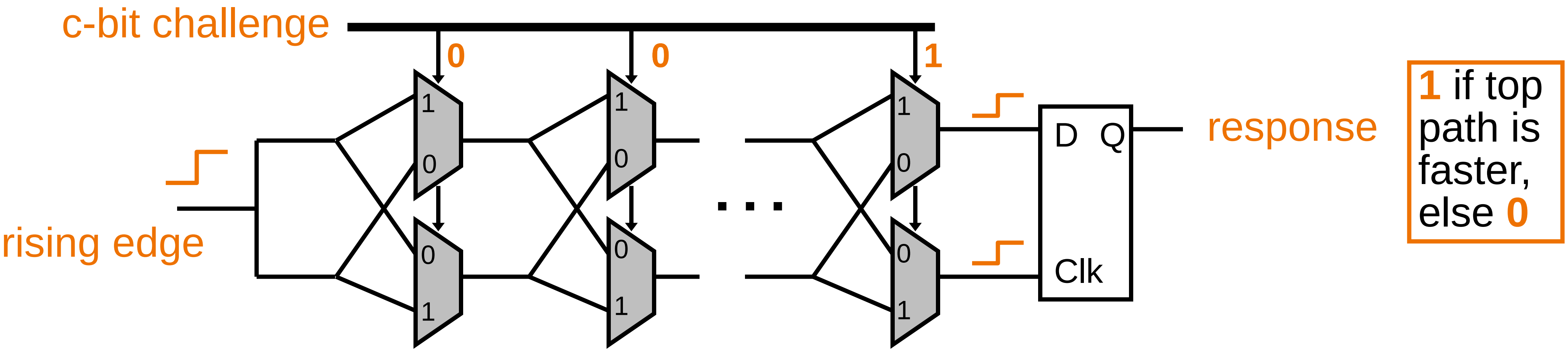
- Compare two paths with an identical delay in design
  - Random process variation determines which path is faster
  - An arbiter outputs 1-bit digital response
- Path delays in an IC are statistically distributed due to random manufacturing variations

Physical Unclonable Functions: Arbiter PUF



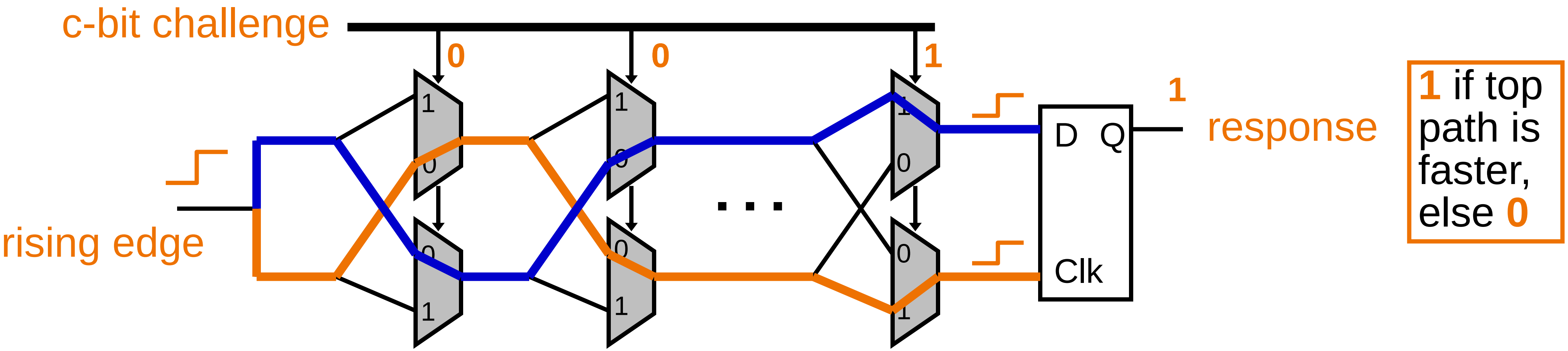
- Compare two paths with an identical delay in design
  - Random process variation determines which path is faster
  - An arbiter outputs 1-bit digital response
- Path delays in an IC are statistically distributed due to random manufacturing variations

Physical Unclonable Functions: Arbiter PUF



- Compare two paths with an identical delay in design
  - Random process variation determines which path is faster
  - An arbiter outputs 1-bit digital response
- Path delays in an IC are statistically distributed due to random manufacturing variations

Physical Unclonable Functions: Arbiter PUF



- Compare two paths with an identical delay in design
  - Random process variation determines which path is faster
  - An arbiter outputs 1-bit digital response
- Path delays in an IC are statistically distributed due to random manufacturing variations

Physical Unclonable Functions

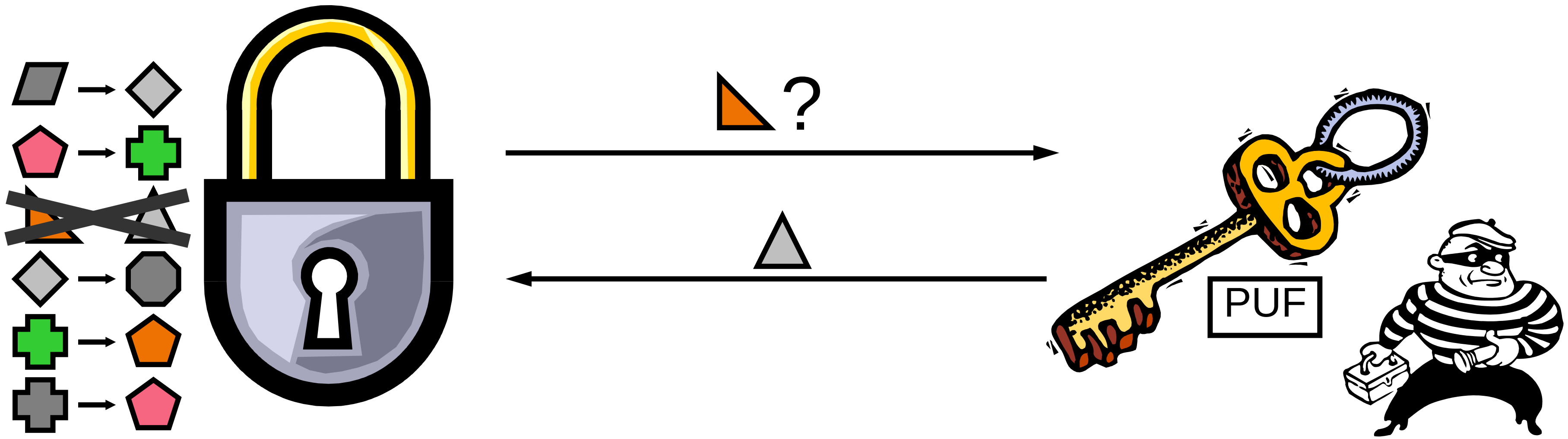
Experiments carried out

- Fabricated arbiter PUF on multiple ICs @ TSMC (Taiwan Semiconductor Manufacturing Company)
- Applied 100 random challenges and observed responses
  - Distance between chip X and chip Y on average 24 bits (out of 100 bits)
  - Measurement noise at 70° Celsius about 2 bits
  - Indeed it is possible to identify individual ICs
  - Almost impossible to model the process variations and to „clone“ a PUF

Physical Unclonable Functions

Using PUFs as unclonable keys

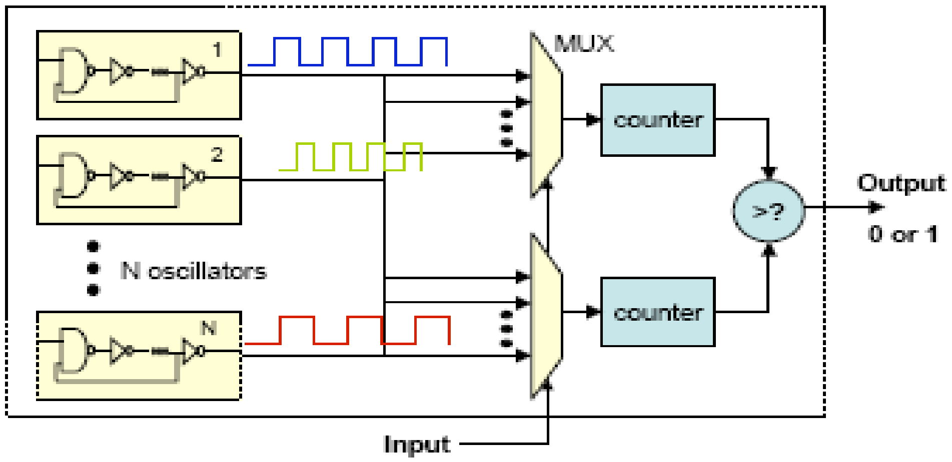
- Lock has a database of challenge/response pairs
- To open the lock, the key has to show that it knows the right response to one or more challenges



Physical Unclonable Functions

Final remarks

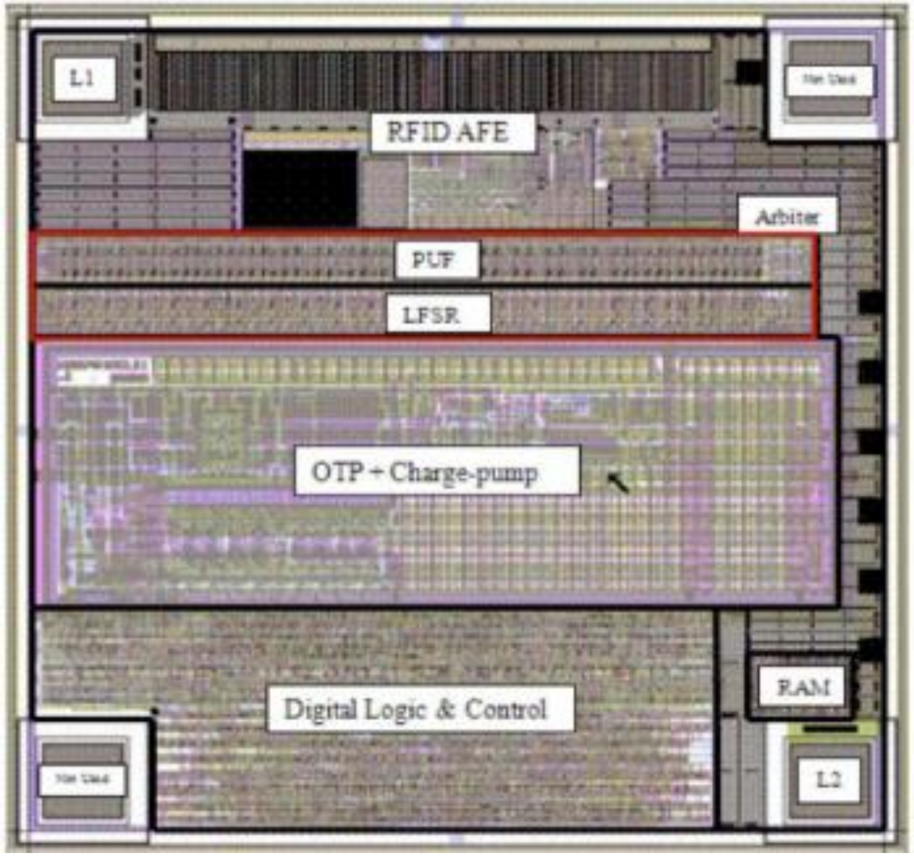
- If PUF delays depend on overlaid metal layers and package an invasive attack changes PUF delays and by this destroys the PUF
- Man-in-the-middle attacks still possible
  - Do not use the same challenge/response pair over and over again
  - Encrypt both, challenge and response
- Unstability is an issue, PUF output depends on temperature, aging, voltage variation → need for „error correction“ methods when used as cryptographic keys!
- Other PUF implementations: Ring-Oscillator PUF



Physical Unclonable Functions

Applications

- Digital signatures
- Message authentication
- Software licensing
- RFID, smartcard, e-passport authentication
- Counterfeit avoidance
- …



Floorplan of an PUF enabled RFID Tag

Counterfeit Detection & Avoidance

A counterfeit component

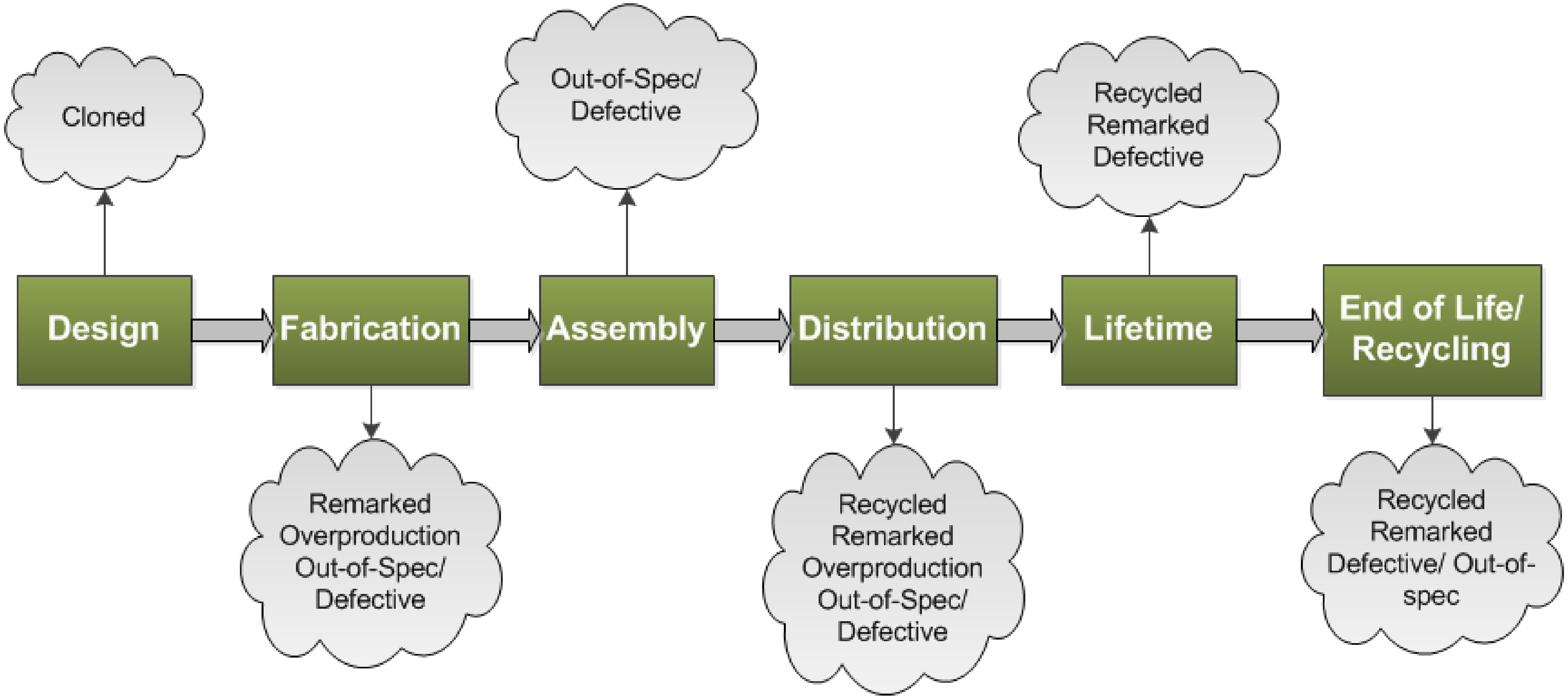
- Is an unauthorized copy
- Does not conform to design, model, or performance standards of the original manufacturer
- Is not produced by the original manufacturer
- Is out-of-specification, defective, or a used original product sold as new
- Has incorrect or false markings/documentation
- Is distributed in violation of intellectual property rights, copyrights, or trademark laws

Why counterfeiting?

- Lucrative business
  - Easy money
  - Easy to make counterfeit components
  - Enough raw material, e.g. ever increasing electronic waste
- Example: Copy one‘s design and fabricate components without paying for any R&D costs

Counterfeit Detection & Avoidance

Supply chain vulnerabilities



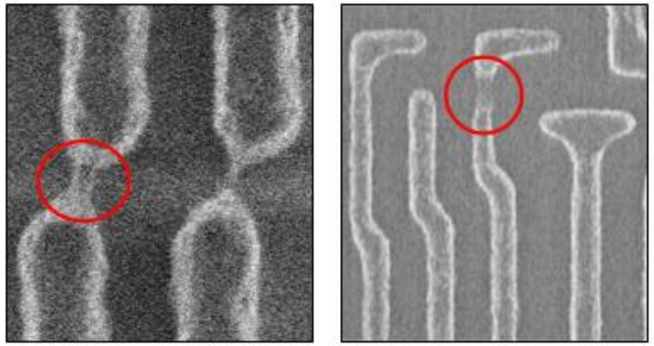
Counterfeit Detection & Avoidance

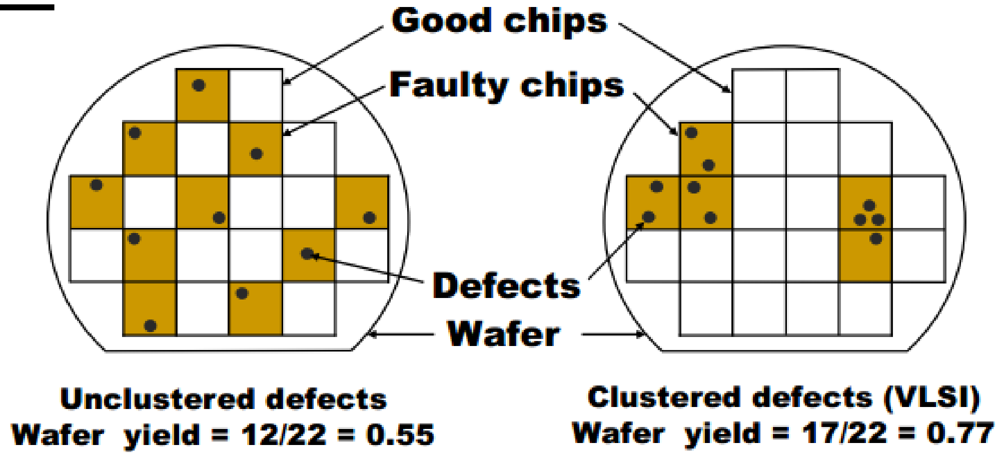
Background: Test and yield

- Errors in fabrication process cause defects on chip which causes chip to malfunction
- Chips are tested in order to detect defects
- Failing chips are discarded
- Fraction of remaining good chips is called the yield

$$\frac{\text{total chips} - \text{discarded chips}}{\text{total chips}}$$

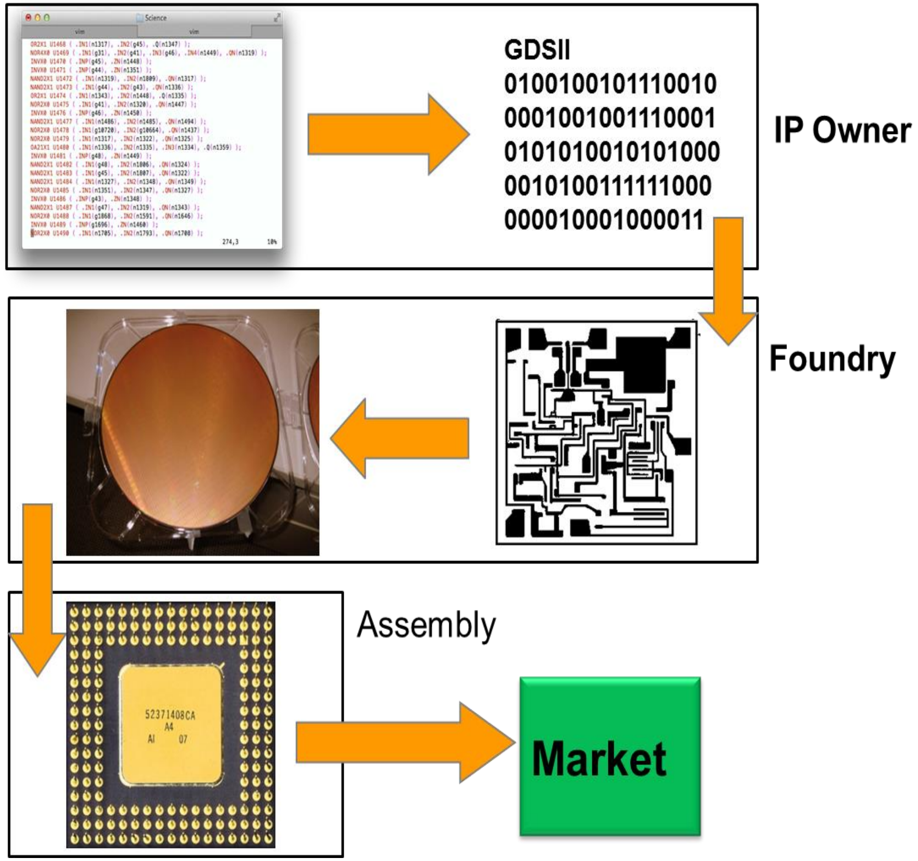
- Foundry predicts yield





Counterfeit Detection & Avoidance

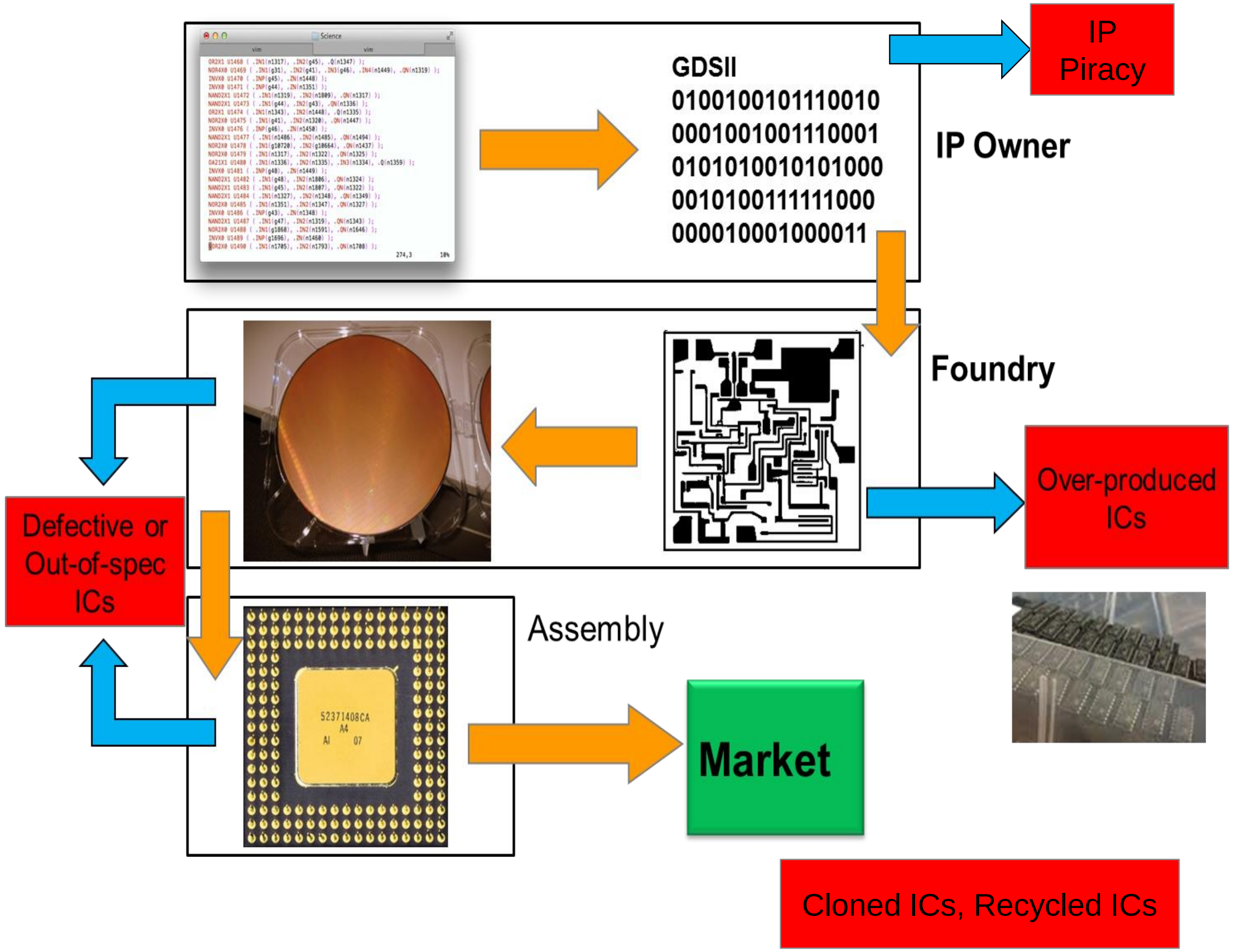
Chip production flow



- Little communication between IP Owner and Foundry
- Foundry is trusted with full design
- Responsible for production of requested amount of chips
- IP holder provides foundry/assembly with all test patterns and responses

Counterfeit Detection & Avoidance

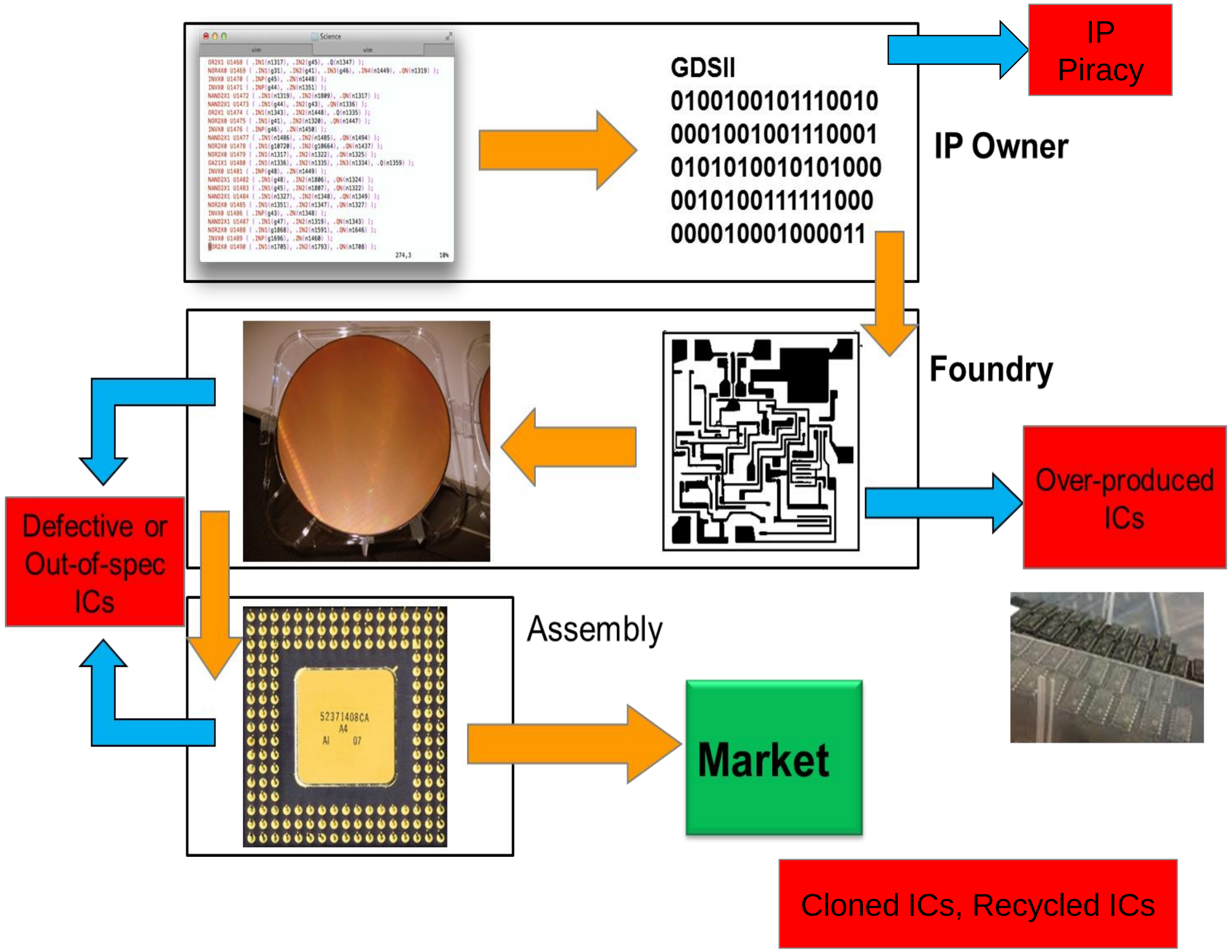
Chip production flow



- Foundry looks for its own profit
- Once mask is produced, producing ICs is simple and cheap
- Lack of communication makes it difficult for owner to track produced chips

Counterfeit Detection & Avoidance

Chip production flow



- Foundry looks for its own profit
- Once mask is produced, producing ICs is simple and cheap
- Lack of communication makes it difficult for owner to track produced chips

Discussed next: PUF-based methods to detect and (to some extent) to avoid defective, out-of-spec, recycled, and over-produced ICs!

Counterfeit Detection & Avoidance

Some remarks on…

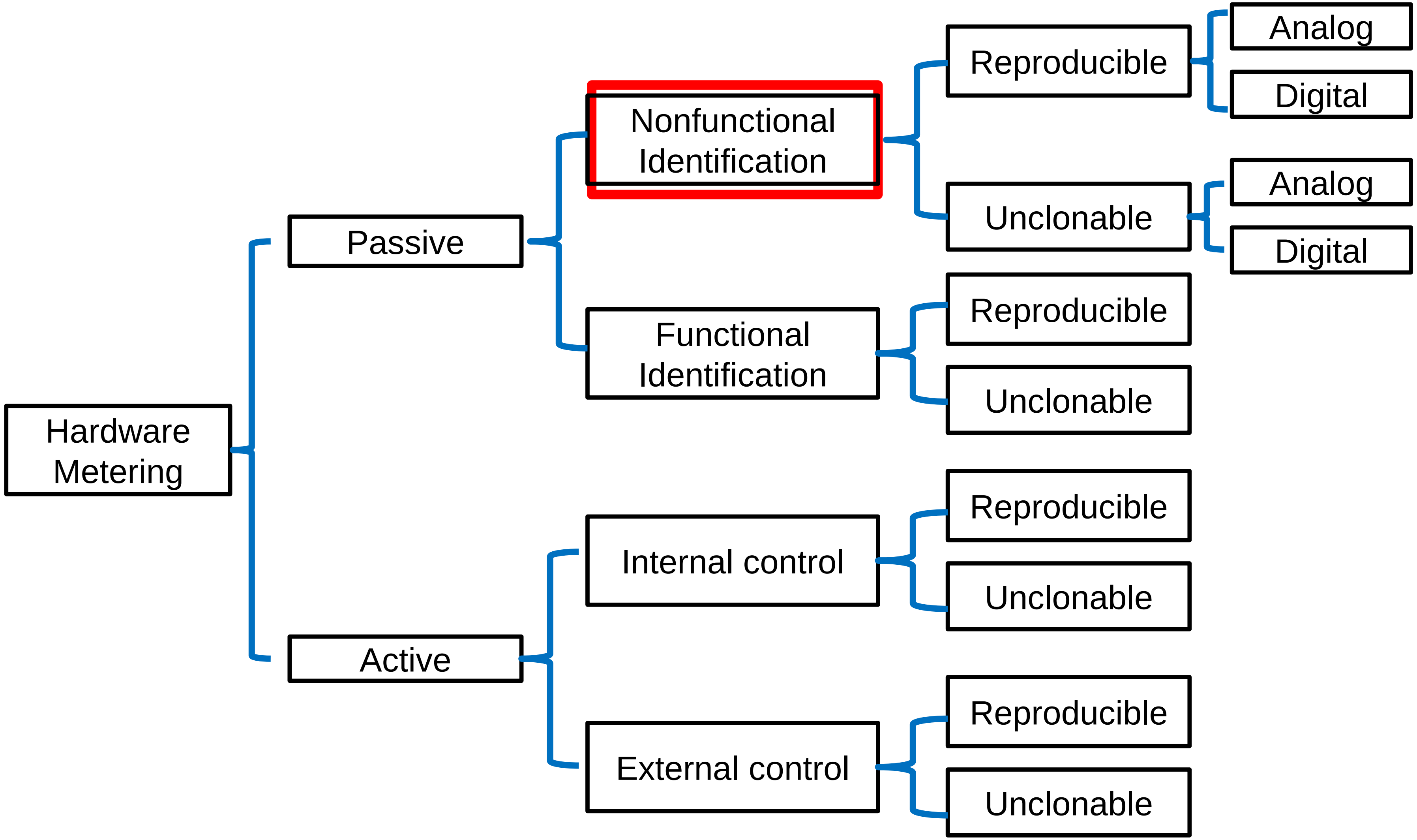
- Defective parts
  - A chip may fail at one particular test pattern
  - It is highly unlikely that defect will appear in normal operation of the chip in the first few hours, days, or months
  - Eventually, it will fail at some point of time
- Out-of-spec parts
  - Fail to perform at the design specification (leakage current, dynamic current, performance, etc.)
  - The chip might fail at extreme physical/environmental conditions

Counterfeit Detection & Avoidance

Hardware metering

- Set of security protocols that enable IP owners to achieve post-fabrication control over their ICs
- Methods attempt to uniquely tag each chip to facilitate tracing them
- Main methods can be classified by being
  - Active vs. passive
  - Nonfunctional vs. functional
  - Internal control vs. external control
  - Reproducible vs. unclonable

Counterfeit Detection & Avoidance

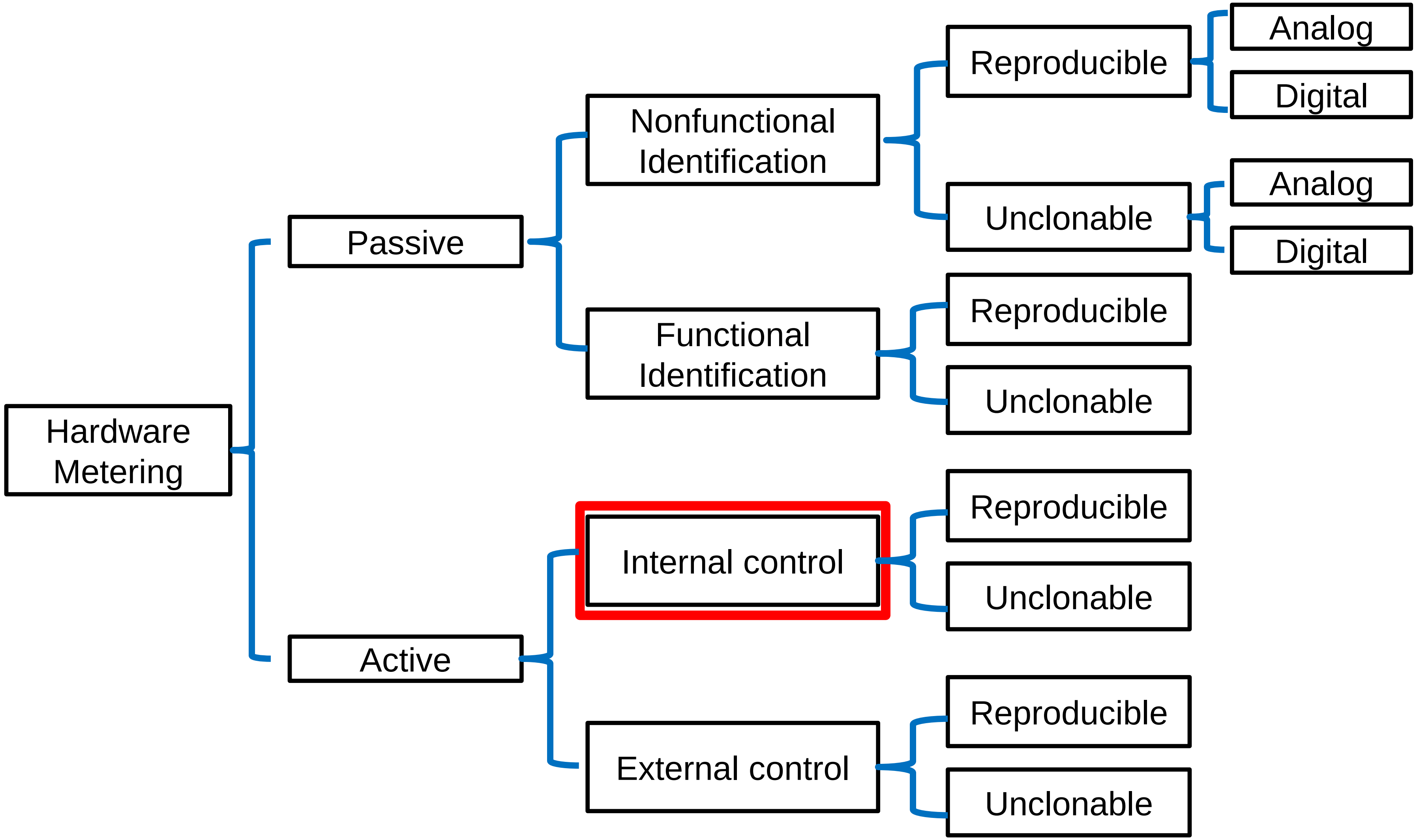


Counterfeit Detection & Avoidance

Nonfunctional identification

- Unique ID is separate from the chip‘s functionality
- Reproducible nonfunctional identification
  - Unique IDs like serial numbers are stored on the chip package, on the die, or in on-chip memory
  - Easy to track, but also easy to clone & to overproduce
- Unclonable nonfunctional identification
  - Use random process variations to generate unique fingerprints → PUFs
  - Values cannot be reproduced due to randomness in process variation, but foundry could overproduce ICs without knowledge of IP owner
- In any case, these methods do not avoid counterfeiting „by construction“, since out of million chips the probability of finding an non-authorized chip is quite small!

Counterfeit Detection & Avoidance



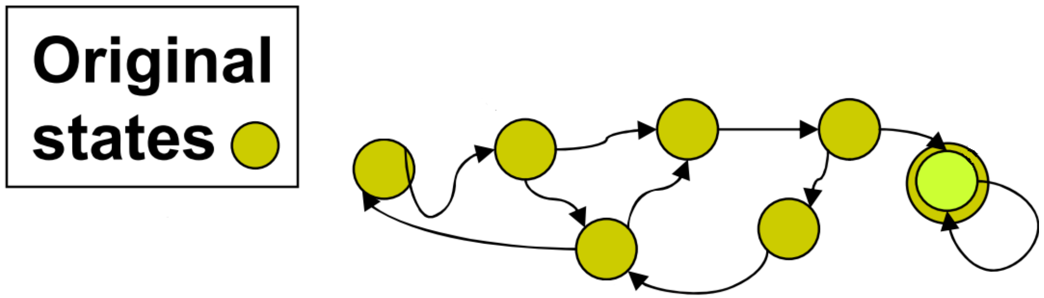
Counterfeit Detection & Avoidance

Internal active metering

- Hides states and transitions in the design that can be accessed by the designer only → knowledge about these states/transitions required to activate the chip
- Locks are embedded via Finite State Machines (FSMs) in the hardware design
- Adding additional states gives the designer the ability to decide which datapath (sequence of states) to use post-silicon
  - Since states are added, specific combinations are needed to bring the FSM to the correct output (back to the original functional states)
  - Only IP owners knows such combinations
  - Without these combinations produced chips are non-functional!

Counterfeit Detection & Avoidance

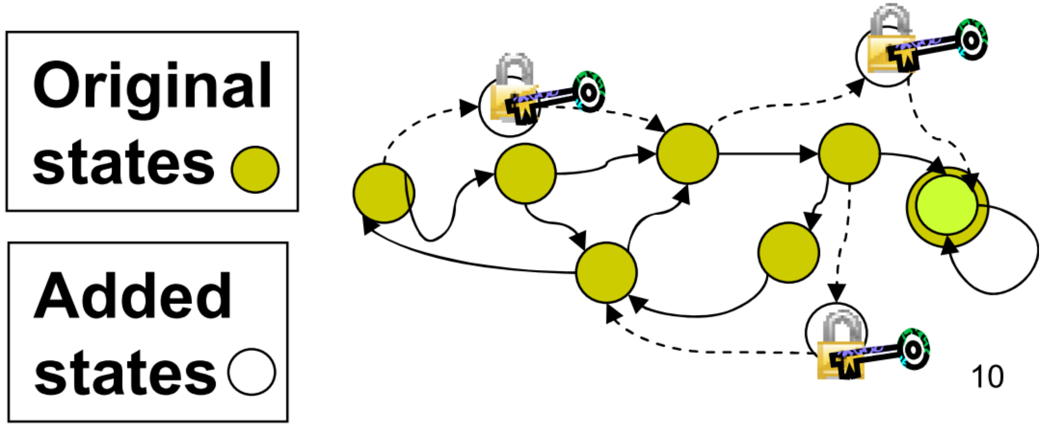
Remote activation of ICs through FSM modification



- Correct transitions give functional output
- Adding states to the FSM gives IP owner controllability over sequence to reach functional states

Counterfeit Detection & Avoidance

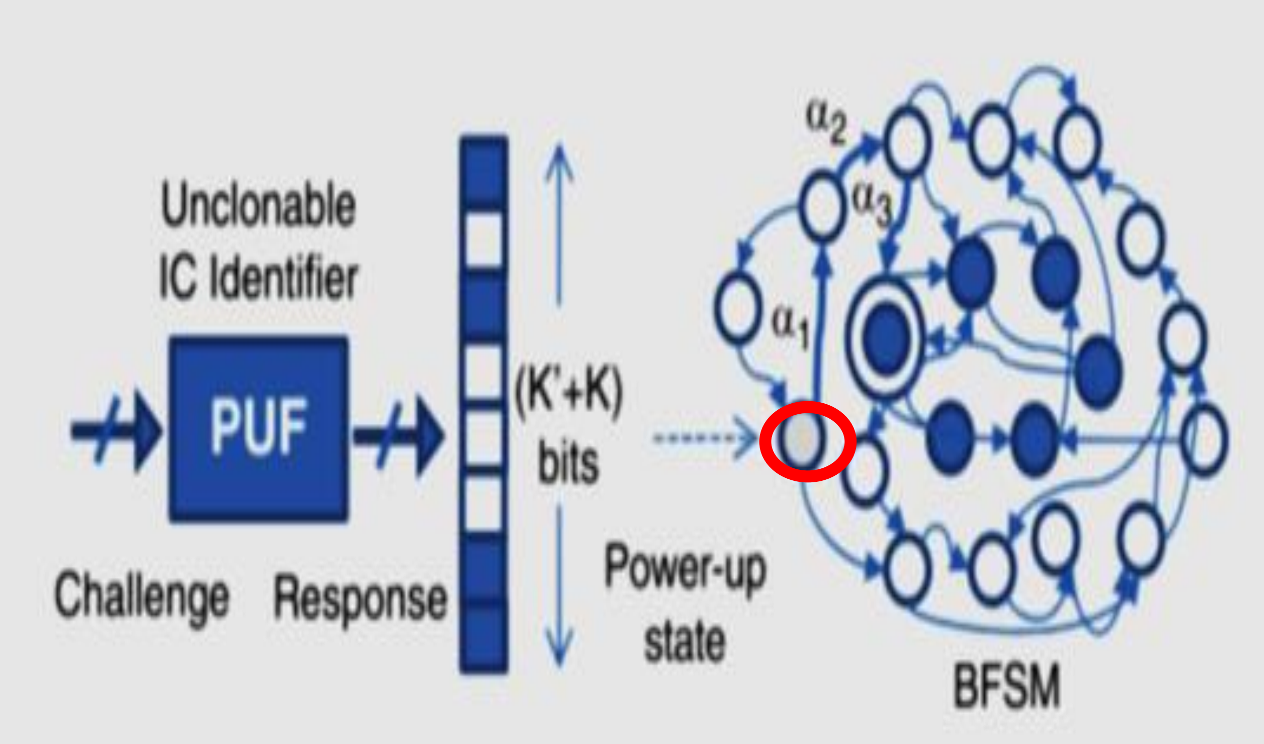
Remote activation of ICs through FSM modification → „Boosted FSM“



- On startup, inputs cause chip to go to one of the (probably) added states
- IP owner is the only one with knowledge of the boosted FSM
- Only IP owner knows right sequence (key) to bring FSM back to functional states → chip activation

Counterfeit Detection & Avoidance

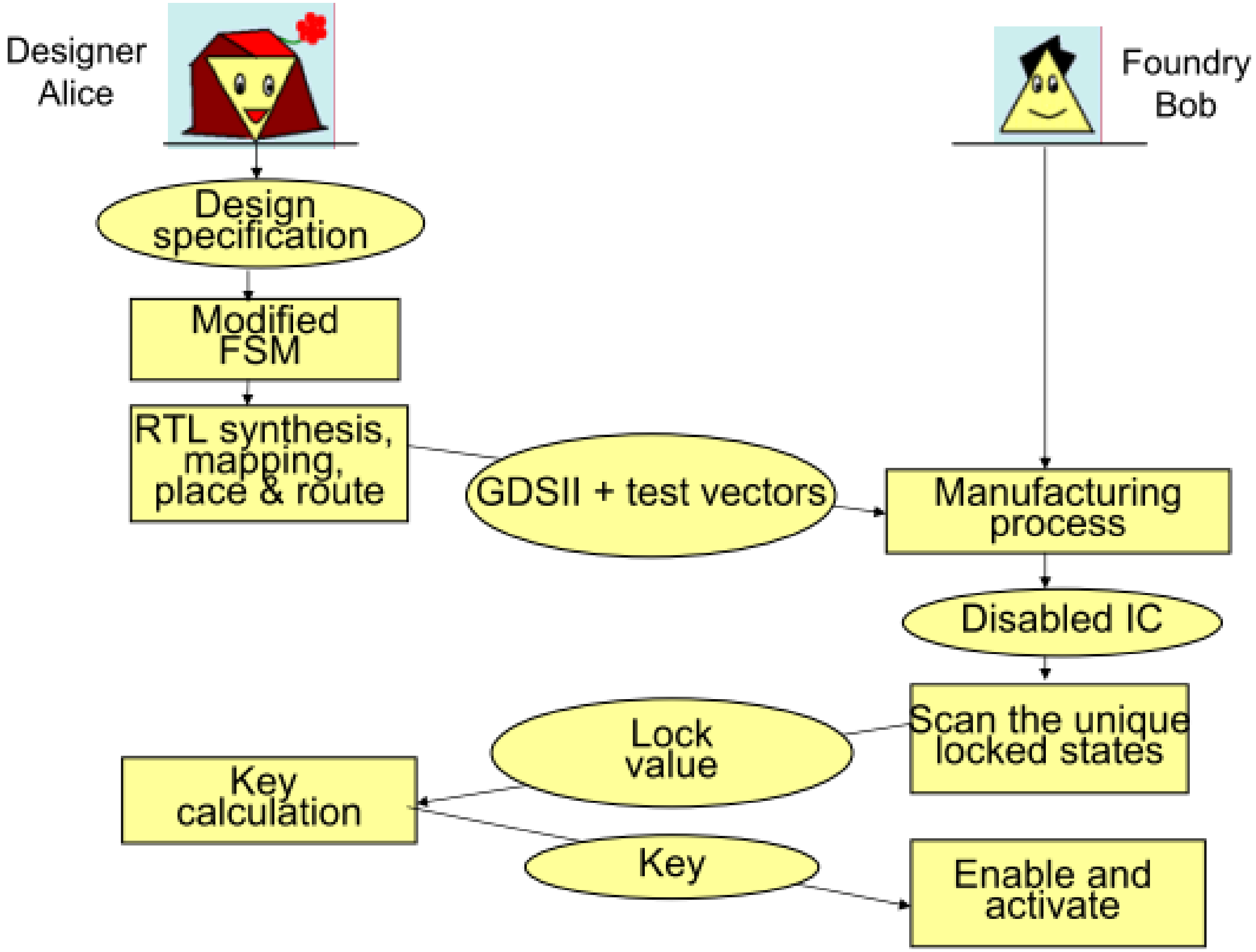
Remote activation of ICs through FSM modification → „Boosted FSM“



- On startup, PUF generates random sequence as input to FSM
- Due to the typically large number of added states, there is a high probability that the starting state will be an added state
- IP owner is the only one with knowledge of the boosted FSM
- Only IP owner knows right sequence (key) to bring FSM back to functional states → chip activation

Counterfeit Detection & Avoidance

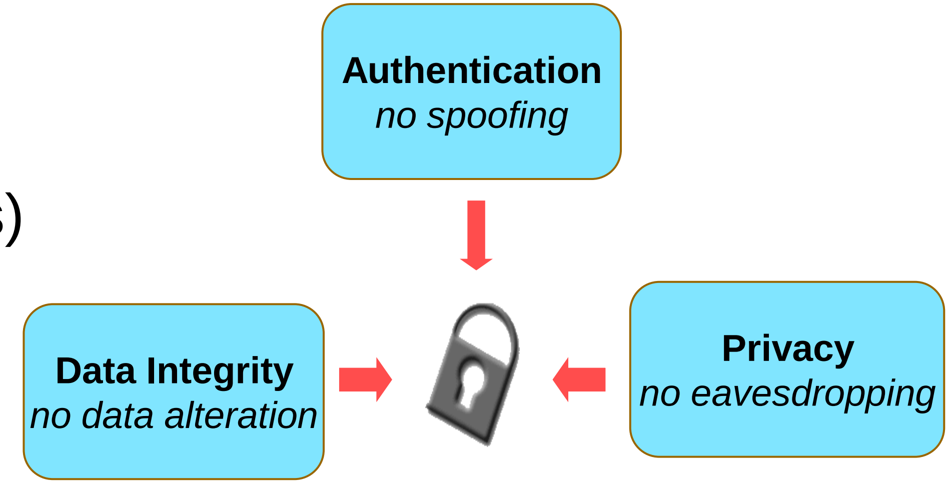
Communication flow during chip production when using remote activation



Security (nicht nur bei Industrie 4.0)

…ist ein sehr breitgefächertes Gebiet mit vielfältigen Aspekten wie u.a.

- Cryptography
- Crypto processor design
- Physical unclonable functions
- Security for “simple” devices (e.g. RFID, smartcards)
- Counterfeit avoidance



Hier anhand einiger weniger Beispiele erläutert!