BITFLIP - Accueil & Introduction

19 nov. 2025
09h25

Réfectoire

Régis LEVEUGLE
Professor Grenoble INP – UGA
TIMA Laboratory

Digital integrated systems' hardening by design: from Reliability and Safety goals to Security, Pitfalls and Challenges

European Cyber Week - The Sovereign Cyber & Defence AI forum, Rennes, France, November 17-20, 2025

Digital integrated systems' hardening by design: from Reliability and Safety goals to Security

Pitfalls and challenges

R. Leveugle

TIMA Laboratory
Grenoble INP - Graduate schools of Engineering and Management
Univ. Grenoble Alpes
France

Context – Pervasive integrated (digital) systems

- An increasingly large panel of application areas …

- … with very different constraints (computation or service complexity and requirements, power/energy efficiency, computation power, acceptable costs, time to market, …
  sources of disturbance and threats, trustworthiness => dependability)

Dependability?

- Notion of service
  - System service: delivered function
  - Correct when it implements the intended/specified system function
- Dependability: alternate definitions
  - Ability to deliver service that can justifiably be trusted
    (=> user confidence, validation/characterization …)
  - Ability to avoid service failures that are more frequent or more severe than is acceptable to the user(s)
- No absolute property

A. Avizienis, J. C. Laprie, B. Randell, "Dependability and its threats: a taxonomy", 18th IFIP World Computing Congress, Topical day 3 "Fault Tolerance for Trustworthy and Dependable Information Infrastructures", Toulouse, France, August 23-24, 2004, pp. 91-120

Various concerns …

The dependability of our systems is a major concern …

… but all electronic systems are at risk due to components (un)reliability and then …

Multi-facet devil!

Particles/Radiations

EM Interferences

Threats?

Bit-flips

Soft errors
(transient errors, remanent errors)
=> SDCs/SDEs, …

SEUs

Not (yet) the whole landscape

… so protections are needed for trustworthiness! => Hardening by design

Bit-flips history, episode 1: particles/radiations

- SEUs in electronics first described during above-ground nuclear testing (1954-1957)
- Then in the 1970s …
  - First SEU paper about Hughes satellite in the IEEE Trans. on Nuclear Science in 1975
    D. Binder, E. C. Smith and A. B. Holman, "Satellite Anomalies from Galactic Cosmic Rays," in *IEEE Transactions on Nuclear Science*, vol. 22, no. 6, pp. 2675-2680, Dec. 1975, doi: 10.1109/TNS.1975.4328188.
  - … but the term was first adopted in 1979
    C. S. Guenzer, E. A. Wolicki and R. G. Allas, "Single Event Upset of Dynamic Rams by Neutrons and Protons," in *IEEE Transactions on Nuclear Science*, vol. 26, no. 6, pp. 5048-5052, Dec. 1979, doi: 10.1109/TNS.1979.4330270.
  - First record of SEU on Ground: Cray-1 Computer at Los Alamos in 1976
    E. Normand *et al.*, "First Record of Single-Event Upset on Ground, Cray-1 Computer at Los Alamos in 1976," in *IEEE Transactions on Nuclear Science*, vol. 57, no. 6, pp. 3114-3120, Dec. 2010, doi: 10.1109/TNS.2010.2083687
  - First evidence of soft errors from alpha particles in packaging materials in 1978
    T. C. May and M. H. Woods, "A New Physical Mechanism for Soft Errors in Dynamic Memories," 16th International Reliability Physics Symposium, San Diego, CA, USA, 1978, pp. 33-40, doi: 10.1109/IRPS.1978.362815

Dependability: historical evolution (attributes)

- Once upon a time …
  - Unreliable components …
  - … then harsh environments

=> Reliability
Continuous correct service
=> Fault Tolerant Computing domain

=> Availability
Probability of correct service at a given time
=> Maintainability

- Increasing use of electronics in critical applications

=> Safety
Avoidance of catastrophic events
May be antagonistic with availability

Hardening

Hardening: main general armored suit collections

Armor?

- Spatial redundancy (DMR, TMR, NMR … systematic, lockstep, partial, w/wo diversification, dynamic, hot or cold spares …)
- Time redundancy (similar variants)
- Information redundancy (codes)
- Checkpointing
- + anti-latchup protection, …
- Multi-level (cross layer), from transistor to SoC
- Hardware and/or software
- Control flow checking
- Assertion-based on-line checking (up to system-level functional assertions)
- Package selection for alpha particles
- …
- Policies: Detection / Tolerance / Detection + Recovery / Masking … taking care of fault accumulation

Beyond natural (external) perturbations?

Multi-facet devil!

Particles/Radiations

EM Interferences

Threats?

PVT variations
+Aging
(+ TID)
(+ e.g., Floating Body Effect in SOI)

Soft errors,
In-field permanent faults
=> SDCs/SDEs, …

And then …

From another world … security!

- Once upon a time …
  - Context of computer networks and software (malware)
  - Concerns limited to information integrity and loss

=> Cybersecurity
Avoidance of unauthorized/improper access or handling of information
Confidentiality, integrity, authentication, authenticity (trusted sources), non-repudiation
May be antagonistic with availability (in all cases, restricted to authorized users)

- Widespread concerns
  - Security can be today one pillar (or prerequisite) for safety in many systems
  - Mission loss can be (at least) as critical as information loss

- Since about two decades … need for Resilience (i.e. robustness)
  - Physical attacks on systems (from smartcard to IoT devices and everything …)
  - … usually with physical access to the devices … but extended to remote attacks …
  - Can be leveraged in a second step to perform remote attacks with wide impact
    => must not be neglected!

=> Hardware security

Bit-flips history, episode 2: towards security concerns

- Seminal paper by Boneh et al. (1997) showed that faults can be catastrophic for cryptosystems – fault attack on RSA deciphering engine

D. Boneh, R.A. DeMillo, R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in: Fumy W (ed) Advances in cryptology – EUROCRYPT'97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, 11–15 May, 1997, Lecture notes in computer science, vol 1233. Springer, pp 37–51. doi: 10.1007/3-540-69053-0_4.

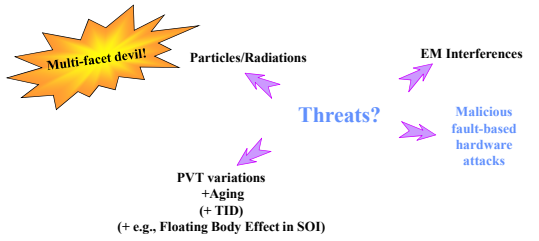
- Another reference paper on early fault attack on RSA

M. Joye, A.K. Lenstra, J.J. Quisquater, "Chinese remaindering cryptosystems in the presence of faults," Journal of Cryptology, Vol.12, pp.241-245, 1999.

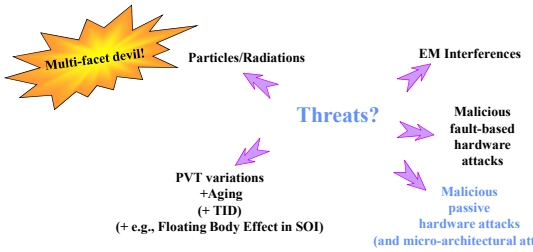
=> "Bellcore attack"

- New security threat: bit-flip(s) … often assumed as "single" in early literature

New bit-flip origins …



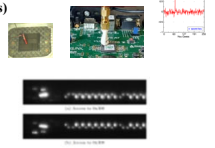
… but are hardware attacks looking only like soft errors?



Wide panel of physical attacks

- Invasive and/or destructive (probing, reverse engineering, …)
- Active, perturbation Fault-based, FAs
  - Global perturbation temperature voltage overclocking …
  - Local perturbation (time) power glitch clock glitch …
  - Local perturbation (space and time) lasers EM pulses … → Most efficient exploitation

- Passive, observation Side channels, SCAs
  - Execution time (TA)
  - Power consumption (SPA, DPA, CPA, …)
  - EM emissions (SEMA, DEMA, …)
  - Light (photons)
  - Heat
  - Sound
  - …



Hardware security: enlarged set of armored suits

- Specific active protections
  - Sensors (voltage levels, glitch, light, temperature, …)
  - On-chip encryption of data
  - Random desynchronizations
  - …
- Specific design methodology
  - Internal clock generation (problem with testing requirements!)
  - Restrictions in design styles (dynamic logic, …)
  - Shielding
  - Protection grid (active) against probing
  - Memory and/or bus scrambling
  - …

Multi-level:
- Software
- OS
- Hardware

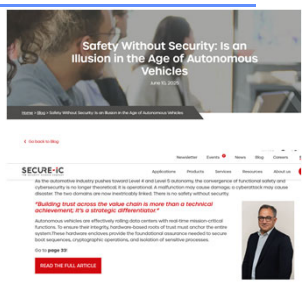
Examples of safety/security links in literature

- Identified since several decades, but …
- "Security" mostly understood as cybersecurity (software/communications)
- Focused on some application domains (mainly industrial control systems, advance manufacturing, then aerospace, automotive …)

Increasingly found at the forefront

Achieving Safety AND Security

Clearly an increasing concern and an up-to-date challenge



https://ebooks.aspencore-media.eu/eetimes/2025/june/index.html

Security vs. Reliability/Safety

- Different communities, different backgrounds, most often different teams in industry
  - No unique terminology (and depends on the application domain)
  - Difficulty of communication and identification of common or conflicting concerns
- Most often, hardening tasks are tackled separately
- In the literature, contributions are most often focused on one aspect (and even a subset!)

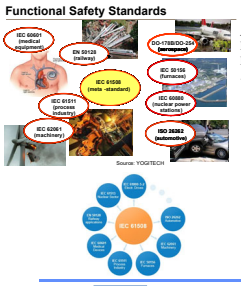
Question:
Are R&S-oriented design hardening measures beneficial from the security point of view, and up to what extent?

Several sub-questions

- Are R&S-oriented design hardening measures sufficient for security (at least to counter fault attacks)?
- Are design for R&S and design for security just complementary?
- Is hardening against faults always beneficial for security?
- …

Are R&S-oriented design hardening measures sufficient for security (at least to counter fault attacks)?

Functional safety – many standards



And:
IEC 62279 - Railways
ISO 13849 - Machinery
…

Functional safety:
absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical/electronic systems

Standards include best practices AND robustness level requirements e.g., ASIL A to D in ISO 26262

=> Hardening by design
e.g., dual core lockstep for ASIL-D

Hardening against faults – assume job done for R&S!

- And then … security! Dream or nightmare?

From usual literature …

Job is done for FAs!

"Just" add SCA countermeasures

(methods will not be detailed in this talk)

Observation on state-of-the-art literature:

Large majority of studies dealing with either FA or SCA (exclusively)

Assuming FA and SCA fighting are two independent (fully complementary) jobs

Hardening against faults – assume job done for R&S!

- And then … security! Dream or nightmare?

From usual literature …

Job is done for FAs!

"Just" add SCA countermeasures

(methods will not be detailed in this talk)

In fact … not so simple!

Is the protection sufficient to counter all FAs (or limited percentage? What fault models?)
Efficiency of combining several countermeasures?
What about the level of leaks? Would SCA sensitivity be worsen?
(+ specific security armors)
…

Hardening for R&S is NOT sufficient to counter all FAs!

Threat characteristics: fault models to be revisited

- **Reliability and Safety**
  - Natural events, "Hazards"
  - Unintentional
  - Pre-determined behavior (physics)
  - Thoroughly analyzed and modeled
  - Often a low occurrence rate
  - One-shot
  - General context rather stable, established fault models
- **Security**
  - Attacks
  - Intentional, malicious
  - Multiple ways to reach the goal, New attacks everyday
  - Multiple trials, hacker learning curve
  - Statistical approaches cannot easily be adopted for characterization (too little data shared in real time)
  - Specific equipments (nuisance capacity larger than natural events)

Are design for R&S and design for security just complementary?

Is hardening against faults always beneficial for security?

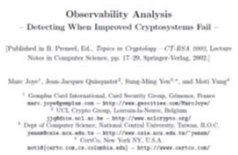
Secure composability
of different attack countermeasures

"Security paradox":

where attempts to strengthen security against some attacks can actually weaken the overall security of the system

Already identified in 1999-2002 (algorithm level)

- **Joye's Observability Analysis**


Observability Analysis
– Detecting When Improved Cryptosystems Fail –

Before:
M. Joye et al., "Security paradoxes: how improving a cryptosystem may weaken it", National Conf. on Information Security, Taichung, Taiwan, May 1999

Abstract. In this paper we show that, paradoxically, what looks like a "universal improvement" or a "straight-forward improvement" which enables better security and better reliability on a theoretical level, may in fact, within certain operational contexts, introduce new exposures and attacks, resulting in a weaker operational cryptosystem. We demonstrate a number of such dangerous "improvements". This implies that careful considerations should be given to the fact that an implemented cryptosystem exists within certain operational environments (which may enable certain types of tampering and other observed information channels via faults, side-channel attacks or behavior of system operators). We use our case studies to draw conclusions about certain investigations required in studying implementations and suggested improvements of cryptosystems; looking at them in the context of their operating environments (combined with their potential adversarial settings). We call these investigations *observability analysis*.

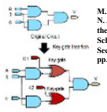
M. Joye, J.-J. Quisquater, S.-M. Yen, M. Yung, "Observability analysis: Detecting when improved cryptosystems fail PDF."
In B. Preneel, Ed., Topics in Cryptology – CT-RSA 2002, vol. 2271 of Lecture Notes in Computer Science, pp. 17-29, Springer-Verlag, 2002

Error detection is leaking secrets

- **First Joye's paradox on RSA computations: an identified error (leading to an error message ending the encryption) allows inferring the value of the secret key without choosing plaintexts and ciphertexts, so allows successful attacks under weaker assumptions than without detection ("oracle" – differences in system behavior can be observed, leaking information on inner workings)**
- **Similar to "safe-error" hardware attacks: undetected errors (or errors not modifying the final result) leak inner data values**
  - **Simple example: forcing a secret bit at a given value with/without impact on the result leaks the value the bit had**
  - **Other case: used/unused modified data can leak the executed branch of a program, thus the condition value**
- **Re-computing after detection is not a solution: it is revealed by a timing analysis**
- **Behavior observation but … What about other leaks?**

Interlude - Enlarged view: beyond error management …

- Same kind of paradox in other contexts
- Other protections can lead to new (or easier) attacks …
- Example: concerns with supply chain and outsourcing of manufacturing to (untrustworthy) offshore foundries
  - Trojan insertions
  - Cloning (counterfeiting) / over-production
  - One answer? Logic locking (secret key inputs)



M. T. Rahman, S. Tajik, M. S. Rahman, M. Tehranipoor, N. Asadizanjani, "The Key is Left under the Mat: On the Inappropriate Security Assumption of Logic Locking Schemes," IEEE Int. Symposium on Hardware Oriented Security and Trust (HOST), San Jose, CA, USA, 2020, pp. 262-272

- But … limitation (key recovery by SCA) and LEDFA (Locking-Enabled DFA): DFA on incorrectly unlocked cryptographic circuits can be simpler than on regular circuits without logic locking

D. Upadhyaya, M. Gay, I. Polian, "Locking-Enabled Security Analysis of Cryptographic Circuits," Cryptography. 2024; 8(1):2

Protecting assets

- Looking at the weaker link in the chain … even if not the most easily accessible
- Any vulnerability, or decrease in resistance, even patched, can help intrusion
- Most often neglected in the literature in the context of FA fighting (not saying it is unknown …)

Worst point: fighting FAs can reduce SCA fighting efficiency

- Little existing literature … Starting point at TIMA (2006-2009 … V. Maingot thesis)
- Then
  - From 2007 - F. Regazzoni (Lugano, Switzerland), T. Eisenbarth (Bochum, Germany), L. Breveglieri (Milano, Italy), P. Ienne (EPFL, Lausanne, Switzerland), I. Koren (Amherst, USA)
  - 2009 – J. Dai and L. Wang (Connecticut, USA)
  - 2014 – P. Luo et al. (Boston, USA)
  - 2016 – H. Pahlevanzadeh, J. Dofe, and Q. Yu (New Hampshire, USA)
  - 2017 – J. Riha, V. Miskovsky, H. Kubatova, and M. Novotny (Prague, Czech republic)
  - 2021 – F. Almeida, L. Aksoy, J. Raik, and S. Pagliarini (Tallinn, Estonia)
  - 2025 – I. Kabin, P. Langendoerfer, and Z. Dyka (IHP Frankfurt & Cottbus, Germany)

R. Leveugle, "Embedded tutorial: Integrated system hardening seen from a security point of view: dream or nightmare?" IEEE Latin American Test Symposium (LATS), San Andrés Island, Colombia, March 11-14, 2025

Main subjects covered in previous studies

- Mainly on register or AES (Sbox + register, then full AES) case study
- From gate level … to transistor level … to FPGAs
- From DPA … to CPA
- From error detecting/correcting codes … to DMR / TMR …

Interlude – Is cryptography the only relevant context?

- Pervasive development of AI-powered embedded systems
- Also in critical domains, from automotive to defence (see ECW program!) and many others
- Attacks on neural networks: no secret key to find, but …
  - Fault attacks
    - Global misclassifications: model accuracy reduction, system efficiency decrease
    - Selective misclassifications of a specified input pattern into an adversarial class
    - Extraction of Embedded Neural Network Models

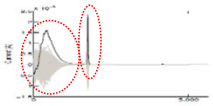
Hector, K., Moëllic, PA., Dutertre, JM., Dumont, M. (2024). Fault Injection and Safe-Error Attack for Extraction of Embedded Neural Network Models. In: Katsikas, S., et al. Computer Security. ESORICS 2023. Lecture Notes in Computer Science, vol 14399. Springer, Cham.

  - SCA attacks
    - Retroengineering, architecture and parameter extraction
    - Mimic a system with a substitute model, even with a limited access to similar training data

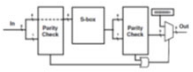
Batina, L., Bhasin, S., Breier, J., Hou, X., Jap, D. (2022). On Implementation-Level Security of Edge-Based Machine Learning Models. In: Batina, L., Bäck, T., Buhan, I., Picek, S. (eds) Security and Artificial Intelligence. Lecture Notes in Computer Science, vol 13049. Springer, Cham. https://doi.org/10.1007/978-3-030-98795-4_14

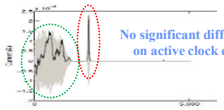
Kocher's DPA attack on AES S-box

Reference implementation of the AES S-box



AES S-box with added complementary parity



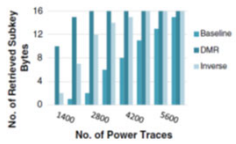


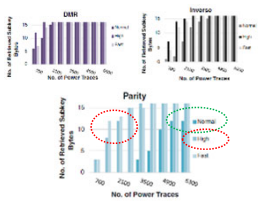
No significant difference on active clock edge

F. Regazzoni, L. Breveglieri, P. Ienne, I. Koren, "Interaction Between Fault Attack Countermeasures and the Resistance Against Power Analysis Attacks," In: Joye, M., Tunstall, M. (eds) Fault Analysis in Cryptography. Information Security and Cryptography. Springer, Berlin, Heidelberg, 257-272, 2012

Attack tuning matters!

CPA attack of the entire AES on FPGA





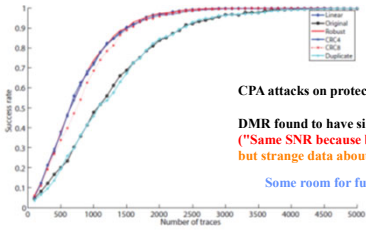
Dual Modular Redundancy clearly accelerates attack success

Round-level inverse function also degrades security w.r.t. CPA

Synthesis effort has also a strong impact
High effort is counterproductive w.r.t. security

J. Dofe, H. Pahlevanzadeh, Q. Yu, "A comprehensive FPGA-based assessment on fault-resistant AES against correlation power analysis attack," Journal of Electronic Testing, 32, 611-624, 2016

Some results sometimes contradictory!



CPA attacks on protected AES implemented on FPGA

DMR found to have similar characteristics as Reference
("Same SNR because both signal and noise are doubled")
but strange data about FPGA resources – synthesis effects?

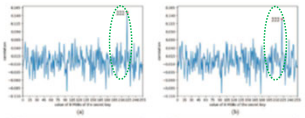
Some room for further works!

P. Luo, Y. Fei, L. Zhang, A. A. Ding, "Side-channel power analysis of different protection schemes against fault attacks on AES," IEEE International Conference on ReConFigurable Computing and FPGAs (ReConFig14), Cancun, Mexico, 2014

Case of TMR: example of AES

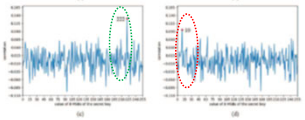
Key guess:

Reference (single, unprotected)



TMR 3 identical AES blocks

TMR 3 physically different AES blocks (physical synthesis)



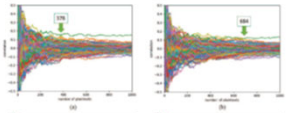
TMR 3 structurally and physically different AES blocks

E. Almeida, L. Aksoy, J. Raik, S. Pagliarini, "Side-Channel Attacks on Triple Modular Redundancy Schemes," IEEE 30th Asian Test Symposium (ATS), Matsuyama, Ehime, Japan, 2021, pp. 79-84

Case of TMR: CPA on AES => diversity

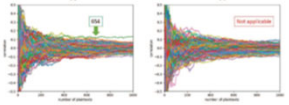
Number of plaintexts necessary to discover the 8 MSBs of the secret key:

Reference (single, unprotected)



TMR 3 identical AES blocks

TMR 3 physically different AES blocks (physical synthesis)



TMR 3 structurally and physically different AES blocks

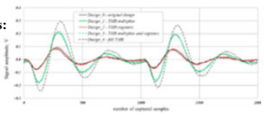
E. Almeida, L. Aksoy, J. Raik, S. Pagliarini, "Side-Channel Attacks on Triple Modular Redundancy Schemes," IEEE 30th Asian Test Symposium (ATS), Matsuyama, Ehime, Japan, 2021, pp. 79-84

New! Asymmetric cryptography and EM traces

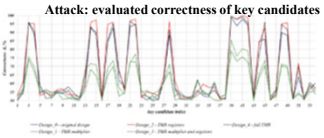
Late News

- Full or partial TMR versions of a hardware accelerator for Elliptic Curve point multiplication

Traces:



Attack: evaluated correctness of key candidates



- Findings: TMR increases leakage and
  - Full redundancy or selective redundancy of registers (key dependent): make SCA attacks more successful and easier
  - Selective redundancy of the multiplier (high power consumption, active each cycle, resistant to DPA): increases noise, reduces the design's vulnerability by masking key-dependent operations

I. Kabin, P. Langendoerfer, Z. Dyka, "On the SCA Resistance of TMR-Protected Cryptographic Designs," Electronics. 2025; 14(16):3318

Conclusion on current literature survey

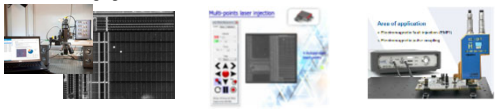
- A few pioneer works, but …
- Many questions remain open, not limited to:
  - Some contradictory conclusions to be revisited/strengthened
  - Impact of synthesis optimizations: what level of trade-off with SCA vulnerability?
  - Separable vs. non-separable codes? Self-checking codes (dual rail, also for power balancing)?
  - Almost limited to AES (or very few ciphers) – what about other functions?
  - Limited to DPA/CPA – what about EMA/DEMA?

=> a lot to do!

… including tool support (protection insertion, synthesis, DfT, P&R, …), still more critical than for "just" R&S-oriented hardening

… and concerns are not limited to FAs vs. SCAs

- More concerns related to implementation …
- Recall: attack equipments can induce more nuisance than natural causes



- Usual hardware space redundancy at risk
  => P&R obfuscation
- Usual time redundancy at risk
  => time distribution obfuscation

Other motivations for diversity!
…
at the expense of costs and TTM

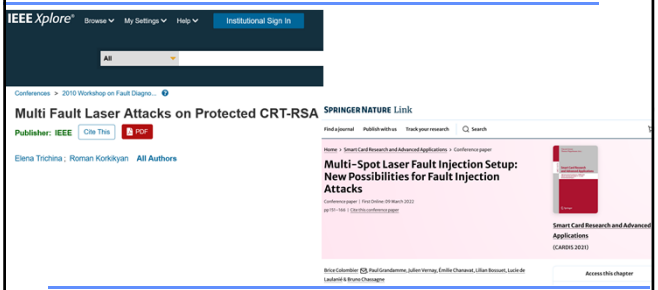
Multi-point injections: setup example, 2 independent points

https://www.alphanov.com/produits-services/injection-de-fautes-laser-double

Multi-point injections: setup example, 4 independent points

https://www.errol-laser.com/smart-cart-laser-bench
https://www.errol-laser.com/_files/ugd/1c6d8e_1e3b60623c454f02b125c891cd53a245.pdf

Exploiting multi-injections with lasers



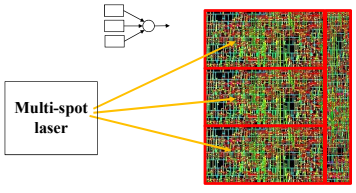
Also available for EMFI, sequence of 2 pulses

Also for Body Bias Injection (BBI)

https://www.langer-emv.de/en/product/fault-injection/116/ici-dp-hh250-15-set-double-pulse-magnetic-field-source-set/1424

Impact on space redundancy

- Malicious, with 4-spot laser station => multiple spatial faults impossible after natural events can be induced



3 copies of the same layout box
=> synchronized attacks at the same location in the 3 boxes
=> TMR defeated without any knowledge on the detailed block functionality

Layout scrambling and/or diversity
not critical for just usual fault tolerance but necessary for security-oriented TMR (in addition to impact on SCAs)

- Identification can be made easier with today's AI-based techniques

Impact on time redundancy

- Malicious, with 1-spot laser station => multiple timing faults impossible after natural events can be induced if fast enough triggering

Example: Duplicated operations in pipeline

Computation step	1	2	3	4	
Duplication	Op1	Op1bis	Op2	Op2 bis	Undetected?
Optimized duplication for long effects	Op1	Op2	Op1bis	Op2 bis	Detected

X-cycle perturbation (maybe natural)

Multiple 1-cycle perturbations

Diversity to avoid identical errors — Undetected?

Diversity to avoid synchronization — Undetected?

Design flow: optimizations, avoiding flaws at all levels

A very sketchy view …

- Specification — R&S and security requirements, TTM requirements!!
- Behavioral design (System/HLS/RTL) — Careful choice of hardening techniques for global efficiency, diversification of replicas
- Gate-level design
- Transistor-level design — Cell-level optimizations
- Synthesis Netlist — Careful control for redundancy preserving and adapted optimization level
- DfT insertion — Protected access to DfT mechanisms, Defensive scan
- Physical synthesis, Placement & routing — Diversified P&R, optimized scrambling

Design hardening and security: short summary

- Information redundancy: many concerns, choice must be very careful!
- Spatial redundancy: diversity advocated for DMR/TMR … both structural and physical, better for both multi-point fault attacks and SCA difficulty
- Time redundancy: diversity also better and more efficient for all targets (including faults in FPGA configuration memory), better to avoid synchronization AND identical fault effects on replicas
- Actions required at all levels in the design flow
- Trade-offs with TTM and costs …
- Need for more unified FA/SCA hardening approaches

Interlude - Security concerns: enlarged overview

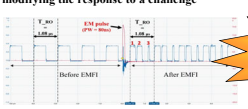
- In addition to main functions and secrets, various attack targets and attack ways e.g.,
- Reconfigurable hardware "downgrade", removing security "patches"
- Concerns related to supply chain and Life Cycle management
  - Hardware Trojans: hardware spys / wireless reporting, hidden "bombs", hidden features …
  - IC cloning (counterfeiting) / over-production (over-building)
  - Fraud in IC recycling: refurbished ICs
- And others!
- Additional protections
  - Version management
  - Unique identification => PUFs
  - Many security features based on random numbers => TRNGs

But security primitives can also be attacked

- PUFs …

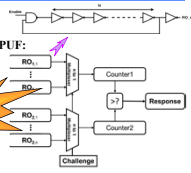
Example based on Ring Oscillators

EM attacks can modify the oscillation frequency of ROs (locked harmonic error), modifying the response to a challenge

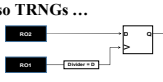


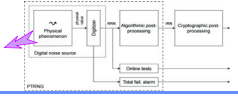
Here also Bit-flips are a threat!

RO-PUF:



- … and also TRNGs …





Conclusion and perspectives

- Strong relationships between hardening against SEEs and security enforcement
- … and variability, aging effects, SDC/SDEs and other concerns discussed in the dependability community, are also very relevant from the security point of view
- Conflicting goals between usual hardening and security must be managed (redundancy vs. side channels but also e.g., safety vs. deny of service)
- Increasing concern: ensuring a coherent global optimization of hardening

A more holistic design practice has to be worked out!

Vast subject – a lot of work and perspectives!