Journée thématique sur les attaques par injection de fautes
Grenoble, France, October 1, 2025

Protection contre les fautes : est-ce bien toujours une bonne action pour la sécurité ?

Protections against faults (design hardening): is it always a good action for security?

R. Leveugle

TIMA Laboratory

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

Provocative?

- Yes, just a bit
- But not looking for a controversy …
- Just wanting to highlight a few points, mainly
  - Usual design hardening practice is not sufficient when security is a concern
  - Worst: it can be counterproductive from a global point of view
  - Lack of holistic (hardware) design practices
  - Only a few studies on this axis since 20 years … but interesting insights

About faults

- Are fault attacks a real concern? Of course, yes.
- Are faults only a (hardware) security concern? Of course, no.
  Reliability, availability, safety are older concerns.
- Well established approaches against faults exist … but security has multiple facets and this should not be neglected.

Disclaimer

In the sequel, focus is mainly on hardware hardening

Hardening against fault attacks – usual literature

- Job done for R&S?

  Job is done for FAs!

  … "Just" add SCA countermeasures

- Otherwise : see hereafter!

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: main general armored suit collections

Multi-level (cross layer), from transistor to SoC

Hardware and/or software

Spatial redundancy (DMR, TMR, NMR … systematic, lockstep, partial, w/wo diversification, dynamic, hot or cold spares …)

Time redundancy (similar variants)

Information redundancy (codes)

Checkpointing

Armor?

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

+ anti-latchup protection, …

Assume job done from R&S perspective!

- And then … security!

Dream?

Or nightmare?

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

- **Reliability and Safety**
  - **Natural events, "Hazards"**
  - **Unintentional**
  - **Pre-determined behavior (physics)**
  - **One-shot**
  - **General context rather stable, established fault models**

- **Security**
  - **Attacks**
  - **Intentional, malicious**
  - **Multiple ways to reach the goal, specific equipments (nuisance capacity larger than natural events)**
  - **Multiple trials, hacker learning curve**
  - **Different types of hardware attacks (micro-architectural, FAs, SCAs, …)**
    => a large panel of different threats
    => the easiest is the right one for the hacker

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)

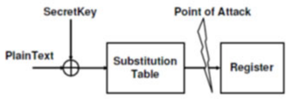
R. Leveugle, "Embedded tutorial: Integrated system hardening seen from a security point of view: dream or nightmare?" IEEE Latin American Test Symposium (LATS), San Andrés Island, Colombia, March 11-14, 2025

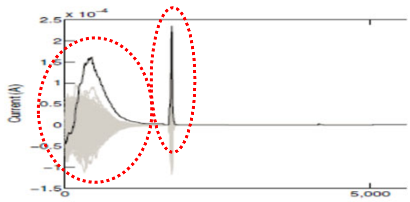
Main subjects covered in previous studies

- 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 …

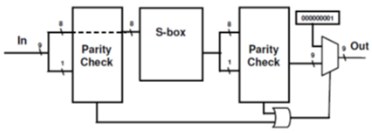
Kocher's DPA attack on AES S-box

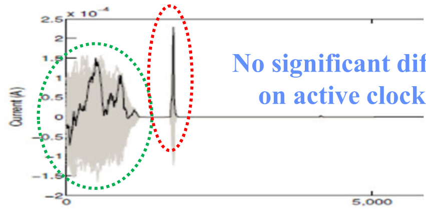
Reference implementation of the AES S-box





AES S-box with added complementary parity





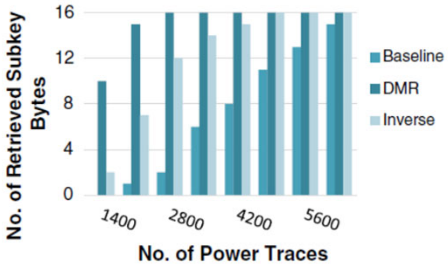
No significant difference on active clock edge

Attack tuning matters!

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

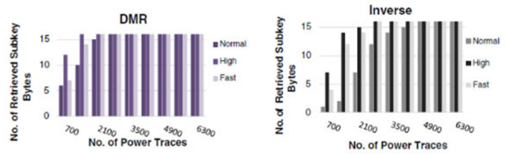
R. Leveugle, TIMA / AMfoRS

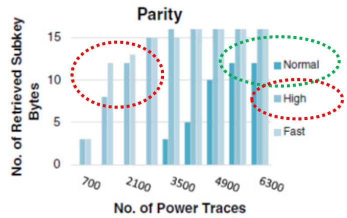
CPA attack of the entire AES on FPGA



Dual Modular Redundancy
clearly accelerates attack success

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

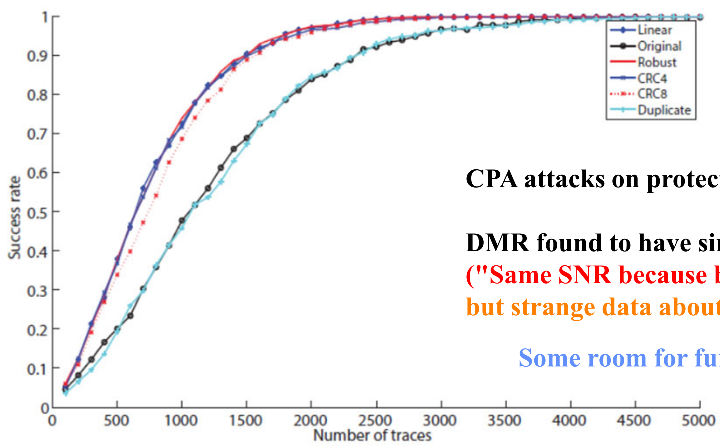




Synthesis effort has also a strong impact
High effort is counterproductive w.r.t. security

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

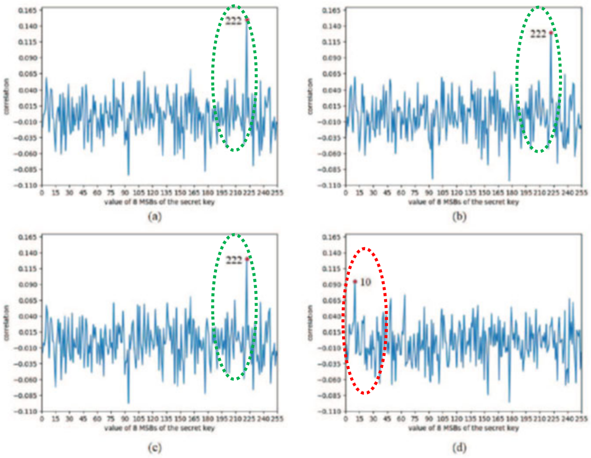
Key guess:

Reference (single, unprotected)

TMR 3 identical AES blocks

TMR 3 physically different AES blocks (physical synthesis)

TMR 3 structurally and physically different AES blocks



F. 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

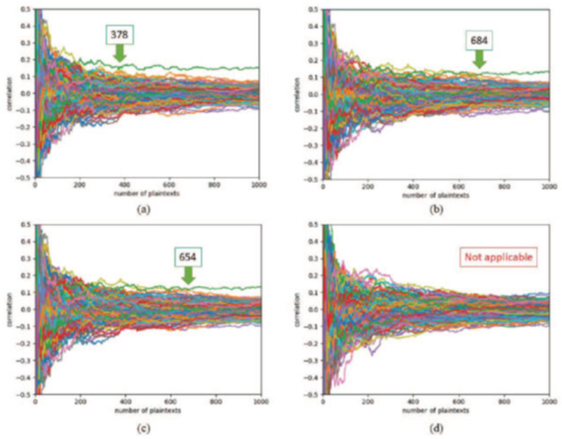
Number of plaintexts necessary to discover the 8 MSBs of the secret key:

Reference (single, unprotected)

TMR 3 identical AES blocks

TMR 3 physically different AES blocks (physical synthesis)

TMR 3 structurally and physically different AES blocks



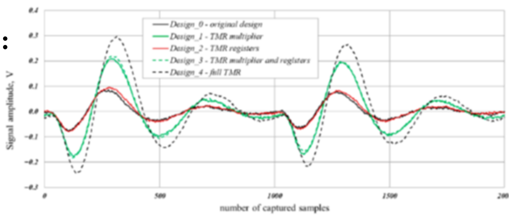
F. Almeida, L. Aksoy, J. Raik, S. Pagliarini, "Side-Channel Attacks on Triple Modular Redundancy Schemes," IEEE 30th Asian Test Symposium (ATS), Matsuyama, Ehime, Japan, 2021, pp. 79-84

New!   Asymmetric cryptography and EM traces

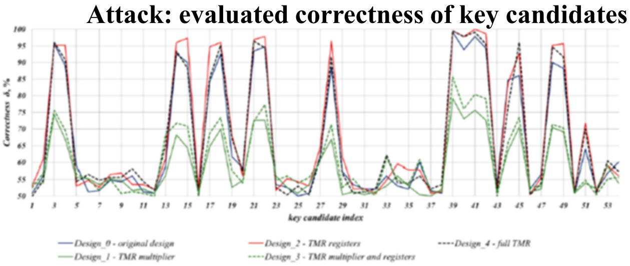
Late News

- 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

TiMA   R. Leveugle, TIMA / AMfoRS   AMfoRS

Some other studies and findings

- Other evaluation approach (2009): impact of the choice of the code confirmed using information theory and the computation of mutual information for a protected memory – here, a parity encoding is found making a memory less vulnerable to side-channel leakage by power analysis, while opposite trends are reported for the Hamming and BCH codes

- Studies also demonstrated (2017-2018) that time/space redundancy techniques applied for AES at the software level on microcontrollers are inherently leaky

- More details and references in:

R. Leveugle, "Embedded Tutorial: Integrated System Hardening Seen from a Security Point of View: Dream or Nightmare?," IEEE 26th Latin American Test Symposium (LATS), San Andres Islas, Colombia, 2025, pp. 1-4, doi: 10.1109/LATS65346.2025.10963950.

TiMA   R. Leveugle, TIMA / AMfoRS   AMfoRS

Conclusion on current literature survey

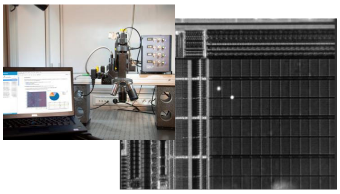
- A few pioneer works, but …
- Many questions remain open, not limited to:
  - Some contradictory conclusions to be revisited/strengthened
  - Impact of synthesis optimizations: what level of trade-off with SCA vulnerability?
  - Separable vs. non-separable codes? Self-checking codes (dual rail, also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

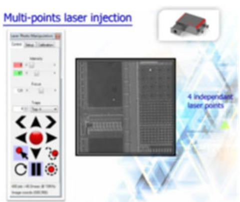
=> a lot to do!

… 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 hardening vs. SCAs

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



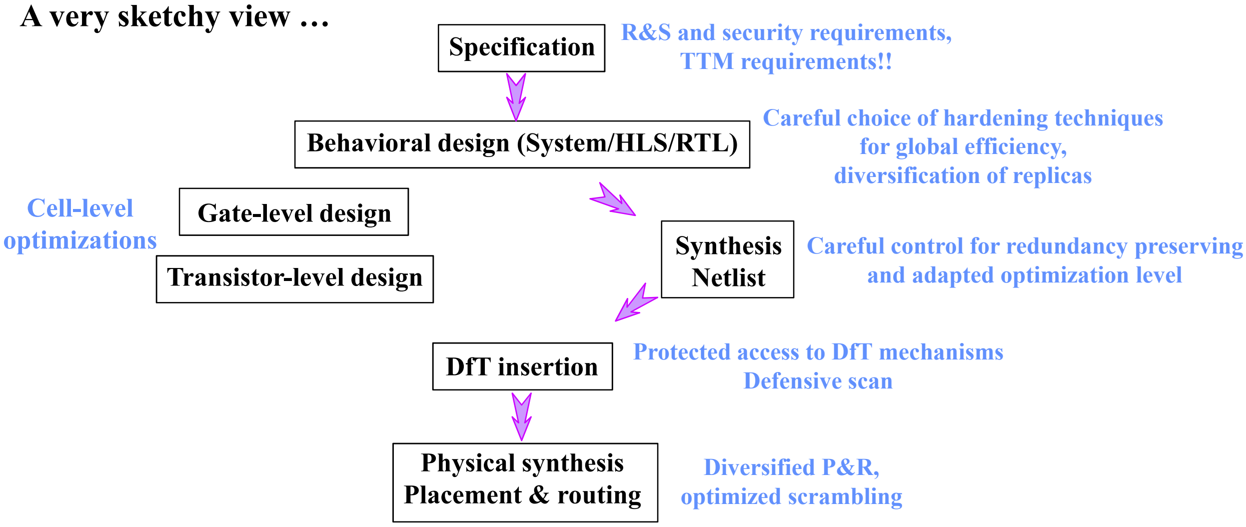


- Usual hardware space redundancy at risk
  => P&R obfuscation
- Usual time redundancy at risk
  => time distribution obfuscation

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

Design flow: optimizations, avoiding flaws at all levels

A very sketchy view …



Conclusion and perspectives

- **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 – good news: a lot of open questions, a lot of research perspectives!